Problem 1. Find C(σ) for each $\sigma \in D_4$.

$$C(R_0) = \{R_0, R_{90}, R_{180}, R_{270}, F_1, F_2, E_1, E_2\}$$
$$C(R_{90}) = \{R_0, R_{90}, R_{180}, R_{270}\}$$
$$C(R_{180}) = \{R_0, R_{90}, R_{180}, R_{270}, F_1, F_2, E_1, E_2\}$$
$$C(R_{270}) = \{R_0, R_{90}, R_{180}, R_{270}\}$$
$$C(F_1) = \{R_0, R_{180}, F_1, F_2\}$$
$$C(F_2) = \{R_0, R_{180}, F_1, F_2\}$$
$$C(E_1) = \{R_0, R_{180}, E_1, E_2\}$$
$$C(E_2) = \{R_0, R_{180}, E_1, E_2\}$$

Problem 2. Show that $Z(G)$, the center of the group G, is a subgroup of G.

To show that $Z(G) \leq G$ I will use corollary 4.2.2. Since $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$ and $ge = eg$ this means $e \in Z(G)$ and since $e \in G$, $Z(G)$ is a nonempty subset of G. To show that the inverse exists in $Z(G)$ for all elements in $Z(G)$ I use the fact that G is a group, $g, g^{-1} \in G$, and g^{-1} has the property that $g^{-1}g = e = gg^{-1}$. By the definition of $Z(G)$ this means that for all $g \in Z(G)$, $g^{-1} \in Z(G)$. Using the associative property, suppose $a, b \in Z(G)$. Then,

$$(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab), \ \therefore ab \in Z(G)$$

Since it has been shown that $Z(G)$ is a non-empty subset of G, is closed under G's binary operation and there exists an inverse in $Z(G)$ for all elements in $Z(G)$, by corollary 4.2.2, $Z(G)$ is a subgroup of G.

Problem 3. Prove that

$$G = \left\{ \begin{bmatrix} 1-n & -n \\ n & 1+n \end{bmatrix} \;\middle|\; n \in \mathbb{Z} \right\}$$

is a group under matrix multiplication. Is G cyclic?

Proof. To prove that G is a group I will prove that it is a subgroup of $SL(2, \mathbb{Z})$. First, G is a nonempty subset of $SL(2, \mathbb{Z})$ because it contains the identity element of $SL(2, \mathbb{Z})$ when $n = 0$, that is, $e = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$. To show closure, assume $A, B \in G$. Since $\det(AB) = \det(A) \cdot \det(B)$ and for all $x \in G, \det(x) = (1-n)(1+n)+n^2 = 1$, then $\det(AB) = \det(A) \cdot (B) = 1 \cdot 1 = 1$. Since $SL(2, \mathbb{Z})$ contains all 2×2 matricies where their determinant is one, $A, B, AB \in SL(2, \mathbb{Z})$. This shows that G is closed. It is also true that for all elements in G, the determinant is nonzero, therefore all elements have an inverse which take the form $\frac{1}{1}\left[\begin{smallmatrix} 1+n & n \\ -n & 1-n \end{smallmatrix}\right]$ which is equivalent to $-1\left[\begin{smallmatrix} 1-n & -n \\ n & 1+n \end{smallmatrix}\right]$ which is the element in G produced by $-n$. So an inverse exists in G for all elements in G. Since G is closed under $SL(2, \mathbb{Z})$'s binary operation, matrix multiplication, and an inverse

exists for all $x \in G$, by corollary 4.2.2 G is a subgroup of $SL(2,\mathbb{Z})$. Therefore G is a group under matrix multiplication. □

G is a cyclic group with a generator of $\langle \left[\begin{smallmatrix} 0 & -1 \\ 1 & 2 \end{smallmatrix}\right] \rangle$ because $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 2 \end{smallmatrix}\right]^n, n \in \mathbb{Z}$ generates all elements in G.

Problem 4. Let x be an element in a group G. Assume $\text{ord}(x) = 8$. List the elements in $\langle x^2 \rangle, \langle x^3 \rangle, \langle x^4 \rangle$ and $\langle x^5 \rangle$. Use your results to determine $\text{ord}(x^2)$, $\text{ord}(x^3)$, $\text{ord}(x^4)$, and $\text{ord}(x^5)$.

The elements of these orders are:

$$\langle x^2 \rangle = \{x^2, x^4, x^6, e\}$$
$$\langle x^3 \rangle = \{x^3, x^6, x^1, x^4, x^7, x^2, x^5, e\}$$
$$\langle x^4 \rangle = \{x^4, e\}$$
$$\langle x^5 \rangle = \{x^5, x^2, x^7, x^4, x^1, x^6, x^3, e\}$$

Since the order of these generators is the cardinality of their set,

$$\text{ord}(x^2) = 4$$
$$\text{ord}(x^3) = 8$$
$$\text{ord}(x^4) = 2$$
$$\text{ord}(x^5) = 8$$

Problem 5. Find the order of the matrix $\begin{bmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}$ in $SL(2,\mathbb{R})$.

The order of the matrix is infinite. This is easy to see using the equivalent representation of this matrix, $\frac{1}{2} - \frac{\sqrt{3}}{2}i$. The order of this element is defined as the smallest positive integer n such that $\begin{bmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}^n = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$or, equivalently, $(\frac{1}{2} - \frac{\sqrt{3}}{2}i)^n = 1 + 0i = 1$. Using De Moivre's theorem

$$(\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta)$$

and expressing $\frac{1}{2}$ and $\frac{\sqrt{3}}{2}$ in terms of sine and cosine, I rewrite $(\frac{1}{2} - \frac{\sqrt{3}}{2}i)^n$ as $\cos(-\frac{n\pi}{3}) + i\sin(-\frac{n\pi}{3})$. So, solving for

$$\cos(-\frac{n\pi}{3}) + i\sin(-\frac{n\pi}{3}) = 1$$

I get

$$n = 6m,\ m \in \mathbb{Z}$$

Since $(\frac{1}{2} - \frac{\sqrt{3}}{2}i)^{6m} = \cos(-\frac{6m\pi}{3}) + i\sin(-\frac{6m\pi}{3}) = 1 + 0i$ is equivalent to $(\frac{1}{2} - \frac{\sqrt{3}}{2}i)^0 = \cos(0) + i\sin(0) = 1 + 0i$ in the complex plane, the only solution for

$$\begin{bmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}^n = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

is

$$\begin{bmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Since $n = 0$ is the only solution, and n is not a positive integer, the order is infinite.

Problem 6.

Problem 7. Let a be an element in a group with $\text{ord}(a) = 15$. *Without* explicitly listing the elements in the subgroup each a^i generates, *compute* (using a formula) the values of $\text{ord}(a^3)$, $\text{ord}(a^6)$, $\text{ord}(a^9)$, and $\text{ord}(a^{12})$.

Using theorem 5.1.6, $|a^k| = n/d$ where $d = \gcd(n, k)$. So

$$\begin{aligned} |a^3| &= \frac{15}{\gcd(15,3)} = \frac{15}{3} = 5 \\ |a^6| &= \frac{15}{\gcd(15,6)} = \frac{15}{3} = 5 \\ |a^9| &= \frac{15}{\gcd(15,9)} = \frac{15}{3} = 5 \\ |a^{12}| &= \frac{15}{\gcd(15,12)} = \frac{15}{3} = 5 \end{aligned}$$

are the values.

Problem 8. Consider $U_{75} = \langle\omega\rangle$, where $\omega = \text{cis}(2\pi/75)$. Compute (using an appropriate formula) the values of $\text{ord}_{U_{75}}(\omega^3), \text{ord}_{U_{75}}(\omega^5), \text{ord}_{U_{75}}(\omega^{15})$, and $\text{ord}_{U_{75}}(\omega^{25})$.

Since $\omega^{75} = \text{cis}(2\pi/75)^{75} = \cos(\frac{75\cdot 2\pi}{75}) + i\sin(\frac{75\cdot 2\pi}{75}) = \cos(2\pi) + i\sin(2\pi) = 1$ and 75 is the smallest power that $\text{cis}(2\pi/75)^{75}$ can be raised to equal one, $|\omega| = 75$. Using theorem 5.1.6, $|\omega^k| = n/d$ where $d = \gcd(n, k)$. So

$$\text{ord}_{U_{75}}(\omega^3) = \frac{75}{\gcd(75,3)} = \frac{75}{3} = 25$$

$$\text{ord}_{U_{75}}(\omega^5) = \frac{75}{\gcd(75,5)} = \frac{75}{5} = 15$$
$$\text{ord}_{U_{75}}(\omega^{15}) = \frac{75}{\gcd(75,15)} = \frac{75}{15} = 5$$
$$\text{ord}_{U_{75}}(\omega^{25}) = \frac{75}{\gcd(75,25)} = \frac{75}{25} = 3$$

Problem 9. Compute the values of $\text{ord}_{\mathbb{Z}_{130}}(7)$ and $\text{ord}_{\mathbb{Z}^*_{130}}(7)$.

Since the order of $\text{ord}_{\mathbb{Z}_{130}}(7) = \text{ord}_{\mathbb{Z}_{130}}(1^7)$. I can use theorem 5.1.6 to show that $\text{ord}_{\mathbb{Z}_{130}}(1^7) = \frac{130}{\gcd(130,7)} = \frac{130}{1} = 130 = \text{ord}_{\mathbb{Z}_{130}}(7)$. To find $\text{ord}_{\mathbb{Z}^*_{130}}(7)$, I show all elements that 7 generates.

$$\langle 7 \rangle = \{7, 49, 83, 61, 37, 129, 123, 81, 47, 69, 93, 1\}.$$

Since all of these elements are in $\mathbb{Z}^*_{130}$, $\text{ord}_{\mathbb{Z}^*_{130}}(7) = |\langle 7 \rangle| = 12$

Problem 10. Show that $\mathbb{Z}^*_{25} = \langle 13 \rangle$. Use this fact to find the other generators of $\mathbb{Z}^*_{25}$

Since all of the numbers relatively prime to 25 are {1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19,21,22,23,24}, I must show that these can be expressed as $13^n \pmod{25}$ where n is some positive integer.

$$13^2 = 19 \pmod{25}$$
$$13^3 = 22 \pmod{25}$$
$$13^4 = 19^2 = 11 \pmod{25}$$
$$13^5 = 13^2 \cdot 13^3 = 19 \cdot 22 = 18 \pmod{25}$$
$$13^6 = (13^3)^2 = 22^2 = 9 \pmod{25}$$
$$13^7 = 13^5 \cdot 13^2 = 19 \cdot 18 = 17 \pmod{25}$$
$$13^8 = (13^4)^2 = 21 \pmod{25}$$
$$13^9 = 13^8 \cdot 13 = 21 \cdot 13 = 23 \pmod{25}$$
$$13^{10} = (13^5)^2 = 18^2 = 24 \pmod{25}$$
$$13^{11} = 13^{10} \cdot 13 = 24 \cdot 13 = 12 \pmod{25}$$
$$13^{12} = 13^{11} \cdot 13 = 12 \cdot 13 = 6 \pmod{25}$$
$$13^{13} = 13^{12} \cdot 13 = 6 \cdot 13 = 3 \pmod{25}$$
$$13^{14} = 13^{13} \cdot 13 = 3 \cdot 13 = 14 \pmod{25}$$
$$13^{15} = 13^{14} \cdot 13 = 14 \cdot 13 = 7 \pmod{25}$$
$$13^{16} = 13^{15} \cdot 13 = 7 \cdot 13 = 16 \pmod{25}$$

$$13^{17} = 13^{16} \cdot 13 = 16 \cdot 13 = 8 \pmod{25}$$
$$13^{18} = 13^{17} \cdot 13 = 8 \cdot 13 = 4 \pmod{25}$$
$$13^{19} = 13^{18} \cdot 13 = 4 \cdot 13 = 2 \pmod{25}$$
$$13^{20} = 13^{19} \cdot 13 = 2 \cdot 13 = 1 \pmod{25}$$

This shows that $\langle 13 \rangle$ generates $\mathbb{Z}_{25}^*$. To show the other generators of $\mathbb{Z}_{25}^*$, I will use corollary 5.1.8. Since $\mathbb{Z}_{25}^* = \langle 13 \rangle$ by corollary 5.1.8, $\langle 13^k \rangle$ where $\gcd(k, n) = 1$ is also a generator of $\mathbb{Z}_{25}^*$. So, I need to find the values of k where $\gcd(20, k) = 1$, or the relative prime numbers to 20. Those are, {1,3,7,9,11,13,17,19}. So the generators are:

$$\langle 13 \rangle, \langle 22 \rangle, \langle 17 \rangle, \langle 23 \rangle, \langle 12 \rangle, \langle 3 \rangle, \langle 8 \rangle, \langle 2 \rangle$$

Problem 11. Without actually computing the orders, explain why the two elements 2 and 28 must have the same order in $\mathbb{Z}_{30}$. How about 8 and 22 in $\mathbb{Z}_{20}$? Do they have the same order? Do the same for the pair 2 and 8 in $\mathbb{Z}_{15}^*$

Using corollary 5.1.6, If $G = \langle a \rangle$, $|G| = n$ and $k|n$, then $|a^k| = n/\gcd(n, k)$, and using the fact that for all integers $n > 1$, $\mathbb{Z}_n = \langle 1 \rangle$, I will show that $|1^2| = |1^{28}|$ in $\mathbb{Z}_{30}$. Rewriting, I get $|1^2| = 30/\gcd(30, 2) = 30/2 = 15$ and $|1^{28}| = 30/\gcd(30, 28) = 30/2 = 15$. Therefore the order of 2 and 28 are equal. Using a similar approach I now want to show that $|1^8| = |1^{22}|$. Rewriting I get $|1^8| = 20/\gcd(20, 8) = 20/4 = 5$ and $|1^{22}| = 20/\gcd(20, 22) = 20/2 = 10$. Therefore 8 and 22 do not have the same order. Next, I want to show that $|a^2| = |a^8|$ in $\mathbb{Z}_{15}^*$. Since the order of $\mathbb{Z}_{15}^* = 8$, and $\gcd(8, 2) = 2$ and $\gcd(8, 8) = 8$. This shows that $|a^2| \neq |a^8|$.

Problem 12. What are the possible orders of the elements of D_{10}? How many elements are there of each order?

The order of D_{10} is 20. But D_{10} is a dihedral group, so its generated by two elements. In other words, it is made up of two cyclic groups. The first cyclic group which is the rotations of D_{10} is of order 10. So using theorem 5.2.2 and the divisiors of 10, 1,2,5, and 10, I find that $\phi(1) = 1, \phi(2) = 1, \phi(5) = 4,$ and $\phi(10) = 4$. In the other cyclic group, all elements have order 2, and there are 10 of them. Since $\phi(2) = 1$, this means there are 10 elements of order 2 in this group. So, in total in D_{10} there is 1 element of order 1, 11 elements of order 2, 4 elements of order 5, and 4 elements of order 10.