Exam December 2024- answers

Question 1

a) $g_1 \circ g_2 = (1\ 3)(4\ 5)$.

b) Since g_1 and g_2 are already written in disjoint cycle decomposition, we get immediately that $ord(g_1) = 3$ and $ord(g_2) = lcm(2,2) = 2$. The cycle type of g_1 is $(2,0,1,0,0)$ while the cycle type of g_2 is $(1,2,0,0,0)$.

c) The answer is no. In fact assume by contradiction $(1\ 2) = g_1^i \circ g_2^j$. Since from (b) g_1 and g_2 have order 3 and 2 respectively we can assume that $i = 0,1,2$ and $j = 0,1$. We treat the cases $j = 0$ and $j = 1$ separately.

- If $j = 0$ then we would need $(1\ 2) = g_1^i$ for $i = 0,1,2$ however $g_1^0 = id \neq (1\ 2)$, $g_1^1 = (1\ 2\ 3) \neq (1\ 2)$ and finally $g_1^2 = (1\ 3\ 2) \neq (1\ 2)$. So a contradiction is obtained.
- If $j = 1$ then we would need $(1\ 2) = g_1^i \circ g_2 = g_1^i \circ (1\ 2) \circ (4\ 5)$ for some $i = 0,1,2$. Hence $(1\ 2) \circ ((1\ 2) \circ (4\ 5))^{-1} = g_1^i$, that is $(1\ 2) \circ (4\ 5) \circ (1\ 2) = (4\ 5) = g_1^i = (1\ 2\ 3)^i$. This is clearly impossible as g_1^i is not a 2-cycle for any $i = 0,1,2$ (as we said above $g_1^0 = id$, $g_1^1 = (1\ 2\ 3)$ and finally $g_1^2 = (1\ 3\ 2)$).

d) Burnside's lemma implies that the number of distinct orbits of the action of H on A is equal to

$$\frac{1}{|H|} \sum_{h \in H} |Fix(h)|,$$

which since $|H| = 6$ gives

$$\frac{1}{6} \sum_{h \in H} |Fix(h)|.$$

If $h = id$ then then $|Fix(h)| = 5$, if h is a composition of two disjoint cycles (we have 3 of them in H) then $|Fix(h)| = 1$ (the only element that does not appear in the cycle is fixed) while if H is a 3-cycle (we have two of them in H) then $|Fix(h)| = 2$ (again, only the elements not appearing in the cycle are fixed, and we have exactly two on them in A). Substituting in the formula above gives

$$\frac{5 + 3 \cdot 1 + 2 \cdot 2}{6} = 2.$$

The two orbits are in fact $\{1,2,3\}$ and $\{4,5\}$.

Question 2

a) Note that H is not empty so we can use the exercise that we solved in class saying *H is a subgroup if and only if for all $f,g \in H$ one has $f^{-1} \circ g \in H$* (equivalently one can check the axioms in the definition of a subgroup). For f and g we have only three possibilities, namely r^2, r^4 and id. Note that since $r^6 = 1$ we have that $r^2 \circ r^4 = r^4 \circ r^2 = id$ that is r^4 and r^2 are eachother's inverse. Let $f,g \in H$. Clearly if $f = id$ then $f^{-1} \circ g = g \in H$. If $g = id$ then $f^{-1} \circ g = f^{-1} \in H$ as if $f = id$ then $f^{-1} = id \in H$, if $f = r^2$ then $f^{-1} = r^4 \in H$ and lastly if $f = r^4$ then $f^{-1} = r^2 \in H$. Hence it remains to study the case in which $f,g \in \{r^2, r^4\}$. We get three possible cases:

- Case 1: $(f,g) = (r^2,r^2)$. Then $f^{-1} \circ g = id \in H$.
- Case 2: $(f,g) = (r^4,r^4)$. Then $f^{-1} \circ g = id \in H$.
- Case 3: $(f,g) = (r^2,r^4)$. Then $f^{-1} \circ g = r^4 \circ r^4 = r^8 = r^2 \in H$ (here we used that $r^6 = id$).
- Case 4: $(f,g) = (r^4,r^2)$. Then $f^{-1} \circ g = r^2 \circ r^2 = r^4 \in H$.

Hence H is a subgroup of $(D_6, \circ)$.

b) The answer is yes. To check that we need to prove that for all $r^i s^j \in D_6$ (with as usual $i = 0,\dots,5$ and $j = 0,1$) one has $r^i s^j H = H r^i s^j$ (left and right cosets are equal). To prove this let $r^i s^j \in D_6$ arbitrary. We divide the case $j = 0$ and $j = 1$:

- If $j = 0$ then $r^i s^j H = r^i H = \{r^i, r^{i+2}, r^{i+4}\} = \{r^i, r^{2+i}, r^{4+i}\} = H r^i = H r^i s^j$.
- If $j = 1$ then $r^i s^j H = r^i s H = \{r^i s, r^i s r^2, r^i s r^4\}$. We now recall that for all $j = 0,\dots,5$ one has $r^j s = s r^{-j}$ so in this case this gives

$$\{r^i s, r^i s r^2, r^i s r^4\} = \{r^i s, r^{i-2} s, r^{i-4} s\}.$$

All in all this shows that

$$r^i s^j H = \{r^i s, r^{i-2} s, r^{i-4} s\}. \tag{1}$$

We know compute the right coset to compare it with what we got in Equation (1):

$$H r^i s = \{r^i s, r^2 r^i s, r^4 r^i s\}.$$

Recall from part (a) that $(r^2)^{-1} = r^{-2} = r^4$ and $(r^4)^{-1} = r^{-4} = r^2$, which implies

$$Hr^is = \{r^is, r^2r^is, r^4r^is\} = \{r^isr^{-4}r^is, r^{-2}r^is\} = \{r^is, r^{i-4}s, r^{i-2}s\}.$$

Hence by Equation (1) we see that $r^is^jH = Hr^is^j$ and H is a normal subgroup.

c) By Lagrange's theorem D_6/H is a group of order $12/3 = 4$ so it is in principle possible for D_6/H to be isomorphic to $\mathbb{Z}_4$. However the multiplication tables of these two groups do not match. A way of seeing it is by recalling that $\mathbb{Z}_4$ is a cyclic group of order 4 generated by 1, that is, $\mathbb{Z}_4$ contains an element of order 4. This is not true for D_6/H. In fact

$$D_6/H = \{H, rH, sH, rsH\}$$

, and H has order 1 (it is the identity element), while

$$(rH)^2 = r^2H = H$$

as $r^2 \in H$ (and H is a subgroup). So rH has order 2. Similarly

$$(sH)^2 = s^2H = idH = H,$$

as $id \in H$ (and H is a subgroup), so sH has order 2. Finally

$$(rsH)^2 = ((rs)^2H) = idH = H,$$

so also rsH has order 2 (here we used that $(rs)^2 = rs \circ rs = rs \circ sr^{-1} = rs^2r^{-1} = r \circ r^{-1} = id$).

This shows that every element in D_6/H has order 1 or 2, so an element of order 4 does not exist.

Question 3

a) Suppose that x is nilpotent. Then there exists a positive integer m such that $x^m = 0_R$. Denote with M the smallest positive integer m such that $x^m = 0$ If $x = 0_R$ then we are done, so let assume that $x \neq 0_R$ and let us prove that x is a zero divisor. Note that $M > 1$ as $x \neq 0$ (if $M = 1$ then $x^M = 0_R$ implies $x = 0_R$). One has

$$0_R = x^M = x \cdot x^{M-1}.$$

This shows that x is a zero-divisor. In fact $x^{M-1} \neq 0_R$ by the minimality of M.

b) Suppose that x is nilpotent. Then there exists a positive integer m such that $x^m = 0_R$. Using that R is commutative we get

$$(r \cdot_r x)^m = r^m \cdot_R x^m = r^m \cdot_R 0_R = 0_R,$$

by an exercise we solved in class. This means that $r \cdot_R x$ fullfills the definition of being nilpotent (with the same positive integer m as x).

c) Suppose that x is nilpotent. Then there exists a positive integer m such that $x^m = 0_R$.To prove that $1_R +_R x$ is a unit we need to find an inverse. Following the hint we see that

$$1_R +_R x^m = 1_R +_R 0_R = 1_R,$$

and

$$1_R +_R (-x^m) = 1_R +_R (-0_R) = 1_R.$$

We dive the case in which m is even and m is odd.

- Case 1: m is even. Consider the polynomial $X^m + (-1_R) \in R[X]$. We claim that -1_R is a root of this polynomial. This is true because

  $$(-1_R)^m +_R (-1_R) = 1_R +_R (-1_R) = 0_R.$$

  Here we used that $(-1_R) \cdot_R (-1_R) = 1_R$ (this was an exercise) and hence -1_R to an even power is equal to 1_R (while to an odd power would be -1_R). By a proposition in the notes this means that $X - (-1_R) = X + 1_R$ divides $X^m + (-1_R)$, say

  $$X^m + (-1_R) = (X + 1_R) \cdot q(X).$$

  Evaluating in our initial x gives (if two polynomials are equal of course their evaluations are equal!)

  $$x^m +_R (-1_R) = (x +_R 1_R) \cdot_R q(x),$$

  where we do not know $q(x)$ but we know that $q(x) \in R$. From above (the hint) we know that $x^m +_R (-1_R) = 1_R$, so substituting above we get

  $$1_R = (x +_R 1_R) \cdot_R q(x) = q(x) \cdot_R (x +_R 1_R),$$

  where in the last equality we used that R is commutative. This proves that $q(x)$ is the multiplicative inverse of $x +_R 1_R$, which is hence a unit.

- Case 2: m is odd. Consider the polynomial $X^m + 1_R \in R[X]$ and argue as above. We claim that -1_R is a root of this polynomial. This is true because
$$(-1_R)^m +_R 1_R = -1_R +_R 1_R = 0_R.$$
By a proposition in the notes this means that $X - (-1_R) = X + 1_R$ divides $X^m + 1_R$, say
$$X^m + 1_R = (X + 1_R) \cdot q(X).$$
Evaluating in our initial x gives (if two polynomials are equal of course their evaluations are equal!)
$$x^m +_R 1_R = (x +_R 1_R) \cdot_R q(x),$$
where we do not know $q(x)$ but we know that $q(x) \in R$. From above (the hint) we know that $x^m +_R 1_R = 1_R$, so substituting above we get
$$1_R = (x +_R 1_R) \cdot_R q(x) = q(x) \cdot_R (x +_R 1_R),$$
where in the last equality we used that R is commutative. This proves that $q(x)$ is the multiplicative inverse of $x +_R 1_R$, which is hence a unit.

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!)
$$q(X) = X^2 + X$$
and
$$r(X) = 1$$
Hence the standard form is $1 + \langle X^4 + 3X^2 + X + 5 \rangle$.

b) The first natural step to factorize $f(X) := X^4 + 3X^2 + 2X + 5$ is to find whether it has roots. Doing so yields that 6 is a root, implying that $(X - 6) = (X + 1)$ divides $f(X)$. Using long division gives $f(X) = (X+1)(X^3 + 6X^2 + 4X + 5)$. Since it has degree 3, the polynomial $g(X) := X^3 + 6X^2 + 4X + 5$ is irreducible if and only if it does not have any root in $\mathbb{F}_7$. However one sees immediately that 3 is a root of $g(X)$ and hence $(X - 3) = (X + 4)$ divides

$g(X)$. Using long division gives $g(X) = (X+4)(X^2+2X+3)$. Since the polynomial (this can be checked by hands) X^2+2X+3 has degree 2 and no roots it is irreducible. All in all we got that the desired factorization of $f(X)$ is

$$f(X) = (X+1)(X+4)(X^2+2X+3).$$

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

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

that is

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

hence multiplying by 3:

$$1 = 3 \cdot (X^4+3X^2+2X+5) + X(4X^3+5X+1)$$

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

$$4X^3+5X+1+\langle X^4+3X^2+2X+5\rangle.$$

d) 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 $h(X)$ is any of those proper factors then $h(X) + \langle X^4+3X^2+2X+5\rangle$ is a zero-divisor and so is $a(X) \cdot h(X) + \langle X^4+3X^2+2X+5\rangle$ for all polynomials $a(X)$ such that $\deg(a(X)) + \deg(h(X)) < 4$. Hence from part b) $h(X) + \langle f(X)\rangle$ is a zero divisor for all polynomials

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

giving rise to 18 distinct zero-divisors in R when we multiply each of them by a non-zero constant $a \in \mathbb{F}_7$. To get the final zero-divisor it is enough to consider

$$(X+1)(X+4) + \langle X^4+3X^2+2X+5\rangle.$$