
Exam May 2023- answers

Question 1

- a) $f = (1\ 2\ 6)(3\ 4\ 5)$.
- b) We recall that for $f \in S_n$, if $f = c_1 \circ c_2 \circ \dots \circ c_k$ is the disjoint cycles decomposition of f and c_i is a cycle of length ℓ_i for $i = 1, \dots, k$ then $ord(f) = lcm(\ell_1, \dots, \ell_k)$. From part a) we get that $ord(f) = 3$ and the cycle type of f is $(0, 0, 2, 0, 0, 0)$.
- c) Note first that if $n = 7$ then a permutation of order 12 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 12 exists. We know that if $f = c_1 \circ c_2 \circ \dots \circ c_k$ is the disjoint cycles decomposition of f and c_i is a cycle of length ℓ_i for $i = 1, \dots, k$ then $12 = ord(f) = lcm(\ell_1, \dots, \ell_k)$. This means the cycles c_i need to be 4-cycles, 2-cycles, 6-cycles, 3-cycles or 12-cycles. Clearly for $n \leq 6$ we do not have 12-cycles, while 6-cycles cannot appear as we have at most 6 elements. So the c_i need to be either 3-cycles or 2-cycles or 4-cycles, and at least one 4-cycle and one 3-cycle needs to appear in the decomposition of f (otherwise the lcm cannot be 12). Since these 4 and 3-cycles are disjoint, this implies that $n \geq 7$, a contradiction.

- d) $f \circ g$ and $g \circ f$ are not equal. In fact for example

$$(f \circ g)[1] = f[g[1]] = f[5] = 3$$

while

$$(g \circ f)[1] = g[f[1]] = g[2] = 4.$$

Question 2

- a) $g_1 \cdot g_2 \cdot \dots \cdot g_p = e$ if and only if $g_1 \cdot \dots \cdot g_{p-1} = g_p^{-1}$. This means that once we choose g_i with $i = 1, \dots, p-1$ arbitrarily, then we cannot choose g_p anymore, as it needs to be true that $g_p = (g_1 \cdot \dots \cdot g_{p-1})^{-1}$. Hence the cardinality of S coincides with the number of choices we have for the g_i for $i = 1, \dots, p-1$. Each g_i can be chosen in exactly $|G|$ ways. Hence $|S| = |G|^{p-1}$. Since by assumption p divides $|G|$, it hence also divides $|S|$

-
- b) We need to show that \sim is reflexive, symmetric and transitive. Reflexivity: Every p -tuple is the shift of itself applied 0 times. Symmetry: if $a \sim b$ then b is a cyclic shift of a , say b is obtained by applying a cyclic shift i times. Applying the cyclic shift $p - i$ times to b gives a (because shifting p times is just the identity map). Hence a is also a cyclic shift of b and hence $b \sim a$. Transitive: if $a \sim b$ and $b \sim c$ it means that b is a cyclic shift of a and c is a cyclic shift of b . Composing the two shifts together gives that c is a cyclic shift of a and hence $a \sim c$.

Note that if $a \in S$ then any shift of a is also an element in S . This is because shifting the entries of the p -tuple a does not change the property that the composition of all the entries is equal to the identity element.

- c) The equivalence class of a p -tuple (g_1, \dots, g_p) always contains (g_1, \dots, g_p) itself (by reflexivity of \sim). This means that the equivalence class of (g_1, \dots, g_p) contains only one element if and only if it contains only (g_1, \dots, g_p) itself, that is no other p -tuple but (g_1, \dots, g_p) can be obtained as a cyclic shift of (g_1, \dots, g_p) . This forces the entries in (g_1, \dots, g_p) to be all equal. In fact if $g_i \neq g_j$ for some $i < j$ the shifting $j - i$ times would give a p -tuple that is different from (g_1, \dots, g_p) . Hence equivalence classes containing one element are exactly those with representative of the form (g, \dots, g) with $g \in G$. The fact that $g^p = e$ is because we are requiring this p -tuple to be in S .
- d) Consider the group S_p of permutations on $\{1, \dots, p\}$ and the 6-cycle $\alpha = (1 2 3 4 5 6)$. The subgroup $\langle \alpha \rangle$ of S_p generated by α has order p , because α has order p . This group has a natural action on S . Namely

$$\varphi : \begin{cases} \langle \alpha \rangle \rightarrow S \\ \alpha^i \mapsto \varphi_i \end{cases}$$

where $\varphi_i : S \rightarrow S$ is the permutation that maps (g_1, \dots, g_p) to the cyclic shift of the entries of (g_1, \dots, g_p) i times. One can in fact use the definition to check that this is a group action (check it yourself!) and that the orbits of this group action coincides with the equivalence classes of \sim . By the orbit stabilizer theorem the length of an orbit divides the order of $\langle \alpha \rangle$, which is a prime p . This proves that orbits (equivalently equivalence classes under \sim) have lengths either 1 or p . Also, since distinct orbits form a partition of S we get that

$$|S| = |G|^{p-1} = k + pd,$$

where k is the number of orbits of length 1 (i.e. equivalence classes with 1 elements) and d is the number of orbits (equivalently equivalence classes of \sim) of length p .

-
- e) Recall that from a) p divides $|S|$ while from part d) we wrote $|S| = |G|^{p-1} = k + pd$ where $k \geq 1$ (because of the class of (e, \dots, e) , which has in fact length 1). This means that k must be congruent to 0 modulo p and hence in particular $k \geq 2$ from c) this means that there exists a $g \neq e$ such that $g^p = e$, and hence an element of order p because p is prime.

Question 3

- a) Associativity (for $+$ and \cdot) and distributive laws hold true in R as they hold in the larger set of matrices with coefficients in \mathbb{Q} (indeed R a subset of it). The zero-matrix and the identity matrix are contained by definition in R , so R has both zero and one-elements.

So to conclude that R is a ring we need to check that R is closed under multiplication and that $(R, +)$ is an abelian group. To do so it is enough to prove by hands that multiplication and addition of upper triangular matrices is upper triangular, the opposite of an upper triangular matrix is upper triangular and that $r + t = t + r$ for all $r, t \in R$.

- b) Here one needs to show that $(I, +)$ is a group and that for all $r \in R$ and $s \in I$ it holds that $r \cdot s \in I$. These properties can be checked by hands. J instead is not an ideal. In fact the one-element (identity matrix) is contained in J , but $J \neq R$ (and we know that if an ideal contains the one-element, then it is the entire ring).
- c) The fact that φ is a homomorphism can be checked by using the definition and a direct computation. Just using the definition of kernel gives $\text{Ker}(\varphi) = I$ while $\text{Im}(\varphi) = \mathbb{Q}$. This last equality is true because for all $q \in \mathbb{Q}$ one can simply consider the matrix in R with $u = 0$ and $v = q$ (hence the map is surjective).
- d) Follows immediately from c) and the isomorphism theorem applied to φ .

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!)

$$q(X) = X^3 + 5X^2 + 5X + 3$$

and

$$r(X) = X^3 + X^2 + 1.$$

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 $(X - 3)(X - 4) = (X + 4)(X + 3)$ divides $f(X)$. Using long division gives $f(X) = (X + 3)(X + 4)(X^2 + 3X + 1)$. Since it has degree 2, the polynomial $g(X) := X^2 + 3X + 1$ is irreducible if and only if it does not have any root in \mathbb{F}_7 . One can check by direct computation that it is the case, meaning that $f(X) = (X + 3)(X + 4)(X^2 + 3X + 1)$ 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 $f(X) := X^4 + 3X^3 + 6X^2 + X + 5$, which is what we did in part (b) of this question. Indeed if $g(X)$ is any of those proper factors then $g(X) + \langle X^4 + 3X^3 + 6X^2 + X + 5 \rangle$ is a zero-divisor and so is $a(X) \cdot g(X) + \langle X^4 + 3X^3 + 6X^2 + X + 5 \rangle$ 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

$$g(X) \in \{X + 3, X + 4, X^2 + 3X + 1, 4X + 5\},$$

giving rise to 4 distinct zero-divisors in R .

- d) Let $h(X) = 6(X^3 + 5X^2 + 2X + 5)$. Then the Euclidian algorithm gives

$$\left[\begin{array}{ccc} X^4 + 3X^3 + 6X^2 + X + 5 & 1 & 0 \\ X + 5 & 0 & 1 \end{array} \right] \xrightarrow{R_1 \mapsto R_1 + h(X)R_2} \left[\begin{array}{ccc} 1 & 1 & h(X) \\ X + 5 & 0 & 1 \end{array} \right],$$

that is

$$\begin{aligned} 1 &= 1 \cdot (X^4 + 3X^3 + 6X^2 + X + 5) + (X + 5)(h(X)) \\ &= X^4 + 3X^3 + 6X^2 + X + 5 + (X + 5)(6(X^3 + 5X^2 + 2X + 5)) \end{aligned}$$

Since this shows that $\gcd(X + 5, X^4 + 3X^3 + 6X^2 + X + 5) = 1$ we get that $X + 5 + \langle X^4 + 3X^3 + 6X^2 + X + 5 \rangle$ is a unit and its multiplicative inverse is

$$6(X^3 + 5X^2 + 2X + 5) + \langle X^4 + 3X^3 + 6X^2 + X + 5 \rangle.$$