Exam 2019- answers

Question 1

a) We write first f_1 and f_2 as compositions of disjoint cycles as: $f_1 = (123)(38) = (1238)$ and $f_2 = (13)(23)(24)(34) = (13)(24)$. Then $f_1 \circ f_2 = (1238)(13)(24) = (18)(243)$.

b) We recall that for $f \in S_n$, if $f = c_1 \circ c_2 \circ \ldots \circ c_k$ is the disjoint cycles decomposition of f and c_i is a cycle of length ℓ_i for $i = 1, \ldots, k$ then $ord(f) = lcm(\ell_1, \ldots, \ell_k)$. From part a) we get that $ord(f_1) = 4$, $ord(f_2) = lcm(2,2) = 2$ and $ord(f_1 \circ f_2) = lcm(2,3) = 6$.

c) Yes. It is enough to consider the 8-cycle (12345678).

d) **YOU CANNOT ANSWER THIS QUESTION!** Indeed the notion of even and odd permutations is not anymore part of the curriculum of the course.

Question 2

a) We need to check, by definition, that $\varphi(0) = 0$ and $\varphi(a +_8 b) = \varphi(a) +_8 \varphi(b)$ for all $a, b \in \mathbb{Z}_8$. Just by using the definition we see that the first condition hold:

$$\varphi(0) = 0 +_8 0 = 0.$$

For the second condition let $a, b \in \mathbb{Z}_8$ arbitrary. Then by definition

$$\varphi(a +_8 b) = (a +_8 b) +_8 (a +_8 b),$$

using associativity and commutativity of $+_8$ we get that

$$(a +_8 b) +_8 (a +_8 b) = a +_8 b +_8 a +_8 b = a +_8 a +_8 b +_8 b = (a +_8 a) +_8 (b +_8 b),$$

which is by definition of φ exactly equal to $\varphi(a) +_8 \varphi(b)$. Hence φ is a group homomorphism.

b) We start by computing the Kernel,

$$\ker(\varphi) = \{a \in \mathbb{Z}_8 \mid \varphi(a) = a +_8 a = 2a \pmod 8 = 0\}.$$

Since $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and $2a \pmod 8 = 0$ if and only if 8 divides $2a$, that is, 4 divides a we get

$$\ker(\varphi) = \{a \in \{0, \ldots, 7\} : 4|a\} = \{0, 4\}.$$

To compute the image, we start by using its definition

$$Im(\varphi) = \{\varphi(a) = a +_8 a \mid a \in \mathbb{Z}_8\} = \{2a \pmod 8 \mid a \in \{0, \ldots, 7\}\}.$$

Computing all possible $2 \cdot a \pmod 8$ with $a = 0, \ldots, 7$ we get

$$Im(\varphi) = \{0, 2, 4, 6\}$$

c) The isomorphism theorem for groups applied to φ and the computation in part b) give

$$(\mathbb{Z}_8/\{0,4\}, +_8) = (\mathbb{Z}_8/\ker(\varphi), +_8) \cong (im(\varphi), +_8) = (\{0,2,4,6\}, +_8).$$

To complete the exercise we have hence to understand whether $(\{0,2,4,6\}, +_8)$ is isomorphic to $(D_2, \circ)$ (they surely have the same number of elements!). In order to do that we can have a look at their multiplication tables and see whether they look the same (this would help us understand eventually how an isomorphism between them work or to find a counterexample).

Doing so, one can see that every element in D_2 has order 2, while the element $2 \in \{0,2,4,6\}$ has order 4 in $(\{0,2,4,6\}, +_8)$, because $2 +_8 2 +_8 2 +_8 2 +_8 2 = 8 \pmod 8 = 0$ and $2, 2 +_8 2, 2 +_8 2 +_8 2 \neq 0$. This implies that an ismorphism between those groups cannot exist.

Question 3

a) Remember that for an ideal I it holds true that $I = R$ if and only if $1_R \in I$. So our aim is to understand whether $\langle 4 \rangle \subset \mathbb{R}$ contains the number 1. However since I is an ideal of $\mathbb{R}$ it must hold that $r \cdot x \in I$ for all $r \in R = \mathbb{R}$ and $x \in I = \langle 4 \rangle$. Choosing $r = 1/4$ and $x = 4$ we see that $r \cdot x = (1/4) \cdot 4 = 1 \in \langle 4 \rangle = I$. Hence $\langle 4 \rangle = \mathbb{R}$.

b) We use the same strategy. We want to prove that $1 \in K$. Recall by definition of finitely generated ideal that

$$\langle X^2, X+1 \rangle = \{p(X) \cdot X^2 + q(X) \cdot (X+1) \mid p(X), q(X) \in \mathbb{R}[X]\}.$$

So we want to find $p(X)$ and $q(X)$ such that $p(X) \cdot X^2 + q(X) \cdot (X+1) = 1$. One can simply take $p(X) = 1$ and $q(X) = -X + 1$.

c) No. In fact $(J, +)$ cannot be a group, as it is not closed under the operation $+$. Take for example $f_1(X) = X^2 + 1$ and $f_2(X) = -X^2$. Then clearly $f_1(X), f_2(X) \in J$ but $f_1(X) + f_2(X) = 1 \notin J$.

Question 4

a) We check first whether $f(X)$ has roots in $\mathbb{F}_3 = \mathbb{Z}_3$.

$$f(0) = 0^3 +_3 0 +_3 2 = 2 \neq 0, \quad f(1) = 1^3 +_3 1 +_3 2 = 4 \pmod 3 = 1 \neq 0,$$

$$f(2) = 2^3 +_3 2 +_3 2 = 12 \pmod 3 = 0.$$

Since this shows that 2 is a root of $f(X)$ we know that $X - 2 = X + 1$ divides $f(X)$. Using division with remainder we get in fact that

$$\begin{array}{r|rrr|l}
X+1 & X^3 & & +\ X+2 & X^2+2X+2 \\
 & X^3+ & X^2 & & \\ \hline
 & & 2X^2+ & X+2 & \\
 & & 2X^2+ & 2X & \\ \hline
 & & & 2X+2 & \\
 & & & 2X+2 & \\ \hline
 & & & 0 &
\end{array}$$

and hence $f(X) = (X+1)(X^2+2X+2)$. We recall that polynomials of degree 1 are always irreducible, hence $X+1$ is irreducible. Also since it has degree 2, $g(X) := X^2+2X+2$ is irreducible if and only if it has no roots in $\mathbb{Z}_3$. We compute the evaluations $g(0) = 2 \neq 0$, $g(1) = 2 \neq 0$ and $g(2) = 1 \neq 0$. This implies that $f(X)$ is the product of the two irreducible polynomials $X+1$ and X^2+2X+2.

b) Let $h(X) := 2X^3 + 2X^2 + 2$. Then the Euclidian algorithm gives

$$\begin{bmatrix} X^4+X^3+X+2 & 1 & 0 \\ X & 0 & 1 \end{bmatrix} \underset{R_1 \mapsto R_1 + h(X)R_2}{\longrightarrow} \begin{bmatrix} 2 & 1 & h(X) \\ X & 0 & 1 \end{bmatrix},$$

that is

$$2 = 1 \cdot (X^4+X^3+X+2) + h(X) \cdot X = (X^4+X^3+X+2) + (2X^3+2X^2+2)X.$$

Multiplying everything (modulo 3) by 2 gives

$$1 = 2 \cdot_3 2 = 2(X^4+X^3+X+2) + 2X(2X^3+2X^2+2) = 2(X^4+X^3+X+2) + X(X^3+X^2+1).$$

Since this shows that $\gcd(X, X^4+X^3+X+2) = 1$ we get that $X + \langle X^4 + X^3 + X + 2 \rangle$ is a unit and its multiplicative inverse is

$$X^3 + X^2 + 1 + \langle X^4 + X^3 + X + 2 \rangle.$$

c) Recall that $g(X)+\langle X^4+X^3+X+2\rangle$ is a zero-divisor if and only if $0 < \deg(GCD(g(X),X^4+X^3+X+2)) < \deg(X4+X^3+X+2)=4$. From the given factorization, since for all $a\in\mathbb{F}_3\setminus\{0\}$, $\gcd(a(X^2+X+2),X^4+X^3+X+2)=X^2+X+2$ and $\gcd(X^2+1,X^4+X^3+X+2)=X^2+1$ we get that

$$X^2+1+\langle X^4+X^3+X+2\rangle,\ X^2+X+2+\langle X^4+X^3+X+2\rangle,\ 2(X^2+X+2)+\langle X^4+X^3+X+2\rangle$$

are three zero-divisors.

d) Let $u=g(X)+\langle X^4+X^3+X+2\rangle$ be a zero-divisor. We can assume that u is in standard form, that if $\deg(g(X))\leq 4-1=3$.

Then as written in the second point $1\leq \deg(GCD(g(X),X^4+X^3+X+2))\leq 3$.

Let $p_1(X)=X^2+X+2$ and $p_2(X)=X^2+1$. Then by direct checking $p_1(X)$ and $p_2(X)$ have no roots in $\mathbb{Z}_3$ and since they have degree 2, they are irreducible. Hence X^4+X^3+X+2 is the product of the two irreducible polynomials $p_1(X)$ and $p_2(X)$. Note that X^4+X^3+X+2 cannot have a factor of degree 1 as it does not have any roots in $\mathbb{Z}_3$. This implies that X^4+X^3+X+2 cannot have a factor of degree 3 either. In fact suppose by contradiction such a factor $d(X)$ exists. Then $X^4+X^3+X+2=d(X)s(X)$ where $\deg(s(X))=4-\deg(d(X))=4-3=1$. Hence X^4+X^3+X+2 has a factor of degree 1, which is not possible. This means that the propert factors of X^4+X^3+X+2 of degree between 1 and 3 all have degree 2. In particular $g(X)+\langle X^4+X^3+X+2\rangle$ is a zero-divisor if and only if $\deg(GCD(g(X),X^4+X^3+X+2))=2$.

Since X^4+X^3+X+2 is the product of the two irreducible, monic degree 2 polynomials $p_1(X)$ and $p_2(X)$ the only possibilities are that either $GCD(g(X),X^4+X^3+X+2)=p_1(X)$ or $GCD(g(X),X^4+X^3+X+2)=p_2(X)$. We analyze the two cases separately:

- $GCD(g(X),X^4+X^3+X+2)=p_1(X)$. Then since $p_1(X)$ divides $g(X)$ and $\deg(g(X))\leq 3$ we get that $g(X)=(aX+b)p_1(X)$ for some $a,b\in\mathbb{Z}_3$ with $(a,b)\neq(0,0)$ (recall that the zero-coset is not a zero-divisor!). We have a total of $3\cdot 3-1=8$ possible choices for $g(X)$ in this case.
- $GCD(g(X),X^4+X^3+X+2)=p_2(X)$. Then since $p_2(X)$ divides $g(X)$ and $\deg(g(X))\leq 3$ we get that $g(X)=(aX+b)p_2(X)$ for some $a,b\in\mathbb{Z}_3$ with $(a,b)\neq(0,0)$. As before we have a total of $3\cdot 3-1=8$ possible choices for $g(X)$ in this case.

Summing everything together, and recalling that cosets in standard for are pairwise distinct, we get a total number of $8+8=16$ zero-divisors.

Question 5

a) We note that since α is already in standard form, $\alpha \neq 1 + \langle X^2 + X + 1 \rangle$ that is it does not have order 1. Also using the definition of product of cosets

$$\alpha^2 = X^2 + \langle X^2 + X + 1 \rangle = -(X+1) + \langle X^2 + X + 1 \rangle \neq 1 + \langle X^2 + X + 1 \rangle,$$

which means α does not have order 2 and so its order is at least 3. Finally

$$\begin{aligned} \alpha^3 = \alpha \cdot \alpha^2 &= (X + \langle X^2 + X + 1 \rangle)(-(X+1) + \langle X^2 + X + 1 \rangle) \\ &= -(X^2 + X) + \langle X^2 + X + 1 \rangle = 1 + \langle X^2 + X + 1 \rangle. \end{aligned}$$

This proves that the order of α is 3.

b) Let $f(X) = X^2 + X + 1$ and let R denote the quotient ring $\mathbb{F}_p[X]/\langle X^2 + X + 1 \rangle$. If $p = 2$ then since $f(0) = 1 = f(1) \neq 0$ we get that R is a field as $f(X)$ is irreducible. If $p = 3$ then $f(0) = 0$ and hence $f(X)$ is not irreducible and R is not a field. Similar computations show that if $p = 5$ then R is a field, while if $p = 7$ then $f(2) = 0$ and R is not a field.

c) **TOO Difficult! This question has been deleted from the exam**