Last time we were proving:

Thm [The fundamental theorem of finite abelian groups] Every finite abelian group is isomorphic to a direct product 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-necessarily-distinct primes.

Our strategy was:

1. decompose a finite abelian group as an internal direct product of p-groups;
2. decompose a p-group as an internal direct product of cyclic groups.

It remains to prove:

Prop. 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 $H \leq G$.

and to finish the proof of:

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

So far we've shown that $G = G_p G_{p'}$, where $G_p = \{g \in G \mid |g| = p^k\}$ & $G_{p'} = \{g \in G \mid p \nmid |g|\}$.

Prop. 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 $H \leq G$.

(Proof.) We'll proceed by induction. i.e., assume that the result holds for any groups of order smaller than $|G|$.

If G is cyclic, then $C = G$, so G is the I.D.P. of C and $\{e\}$, and we're finished.

If G is not cyclic, then it has at least two distinct subgroups of order p.

(Cauchy's thm $\Rightarrow \exists$ elt of order p
$\exists!$ subgroup of order $p \Rightarrow$ cyclic)

OTOH, C is a cyclic p-group. So C has a unique subgroup of order p.

So G has a subgroup $K \leq G$ of order p not contained in C.

Since $K \cap C \leq K$ & $K \cap C \neq K$, $K \cap C = \{e\}$, so the I.D.P. $CK \leq G$ is defined and $K \trianglelefteq CK$.

By the 2nd I.T., $CK/K \cong C/C \cap K \cong C$.

So CK/K is a cyclic subgroup of G/K.

Recall that the order of gK as an elt. of G/K divides $|g|$, $\forall g \in G$. So $|gK| \leq |g| \leq |C|$.

(We have $|g| \leq |C|$ b/c C is a cyclic subgroup of maximal order.)

Upshot: G/K has no cyclic subgroups of order greater than $|C|$. So CK/K is a cyclic subgroup of G/K of maximal order $|CK/K| = |C|$.

By the inductive hypothesis, $\exists\, H' \leq G/K$ s.t. G/K is the I.D.P. of CK/K & H'. i.e.,

$$G/K = (CK/K)H' \quad \& \quad (CK/K) \cap H' = \{K\}.$$

The correspondence thm provides $K \leq H \leq G$ s.t. $H/K = H'$.

So

$$G/K = (CK/K)(H/K) \quad \text{(b/c } K \leq H\text{)}$$
$$\Rightarrow G = (CK)H = CH.$$

Still need to check that $C \cap H = \{e\}$.

Pick $h \in H \cap C$. Then $hK \in (H/K) \cap (CK/K)$.

So $hK \in H' \cap (CK/K) = \{K\}$.

$\therefore hK = K \Rightarrow h \in K$.

$\therefore H \cap C \subseteq K \cap C = \{e\}$.

So G is the I.D.P. of C & H. ∎

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

So far we've shown that $G = G_p G_{p'}$, where (G_p a p-group)

$G_p = \{g \in G \mid |g| = p^k\}$ & $G_{p'} = \{g \in G \mid p \nmid |g|\}$.

It remains to write G_p as an I.D.P. of cyclic subgroups. Pick a maximal cyclic subgroup $C \leq G_p$. Use previous prop to write $G_p = CH$. Now apply previous prop to H, continue. ∎

Not all finite groups are isomorphic to direct products of cyclic groups. Here's a different way to decompose a group.

Def. A **subnormal series** of (or for) a group G is a finite sequence of nested subgroups

$$\{e\} = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_{n-1} \leq H_n = G$$

s.t. H_{i-1} is normal as a 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.
We call a subnormal series a **composition series** if each quotient H_i/H_{i-1} is simple.

Ex. ① $0 \leq 6\mathbb{Z} \leq 18\mathbb{Z} \leq \mathbb{Z}$ ($\mathbb{Z}$, $\mathbb{Z}_3$, $\mathbb{Z}_{18}$)

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

Neither $0 \leq 3\mathbb{Z} \leq 9\mathbb{Z} \leq 18\mathbb{Z} \leq \mathbb{Z}$ ($\mathbb{Z}_{18}$)

nor $0 \leq 3\mathbb{Z} \leq 6\mathbb{Z} \leq 12\mathbb{Z} \leq \mathbb{Z}$ ($\mathbb{Z}_{12}$) is a refinement.

Are they composition series? No.

② $\langle 0 \rangle \leq \langle 15 \rangle \leq \langle 5 \rangle \leq \mathbb{Z}_{30}$

$\mathbb{Z}_2$ $\mathbb{Z}_3$ $\mathbb{Z}_5$ ← all simple

is a composition series for $\mathbb{Z}_{30}$

Check: So is

$\langle 0 \rangle \leq \langle 15 \rangle \leq \langle 3 \rangle \leq \mathbb{Z}_{30}$.