4 Cyclic Groups

Definition & Basic Concepts

Recall: A group G is called **cyclic** if there exists an element $a \in G$ such that $G = \{a^n \mid n \in \mathbb{Z}\}$.

- Such an element a is called a **generator** of G
- We write $G = \langle a \rangle$ to indicate G is cyclic with generator a
- Focus: Examine cyclic groups in detail and determine their characteristics

Example 1: The Integers $\mathbb{Z}$

Claim: $\mathbb{Z}$ under ordinary addition is cyclic

Generators: Both 1 and -1 are generators

Explanation:

- When operation is addition, 1^n means:
  - $1 + 1 + \cdots + 1$ (n terms) when $n > 0$
  - $(-1) + (-1) + \cdots + (-1)$ ($|n|$ terms) when $n < 0$
- Every integer can be written as $n \cdot 1$ or $n \cdot (-1)$
- Therefore $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

Example 2: The Group $\mathbb{Z}_n$

Claim: $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ is cyclic under addition modulo n

Generators: 1 and $-1 = n-1$ are always generators

Key Insight: Unlike $\mathbb{Z}$ (which has only two generators), $\mathbb{Z}_n$ may have many generators depending on the value of n.

Example 3: Generators of $\mathbb{Z}_8$

Detailed Analysis:

- $\mathbb{Z}_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$

Verification that 3 generates $\mathbb{Z}_8$:

- $\langle 3 \rangle = \{3^0, 3^1, 3^2, 3^3, \ldots\} = \{0, 3, 6, 1, 4, 7, 2, 5\}$

2 is not a generator since $\langle 2 \rangle = \{0, 2, 4, 6\} \neq \mathbb{Z}_8$

Non-Example: $U(8)$ is Not Cyclic

Analysis: $U(8) = \{1, 3, 5, 7\}$

Checking each element:

- $\langle 1 \rangle = \{1\}$
- $\langle 3 \rangle = \{3, 9 \equiv 1\} = \{3, 1\}$
- $\langle 5 \rangle = \{5, 25 \equiv 1\} = \{5, 1\}$
- $\langle 7 \rangle = \{7, 49 \equiv 1\} = \{7, 1\}$

Conclusion: No element generates all of $U(8)$, so $U(8)$ is not cyclic.

Theorem 4.1: Criterion for $a^i = a^j$

Statement: Let G be a group, and let $a \in G$.

1. If a has infinite order, then $a^i = a^j$ if and only if $i = j$
2. If a has finite order n, then:

- $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$
- $a^i = a^j$ if and only if n divides $(i - j)$

Proof of Theorem 4.1

Part 1 (Infinite Order):
If $|a| = \infty$, there is no nonzero n such that $a^n = e$.
Since $a^i = a^j$ implies $a^{i-j} = e$, we must have $i - j = 0$, so $i = j$.

Part 2 (Finite Order): Assume $|a| = n$.

First, prove $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$*:*

- Clearly $\{e, a, \ldots, a^{n-1}\} \subseteq \langle a \rangle$
- Let $a^k \in \langle a \rangle$ be arbitrary
- By division algorithm: $k = nq + r$ where $0 \leq r < n$
- Then $a^k = a^{nq+r} = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$
- So $a^k \in \{e, a, \ldots, a^{n-1}\}$

Next, prove the equivalence for $a^i = a^j$:

($\Rightarrow$) Assume $a^i = a^j$, prove $n \mid (i - j)$:

- $a^i = a^j$ implies $a^{i-j} = e$
- By division algorithm: $i - j = nq + r$ where $0 \leq r < n$
- Then $e = a^{i-j} = a^{nq+r} = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$
- Since n is the smallest positive integer with $a^n = e$, we need $r = 0$
- Therefore $n \mid (i - j)$

($\Leftarrow$) If $i - j = nq$, then $a^{i-j} = a^{nq} = (a^n)^q = e^q = e$, so $a^i = a^j$

Corollaries of Theorem 4.1

Corollary 1: For any group element a, $|a| = |\langle a \rangle|$

Corollary 2: For any group element a, $a^k = e$ if and only if $|a|$ divides k

Corollary 3: For any group element a, $a^k = e$ if and only if k is a multiple of $|a|$

Corollary 4: If a and b belong to a finite group and $ab = ba$, then $|ab|$ divides $|a||b|$

Proof of Corollary 4: Let $|a| = m$ and $|b| = n$. Then $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e^n e^m = e$. By Corollary 2, $|ab|$ divides mn.

Key Insight: Multiplication in $\langle a \rangle$ is essentially addition modulo n.
If $(i + j) \bmod n = k$, then $a^i a^j = a^k$.

Theorem 4.2: Order and Subgroup Generation

Statement: Let a be an element of order n in a group and let k be a positive integer. Then:

- $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$
- $|a^k| = \dfrac{n}{\gcd(n, k)}$

Significance: This theorem provides a simple method for computing $|a^k|$ and determining when $\langle a^i \rangle = \langle a^j \rangle$.

Proof of Theorem 4.2

Let $d = \gcd(n, k)$ and write $k = dr$.

Part 1: $\langle a^k \rangle = \langle a^d \rangle$

Show $\langle a^k \rangle \subseteq \langle a^d \rangle$*:*
Since $a^k \in \langle a^d \rangle$, by closure $\langle a^k \rangle \subseteq \langle a^d \rangle$.

Show $\langle a^d \rangle \subseteq \langle a^k \rangle$*:*

- By gcd theorem: $d = ns + kt$ for integers s, t
- So $a^d = a^{ns+kt} = a^{ns} \cdot a^{kt} = (a^n)^s (a^k)^t = e^s (a^k)^t = (a^k)^t \in \langle a^k \rangle$
- Therefore $\langle a^d \rangle \subseteq \langle a^k \rangle$

Part 2: $|a^k| = \dfrac{n}{\gcd(n, k)}$

From Part 1: $|a^k| = |\langle a^k \rangle| = |\langle a^d \rangle| = |a^d| = \dfrac{n}{d} = \dfrac{n}{\gcd(n, k)}$

Example 5: Applications of Theorem 4.2

Given: $|a| = 30$. Find $\langle a^{26} \rangle$, $\langle a^{17} \rangle$, $\langle a^{18} \rangle$ and $|a^{26}|$, $|a^{17}|$, $|a^{18}|$.

Solution:

For a^{26}:

- $\gcd(30, 26) = 2$
- $\langle a^{26} \rangle = \langle a^2 \rangle = \{e, a^2, a^4, a^6, \ldots, a^{28}\}$
- $|a^{26}| = \frac{30}{2} = 15$

For a^{17}:

- $\gcd(30, 17) = 1$
- $\langle a^{17} \rangle = \langle a^1 \rangle = \langle a \rangle = \{e, a, a^2, \ldots, a^{29}\}$
- $|a^{17}| = \frac{30}{1} = 30$

For a^{18}:

- $\gcd(30, 18) = 6$
- $\langle a^{18} \rangle = \langle a^6 \rangle = \{e, a^6, a^{12}, a^{18}, a^{24}\}$
- $|a^{18}| = \frac{30}{6} = 5$

Example 6: Large Values Using Prime Factorization

Given: $|a| = 1000$. Find $\langle a^{140} \rangle$, $\langle a^{400} \rangle$, $\langle a^{62} \rangle$ and their orders.

Prime factorizations: $1000 = 2^3 \cdot 5^3$, $140 = 2^2 \cdot 5 \cdot 7$, $400 = 2^4 \cdot 5^2$, $62 = 2 \cdot 31$

- $\gcd(1000, 140) = 2^2 \cdot 5 = 20$: $\langle a^{140} \rangle = \langle a^{20} \rangle$, $|a^{140}| = \frac{1000}{20} = 50$.
- $\gcd(1000, 400) = 2^3 \cdot 5^2 = 200$: $\langle a^{400} \rangle = \langle a^{200} \rangle$, $|a^{400}| = \frac{1000}{200} = 5$
- $\gcd(1000, 62) = 2$: $\langle a^{62} \rangle = \langle a^{2} \rangle$, $|a^{62}| = \frac{1000}{2} = 500$

Corollaries of Theorem 4.2

Corollary 1: In a finite cyclic group, the order of an element divides the order of the group.

Corollary 2: Let $|a| = n$. Then:

- $\langle a^i \rangle = \langle a^j \rangle$ if and only if $\gcd(n, i) = \gcd(n, j)$ if and only if $|a^i| = |a^j|$.

Corollary 3: Let $|a| = n$. Then $\langle a^j \rangle = \langle a \rangle$ if and only if $\gcd(n, j) = 1$.

Corollary 4: An integer k in $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ if and only if $\gcd(n, k) = 1$.

Application: Finding All Generators

Example: $U(50)$

- First determine $|U(50)| = \varphi(50) = \varphi(2 \cdot 5^2) = \varphi(2)\varphi(5^2) = 1 \cdot 20 = 20$
- Direct computation shows 3 is a generator
- By Corollary 3, all generators are: 3^j where $\gcd(20, j) = 1$

Complete list of generators:

- $j = 1$: $3^1 \equiv 3 \pmod{50}$
- $j = 3$: $3^3 \equiv 27 \pmod{50}$
- $j = 7$: $3^7 \equiv 37 \pmod{50}$
- $j = 9$: $3^9 \equiv 33 \pmod{50}$
- $j = 11$: $3^{11} \equiv 47 \pmod{50}$
- $j = 13$: $3^{13} \equiv 23 \pmod{50}$
- $j = 17$: $3^{17} \equiv 13 \pmod{50}$
- $j = 19$: $3^{19} \equiv 17 \pmod{50}$

Theorem 4.3: Fundamental Theorem of Cyclic Groups

Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a\rangle| = n$, then:

1. The order of any subgroup of $\langle a\rangle$ is a divisor of n
2. For each positive divisor k of n, the group $\langle a\rangle$ has exactly one subgroup of order k—namely, $\langle a^{n/k}\rangle$

Interpretation: For cyclic group of order 30:

- Has subgroups of orders $1, 2, 3, 5, 6, 10, 15, 30$ only.
- Exactly one subgroup of each order.
- Subgroup of order k is $\langle a^{30/k}\rangle$.

Proof of Theorem 4.3: Let $G = \langle a \rangle$ and H be a subgroup of G.

Step 1: H is cyclic: If $H = \{e\}$, then H is cyclic

- Otherwise, H contains some a^t with $t > 0$ (if $a^t \in H$ with $t < 0$, then $a^{-t} \in H$)
- Let m be the least positive integer such that $a^m \in H$. Claim: $H = \langle a^m \rangle$

Proof of claim: Let $b \in H$ be arbitrary. Since $b \in G = \langle a \rangle$, we have $b = a^k$.

- By division algorithm: $k = mq + r$ where $0 \leq r < m$
- Then $a^r = a^{k-mq} = a^k(a^m)^{-q} \in H$ (since $a^k \in H$ and $a^m \in H$)
- Since m is minimal and $0 \leq r < m$, we must have $r = 0$
- Therefore $b = a^k = a^{mq} = (a^m)^q \in \langle a^m \rangle$

Step 2: Orders divide n

From Step 1 and Theorem 4.2: $H = \langle a^m \rangle$ where m divides n, and $|a^m| = \frac{n}{m}$.

So $|H| = \frac{n}{m}$, which divides n.

Step 3: Unique subgroup of each order

- If k divides n, then $|\langle a^{n/k} \rangle| = k$
- If K is any subgroup of order k, then $K = \langle a^s \rangle$ where s divides n and $|a^s| = \frac{n}{s} = k$
- This gives $s = \frac{n}{k}$, so $K = \langle a^{n/k} \rangle$

Conclusion: Each divisor k of n corresponds to exactly one subgroup $\langle a^{n/k} \rangle$ of order k.

Example 7: Subgroups of $\mathbb{Z}_{30}$

Complete list of subgroups of $\mathbb{Z}_{30}$: The divisors of 30 are $30, 15, 10, 6, 5, 3, 2,$ and $1.$

- $\langle 1 \rangle = \{0, 1, 2, \ldots, 29\}$, order 30
- $\langle 2 \rangle = \{0, 2, 4, \ldots, 28\}$, order 15
- $\langle 3 \rangle = \{0, 3, 6, \ldots, 27\}$, order 10
- $\langle 5 \rangle = \{0, 5, 10, 15, 20, 25\}$, order 6
- $\langle 6 \rangle = \{0, 6, 12, 18, 24\}$, order 5
- $\langle 10 \rangle = \{0, 10, 20\}$, order 3
- $\langle 15 \rangle = \{0, 15\}$, order 2
- $\langle 30 \rangle = \{0\}$, order 1

Pattern: For divisor k of 30, the subgroup of order k is $\langle 30/k \rangle$.

Corollary: Subgroups of $\mathbb{Z}_n$

Statement: For each positive divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k; moreover, these are the only subgroups of $\mathbb{Z}_n$.

General Pattern:

- Divisors of n: $d_1, d_2, \ldots, d_t$
- Subgroups: $\langle n/d_1 \rangle, \langle n/d_2 \rangle, \ldots, \langle n/d_t \rangle$
- Orders: $d_1, d_2, \ldots, d_t$ respectively

Definition:The Euler Phi Function

- $\varphi(1) = 1$
- For $n > 1$: $\varphi(n) =$ number of positive integers less than n and relatively prime to n
- Note: $|U(n)| = \varphi(n)$

n	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4

Key formulas:

- $\varphi(p^r) = p^r - p^{r-1}$ for prime p
- $\varphi(p_1^{r_1} \cdot p_2^{r_2} \cdots p_m^{r_m}) = \varphi(p_1^{r_1})\varphi(p_2^{r_2}) \cdots \varphi(p_m^{r_m})$ for distinct primes

Theorem 4.4: Number of Elements of Each Order

If $d|n$, $d > 0$. The number of elements of order d in a cyclic group of order n is $\varphi(d)$.

Proof: Let a be a generator.

- By Theorem 4.3, there is exactly one subgroup of order d: $\langle a^{n/d} \rangle$
- Every element of order d generates this subgroup
- By Corollary 3 of Theorem 4.2, a^k generates $\langle a^{n/d} \rangle$ iff $\gcd(k, d) = 1$
- Number of such k is precisely $\varphi(d)$

Example: $\mathbb{Z}_8$, $\mathbb{Z}_{640}$, and $\mathbb{Z}_{80000}$ each have $\varphi(8) = 4$ elements of order 8.

Example 9: Orders in $U(50)$ and $U(13)$

For element 3 in $U(50)$:

- $\varphi(50) = \varphi(2 \cdot 5^2) = \varphi(2)\varphi(5^2) = 1 \cdot 20 = 20$
- So $|U(50)| = 20$, possible orders for $|3|$: $1, 2, 4, 5, 10, 20$
- $3^4 \equiv 81 \equiv 31 \not\equiv 1 \pmod{50}$, so $|3| \neq 2, 4$
- $3^{10} \equiv 3^5 \cdot 3^5 \equiv 243 \cdot 243 \equiv (-7)(-7) \equiv 49 \not\equiv 1 \pmod{50}$
- So $|3| \neq 5, 10$, therefore $|3| = 20$ and $U(50) = \langle 3 \rangle$

For element 2 in $U(13)$:

- $|U(13)| = \varphi(13) = 12$
- $2^4 \equiv 16 \equiv 3 \not\equiv 1 \pmod{13}$, so $|2| \neq 2, 4$
- $2^6 \equiv 64 \equiv 12 \equiv -1 \not\equiv 1 \pmod{13}$, so $|2| \neq 3, 6$
- Therefore $|2| = 12$

Non-Cyclic Examples

$U(80)$ is not cyclic:

- Note that $9^2 = 81 \equiv 1 \pmod{80}$
- Since $-1 \not\equiv 9 \pmod{80}$, we have two distinct elements of order $\mathbf{2}$
- For cyclic groups, $-\mathbf{1}$ must be the unique element of order $\mathbf{2}$
- Therefore $U(80)$ is not cyclic

Non-Cyclic Examples

$U(80)$ **is not cyclic:**

- Note that $79^2 \equiv (-1)^2 \equiv 1 \pmod{80}$ and $9^2 = 81 \equiv 1 \pmod{80}$
- Since $-1 \not\equiv 9 \pmod{80}$, we have two distinct elements of order 2
- Therefore $U(80)$ is not cyclic

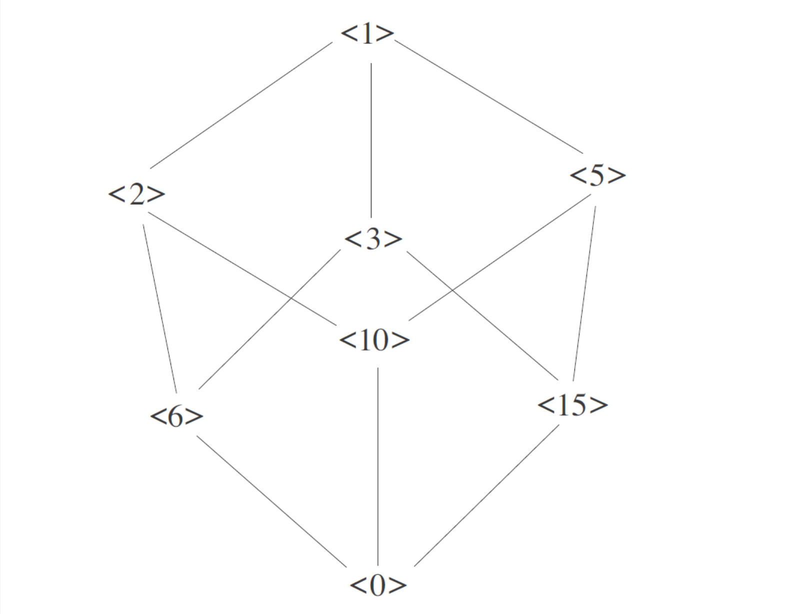
Key insight: For cyclic groups $U(n)$, -1 ($= n - 1$) must be the unique element of order 2

$U(120)$ is not cyclic:

- Note that $11^2 = 121 \equiv 1 \pmod{120}$
- Again, multiple elements of order 2 exist
- Therefore $U(120)$ is not cyclic

Subgroup Lattice Diagram

Subgroup Lattice of $\mathbb{Z}_{30}$:



Reading the diagram:

- Each line represents a proper subgroup relation
- $\langle 10 \rangle$ is a subgroup of both $\langle 2 \rangle$ and $\langle 5 \rangle$
- $\langle 6 \rangle$ is not a subgroup of $\langle 10 \rangle$

Comparison: Cyclic vs. Non-Cyclic Groups

Cyclic groups (like $\mathbb{Z}_{30}$):

- Subgroups easily identified by Theorem 4.3
- Exactly one subgroup per divisor of the order
- Simple, predictable structure

Non-cyclic groups (like $U(30)$ or D_{30}):

- Much more complex subgroup structure
- May have zero, one, or many subgroups for each divisor
- Example: D_4 has five subgroups of order 2 and three of order 4