Krull Schmidt Theorem

MTH304 Presentation

Subham Das, (MS20121)

Department of Mathematical Sciences
Indian Institute of Science Education and Research, Mohali

25.11.2022

Primary Question

Previously, we have seen two structure theorems of groups as follows :

Primary Question

Previously, we have seen two structure theorems of groups as follows :

- Structure theorem for finite abelian groups
- The Sylow theorems

Primary Question

Previously, we have seen two structure theorems of groups as follows :

- Structure theorem for finite abelian groups
- The Sylow theorems

If a (not necessarily abelian) group is a direct product of subgroups, each of which cannot be decomposed further, are the factors unique up to isomorphism?

A bit of history

The Krull Schmidt theorem was actually first stated by J.M.H. Wedderburn in 1909, but his proof for the theorem had an error. The first correct proof for finite groups was given by R. Remak in 1911, with a simplification by O.J. Schmidt in 1912. The extension of this theorem to modules was done by W. Krull in 1925.

Indecomposable groups

Definition (Indecomposable groups)

A group G is called **indecomposable** if $G \neq (e)$ and G is not the direct product of any two of its proper subgroups.

Indecomposable groups

Definition (Indecomposable groups)

A group G is called **indecomposable** if $G \neq (e)$ and G is not the direct product of any two of its proper subgroups.

Examples: $\mathbb{Z}, \mathbb{Z}_p$, the symmetric group S_n. By definiton of simple groups, all simple groups are indecomposable

Chain Conditions

Definition (ACC & DCC)

A group G is to said to satisfy the

- **Ascending chain condition (ACC)** on [normal] subgroups if for every chain $G_1 < G_2 < \ldots$ of [normal] subgroups of G there is an integer n such that $G_i = G_n$, for all $i \leq n$
- **Descending chain condition (DCC)** on [normal] subgroups if for every chain $G_1 > G_2 > \ldots$ of [normal] subgroups of G there is an integer n such that $G_i = G_n$, for all $i \leq n$

Chain Conditions

Definition (ACC & DCC)

A group G is to said to satisfy the

- **Ascending chain condition (ACC)** on [normal] subgroups if for every chain $G_1 < G_2 < \dots$ of [normal] subgroups of G there is an integer n such that $G_i = G_n$, for all $i \leq n$
- **Descending chain condition (DCC)** on [normal] subgroups if for every chain $G_1 > G_2 > \dots$ of [normal] subgroups of G there is an integer n such that $G_i = G_n$, for all $i \leq n$

Examples: Every finite group satisfies both chain conditions. $\mathbb{Z}$ satisfies ACC but not DCC, whereas the group $\mathbb{Z}(p^\infty)$ satisfies DCC but not ACC (Check yourself!)

Theorem

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.

Theorem

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 Sketch : Suppose G is not a finite product of indecomposable subgroups. Let S be the set of all normal subgroups H of G such that H is a direct factor ($G = H \times T_H$, for some group T_H of G and H is not a finite direct product of indecomposable subgroups). Clearly $G \in S$. If $H \in S$, the H is clearly not indecomposable, thus there exists proper subgroups $K_H \times J_H$ such that one of them (say K_H) lies in S.

Theorem

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 Sketch : Suppose G is not a finite product of indecomposable subgroups. Let S be the set of all normal subgroups H of G such that H is a direct factor ($G = H \times T_H$, for some group T_H of G and H is not a finite direct product of indecomposable subgroups). Clearly $G \in S$. If $H \in S$, the H is clearly not indecomposable, thus there exists proper subgroups $K_H \times J_H$ such that one of them (say K_H) lies in S. Let $f : S \to S$ be the map $f(H) = K_H$. Next we repeat this process on one of the proper subgroups of K_H. Let's re-index these groups as $K_H, K_{H_1}, K_{H_2} \ldots$ such that each K_{H_i} is normal in G and $G > K_H > K_{H_1} > K_{H_2} > \ldots$. If G satisfies the descending chain condition on normal subgroups, this is a contradiction.

Furthermore an inductive argument shows that for each $n \geq 1$, $G = K_{H_n} \times J_{n-1} \times J_{n-2} \times \cdots \times J_0$ with each J_i, a proper subgroup of G. Hence there is a properly ascending chain of normal subgroups: $J_0 < J_l \times J_0 < J_2 \times J_1 \times J_0 < \times \ldots$ Since G satisfies the ascending chain condition on normal subgroups, this is a contradiction. Hence our theorem is proved $\square$

Furthermore an inductive argument shows that for each $n \geq 1$, $G = K_{H_n} \times J_{n-1} \times J_{n-2} \times \cdots \times J_0$ with each J_i, a proper subgroup of G. Hence there is a properly ascending chain of normal subgroups: $J_0 < J_l \times J_0 < J_2 \times J_1 \times J_0 < \times \ldots$ Since G satisfies the ascending chain condition on normal subgroups, this is a contradiction. Hence our theorem is proved $\square$

Next we shall determine the uniqueness of the decomposition obtained from the above theorem. For that we shall develop some machinery as follows.

A few definitions

We shall introduce a few elementary definitions now:

A few definitions

We shall introduce a few elementary definitions now:

Definition (Endomorphisms)

An **endomorphism** of a group G is a homomorphism $\psi : G \to G$.

A few definitions

We shall introduce a few elementary definitions now:

Definition (Endomorphisms)

An **endomorphism** of a group G is a homomorphism $\psi : G \to G$.

Definition (Projections)

If $G = H_1 \times \cdots \times H_m$ then the maps are $\pi_i : G \to H_i$ defined by $\pi_i(h_1, h_2 \ldots h_m) = h_i$ are called **projections**.

A few definitions

We shall introduce a few elementary definitions now:

Definition (Endomorphisms)

An **endomorphism** of a group G is a homomorphism $\psi : G \to G$.

Definition (Projections)

If $G = H_1 \times \cdots \times H_m$ then the maps are $\pi_i : G \to H_i$ defined by $\pi_i(h_1, h_2 \ldots h_m) = h_i$ are called **projections**.

Definition (Normal maps)

An endomorphism ψ of a group G is **normal** if $\psi(axa^{-1}) = a\psi(x)a^{-1}$ for all $a, x \in G$

Lemma (i)

1. If ψ and ϕ are normal endomorphisms of a group G, then so is $\psi \circ \phi$
2. If ψ is a normal endomorphism of G and H such that $H \trianglerighteq G$, then $\psi(H) \trianglerighteq G$
3. If ψ is a normal automorphism of G then ψ^{-1} is also normal.

Lemma (ii)

Let G be a group that satisfies the ascending [resp. descending] chain condition on normal subgroups and f is a normal endomorphism of G. Then f is an automorphism iff f is a surjective homomorphism [resp. injective homomorphism]

Lemma (ii)

Let G be a group that satisfies the ascending [resp. descending] chain condition on normal subgroups and f is a normal endomorphism of G. Then f is an automorphism iff f is a surjective homomorphism [resp. injective homomorphism]

Proof Sketch : Let G satisfy the ACC and f is an surjective homomorphism. The ascending chain of normal subgroups $(e) < \ker f < \ker f^2 < ...$ (where $f^k = f \dots f$) must become constant, say $\ker f^n = \ker f^{n+1}$. Since f is surjective, so is f^n. If $a \in G, f(a) = e$, then $a = f^n(b)$ for some $b \in G$ and $e = f(a) = f^{n+1}(b)$. Thus $b \in \ker f^{n+1} = \ker f^n$, which implies that $a = f^n(b) = e$. Therefore, f is also injective and hence an automorphism.

Now let G satisfy the DCC and f is an injective homomorphism. For each $k \geq 1$, $\mathrm{Im} f^k$ is normal in G since f is a normal endomorphism. Consequently, the descending chain $G > \mathrm{Im} f > \mathrm{Im} f^2 > \dots$ must become constant, say $\mathrm{Im} f^n = \mathrm{Im} f^{n+1}$. Thus for any $a, b \in G$, $f^{n+1}(b) = f^n(a)$,. Since f is a injective, so is f^n and hence $f^n(a) = f^{n+1}(b) = f(f^n(b))$ implies $a = f(b)$. Therefore f is surjective, and hence an automorphism. □

Fitting's Lemma

If G is a group that satisfies both the ascending and descending chain conditions on normal subgroups and f is a normal endomorphism of G, then for some $n \geq 1, G = \ker f^n \times \mathrm{Im} f^n$

Proof Sketch: Since f is a normal endomorphism each $\mathrm{Im} f^k (k \geq 1)$ is normal in G. Hence we have two chains of normal subgroups: $G > \mathrm{Im} f > \mathrm{Im} f^2 > \ldots$ and $(e) < \ker f < \ker f^2 < \ldots$. By hypothesis there is an n such that $\mathrm{Im} f^k = \mathrm{Im} f^n$ and $\ker f^k = \ker f^n$ for all k $\geq$n. Suppose $a \in \ker f^n \cap \mathrm{Im} f^n$. Then $a = f^n(b)$ for some $b \in G$ and $f^{2n}(b) = f^n(f^n(b)) = f^n(a) = e$. Consequently, $b \in \ker f^{2n} = \ker f^n$ so that $a = f^n(b)(b) = e$. Therefore, $\ker f^n \cap \mathrm{Im} f^n = (e)$.

For any $c \in G, f^n(c) \in \mathrm{Im} f^n = \mathrm{Im} f^{2n}$, whence $f^n(c) = f^{2n}(d)$ for some $d \in G$. Thus $f^n(cf^n(d^{-1})) = f^n(c)f^{2n}(d^{-1}) = f^n(c)f^{2n}(d)^{-1} = f^n(c)f^n(c)^{-1} = e$ and hence $cf^n(d^{-1}) \in \ker f^n$. Since $c = cf^n(d^{-1})f^n(d)$, we conclude that $G = (\ker f^n)(\mathrm{Im} f^n)$. Hence $G = \ker f^n \times \mathrm{Im} f^n$ by the definiton of direct product of normal subgroups. $\square$

For any $c \in G, f^n(c) \in \mathrm{Im} f^n = \mathrm{Im} f^{2n}$, whence $f^n(c) = f^{2n}(d)$ for some $d \in G$. Thus $f^n(cf^n(d^{-1})) = f^n(c)f^{2n}(d^{-1}) = f^n(c)f^{2n}(d)^{-1} = f^n(c)f^n(c)^{-1} = e$ and hence $cf^n(d^{-1}) \in \ker f^n$. Since $c = cf^n(d^{-1})f^n(d)$, we conclude that $G = (\ker f^n)(\mathrm{Im} f^n)$. Hence $G = \ker f^n \times \mathrm{Im} f^n$ by the definiton of direct product of normal subgroups. $\square$

We have the following two important corollaries of the Fitting's Lemma which shall be important ingredients to prove the Krull-Schmidt Theorem.

Definition (Nilpotency)

An endomorphism f of a group G is said to be **nilpotent** if there exists a positive integer n such that $f^n(g) = e$ for all $g \in G$.

Definition (Nilpotency)

An endomorphism f of a group G is said to be **nilpotent** if there exists a positive integer n such that $f^n(g) = e$ for all $g \in G$.

Corollary (i)

If G is an indecomposable group that satisfies both the ascending and descending chain conditions on normal subgroups and f is a normal endomorphism of G, then either f is nilpotent or f is an automorphism.

Definition (Nilpotency)

An endomorphism f of a group G is said to be **nilpotent** if there exists a positive integer n such that $f^n(g) = e$ for all $g \in G$.

Corollary (i)

If G is an indecomposable group that satisfies both the ascending and descending chain conditions on normal subgroups and f is a normal endomorphism of G, then either f is nilpotent or f is an automorphism.

Proof : For some $n \geq 1, G = \ker f^n \times \text{Im}$ by Fitting's Lemma. Since G is indecomposable either $\ker f^n = (e)$ or $\text{Im} f^n = (e)$. The latter implies that f is nilpotent. If $\ker f^n = (e)$, then $\ker f = (e)$ which implies f is injective. Hence, f is an automorphism by Lemma (ii).

Notation

If ψ and ϕ are endomorphisms then $\psi + \phi : G \to G$ is the function defined by $x \mapsto \psi(x)\phi(x)$

Notation

If ψ and ϕ are endomorphisms then $\psi + \phi : G \to G$ is the function defined by $x \mapsto \psi(x)\phi(x)$

Exercise : Show that the sum is not an endomorphism if G is not abelian through a counterexample.

Notation

If ψ and ϕ are endomorphisms then $\psi + \phi : G \to G$ is the function defined by $x \mapsto \psi(x)\phi(x)$

Exercise : Show that the sum is not an endomorphism if G is not abelian through a counterexample.

Corollary (ii)

Let $G \neq < e >$ be an indecomposable group that satisfies both the ascending and descending chain conditions on normal subgroups. If $f_1 ..., f_n$ are normal nilpotent endomorphisms of G such that every $\sum_{k=1}^{r} f_{i_k}$, $(l \leq i_1 < i_2 < \cdots < i_r \ldots n)$ is an endomorphism, then $f_l + f_2 + \cdots + f_n$ is nilpotent.

Main Theorem

Theorem (Krull Schmidt Theorem)

Let G be a group that satisfies both the ascending and descending chain conditions 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 re-indexing $G_i \cong H_i$ for every i and for each $r < t$ we have:

$$G = G_1 \times \cdots \times G_r \times H_{r+1} \times \cdots \times H_i$$

Main Theorem

Theorem (Krull Schmidt Theorem)

Let G be a group that satisfies both the ascending and descending chain conditions 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 re-indexing $G_i \cong H_i$ for every i and for each $r < t$ we have:

$$G = G_1 \times \cdots \times G_r \times H_{r+1} \times \cdots \times H_i$$

Note : G has at least one such decomposition by our previous theorem. The uniqueness statement here is stronger than simply saying that the indecomposable factors are determined up to isomorphism. One can replace factors of one decomposition with suitable factors from the other.

References

[**1**] Algebra, Thomas W.Hungerford

[**2**] An Introduction to Theory of Groups, J. Rotman