Thm. Every finite abelian group is isomorphic to a direct of the form

$$\mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}},$$

where $p_1, \ldots, p_n$ are not-nec.-distinct primes.

Thm (Cauchy) If G is a finite group and p is a prime which divides $|G|$, then G has an elt. of order p.

Lemma ① If G is a finite abelian p-group with a unique subgroup H of order p, then G is cyclic.

Prop ② If G is a finite abelian p-group and $C \leq G$ is a cyclic subgroup of maximal order, then G is the internal direct product CH, for some subgroup $H \leq G$.

Prop ③ Any finite abelian group is an internal direct product of cyclic subgroups of prime-power order.

(Proof) Given a prime p s.t. $p \mid |G|$, define

$$G_p = \{g \in G \mid |g| = p^k, \text{ for some } k\} \quad ; \quad G_{p'} = \{g \in G \mid p \nmid |g|\}.$$

Claim: These are subgroups, with $G_p \cap G_{p'} = \{e\}$.

We WTS: $G = G_p G_{p'}$.

Given $g \in G$, write $|g| = p^k m$, with $p \nmid m$.

Then $|g^m| = p^k$ and $|g^{p^k}| = m$.

So $g^m \in G_p$ and $g^{p^k} \in G_{p'}$.

$\gcd(p^k, m) = 1 \Rightarrow \exists\ r, s \in \mathbb{Z}$ s.t.

$$r p^k + sm = 1$$

Then $g = g^1 = g^{rp^k + sm} = (g^{p^k})^r (g^m)^s$

$$= (g^m)^s (g^{p^k})^r \in G_p G_{p'}.$$

Repeat this process on $G_{p'}$ until we've written G as an internal direct product of p-groups.

Finally, we'll write any abelian p-group as an internal direct product of cyclic subgroups.

Induct on the order of G_p.

Let $C \leq G_p$ be a cyclic subgroup of maximal order.

Prop (2) $\Rightarrow G_p = CH$. Then H is a p-group with $|H| < |G_p|$.

Inductive hypothesis: H is an I.D.P. of cyclic subgroups. $\therefore$ so is G_p. ∎

Combining Prop (3) with our classification of cyclic groups gives the theorem.

Ex. $G = \mathbb{Z}_3 \times \mathbb{Z}_3$.

$H_1 = \langle (1,0) \rangle$; $K_1 = \langle (0,1) \rangle$

$\rightsquigarrow G = H_1 K_1$

$H_2 = \langle (1,1) \rangle$; $K_2 = \langle (1,2) \rangle$

$\rightsquigarrow G = H_2 K_2$

Uniqueness is only up to isomorphism.

Decomposition by subnormal series

(or finding structure in non-abelian finite groups)

Def. A **subnormal series** of a group G is a finite sequence of nested subgroups

$$\{e\} = H_0 \leq H_1 \leq \cdots \leq H_{n-1} \leq H_n = G,$$

with $H_{i-1} \leq H_i$ a normal subgroup of H_i, $1 \leq i \leq n$.

The **length** of a subnormal series is the number of proper inclusions.

We call $(K_j)_{j=0}^{m}$ a **refinement** of $(H_i)_{i=0}^{n}$ if each H_i appears as some K_j.

Ex

① $\{0\} \overset{①}{\leq} 6\mathbb{Z} \overset{②}{\leq} 6\mathbb{Z} \overset{③}{\leq} 18\mathbb{Z} \leq \mathbb{Z}$ (★)

length = 3

$\{0\} \leq 2\mathbb{Z} \leq 6\mathbb{Z} \leq 18\mathbb{Z} \leq \mathbb{Z}$ is a refinement of (★)

length = 4

$\{0\} \leq 3\mathbb{Z} \leq 9\mathbb{Z} \leq 18\mathbb{Z} \leq \mathbb{Z}$

$\{0\} \leq 3\mathbb{Z} \leq 6\mathbb{Z} \leq 12\mathbb{Z} \leq \mathbb{Z}$

} not refinements of (★) (and no common refinement exists)

② $\{(1)\} \overset{H_0}{\leq} \{(1), (12)(34)\} \overset{H_1}{\leq} \{(1), (12)(34), (13)(24), (14)(23)\} \overset{H_2}{\leq} D_4 \overset{H_3}{}$

is a subnormal series of D_4

Note: H_1 is <u>not</u> a normal subgroup of D_4.

Fine, b/c H_1 is normal in H_2.

Def We call $(H_i)_{i=0}^{n}$ & $(K_j)_{j=0}^{m}$ of a fixed group G **isomorphic** if there is a bijection btwn

$$\left(H_i/H_{i-1}\right)_{i=1}^{n} \quad \& \quad \left(K_j/K_{j-1}\right)_{j=1}^{m}.$$

Ex. $\{0\} \leq 2\mathbb{Z} \leq 6\mathbb{Z} \leq 30\mathbb{Z} \leq \mathbb{Z}$

$\mathbb{Z}_2 \quad \mathbb{Z}_3 \quad \mathbb{Z}_5 \quad \mathbb{Z}_{30}$

$\{0\} \leq 2\mathbb{Z} \leq 10\mathbb{Z} \leq 30\mathbb{Z} \leq \mathbb{Z}$

$\mathbb{Z}_2 \quad \mathbb{Z}_5 \quad \mathbb{Z}_3 \quad \mathbb{Z}_{30}$

NOT composition series

Isomorphic b/c they have the same set of factors.

Idea: Move from H_{i-1} to H_i by "extending by H_i/H_{i-1}." It's these "extension factors" that build us up to G.

Def. A subnormal series $(H_i)_{i=0}^{n}$ is called a **composition series** if each factor H_i/H_{i-1} is simple.

(i.e., a subnormal series which cannot be refined to have greater length)

Fact. Every finite group admits a composition series.

(Idea) If $(H_i)_{i=0}^{n}$ is not a composition series,

then H_i / H_{i-1} is not simple for some $1 \leq i \leq n$.

$\rightsquigarrow \exists\ N \leq H_i$ normal, proper, properly containing H_{i-1}.

$\rightarrow H_0 \leq \cdots \leq H_{i-1} \leq N \leq H_i \leq \cdots \leq H_n$.

Repeat until you get a comp. series. ∎

Exercise. $\mathbb{Z}$ does not admit a composition series.