Finitely Generated Groups

Let $(G,*)$ be a group and $X \subset G$ a subset.

Let $X^{-1} = \{x^{-1} \mid x \in X\}$.

Definition Exercise to check

The subgroup generated by X, denoted $gp(X) \subset G$ is the set of all finite compositions of elements in $X \cup X^{-1} \cup \{e\}$.

For example, if $x, y, z \in X \Rightarrow x * y^{-1} * z^{-1} * y \in gp(X)$.

Remark

minimal subgroup of G containing X.

1) $H \subset G$ a subgroup and $X \subset H \Rightarrow gp(X) \subset H$

2) Similar to $\text{Span}(X) \subset V$, where V is a vector space.

3) Given $x \in G$, $gp(\{x\}) = \{x^a \mid a \in \mathbb{Z}\}$.

Definition

If $\exists X \subset G$, $|X| < \infty$ such that $gp(X) = G$, we say G is finitely generated. If $\exists x \in G$ such that $gp(\{x\}) = G$ we say G is cyclic.

similar to being finite dimensional in linear algebra

Examples

$|G| < \infty \Rightarrow G$ finitely generated.

$(\mathbb{Z}, +)$, $(\mathbb{Z}/m\mathbb{Z}, +)$ are cyclic, $gp(\{1\}) = \mathbb{Z}$, $gp(\{[1]\}) = \mathbb{Z}/m\mathbb{Z}$

$(\mathbb{Q}, +)$ not finitely generated. Good exercise

Proposition G cyclic $\Rightarrow$ G Abelian

Proof Given $a, b \in \mathbb{Z}$ $x^a * x^b = x^{(a+b)} = x^{(b+a)} = x^b * x^a$ $\square$

Definition Let $(G, *)$ be a group and $x \in G$. We say

x is finite order if $\exists\, m \in \mathbb{N}$ such that $x^m = e$

In this case, $\text{ord}(x) =$ minimal $m \in \mathbb{N}$ such that $x^m = e$. ← order of x

Otherwise we say that x is infinite order. so $x^{\text{ord}(x)} = e$

Example

$[1] \in \mathbb{Z}/_m\mathbb{Z}$ has order m, $1 \in \mathbb{Z}$ has infinite order

Proposition $x \in G$, $n \in \mathbb{N}$ then $x^n = e \iff \text{ord}(x) \mid n$

Proof Assume $x^n = e$ and $\text{ord}(x) \nmid n$

Remainder Theorem $\Rightarrow$ $n = q\,\text{ord}(x) + r$, $0 < r < \text{ord}(x)$

$$\Rightarrow e = x^n = x^{q\,\text{ord}(x) + r} = \left(x^{\text{ord}(x)}\right)^q * x^r = e^q * x^r = x^r$$

Contradiction as $0 < r < \text{ord}(x)$. $\Rightarrow$ $\text{ord}(x) \mid n$

$\text{ord}(x) \mid n \Rightarrow \exists\, q \in \mathbb{N}$ such that $n = q\,\text{ord}(x)$

$$\Rightarrow x^n = x^{q\,\text{ord}(x)} = \left(x^{\text{ord}(x)}\right)^q = e^q = e$$ $\square$

Theorem If $x \in G$ is infinite order then $gp(x) \cong (\mathbb{Z}, +)$.

Proof

$$gp(\{x\}) = \{x^a \mid a \in \mathbb{Z}\}.$$

Define the map
$$f : \mathbb{Z} \longrightarrow gp(\{x\})$$
$$a \longmapsto x^a$$

- f surjective by definition.
- Let $a, b \in \mathbb{Z}$ and $f(a) = f(b)$

$\Rightarrow x^a = x^b$

$b > a \Rightarrow b-a \in \mathbb{N}$ and $x^{(b-a)} = e \Rightarrow x$ finite order
$a > b \Rightarrow a-b \in \mathbb{N}$ and $x^{(a-b)} = e \Rightarrow x$ finite order

$\Big\}$ Contradiction

$\Rightarrow a = b \Rightarrow f$ injective

- Given $a, b \in \mathbb{Z}$ $\quad f(a+b) = x^{(a+b)} = x^a * x^b = f(a) * f(b)$

$\square$

<u>Theorem</u> $x \in G$, $\mathrm{ord}(x) = m \Rightarrow gp(\{x\}) \cong (\mathbb{Z}/m\mathbb{Z}, +)$

In particular $\mathrm{ord}(x) = |gp(\{x\})|$

<u>Proof</u> Let $a, b \in \mathbb{Z}$ and $a \equiv b \bmod m$

$\Rightarrow a = b + qm$ for some $q \in \mathbb{Z}$

$\Rightarrow x^a = x^{(b+qm)} = x^b * (x^m)^q = x^b * e^q = x^b$

$$\Rightarrow \quad f : \mathbb{Z}/m\mathbb{Z} \longrightarrow gp(\{x\}) \quad \text{is well defined}$$
$$[a] \longrightarrow x^a$$

- f surjective by definition
- Let $[a], [b] \in \mathbb{Z}/m\mathbb{Z}$ such that $f([a]) = f([b])$

$\Rightarrow x^a = x^b \Rightarrow x^{(a-b)} = e \Rightarrow \underset{\mathrm{ord}(x)}{m} \mid (a-b) \Rightarrow [a] = [b]$

$\Rightarrow f$ injective

- Given $[a], [b] \in \mathbb{Z}/m\mathbb{Z}$

$f([a] + [b]) = f([a+b]) = x^{(a+b)} = x^a * x^b = f([a]) * f([b])$

$\square$

<u>Corollary</u> G cyclic $\Rightarrow G \cong (\mathbb{Z}, +)$ or $G \cong (\mathbb{Z}/m\mathbb{Z}, +)$ for $m \in \mathbb{N}$.

<u>Proof</u> G cyclic $\Rightarrow \exists\, x \in G$ such that $gp(\{x\}) = G$

$\mathrm{ord}(x) = m \in \mathbb{N} \Rightarrow gp(\{x\}) \cong \mathbb{Z}/m\mathbb{Z} \Rightarrow G \cong \mathbb{Z}/m\mathbb{Z}$

$\mathrm{ord}(x) = \infty \Rightarrow gp(\{x\}) \cong \mathbb{Z} \Rightarrow G \cong \mathbb{Z}$

$\square$

Corollary Let $|G| < \infty$. Given $x \in G$, $\text{ord}(x) < \infty \Rightarrow \text{ord}(x) \mid |G|$

In particular $x^{|G|} = e \quad \forall\, x \in G$.

Proof $\text{ord}(x) = |gp(\{x\})|$, Lagrange $\Rightarrow |gp(\{x\})| \,\Big|\, |G|$

$\Rightarrow \text{ord}(x) \,\Big|\, |G|$ $\square$

Theorem $|G| = p$, a prime $\Rightarrow G \cong (\mathbb{Z}/p\mathbb{Z}, +)$

Up isomorphism there is only one group of prime order!

Proof Let $x \in G$, $x \neq e$.

$\Rightarrow e, x \in gp(\{x\}) \Rightarrow |gp(\{x\})| > 1$

Lagrange $\Rightarrow |gp(\{x\})| \,\Big|\, p \Rightarrow |gp(\{x\})| = p \Rightarrow gp(\{x\}) = G$

$\Rightarrow G \cong (\mathbb{Z}/p\mathbb{Z}, +)$

$\square$

Remarks

cyclic $gp(\{m\})$

$H \subset \mathbb{Z}$ subgroup $\Leftrightarrow H = m\mathbb{Z}$ for some $m \in \mathbb{N}$

Given $k \in \mathbb{N}$ such that $k \mid m$ there is a <u>unique</u> subgroup of $\mathbb{Z}/m\mathbb{Z}$ of order k. Namely $gp([\tfrac{m}{k}]) \subset \mathbb{Z}/m\mathbb{Z}$.

For example, $gp(\{[5]\}) =$ unique subgroup of $\mathbb{Z}/45\mathbb{Z}$ of order 9.

Very special property of finite cyclic groups