Exam 2020- answers

Question 1

a) $f = (123)(345)(456) = (1234)(56)$.

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 $ord(f) = lcm(4,2) = 4$.

c) Let $f \in S_6$ and write $f = c_1 \circ c_2 \circ \ldots \circ c_k$ disjoint cycles decomposition where c_i is a cycle of length ℓ_i for $i = 1, \ldots, k$. To compute $ord(f) = lcm(\ell_1, \ldots, \ell_k)$ we need to understand how the different cycle lengths ℓ_i can be.

To do so, let m denote the maximum of the lengths ℓ_i of the cycles c_i with $i = 1, \ldots, k$. Clearly $m \leq 6$. We divide some cases:

- $m = 6$. Then $k = 1$ and f is a 6-cycle. The order of f is 6 in this case.
- $m = 5$. Then f is a 5-cycle (recall that any 1-cycle is just the identity permutation). Hence the order of f is 5 in this case.
- $m = 4$. Hence either f is a 4-cycle, or the composition of a 4-cycle and a 2-cycle. In any case the order of f is 4 as $lcm(4,2) = 4$.
- $m = 3$. Here either f is a 3-cycle, or the composition of 2 3-cycles or the composition of a 3-cycle and a 2-cycle. In the first 2 cases the order of f is 3 while in the last case $ord(f) = lcm(3,2) = 6$.
- $m = 2$. Then f is composition of 2-cycles and hence its order is 2.

We conclude that the order of f is at most 6.

Question 2

a) First of all note that $H := \{g \in G \mid \psi(g) = g\}$ is not empty as $e \in H$ from one of the axioms of ψ being a group homomorphism. Since H is not empty we can use the characterization that H is a subgroup if and only if $f^{-1} \cdot g \in H$ for all $f, g \in H$. So let $f, g \in H$ arbitrary. Clearly $f^{-1} \cdot g \in G$. Then by definition of H we need to check that $\psi(f^{-1} \cdot g) = f^{-1} \cdot g$. However this is true because using ψ being a group homomorphism one has

$$\psi(f^{-1} \cdot g) = \psi(f^{-1}) \cdot \psi(g) = \psi(f)^{-1} \cdot \psi(g).$$

Since $f, g \in H$ we know that $\psi(f) = f$ and $\psi(g) = g$ and hence

$$\psi(f^{-1} \cdot g) = \psi(f)^{-1} \cdot \psi(g) = f^{-1} \cdot g,$$

and H is a subgroup of G.

b) We need to check that $\varphi(e) = e$ and that $\varphi(f \circ g) = \varphi(f) \circ \varphi(g)$ for all $f, g \in D_6$. Simply by using the definition of φ and remembering that $s^2 = e$ we see that

$$\varphi(e) = s \circ e \circ s = s \circ s = s^2 = e,$$

and the first axiom holds. For the second one, let $f, g \in D_6$. Then using associativity and again $s^2 = e$,

$$\varphi(f \circ g) = s \circ (f \circ g) \circ s = s \circ f \circ e \circ g \circ s = s \circ f \circ s^2 \circ g \circ s$$

$$= (s \circ f \circ s) \circ (s \circ g \circ s) = \varphi(f) \circ \varphi(g),$$

and so φ is a group homomorphism.

c) The 12 elements in D_6 can be divided into two categories:

- **Type I**: r^i with $i = 0, \ldots, 5$ and
- **Type II**: $r^i s$ with $i = 0, \ldots, 5$.

Now clearly

$$\{g \in D_6 \varphi(g) = g\} = \{r^i \mid i = 0, \ldots 5,\ \varphi(r^i) = r^i\} \cup \{r^i s \mid i = 0, \ldots 5,\ \varphi(r^i s) = r^i s\}.$$

Note that since for all $i = 0, \ldots, 5$ it holds $r^i \circ s = s \circ r^{6-i}$ one has

$$\varphi(r^i) = s \circ r^i \circ s = r^{6-i} \circ s^2 = r^{6-i}.$$

Hence $\varphi(r^i) = r^i$ if and only if $i = 0$ or $i = 3$. This shows that

$$\{r^i \mid i = 0, \ldots 5,\ \varphi(r^i) = r^i\} = \{r^0, r^3\} = \{e, r^3\}.$$

Omn the other hand for all $i = 0, \ldots, 5$,

$$\varphi(r^i s) = s \circ r^i \circ s^2 = s \circ r^i = r^{6-i} \circ s.$$

This shows that again $\varphi(r^i s) = r^i s$ if and only if $i = 0$ or $i = 3$ and so

$$\{r^i s \mid i = 0, \ldots 5,\ \varphi(r^i s) = r^i s\} = \{s, r^3 s\}.$$

We have just proved that

$$\{g \in D_6 \varphi(g) = g\} = \{e, r^3, s, r^3 s\}.$$

Question 3

a) The ring R contains 5^3 elements.

b) Yes, an example is $X+4+\langle X^3+X-2\rangle$.

c) We use the Euclidean algorithm which gives (recall that $-2 \pmod 5 = 3$):

$$\begin{bmatrix} X^3+X+3 & 1 & 0 \\ X^2 & 0 & 1 \end{bmatrix} \begin{array}{c} \longrightarrow \\ R_1 \mapsto R_1+4XR_2 \end{array} \begin{bmatrix} X+3 & 1 & 4X \\ X^2 & 0 & 1 \end{bmatrix}.$$

We interchange the rows R_1 and R_2 and proceed then in the same way

$$\begin{bmatrix} X^2 & 0 & 1 \\ X+3 & 1 & 4X \end{bmatrix} \begin{array}{c} \longrightarrow \\ R_1 \mapsto R_1+4XR_2 \end{array} \begin{bmatrix} 2X & 4X & 1+X^2 \\ X+3 & 1 & 4X \end{bmatrix}$$

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

that is

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

Multiplying everything by 4 (modulo 5) we get

$$1 = 4 \cdot_5 4 = 4\cdot(4X+3)\cdot(X^3+X+3)+4\cdot(X^2+2X+1)\cdot X^2.$$

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

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

d) Let $u = g(X)+\langle X^3+X-2\rangle \in R$ and assume without loss of generality that u is in standard form, that is, $\deg(g(X)) \leq 2$. If $g(X) \neq 0$ then u is not the zero-element and we know that either u is a zero-divisor or a unit. To count the number of units we count the number of zero-divisors instead. Indeed $|R| = 5^3 = N_z + N_u + 1$ where N_z is the number of zero-divisors, N_u is the number of units (and the $+1$ comes from adding the zero-coset).

So if we compute N_z then N_u will just be computed as $5^3 - 1 - N_z$.

Our coset $u = g(X)+\langle X^3+X-2\rangle \in R$ where $\deg(g(X)) \leq 2$ and $g(X) \neq 0$ is a zero-divisor if and only if $1 \leq \deg(GCD(X^3+X-2, g(X))) \leq 2$. Note that 1 is a root of X^3+X-2 and hence $X-1 = X+4$ divides X^3+X-2. Using division with remainder one sees that

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

The polynomial $X+4$ is clearly irreducible as it has degree 1. The polynomial X^2+X+2 is also irreducible as it has degree 2 and it has no roots in $\mathbb{Z}_5$ (this fact can be checked by computing by hands all the evaluations).

Since X^3+X+3 has only 1 as a root, its only monic factor of degree 1 is $X+4$. Also the only monic factor of degree 2 that X^3+X-2 can have is X^2+X+2. This means that $u = g(X)+\langle X^3+X-2\rangle \in R$ where $\deg(g(X)) \leq 2$ and $g(X) \neq 0$ is a zero-divisor if and only if $1 \leq \deg(GCD(X^3+X-2, g(X))) \leq 2$ and so if and only if either $GCD(X^3+X-2, g(X)) = X+4$ or $GCD(X^3+X-2, g(X)) = X^2+X+2$.

If $GCD(X^3+X-2, g(X)) = X+4$ since $\deg(g(X)) \leq 2$ we get that $g(X) = (X+4)(aX+b)$ for some $a,b \in \mathbb{Z}_5$ where $(a,b) \neq (0,0)$ (remember that $g(X) \neq 0$). This gives rise to $5^2-1 = 24$ zero-divisors.

If $GCD(X^3+X-2, g(X)) = X^2+X+2$ since $\deg(g(X)) \leq 2$ one has $g(X) = a(X^2+X+2)$ for some $a \in \mathbb{Z}_5 \setminus \{0\}$. This gives a total of 4 distinct zero-divisors.

Summing everything together we got $N_z = 24+4 = 28$ and hence the numner of units is $N_u = 5^3-1-28 = 96$.

Question 4

This is part of Homework Assignment 4! (so no solution will be added)