1. Grupet (Grupet)

Një grup $(G, *)$ është bashkësi me veprim binar që plotëson:

- **Mbyllje**: $\forall a, b \in G, a * b \in G$
- **Asociativitet**: $(a * b) * c = a * (b * c)$
- **Element Neutral** $\exists e \in G : a * e = e * a = a$
- **Invers**: $\forall a \in G, \exists a^{-1} \in G : a * a^{-1} = e$

2. NënGrupet

$H \subseteq G$ është nëngrup $(H \leq G)$ nëse:

- $e \in H$
- $\forall a, b \in H, a * b \in H$
- $\forall a \in H, a^{-1} \in H$

Testi i Shpejtë: $\forall a, b \in H, a * b^{-1} \in H$.

3. Grupet Ciklike

G është ciklik nëse $\exists g \in G$ (gjenerator) i tillë që $G = \langle g \rangle = \{g^n | n \in \mathbb{Z}\}$.
G ciklik $\Leftrightarrow \exists g \in G$ me $r(g) = |G|$.

4. Klasat Fqinje (Cosets)

Për $H \leq G$ dhe $a \in G$:

- Klasa e majtë: $aH = \{ah | h \in H\}$
- Klasa e djathtë: $Ha = \{ha | h \in H\}$

5. Teorema e Lagranzhit

Nëse $H \leq G$ e fundme, atëherë $|H|$ pjesëton $|G|$.
Numri i klasave fqinje: $[G : H] = \frac{|G|}{|H|}$.

6. Teorema e Vogël e Fermatit

Për p prim dhe $a \in \mathbb{Z}$ me $\gcd(a, p) = 1$:

$$a^{p-1} \equiv 1 \pmod{p}$$

Përgjigje për pyetjet specifike

- Grupi është ciklik nëse $\exists n \in G$ me $r(n) = |G|$.
- Numri gjeneratorëve: $\phi(|G|)$ (funksioni i Euler-it).
- Gjetja e $r(n)$, $\langle n \rangle$ dhe klasave fqinje:
- $r(n) = \min\{k > 0 | n^k = e\}$
- $\langle n \rangle = \{n^0, n^1, \ldots, n^{r(n)-1}\}$
- Klasat fqinje: $a\langle n \rangle$ ku a është elementi më i vogël në G por jo në $\langle n \rangle$
- Eksponenti i grupit: $\max\{r(a) | a \in G\}$.
- Klasat fqinje të $\langle n \rangle$ janë $a\langle n \rangle$ ku a është elementi më i vogël në G por jo në $\langle n \rangle$.