2.3 The Krull-Schmidt Theorem

Every finitely generated abelian group is a direct sum of finitely many indecomposable abelian groups $\mathbb{Z}$ and $\mathbb{Z}_{p^n}$. We will study a large class of (not necessarily abelian) groups which can be decomposed into a direct product of indecomposable groups.

**Def.** A group $G$ is **indecomposable** if $G \neq \{e\}$ and $G$ is not the direct product of two of its proper subgroups.

Every simple group is indecomposable (e.g. $A_n$ for $n \neq 4$, $\mathbb{Z}_p$ for prime $p$). However indecomposable groups need not be simple (e.g. $\mathbb{Z}$, $\mathbb{Z}_{p^n}$ for $n \geq 2$, and $S_n$)

**Def.** Let $G$ be a group.

- $G$ satisfies the **ascending chain condition (ACC)** if for every chain $G_1 < G_2 < \cdots$ of normal subgroups of $G$ there is an integer $n$ such that $G_i = G_n$ for all $i > n$;
- $G$ satisfies the **descending chain condition (DCC)** if for every chain $G_1 > G_2 > \cdots$ of normal subgroups of $G$ there is an integer $n$ such that $G_i = G_n$ for all $i > n$.

**Ex.** Every finite group satisfies both chain conditions.

**Ex.** (HW) $\mathbb{Z}$ satisfies ACC but not DCC.

**Ex.** (HW) $\mathbb{Z}(p^\infty) = \left\{a/b \in \mathbb{Q}/\mathbb{Z} \mid b = p^n \text{ for some } n \in \mathbb{N}\right\}$ satisfies DCC but not ACC.

**Thm 2.13.** If $G$ satisfies either ACC or DCC, then $G$ is a direct product of a finite number of indecomposable subgroups.

**Proof.** Call a group **good** if it is a direct product of a finite number of indecomposable subgroups; call it **bad** otherwise. Facts:

1. Indecomposable groups are good.
2. If $P = H \times K$ and both $H$ and $K$ are good, then $P$ is good.

Suppose on the contrary, $G$ is bad. Then $G$ is not indecomposable. So $G = H_1 \times K_1$ for some $H_1, K_1 \lhd G$. At least one of $H_1$ and $K_1$ should be bad. Without lost of generality, assume that $K_1$ is bad. Then $K_1 = H_2 \times K_2$ for $H_2, K_2 \lhd K_1$, where at least one of $H_2$ and $K_2$ is bad, say $K_2$ is bad. Repeating the process, we have

$$G = H_1 \times (H_2 \times (H_3 \times \cdots)) \simeq H_1 \times H_2 \times H_3 \times \cdots$$

There are an infinite strictly ascending chain and an infinite strictly descending chain of $G$:

$$H_1 < H_1 \times H_2 < H_1 \times H_2 \times H_3 < \cdots \quad \text{and} \quad G > K_1 > K_2 > \cdots$$

These violate both ACC and DCC. Therefore $G$ is good. \qed
CHAPTER 2. THE STRUCTURE OF GROUPS

Def. An endomorphism \( f \) of a group \( G \) is called a normal endomorphism if \( af(b)a^{-1} = f(aba^{-1}) \) for all \( a, b \in G \).

Lem 2.14.

1. If \( \varphi \) and \( \psi \) are normal endomorphisms of a group \( G \), then so is \( \varphi \circ \psi \).
2. If \( \varphi \) is a normal endomorphism of \( G \) and if \( H \triangleleft G \), then \( \varphi(H) \triangleleft G \).
3. If \( \varphi \) is a normal automorphism of a group \( G \), then \( \varphi^{-1} \) is also normal.

Def. If \( \varphi \) and \( \psi \) are endomorphisms of \( G \), then \( \varphi + \psi : G \to G \) is the function defined by \( x \mapsto \varphi(x)\psi(x) \).

For general group \( G \), \( \varphi + \psi \) is not necessarily commutative on \( + \), and it is not necessarily a homomorphism.

Lem 2.15. Let \( G = H_1 \times \cdots \times H_m \) have projections \( \pi_i : G \to H_i \) and inclusion \( \iota_i : H_i \hookrightarrow G \). Then the sum of any \( k \) distinct \( \iota_i\pi_i \) is a normal endomorphism of \( G \). Moreover, the sum of all the \( \iota_i\pi_i \) is the identity function on \( G \).

Proof. If \( \varphi = \sum_{i=1}^k \iota_i\pi_i \), then \( \varphi(h_1, \cdots, h_m) = h_1 \cdots h_k \), that is, \( \varphi = \iota\pi \), where \( \pi \) is the projection of \( G \) onto the direct factor \( H_1 \times \cdots \times H_k \) and \( \iota \) is the inclusion of \( H_1 \times \cdots \times H_k \) into \( G \). It follows that \( \varphi \) is a normal endomorphism of \( G \) and, if \( k = m \), that \( \varphi = 1_G \).

Lem 2.16. Let \( G \) have both chain conditions. If \( \varphi \) is a normal endomorphism of \( G \), then \( \varphi \) is an injection if and only if it is a surjection. (Thus, either property ensures that \( \varphi \) is an automorphism.)

Proof. Suppose that \( \varphi \) is an injection and that \( g \notin \varphi(G) \). Then \( \varphi^n \) is an injection, and thus \( \varphi^n(g) \notin \varphi^n(\varphi(G)) = \varphi^{n+1}(G) \). There is a strictly descending chain of subgroups

\[ G > \varphi(G) > \varphi^2(G) > \cdots. \]

Now \( \varphi \) normal implies \( \varphi^n \) is normal. By Lemma 2.14, \( \varphi^n(G) \triangleleft G \) for all \( n \), and so the DCC is violated. Therefore, \( \varphi \) is a surjection.

Assume that \( \varphi \) is a surjection. Then \( \varphi^n \) is a surjection for all \( n \). We claim that \( \text{Ker} \varphi = \{e\} \). Otherwise, there is \( x \neq e \) and \( x \in \text{Ker} \varphi \). Write \( x = \varphi^n(g) \) for some \( g \in G \). Then \( g \notin \text{Ker} \varphi^n \) but \( g \in \text{Ker} \varphi^{n+1} \). Thus we have a strictly ascending chain of normal subgroups

\[ \{e\} = \text{Ker} \varphi^0 < \text{Ker} \varphi^1 < \text{Ker} \varphi^2 < \cdots. \]

So the ACC is violated. Thus \( \varphi \) is an injection.
Lem 2.17 (Fitting’s Lemma). Let $G$ have both chain conditions and $\varphi$ a normal endomorphism of $G$. Then $G = \ker \varphi^n \times \operatorname{Im} \varphi^n$ for some $n \geq 1$.

Proof. Since $\varphi$ is normal, we have the following two chains of normal subgroups

$$G \geq \ker \varphi^1 \geq \ker \varphi^2 \geq \cdots \quad \text{and} \quad \{e\} \leq \ker \varphi^1 \leq \ker \varphi^2 \leq \cdots$$

By hypothesis there is an $n$ such that $\operatorname{Im} \varphi^k = \operatorname{Im} \varphi^n$ and $\ker \varphi^k = \ker \varphi^n$ for all $k \geq n$.

Claim: $\ker \varphi^n \cap \operatorname{Im} \varphi^n = \{e\}$. Otherwise, there is $x \neq e$ and $x \in \ker \varphi^n \cap \operatorname{Im} \varphi^n$. Let $x = \varphi^n(g)$. Then $\varphi^{2n}(g) = \varphi^n(x) = e$. So $g \in \ker \varphi^{2n} = \ker \varphi^n$. So $x = \varphi^n(g) = e$, a contradiction. Thus $\ker \varphi^n \cap \operatorname{Im} \varphi^n = \{e\}$.

Given $x \in G$, $\varphi^n(x) = \varphi^{2n}(g)$ by $\operatorname{Im} (\varphi^n) = \operatorname{Im} (\varphi^{2n})$. So $x = k \varphi^n(g)$ for some $k \in \ker \varphi^n$.

This shows that $G = \ker \varphi^n \operatorname{Im} \varphi^n$.

Therefore $G = \ker \varphi^n \times \operatorname{Im} \varphi^n$. \hfill \Box

Def. An endomorphism $\varphi$ of a group $G$ is nilpotent if $\varphi^n(G) = \{e\}$ for some $n$.

Cor 2.18. If $G$ is an indecomposable group having both chain conditions, then every normal endomorphism $\varphi$ of $G$ is either nilpotent or an automorphism.

Proof. There is $n \geq 1$ such that $G = \ker \varphi^n \times \operatorname{Im} \varphi^n$. Then either $\ker \varphi^n = \{e\}$ or $\operatorname{Im} \varphi^n = \{e\}$ since $G$ is indecomposable. If $\ker \varphi^n = \{e\}$, then $\ker \varphi = \{e\}$, and thus $\varphi$ is an injection, and thus $\varphi$ is an automorphism by Lemma 2.16. If $\operatorname{Im} \varphi^n = \{e\}$, then $\varphi$ is nilpotent. \hfill \Box

Lem 2.19. Let $G$ be an indecomposable group with both chain conditions, and let $\varphi$ and $\psi$ be normal nilpotent endomorphisms of $G$. If $\varphi + \psi$ is an endomorphism of $G$, then it is normal nilpotent.

Proof.

$$a(\varphi + \psi)(b)a^{-1} = a\varphi(b)a^{-1} + b\psi(b)a^{-1} = \varphi(aba^{-1}) + \psi(aba^{-1}) = (\varphi + \psi)(aba^{-1}).$$

If $\varphi + \psi$ is an endomorphism, then it is normal. By Lemma 2.18, $\varphi + \psi$ is either nilpotent or an automorphism. If $\varphi + \psi$ is an automorphism, then Lemma 2.14 says that its inverse $\gamma$ is also normal. One has $1_G = (\varphi + \psi)\gamma = \varphi\gamma + \psi\gamma$ where $\varphi\gamma := \varphi \circ \gamma$. Let $\lambda = \varphi\gamma$ and $\mu = \psi\gamma$. Then $1_G = \lambda + \mu$. So $x^{-1} = \lambda(x^{-1})\mu(x^{-1})$ and, taking inverses, $x = \mu(x)\lambda(x)$; that is, $\lambda + \mu = \mu + \lambda$. The equation $\lambda(\lambda + \mu) = (\lambda + \mu)\lambda$ implies that $\lambda\mu = \mu\lambda$. Then for any integer $m > 0$,

$$(\lambda + \mu)^n = \sum_i \binom{m}{i} \lambda^i \mu^{m-i}. \quad (2.2)$$

Nilpotence of $\varphi$ and $\psi$ implies nilpotence of $\lambda = \varphi\gamma$ and $\mu = \psi\gamma$ (they cannot be automorphisms because they have nontrivial kernels); there are $r, s \in \mathbb{Z}^+$ with $\lambda^r = 0$ and $\mu^s = 0$. If $m = r + s - 1$, then (2.2) shows that $1_G = (\lambda + \mu)^m = 0$, forcing $G = \{e\}$. This is a contradiction, for every indecomposable group is nontrivial. \hfill \Box
Cor 2.20. Let $G$ be an indecomposable group having both chain conditions. If $\varphi_1, \ldots, \varphi_n$ is a set of normal nilpotent endomorphisms of $G$ such that every sum of distinct $\varphi$’s is an endomorphism, then $\varphi_1 + \cdots + \varphi_n$ is nilpotent.

Proof. Induction on $n$. □

Thm 2.21 (Krull-Schmidt). Let $G$ be a group having both ACC and DCC. If

$$G = H_1 \times \cdots \times H_s = K_1 \times \cdots \times K_t$$

are two decompositions of $G$ into indecomposable factors, then $s = t$ and there is a reindexing of $K$’s so that $H_i \cong K_i$ for all $i$. Moreover, given any $r$ between 1 and $s$, the reindexing may be chosen so that

$$G = H_1 \times \cdots \times H_r \times K_{r+1} \times \cdots \times K_s.$$

Remark. The last conclusion is stronger than saying that the factors are determined up to isomorphism; one can replace factors of one decomposition by suitable factors from the other.

Proof. We shall give the proof when $r = 1$; the reader may complete the proof for general $r$ by induction. Given the first decomposition, we must find a reindexing of the $K$’s so that $H_i \cong K_i$ for all $i$ and $G = H_1 \times K_2 \times \cdots \times K_t$. Let $\pi_i : G \to H_i$ and $\iota_i : H_i \hookrightarrow G$ be the projection and inclusion from $G = H_1 \times \cdots \times H_s$, and $\pi'_i : G \to K_i$ and $\iota'_i : K_i \hookrightarrow G$ the projection and inclusion from $G = K_1 \times \cdots \times K_t$. The maps $\iota_i \pi_i$ and $\iota'_i \pi'_i$ are normal endomorphisms of $G$.

By Lemma 2.15, every partial sum $\sum \iota'_i \pi'_i$ is a normal endomorphism of $G$. Hence, every partial sum of

$$1_{H_1} = \pi_1 \iota_1 = \pi_1 \circ 1_G \circ \iota_1 = \pi_1(\sum \iota'_i \pi'_i) \iota_1 = \sum \pi_1 \iota'_i \pi'_i \iota_1$$

is a normal endomorphism of $H_1$. Since $1_{H_1}$ is not nilpotent and $H_1$ satisfies both chain conditions (as $G$ does and every normal subgroup of $H_1$ is also normal in $G$), Corollary 2.20 gives an index $j$ with $\pi_1 \iota'_j \pi'_j \iota_1$ an automorphism. We reindex so that $\pi_1 \iota'_i \pi'_i \iota_1$ is an automorphism of $H_1$; let $\gamma$ be its inverse.

We claim that $\pi'_i \iota_1 : H_1 \to K_1$ is an isomorphism. We have $(\gamma \pi_1 \iota'_i)(\pi'_i \iota_1) = 1_{H_1}$. Let us show that $\theta = (\pi'_i \iota_1)(\gamma \pi_1 \iota'_i) = 1_{K_1}$. First, $\theta^2 = \theta$. Second,

$$1_{H_1} = 1_{H_1} \cdot 1_{H_1} = (\gamma \pi_1 \iota'_i)(\pi'_i \iota_1)(\gamma \pi_1 \iota'_i)(\pi'_i \iota_1) = (\gamma \pi_1 \iota'_i)(\theta(\pi'_i \iota_1)),$$

so that $\theta \neq 0$. Were $\theta$ nilpotent, then $\theta^2 = \theta$ forces $\theta = 0$. Therefore, $\theta$ is an automorphism of $K_1$, and so $\theta^2 = \theta$ gives $\theta = 1_{K_1}$. Thus $\pi'_i \iota_1 : H_1 \to K_1$ is an isomorphism.

Now $\pi'_i$ sends $K_2 \times \cdots \times K_t$ into $\{e\}$ while $\pi'_i \iota_1$ restricts to an isomorphism on $H_1$. Therefore $H_1 \cap (K_2 \times \cdots \times K_t) = \{e\}$. Then

$$G^* := \langle H_1, K_2 \times \cdots \times K_t \rangle = H_1 \times K_2 \times \cdots \times K_t.$$
If \( x \in G \), then \( x = k_1 k_2 \cdots k_t \), where \( k_j \in K_j \). Since \( \pi_1' \) is an isomorphism, the map \( \beta : G \to G \), defined by \( x \mapsto \pi_1'(k_1)k_2 \cdots k_t \), is an injection with image \( G^* \). By Lemma 2.16, \( \beta \) is a surjection; that is, \( G = G^* = H_1 \times K_2 \times \cdots \times K_t \). Finally,

\[
K_2 \times \cdots \times K_t \simeq G/H_1 \simeq H_2 \times \cdots H_s,
\]

so that the remaining uniqueness assertions follow by induction on \( \max\{s,t\} \). \( \square \)