Modern Algebra 2 — Lecture notes
MAT 514/614, Spring 2025 — D. Ivanšić

9 Normal Subgroups and Quotient Groups

We have seen in section 7 that, in general, $aH \neq Ha$ for left and right cosets of a subgroup H in G. The equality of those cosets for all $a \in G$ turns out to be a useful property.

Definition. A subgroup H of a group G is called *normal* if $aH = Ha$ for all $a \in G$. Notation: $H \lhd G$.

Theorem 9.1. A subgroup H of G is normal if and only if $aHa^{-1} \subseteq H$ for all $a \in G$.

Proof.

Example. In an abelian group, every subgrop is normal. The center $Z(G)$ is a normal subgroup in any group G. The trivial group $\{e\}$ and G are normal subgroups of G.

Example. If H has index 2 in G, then H is a normal subgroup of G.

Example. $SL(n, \mathbf{R})$ is a normal subgroup of $GL(n, \mathbf{R})$.

Example. In D_n, the subgroup of rotations is normal. If F is a reflection, $\langle F \rangle$ is not a normal subgroup.

Example. If H and K are subgroups of G, we have seen that the set HK need not be a subgroup. However, if either H or K is normal, then HK is a subgroup of G.

Theorem 9.2. Let H be a normal subgroup of group G. Then the set $G/H = \{aH \mid a \in H\}$ of all left cosets of H in G is a group under the operation $(aH)(bH) = (ab)H$.

The group G/H is called the *quotient group of G by H* and the homomorphism $q : G \to G/H$, $q(g) = gH$ is called the *quotient map*. The same is true for right cosets.

Proof.

Example. Write the table of multiplication for $\mathbf{Z}/4\mathbf{Z}$. What known group is it identical to?

Example. Let $H \leq GL(2, \mathbf{R})$, $H = \left\{ I, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$. Use the matrix $A = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix}$ to show that H is not normal, and then use it again to show that multiplication in $GL(2, \mathbf{R})/H$ is not well defined: let $B = A \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, so $B \in AH$, thus $BH = AH$. If $(AH)(AH) = A^2H$, do we get the same answer for $(BH)(BH) = B^2H$?

Theorem 9.3. Let G be a group. If $G/Z(G)$ is cyclic, then G is abelian (so $G/Z(G) \approx \{e\}$).

Proof.

Note. The more often-used version of this theorem is the contrapositive: if G is not abelian, then $G/Z(G)$ is not cyclic.

Cauchy's Theorem for Abelian Groups 9.5. Let G be a finite abelian group and let p be a prime that divides $|G|$. Then G has an element of order p.

Proof.

Example. Suppose H and K normal subgroups of G, $G = HK$ and $H \cap K = \{e\}$. Then $G \approx H \times K$. (This is a simplified example of the book's discussion on "internal direct product," perhaps an unneccessary concept.)

Theorem 9.7. Let p be a prime. Every group of order p^2 is isomorphic to either $\mathbf{Z}_{p^2}$ or $\mathbf{Z}_p \times \mathbf{Z}_p$. In particular, it is abelian.

Proof.

10 Isomorphism Theorems

Theorem 10.2. Let $\phi : G \to \overline{G}$ be a homomorphism between groups G and $\overline{G}$ and let H be a subgroup of G and $\overline{K}$ a subgroup of $\overline{G}$. Then

4) If H is normal in G, then $\phi(H)$ is normal in $\phi(G)$.
8) If $\overline{K}$ is a normal subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K})$ is a normal subgroup of G. In particular, $\ker\phi$ is normal.

Proof.

First Isomorphism Theorem 10.3. Let $\phi : G \to \overline{G}$ be a homomorphism between groups G and $\overline{G}$. Then the map $\overline{\phi} : G/\ker\phi \to \phi(G)$ given by $g\ker\phi \mapsto \phi(g)$ is an isomorphism, so $G/\ker\phi \approx \phi(G)$.

Proof.

Example. What group is $\mathbf{Z}/n\mathbf{Z}$ isomorphic to?

Example. The set $2\pi\mathbf{Z}$ is a subgroup of $(\mathbf{R}, +)$. What group is $\mathbf{R}/2\pi\mathbf{Z}$ isomorphic to?

Example. Show that $GL(n, \mathbf{R})/SL(n, \mathbf{R}) \approx \mathbf{R}^*$.

Corollary. If $\phi : G \to \overline{G}$ is a homomorphism from a finite group G, then $|\phi(G)|$ divides G.

Theorem 9.4. Recall that an inner automorphism of G induced by $g \in G$ is an automorphism of form $x \mapsto gxg^{-1}$. For every group G, $G/Z(G) \approx \mathrm{Inn}(G)$.

Proof.

Note. The First Isomorphism Theorem can be interpreted this way: Let $\phi : G \to \overline{G}$ be surjective. Then there exists a group $\widetilde{G}$ and homomorphisms $q : G \to \widetilde{G}$ and $\overline{\phi} : \widetilde{G} \to \overline{G}$ such that $\phi = \overline{\phi} \circ q$ and $\overline{\phi}$ is an isomorphism. We also say ϕ factors through an isomorphism, meaning it is a composite of two homomorphisms, one an isomorphism. Pictorially, we say the *diagram commutes.*

Theorem 10.4. Every normal subgroup N of a group G is the kernel of some homomorphism from G, in particular the quotient map $q : G \to G/N$.

Proof.

Second Isomorphism Theorem. Let N, K be subgroups of G, where N is normal in G. Then KN is a subgroup of G, $K \cap N$ is a normal subgroup of K and $K/(K \cap N) \approx KN/N$.

Third Isomorphism Theorem. Let M and N be normal subgroups of G and $N \leq M$. Then M/N is a normal subgroup of G/N and $(G/N)/(M/N) \approx G/M$.

Proof. Homework!

11. Fundamental Theorem of Finite Abelian Groups

Commutativity makes life a lot easier when considering groups, so finite abelian groups can be classified fairly easily.

Definition. A *partition* of a natural number n is a decreasing sequence of natural numbers $j_1, \dots, j_m$ such that $j_1 + \cdots + j_m = n$.

Example. Write all the partitions of the number 3.

Fundamental Theorem of Finite Abelian Groups 11.1. Let G be a finite abelian group, $|G| = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$, where $p_1, \dots, p_k$ are distinct primes. Then

$$G \approx G_{p_1} \times G_{p_2} \times \cdots \times G_{p_k}, \text{ where } |G_{p_i}| = p_i^{n_i}, i = 1, \dots, k$$

and every G_{p_i} has the form

$$G_{p_i} \approx \mathbf{Z}_{p_i^{j_1}} \times \mathbf{Z}_{p_i^{j_2}} \times \mathbf{Z}_{p_i^{j_{m_i}}}, \text{ for some partition } j_1, \dots, j_{m_i} \text{ of } n_i$$

Moreover, two finite abelian groups are isomorphic if and only if their orders have the same prime factorizations, and, in the factorizations above, the partitions corresponding to each of the primes p_i are identical.

Example. According to the theorem, every abelian group of order $125 = 5^3$ is isomorphic to one of $\mathbf{Z}_{5^3}$, $\mathbf{Z}_{5^2} \times \mathbf{Z}_5$ and $\mathbf{Z}_5 \times \mathbf{Z}_5 \times \mathbf{Z}_5$, and no two of those are isomorphic. One says they represent the *isomorphism classes* of abelian groups of order 125.

Example. Find all the isomorphism classes of groups of order $9680 = 2^4 \cdot 5 \cdot 11^2$.

Note. The decomposition into a product can also be done in the following way, which is more in line with how one would algorithmically find the product into which a given abelian group factors:

$$G \approx \mathbf{Z}_{r_1} \times \mathbf{Z}_{r_2} \times \cdots \times \mathbf{Z}_{r_s}, \text{ where } r_i \text{ divides } r_{i-1} \text{ for every } i = 2, \ldots, s$$

In the notation of previous theorem, $r_i = p_1^{s_i} p_2^{t_i} \ldots p_k^{u_i}$, where $s_i, t_i, \ldots, u_i$ are the i-th terms in the partitions of $n_1, n_2, \ldots, n_k$, or 0 if we have already used all the terms.

Example. Write all the isomorphism classes of groups of order 9860 in this way.

Corollary. If m divides the order of a finite abelian group G, then G has a subgroup of order m.

Proof.

The proof of the Fundamental Theorem of Finite Abelian Groups unfolds in several steps.

Lemma 1. If G is finite abelian and $|G| = p^n m$, where p is prime and does not divide m, then

$$G \approx H \times K, \text{ where } H = \{x \in G \mid x^{p^n} = e\}, \; K = \{x \in G \mid x^m = e\}$$

Moreover, $|H| = p^n$.

Proof.

Lemma 2. Let G be finite abelian and $|G| = p^n$, where p is prime, and let a be an element of maximum order in G. Then $G \approx \langle a \rangle \times K$ for some abelian group K in which the maximum order of an element is less than or equal to $|a|$.

Proof.

Corollary 3. Let G be finite abelian and $|G| = p^n$, where p is prime. Then G is a product of cyclic groups.

Proof.

Lemma 4. Let G be finite abelian and $|G| = p^n$, where p is prime. If $G \approx H_1 \times \cdots \times H_m$ and $G \approx K_1 \times \cdots \times K_n$ where H_i and K_i are all cyclic groups with $|H_1| \geq |H_2| \geq \cdots \geq |H_m|$ and $|K_1| \geq |K_2| \geq \cdots \geq |K_n|$, then $m = n$ and $|H_i| = |K_i|$ for all i.

Proof.