Exam December 2023- answers

Question 1

a) $f = (1\ 6\ 5)(2\ 3)$.

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 $ord(f) = 6$ and the cycle type of f is $(1,1,1,0,0,0)$.

c) The answer is NO. In fact assume by contradiction that a permutation $f \in S_6$ with cycle type $(0,1,1,1,0,0)$ exists. Then by definition of cycle type, the disjoint cycle decomposition of f is $f = c_2 \circ c_3 \circ c_4$ where for $i = 2,3,4$, c_i is a cycle of length i and c_i and c_j are mutually disjoint if $i \neq j$. In other words there must exist $a_1, \ldots, a_9 \in \{1, \ldots, 6\}$ pairwise distinct such that $f = (a_1\ a_2)(a_3\ a_4\ a_5)(a_6\ a_7\ a_8\ a_9)$. Thus it needs to be true that $6 = |\{1, \ldots, 6\}| \geq |\{a_1, \ldots, a_9\}| = 9$, which is clearly impossible.

d) First note that $g = (1\ 5\ 2\ 3)$. Hence recalling that $(f \circ g)[a] = f[g[a]]$ and $(g \circ f)[a] = g[f[a]]$ for all $a \in \{1, \ldots, 6\}$, we get

$$f \circ g = (1\ 6\ 5)(2\ 3)(1\ 5\ 2\ 3) = (5\ 3\ 6),$$

while

$$g \circ f = (1\ 5\ 2\ 3)(1\ 6\ 5)(2\ 3) = (2\ 1\ 6).$$

Question 2

a) No, in fact it is not true for example that $id \in U$ (which is one of the proprties that a subgroup always satisfies). The reason is that since the identity map id satisfies by definition that $id[a] = a$ for all $a \in \{1, \ldots, n\}$ one has in particular that $id[n] = n$.

The cardinality of U is $|U| = n! - (n-1)!$. A possible proof of this fact follows by observing that by definition

$$U = S_n \setminus \{f \in S_n \mid f[n] = n\} =: S_n \setminus \bar{U}.$$

Hence $|U| = |S_n| - |\bar{U}| = n! - |\bar{U}|$. In this way our exercise is complete if we show that $|\bar{U}| = (n-1)!$. There is many ways. A very formal one is to consider the following map, with $A = \{1, \ldots, n-1\}$,

$$\varphi : \begin{cases} \bar{U} \to S_A \\ f \mapsto \varphi_f \end{cases},$$

with

$$\varphi_f[a] = f[a],\ for\ a \in A$$

is a bijection. If this is the case since $|S_A| = (n-1)!$, we get $|\bar{U}| = (n-1)!$.

To prove it is a bijection, first note that φ makes sense, that is, if $f \in \bar{U}$ then $\varphi_f \in S_A$ (it is a bijection from A to A). In fact since $f[n] = n$ and $f \in S_n$ the restriction of f to $A = \{1,\dots,n-1\}$ (which is what φ_f is) is a bijection on A, that is, $\varphi_f \in S_A$.

Now we prove that φ is injective. To do so, assume that $\varphi_f = \varphi_g$ for some $f, g \in \bar{U}$. Then $f[n] = n = g[n]$ (by definition of $\bar{U}$) and since $\varphi_f = \varphi_g$ we have that $f[a] = g[a]$ for all $a \in \{1,\dots,n-1\}$. Putting everything together we have that $f[a] = g[a]$ for all $a \in \{1,\dots,n\}$, which means that $f = g$ (they are the same map!). This shows that φ is injective.

Finally we prove that φ is surjective. To do so, let $g \in S_A$ be arbitrary. We want to find $f \in \bar{U}$ such that $\varphi_f = g$.It is sufficient to define $f : \{1,\dots,n\} \to \{1,\dots,n\}$ with

$$f[a] = \begin{cases} n,\ if\ a = n, \\ g[a],\ otherwise. \end{cases}$$

In fact not only $f \in S_n$ and particularly in $\bar{U}$ because $g \in S_A$ and we forced $f[n] = n$, but clearly $\varphi_f = g$ by construction.

b) We aim to prove an if and only if, so as usual we approach one implication at the time. The implication *If $H = S_n$ then H is a subgroup of S_n containing U* is trivial, as cleary S_n is a subgroup of itself (and it contains U by definition).

For the other implication, let H be a subgroup of S_n containing U. Our claim is that the only way is that $H = S_n$.

Note that since H contains U, we have from Question 2 (a) that $|H| \geq |U| > n! - (n-1)! = (n-1)(n-1)!$ (recall that $H = U$ cannot occur as U is not a subgroup of S_n) while from Lagrange's theorem $|H|$ divides $|S_n| = n! = n \cdot [(n-1)!]$. This means that $|H|$ needs to be a divisor of $n(n-1)!$ that is strictly larger than $(n-1)(n-1)!$ and the only option is that actually $|H| = n(n-1)! = |S_n|$, implying $H = S_n$.

A way to very formally prove the last part is the following. Given our $n \geq 2$ we got that $|H|$ divides $|S_n|$. This means that either $|H| = |S_n|$ or $|H|$ is a proper divisor of $n!$, that is $|H| \leq n!/2$. Since we know that $|H| > (n-1)(n-1)!$, if the latter case $|H| \leq n!/2$ occurs, it must be true that

$$(n-1)(n-1)! < \frac{n!}{2} = \frac{n(n-1)!}{2}.$$

This clearly implies that $n-1 < n/2$ that is $2n-2 < n$. Since this means that $n < 2$ we get a contradiction.

c) We need to prove that the relation is reflexive, symmetric and transitive. Reflexivity is trivial as $g \sim g$ is equivalent to say $g[n] = g[n]$ which is obviously true. To prove symmetry, assume that $f, g \in S_n$ are given and $f \sim g$. This means that $f[n] = g[n]$, and clearly $g[n] = f[n]$ (by symmetry of equality). This shows that $g[n] = f[n]$ which is equivalent to $g \sim f$.

Finally to show symmetry assume $f, g, h \in S_n$ with $f \sim g$ and $g \sim h$. These two hypotheses means that $f[n] = g[n]$ and $g[n] = h[n]$ respectively. Hence (by transitivity of equality) $f[n] = h[n]$ which is by definition equivalent to saying that $f \sim h$.

d) Let $f \in S_n$ then by definition of equivalence class, and the relation $\sim$ we have

$$[f]_\sim = \{g \in S_n \mid f \sim g\} = \{g \in S_n \mid f[n] = g[n]\}.$$

Independently on the specific choice of f, this set has cardinality $(n-1)!$. In fact to an element $g \in [f]_\sim$ is a map, so it is indetified by assigning $g[a]$ is for all $a \in \{1, \ldots, n\}$. Counting how many $g \in [f]_\sim$ there is, is the same as counting in how many different ways my map g can be constructed, that is, in how many different ways the $g[a]'s$ can be assigned. The condition $f[n] = g[n]$ poses only one condition for g, which then is allowed to map any other element in $\{1, \ldots, n-1\}$ to any other $\{1, \ldots, n\} \setminus \{f[n]\}$ as long as there is no repetitions (f needs to be injective) and all $\{1, \ldots, n\} \setminus \{f[n]\}$ are in the image of g. This means that the number of choices for $g \in [f]_\sim$ is the same as the number of bijections between the sets $\{1, \ldots, n-1\}$ and $\{1, \ldots, n\} \setminus \{f[n]\}$, which is $(n-1)!$.

e) Note that by definition

$$[id_n]_\sim = \{g \in S_n \mid id_n \sim g\} = \{g \in S_n \mid id_n[n] = g[n]\} = \{g \in S_n \mid g[n] = n\} = \bar{U},$$

as per definition we gave in part (a) of this question. As we pointed out in Question 2 (a), $S_n = U \cup \bar{U} = U \cup [id_n]_\sim$. This union is clearly disjoint as $f \in U$ satisfies $f[n] \neq n$ and hence $f \notin [id_n]_\sim$ (and viceversa).

Question 3

a) Let $p(X) \in \mathbb{Z}[X]$ be arbitrary. Use division with remainder to write

$$p(X) = q(X) \cdot (X-3) + r(X),$$

with either $r(X) = 0$ or $\deg(r(X)) < 1$. This means that $r(X) = r_0 \in \mathbb{Z}$. Using division with remainder of integers we can also now write

$$r(X) = r_0 = q_0 \cdot 7 + \alpha_P,$$

for some $0 \leq \alpha_P \leq 7-1 = 6$. This means that all in all we got that

$$P(X) = q(X)(X-3) + r_0 = q(X) \cdot (X-3) + q_0 \cdot 7 + \alpha_P.$$

Hence

$$P(X) - \alpha_P = q(X)(X-3) + 7q_0 \in \langle X-3, 7 \rangle = I.$$

b) First of all note that if we use the division algorithm to 0 with respect to $X-3$ and then to 7 as we did in part (a), then we would clearly get $0 = 0(X-3) + 07 + 0$, which implies that $\varphi(0) = \alpha_0 = 0$ (so the 0-element is preserved). The same is true for the polynomial 1 as clearly $1 = 0(X-3) + 07 + 1$, and hence also the one-element is preserved. Now we wish to show that φ respect addition and multiplication. So let $P(X), Q(X) \in \mathbb{Z}[X]$ and write

$$P(X) = q_P(X)(X-3) + p_0 \cdot 7 + \alpha_P$$

and

$$Q(X) = q_Q(X)(X-3) + q_0 \cdot 7 + \alpha_Q$$

where $q_0, p_0 \in \mathbb{Z}$ and $\alpha_P, \alpha_Q \in \mathbb{Z}_7$. Then

$$P(X) + Q(X) = (q_P(X) + q_Q(X))(X-3) + (p_0 + q_0) \cdot 7 + (\alpha_P + \alpha_Q).$$

Since seen as a polynomial $(p_0 + q_0) \cdot 7 + (\alpha_P + \alpha_Q)$ is constant, then either its degree is smaller than that of $X-3$ or it is the zero polynomial. By uniqueness of the remainder this means that $(p_0 + q_0) \cdot 7 + (\alpha_P + \alpha_Q)$ is the remainder of the division of $P(X) + Q(X)$ by $X-3$. By definition of φ, $\varphi(P(X) + Q(X))$ is hence the remainder of the division of $(p_0 + q_0) \cdot 7 + (\alpha_P + \alpha_Q)$ by 7, which is $(\alpha_P + \alpha_Q) \mod 7 = \alpha_P +_7 \alpha_Q$. Hence

$$\varphi(P(X) + Q(X)) = \alpha_P +_7 \alpha_Q = \varphi(P(X)) +_7 \varphi(Q(X)),$$

and φ respects addition. For multiplication note instead that

$$P(X)\cdot Q(X) = (q_P(X)(X-3)+p_0\cdot 7+\alpha_P)(q_Q(X)(X-3)+q_0\cdot 7+\alpha_Q) =$$

$$= (q_P(X)(X-3)+p_0\cdot 7+\alpha_P)q_Q(X)(X-3)+(q_0\cdot 7+\alpha_Q)q_P(X)(X-3)$$
$$+(q_0\cdot 7+\alpha_Q)(p_0\cdot 7+\alpha_P) =$$
$$= q(X)(X-3)+r,$$

with

$$q(X) = (q_P(X)(X-3)+p_0\cdot 7+\alpha_P)q_Q(X)+(q_0\cdot 7+\alpha_Q)q_P(X)$$

and

$$r = (q_0\cdot 7+\alpha_Q)(p_0\cdot 7+\alpha_P) = (q_0p_07+q_0\alpha_P+\alpha_Qp_0)7+\alpha_P\cdot\alpha_Q.$$

Since r is a constant we see again that by uniqueness of remainder r is the remainder of the division of $P(X)\cdot Q(X)$ by $X-3$. Since $r = (q_0p_07+q_0\alpha_P+\alpha_Qp_0)7+\alpha_P\cdot\alpha_Q$ the remainder of the division of r by 7 is $(\alpha_P\cdot\alpha_Q)\ mod\ 7 = \alpha_P\cdot_7\alpha_Q$. Summing up, we got that

$$\varphi(P(X)\cdot Q(X)) = \alpha_P\cdot_7\alpha_Q = \varphi(P(X))\cdot_7\varphi(Q(X)).$$

c) We simply use the definition of Kernel and image. First of all note that

$$Im(\varphi) = \mathbb{Z}_7.$$

In fact for all $a\in\mathbb{Z}_7$ consider the polynomial $P_a(X) := (X-3)+a$ Then division with remainder of $P_a(X)$ with respect to $X-3$ would give a, and since $a\in\mathbb{Z}_7$ (so $0\leq a<7$) the remainder of the division of a by 7 is just a itself. Hence $\alpha_{P_a} = a$ and over map φ is surjective.

By definition of Kernel

$$\ker(\varphi) = \{P(X)\in\mathbb{Z}[X] \mid \alpha_P = 0\} = \langle X-3, 7\rangle =: I.$$

In fact if $P(X)\in I$ then there exist $q(X), r(X)\in\mathbb{Z}[X]$ such that $P(X) = q(X)(X-3)+7r(X)$. Using division with remainder of $r(X)$ with respect to $X-3$ gives that

$$r(X) = q_1(X)(X-3)+r_0,$$

where $r_0\in\mathbb{Z}$. Hence

$$p(X) = (q(X)+q_1(X))(x-3)+7r_0.$$

This implies that the division with remainder of $P(X)$ by $X-3$ is $7r_0$, whose remainder dividing by 7 is clearly 0. Hence $\alpha_P = \varphi(P(X)) = 0$. This shows that $\langle X-3,7\rangle \subseteq I$.

For the other inclusion let $P(X) \in \ker(\varphi)$. This means that $\varphi(P(X)) = \alpha_P = 0$. This means that using division with remainder by $X-3$ first and then by 7 we can write $P(X)$ as

$$q_P(X)(X-3) + p_0 \cdot 7 + \alpha_P = q_P(X)(X-3) + p_0 \cdot 7 \in \langle X-3,7\rangle = I.$$

d) This follows by applying the isomorphism theorem for rings to $\varphi : \mathbb{Z}[X] \to \mathbb{Z}_7$ as we just shows that $\ker(\varphi) = I$ and $Im(\varphi) = \mathbb{Z}_7$.

Question 4

a) To compute the standard form we use long division of polynomials (division with remainder) and the standard representative will be given by the remainder itself. Doing so one gets (computations are omitted in this solution, but you should provide them!)

$$q(X) = X^2 + X + 4$$

and

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

Hence the standard form is $3X^3 + 3X^2 + X + 4 + \langle X^4 + 2X^3 + 4X + 3\rangle$.

b) The first natural step to factorize $f(X)$ is to find whether it has roots. Doing so yields that both 3 and 1 are roots, implying that $(X-3)(X-1) = (X+2)(X+4)$ divides $f(X)$. Using long division gives $f(X) = (X+2)(X+4)(X^2+X+1)$. Since it has degree 2, the polynomial $g(X) := X^2+X+1$ is irreducible if and only if it does not have any root in $\mathbb{F}_5$. One can check by direct computation that it is the case, meaning that $f(X) = (X+2)(X+4)(X^2+X+1)$ is the desired product of irreducible factors for $f(X)$.

c) The natural idea is to try to find proper monic factors of the generator of the ideal $f(X) := X^4 + 2X^3 + 4X + 3$, which is what we did in part (b) of this question. Indeed if $g(X)$ is any of those proper factors then $g(X) + \langle X^4 + 2X^3 + 4X + 3\rangle$ is a zero-divisor and so is $a(X) \cdot g(X) + \langle X^4 + 2X^3 + 4X + 3\rangle$ for all polynomials $a(X)$ such that $\deg(a(X)) + \deg(g(X)) < 4$ (in this way the cosets are in standard form so we know there is no overlap!). Hence from part b) $g(X) + \langle f(X)\rangle$ is a zero divisor for all polynomials

$$g(X) \in \{X+2, X+4, X^2+X+1\}.$$

If we choose $a(X) \in \mathbb{Z}_5 \setminus \{0\}$ then $a(X) \cdot g(X)$ will give rise to a zero-divisor (in standard form), and hence we already get in this way $4 \cdot 3 = 12$ zero-divisors. To find a last one, it is enough to consider $(X+2)(X+4)$ as in this way $\gcd((X+2)(X+4), X^4+2X^3+4X+3) = (X+2)(X+4)$ and since its degree is strictly contained between 0 and 4 we get that $(X+2)(X+4)$ gives rise to a zero-divisor. All in all we found at least 13 zero-divisors.

d) Let $h(X) = 4(X^3+2X^2+4)$. Then the Euclidian algorithm gives

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

that is

$$\begin{aligned} 3 &= 1 \cdot (X^4+2X^3+4X+3) + X(h(X)) \\ &= (X^4+2X^3+4X+3) + X(4X^3+3X^2+1), \end{aligned}$$

and hence multiplying everything by 2 (modulo 5):

$$2 \cdot_5 3 = 1 = 2(X^4+2X^3+4X+3) + 2X(4X^3+3X^2+1),$$

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

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