Big Theorem [Lagrange's theorem] Let $(G,*)$ be a finite group and $H \subseteq G$ a subgroup. Then $|H| \mid |G|$.
↑ divides

Lemma: Given an arbitrary group G and a subgroup $H \subseteq G$, if $x \in H$, the map of sets $\phi_x : H \to xH$ is a bijection.

Pf ϕ_x is injective: $\phi_x(a) = \phi_x(b) \Rightarrow xa = xb \Rightarrow a = b$

ϕ_x is surjective: Given $y \in xH \Rightarrow x^{-1}y \in H \Rightarrow y = \phi_x(h)$
(or $\exists\, h \in H$ s.t. $x \cdot h = y$) $= \phi_x(x^{-1}y)$.

Thus, if G is a finite group, $\phi_x : H \to xH$ is a bijection of finite sets

$$\Rightarrow |H| = |xH|.$$

Pf of Lagrange The equivalence classes generated by $\sim_L$ are of the form $x \cdot H$ and the collection of them partition G. Since G has finite order, the collection is finite i.e. $\{x_1 H, \dots, x_p H\}$ is a partition of G. Thus

$$|G| = \sum_{i=1}^{p} |x_i H| \quad \text{(disjointness)}$$
$$= \sum_{i=1}^{p} |H|$$
$$= p \cdot |H|$$
$$\Rightarrow |H| \mid |G| \quad \blacksquare$$

Cor If $|G,*)$ is finite, then $[G:H] = |G/H| = |G|/|H|$.

Cor Let $p \geq 1$ be a prime number and let $(G,*)$ be a group of size p. Then the only subgroups of G are $\{e\}$ and G.

These are all useful if we want to classify all subgroups of a group / understand the group.

Pf Let $H \leq G$ be a subgroup. By Lagrange's theorem, $|H| \mid |G|$

$\Rightarrow |H| \mid p$

$\Rightarrow |H| = 1$ or p by definition of prime.

If $|H| = 1 \Rightarrow H = \{e\}$ and if $|H| = p \Rightarrow H = G$ ∎

Ex • $\mathbb{Z}/p\mathbb{Z}$ for p a prime

• $\langle [2] \rangle \leq \mathbb{Z}/4\mathbb{Z}$ is a subgroup: More precisely $\langle 2 + 4\mathbb{Z} \rangle = \{[0], [2]\}$.

• $\langle 2 \rangle, \langle 3 \rangle \leq \mathbb{Z}/6\mathbb{Z}$ are subgroups of different sizes

↑ we "dropped" the brackets.

Prop A group of prime order (size) is cyclic.

Pf Let G have prime order. For any $a \neq e_G$, consider $\langle a \rangle$. Then $\langle a \rangle \leq G$ is a nontrivial subgroup $\Rightarrow |\langle a \rangle| > 1$. But by Lagrange (or it's corollary) $\Rightarrow |\langle a \rangle| \mid p \Rightarrow \langle a \rangle = p \Rightarrow \langle a \rangle = G$.

Non ex: $(\mathbb{R}^*, \times)$ is not cyclic

Thm Let G be a cyclic group. Then

① If G is infinite, then $G \cong (\mathbb{Z}, +)$

② If G is finite of size m, then $G \cong (\mathbb{Z}/m\mathbb{Z}, +)$.

Pf By assumption $G = \langle x \rangle = \{x^n : n \in \mathbb{Z}\}$. If all the elements of G are distinct (i.e. $x^n \neq x^m \ \forall n \neq m$), the map of sets, $\psi : (\mathbb{Z}, +) \longrightarrow G$,

$$n \longmapsto x^n$$

is bijective. But $\psi(n+m) = x^{n+m} = x^n \cdot x^m = \psi(n)\psi(m) \Rightarrow \psi$ is a homorphism. Thus ψ is an isomorphism and $(\mathbb{Z}, +) \cong G$.

Now assume the elements of G are not distinct, say $x^n = x^m$ with $m > n$. Then, $e = x^{m-n} \Rightarrow x^{-1} = x^{m-n-1}$

$$\Rightarrow G = \{e_G, x, \ldots, x^{m-n-1}\}.$$

A better choice would be to choose ℓ minimal such that $x^\ell = e_G$.
Then $G = \{e, x, \dots, x^{\ell-1}\}$. Consider the map,

(so all elements are distinct (minimality of ℓ))

$$\psi: G \longrightarrow \mathbb{Z}/\ell\mathbb{Z}, \quad x^i \longmapsto [i]$$

This is a surjection of finite sets of the same size its ℓ. $\Rightarrow \psi$ is a bijection.

Since $\psi(x^i \cdot x^j) = \psi(x^{i+j}) = [i+j] = [i] + [j] \Rightarrow \psi$ is a homomorphism.
Thus ψ is an isomorphism ∎

Thm Every subgroup of a cyclic group is cyclic.

Pf ① Assume $G \cong (\mathbb{Z}, +)$: Let H be a subgroup. Since $\{e_G\}$ is cyclic we may assume $H \neq \{e_G\}$. Choose $m > 0$ minimal such that $m \in H$ (exists because H is non-trivial). ~~by division algorithm, [illegible] and [illegible]~~. Then $m\mathbb{Z} \subseteq H$ and we will show equality!
Assume for the sake of a contradiction, $\exists\, n \in H - m\mathbb{Z}$.
Then by division algorithm $n = mq + r$ with $0 \leq r < m$.
Since $n, mq \in H$ by definition of subgroup, $n - mq \in H \Rightarrow r \in H$ and this contradicts minimality of m. Thus $m\mathbb{Z} = H$.

② Assume $G \cong (\mathbb{Z}/m\mathbb{Z}, +)$: As above let $H \subseteq \mathbb{Z}/m\mathbb{Z}$ be a non trivial subgroup and choose $m > 0$ minimal satisfying $[m] \in H$.
Then $\langle [m] \rangle \subseteq H$ and proceed as before ∎

So we know all cyclic groups (up to) isomorphism. By the above theorem we also know it's subgroups upto isomorphism. But how many of them are there, assuming G is finite?

Thm Let G be a finite cyclic group [i.e. $\cong (\mathbb{Z}/m\mathbb{Z}, +)$] of size n.
Then for each $d > 0$, $d \mid n$ there is a unique subgroup of size d.
Combing this with Lagrange's theorem we know "everything" about the subgroups of finite cyclic groups.

Pf Via the isomorphism $G \cong \mathbb{Z}/n\mathbb{Z}$, we may assume $H \subseteq \mathbb{Z}/n\mathbb{Z}$.

Now, $\langle [\frac{n}{d}] \rangle$ is a subgroup of size $n/\frac{n}{d} = d$. We just need to show $H = \langle [\frac{n}{d}] \rangle$. Well in our proof previous thm. we showed $H = \langle [m] \rangle$ where m is the minimal non-zero element (if $H \neq \{e\}$).
$\in H$

Thus $H = \langle [m] \rangle = \{[0], [m], [m]\cdot 2, \dots, [m]\cdot(d-1)\}$ (it's cyclic of size d).

In particular, $[m]\cdot d = [0] \Rightarrow n \mid (m\cdot d) \Rightarrow md = k\cdot n$ for $k \geq 1$.

$\Rightarrow m = k\cdot\frac{n}{d}$

$\Rightarrow m \in \langle [\frac{n}{d}] \rangle$

$\Rightarrow H \subseteq \langle [\frac{n}{d}] \rangle$.

But they have the same size $\Rightarrow H = \langle [\frac{n}{d}] \rangle$ ∎

Def Given an element $x \in G$, it's said to have infinite order if $|\langle x \rangle| = \infty$. x is said to have finite order if $|\langle x \rangle| < \infty$. Moreover, the order of x is $|\langle x \rangle|$ and denoted by $\text{ord}(x)$.

- Equivalently, $\text{ord}(x) = \min\{m \in \mathbb{Z}_{>0} : x^m = e_G\}$.

Ex
- $e \in G$ has finite order
- $2 \in \mathbb{Z}$ has infinite order
- $[2] \in \mathbb{Z}/6\mathbb{Z}$ is of order 3.

Cor Let G be a finite group and $x \in G$. Then $\text{ord}(x) \mid |G|$ and $x^{|G|} = e_G$.

Pf $\text{ord}(x) \mid |G|$ follows from Lagrange's theorem with $H = \langle x \rangle$.

By our remark $x^{\text{ord}(x)} = e_G$

$\Rightarrow x^{\text{ord}(x)\cdot\frac{|G|}{\text{ord}x}} = e_G^{\frac{|G|}{\text{ord}x}}$

$\Rightarrow x^{|G|} = e_G$ ∎