Exam May 2024- answers

Question 1

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

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 $ord(f) = 2$ and the cycle type of f is $(1,2,0,0,0)$.

c) We first note that since an m-cycle has order m, one has $(1\ 2\ 5\ 4)^4 = id$ and hence (composing with $(1\ 2\ 5\ 4)^{-2}$ both sides)

$$(1\ 2\ 5\ 4)^{-2} = (1\ 2\ 5\ 4)^2 = (1\ 2\ 5\ 4)(1\ 2\ 5\ 4) = (1\ 5)(2\ 4).$$

Now we can complete the exercise by computing

$$(1\ 2\ 3)(4\ 5)(1\ 2\ 5\ 4)^{-2} = (1\ 2\ 3)(4\ 5)(1\ 5)(2\ 4) = (1\ 4\ 3)(2\ 5).$$

d) The answer is YES. In fact note that $g = (1\ 3)(2\ 4)$ and

$$f \circ g = (1\ 4)(2\ 3)(1\ 3)(2\ 4) = (1\ 2)(3\ 4)$$

while

$$g \circ f = (1\ 3)(2\ 4)(1\ 4)(2\ 3) = (1\ 2)(3\ 4).$$

Question 2

a) Let $f \in S_n$ be homocyclic. This means that if $f = c_1 \circ c_2 \circ \ldots \circ c_k$ is the disjoint cycles decomposition of f then c_i is a cycle of some length ℓ for all $i = 1, \ldots, k$ (i.e. cycles have all the same lengths, by definition of beign homocyclic). We have two possibilities now: either $\ell = 1$ or $\ell > 1$.

If $\ell = 1$ then f is the identity map, whose order is 1 (clearly dividing n), and the claim about the order of f dividing n is trivially true.

So we can assume that $\ell > 1$. Since f is not allowed to have 1-cycles in its decomposition (otherwise it would not be homocyclic, because it would have both 1-cycles and ℓ-cycles in its decomposition) it needs to be true that $k \cdot \ell = n$. In fact by definition the disjoint cycles in the disjoint cycle decomposition of a permutation (if also eventual 1-cycles are included) cover the entire set $\{1, \ldots, n\}$ and in this specific case we have k ℓ-cycles in total.

Hence ℓ divides n. Now we can simply use that the order of f is the least common multiple of the lengths of the cycle appearing in its decomposition, which in this case reads as $ord(f) = lcm(\ell, \dots, \ell) = \ell$. This shows both that $ord(f) = \ell$ and that ℓ divides n. We conclude, as claimed, that the order of our arbitrary homocyclic permutation divides n.

b) Let $f \in S_n$ be homocyclic. This means as before that writing $f = c_1 \circ c_2 \circ \dots \circ c_k$ in disjoint cycles decomposition the c_i is a cycle of some length ℓ for all $i = 1, \dots, k$ (i.e. cycles have all the same length). Let $p \in \mathbb{Z}$ arbitrary and use division with remainder of integers to write $p = q\ell + r$ with $r \in \{0, \dots, \ell - 1\}$. Then since from part (a) we know that f has order ℓ,

$$f^p = f^{q\ell + r} = (f^\ell)^q \circ f^r = id_n \circ f^r = f^r.$$

This shows that it is enough to show that f^r is homocyclic for all $r \in \{0, \dots, \ell - 1\}$. Note first that

$$f^r = (c_1 \circ c_2 \circ \dots \circ c_k)^r = c_1^r \circ c_2^r \circ \dots \circ c_k^r.$$

In fact c_i^r will permute only the elements that c_i itself was permuting (simply because if $c_i[a] = a$ then also $c_i^r[a] = a$), for all i, which means that the permutations c_i^r will remain disjoint (and so will their disjoint cycle decompositions), and hence will commute.

We now want to show that the expression $c_1^r \circ c_2^r \circ \dots \circ c_k^r$ gives rise to the composition of cycles of the same lengths, for all r, because this would imply that f^r is homocyclic as claimed.

A way to prove this, is to show something a bit more general, that is, the following claim.

CLAIM: If $c \in S_n$ is a cycle of length ℓ then the disjoint cycle decomposition of c^r is given by d cycles of length ℓ/d, where $d = \gcd(\ell, r)$.

This in fact would imply that each c_i^r has disjoint cycle decomposition given by cycles of the same lengths, and since the c_i^r are disjoint for different i, we get that all these k cycles of length ℓ/d give the disjoint cycle decomposition of f^r.

Proof of the CLAIM: Wwrite $c = (a_0 \dots a_{\ell-1})$ cycle of length ℓ and let $r \in \{0, \dots, \ell - 1\}$. Denote with $d = \gcd(r, \ell)$. Then for all $j = 0, \dots, \ell - 1$ one has

$$c^r[a_j] = a_{j + r \bmod \ell}.$$

So let us now try to describe the disjoint cycle decomposition of c^r. A cycle in the decomposition will start with some a_j for some $j = 0, \dots, \ell - 1$ and

we will be

$$(a_j\ a_{j+r\ mod\ \ell}\ a_{j+2r\ mod\ell}\ a_{j+3r\ mod\ell}\ \dots\ \ a_{j+(s-1)r\ mod\ell}),$$

where $s-1$ is the smallest non-negative integer such that $c^r[a_{j+(s-1)r\ mod\ell}] = a_{j+sr\ mod\ell} = a_j$ (which is the point where we close the cycle). This means that the length s of the cycle in the decomposition of c^r, containing a_j, is the smallest non-negative integer $s-1$ such that

$$j + sr\ mod\ell = j$$

that is

$$sr \equiv 0 \pmod{\ell}.$$

This means that independently on j, the length of the cycle containing a_j is the smallest s such that $sr = k\ell$ for some $k \in \mathbb{Z}$. Such a smallest s is clearly $s = \ell/d$. The reason is that if $sr = k\ell$ then dividing by d both sides $s(r/d) = k(\ell/d)$ where now $\gcd(r/d, \ell/d) = 1$. Hence ℓ/d needs to divide s, and so $s \geq \ell/d$.

This proves that each cycle in the decomposition of c^r (as we got something independent on j at the end) is of length ℓ/d

c) No. In fact consider the case $n = 4$ and $f = (1\ 2\ 3\ 4)$ and $g = (1\ 4)(2\ 3)$. Then

$$f \circ g = (1\ 2\ 3\ 4)(1\ 4)(2\ 3) = (2\ 4),$$

which is not homocyclic (it has both 1-cycles and a 2-cycle in its decomposition).

d) We show one implication at the time. Assume first that all the elements of G are homocyclic and let $a \in \{1, \dots, n\}$. If $f \in G \setminus \{id_n\}$ then write $f = c_1 \circ c_2 \circ \dots \circ c_k$ disjoint cycles decomposition of f where c_i is a cycle of some length ℓ for all $i = 1, \dots, k$. Since $f \neq id_n$, $\ell \geq 2$. This means that f has no 1-cycles in its decomposition, that is, it fixes no elements in $\{1, \dots, n\}$. Hence in particular $f \notin G_a$. This shows that $G_a = \{id_n\}$ for all $a \in \{1, \dots, n\}$ and hence G is semiregular as claimed.

Suppose now viceversa that G is semiregular. This means that for all $g \in G \setminus \{id_n\}$, $g[a] \neq a$ for all $a \in \{1, \dots, n\}$, that is, no $g \in G \setminus \{id_n\}$ has a 1-cycle in its decomposition. Suppose by contradiction that there exists $f \in G \setminus \{id_n\}$ that is not homocyclic, that is when writing the disjoint cycle decomposition of $f = c_1 \circ c_2 \circ \dots \circ c_k$ the lengths of the cycles c_i are not all the same. Call ℓ the smallest length among those of the cycles c_i, and assume without loss

of generality (the cycles commute!) that it is c_1 the cycle of smallest length ℓ. Note that since the cycles don't all have the same lengths, there must exist a cycle in the decomposition of length strictly larger than ℓ. Write $c_1 = (a_0\ a_1 \dots a_{\ell-1})$

Then $f^\ell \in G$ because G is a subgroup and $f^\ell \neq id_n$ as $ord(f)$ is the least common multiple of the lengths of the cycles c_i, which strictly larger than ℓ. However $f^\ell[a_0] = c_1^\ell[a_0] = id_n[a_0] = a_0$. This means that $f^\ell \in G_{a_0}$ which is not possible as G is semiregular. We got our desired contradiction.

Question 3

a) First of all note that $+_K$ and $\cdot_K$ are operations on R. To see this $x, y \in R$. Then $v(x), v(y) \geq 0$. If $x +_K y = 0_K$ then $x +_K y \in R$. So assume without loss of generality that $x +_K y \neq 0_K$ and that $v(x) \geq v(y)$. Then

$$v(x +_K y) \geq \min\{v(x), v(y)\} = v(y) \geq 0,$$

which shows that $x +_K y \in R$. Similarly (now independently on whether or not $x +_K y \neq 0_K$)

$$v(x \cdot_K y) = v(x) +_K v(y) \geq 0 +_K 0 = 0,$$

proving that also $x \cdot_K y \in R$. The associativity of the operations, the commutativity of $+_K$, as well as the distributive laws follow because $(K, +_k, \cdot_K)$ is a field (so we know that those rules are true in K so in particular in $R \subseteq K$). The zero-element 0_K is in R by definition. While since

$$v(1_K) = v(1_K \cdot 1_K) = v(1_K) + v(1_K),$$

we get that $v(1_K) = 0$, giving that also the one-element 1_K is in R. To complete the proof we are left to show that $(R, +_K)$ is a group, more precisely that R is closed under additive inversion. For that, let $x \in R$. Then $v(x) \geq 0$. Note first that

$$0 = v(1_K) = v(-1_K \cdot_K -1_K) = v(-1_K) + v(-1_K),$$

which implies that $v(-1_R) = 0$. Using now from an exercise that $-x = (-1_K) \cdot_K x$, we have

$$v(-x) = v(-1_K \cdot_K x) = v(-1_K) +_K v(x) = v(x) \geq 0,$$

and hence $-x \in R$.

b) Let $x \in K$. If $v(x) \geq 0$ then $x \in R$ and we are done. So let us assume that $x \notin R$, that is, $v(x) < 0$. We aim to show that $x^{-1} \in R$. To do so note that

$$0 = v(1_K) = v\left(x \cdot_K x^{-1}\right) = v(x) + v(x^{-1}) < v(x^{-1}).$$

Since this shows that $v(x^{-1}) > 0$ we deduce that $x^{-1} \in R$ as claimed.

c) This is just an immediate consequence of b). In fact $x \in R$ is a unit if and only if $x^{-1} \in R$. However as shown in b)

$$0 = v(x) + v(x^{-1}),$$

that is

$$-v(x) = v(x^{-1}).$$

So $x, x^{-1} \in R$ if and only if both $v(x), -v(x) \geq 0$, that is, $v(x) = 0$ as claimed.

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!)

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

and

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

Hence the standard form is $X^3 + 3X^2 + X + 4 + \langle X^4 + 3X^3 + 2X^2 + X + 1 \rangle$.

b) The first natural step to factorize $f(X)$ is to find whether it has roots. Doing so yields that 4 is a root, implying that $(X - 4) = (X + 1)$ divides $f(X)$. Using long division gives $f(X) = (X+1)(X^3+2X^2+1)$. Since it has degree 3, the polynomial $g(X) := X^3 + 2X^2 + 1$ 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 $f(X) = (X + 1)(X^3 + 2X^2 + 1)$ 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 $f(X) := X^4 + 3X^3 + 2X^2 + X + 1$, which is what we did in part (b) of this question. Indeed if $g(X)$ is any of those proper factors then

$g(X) + \langle X^4 + 3X^3 + 2X^2 + X + 1 \rangle$ is a zero-divisor and so is $a(X) \cdot g(X) + \langle X^4 + 3X^3 + 2X^2 + X + 1 \rangle$ 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

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

giving rise to 8 distinct zero-divisors in R when we multiply each of them by a constant $a \in \mathbb{F}_5$.

d) Let $h(X) = 4(X^3 + 3X^2 + 2X + 1)$. Then the Euclidian algorithm gives

$$\begin{bmatrix} X^4 + 3X^3 + 2X^2 + X + 1 & 1 & 0 \\ X & 0 & 1 \end{bmatrix} \begin{array}{c} \longrightarrow \\ R_1 \mapsto R_1 + h(X)R_2 \end{array} \begin{bmatrix} 1 & 1 & h(X) \\ X & 0 & 1 \end{bmatrix},$$

that is

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

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

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