

Lagrange's Theorem & Cyclic Groups — CSIR NET Mathematical Sciences

Algebra | Unit: Group Theory | Concept + Formulas + Solved Examples

1. Definitions

DEFINITION — ORDER OF A GROUP / ELEMENT

The **order** of a finite group G , denoted $|G|$, is the number of elements in G . The **order of an element** $g \in G$, denoted $o(g)$, is the smallest positive integer n such that $g^n = e$ (identity).

DEFINITION — CYCLIC GROUP

A group G is **cyclic** if there exists $g \in G$ such that $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. Such g is called a **generator** of G .

2. Lagrange's Theorem

THEOREM — LAGRANGE'S THEOREM

If G is a finite group and H is a subgroup of G , then $|H|$ divides $|G|$:

$$|G| = |H| \cdot [G : H]$$

where $[G : H]$ is the number of (left or right) cosets of H in G , called the **index** of H .

COROLLARY — ORDER OF AN ELEMENT DIVIDES $|G|$

For any $g \in G$, $o(g)$ divides $|G|$. Consequently, $g^{|G|} = e$ for every $g \in G$.

CONVERSE IS FALSE

The converse of Lagrange's theorem does **not** hold in general: if d divides $|G|$, G need not have a subgroup of order d . Classic counterexample: A_4 (alternating group on 4 letters) has order 12, but has **no subgroup of order 6**.

3. Key Points to Remember

- Every group of **prime order** p is cyclic, and is generated by any non-identity element (direct consequence of Lagrange's theorem, since the only divisors of p are 1 and p).
- Every cyclic group is **abelian**, but not every abelian group is cyclic (e.g. $\mathbb{Z}_2 \times \mathbb{Z}_2$).
- A cyclic group of order n has exactly $\varphi(n)$ generators, where φ is Euler's totient function.
- Every subgroup of a cyclic group is itself cyclic.
- For each positive divisor d of n , a cyclic group of order n has **exactly one** subgroup of order d .
- Two cyclic groups of the same order are isomorphic — up to isomorphism, there is exactly **one** cyclic group of each order n , namely $\mathbb{Z}_n$ (or $\mathbb{Z}$ if infinite).
- Fermat's Little Theorem and Euler's Theorem in number theory are direct consequences of Lagrange's Theorem applied to $(\mathbb{Z}/n\mathbb{Z})^*$.

4. Important Formulas

LAGRANGE'S FORMULA

$$|G| = |H| \times [G : H]$$

NUMBER OF GENERATORS OF $\mathbb{Z}_N$

$$\#\{\text{generators}\} = \varphi(n)$$

where $\varphi(n)$ counts integers in $\{1, \dots, n\}$ coprime to n .

EULER / FERMAT (VIA LAGRANGE)

For $\gcd(a, n) = 1$: $a^{\varphi(n)} \equiv 1 \pmod{n}$. In particular, for prime p and $\gcd(a, p) = 1$:
 $a^{p-1} \equiv 1 \pmod{p}$.

5. Worked Examples

EXAMPLE 1 — APPLYING LAGRANGE'S THEOREM

Can a group of order 15 have a subgroup of order 4?

Solution: By Lagrange's Theorem, the order of any subgroup must divide $|G| = 15$. Since $4 \nmid 15$, **no** subgroup of order 4 can exist.

EXAMPLE 2 — GROUPS OF PRIME ORDER

Show every group of order 7 is cyclic.

Solution: Let $|G| = 7$ (prime). Take any $g \neq e$. By Lagrange, $o(g)$ divides 7, so $o(g) \in \{1, 7\}$. Since $g \neq e$, $o(g) \neq 1$, hence $o(g) = 7 = |G|$. So $\langle g \rangle = G$, meaning G is cyclic.

EXAMPLE 3 — GENERATORS OF $\mathbb{Z}_{12}$

Find the number of generators of the cyclic group $\mathbb{Z}_{12}$.

Solution: Number of generators $= \varphi(12)$. Since $12 = 2^2 \times 3$:

$$\varphi(12) = 12 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$$

The generators are $\{1, 5, 7, 11\}$ (elements coprime to 12).

EXAMPLE 4 — SUBGROUPS OF A CYCLIC GROUP

List all subgroups of $\mathbb{Z}_{12}$.

Solution: Divisors of 12: 1, 2, 3, 4, 6, 12. By the theorem, there is exactly one subgroup for each divisor: $\{0\}$ (order 1), $\{0, 6\}$ (order 2), $\{0, 4, 8\}$ (order 3), $\{0, 3, 6, 9\}$ (order 4), $\{0, 2, 4, 6, 8, 10\}$ (order 6), and $\mathbb{Z}_{12}$ itself (order 12).

6. Common Pitfalls (Exam Traps)

WATCH OUT

- Never assume the **converse** of Lagrange's theorem — " d divides $|G|$ " does **not** guarantee a subgroup of order d exists (fails for non-cyclic groups like A_4).
- The unique-subgroup-per-divisor property holds only for **cyclic** groups — do not apply it to general finite groups.
- Cyclic $\implies$ abelian, but abelian $\not\implies$ cyclic — a very common confusion point.
- The order of an element must divide $|G|$, but not every divisor of $|G|$ is necessarily the order of some element (again, only guaranteed for cyclic groups by direct construction).

7. Quick Revision Summary

Concept	Key Fact
Lagrange's Theorem	$ G = H \cdot [G : H]$
Order of element	$o(g)$ divides $ G $; $g^{ G } = e$
Converse of Lagrange	False in general (e.g. A_4 , order 12, no subgroup of order 6)
Prime order groups	Always cyclic
Cyclic $\implies$ Abelian	True; converse false
Generators of $\mathbb{Z}_n$	$\varphi(n)$ of them
Subgroups of cyclic group	Exactly one per divisor of n ; all cyclic

CSIR NET

Algebra

Group Theory

Lagrange's Theorem