MATH 417, HOMEWORK 9

CHARLES ANCEL

Exercise 1. Describe all the elementary divisor forms for abelian groups of order 360. Then determine the corresponding invariant factor forms. (There are six. Forgot to specify "abelian" in the original statement, but it should be clear from context.)

To describe the elementary divisor forms and the corresponding invariant factor forms for abelian groups of order 360, we begin by factorizing 360 into its prime factors:

$$360 = 2^3 \cdot 3^2 \cdot 5.$$

An abelian group of order 360 can be expressed as a direct product of cyclic groups, whose orders are divisors of 360. The elementary divisors are the orders of these cyclic groups. The invariant factor form is obtained by arranging these cyclic group orders into a non-decreasing sequence.

Elementary Divisor Forms. To find the elementary divisor forms, we consider all possible ways to factorize 360 into products of integers greater than 1:

(1) $360 = 2^3 \cdot 3^2 \cdot 5$:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

(2) $360 = 4 \cdot 90$:

$$\mathbb{Z}_4 \times \mathbb{Z}_{90}$$

(3) $360 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 2$:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_2$$

(4) $360 = 6 \cdot 60$:

$$\mathbb{Z}_6 \times \mathbb{Z}_{60}$$

(5) $360 = 8 \cdot 45$:

$$\mathbb{Z}_8 \times \mathbb{Z}_{45}$$

(6) $360 = 10 \cdot 36$:

$$\mathbb{Z}_{10} \times \mathbb{Z}_{36}$$

Invariant Factor Forms. The invariant factor form is found by expressing each product of cyclic groups as a product of cyclic groups of order dividing the previous one in the sequence. The invariant factor forms corresponding to the above elementary divisor forms are:

(1) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

(2) $\mathbb{Z}_4 \times \mathbb{Z}_{90}$:

$$\mathbb{Z}_4 \times \mathbb{Z}_{90}$$

(3) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_2$:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_2$$

(4) $\mathbb{Z}_6 \times \mathbb{Z}_{60}$:

$$\mathbb{Z}_6 \times \mathbb{Z}_{60}$$

(5) $\mathbb{Z}_8 \times \mathbb{Z}_{45}$:

$$\mathbb{Z}_8 \times \mathbb{Z}_{45}$$

(6) $\mathbb{Z}_{10} \times \mathbb{Z}_{36}$:

$$\mathbb{Z}_{10} \times \mathbb{Z}_{36}$$

Hence, the six elementary divisor forms and their corresponding invariant factor forms for abelian groups of order 360 are listed above.

Exercise 3.6.7. Find the elementary divisor and invariant factor decomposition of $\mathbb{Z}_{108} \times \mathbb{Z}_{144} \times \mathbb{Z}_9$

Solution

To find the elementary divisor and invariant factor decomposition of $\mathbb{Z}_{108} \times \mathbb{Z}_{144} \times \mathbb{Z}_9$, we first factorize each number into its prime power components.

$$\begin{aligned} 108 &= 2^2 \cdot 3^3, \\ 144 &= 2^4 \cdot 3^2, \\ 9 &= 3^2. \end{aligned}$$

The group $\mathbb{Z}_{108} \times \mathbb{Z}_{144} \times \mathbb{Z}_9$ can be expressed as:

$$\mathbb{Z}_{108} \times \mathbb{Z}_{144} \times \mathbb{Z}_9 \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^3} \times \mathbb{Z}_{2^4} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{3^2}.$$

Elementary Divisor Decomposition. The elementary divisors are the prime power components of the orders of the cyclic groups in the direct product. We combine all terms for each prime factor:

$$2^2,\ 2^4,\ 3^3,\ 3^2,\ 3^2.$$

Sorting these elementary divisors in non-decreasing order, we get:

$$2^2,\ 2^4,\ 3^2,\ 3^2,\ 3^3.$$

Therefore, the elementary divisor decomposition of $\mathbb{Z}_{108} \times \mathbb{Z}_{144} \times \mathbb{Z}_9$ is:

$$\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^4} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{3^3}.$$

Invariant Factor Decomposition. The invariant factors are obtained by grouping the elementary divisors into products, each factor dividing the next:

- Grouping the 2's:
$$2^2 \cdot 2^4 = 2^6.$$
- Grouping the 3's:
$$3^2 \cdot 3^2 \cdot 3^3 = 3^7.$$

Therefore, the invariant factor decomposition is:

$$\mathbb{Z}_{2^6} \times \mathbb{Z}_{3^7}.$$

Hence, the elementary divisor decomposition of $\mathbb{Z}_{108} \times \mathbb{Z}_{144} \times \mathbb{Z}_9$ is:

$$\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^4} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{3^3},$$

and the corresponding invariant factor decomposition is:

$$\mathbb{Z}_{2^6} \times \mathbb{Z}_{3^7}.$$

Exercise 3.6.10. Let p be a prime number. How many abelian groups are there of order p^7, up to isomorphism?

To determine the number of abelian groups of order p^7 up to isomorphism, we use the classification theorem for finitely generated abelian groups. This theorem states that every finitely generated abelian group can be expressed as a direct sum of cyclic groups whose orders are powers of the prime p.

For a group of order p^7, we need to find all possible partitions of 7 (since the exponent in each term of the cyclic groups must sum to 7). Each partition corresponds to a unique isomorphism class of abelian groups. The partitions of 7 are:

(1) 7

(2) $6+1$

(3) $5+2$

(4) $5+1+1$

(5) $4+3$

(6) $4+2+1$

(7) $4+1+1+1$

(8) $3+3+1$

(9) $3+2+2$

(10) $3+2+1+1$

(11) $3+1+1+1+1$

(12) $2+2+2+1$

(13) $2+2+1+1+1$

(14) $2+1+1+1+1+1$

(15) $1+1+1+1+1+1+1$

These partitions correspond to the following abelian groups (written as products of cyclic groups):

(1) $\mathbb{Z}_{p^7}$

(2) $\mathbb{Z}_{p^6} \times \mathbb{Z}_p$

(3) $\mathbb{Z}_{p^5} \times \mathbb{Z}_{p^2}$

(4) $\mathbb{Z}_{p^5} \times \mathbb{Z}_p \times \mathbb{Z}_p$

(5) $\mathbb{Z}_{p^4} \times \mathbb{Z}_{p^3}$

(6) $\mathbb{Z}_{p^4} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_p$

(7) $\mathbb{Z}_{p^4} \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$

(8) $\mathbb{Z}_{p^3} \times \mathbb{Z}_{p^3} \times \mathbb{Z}_p$

(9) $\mathbb{Z}_{p^3} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$

(10) $\mathbb{Z}_{p^3} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p$

(11) $\mathbb{Z}_{p^3} \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$

(12) $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_p$

(13) $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$

(14) $\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$

(15) $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$

There are 15 distinct partitions of 7, and thus, there are 15 abelian groups of order p^7, up to isomorphism.

Exercise 3.6.15. Show that $\mathbb{Z}_a \times \mathbb{Z}_b$ is not cyclic if $\gcd(a, b) \geq 2$.

To show that $\mathbb{Z}_a \times \mathbb{Z}_b$ is not cyclic if $\gcd(a, b) \geq 2$, we need to show that there does not exist an element in $\mathbb{Z}_a \times \mathbb{Z}_b$ that generates the entire group.

Definition of Cyclic Group. A group G is cyclic if there exists an element $g \in G$ such that every element of G can be written as g^k for some integer k. In other words, $G = \langle g \rangle$.

Structure of $\mathbb{Z}_a \times \mathbb{Z}_b$. Consider the group $\mathbb{Z}_a \times \mathbb{Z}_b$. The order of this group is ab, which means it has ab elements. Each element of $\mathbb{Z}_a \times \mathbb{Z}_b$ can be written as (x, y) where $x \in \mathbb{Z}_a$ and $y \in \mathbb{Z}_b$. The orders of the elements are determined by the smallest positive integer k such that:

$$(x, y)^k = (0, 0) \pmod{(a, b)}.$$

Element Order in $\mathbb{Z}_a \times \mathbb{Z}_b$. Let (x, y) be an element of $\mathbb{Z}_a \times \mathbb{Z}_b$. The order of (x, y) is the least common multiple (LCM) of the orders of x in $\mathbb{Z}_a$ and y in $\mathbb{Z}_b$. The order of x in $\mathbb{Z}_a$ is $\frac{a}{\gcd(a,x)}$, and the order of y in $\mathbb{Z}_b$ is $\frac{b}{\gcd(b,y)}$.

Thus, the order of (x, y) in $\mathbb{Z}_a \times \mathbb{Z}_b$ is:

$$\operatorname{lcm}\left(\frac{a}{\gcd(a, x)}, \frac{b}{\gcd(b, y)}\right).$$

Non-cyclic Property for $\gcd(a, b) \geq 2$. Assume $\gcd(a, b) = d \geq 2$. We want to show that $\mathbb{Z}_a \times \mathbb{Z}_b$ is not cyclic.

Suppose for contradiction that $\mathbb{Z}_a \times \mathbb{Z}_b$ is cyclic. Then, there exists an element $(x, y) \in \mathbb{Z}_a \times \mathbb{Z}_b$ that generates the entire group. The order of (x, y) must be ab because the order of $\mathbb{Z}_a \times \mathbb{Z}_b$ is ab.

For (x, y) to have order ab, we must have:

$$\operatorname{lcm}\left(\frac{a}{\gcd(a, x)}, \frac{b}{\gcd(b, y)}\right) = ab.$$

Given that $\gcd(a, b) = d$, we can write $a = da_1$ and $b = db_1$ where $\gcd(a_1, b_1) = 1$. The order of (x, y) in $\mathbb{Z}_a \times \mathbb{Z}_b$ is:

$$\operatorname{lcm}\left(\frac{da_1}{\gcd(da_1, x)}, \frac{db_1}{\gcd(db_1, y)}\right).$$

Since (x, y) must generate $\mathbb{Z}_a \times \mathbb{Z}_b$, (x, y) must have order $ab = d^2 a_1 b_1$. This implies that:

$$\frac{da_1}{\gcd(da_1, x)} \text{ and } \frac{db_1}{\gcd(db_1, y)}$$

must have LCM equal to $d^2 a_1 b_1$. However, because $d \geq 2$, $\frac{da_1}{\gcd(da_1,x)} \leq da_1$ and $\frac{db_1}{\gcd(db_1,y)} \leq db_1$. The LCM of two such terms cannot be $d^2 a_1 b_1$ unless $\gcd(a, b) = 1$, contradicting $\gcd(a, b) = d \geq 2$.

Therefore, $\mathbb{Z}_a \times \mathbb{Z}_b$ cannot be cyclic if $\gcd(a, b) \geq 2$.

Exercise 3.6.17. Suppose a finite abelian group has invariant factors $d_1, d_2, \ldots, d_k$, so that $d_i | d_{i+1}$. Show that G has an element of order s if and only if s divides d_k(= the largest of the invariant factors).

Solution

Let G be a finite abelian group with invariant factors $d_1, d_2, \ldots, d_k$ such that $d_i \mid d_{i+1}$ for all i. The group G can be expressed as:

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k}.$$

The order of an element $(x_1, x_2, \ldots, x_k) \in G$ is the least common multiple of the orders of the components $x_i \in \mathbb{Z}_{d_i}$.

Necessary Condition: If G Has an Element of Order s, Then s Divides d_k. Suppose G has an element of order s. Let $(x_1, x_2, \ldots, x_k) \in G$ be such an element. Then the order of $(x_1, x_2, \ldots, x_k)$ is:

$$\operatorname{lcm}(\operatorname{ord}(x_1), \operatorname{ord}(x_2), \ldots, \operatorname{ord}(x_k)) = s.$$

Since $\operatorname{ord}(x_i)$ divides d_i for each i, and $d_i \mid d_k$, it follows that $\operatorname{ord}(x_i) \mid d_k$. Therefore, $s = \operatorname{lcm}(\operatorname{ord}(x_1), \operatorname{ord}(x_2), \ldots, \operatorname{ord}(x_k)) \mid d_k$.

Sufficient Condition: If s Divides d_k, Then G Has an Element of Order s. Suppose $s \mid d_k$. We need to construct an element in G with order s.

Since d_k is the largest invariant factor and $s \mid d_k$, we can find an element $y \in \mathbb{Z}_{d_k}$ with $\operatorname{ord}(y) = s$. Let $y = \frac{d_k}{s}$. Then:

$$y \times s = \left(\frac{d_k}{s}\right) \times s = d_k,$$

which implies $\operatorname{ord}(y) = s$.

Construct the element $(0, 0, \ldots, y) \in G$. The order of $(0, 0, \ldots, y)$ is:

$$\operatorname{lcm}(\operatorname{ord}(0), \operatorname{ord}(0), \ldots, \operatorname{ord}(y)) = \operatorname{lcm}(1, 1, \ldots, s) = s.$$

Therefore, if s divides d_k, then G has an element of order s.

Conclusion. A finite abelian group G with invariant factors $d_1, d_2, \ldots, d_k$ has an element of order s if and only if s divides the largest invariant factor d_k.

Exercise 6. Let $G = (\mathbb{Q}, +)$, the group of rational numbers with addition. SHow that any finite subset $S \subset G$ is contained in a cyclic subgroup, and conclude from this that G is not finitely generated. (Hint: clear denominators.)

Solution

Let $S = \{q_1, q_2, \ldots, q_n\}$ be a finite subset of $G = (\mathbb{Q}, +)$, where each $q_i \in \mathbb{Q}$.

Clearing Denominators. Each rational number q_i can be written as $\frac{a_i}{b_i}$, where $a_i \in \mathbb{Z}$ and $b_i \in \mathbb{N}$. Let $b = \operatorname{lcm}(b_1, b_2, \ldots, b_n)$ be the least common multiple of the denominators. Then each q_i can be expressed with a common denominator b as:

$$q_i = \frac{a_i}{b} \quad \text{for some } a_i \in \mathbb{Z}.$$

Generating a Cyclic Subgroup. Consider the rational number $\frac{1}{b}$. The cyclic subgroup generated by $\frac{1}{b}$ is:

$$\left\langle \frac{1}{b} \right\rangle = \left\{ k \cdot \frac{1}{b} \mid k \in \mathbb{Z} \right\}.$$

Since each $q_i = \frac{a_i}{b}$, we have:

$$q_i = a_i \cdot \frac{1}{b} \quad \text{for each } q_i \in S.$$

Therefore, each $q_i \in \left\langle \frac{1}{b} \right\rangle$, and hence the finite subset S is contained in the cyclic subgroup generated by $\frac{1}{b}$.

Conclusion: G is Not Finitely Generated. Suppose for contradiction that $G = (\mathbb{Q}, +)$ is finitely generated. Then there exists a finite set of generators $\{g_1, g_2, \ldots, g_m\} \subseteq \mathbb{Q}$ such that every rational number can be expressed as a finite linear combination of these generators with integer coefficients.

Let $S = \{g_1, g_2, \ldots, g_m\}$. By the previous argument, S is contained in a cyclic subgroup $\left\langle \frac{1}{b} \right\rangle$ for some $b \in \mathbb{N}$. Hence, every element of $\mathbb{Q}$ would be a multiple of $\frac{1}{b}$, which implies that $\mathbb{Q}$ is cyclic. However, this is a contradiction because $\mathbb{Q}$ is not cyclic; there is no single rational number whose integer multiples cover all of $\mathbb{Q}$.

Therefore, $G = (\mathbb{Q}, +)$ is not finitely generated.

Exercise 7. Let $G = \Phi(35)$. Determine the elementary divisor and invariant factor decompositions of this group of order 24.

Solution

First, recall that $\Phi(35)$ is the group of units modulo 35. The order of $\Phi(35)$ is given by Euler's totient function:

$$\phi(35) = \phi(5 \times 7) = \phi(5) \cdot \phi(7) = 4 \cdot 6 = 24.$$

Therefore, $\Phi(35)$ is a group of order 24.

Finding the Structure of $\Phi(35)$. The group $\Phi(35)$ is isomorphic to the direct product of $\Phi(5)$ and $\Phi(7)$:

$$\Phi(35) \simeq \Phi(5) \times \Phi(7).$$

Since $\phi(5) = 4$ and $\phi(7) = 6$, we have:

$$\Phi(5) \simeq \mathbb{Z}_4 \quad \text{and} \quad \Phi(7) \simeq \mathbb{Z}_6.$$

Therefore:

$$\Phi(35) \simeq \mathbb{Z}_4 \times \mathbb{Z}_6.$$

Elementary Divisors. To find the elementary divisor decomposition, we need to express $\mathbb{Z}_4 \times \mathbb{Z}_6$ in terms of its elementary divisors. We start by finding the orders of the elements:

$$\mathbb{Z}_4 \simeq \{0, 1, 2, 3\} \quad \text{with orders} \quad 1, 4, 2, 4.$$

$$\mathbb{Z}_6 \simeq \{0, 1, 2, 3, 4, 5\} \quad \text{with orders} \quad 1, 6, 3, 2, 3, 6.$$

For the product group $\mathbb{Z}_4 \times \mathbb{Z}_6$, the order of an element (a, b) is $\text{lcm}(\text{ord}(a), \text{ord}(b))$.

The elementary divisors can be found by listing the orders of all elements and taking the corresponding least common multiples:

$(0,0), (0,3), (0,6), (2,0), (2,3), (2,6)$	order 1, 2, 3, 2, 6, 6 respectively
$(1,0), (3,0)$	order 4
$(1,3), (3,3)$	order 12
$(1,2), (3,2)$	order 6
$(1,4), (3,4)$	order 12
$(1,1), (3,1), (1,5), (3,5)$	order 12

From these, the elementary divisors are:

$$1, 2, 2, 3, 3, 4, 6, 6, 12, 12.$$

Invariant Factors. The invariant factors are obtained by dividing the group order by the greatest common divisor of the group order and the orders of the preceding invariant factors:

The first invariant factor d_1 is the smallest prime dividing 24, which is 2.

The second invariant factor d_2 is the smallest factor of the remaining group order after dividing by d_1, giving us $d_2 = \frac{24}{2} = 12$.

Therefore, the invariant factor decomposition is:

$$\Phi(35) \simeq \mathbb{Z}_2 \times \mathbb{Z}_{12}.$$

Combining the orders of the individual groups:

$$\Phi(35) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3.$$

Conclusion. The elementary divisors of $\Phi(35)$ are:

$$1, 2, 2, 3, 3, 4, 6, 6, 12, 12.$$

The invariant factor decomposition of $\Phi(35)$ is:

$$\mathbb{Z}_2 \times \mathbb{Z}_{12}.$$

Exercise 8. Find the structure (elementary divisor and invariant factor) of the group $\Phi(n)$ for all $n \leq 20$.

Solution

To find the structure of $\Phi(n)$ for all $n \leq 20$, we first compute the group $\Phi(n)$, which is the group of units modulo n, and then determine the elementary divisor and invariant factor decompositions.

Structure of $\Phi(n)$ for $n = 1$ to 20.

- $n = 1$: $\Phi(1)$ is trivial.
$$\Phi(1) = \{1\}$$
Invariant factors: $\{1\}$.
- $n = 2$: $\Phi(2) \simeq \{1\}$.
$$\Phi(2) = \{1\}$$
Invariant factors: $\{1\}$.
- $n = 3$: $\Phi(3) \simeq \mathbb{Z}_2$.
$$\Phi(3) = \{1, 2\}$$
Invariant factors: $\{2\}$.
- $n = 4$: $\Phi(4) \simeq \mathbb{Z}_2$.
$$\Phi(4) = \{1, 3\}$$
Invariant factors: $\{2\}$.
- $n = 5$: $\Phi(5) \simeq \mathbb{Z}_4$.
$$\Phi(5) = \{1, 2, 3, 4\}$$
Invariant factors: $\{4\}$.
- $n = 6$: $\Phi(6) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.
$$\Phi(6) = \{1, 5\}$$
Invariant factors: $\{2, 2\}$.
- $n = 7$: $\Phi(7) \simeq \mathbb{Z}_6$.
$$\Phi(7) = \{1, 2, 3, 4, 5, 6\}$$
Invariant factors: $\{6\}$.
- $n = 8$: $\Phi(8) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.
$$\Phi(8) = \{1, 3, 5, 7\}$$
Invariant factors: $\{2, 2\}$.
- $n = 9$: $\Phi(9) \simeq \mathbb{Z}_6$.
$$\Phi(9) = \{1, 2, 4, 5, 7, 8\}$$
Invariant factors: $\{6\}$.

- $n = 10$: $\Phi(10) \simeq \mathbb{Z}_4$.
$$\Phi(10) = \{1, 3, 7, 9\}$$
Invariant factors: $\{4\}$.
- $n = 11$: $\Phi(11) \simeq \mathbb{Z}_{10}$.
$$\Phi(11) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$
Invariant factors: $\{10\}$.
- $n = 12$: $\Phi(12) \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$.
$$\Phi(12) = \{1, 5, 7, 11\}$$
Invariant factors: $\{2, 4\}$.
- $n = 13$: $\Phi(13) \simeq \mathbb{Z}_{12}$.
$$\Phi(13) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$
Invariant factors: $\{12\}$.
- $n = 14$: $\Phi(14) \simeq \mathbb{Z}_6$.
$$\Phi(14) = \{1, 3, 5, 9, 11, 13\}$$
Invariant factors: $\{6\}$.
- $n = 15$: $\Phi(15) \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$.
$$\Phi(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$$
Invariant factors: $\{4, 2\}$.
- $n = 16$: $\Phi(16) \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$.
$$\Phi(16) = \{1, 3, 5, 7, 9, 11, 13, 15\}$$
Invariant factors: $\{4, 2\}$.
- $n = 17$: $\Phi(17) \simeq \mathbb{Z}_{16}$.
$$\Phi(17) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$$
Invariant factors: $\{16\}$.
- $n = 18$: $\Phi(18) \simeq \mathbb{Z}_6 \times \mathbb{Z}_2$.
$$\Phi(18) = \{1, 5, 7, 11, 13, 17\}$$
Invariant factors: $\{6, 2\}$.
- $n = 19$: $\Phi(19) \simeq \mathbb{Z}_{18}$.
$$\Phi(19) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18\}$$
Invariant factors: $\{18\}$.
- $n = 20$: $\Phi(20) \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$.
$$\Phi(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$$
Invariant factors: $\{4, 2\}$.

Summary.

n	$\Phi(n)$	Elementary Divisors	Invariant Factors
1	$\{1\}$	$\{1\}$	$\{1\}$
2	$\mathbb{Z}_1$	$\{1\}$	$\{1\}$
3	$\mathbb{Z}_2$	$\{2\}$	$\{2\}$
4	$\mathbb{Z}_2$	$\{2\}$	$\{2\}$
5	$\mathbb{Z}_4$	$\{4\}$	$\{4\}$
6	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\{2,2\}$	$\{2,2\}$
7	$\mathbb{Z}_6$	$\{6\}$	$\{6\}$
8	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\{2,2\}$	$\{2,2\}$
9	$\mathbb{Z}_6$	$\{6\}$	$\{6\}$
10	$\mathbb{Z}_4$	$\{4\}$	$\{4\}$
11	$\mathbb{Z}_{10}$	$\{10\}$	$\{10\}$
12	$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\{2,4\}$	$\{2,4\}$
13	$\mathbb{Z}_{12}$	$\{12\}$	$\{12\}$
14	$\mathbb{Z}_6$	$\{6\}$	$\{6\}$
15	$\mathbb{Z}_4 \times \mathbb{Z}_2$	$\{4,2\}$	$\{4,2\}$
16	$\mathbb{Z}_4 \times \mathbb{Z}_2$	$\{4,2\}$	$\{4,2\}$
17	$\mathbb{Z}_{16}$	$\{16\}$	$\{16\}$
18	$\mathbb{Z}_6 \times \mathbb{Z}_2$	$\{6,2\}$	$\{6,2\}$
19	$\mathbb{Z}_{18}$	$\{18\}$	$\{18\}$
20	$\mathbb{Z}_4 \times \mathbb{Z}_2$	$\{4,2\}$	$\{4,2\}$

Exercise 9. Given a commutative ring A with identity, let $C(A)$ be the group defined in PS 5, with underlying set $C(A) = \{(x, y) \in A^2 \mid x^2 + y^2 = 1\}$. Determine the elementary divisor and invariant factor decompositions of the following groups: $C(\mathbb{Z}_2), C(\mathbb{Z}_4), C(\mathbb{Z}_8), C(\mathbb{Z}_3), C(\mathbb{Z}_5), C(\mathbb{Z}_7), C(\mathbb{Z}$ (Hint: these are groups of orders 2, 8, 16, 4, 4, 8, 12, 12 respectively. To figure out what the elements of $C(\mathbb{Z}_n)$ are, first determine which elements of Z_n can be squares of elements of Z_n.)

Revised: I had the orders wrong for $C(\mathbb{Z}_4)$, $C(\mathbb{Z}_8)$, $C(\mathbb{Z}_{16})$. I fixed the first two, and removed the third one entirely. Make a conjecture about the structure of $C(\mathbb{Z}_p)$ when p is an arbitrary odd prime.

Solution

Order of the Elements in $C(A)$.

1. $C(\mathbb{Z}_2)$. The set of elements is $(x, y) \in \mathbb{Z}_2^2$ such that $x^2 + y^2 = 1$:

$$C(\mathbb{Z}_2) = \{(1, 0), (0, 1)\}.$$

This group has order 2, and it is isomorphic to $\mathbb{Z}_2$.

2. $C(\mathbb{Z}_4)$. The set of elements is $(x, y) \in \mathbb{Z}_4^2$ such that $x^2 + y^2 = 1$:

$$C(\mathbb{Z}_4) = \{(1, 0), (3, 0), (0, 1), (0, 3), (2, 2)\}.$$

This group has order 4, and it is isomorphic to $\mathbb{Z}_4$.

3. $C(\mathbb{Z}_8)$. The set of elements is $(x, y) \in \mathbb{Z}_8^2$ such that $x^2 + y^2 = 1$:

$$C(\mathbb{Z}_8) = \{(1, 0), (7, 0), (0, 1), (0, 7), (3, 3), (5, 5)\}.$$

This group has order 8, and it is isomorphic to $\mathbb{Z}_8$.

4. $C(\mathbb{Z}_3)$. The set of elements is $(x, y) \in \mathbb{Z}_3^2$ such that $x^2 + y^2 = 1$:

$$C(\mathbb{Z}_3) = \{(1, 0), (2, 0), (0, 1), (0, 2)\}.$$

This group has order 4, and it is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

5. $C(\mathbb{Z}_5)$. The set of elements is $(x, y) \in \mathbb{Z}_5^2$ such that $x^2 + y^2 = 1$:

$$C(\mathbb{Z}_5) = \{(1, 0), (4, 0), (0, 1), (0, 4), (2, 3), (3, 2)\}.$$

This group has order 6, and it is isomorphic to $\mathbb{Z}_6$.

6. $C(\mathbb{Z}_7)$. The set of elements is $(x, y) \in \mathbb{Z}_7^2$ such that $x^2 + y^2 = 1$:

$$C(\mathbb{Z}_7) = \{(1, 0), (6, 0), (0, 1), (0, 6), (3, 4), (4, 3), (2, 5), (5, 2)\}.$$

This group has order 8, and it is isomorphic to $\mathbb{Z}_8$.

7. $C(\mathbb{Z}_{11})$. The set of elements is $(x, y) \in \mathbb{Z}_{11}^2$ such that $x^2 + y^2 = 1$:

$$C(\mathbb{Z}_{11}) = \{(1, 0), (10, 0), (0, 1), (0, 10), (3, 4), (4, 3), (5, 9), (9, 5), (2, 6), (6, 2)\}.$$

This group has order 10, and it is isomorphic to $\mathbb{Z}_{10}$.

8. $C(\mathbb{Z}_{13})$. The set of elements is $(x, y) \in \mathbb{Z}_{13}^2$ such that $x^2 + y^2 = 1$:

$$C(\mathbb{Z}_{13}) = \{(1,0), (12,0), (0,1), (0,12), (5,6), (6,5), (4,9), (9,4), (3,10), (10,3)\}.$$

This group has order 12, and it is isomorphic to $\mathbb{Z}_{12}$.

Conjecture for $C(\mathbb{Z}_p)$ When p is an Odd Prime. Based on the patterns observed, we can conjecture that for an odd prime p, the group $C(\mathbb{Z}_p)$ is isomorphic to $\mathbb{Z}_{p-1}$. This is because the elements $(x, y) \in \mathbb{Z}_p^2$ that satisfy $x^2 + y^2 = 1$ form a cyclic group of order $p - 1$.