Exam 2021- answers

Question 1

a) $f = (1\ 7\ 14)(2\ 13\ 9\ 10\ 6)(3\ 12\ 11\ 5\ 8\ 4)$.

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 $ord(f) = lcm(3,5,6) = 30$.

c) Recall that since f has order 30, $G = \{f^0, \ldots, f^{29}\}$. Also for all exponent $i = 0, \ldots, 29$, $ord(f^i) = ord(f)/GCD(i, ord(f)) = 30/GCD(i,30)$. So the order of f^i is odd if and only if i is even (because in this way 2 divides $GCD(i,30)$ and hence $30/GCD(i,30)$ is odd). Hence

$$H = \{f^i \mid i = 0, \ldots, 29 \textit{ and } i \equiv 0 \pmod 2\} = \{f^{2k} \mid k = 0, \ldots, 14\}$$

$$= \{(f^2)^k \mid k = 0, \ldots, 14\}) = \langle f^2 \rangle.$$

For the last equality note that since $\langle f^2 \rangle$ contains all the powers of f^2 clearly $\{(f^2)^k \mid k = 0, \ldots, 14\} \subseteq \langle f^2 \rangle$. On the other hand since $ord(f^2) = 30/GCD(30,2) = 30/2 = 15$, $|\langle f^2 \rangle = 15 = |\{(f^2)^k \mid k = 0, \ldots, 14\}|$, the two sets must coincide. Since this proves that H is the cyclic subgroup of G generated by f^2, we have both that H is a subgroup of G and H is cyclic.

Question 2

a) Since ϕ is assumed to be a group homomorphism we know that $\phi(rs) = \phi(r) \circ \phi(s)$ and $\phi(r^2) = \phi(r)^2 = \phi(r) \circ \phi(r)$. Hence

$$\phi(rs) = (1234)(24) = (12)(34),$$

and similarly

$$\phi(r^2) = (1234)(1234) = (13)(24).$$

b) By definition

$$\phi(C_4) = \{\phi(e), \phi(r), \phi(r)^2, \phi(r)^3\}.$$

From part a) we know that $phi(r)^2 = (13)(24)$, while from the assumption ϕ homomorphism we also know that $\phi(e) = id$, the identiy permutation. We can compute $\phi(r)^3$ as $\phi(r^2) \circ \phi(r)$ obtaining

$$\phi(r^3) = (13)(24)(1234) = (1432).$$

Hence

$$\phi(C_4) = \{id, (1234), (13)(24), (1432)\}.$$

note that $\phi(C_4)$ is a subgroup of S_4 as $\phi(C_4) = \{\phi(r)^i \mid i = 0, \ldots 3\} = \langle(1234)\rangle$, the cyclic subgroup generated by (1234). However this subgroup is not normal as the following counterexample shows. Following the hint we prove indeed that $(12) \circ \phi(C_4) \neq \phi(C_4) \circ (12)$. In fact one has

$$(12) \circ \phi(C_4) = \{(12), (12)(1234), (12)(13)(24), (12)(1432)\} = \{(12), (234), (1324), (143)\}$$

while

$$\phi(C_4) \circ (12) = \{(12), (1234)(12), (13)(24)(12), (1432)(12)\} = \{(12), (134), (1423), (243)\},$$

which do not coincide. This shows that it is not true for all $f \in S_4$ that $f \circ \phi(C_4) = \phi(C_4) \circ f$ and so $\phi(C_4)$ is not a normal subgroup.

c) We first show that $\psi(H)$ is a subgroup of G_2 and then we show its normality. Note that $\psi(H)$ is not empty, as $e_1 \in H$ (as H is a subgroup of G_1 it contains the identity element of G_1) and hence $\psi(e_1) = e_2 \in H$. So $\psi(H)$ is a subgroup of G_2 if and only if $f^{-1} \cdot_2 g \in \psi(H)$ for all $f, g \in \psi(H)$. Note that this property holds for H as it is a subgroup of G_1, that is for all $h_f, h_g \in H$ it is true that $h_f^{-1} \cdot_1 h_g^{-1} \in H$.

Let so $f, g \in \psi(H)$. By definition we can find $h_f, h_g \in H$ such that $f = \psi(h_f)$ and $g = \psi(h_g)$. Hence

$$f^{-1} \cdot_2 g = \psi(h_f)^{-1} \cdot_2 \psi(h_g),$$

since φ is a group homomorphism

$$f^{-1} \cdot_2 g = \psi(h_f)^{-1} \cdot_2 \psi(h_g) = \psi(h_f^{-1} \cdot_1 h_g).$$

This shows that $f^{-1} \cdot_2 g$ is the image of $h_f^{-1} \cdot_1 h_g$ which is in H as $h_f, h_g \in H$. This implies by definition that $f^{-1} \cdot_2 g \in \psi(H)$ which is hence a subgroup of G_2.

To prove normality we want to show that $f \cdot_2 \psi(H) = \psi(H) \cdot_2 f$ for all $f \in G_2$. Since H is normal in G_1 we know that $h_f \cdot_1 H = H \cdot_1 h_f$ for all $h_f \in G_1$.

So let $f \in G_2$ arbitrary. Since ψ is surjective there must exist $h_f \in G_1$ such that $f = \psi(h_f)$. Hence

$$f \cdot_2 \psi(H) = \psi(h_f) \cdot_2 \psi(H) = \{\psi(h_f) \cdot_2 \psi(h) \mid h \in H\} = \{\psi(h_f \cdot_1 h) \mid h \in H\}.$$

Since $h_f \cdot_1 H = H \cdot_1 h_f$ we know that for all $h \in H$ there must exist $h' \in H$ such that $h_f \cdot_1 h = h' \cdot_1 h_f$. Thus

$$\{\psi(h_f \cdot_1 h) \mid h \in H\} = \{\psi(h' \cdot_1 h_f) \mid h' \in H\} = \{\psi(h') \cdot_2 \psi(h_f) \mid h' \in H\} = \psi(H) \cdot_2 f.$$

Question 3

This is part of Homework Assignment 3 (so no solution will be added)

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

$$q(X) = X^3 + X + 1$$

and

$$r(X) = 1.$$

Indeed

$$q(X)(X^4 + X^3 + X^2 + 2X + 1) + r(X) =$$
$$(X^3 + X + 1)(X^4 + X^3 + X^2 + 2X + 1) + 1 = X^7 + X^6 + 2X^5 + X^4 + 2.$$

Hence the standard form is $1 + \langle X^4 + X^3 + X^2 + 2X + 1 \rangle$, the one-element of the ring.

b) The natural idea is to try to find proper monic factors of the generator of the ideal $f(X) := X^4 + X^3 + X^2 + 2X + 1$. Indeed if $g(X)$ is any of those proper factors then $g(X) + \langle X^4 + X^3 + X^2 + 2X + 1 \rangle$ is a zero-divisor and so is $a(X) \cdot g(X) + \langle X^4 + X^3 + X^2 + 2X + 1 \rangle$ for all polynomials $a(X)$ such that $\deg(a(X)) + \deg(g(X)) < 4$. To obtain proper factors the easiest idea is to try first to find roots of the polynomial. Note that

$$f(2) = 2^4 +_3 2^3 +_3 2^2 +_3 2 \cdot_3 2 +_3 1 = 33 \pmod 3 = 0$$

and

$$f(1) = 1^4 +_3 1^3 +_3 1^2 +_3 2 \cdot_3 1 +_3 1 = 6 \pmod 3 = 0.$$

Hence both $X - 2 = X + 1$ and $X - 1 = X + 2$ are proper factors of $f(X)$. Hence $g(X) + \langle f(X) \rangle$ is a zero divisor for all polynomials

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

giving rise to 4 distinct zero-divisors in R.

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

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

that is

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

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

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

d) No, as from the characterization of elements in quotient rings of polynomials every coset is either a unit, or a zero-divisor of the zero-coset $0 + \langle X^4 + X^3 + X^2 + 2X + 1 \rangle$.