Math 417 **Homework 3** **Due Friday, September 18, 2020, 11:59pm**

It's ok to work together, but don't copy without comprehension. The symbol ($\mathcal{E}$) means that at least part of this problem is a former exam question.

---

1. ($\mathcal{E}$) Don't answer this question by citing the multiplication table for S_3, although I can't stop you from checking your answer. Let

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Determine α^2, $\alpha\beta$, $\beta\alpha$, and β^2.

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad (1 \to 2 \to 3, 2 \to 3 \to 1, 3 \to 1 \to 2) \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad (1 \to 1 \to 2, 2 \to 3 \to 1, 3 \to 2 \to 3) \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad (1 \to 2 \to 3, 2 \to 3 \to 2, 3 \to 1 \to 1) \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\beta^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad (1 \to 1 \to 1, 2 \to 3 \to 2, 3 \to 2 \to 3) \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

There are disguises: $\alpha = \rho_1$ and $\beta = \mu_1$, and $\rho_1^2 = \rho_2, \rho_1\mu_1 = \mu_3, \mu_1\rho_1 = \mu_2, \mu_1^2 = \rho_0$.

2. We have already seen that $G = ((\mathbb{Z}/9\mathbb{Z})^*, \odot)$ and $H = ((\mathbb{Z}/14\mathbb{Z})^*, \odot)$ are each cyclic groups of order 6. Write out, with explanation, an explicit isomorphism Φ from G to H. It should include six equations that look like $\Phi([a]_9) = [b]_{14}$, with specific integers for a, b.

We have seen that G is a cyclic group and $[2]_9$ is a generator: its powers are

$$\{[1]_9, [2]_9, [4]_9, [8]_9, [7]_9, [5]_9\}.$$

We have also seen that H is a cyclic group and $[3]_{14}$ is a generator: its powers are

$$\{[1]_{14}, [3]_{14}, [9]_{14}, [13]_{14}, [11]_{14}, [5]_{14}\}.$$

so a map Φ defined by

$$\Phi([2]_9^k) = [3]_{14}^k$$

will be a bijection and preserve the operation, hence is an isomorphism. To fulfill the request made:

$$\Phi([1]_9) = [1]_{14}, \quad \Phi([2]_9) = [3]_{14}, \quad \Phi([4]_9) = [9]_{14},$$
$$\Phi([8]_9) = [13]_{14}, \quad \Phi([7]_9) = [11]_{14}, \quad \Phi([5]_9) = [5]_{14}.$$

3. ($\mathcal{E}$) You are given the following two permutations in S_5

$$\sigma = \begin{pmatrix} 12345 \\ 13425 \end{pmatrix} = (1)(234)(5), \qquad \tau = \begin{pmatrix} 12345 \\ 34152 \end{pmatrix} = (13)(245).$$

Compute $\sigma\tau$ and $\tau\sigma$ and determine the smallest positive integer k so that τ^k is the identity.

$$\sigma\tau = \begin{pmatrix} 12345 \\ 13425 \end{pmatrix}\begin{pmatrix} 12345 \\ 34152 \end{pmatrix} \quad (1 \to 3 \to 4, 2 \to 4 \to 2, 3 \to 1 \to 1, 4 \to 5 \to 5, 5 \to 2 \to 3) :$$

$$\sigma\tau = \begin{pmatrix} 12345 \\ 42153 \end{pmatrix} = (1453)(2).$$

$$\tau\sigma = \begin{pmatrix} 12345 \\ 34152 \end{pmatrix}\begin{pmatrix} 12345 \\ 13425 \end{pmatrix} \quad (1 \to 1 \to 3, 2 \to 3 \to 1, 3 \to 4 \to 5, 4 \to 2 \to 4, 5 \to 5 \to 2) :$$

$$\tau\sigma = \begin{pmatrix} 12345 \\ 31542 \end{pmatrix} = (1352)(4).$$

For the powers of τ, it is easier to use the cycle notation, because the two cycles don't interfere with each other.

$$\tau = (13)(245), \tau^2 = (1)(3)(254), \tau^3 = (13)(2)(5)(4),$$
$$\tau^4 = (1)(3)(245), \tau^5 = (13)(254), \tau^6 = (1)(3)(2)(4)(5)$$

Another way to see this is that $\tau^k = (13)^k(245)^k$, and $(13)^k = (1)(3)$ if and only if k is a multiple of 2 and $(245)^k = (2)(4)(5)$ if and only if k is a multiple of 3, and so the smallest k for which $\tau^k = e$ is $lcm(2, 3) = 6$.

4. ($\mathcal{E}$) It is an arithmetic fact that

$$10^6 - 1 = 999999 = 999 \cdot 1001 = (3^3 \cdot 37) \cdot (7 \cdot 11 \cdot 13) \quad \text{and} \quad 5291 = 11 \cdot 13 \cdot 37.$$

Using this information, and without doing any more calculation, determine the decimal expansion of

$$\frac{400}{5291}.$$

Following previous examples, I'd note that $999999 = 5291 \cdot (3^3 \cdot 7) = 5291 \cdot 189$, so

$$\frac{400}{5291} = \frac{400 \cdot 189}{5291 \cdot 189} = \frac{75600}{999999} = .075600\ 075600\ 075600\ .$$

5. ($\mathcal{E}$) Someone tells you, correctly, that $((\mathbb{Z}/13\mathbb{Z})^*, \odot)$ is a cyclic group of order 12 and $[2]_{13}$ is a generator; that is, $\langle [2]_{13} \rangle = (\mathbb{Z}/13\mathbb{Z})^*$.

a. Determine all generators of $((\mathbb{Z}/13\mathbb{Z})^*, \odot)$.

b. Since 3 and 4 are divisors of 12, a cyclic group order 12 has a subgroup of order 3 and a subgroup of order 4. Write down the elements of the subgroups of $((\mathbb{Z}/13\mathbb{Z})^*, \odot)$ of order 3 and of order 4.

You will find it helpful to recall that for a cyclic group $C_n = \langle a \rangle$, we already know the formula $|\langle a^k \rangle| = \frac{n}{gcd(k,n)}$.

So, in C_{12}, since $\gcd(1, 12) = \gcd(5, 12) = \gcd(7, 12) = \gcd(11, 12) = 1$,

$$\langle a \rangle = \langle 5 \rangle = \langle a^7 \rangle = \langle a^{11} \rangle = C_{12}.$$

For example, the powers of a^5 in order are:

$$a^5, a^{10}, a^3, a^8, a, a^6, a^{11}, a^4, a^9, a^2, a^7.$$

which gives all of C_{12}. Since a^5 is a generator of the same group, the same reasoning implies that $(a^5), (a^5)^5, (a^5)^7, (a^5)^{11}$ are also generators. But we know $((\mathbb{Z}/12\mathbb{Z})^*, \odot)$ is a group, so this is just a rearrangment: a^5, a, a^{11}, a^7.

Moving on, $\gcd(2, 12) = \gcd(10, 12) = 2$, so

$$\langle a^2 \rangle = \langle a^{10} \rangle = \{e, a^2, a^4, a^6, a^8, a^{10}\}$$

is a subgroup of order $\frac{12}{2} = 6$.

And $\gcd(3, 12) = \gcd(9, 12) = 3$, so

$$\langle a^3 \rangle = \langle a^9 \rangle = \{e, a^3, a^6, a^9\}$$

is a subgroup of order $\frac{12}{3} = 4$, and

And $\gcd(4, 12) = \gcd(8, 12) = 4$, so

$$\langle a^4 \rangle = \langle a^8 \rangle = \{e, a^4, a^8\}$$

is a subgroup of order $\frac{12}{4} = 3$. Finally, And $\gcd(6, 12) = 6$, so

$$\langle a^6 \rangle = \{e, a^6\}$$

is a subgroup of order $\frac{12}{6} = 2$.

What was the question? Since you know that $[2]_{13}$ is a generator, the other generators are $[2^5]_{13} = [6]_{13}$, $[2^7]_{13} = [11]_{13}$, and $[2^1 1]_{13} = [2]_{13}$.

Since $[2^3]_{13} = [8]_{13}$, $[2^6]_{13} = [12]_{13}$, $[2^9]_{13} = [5]_{13}$, the subgroup of order 4 is

$$\{[1]_{13}, [8]_{13}, [12]_{13}, [5]_{13}\}.$$

Since $[2^4]_{13} = [16]_{13} = [3]_{13}$, $[2^8]_{13} = [9]_{13}$, the subgroup of order 3 is

$$\{[1]_{13}, [3]_{13}, [9]_{13}\}.$$