Krull-Schmidt theorem

written by Night Shift in Math on Functor Network
original link: https://functor.network/user/854/entry/369

To discuss the Krull-Schmidt theorem, we must first define the ascending chain condition and descending chain condition.

Definition 1. *A group G is said to satisfy the ascending chain condition (ACC) on subgroups iff for every chain $G_1 \leq G_2 \leq \cdots$ of subgroups of G there is an integer n such that $G_i = G_n$ for all $i \geq n$. G is said to satisfy the descending chain condition (DCC) on subgroups iff for every chain $G_1 \geq G_2 \geq \cdots$ of subgroups of G there is an integer n such that $G_i = G_n$ for all $i \geq n$. We say G satisfies ACC on normal subgroups if every increasing sequence of normal subgroups of G eventually becomes constant. Similarly with DCC on normal subgroups.*

Theorem 1. *If a group G satisfies either ACC or DCC on normal subgroups, then G is the direct product of a finite number of indecomposable subgroups.*

Proof. Suppose G is not a finite direct product of indecomposable subgroups. Let S be the set of all normal subgroups H of G such that H is a direct factor of G and H is not a finite direct product of indecomposable subgroups. Clearly $G \in S$. If $H \in S$, then H is not indecomposable, whence there exist proper subgroups K_H and J_H of H such that $H = K_H \times J_H$. Furthermore, one of these groups, say K_H, must lie in S. Let $f : S \to S$ defined by $f(H) = K_H$. There exists a function $\phi : \mathbb{N} \cup \{0\} \to S$ such that $\phi(0) = G$ and $\phi(n+1) = f(\phi(n)) = K_{\phi(n)}$. Denoting $\phi(n)$ by G_n, we have a sequence of normal subgroups $G_0, G_1, G_2, \cdots$ of G such that $G > G_1 > G_2 > \cdots$. If G satisfies the DCC on normal subgroups, this is a contradiction. A routine inductive argument shows $\forall n \in \mathbb{N}$,

$$G = G_n \times J_{G_{n-1}} \times J_{G_{n-2}} \times \cdots \times J_{G_0}$$

with each J_{G_i} a proper subgroup of G. Thus there is a properly ascending chain of normal subgroups:

$$J_{G_0} < J_{G_1} \times J_{G_0} < J_{G_2} \times J_{G_1} \times J_{G_0} < \cdots$$

If G satisfies the ACC on normal subgroups, this is a contradiction. □

While it was easy to prove the existence of such a decomposition, proving that such a decomposition is unique turns out to be much more challenging. Unlike in the existence case, proving uniqueness requires both ACC and DCC on normal subgroups to hold.

Definition 2. *An endomorphism f of a group G is called a normal endomorphism iff $\forall a, b \in G, af(b)a^{-1} = f(aba^{-1})$.*

Lemma 1. *Let G be a group satisfying the ACC (resp. DCC) on normal subgroups and f a normal endomorphism of G. Then f is an automorphism iff f is an epimorphism (resp. monomorphism).*

Proof. Suppose G satisfies the ACC and f is an epimorphism. The ascending chain of normal subgroups

$$\langle e\rangle \leq \ker f \leq \ker f^2 \leq \cdots$$

must eventually become constant, say at n. Since f is an epimorphism, so is f^n. If $a \in G, f(a) = e, a = f^n(b)$ for some $b \in G$ and $e = f(a) = f^{n+1}(b)$. $b \in \ker f^{n+1} = \ker f^n$ so $a = f^n(b) = e$. Thus f is a monomorphism. Next suppose G satisfies the DCC and f is a monomorphism. $\forall k \in \mathbb{N}, \operatorname{im} f^k$ is normal since f is a normal endomorphism. The descending chain of normal subgroups

$$G \geq \operatorname{im} f \geq \operatorname{im} f^2 \geq \cdots$$

must become constant, say at n. $\forall a \in G, f^n(a) = f^{n+1}(b)$ for some $b \in G$. Since f is a monomorphism, so is f^n and hence $f^n(a) = f^n(f(b)), a = f(b)$. Thus f is an epimorphism. □

Lemma 2. *If G is a group that satisfies both the ACC and DCC on normal subgroups and f is a normal endomorphism of G, then for some $n \in \mathbb{N}, G = \ker f^n \times \operatorname{im} f^n$.*

Proof. Consider the two chains of normal subgroups:

$$G \geq \operatorname{im} f \geq \operatorname{im} f^2 \geq \cdots, \quad \langle e\rangle \leq \ker f \leq \ker f^2 \leq \cdots$$

By hypothesis there is an n such that $\operatorname{im} f^k = \operatorname{im} f^n, \ker f^k = \ker f^n$ for all $k \geq n$. Suppose $a \in \ker f^n \cap \operatorname{im} f^n$. Then $a = f^n(b)$ for some $b \in G, f^{2n}(b) = f^n(f^n(b)) = f^n(a) = e$. Thus $b \in \ker f^{2n} = \ker f^n$ so $a = f^n(b) = e$. Thus $\ker f^n \cap \operatorname{im} f^n = \langle e\rangle$. $\forall c \in G, f^n(c) \in \operatorname{im} f^n = \operatorname{im} f^{2n}$ so $f^n(c) = f^{2n}(d)$ for some $d \in G$. $f^n(cf^n(d^{-1})) = f^n(c)f^{2n}(d)^{-1} = e$ thus $cf^n(d^{-1}) \in \ker f^n$. Since $c = cf^n(d^{-1})f^n(d)$, $G = \ker f^n \times \operatorname{im} f^n$. □

Definition 3. *An endomorphism f of a group G is said to be nilpotent iff $\exists n \in \mathbb{N}, \forall g \in G, f^n(g) = e$.*

Corollary 1. *If G is an indecomposable group that satisfies both the ACC and DCC on normal subgroups and f is a normal endomorphism of G, then either f is nilpotent or f is an automorphism.*

Proof. $\exists n \in \mathbb{N}, G = \ker f^n \times \operatorname{im} f^n$. Since G is indecomposable, either $\ker f^n = \langle e\rangle$ or $\operatorname{im} f^n = \langle e\rangle$. The latter implies f is nilpotent. If $\ker f^n = \langle e\rangle$, then $\ker f = \langle e\rangle$ and f is a monomorphism, which implies that f is an automorphism. □

We define some unconventional notation: if G is a group and $f, g : G \to G$ are functions, let $f + g : G \to G$ be defined by $a \mapsto f(a)g(a)$. With $0_G : G \to G$ given by $a \mapsto e$, G^G is a group under $+$.

Corollary 2. *Let $G \neq \langle e\rangle$ be an indecomposable group satisfying both ACC and DCC on normal subgroups. If $f_1, \cdots, f_n$ are normal nilpotent endomorphisms of G such that every $f_{i_1} + \cdots + f_{i_r} (1 \leq i_1 < i_2 < \cdots < i_r \leq n)$ is an endomorphism, then $f_1 + f_2 + \cdots + f_n$ is nilpotent.*

Proof. Since each $f_{i_1} + \cdots + f_{i_r}$ is a normal endomorphism, the proof will follow by induction once the $n = 2$ case is established. If $f_1 + f_2$ is not nilpotent, it is an automorphism. Note that the inverse g of $f_1 + f_2$ is a normal automorphism. If $g_1 = f_1 \circ g, g_2 = f_2 \circ g$, then $\mathrm{id}_G = g_1 + g_2$ and $\forall x \in G, x^{-1} = (g_1 + g_2)(x^{-1}) = g_1(x^{-1})g_2(x^{-1})$. Thus $x = g_2(x)g_1(x) = (g_2 + g_1)(x)$ and $\mathrm{id}_G = g_2 + g_1$. Thus $g_1 + g_2 = g_2 + g_1 = \mathrm{id}_G$ and $g_1 \circ (g_1 + g_2) = (g_1 + g_2) \circ g_1$ implying $g_1 \circ g_2 = g_2 \circ g_1$. An inductive argument shows that $(g_1 + g_2)^m = \sum_{i=0}^{m} \binom{m}{i} g_1^i g_2^{m-i}$. Since each f_i is nilpotent, $g_i = f_i \circ g$ has a nontrivial kernel, whence g_i is nilpotent. For large enough m and all $a \in G$, $(g_1 + g_2)^m(a) = \sum_{i=0}^{m} \binom{m}{i} g_1^i g_2^{m-i}(a) = e$. But this contradicts that $g_1 + g_2 = \mathrm{id}_G$ and $G \neq \langle e \rangle$. □

Theorem 2 (Krull-Schmidt theorem)**.** *Let G be a group that satisfies both ACC and DCC on normal subgroups. If $G = G_1 \times G_2 \times \cdots \times G_s$ and $G = H_1 \times H_2 \times \cdots \times H_t$ with each G_i, H_j indecomposable, then $s = t$ and after reindexing, $G_i \cong H_i$ for every i and for each $r < t$, $G = G_1 \times \cdots \times G_r \times H_{r+1} \times \cdots \times H_t$.*

Proof. Let $P(0)$ be the statement $G = H_1 \times H_2 \times \cdots \times H_t$. For $1 \leq r \leq \min(s,t)$, let $P(r)$ be the statement: there is a reindexing of $H_1, H_2, \cdots, H_t$ such that $G_i \cong H_i$ for $i \in \{1, 2, \cdots, r\}$ and $G = G_1 \times \cdots \times G_r \times H_{r+1} \times \cdots \times H_t$. We shall show inductively that $P(r)$ is true for all r such that $0 \leq r \leq \min(s,t)$. $P(0)$ is true by hypothesis. Assume $P(r-1)$ is true. $G_i \cong H_i$ for all $i \in \{1, 2, \cdots, r-1\}$ and $G = G_1 \times \cdots \times G_{r-1} \times H_r \times \cdots \times H_t$. Let $\pi_1, \cdots, \pi_s$ be the canonical epimorphisms to $G_1, G_2, \cdots, G_s$. Similarly for $\pi'_1, \pi'_2, \cdots, \pi'_t$ to $H_1, H_2, \cdots, H_t$. Let λ_i, λ'_i be the inclusion map sending G_i, H_i to G. Let $\phi_i = \lambda_i \circ \pi_i : G \to G$ and let $\psi_i = \lambda'_i \circ \pi'_i : G \to G$. Verify the following identities:

$$\begin{array}{rll} \phi_i|_{G_i} = \mathrm{id}_{G_i} & \phi_i \circ \phi_i = \phi_i & \phi_i \circ \phi_j = 0_G \text{ for } i \neq j \\ \psi_1 + \psi_2 + \cdots + \psi_t = \mathrm{id}_G & \psi_i \circ \psi_i = \psi_i & \psi_i \circ \psi_j = 0_G \text{ for } i \neq j \\ \mathrm{im}\, \phi_i = G_i & \mathrm{im}\, \psi_i = G_i, i < r & \mathrm{im}\, \psi_i = H_i \text{ for } i \geq r \end{array}$$

Thus $\phi_r \circ \psi_i = 0_G$ for all $i < r$. The identities show that

$$\phi_r = \phi_r \circ \mathrm{id}_G = \phi_r \circ (\psi_1 + \cdots + \psi_t) = \phi_r \circ \psi_r + \phi_r \circ \psi_{r+1} + \cdots + \phi_r \circ \psi_t$$

Every sum of distinct $\phi_r \circ \psi_i$ is a normal endomorphism. Since $\phi_r|_{G_r} = \mathrm{id}_{G_r}$ is a normal automorphism of G_r and G_r satisfies both ACC and DCC on normal subgroups, for some j, $r \leq j \leq t$, $\phi_r \circ \psi_j|_{G_r}$ is an automorphism on G_r. $\forall n \in \mathbb{N}, (\phi_r \circ \psi_j)^{n+1}$ is an automorphism of G_r. Since $G_r \neq \langle e \rangle$ and $(\phi_r \circ \psi_j)^{n+1} = \phi_r(\psi_j \circ \phi_r)^n \psi_j$, $\psi_j \circ \phi_r|_{H_j} : H_j \to H_j$ cannot be nilpotent. Since H_j satisfies both chain conditions, $\psi_j \circ \phi_r|_{H_j}$ must be an automorphism of H_j. Therefore $\psi_j|_{G_r} : G_r \to H_j$ is an isomorphism and so is $\phi_r|_{H_j} : H_j \to G_r$. To see this, note that

$$(\phi_r \circ \psi_j)|_{G_r} = \pi_r \phi_r \psi_j \lambda_r = \pi_r \lambda'_j \pi'_j \lambda_r$$
$$(\psi_j \circ \phi_r)|_{H_j} = \pi'_j \psi_j \phi_r \lambda'_j = \pi'_j \lambda_r \pi_r \lambda'_j$$

$\psi_j|_{G_r} : G_r \to H_j$ is equivalent to $\pi'_j \psi_j \lambda_r = \pi'_j \lambda_r$.
$\phi_r|_{H_j} : H_j \to G_r$ is equivalent to $\pi_r \phi_r \lambda'_j = \pi_r \lambda'_j$. Reindex the H_k so that we

may assume $j = r$ and $G_r \cong H_r$. Since $G = G_1 \times \cdots \times G_{r-1} \times H_r \times \cdots \times H_t$ by the induction hypothesis, $G_1 G_2 \cdots G_{r-1} H_{r+1} \cdots H_t$ is an internal direct product. For $j < t, \psi_r(G_j) = \langle e \rangle$ and for $j > r, \psi_r(H_j) = \langle e \rangle$. Thus

$$\psi_r(G_1 \cdots G_{r-1} H_{r+1} \cdots H_t) = \langle e \rangle$$

Since $\psi_r|_{G_r}$ is an isomorphism, $G_r \cap (G_1 \cdots G_{r-1} H_{r+1} \cdots H_t) = \langle e \rangle$. Thus $G^* = G_1 \cdots G_r H_{r+1} \cdots H_t$ is an internal direct product. Define $\theta : G \to G$ as follows. Every $g \in G$ can be written as $g = g_1 \cdots g_{r-1} h_r \cdots h_t$. Let $\theta(g) = g_1 \cdots g_{r-1} \phi_r(h_r) h_{r+1} \cdots h_t$. Clearly $\operatorname{im} \theta = G^*$. θ is a monomorphism that is normal. Thus θ is an automorphism so $G = \operatorname{im} \theta = G^* = G_1 \times G_2 \times \cdots \times G_r \times H_{r+1} \times \cdots \times H_t$. This proves $P(r)$ and completes the inductive argument. Therefore, after reindexing, $G_1 \cong H_i$ for $0 \leq i \leq \min(s,t)$. If $\min(s,t) = s, G_1 \times \cdots \times G_s = G = G_1 \times \cdots \times G_s \times H_{s+1} \times \cdots \times H_t$ and if $\min(s,t) = t$, $G_1 \times \cdots \times G_s = G = G_1 \times \cdots \times G_t$. Since G_i, H_j are not trivial groups for all i, j, we must have $s = t$ in either case. $\square$