Technical University of Denmark

Written exam, the 15th of December 2020

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

Aid: All Aid including access to internet

“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 $(S_6, \circ)$ be the symmetric group on 6 letters and consider the permutation $f = (1\,2\,3)(3\,4\,5)(4\,5\,6)$ from S_6.

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

b) What is the order of the permutations f?

c) What is the maximal order a permutation of S_6 can have? Motivate your answer.

Question 2

Let $(G, \cdot)$ be a group and $\psi : G \to G$ a group homomorphism.

a) Show that the set $\{g \in G \mid \psi(g) = g\}$ is a subgroup of $(G, \cdot)$.

b) Now let $(G, \cdot) = (D_6, \circ)$, where $(D_6, \circ)$ denotes the dihedral group of order 12. Further let $\varphi : D_6 \to D_6$ be the map defined as $\varphi(g) = s \circ g \circ s$, where as usual $s \in D_6$ corresponds to reflection in the x-axis. Show that φ is a group homomorphism.

c) Let $\varphi : D_6 \to D_6$ be the same as in part b). Determine $\{g \in D_6 \mid \varphi(g) = g\}$.

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 $\mathbb{F}_5$. Further define the quotient ring $(R, +, \cdot)$, where $R := \mathbb{F}_5[X]/\langle X^3 + X - 2\rangle$.

a) How many elements does R contain?

b) Does R contain zero divisors? Motivate your answer.

c) Show that $X^2 + \langle X^3 + X - 2\rangle$ is a unit of R and compute its multiplicative inverse.

d) Determine how many units R contains.

Question 4

Define the set Gaussian integers $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$. You may use in this exercise that $(\mathbb{Z}[i], +, \cdot)$ is a ring, where $+$ and $\cdot$ denote the usual addition and multiplication of complex numbers. Further, let $\psi : \mathbb{Z}[i] \to \mathbb{Z}_2$ be the map defined by $\psi(a+bi) = (a+b) \mod 2$.

a) Show that ψ is a ring homomorphism.

b) Show that the kernel of ψ is equal to the ideal $\langle 1+i \rangle$ of $\mathbb{Z}[i]$. Hint: you might need the equality $2 = (1+i)(1-i)$.

c) Let $n \in \mathbb{Z}$ be a positive integer. Show that $|\mathbb{Z}[i]/\langle n \rangle| = n^2$.

END OF THE EXAM