Exam May 2022- answers

Question 1

a) $f=(1856)(249)(37)$.

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 $ord(f)=lcm(\ell_1,\ldots,\ell_k)$. Hence from part a) we see that $ord(f)=lcm(2,3,4)=12$.

c) Yes. An example is $h:=(1234)(56789)$ as $ord(h)=lcm(4,5)=20$.

d) We remember from the first homework assignment that for all $g \in S_9$, $g \circ (1234) \circ g^{-1}=(g[1]\ g[2]\ g[3]\ g[4])$. This can also be double-checked by observing that for all $i=1,2,3,4$, $g \circ (1234) \circ g^{-1}[g[i]]=g \circ (1234)[i]=g[i+1 \pmod 4]$. So to answer the question we need to find $g \in S_9$ such that $(g[1]\ g[2]\ g[3]\ g[4])=(5678)$. One example is

$$g=(15)(26)(37)(48).$$

Question 2

a) Recall that from the Orbit-Stabilizer theorem $|G|=|G_x||O_x|$ for all $x \in X$. Hence the cardinalities (or lengths) of all the orbits and the stabilizers need to divide $|G|$. Since $O_x \subseteq X$ for all $x \in X$, we also have $|O_x| \leq 20$ for all $x \in X$. Looking at all possible divisors of $|G|$, we deduce that

$$|O_x| \in \{1,2,17\},$$

for all $x \in X$. Furthermore we know that distinct orbits form a partition of X, so we must be able to find $k \geq 1$ orbits $O_{x_1},\ldots,O_{x_k} \subseteq X$ such that O_{x_i} and O_{x_j} are disjoint for $i \neq j$ and $X=O_{x_1} \cup,\ldots,\cup O_{x_k}$. Hence

$$20=|X|=|O_{x_1} \cup,\ldots,\cup O_{x_k}|=|O_{x_1}|+\ldots+|O_{x_k}|.$$

The problem now becomes understanding how we can have that for $k \geq 1$ that $20=|O_{x_1}|+\ldots+|O_{x_k}|$ with $|O_{x_i}| \in \{1,2,17\}$. Clearly $k=1$ (hence only one orbit) cannot occur as $|O_{x_1}| \leq 17 \neq 20$. Neither the case $k=2$ cannot happen as the sum of two numbers in $\{1,2,17\}$ is never 20. This proves that $k \geq 3$ (so that we have at least three orbits as desired). Note that $k=3$ can occur. In fact one could have $|O_{x_1}|=1$, $|O_{x_2}|=2$ and $|O_{x_3}|=17$, giving $1+2+17=20$. If there is no orbit of length 1, then for the same argument as before we must have all orbits of length 2 and/or 17. Say again that we have k distinct orbits, of which k_1 are of length 2 and k_2 are of length 17 (so $k = k_1 + k_2$ as all orbits are of length either 2 or 17). We get

$$20 = |X| = |O_{x_1} \cup, \ldots, \cup O_{x_k}| = |O_{x_1}| + \ldots + |O_{x_k}| = 2k_1 + 17k_2.$$

Note that $k_2 \leq 1$ (as $2 \cdot 17 > 20$) and so $k_1 \geq 1$ (as $17k_2 \leq 17 < 20$). One sees immediately that the only possibility is $k_1 = 10$ and $k_2 = 0$ and hence the exact number of orbits is $k = 10 + 0 = 10$. This is true because if $k_2 = 1$ then we must have $20 = 2k_1 + 17$, which is not possible as $20 - 17 = 3$ is not divisible by 2.

b) First we prove the hint using the definition. Let $g, h \in G$, then

$$[g^{-1}, h^{-1}] \cdot h = [(g^{-1})^{-1} \cdot (h^{-1})^{-1} \cdot g^{-1} \cdot h^{-1}] \cdot h = g \cdot h \cdot g^{-1} \cdot (h^{-1} \cdot h) = g \cdot h \cdot g^{-1}.$$

Note that since this is true for arbitrary $g, h \in G$ it is also true when replacing g^{-1} with g, that is,

$$[g, h^{-1}] \cdot h^{-1} = g^{-1} \cdot h \cdot g.$$

Suppose now that H is a subgroup of G containing $[G]$. We want to show that $gH = Hg$ for all $g \in G$. We do that by proving $gH \subseteq Hg$ and $gH \supseteq Hg$ separately. So let $g \in G$.

We prove first $gH \subseteq Hg$. To do so, let $g \cdot h \in gH$ arbitrary (so $h \in H$). Since from the hint $g \cdot h \cdot g^{-1} = [g^{-1}, h^{-1}] \cdot h$ we have that

$$g \cdot h = (g \cdot h \cdot g^{-1}) \cdot g = ([g^{-1}, h^{-1}] \cdot h) \cdot g \in Hg.$$

The fact that $([g^{-1}, h^{-1}] \cdot h) \cdot g \in Hg$ follows by observing that $[g^{-1}, h^{-1}] \cdot h \in H$, from the fact that H is a subgroup, $h \in H$ and $[G] \subseteq H$.

The proof of $Hg \subseteq gH$ is very similar. In fact, let $h \cdot g \in Hg$ arbitrary (so $h \in H$). Since from the hint $[g, h^{-1}] \cdot h^{-1} = g^{-1} \cdot h \cdot g$ we have that

$$h \cdot g = g \cdot (g^{-1} \cdot h \cdot g) = g \cdot ([g, h^{-1}] \cdot h^{-1}) \in gH.$$

Question 3

a) We start by trying to find roots of $f(X)$ as we know that whenever $a \in \mathbb{F}_5$ is a root of $f(X)$ then $X - a$ divides $f(X)$, providing a proper (and irreducible, because of degree 1) factor.

We see that

$$f(3) = 3^3 +_5 2 \cdot_5 3^2 +_5 3 \cdot_5 3 +_5 1 = 2 +_5 3 +_5 4 +_5 1 = 0,$$

hence $X - 3 = X + 2$ is an irreducible factor of $f(X)$. Using division with remainder we see that

$$f(X) = (X+4)(X^2+3).$$

The polynomial $g(X) := X^2 + 3 \in \mathbb{F}_5[X]$ is irreducible as it has no roots in $\mathbb{F}_5$ and it has degree 2 (the fact that it has no roots should be checked by evaluating $g(a)$ for all $a \in \mathbb{F}_5$). Hence $f(X)$ is the product of the two irreducible factors $X+4$ and X^2+3.

b) Using the extended euclidean algorithm gives inverse $2(X^2 + X^2 + 1) + \langle X^4 + X^3 + X + 2 \rangle$. This is pretty easy to check, in fact

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

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

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

c) $X + 4 + \langle X^4 + X^3 + X + 2 \rangle$, $X^3 + 2X^2 + 3X + 3 + \langle X^4 + X^3 + X + 2 \rangle$ and $2(X+4) + \langle X^4 + X^3 + X + 2 \rangle$ are all examples of zero-divisor. The reason is the characterization of zero-divisors in quotient rings: namely cosets $g(x) + \langle X^4 + X^3 + X + 2 \rangle$ where $0 < \deg(GCD(g(x), X^4 + X^3 + X + 2)) < 4$. Choosing $g(x)$ as proper factors of $X^4 + X^3 + X + 2$ always works, as in those cases the GCD is $g(x)$ itself.

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

$$X^4 + X^3 + X + 2 = (X+4)(X^3 + 2X^2 + 2X + 3).$$

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

Now let $u = g(X) + \langle X^4 + X^3 + X + 2 \rangle$ be an arbitrary coset in standard form, that is $g(X)$ has degree at most 3. We know that u is a zero-divisor if and only if $0 < \deg(GCD(g(X), ^4 + X^3 + X + 2)) < 4$. Clearly $X + 4$ is the only factor of degree 1 of $^4+X^3+X+2$ as 1 is the only root of $^4+X^3+X+2$ in $\mathbb{Z}_5$. Also X^3+2X^2+2X+3 is the only monic factor of degree 3 of X^4+X^3+X+2 as shown by the unique factorization into irreducible polynomials X^4+X^3+X+2 has. Also X^4+X^3+X+2 cannot have factors of degree 2.

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

If $GCD(g(X),X^4+X^3+X+2)=X+4$ then since $g(X)$ has degree at most 3, $g(X)=(aX^2+bX+c)(X+4)$ for some $a,b,c\in\mathbb{Z}_5$ with $(a,b,c)\neq(0,0,0)$ (remember that the zero-coset is not a zero-divisor!). Also each coset of type $u=g(X)+\langle X^4+X^3+X+2\rangle$ with $g(X)=(aX^2+bX+c)(X+4)$ for some $a,b,c\in\mathbb{Z}_5$ with $(a,b,c)\neq 0$ is a zero-divisor as $GCD(g(X),X^4+X^3+X+2)=X+4$. Since standard forms are all distinct cosets, this gives a total of $5^3-1=124$ zero-divisors.

if $GCD(g(X),X^4+X^3+X+2)=X^3+2X^2+2X+3$ then since $g(X)$ has degree at most 3, $g(X)=c(X^3+2X^2+2X+3)$ 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^3+2X^2+2X+3. This gives a total number of 4 zero-divisors.

We obtained in total $124+4=128$ zero-divisors.

Question 4

a) Associativity (for $+$ and $\cdot$) and distributive laws hold true in R_p as they hold in the larger set $\mathbb{Q}$ (indeed R_p a subset of it). The zero-element and one-element in $\mathbb{Q}$ are contained in R_p as $0=0/1$ and $1=1/1$.

   So to conclude that R_p is a ring we need to check that R_p is closed under multiplication and that $(R_p,+)$ is an abelian group. To do so, let $a/b, c/d\in R_p$ where p does not divide b nor d. Then

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}.$$

   The rational number $\frac{ac}{bd}\in R_p$ because p does not divide $bd>0$ (as it does not divide b and not d) and clearly $ac\in\mathbb{Z}$. This shows that R_p is closed under multiplication.

   To check that $(R_p,+)$ is an abelian group we only need to check it is a group. Indeed $r+t=t+r$ for all $r,t\in\mathbb{Q}$ so this is in particularly true if $r,t\in R_p\subset$

$\mathbb{Q}$. To see that $(R_p, +)$ is a group we only need to check that $+$ defines an operation on R_p and that each element in R_p admits an additive inverse (associativity and identity element have been treated at the beginning of this solution!). Hence let $a/b, c/d \in R_p$ where p does not divide b nor d. Then

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}.$$

The rational number $\frac{ad+cb}{bd} \in R_p$ because p does not divide $bd > 0$ (as it does not divide b and not d) and clearly $ad + cb \in \mathbb{Z}$. This shows that R_p is closed under addition. The additive inverse of an element $a/b \in R_p$ is $-(a/b) = (-a)/b$, which is an element of R_p as $-a \in \mathbb{Z}$.

No, R_p is not a ring when p is not a prime. Indeed suppose that $p = p_1 \cdot p_2$ where $p_i < p$ for all $i = 1, 2$. Then $1/p_1, 1/p_2 \in R_p$ but

$$\frac{1}{p1} \cdot \frac{1}{p_2} = \frac{1}{p_1 p_2} = \frac{1}{p} \notin R_p.$$

b) We need to show that $(J, +)$ is a group and that for all $r(X) \in \mathbb{Z}[X]$ and $s(X) \in J$ it holds that $r(X)s(X) \in J$. First note that $0 = 2 \cdot 0 \in 2\mathbb{Z}$ hence the zero-element $0 \in J$ (as it coincides with its own evaluation in zero).

Suppose that $s_1(X), s_2(X) \in J$, that is $s_1(0), s_2(0) \in 2\mathbb{Z}$. This means that $s_1(0) = 2k_1$ and $s_2(0) = 2k_2$ for some $k_1, k_2 \in \mathbb{Z}$. Then the evaluation in zero of $s_1(X) + s_2(X)$ is

$$s_1(0) + s_2(0) = 2k_1 + 2k_2 = 2(k_1 + jk_2) \in 2\mathbb{Z}.$$

This shows that $s_1(X) + s_2(X)$ has evaluation multiple of 2 in zero, that is, $s_1(X) + s_2(X) \in J$. So J is closed under addition. We need to check that additive inverses of elements in J are in J. However taking again $s_1(X) \in J$ and writing $s_1(0) = 2k_1$ we see that

$$-s_1(0) = -2k_1 = 2(-k_1) \in 2\mathbb{Z}.$$

Hence also $-s_1(X) \in J$ and $(J, +)$ is a group. To check the last property let $r(X) \in \mathbb{Z}[X]$ and $s(X) \in J$ be arbitrary. Write as before $s(0) = 2k$ for some $k \in \mathbb{Z}$. Then the evaluation in zero of $p(X)s(X)$ in zero is

$$p(0)s(0) = p(0)2k = 2\Big(p(0) \cdot k\Big) \in 2\mathbb{Z}.$$

This shows that $p(X)s(X) \in J$ and the proof is complete.

---

c) Following the hint we consider the map

$$\varphi : \begin{cases} \mathbb{Z}[X] \longrightarrow \mathbb{Z}_2 \\ p(X) \mapsto p(0) \pmod 2. \end{cases}$$

We want to show that φ is a ring homomorphism. We do that by checking the axioms. Let $p_1(X), p_2(X) \in \mathbb{Z}[X]$ and write $p_1(0) = 2q_1 + r_1$ and $p_2(0) = 2q_2 + r_2$ where $r_1, r_2 \in \{0, 1\}$ (we use division with remainder to do that).

- By definition $\varphi(0) = 0(0) \pmod 2 = 0 \pmod 2 = 0$. Hence φ send zero-element to zero-element.
- Note that

  $$\varphi(p_1(X) + p_2(X)) = (p_1(0) + p_2(0)) \pmod 2 =$$

  $$(2q_1 + r_1 + 2q_2 + r_2) \pmod 2 = (r_1 + r_2) \pmod 2 = r_1 +_2 r_2.$$

  On the other hand

  $$\varphi(p_1(X)) +_2 \varphi(p_2(X)) = (p_1(0) \pmod 2) +_2 (p_2(0) \pmod 2) =$$

  $$((2q_1 + r_1) \pmod 2) +_2 (2q_2 + r_2) \pmod 2) = r_1 +_2 r_2.$$

  This shows that $\varphi(p_1(X) + p_2(X)) = \varphi(p_1(X)) +_2 \varphi(p_2(X))$, that is, φ respects addition.
- By definition $\varphi(1) = 1(0) \pmod 2 = 1 \pmod 2 = 1$. Hence φ send one-element to one-element.
- Note that

  $$\varphi(p_1(X) \cdot p_2(X)) = (p_1(0) \cdot p_2(0)) \pmod 2 =$$

  $$(2q_1 + r_1)(2q_2 + r_2) \pmod 2 = (4q_1q_2 + 2q_1r_2 + 2q_2r_1 + r_1r_2) \pmod 2 =$$
  $$r_1r_2 \pmod 2 = r_1 \cdot_2 r_2.$$

  On the other hand

  $$\varphi(p_1(X)) \cdot_2 \varphi(p_2(X)) = (p_1(0) \pmod 2) \cdot_2 (p_2(0) \pmod 2) =$$

  $$((2q_1 + r_1) \pmod 2) \cdot_2 (2q_2 + r_2) \pmod 2) = r_1 \cdot_2 r_2.$$

  This shows that $\varphi(p_1(X) \cdot p_2(X)) = \varphi(p_1(X)) cdot_2 \varphi(p_2(X))$, that is, φ respects multiplication. Hence φ is a ring homomorphism.

  Now we compute kernel and image of φ. By definition

$$ker(\varphi) = \{p(X) \in \mathbb{Z}[X] \mid \varphi(p(X)) = 0\} = \{p(X) \in \mathbb{Z}[X] \mid p(0) \pmod 2 = 0\}$$
$$= \{p(X) \in \mathbb{Z}[X] \mid p(0) \in 2\mathbb{Z}\} = J.$$

On the other hand $Im(\varphi) = \mathbb{Z}_2$, that is φ is surjective. This is true because both 0 and 1 can be realized as images of some polynomials in $\mathbb{Z}[X]$ through φ. Indeed we observa for example that

$$\varphi(X) = 0,$$

and

$$\varphi(X+1) = 1.$$

The isomorphism theorem for rings applied with respect to φ now gives the desired isomorphism between $\mathbb{Z}[X]/J = \mathbb{Z}[X]/ker(\varphi)$ and $Im(\varphi) = \mathbb{Z}_2$.