CHAPTER 4

Cyclic Groups

Properties of Cyclic Groups

DEFINITION (Cyclic Group). A group G is called cyclic if $\exists\ a \in G \ni$

$$G = \langle a \rangle = \{a^n | n \in \mathbb{Z}\}.$$

We say a is a generator of G. (A cyclic group may have many generators.) Although the list $\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots$ has infinitely many entries, the set $\{a^n | n \in \mathbb{Z}\}$ may have only finitely many elements. Also, since

$$a^i a^j = a^{i+j} = a^{j+i} = a^j a^i,$$

every cyclic group is Abelian.

EXAMPLE. $\mathbb{Z}$ under addition is an infinite cyclic group.

$$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle \text{ (1 and } -1 \text{ are the only generators).}$$

$$0 = 0 \cdot 1 = 0 \cdot (-1) \text{ (interpretation of } 1^0 \text{ and } (-1)^0\text{).}$$

$$\text{For } n > 0, n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ terms}} \text{ (interpretation of } 1^n\text{).}$$

$$\text{For } n < 0, n = \underbrace{(-1) + (-1) + \cdots + (-1)}_{|n| \text{ terms}} \text{ (interpretation of } (-1)^n\text{).}$$

EXAMPLE. $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ with addition modulo n is a finite cyclic group.

$$\mathbb{Z}_n = \langle 1 \rangle = \langle n - 1 \rangle \quad (\text{Note } n - 1 = -1 \bmod n).$$

Other generators are possible depending on n:

$$\mathbb{Z}_{10} = \langle 1 \rangle = \langle 9 \rangle = \langle 3 \rangle = \langle 7 \rangle.$$

EXAMPLE. For $U(12) = \{1, 5, 7, 11\}$,

$$\langle 1\rangle = \{1\}, \quad \langle 5\rangle = \{1, 5\}, \quad \langle 7\rangle = \{1, 7\}, \quad \langle 11\rangle = \{1, 11\}.$$

Thus $U(12)$ is not cyclic since none of its elements generate the group.

THEOREM (4.1 — Criterion for $a^i = a^j$). *Let G be a group and $a \in G$. If $|a| = \infty$, then all distinct powers of a are distinct group elements ($a^i = a^j \iff i = j$). If $|a| < \infty$, say $|a| = n$, $\langle a\rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j \iff n|i - j$.*

PROOF.

(1) If $|a| = \infty$, $\nexists\ n \in \mathbb{Z}^+ \ni a^n = e$. Then

$$a^i = a^j \iff a^{i-j} = e \iff i - j = 0 \iff i = j.$$

(2) Assume $|a| < \infty$. [To show $\langle a\rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.]

Clearly, $e, a, a^2, \ldots, a^{n-1}$ are distinct since $|a| = n$. For if $a^i = a^j$ with $0 \le j < i \le n - 1$, then $a^{i-j} = e$, contradicting that

n is the least positive integer such that $a^n = e$.

Now suppose $a^k \in \langle a\rangle$. Then

$\exists\ q, r \in \mathbb{Z} \ni k = qn + r, 0 \le r < n$. Then

$$a^k = a^{qn+r} = (a^n)^q a^r = e^q a^r = a^r,$$

so $a^k \in \{e, a, a^2, \ldots, a^{n-1}\} \Longrightarrow \langle a\rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.

(3) ($\Longrightarrow$) Suppose $a^i = a^j$. [To show $n|i - j$.] Then $a^{i-j} = e$. Now

$\exists\ q, r \in \mathbb{Z} \ni i - j = qn + r, 0 \le r < n$, and so

$$e = a^{i-j} = a^{qn+r} = (a^n)^q a^r = e^q a^r = a^r$$

Since n is the least positive integer such that $a^n = e$, $r = 0$, so $n|i - j$.

($\Longleftarrow$) If $n|i - j$, then $\exists\ q \in \mathbb{Z} \ni i - j = nq \Longrightarrow$

$$a^{i-j} = a^{nq} = (a^n)^q = e^q = e \Longrightarrow a^i = a^j.$$

□

COROLLARY (1 — $|a| = |\langle a \rangle|$).

For any group element a, $|a| = |\langle a \rangle|$.

COROLLARY (2 — $a^k = e \Longrightarrow |a||k$).

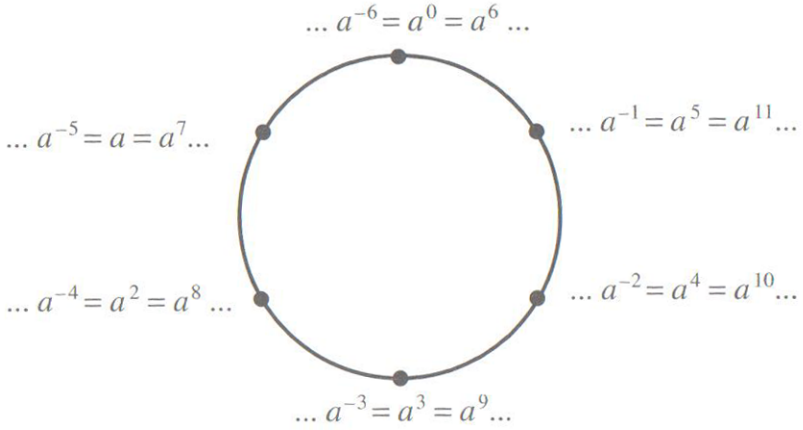
Let G be a group and let a be an element of order n in G. If $a^k = e$, then n divides k.

PROOF.

Since $a^k = e = a^0$, by Theorem 4.1, $n|k - 0 \Longrightarrow n|k$. □

NOTE.

Referring to Figure 4.1 on page 80 (shown below),



Theorem 4.1 says that multiplication in $\langle a \rangle$ is essentially done by addition modulo n, i.e., if $(i + j)$ mod $n = k$, then $a^i a^j = a^k$. This is for any G and any a. Multiplication in $\langle a \rangle$ works like addition in $\mathbb{Z}_n$.

Similarly, if $|a| = \infty$, multiplication in $\langle a \rangle$ works like addition in $\mathbb{Z}$ since $a^i a^j = a^{i+j}$.

Thus $\mathbb{Z}_n$ and $\mathbb{Z}$ are the prototypical cyclic groups.

How can one compute $|a^k|$ from $|a|$ only? Also, how can one tell when $\langle a^i \rangle = \langle a^j \rangle$?

THEOREM (4.2 — $\langle a^k\rangle = \langle a^{\gcd(n,k)}\rangle$ and $|a^k| = n/\gcd(n,k)$).

Let G be a group, $a \in G$, $|a| = n$, and $k \in \mathbb{N}$. Then

$$\langle a^k\rangle = \langle a^{\gcd(n,k)}\rangle \text{ and } |a^k| = \frac{n}{\gcd(n,k)}.$$

PROOF.

(1) To simplify notation, let $d = \gcd(n,k)$ and $k = dr$. Since $a^k = (a^d)^r$, $\langle a^k\rangle \subseteq \langle a^d\rangle$.

Now $\exists\ s,t \in \mathbb{Z} \ni d = ns + kt$. Then

$$a^d = a^{ns+kt} = a^{ns}a^{kt} = (a^n)^s(a^k)^t = e(a^k)^t = (a^k)^t \in \langle a^k\rangle.$$

Thus $\langle a^d\rangle \subseteq \langle a^k\rangle \Longrightarrow \langle a^d\rangle = \langle a^k\rangle$ by mutual set inclusion.

(2) Since $d|n$, $(a^d)^{n/d} = a^n = e$, so $|a^d| \leq \frac{n}{d}$. But if $i \in \mathbb{N}$ with $i < \frac{n}{d}$, then $(a^d)^i \neq e$ by the definition of $|a|$, so $|a^d| = \frac{n}{d}$.Then

$$|a^k| = |\langle a^k\rangle| = |\langle a^d\rangle| = |a^d| = \frac{n}{d} = \frac{n}{\gcd(n,k)}.$$

□

COROLLARY (1 — Orders of Elements in Finite Cyclic Groups).

In a finite cyclic group, the order of an element divides the order of the group.

COROLLARY (2 — Criterion for $\langle a^i \rangle = \langle a^j \rangle$ and $|a^i| = |a^j|$.).

Let $|a| = n$. *Then* $\langle a^i \rangle = \langle a^j \rangle \iff \gcd(n,i) = \gcd(n,j)$, *and* $|a^i| = |a^j| \iff \gcd(n,i) = \gcd(n,j)$.

PROOF.

(1) By Theorem 4.2, $\langle a^i \rangle = \langle a^{\gcd(n,i)} \rangle$ and $\langle a^j \rangle = \langle a^{\gcd(n,j)} \rangle$.

Then $\langle a^i \rangle = \langle a^j \rangle \iff \langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle$.

($\Longleftarrow$) $\gcd(n,i) = \gcd(n,j) \Longrightarrow \langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle \Longrightarrow \langle a^i \rangle = \langle a^j \rangle$.

($\Longrightarrow$) $\langle a^i \rangle = \langle a^j \rangle \Longrightarrow \langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle \Longrightarrow |a^{\gcd(n,i)}| = |a^{\gcd(n,j)}| \Longrightarrow \dfrac{n}{\gcd(n,i)} = \dfrac{n}{\gcd(n,j)} \Longrightarrow \gcd(n,i) = \gcd(n,j)$.

(2) Follows from the first part and Corollary 1 of Theorem 4.1. □

COROLLARY (3 — Generators of Finite Cyclic Groups.).

Let $|a| = n$. *Then* $\langle a \rangle = \langle a^j \rangle \iff \gcd(n,j) = 1$, *and* $|a| = |\langle a^j \rangle| \iff gcd(n,j) = 1$.

NOTE. Now, once one generator of a cyclic group is found, all generators can then be easily determined.

EXAMPLE.

$U(25) = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$,

so $|U(25)| = 20$.

Now $U(25) = \langle 2 \rangle$. By Corollary 3, the following are generators:

$2^1 \bmod 25 = 2$	$2^{13} \bmod 25 = 17$
$2^3 \bmod 25 = 8$	$2^{17} \bmod 25 = 22$
$2^7 \bmod 25 = 3$	$2^{19} \bmod 25 = 13$
$2^9 \bmod 25 = 12$	$2^{21} \bmod 25 = 2$
$2^{11} \bmod 25 = 23$	$2^{23} \bmod 25 = 8$

Thus $U(25) = \langle 2 \rangle = \langle 3 \rangle = \langle 8 \rangle = \langle 12 \rangle = \langle 13 \rangle = \langle 17 \rangle = \langle 22 \rangle = \langle 23 \rangle$.

COROLLARY (4 — Generators of $\mathbb{Z}_n$).

An integer $k \in \mathbb{Z}_n$ is a generator of $\mathbb{Z}_n \iff \gcd(n,k) = 1$.

PROBLEM (Page 87 # 10). (1) In $\mathbb{Z}_{24}$, list all generators for the subgroup of order 8. (2) Let $G = \langle a \rangle$ and let $|a| = 24$. List all generators of the subgroup of order 8.

SOLUTION.

(1) $\langle 3 \rangle = \{0, 3, 6, 9, 12, 15, 18, 21\}$ has order 8.

From Corollary 3, the generators are $1 \cdot 3, 3 \cdot 3, 5 \cdot 3, 7 \cdot 3$ or $3, 9, 15, 21$.

(2) $\langle a^3 \rangle = \{e, a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}\}$ has order 8.

From Corollary 3, the generators are $(a^3)^1, (a^3)^3, (a^3)^5, (a^3)^7$ or a^3, a^9, a^{15}, a^{21}. □

Classification of Subgroups of Cyclic Groups

THEOREM (4.3 — Fundamental Theorem of Cyclic Groups).

Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k—namely $\langle a^{n/k} \rangle$.

EXAMPLE. Suppose $G = \langle a \rangle$ and $|G| = 42$. By the Theorem 4.3, if $H \leq G$, $H = \langle a^{42/k} \rangle$ where $k|42$. Also, G has one subgroup of the orders $1, 2, 3, 6, 7, 14, 21, 42$, and no others. The proof of the theorem shows how to find these subgroups.

PROOF.

(1) Let $G = \langle a \rangle$ and suppose $H \leq G$. [To show H is cyclic.] If $H = \{e\}$, H is cyclic. Assume $H \neq \{e\}$. Since $G = \langle a \rangle$, every element of H has the form a^t. If $t < 0$, $a^{-t} \in H$ and $-t$ is positive. Thus H contains an element a^t with $t > 0$. Let m be the least positive integer such that $a^m \in H$ (guaranteed by the Well-Ordering Principle). By closure, $\langle a^m \rangle \subseteq H$.

[To show $\langle a^m \rangle = H$.] Suppose $b \in H$. Then $b \in G \Longrightarrow \exists\ k \in G \ni b = a^k$. Then $\exists\ q, r \in \mathbb{Z} \ni k = mq + r, 0 \leq r < m$.

[To show $r = 0$.] Then $a^k = a^{mq+r} = a^{mq}a^r \Longrightarrow a^r = a^k a^{-mq}$. Since $a^k = b \in H$ and $a^{-mq} = (a^m)^{-q} \in H$, $a^r \in H$. But m is the least positive integer $\ni a^m \in H$, and $0 \leq r < m$, so $r = 0$. Thus

$$b = a^k = a^{mq} = (a^m)^q \in \langle a^m \rangle,$$

so $H \leq \langle a^m \rangle$. By mutual inclusion, $\langle a^m \rangle = H$, and so H is cyclic.

(2) Suppose $|\langle a \rangle| = n$ and $H \leq G$. Then, from (1), $H = \langle a^m \rangle$ for some $m \in \mathbb{Z}$. Since $(a^m)^n = (a^n)^m = e^m = e$, from Corollary 2 of Theorem 4.1, $|a^m| \big| n$. Thus$|H| \big| n$.

(3) Let $k \in \mathbb{N} \ni k|n$. [To show $\langle a^{n/k} \rangle$ is the unique subgroup of $\langle a \rangle$ of order k.] By Theorem 4.2,

$$|\langle a^{n/k} \rangle| = \frac{n}{\gcd(n, \frac{n}{k})} = \frac{n}{\frac{n}{k}} = k.$$

Now let $H \leq \langle a \rangle$ with $|H| = k$. From (1) and (2), $H = \langle a^m \rangle$ and $m|n$. Then $m = \gcd(n, m)$ and

$$k = |a^m| = |a^{\gcd(n,m)}| = \frac{n}{\gcd(n, m)} = \frac{n}{m}.$$

Thus $m = \dfrac{n}{k}$ and $H = \langle a^{n/k} \rangle$. □

COROLLARY (Subgroups of $\mathbb{Z}_n$). *For each $k \in \mathbb{N} \ni k|n$, the set $\left\langle \frac{n}{k} \right\rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k; moreover, these are the only subgroups of $\mathbb{Z}_n$.*

PROOF.

Apply Theorem 4.3 with $G = \mathbb{Z}_n$ and $a = 1$. □

EXAMPLE.

$\lvert\langle a\rangle\rvert = 42$	$\mathbb{Z}_{42}$	order
$\langle a\rangle = \{e, a, a^2, \ldots, a^{41}\}$	$\langle 1\rangle = \{0, 1, 2, \ldots, 41\}$	42
$\langle a^2\rangle = \{e, a^2, a^4, \ldots, a^{40}\}$	$\langle 2\rangle = \{0, 2, 4, \ldots, 40\}$	21
$\langle a^3\rangle = \{e, a^3, a^6, \ldots, a^{39}\}$	$\langle 3\rangle = \{0, 3, 6, \ldots, 39\}$	14
$\langle a^6\rangle = \{e, a^6, a^{12}, \ldots, a^{36}\}$	$\langle 6\rangle = \{0, 6, 12, \ldots, 36\}$	7
$\langle a^7\rangle = \{e, a^7, a^{14}, \ldots, a^{35}\}$	$\langle 7\rangle = \{0, 7, 14, \ldots, 35\}$	6
$\langle a^{14}\rangle = \{e, a^{14}, a^{28}\}$	$\langle 14\rangle = \{0, 14, 28\}$	3
$\langle a^{21}\rangle = \{e, a^{21}\}$	$\langle 21\rangle = \{0, 21\}$	2
$\langle a^{42}\rangle = \{e\}$	$\langle 42\rangle = \{0\}$	2

This is an example of isomorphic groups, groups with exactly the same structure.

DEFINITION. The Euler Phi function is defined by $\phi(1) = 1$ and, for $n > 1$, $\phi(1)$ is the number of positive integers less than n and relatively prime to n.

COROLLARY. $\forall n > 1, |U(n)| = \phi(n)$.

NOTE. Some values of $\phi(n)$ are found in Table 4.1 on page 84 of the text.

THEOREM (4.4 — Number of Elements of Each Order of a Cyclic Group).

If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.

PROOF.

By Theorem 4.3 $\exists$ exactly one subgroup of order d — say $\langle a \rangle$. Then every element of order d generates $\langle a \rangle$. By Corollary 3 of Theorem 5.2, an element a^k generates $\langle a \rangle \iff \gcd(k, d) = 1$. The number of such elements is $\phi(d)$. □

NOTE. For a finite cyclic group of order n, this means the number of elements of order d where $d|n$ depends only on d.

EXAMPLE. $\mathbb{Z}_7$, $\mathbb{Z}_{490}$, and $\mathbb{Z}_{7000}$ each has $\phi(7) = 6$ elements of order 7.

COROLLARY (Number of Elements of Order d in a Finite Group).

In a finite group (not necessarily cyclic), the number of elements of order d is divisible by $\phi(d)$.

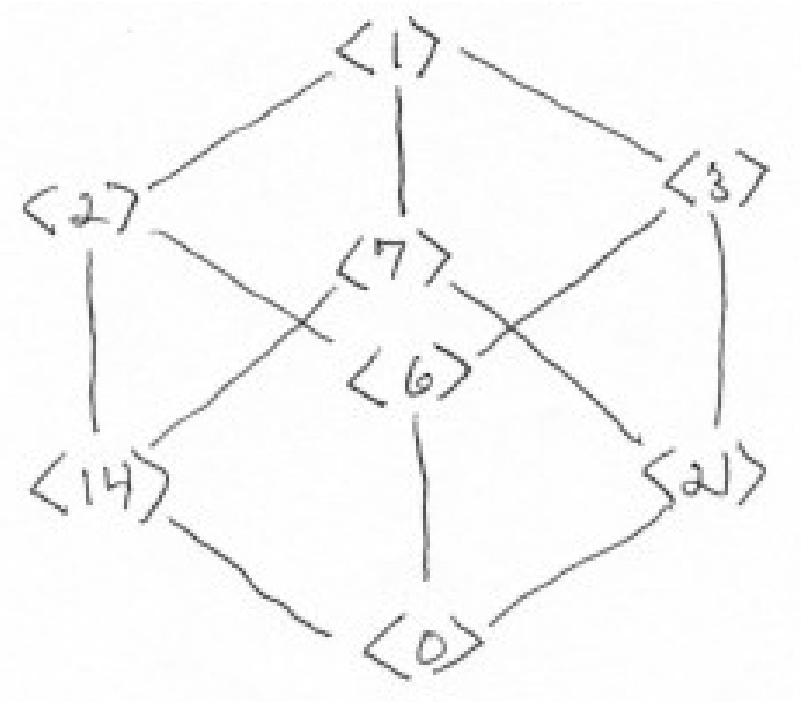
PROOF.

Let G be a finite group. If G has no elements of order d, $\phi(d)|0$. So suppose $a \in G$ with $|a| = d$. By Theorem 4.4, $\langle a \rangle$ had $\phi(d)$ elements of order d. If all elements of order d are in $\langle a \rangle$, we are done.

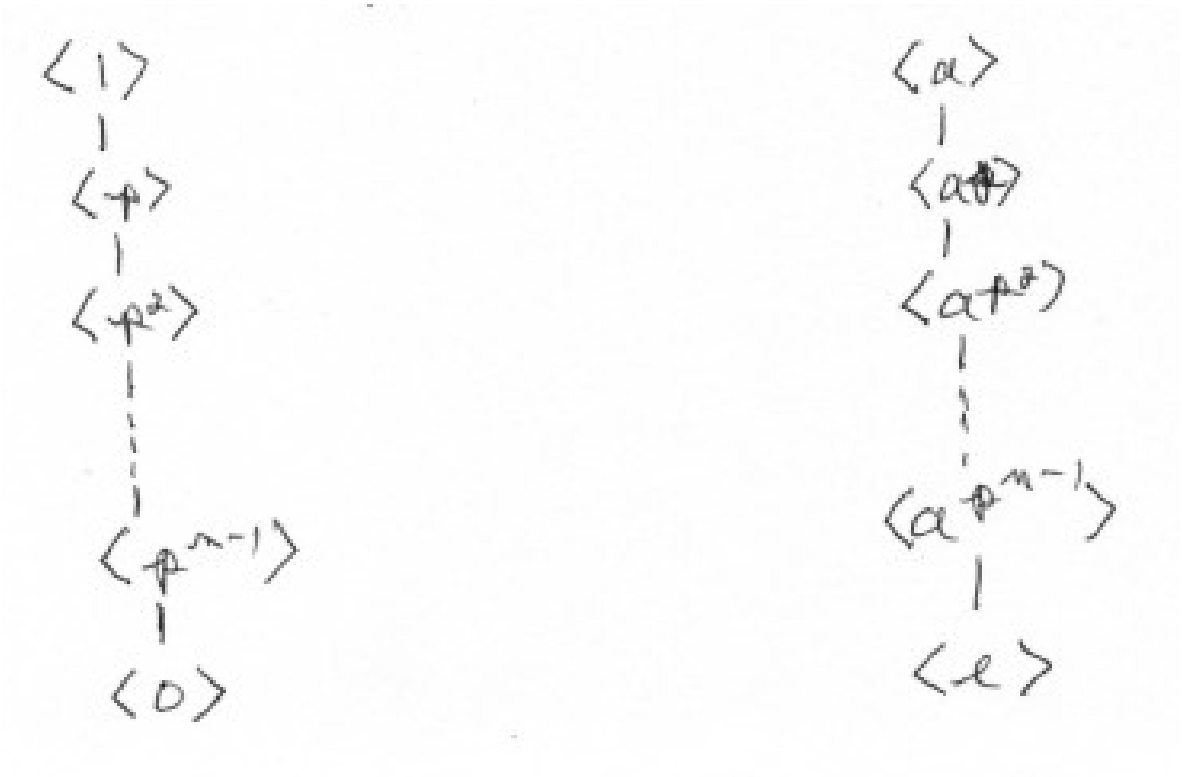
So suppose $b \in G,\ |b| = d,\ b \notin \langle a \rangle$. Then $\langle b \rangle$ also has $\phi(d)$ elements of order d. Thus, if $\langle a \rangle$ and $\langle b \rangle$ have no elements of order d in common, we have found $2\phi(d)$ elements of order d. If $|c| = d$ and $c \in \langle a \rangle \bigcap \langle b \rangle$, $\langle a \rangle = \langle c \rangle = \langle b \rangle$, a contradiction.

Continuing, the number of elements of order d is a multiple of $\phi(d)$. □

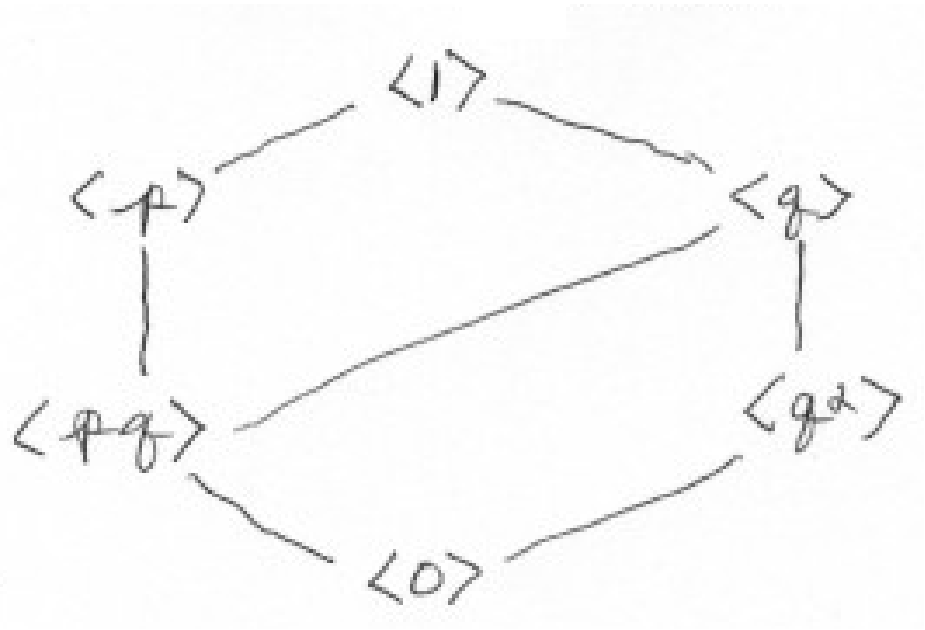
Subgroup Lattice for $\mathbb{Z}_{42}$.



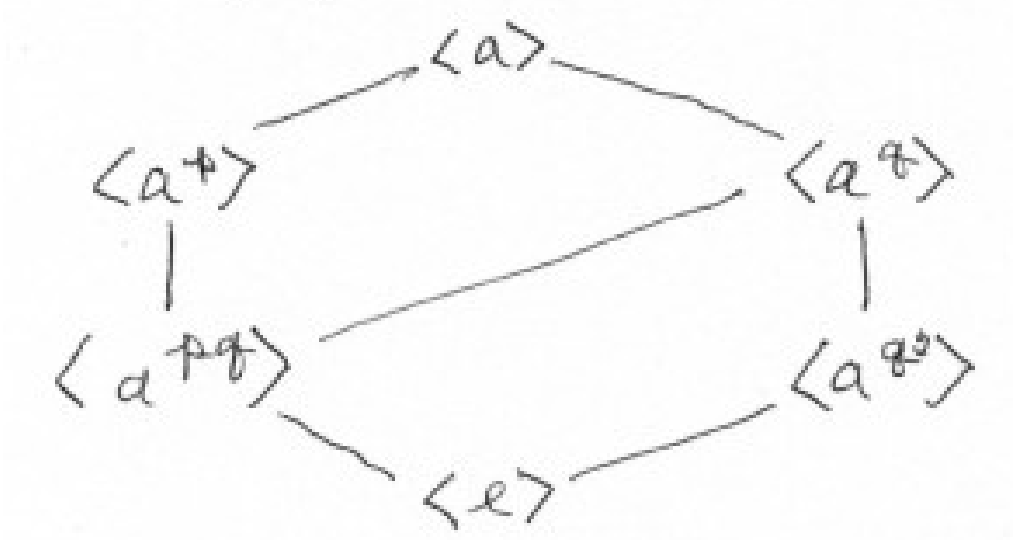
Problem (Page 89 # 35 (Adjusted)). Determine the subgroup lattices for $\mathbb{Z}_{p^n}$ and $\langle a \rangle$ with $|a| = p^n$, where p is a prime and n is some positive integer.



Subgroup Lattice for $\mathbb{Z}_{pq^2}$, where p and q are distinct primes.



Corresponding Subgroup Lattice for $\langle a \rangle$, where $|a| = pq^2$ and p and q are distinct primes.



EXAMPLE. How many elements of order 4 does D_{12} have? How many elements of order 4 does D_{4n} have?

SOLUTION. Consider D_{4n}. Since all reflections have order 2, elements of order 4 must be rotations and elements of $\langle R_{360/4n} \rangle$ where $|\langle R_{360/4n} \rangle| = 4n$. Since $4|4n$, by Theorem 4.4, the number of elements of order 4 is $\phi(4) = 2$. For D_{12}, just let $n = 3$. □

NOTE. Cyclic groups will later be shown to be building blocks for all Abelian groups in much the same way as primes are building blocks for the integers.

MAPLE. See cyclic.mw or cyclic.pdf.