Exam 2022- answers

Question 1

a) $f = (1\ 2\ 4\ 5\ 3)$.

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 $ord(f) = 5$ and the cycle type of f is $(0,0,0,0,1)$.

c) Note first that if $n = 7$ then a permutation of order 10 can be found. An example is in fact $(1\ 2)(3\ 4\ 5\ 6\ 7)$. We want to show that such a permutation does not exist if $n \leq 6$, implying that the answer to this question is in fact $n = 7$.

Assume that $n \leq 6$ and that by contradiction $f \in S_n$ of order 10 exists. We know that 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 $10 = ord(f) = lcm(\ell_1, \ldots, \ell_k)$. This means the cycles c_i need to be 5-cycles, 2-cycles or 10-cycles. Clearly for $n \leq 6$ we do not have 10-cycles, so the c_i need to be either 5-cycles of 2-cycles, and at least one of each needs to appear in the decomposition of f. Since these 5 and 2-cycles are disjoint, this implies that $n \geq 7$, a contradiction.

d) Note first that $g = (1\ 5)(2\ 3)$. Then $f \circ g = (1\ 2\ 4\ 5\ 3)(1\ 5)(2\ 3) = (1\ 3\ 4\ 5\ 2)$ while $g \circ f = (1\ 5)(2\ 3)(1\ 2\ 4\ 5\ 3) = (1\ 3\ 5\ 2\ 4)$. The answer is hence no.

Question 2

a) The identity permutation $id_n \in H$ as $id_n[i] = i$ for all $i = 1, \ldots, n$. This means that H is not empty and so we can use Exercise 17 from Chapter 4 in the course notes, which says that H (since it is not empty) is a subgroup of S_n if and only if $g \circ f^{-1} \in H$ for all $f, g \in H$.

Hence let $f, g \in H$. This means that $f[1] = g[1] = 1$ and $f[n] = g[n] = n$. Note that in particular $1 = id_n[1] = f^{-1} \circ f[1] = f^{-1}(f[1]) = f^{-1}[1]$ and $n = id_n[n] = f^{-1} \circ f[n] = f^{-1}(f[n]) = f^{-1}[n]$. This proves that f^{-1} also fixes 1 and n. Now

$$g \circ f^{-1}[1] = g(f^{-1}[1]) = g[1] = 1$$

and analogously

$$g \circ f^{-1}[n] = g(f^{-1}[n]) = g[n] = n.$$

Hence $g \circ f^{-1} \in H$, and H is a subgroup of S_n from Exercise 17 Chapter 4.

b) Let $f \in S_n$ and call $i := f[1]$ and $j := f[n]$. Clearly $i \neq j$ as f is bijective, and $1 \leq i, j \leq n$. The by definition of coset, of H and the fact that $f[1] = i$ and $f[n] = j$ we get

$$\begin{aligned} f \circ H &= \{f \circ h \mid h \in H\} \\ &= \{f \circ h \mid h[1] = 1 \textit{ and } h[n] = n\} \\ &= \{f \circ h \mid f \circ h[1] = i \textit{ and } f \circ h[n] = j\}. \end{aligned}$$

Recalling that clearly $f \circ h \in S_n$ and the definition of $X_{i,j}$ we get

$$\{f \circ h \mid f \circ h[1] = i \textit{ and } f \circ h[n] = j\} \subseteq \{g \in S_n \mid g[1] = 1 \textit{ and } g[n] = j\} = X_{i,j}.$$

This proves that $f \circ H \subseteq X_{i,j}$. For the viceversa, let $g \in X_{i,j}$ arbitrary. Then $g[1] = i$ and $g[n] = j$. Note that $f[1] = i$ and $f[n] = j$ imply $f^{-1}[i] = 1$ and $f^{-1}[j] = n$. Hence

$$f^{-1} \circ g[1] = f^{-1}[i] = 1$$

and

$$f^{-1} \circ g[n] = f^{-1}[j] = n.$$

This proves that $f^{-1} \circ g \in H$ and hence $g = f \circ (f^{-1} \circ g) \in f \circ H$. Since this shows that $X_{i,j} \subseteq f \circ H$, the exercise is complete.

c) Since H is given by all the elements in S_n fixing 1 and n, it can be seen as a permutation in S_{n-2}. Doing so yields $|H| = (n-2)!$.

d) Following the hint, for $n \geq 4$ we see that using our answer to part $b)$

$$(1\ 2) \circ H = \{f \in S_n \mid f[1] = 2 \textit{ and } f[n] = n\}.$$

On the other hand we can compute using the definition of coset

$$H \circ (1\ 2) = \{h \circ (1\ 2) \mid h[1] = 1 \textit{ and } h[n] = n\}.$$

$$\{h \circ (1\ 2) \mid h \circ (1\ 2)[1] = h[2] \textit{ and } h \circ (1\ 2)[n] = n\}.$$

To prove that H is not normal it is enough to show that $H \circ (1\ 2) \neq (1\ 2) \circ H$. Consider for example $h = (2\ 3)$. Since $n \geq 4$, $h \in H$. Then $f := h \circ (1\ 2) = (2\ 3) \circ (1\ 2) = (1\ 3\ 2) \in H \circ (1\ 2)$ by construction, however $f \notin (1\ 2) \circ H$, because $f[1] = 3 \neq 2$. This shows that if $n \geq 4$ then H is not normal. If $n = 3$ then $H = \{id_3\}$ and hence it is trivially a normal subgroup.

Question 3

a) The zero-element and one-element in S are respectively $0/3$ and $1/1$. $(S,+)$ is an abelian group. The fact that $+$ is associative and commutative follows from the fact the these properties hold in $(\mathbb{Q},+)$. The additive inverse of $a/b \in S$ is $-a/b \in S$. Also if $a/banda_1/b_1 \in S$ then

$$\frac{a}{b}+\frac{a_1}{b_1}=\frac{ab_1+a_1b}{bb_1}\in S$$

because bb_1 keeps being odd when reduced. Associativity of $\cdot$ in S is true because it is true more generally in $(\mathbb{Q},+)$.

b) We have to prove that $(I,+)$ is a subgroup of $(S,+)$ and that for all $s \in S$ and all $x \in I$, $s \cdot x \in I$. Clearly $0/1 \in I$ and I is closed under addition. This is true because if a/b and a_1/b_1 are in I then

$$\frac{a}{b}+\frac{a_1}{b_1}=\frac{ab_1+a_1b}{bb_1}.$$

Since both a and a_1 are even, so is ab_1+a_1b (even where reduced, because bb_1 is odd). Clearly I is also closed under additive inversion as if $a/b \in I$ then also $-a/b \in I$ (if a is even, so is $-a$).

To check the last property let $a/b \in S$ and $a_1/b_1 \in I$. Then

$$\frac{a}{b}\frac{a_1}{b_1}=\frac{aa_1}{bb_1}.$$

Then bb_1 is odd even when reduced, while aa_1 is even (because a is even), even when reduced (because bb_1 is odd).

c) Following the hint we consider the map

$$\varphi:\begin{cases} S\to\mathbb{Z}_2, \\ \frac{a}{b}\mapsto a \; mod \; 2. \end{cases}$$

Then φ is a ring homomorphism. In fact $\varphi(0/3)=0 \; mod \; 2=0$ and $\varphi(1/3)=1 \; mod \; 2=1$. Also if $a/b \in S$ and $a_1/b_1 \in S$:

$$\varphi(a/b+a_1/b_1)=\varphi((ab_1+a_1b)/(bb_1))$$

Note that when $(ab_1+a_1b)/(bb_1)$ is reduced then the parity of the reduction of the numerator is equal to that of ab_1+a_1b. Hence

$$\varphi(a/b+a_1/b_1)=(ab_1+a_1b) \; mod \; 2.$$

Since b and b_1 are odd, they are congruent to 1 modulo 2. This gives

$$(ab_1 + a_1 b)\ mod\ 2 = (a + a_1)\ mod\ 2 = a +_2 a_1 =$$

$$(a\ mod\ 2) +_2 (a_1\ mod\ 2) = \varphi(a/b) +_2 \varphi(a_1/b_1).$$

Analogously

$$\varphi(a/b \cdot a_1/b_1) = \varphi((aa_1)/(bb_1)).$$

Note again that when $(aa_1)/(bb_1)$ is reduced then the parity of the reduction of the numerator is equal to that of aa_1. Hence

$$\varphi(a/b \cdot a_1/b_1) = (aa_1)\ mod\ 2 = a \cdot_2 a_1 = (a\ mod\ 2) \cdot_2 (a_1\ mod\ 2) = \varphi(a/b) \cdot_2 \varphi(a_1/b_1).$$

To complete the exercise we wish to apply the isomorphism for rings to φ. This follows simply by showing that $Ker(\varphi) = I$ and $Im(\varphi) = \mathbb{Z}_2$. The fact that $Im(\varphi) = \mathbb{Z}_2$ follows by noting that $\varphi(1/3) = 1$ and $\varphi(0/3) = 0$, which implies φ is surjective. By definition of Kernel

$$Ker(\varphi) = \{a/b \in S \mid a \text{ is even}\} = I.$$

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

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

and

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

Indeed

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

$$(X^3 + 4X^2 + 4X + 2)(X^4 + 2X^3 + X + 2) + 3X^2 + 3 = X^7 + X^6 + 2X^5 + X^4 + 2.$$

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

b) The first natural step to factorize $f(X)$ is to find whether it has roots. Doing so yields that both 3 and 4 are roots, implying that $(X+2)(X+1) = (X-3)(X-4)$ divides $f(X)$. Using long division gives $f(X) = (X+2)(X+1)(X^2+4X+1)$. Since it has degree 2, the polynomial $g(X) := X^2 + 4X + 1$ is irreducible if and only if it does not have any root. One can check by direct computation that it is the case, meaning that $f(X) = (X+2)(X+1)(X^2+4X+1)$ 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 $f(X) := X^4+X^3+X^2+2X+1$, which is what we did in part (c) of this question. Indeed if $g(X)$ is any of those proper factors then $g(X)+\langle X^4+2X^3+X+2\rangle$ is a zero-divisor and so is $a(X)\cdot g(X)+\langle X^4+2X^3+X+2\rangle$ for all polynomials $a(X)$ such that $\deg(a(X))+\deg(g(X))<4$. Hence from part b) $g(X)+\langle f(X)\rangle$ is a zero divisor for all polynomials

$$g(X) \in \{X+1, X+2, X^2+4X+1, 4X+3\},$$

giving rise to 4 distinct zero-divisors in R.

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

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

that is

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

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

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