# Exam May 2020- answers

## Question 1

a) We first compute $f_1 = (1342)(57869)$. Then

$$f_1 \circ f_2 = (1342)(57869)(1324)(2536)(349)$$

$$= (145)(2786)(3) = (145)(2786).$$

**You cannot answer the part on even permutation as this notion has been removed from the curriculum of the course**.

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 $\ell_i$ for $i = 1, \ldots, k$ then $ord(f) = lcm(\ell_1, \ldots, \ell_k)$. We wrote $f_1 \circ f_2$ as composition of mutually disjoint cycles in part a), while $f_1 = (1342)(57869)$ and $f_2 = (1324)(2536)(349) = (13)(25)(496)$ are also written in disjoint cycles decomposition. Hence $ord(f_1 \circ f_2) = lcm(3,4) = 12$, $ord(f_1) = lcm(5,4) = 20$ and $ord(f_2) = lcm(2,2,3) = 6$.

c) Yes. An example is $f_1 \circ f_2$ provided above.

d) No. Indeed if $f \in S_9$ and we write $f = c_1 \circ c_2 \circ \ldots \circ c_k$ disjoint cycles decomposition where $c_i$ is a cycle of length $\ell_i$ for $i = 1, \ldots, k$ then as recalled before $ord(f) = lcm(\ell_1, \ldots, \ell_k)$. To have $ord(f) = 18 = lcm(\ell_1, \ldots, \ell_k)$ then $\ell_i$ need to be a divisor of 18 and at most equal to 9, so a value in the set $\{1,2,3,6,9\}$. If there is no cycle of length 9 in the decomposition then each of the $\ell_1, \ldots, \ell_k$ are either not divisible by 3 or divisible by 3 but not 9. If this is the case then $lcm(\ell_1, \ldots, \ell_k)$ is also either not divisible by 3 or divisible by 3 but mot 9, and so not possibly equal to 18. On the other hand if a cycle of length 9 appears then no other cycle can appear in the decomposition. So $f$ is a 9-cycle and hence its order is 9. This shows that an element of order 18 in $S_9$ cannot exist.

## Question 2

a) **This is part of a question in homework assignment 2, so the answer is not provided here!**

b) Note that the identity element of $G$ is $f_{1,0}$. Hence by definition of $\varphi$, $\varphi(f_{1,0}) = 1$, that is, $\varphi$ maps the identity element in $G$ to the identity element in $\mathbb{R}^*$. To show that $\varphi$ is a group homomorphism we have to check that $\varphi(f_{a,b} \circ f_{c,d}) = \varphi(f_{a,b}) \cdot \varphi(f_{c,d})$ for all $a,b,c,d \in \mathbb{R}$, $a,c \neq 0$. This is true because from part a) $f_{a,b} \circ f_{c,d} = f_{ac,ad+b}$ and so

$$\varphi(f_{a,b} \circ f_{c,d}) = \varphi(f_{ac,ad+b}) = ac = \varphi(f_{a,b}) \cdot \varphi(f_{c,d}).$$

c) By definition

$$ker(\varphi) = \{f_{a,b} \in G \mid \varphi(f_{a,b}) = 1\} = \{f_{a,b} \in G \mid a = 1\} = \{f_{1,b} \mid b \in \mathbb{R}\} \subset G.$$

This is exactly the subgroup $T$ written in part d) of the assignment. We want to show that $Im(\varphi) = \mathbb{R}^*$, that is, the map $\varphi$ is surjective. This is true because clearly $Im(\varphi) \subseteq \mathbb{R}^* = \mathbb{R} \setminus \{0\}$, but on the other hand if $a \in \mathbb{R} \setminus \{0\}$ is fixed arbitrarily then $a = \varphi(f_{a,0})$. This shows that $\mathbb{R}^* \subseteq Im(\varphi)$ and hence the two sets coincide.

d) **This is part of a question in homework assignment 2, so the answer is not provided here!**

**Question 3**

a) Let $a,b \in R$ and assume $a^2, a+b \in I$. Note that $b^2 = (b-a)(b+a) + a^2$.

Now recall that for all $r \in R$ and $x \in I$ it holds by definition of ideal that $r \cdot x \in I$. Clearly $b-a \in R$ as $a,b \in R$. So if we choose $r = b-a \in R$ and $x = a+b \in I$ we get that $(b-a)(b+a) \in I$. Since also $a^2 \in I$ and $I$ is closed under addition $(b-a)(b+a) + a^2 \in I$. Since this coincides with $b^2 \in I$, the proof is complete.

b) To prove that $P(X)$ is reducible it is natural to we start by trying to find a root of it. Indeed we know that for $a \in \mathbb{F}_3$, $P(a) = 0$ if and only if $X - a$ is a factor of $P(X)$. Since $0 < \deg(X-a) < \deg(P(X))$ this factor would also be a proper factor, implying reducibility of $P(X)$. However computing $P(a)$ for $a = 0,1,2$ we see that $P(a)$ is never equal to zero. This means that if $P(X)$ is reducible then it is the product of two irreducible polynomials of degree 2 (having a degree 1 factor implies indeed having a root).

Hence we want to find all the monic irreducible polynomials of degree 2, as we expect the product of two of those to coincide with our $P(X)$. The monic polynomials of degree 2 in $\mathbb{F}_3[X]$ are

$$X^2,\ X^2+X,\ X^2+2X,$$

$$X^2+X+1,\ X^2+2X+1,\ X^2+2,$$
$$X^2+1,\ X^2+X+2,\ X^2+2X+2.$$

To find the irreducible ones we remember that a polynomial of degree 2 is irreducible if and only if it has no roots. The first 3 polynomials have root 0 and hence are not irreducible. $X^2+X+1$ admits root 1, $X^2+2X+1$ admits root 2 and $X^2+2$ admits root 1. This leaves only the three options

$$X^2+1,\ X^2+X+2,\ X^2+2X+2.$$

Note that (computing division with remainder):

$$P(X)=X^4-X^2+1=(X^2+X+1)(X^2+2X+2)+2X+2,$$

so $X^2+2X+2$ cannot be a factor of $P(X)$ (we have remainder $2X+2$). Also similarly

$$P(X)=X^4-X^2+1=(X^2+2X+1)(X^2+X+2)+(X+2),$$

so $X^2+X+2$ cannot be a factor of $P(X)$ (we have remainder $X+2$).

Hence $X^2+1$ is the only possible factor of $P(X)$ and so it must hold $P(X)=(X^2+1)^2$. At this point that this is true can also be checked by hands. This shows that $P(X)$ is reducible as it has $X^2+1$ as irreducible factor.

c) No. This is the case because $X^5+X^4+X^2+1\in\mathbb{F}_2$ is reducible. This is shown by observing that 1 is a root and hence $X-1=X+1$ is a proper factor of $X^5+X^4+X^2+1$.

**Question 4**

a) Since $\alpha$ is already in standard form we have that $\alpha\neq 1+\langle X^3+X^2+X+1\rangle$, that is, its order is not 1. Since $\alpha^2=X^2+\langle X^3+X^2+X+1\rangle$ is also in standard form, $\alpha^2\neq 1+\langle X^3+X^2+X+1\rangle$, that is, its order is not 2 either. Continuing this way

$$\alpha^3=X^3+\langle X^3+X^2+X+1\rangle=-(X^2+X+1)+\langle X^3+X^2+X+1\neq 1+\langle X^3+X^2+X+1\rangle,$$

$$\alpha^4=\alpha^3\cdot\alpha=-X(X^2+X+1)+\langle X^3+X^2+X+1\rangle=$$
$$-(X^3+X^2+X+1)+1+\langle X^3+X^2+X+1\rangle=1+\langle X^3+X^2+X+1\rangle.$$

Hence the order of $\alpha$ is equal to 4.

b) The Euclidian algorithm gives

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

Now,

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

that is

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

Multiplying everything (modulo 5) by 2 gives

$$2 \cdot_5 3 = 2 \cdot (X^3+3X+2) + 2(4X^2+2X+3) \cdot (X+2).$$

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

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

c) Note that $R := \mathbb{F}_2[X]/\langle X^2+X+1\rangle$ is a finite field with $2^2 = 4$ elements as $X^2+X+1 \in \mathbb{F}_2[X]$ is irreducible (it has no roots).

This implies that $R^* = R \setminus \{0+\langle X^2+X+1\rangle\}$ is a cyclic group of order $4-1=3$. Primitive elements are all the elements in $R^*$ of order 3, however by Lagrange's theorem every element in $R^*$ has order dividing 3, that is either 1 or 3.

Since the identity element $1+\langle X^2+X+1\rangle$ is the only element of degree 1 in the group, this means that every element in $R^* \setminus \{1+\langle X^2+X+1\rangle\} = R \setminus \{0+\langle X^2+X+1\rangle, 1+\langle X^2+X+1\rangle\}$ is a primitive element. This means that $R^*$ has exactly $3-1=2$ primitive elements. We can write them in standard form as $X+\langle X^2+X+1\rangle$ and $X+1+\langle X^2+X+1\rangle$.

d) First of all note that 4 is a root of the polynomial $X^3+1 \in \mathbb{F}_5[X]$. This means that $X^3+1$ admits $X-4 = X+1$ as a factor. Using division with remainder one gets indeed that $X^3+1 = (X+1)(X^2+4X+1)$.

Note that the polynomial $X+1$ is irreducible as it has degree one, but actually also $X^2+X+1$ is irreducible. This is proven by checking that it has no roots in $\mathbb{F}_5$ (and this is enough as it has degree 2). This means that $X^3+1 = (X+1)(X^2+4X+1)$ is the factorization of $X^3+1$ into irreducible factors.

Now let $u = g(X) + \langle X^3 + 1 \rangle$ be an arbitrary coset in standard form, that is $g(X)$ has degree at most 2. We know that $u$ is a zero-divisor if and only if $0 < \deg(GCD(g(X), X^3 + 1)) < 3$. Clearly $X + 1$ is the only factor of degree 1 of $X^3 + 1$ as 4 is the only root of $X^3 + 1$ in $\mathbb{Z}_5$. Also $X^2 + 4X + 1$ is the only factor of degree 2 of $X^3 + 1$ as shown by the unique factorization into irreducible polynomials $X^3 + 1$ has.

This proves that $u = g(X) + \langle X^3 + 1 \rangle$ with $g(X)$ has degree at most 2,is a zero-divisor if and only if either $GCD(g(X), X^3 + 1) = X + 1$ or $GCD(g(X), X^3 + 1) = X^2 + 4X + 1$.

If $GCD(g(X), X^3 + 1) = X + 1$ then since $g(X)$ has degree at most 2, $g(X) = (aX + b)(X + 1)$ for some $a, b \in \mathbb{Z}_5$ with $(a, b) \neq 0$ (remember that the zero-coset is not a zero-divisor!). Also each coset of type $u = g(X) + \langle X^3 + 1 \rangle$ with $g(X) = (aX + b)(X + 1)$ for some $a, b \in \mathbb{Z}_5$ with $(a, b) \neq 0$ is a zero-divisor as $GCD(g(X), X^3 + 1) = X + 1$. Since standard forms are all distinct cosets, this gives a total of $5^2 - 1 = 24$ zero-divisors.

if $GCD(g(X), X^3 + 1) = X^2 + 4X + 1$ then since $g(X)$ has degree at most 2, $g(X) = c(X + 1)$ for some $c \in \mathbb{Z}_5$ with $c \neq 0$. For the same reason as before each of such $g(X)$ gives rise to a zero-divisor as the GCD is going to be $X^2 + 4X + 1$. This gives a total number of 4 zero-divisors.

We obtained in total $24 + 4 = 28$ zero-divisors.