Exam May 2025- answers

Question 1

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

b) First note that $g_1 = (1\ 4)(2\ 6\ 3)$ and $g_2 = (1\ 5)(2\ 3\ 4\ 6)$. Hence the orders of g_1 and g_2 are $6 = lcm(2,3)$ and $4 = lcm(2,4)$ respectively. The cycle type of g_1 is $(1,1,1,0,0,0)$ and the one of g_2 is $(0,1,0,1,0,0)$.

c) If $\tau \circ g_1 = g_1 \circ \tau$ then applying these map to 5 gives

$$\tau[g_1[5]] = g_1[\tau[5]].$$

Using that $g_1[5] = 5$ we get

$$\tau[g_1[5]] = \tau[5] = g_1[\tau[5]].$$

Hence g_1 fixes $\tau[5]$ and since 5 is the only element fixed by g_1 we obtain that necessarily $\tau[5] = 5$. Using the same trick for 1 and 4 gives

$$\tau[4] = \tau[g_1[1]] = g_1[\tau[1]],$$

and

$$\tau[1] = \tau[g_1[4]] = g_1[\tau[4]].$$

Combining the two espressions obtained above we get

$$\tau[4] = g_1[\tau[1]] = g_1[g_1[\tau[4]]] = g_1^2[4],$$

which means that $g_1^2 = (2\ 3\ 6)$ fixes $\tau[4]$.Since g_1^2 fixes only 1, 4 and 5 and $\tau[5] = 5$ this shows that $\tau[4] \in \{1,4\}$. If $\tau[4] = 4$ then $\tau[1] = g_1[\tau[4]] = g_1[4] = 1$. If instead $\tau[4] = 1$ then $\tau[1] = g_1[\tau[4]] = g_1[1] = 4$. In any case we got that $\tau[1] \in \{1,4\}$ and so $\tau(\{1,4\}) = \{1,4\}$.

d) From (c) we know that $\tau[5] = 5$ and either $(\tau[1], \tau[4]) = (1,4)$ or $(\tau[1], \tau[4]) = (4,1)$ (that is either τ acts as the two cycle $(1\ 4)$ on $\{1,4\}$ or the identity). Since τ is a permutation (it is bijective) we necessarily have that $\tau(\{2,3,6\}) = \{2,3,6\}$. In order to understand the action of τ in this set note that

$$g_1[\tau[2]] = \tau[g_1[2]] = \tau[6],$$
$$g_1[\tau[3]] = \tau[g_1[3]] = \tau[2],$$
$$g_1[\tau[6]] = \tau[g_1[6]] = \tau[3].$$

With this in mind, we treat the cases τ acts as the two cycle $(1\ 4)$ on $\{1,4\}$ or the identity, separately:

– Case 1: τ acts as the two cycle $(1\ 4)$ on $\{1,4\}$. Recall that $\tau[2] \in \{2,3,6\}$. From the three identity above if $\tau[2] = 2$ then $g_1[\tau[3]] = 2$ and hence $\tau[3] = 3$ and lastly $\tau[6] = g_1[\tau[2]] = g_1[2] = 6$. Hence in this case $\tau = (1\ 4) = g_1^3$. Suppose instead $\tau[2] = 3$. Then $g_1(\tau[3]) = \tau[2] = 3$ and hence $\tau[3] = 6$ and finally $\tau[6] = g_1(\tau[2]) = g_1(3) = 2$. Hence in this case $\tau = (1\ 4)(2\ 3\ 6) = g_1^5$. Finally suppose instead $\tau[2] = 6$. Then $g_1(\tau[3]) = 6$ which means that $\tau[3] = 2$ and $\tau[6] = 3$. Hence $\tau = (1\ 4)(2\ 6\ 3) = g_1$.
– Case 2: τ acts as the identity on $\{1,4\}$. Then recall as before that $\tau[2] \in \{2,3,6\}$. From the three identity above if $\tau[2] = 2$ then $g_1[\tau[3]] = 2$ and hence $\tau[3] = 3$ and lastly $\tau[6] = g_1[\tau[2]] = g_1[2] = 6$. Hence in this case $\tau = id = g_1^6$. Suppose instead $\tau[2] = 3$. Then $g_1(\tau[3]) = \tau[2] = 3$ and hence $\tau[3] = 6$ and finally $\tau[6] = g_1(\tau[2]) = g_1(3) = 2$. Hence in this case $\tau = (2\ 3\ 6) = g_1^2$. Finally suppose instead $\tau[2] = 6$. Then $g_1(\tau[3]) = 6$ which means that $\tau[3] = 2$ and $\tau[6] = 3$. Hence $\tau = (2\ 6\ 3) = g_1^4$.

Question 2

a) Note that A is not empty as $e_1 \in A$ (the identity element of G_1). In fact $f(e_1) = e_2 = g(e_1)$ as both f and g are homomorphisms. We can use a result from the notes that says that A is a subgroup of G_1 if and only if $x^{-1} \cdot_1 y \in A$ for all $x, y \in A$. This means that we need to check that for all $x, y \in A$ one has $x^{-1} \cdot_1 y \in A$. Let $x, y \in A$ arbitrary. This means that $f(x) = g(x)$ and $f(y) = g(y)$. Then using that f and g are homomorphisms (and so they preserves the group operations and inverses)

$$f(x^{-1} \cdot_1 y) = f(x^{-1}) \cdot_2 f(y) = f(x)^{-1} \cdot_2 f(y) = g(x)^{-1} \cdot_2 g(y) = g(x^{-1}) \cdot g(y) = g(x^{-1} \cdot_1 y),$$

which shows that $x^{-1} \cdot_1 y \in A$.

b) Suppose that G_2 is abelian. We want to prove that H is a normal subgroup, and to do that it is enough to recognize it as the kernel of a group homomorphism. Consider in fact the map

$$\varphi : \begin{cases} G_1 \to G_2, \\ x \mapsto f(x^{-1}) \cdot_2 g(x). \end{cases}$$

Then φ is a group homomorphism. In fact $\varphi(e_1) = f(e_1^{-1}) \cdot_2 g(e_1) = e_2 \cdot_2 e_2 = e_2$ (here I used that both f and g are group homomorphisms). Also in

$x, y \in G_1$ then

$$\varphi(x \cdot_1 y) = f((x \cdot_1 y)^{-1}) \cdot_2 g(x \cdot_1 y) = f(y^{-1} \cdot_2 x^{-1}) \cdot_2 g(x) \cdot_2 g(y) = f(y^{-1}) \cdot_2 f(x^{-1}) \cdot_2 g(x) \cdot_2 g(y).$$

Using that G_2 is abelian (and associative) we get

$$\varphi(x \cdot_1 y) = f(y^{-1}) \cdot_2 f(x^{-1}) \cdot_2 g(x) \cdot_2 g(y) = (f(x^{-1}) \cdot_2 g(x)) \cdot_2 (f(y^{-1}) \cdot_2 g(y)) = \varphi(x) \cdot_2 \varphi(y).$$

On the other hand by definition of Kernel:

$$\ker \varphi = \{x \in G_1 \mid f(x^{-1}) \cdot_2 f(x) = e_2\} = \{x \in G_1 \mid f(x) \cdot_2 f(x^{-1}) \cdot_2 g(x) = f(x) \cdot_2 e_2\}$$

$$= \{x \in G_1 \mid f(x) \cdot_2 f(x)^{-1} \cdot_2 g(x) = f(x)\} = \{x \in G_1 \mid g(x) = f(x)\} = A.$$

Hence A is the Kernel of the group homomorphism φ, and so a normal subgroup of G_1.

c) Assume that the order of G_1 is 36, the order of G_2 is 3 and $|A|$ is divisible by 9. Then the isomorphism theorem applied to φ from (b) gives $G_1/A \cong Im\varphi$, where $Im\varphi$ is a subgroup of G_2. Looking at the orders of these groups (and recalling that from Lagrange's theorem the order of a subgroup divides the order of the group) we get that

$$\frac{|G_1|}{|A|} = \frac{36}{|A|} \textit{ divides } |G_2| = 3.$$

Since 9 divides $|A|$ and $36 = 9 \cdot 4$ then $|G_1|/|A|$ is not divisible by 3 (and hence it cannot be three). Since the only divisors of 3 are 1 and 3, we get that $36/|A| = 1$, that is, $|A| = 36 = |G_1|$. Since $A \subseteq G_1$ then $A = G_1$ which means that $f(x) = g(x)$ for all $x \in G_1$. This implies that the two maps $f, g : G_1 \to G_2$ are equal, that is, $f = g$ as claimed.

Question 3

a) The zero-element E_0 (respectively one-element E_1) need to be a subgroup of S such that $(E_0 \cup Y) \setminus (E_0 \cap Y) = Y$ for all subset Y of S (respectively $E_1 \cap Y = Y$ for all Y subset of S). Hence $E_0 = \emptyset$ and $E_1 = S$. This can be checked by inserting in the equality above.

b) We need to prove that for all subset $X \subsetneq S$ there exists another subset $Y \subsetneq S$ such that $X \cap Y = E_0 = \emptyset$ (here we used part (a)). It is enough to choose $Y := S \setminus X$. In fact this is a proper subset of S and clearly $X \cap (S \setminus X) = \emptyset$.

c) By definition of principal ideal

$$\langle Y \rangle = \{Y \cap X \mid X \subseteq S\} = \{Z \mid Z \subseteq Y\} = \mathscr{P}(Y).$$

d) Suppose that S is finite, so that $\mathscr{P}(S)$ is finite as well. Let I be an ideal of S. If $I = \{E_0\} = \emptyset$ then $I = \langle \emptyset \rangle = \mathscr{P}(\emptyset)$ (here I used part (c)). Suppose so that I is not empty. Since I contains a finite number of elements write $I = \{X_1, \ldots, X_s\}$. Let $Y := X_1 \cup X_2 \cup \ldots \cup X_s$. Then $I = \langle Y \rangle$. One can show this by first noting that $Y \in I$ (one can prove this by induction on s), which implies $\langle Y \rangle \subseteq I$. But since $X_i \in \langle Y \rangle$ for all $i = 1, \ldots, s$ also the other inclusion holds.

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

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

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

b) The first natural step to factorize $f(X) := X^4 + 3X^2 + X + 2$ 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 $f(X) = (X+1)(X^3 + 4X^2 + 4X + 2)$. Since it has degree 3, the polynomial $g(X) := (X^3 + 4X^2 + 4X + 2$ 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 $f(X) = (X+1)(X^3 + 4X^2 + 4X + 2)$ is the desired product of irreducible factors for $f(X)$.

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

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

swapping the rows gives

$$\begin{bmatrix} X^2 + 2 & 0 & 1 \\ X & 1 & h(X) \end{bmatrix}, \underset{R_1 \mapsto R_1 + 4XR_2}{\longrightarrow} \begin{bmatrix} 2 & 4X & 4Xh(X) + 1 \\ X & 1 & h(X) \end{bmatrix},$$

that is

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

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

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

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

d) The natural idea is to try to find proper monic factors of the generator of the ideal $f(X) := X^4 + 3X^2 + X + 2$, which is what we did in part (b) of this question. Indeed if $g(X)$ is any of those proper factors then $g(X) + \langle X^4 + 3X^2 + X + 2\rangle$ is a zero-divisor and so is $a(X) \cdot g(X) + \langle X^4 + 3X^2 + X + 2\rangle$ for all polynomials $a(X)$ such that $\deg(a(X)) + \deg(g(X)) < 4$. Hence from part b) $g(X) + \langle X^4 + 3X^2 + X + 2\rangle$ is a zero divisor for all polynomials

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

Considering $a(X)$ any polynomial of degree at most 2 gives $a(X)(X + 1) + \langle X^3 + 4X^2 + 4X + 2\rangle$ is a zero-divisor. We can construct 4^3 any such polynomials (4 choices per each of the coefficients of $a(X)$), giving already more than required.