Cor. Let $m, n \geq 1$. Then $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z} \iff m, n$ coprime

PF $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic $\iff \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} = \langle ([a], [b]) \rangle$ for some a, b

$\iff \operatorname{ord}([a], [b]) = mn$.

- If $\gcd(m,n) = 1 \Rightarrow \operatorname{ord}([1],[1])$
$= \operatorname{lcm}(m, n)$
$= \frac{mn}{\gcd(m,n)}$
$= mn$

- If $\gcd(m,n) = s \Rightarrow \operatorname{lcm}(m,n) = \frac{mn}{s} < mn$

Note $m \mid \frac{mn}{s}$ and $n \mid \frac{mn}{s}$. Thus $\underbrace{[a] + \cdots + [a]}_{\frac{mn}{s}} = [0]$ in $\mathbb{Z}/m\mathbb{Z}$

and similarly $\underbrace{[b] + \cdots + [b]}_{\frac{mn}{s}} = [0]$ in $\mathbb{Z}/n\mathbb{Z}$.

Thus $\underbrace{([a],[b]) + \cdots + ([a],[b])}_{\frac{mn}{s}} = ([0],[0])$

$\Rightarrow \operatorname{ord}([a],[b]) < mn \quad \forall a, b \in \mathbb{Z}$

Thus $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is not cyclic.

Ex If $n = p_1^{n_1} \cdots p_r^{n_r}$ is a prime factorization, then

$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{n_r}\mathbb{Z}$.

Defn Let G be a group and $S \subseteq G$ a subset. The subgroup generated by S is defined to be the intersection of all subgroups containing S. It's denoted by $\langle S \rangle = gp(S)$.

- Given a collection of subgroups $\{H_i\}$, the intersection
$$\bigcap_i H_i = \{h \in G \mid h \in H_i \forall i\} \text{ is a subgroup of } G.$$
- Here's an equivalent description:
$$\langle S \rangle = \{a_1 \cdots a_n \mid a_i \in S \cup S^{-1} \cup \{e\}\}$$
↑ only finite products ↑ inverse of elements of S

Analogy: Given $v_1, \ldots, v_k$ elements of a vector space,
$\text{span}\{v_1, \ldots, v_k\}$ = intersection of all subspaces containing $v_1, \ldots, v_k$
$= \{\lambda_1 v_1 + \cdots + \lambda_k v_k \mid \lambda_i \in \mathbb{R}\}$.

Ex • $G = (\mathbb{Z}, +)$, $S = \{1\}$.
Then $\langle \{1\} \rangle = \langle 1 \rangle = \mathbb{Z}$.
↑ usually drop brackets for 1 element

- More generally, if G is cyclic, then $G = \langle \{a\} \rangle$ for $a \in G$
- $\mathbb{Z} \times \mathbb{Z} := \mathbb{Z}^2 = \langle \{(0,1), (1,0)\} \rangle$

Defn A group $(G, *)$ is said to be finitely generated if $\exists$ a finite subset $S \subseteq G$ such that $\langle S \rangle = G$.

Ex • Finite groups are finitely generated
- $\mathbb{Z}^n = \langle \{e_1, \ldots, e_n\} \rangle$ is finitely generated
$\mathbb{Z}^n = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n \text{ times}}$

Analogy: "Finitely generated" vector spaces are the finite dimensional ones.

Thm ∃ infinitely many primes in $\mathbb{Z}$.

Cor $(\mathbb{Q}^*, \times)$ is not finitely generated.

PF Assume $S = \{\frac{a_1}{b_1}, \dots, \frac{a_n}{b_n}\}$ is a generating set. Then $m \in \mathbb{Z}$ is of the form $m = \left(\frac{a_1}{b_1}\right)^{r_{11}} \left(\frac{b_1}{a_1}\right)^{r_{12}} \cdots \left(\frac{a_n}{b_n}\right)^{r_{n1}} \left(\frac{b_n}{a_n}\right)^{r_{n2}}$.

$$\Rightarrow b_1^{r_{11}} a_1^{r_{12}} \cdots b_n^{r_{n1}} a_n^{r_{12}} \cdot m = a_1^{r_{11}} b_1^{r_{12}} \cdots a_n^{r_{n1}} b_n^{r_{n2}}.$$

By uniqueness of prime factorization, the prime factors of m must divide $a_1^{r_{11}} b_1^{r_{12}} \cdots a_n^{r_{n1}} b_n^{r_{n2}}$. But the latter product only has finitely many primes dividing it. By the theorem, we may choose m a prime ~~Proof~~ not equal to those primes dividing the product and obtain a contradiction ∎

Big [Fundamental theorem of finitely generated Abelian groups]

Every finitely generated group G is isomorphic to,

$$\mathbb{Z}^n \times \mathbb{Z}/_{p_1^{r_1}\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{p_n^{r_n}\mathbb{Z}}.$$

Here the p_i are prime and not necessarily distinct. Moreover, this is unique up to reordering the product

- Unique up to reordering the product means: $\mathbb{Z}^n \times \mathbb{Z}/_{p\mathbb{Z}} \cong \mathbb{Z}/_{p\mathbb{Z}} \times \mathbb{Z}^n$ etc.
  Exercise: $G \times H \cong H \times G$, for G, H groups.
- The theorem implies that $\mathbb{Z}^m \not\cong \mathbb{Z}^n$ for $n \neq m$.
- The "power" of $\mathbb{Z}$ is unique: If $G \cong \mathbb{Z}^n \times T_1$ and $G \cong \mathbb{Z}^n \times T_2$ where T_1, T_2 are finite abelian groups, then $n = m$. Also, $T_1 \cong T_2$.

"Problem" Given a positive integer n, list all groups of order n.

Of course this is sort of hopeless, because if I relabel the elements of a group, I get a different group of the same size. So a better question would be:

Problem Given a positive integer n, list all non-isomorphic groups of order n.

General Problem Given a property P of a group, classifying all groups satisfying P up to isomorphism means list all non-isomorphic groups satisfying P. We call elements of this list isomorphism classes.

[Notice that $G \cong H$ is an equivalence relation!]

So, if P was the property "Finite abelian group of order n", we can use our classification theorem to solve the problem:

Ex
- $n = 2$: $\mathbb{Z}/2\mathbb{Z}$ is the only isomorphism class
- $n = p$ a prime: $\mathbb{Z}/p\mathbb{Z}$ is the only isomorphism class
- $n = 4$: $\{\mathbb{Z}/2^2\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\}$ the two groups in the set are not isomorphic
- $n = 24 = 2^3 \cdot 3$:

$$\left\{(\mathbb{Z}/2^3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}),\ (\mathbb{Z}/2^2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}),\ (\mathbb{Z}/2\mathbb{Z})^3 \times (\mathbb{Z}/3\mathbb{Z})\right\}$$

No two of these groups are isomorphic!

[This follows from the theorem]