Section II.3. The Krull-Schmidt Theorem

Note. In the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem II.2.6), we say that every such group can be written as a finite direct sum of groups of the form $\mathbb{Z}$ and $\mathbb{Z}_{p^n}$ (p prime). The purpose of this section is to extend this idea to some other types of groups.

Note. In Exercise I.8.1, it is shown that the groups $\mathbb{Z}$ and $\mathbb{Z}_{p^n}$ are "indecomposable" in the sense that neither is a direct sum of proper subgroups. We now formally define "indecomposable." Throughout this section we use multiplicative notation. First, we elaborate on some notational details.

Note II.3.A. Hungerford is a bit informal in this section writing "$G = H \times K$" where H and K are subgroups of G. This is consistent with his simplified notation (and Notes I.8.B and Notes I.8.C in Section I.8. Direct Products and Direct Sums), but it cannot be the case since $H \times K$ consists of *pairs* of elements of G. We will be careful in these notes and write "$G = H \times K$" to indicate an external direct product. For internal direct products we write $G = H \times^i K$ (a notation of my own making, so beware of this in your future studies).

Definition. (From Dummit and Foote's *Abstract Algebra*, 3rd Edition, page 180.) If $G = H \times^i K$, then group H is a *complement* of group K in G (and similarly, K is a complement of H in G).

Definition II.3.1. A group G is *indecomposable* if $G \neq \langle e \rangle$ and G is not the internal direct product of two of its proper subgroups.

Note II.3.B. Recall the definition of internal direct product:

> **Definition I.8.8.** Let $\{N_i \mid i \in I\}$ be a family of normal subgroups of a group G such that $G = \langle \cup_{i\in I} N_i \rangle$ and for each $k \in I$ we have $N_k \cap \langle \cup_{i\neq k} N_i \rangle = \langle e \rangle$. Then G is an *internal weak direct product* of the family $\{N_i \mid i \in I\}$ (or the *internal direct sum* if G is additive and abelian).

So if G is decomposable then G must have normal subgroups N_1 and N_2 such that $G = \langle N_1 \cup N_2 \rangle$ and $N_1 \cap N_2 = \{e\}$. Therefore, one way to prove that a group is indecomposable is to prove that any two normal subgroups have an intersection including more than just the identity. This technique can be used in some of the exercises.

Note II.3.C. In Exercise II.3.1, it is shown that G is indecomposable if $G \neq \langle e \rangle$ and $G = H \times^w K$ implies either $K = \langle e \rangle$ or $H = \langle e \rangle$. We also know that if $G = H \times^w K$ then both H and K are proper normal subgroups of G by the definition of internal direct product and indecomposable. So G can be decomposed only if it has a proper normal subgroup. In other words, a group G without a proper normal subgroup is indecomposable. Therefore, all simple groups are indecomposable. However, the converse does not hold. The group $\mathbb{Z}/p^2\mathbb{Z} \cong \mathbb{Z}_{p^2}$, where p is prime, is not simple since it has a subgroup of order p (namely, $\langle \overline{p} \rangle = \{\overline{0}, \overline{p}, \overline{2p}, \ldots, \overline{p^2 - 1}\}$) which is normal since $\mathbb{Z}_{p^2}$ is abelian, but $\mathbb{Z}_{p^2}$ is indecomposable because the only proper subgroups of $\mathbb{Z}_{p^2}$ are of order p by Lagrange's Theorem (Corollary I.4.6) and are cyclic by Theorem I.3.5, and so are isomorphic to $\mathbb{Z}_p$ by Theorem I.3.2, but $\mathbb{Z}_{p^2} \not\cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ (every element of $\mathbb{Z}_p \oplus \mathbb{Z}_p$, except $(\overline{0}, \overline{0})$, generates a group of order p so $\mathbb{Z}_p \oplus \mathbb{Z}_p$ is not cyclic). We therefore have:

Lemma II.3.A. Every nontrivial simple group is indecomposable, but there exist indecomposable groups which are not simple.

Note. In Exercise II.3.2, it is shown that S_n is indecomposable for $n \geq 2$. In Exercise II.3.3, it is shown that $\mathbb{Q}$ is indecomposable.

Note. The Krull-Schmidt Theorem deals with writing certain types of groups as products of indecomposable groups. The "certain type" involves the following condition.

Definition II.3.2. A group G satisfies the *ascending chain condition* (ACC) on [normal] subgroups if every chain $G_1 < G_2 < \cdots$ of [normal] subgroups of G there is $n \in \mathbb{N}$ such that $G_i = G_n$ for all $i > n$. Group G satisfies the *descending chain condition* (DCC) on [normal] subgroups if for every chain $G_1 > G_2 > \ldots$ of [normal] subgroups of G there is $n \in \mathbb{N}$ such that $G_i = G_n$ for all $i > n$.

Example II.3.D. Of course, a finite group must satisfy both the ascending and descending chain conditions. In Exercise II.3.5 you are asked to show that $\mathbb{Z}$ satisfies the ascending chain condition but not the descending chain condition. In Exercise II.3.13 you are asked to show that the Prüfer group satisfies the descending chain condition but not the ascending chain condition.

Note. We only need the ACC and DCC on normal subgroups, though the condition could be considered on any subgroups.

Note II.3.E. The ACC and DCC involve, in some informal sense, a finiteness condition. In particular, every finite group satisfies both the ACC and DCC. In Exercise II.3.5(a), it is shown that $\mathbb{Z}$ satisfies the ACC but not the DCC. As a consequence, a finitely generated abelian group will satisfy the ACC (Exercise II.3.5(b)) but not necessarily the DCC. Further evidence for the finiteness claim is given in the following result.

Theorem II.3.3. If a group G satisfies either the ascending or descending chain condition on normal subgroups, then G is isomorphic to the direct product of a finite number of indecomposable subgroups.

Note II.3.F. Since all finite groups satisfy both the ACC and the DCC, then a corollary to Theorem II.3.3 is that every finite group is isomorphic to the direct product of a finite number of indecomposable subgroups.

Note. The Krull-Schmidt Theorem states that the direct product of indecomposables in Theorem II.3.3 is unique.

Definition. An endomorphism f of a group G (that is, f is a homomorphism mapping $G \to G$) is a *normal endomorphism* if $af(b)a^{-1} = f(aba^{-1})$ for all $a, b \in G$.

Lemma II.3.4. Let G be a group that satisfies the ascending chain condition on normal subgroups and let f be an endomorphism of G. Then f is an automorphism if and only if f is an epimorphism (i.e., an onto homomorphism). Let G be a group that satisfies the descending chain condition on normal subgroups and let f be a normal endomorphism of G. Then f is an automorphism if and only if f is a monomorphism (i.e., a one to one homomorphism).

Note. The following is known as "Fitting's Lemma," named after Hans Fitting (1906–1938; he died at age 31 from a "sudden bone disease," according to Wikipedia). Generalizations exist involving modules over rings.

Lemma II.3.5. (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 $n \geq 1$, we have $G = \mathrm{Ker}(f^n) \times \mathrm{Im}(f^n)$.

Definition. An endomorphism f if a group G is *nilpotent* if there exists a $n \in \mathbb{N}$ such that $f^n(g) = e$ for all $g \in G$.

Corollary II.3.6. 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.

Note II.3.G. The converse of Corollary II.3.6 also holds (as shown in Exercise II.3.A) and so we have a necessary and sufficient condition in terms of normal endomorphisms for a group satisfying both the ACC and DCC to be indecomposable. Namely, a group G which satisfies both the ascending and descending chain conditions on normal subgroups is an indecomposable group if and only if any normal endomorphism f of G is either nilpotent or is an automorphism.

Note. If G is a multiplicative group and f, g are functions from G to G, then $f+g$ denotes the function mapping $G \to G$ defined as $a \mapsto f(a)g(a)$. We can verify that the set of all such functions form a group. If we restrict ourselves to endomorphisms (i.e., homomorphisms mapping $G \to G$), since f and g can be endomorphisms but $f+g$ not an endomorphism (as shown in Exercise II.3.7).

Corollary II.3.7. Let G (where $G \neq \langle e \rangle$) be an indecomposable group that satisfies both the ascending and descending chain conditions on normal subgroups. If $f_1, f_2, \ldots, f_n$ are normal nilpotent epimorphisms of G such that $f_{i_1} + f_{i_2} + \cdots + f_{i_r}$ (where $1 \leq i_1 < i_2 < \cdots < i_r \leq n$) is an epimorphism, then $f_1 + f_2 + \cdots + f_n$ is nilpotent.

Note II.3.H. In the proof of the Krull-Schmidt Theorem, we address the subtle difference between G as an *internal* versus *external* direct product. If G is the internal direct product of subgroups $G_1, G_2, \ldots, G_s$, $G = G_1 \times^i G_2 \times^i \cdots \times^i G_s$, then as shown in the proof of Theorem I.8.6 (and in our Exercise I.8.C(c) for $s = 2$) there is an isomorphism $\varphi : G_1 \times G_2 \times \cdots \times G_s \to G$ given by $(g_1, g_2, \ldots, g_n) \mapsto g_1 g_2 \cdots g_s$. Consequently, every element of G may be written uniquely (the uniqueness is from Theorem I.8.9) as a product $g_1 g_2 \cdots g_s$, where $g_i \in G$ for $1 \leq i \leq s$. For each i, the map $\pi_i : G \to G_i$ given by mapping $g_1 g_2 \cdots g_s \mapsto g_i$ is therefore well-defined and is a homomorphism (and so is an epimorphism; it is onto but not likely one to one). In fact, $\pi_i : G \to G_i$ is the composition of isomorphism $\varphi^{-1} : G \to G_1 \times G_2 \times \cdots \times G_s$ with the canonical projection mapping $G_1 \times G_2 \times \cdots \times G_s \mapsto G_i$.

Definition. With G expressed as an internal direct product of its subgroups, $G = G_1 \times^i G_2 \times^i \cdots \times^i G_s$, the mapping $\pi_i : G \to G_i$ described in the previous note is the *canonical epimorphism associated with the internal direct product.*

Note. In the statement and proof of the Krull-Schmidt Theorem, unlike Hungerford, we notationally distinguish between internal direct products (with "$\times^i$") and external direct products (with "$\times$").

Theorem II.3.8. (The Krull-Schmidt Theorem)
Let G be a group that satisfies both the ascending and descending chain conditions on normal subgroups. If $G = G_1 \times^i G_2 \times^i \cdots \times^i G_s$ and $G = H_1 \times^i H_2 \times^i \cdots \times^i H_t$ with each G_i, H_j indecomposable, then $s = t$ and after reindexing, $G_i \cong H_i$ for every i and for each $r < t$,

$$G = G_1 \times^i G_2 \times^i \cdots \times^i G_r \times^i H_{r+1} \times^i H_{r+2} \times^i \cdots \times^i H_t.$$

Note II.3.I. Since all finite groups satisfy both the ACC and the DCC, then a corollary to Theorem II.3.3 and the Krull-Schmidt Theorem is that every finite group is isomorphic to a unique direct product of a finite number of indecomposable subgroups (up to isomorphism).

Note II.3.J. The Encyclopedia of Math website (accessed 1/5/2024) gives some history of the Krull-Schmidt Theorem (which it calls the "Krull-Remak-Schmidt Theorem"). These ideas are roughly 100 years old. It seems that Robert Remak first proved the result for finite groups "Ueber die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren" *J. Reine Angew. Math.* **139**, 293–308 (1911). Wolfgang Krull proved the result for rings in "Algebraische Theorie der Ringe II" *Math. Ann.* **91**, 1–46 (1924). Otto J. Schmidt enters the scene in 1929 and presents a result involving groups series (we see some group series in Hungerford's Section II.8) in "Ueber unendliche Gruppen mit endlicher Kette" *Math. Z.* **29**, 34–41 (1929). A Google search reveals that a number of generalizations exist involving rings, modules, and categories.

Revised: 1/5/2024