MA441: Algebraic Structures I

Lecture 24

3 December 2003

Review from Lecture 23:

Theorem 9.3:
Let G be a group with center $Z(G)$. If $G/Z(G)$ is cyclic, then G is Abelian.

Theorem 9.4:
For any group G, $G/Z(G) \approx \text{Inn}(G)$.

Theorem 9.5: Cauchy's Theorem (Abelian)
Let G be a finite Abelian group and let p be a prime that divides the order of G. Then G has an element of order p.

Internal Direct Products

Notation: for subgroups $H, K < G$,
$HK = \{hk|h \in H, k \in K\}$.

Definition:
We say that G is the **internal direct product** of H and K and write $G = H \times K$
if $H, K \lhd G$ and
$G = HK$ and $H \cap K = \{e\}$.

Definition:
Let $H_1, H_2, \ldots, H_n$ be a finite collection of normal subgroups of G. We say that G is the **internal direct product** of $H_1, H_2, \ldots, H_n$ and write

$$G = H_1 \times H_2 \times \cdots \times H_n$$

if the following two conditions hold:

1. $G = H_1 H_2 \cdots H_n = \{h_1 h_2 \cdots h_n | h_i \in H_i\}$,

2. $(H_1 H_2 \cdots H_i) \cap H_{i+1} = \{e\}$ $(i = 1, \ldots, n-1)$.

Note:
For the internal direct product $H \times K$, both H and K must be normal subgroups of the same group. For the external direct product, H and K can be any groups.

Theorem 9.6
If a group G is the internal direct product of a finite number of subgroups $H_1, H_2, \ldots, H_n$, then G is isomorphic to the external direct product of $H_1, H_2, \ldots, H_n$.

(We skip the proof.)

Chapter 10: Group Homomorphisms

(page 194)

Definition:
A **homomorphism** ϕ from a group G_1 to a group G_2 is a mapping from G_1 to G_2 that preserves the group operation; that is, for all $a, b \in G$,

$$\phi(ab) = \phi(a)\phi(b).$$

The term homomorphism comes from the Greek words “homo” (like) and “morphe” (form).

There is no requirement for a homomorphism to be one-to-one or onto.

Note: A **monomorphism** is a one-to-one homomorphism. An **epimorphism** is an onto homomorphism. And of course, an isomorphism is a homomorphism that is both one-to-one and onto.

An **endomorphism** of a group is a homomorphism from a group to itself. An automorphism is an endomorphism that is also an isomorphism.

Definition:
The **kernel** of a homomorphism $\phi : G_1 \to G_2$ is the set $\{x \in G | \phi(x) = e\}$.

We denote the kernel of ϕ by $\mathrm{Ker}\,\phi$.

Example 1:
The kernel of an isomorphism is the trivial group $\{e\}$.

Example 2:
Let $\mathbb{R}^*$ be the group of nonzero real numbers under multiplication. The determinant mapping $A \mapsto \det A$ is a homomorphism from $\mathrm{GL}(2, \mathbb{R})$ to $\mathbb{R}^*$.

The kernel of the determinant mapping is the special linear group $\mathrm{SL}(2, \mathbb{R})$, consisting of determinant 1 matrices.

Example 4:
Let $\mathbb{R}[x]$ denote the group of all polynomials with real coefficients under addition. For any $f \in \mathbb{R}[x]$, let f' denote the derivative of f. Then the derivative map $f \mapsto f'$ is an endomorphism of $\mathbb{R}[x]$ whose kernel is the set of all constant polynomials.

Example 5:
The mapping ϕ from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ defined by $\phi(m) = r$, where r is the remainder of m divided by n. That is, $\phi(m) = (m \mod n)$. The kernel is $\langle n \rangle$.

Theorem 10.1

Let $\phi : G_1 \to G_2$ be a homomorphism. Let g be in G. Then

1. ϕ sends the identity of G_1 to the identity of G_2.

2. $\phi(g^n) = \phi(g)^n \ (\forall n \in \mathbb{Z})$

3. If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$.

4. $\operatorname{Ker} \phi < G$.

5. If $\phi(g_1) = g_2$, then
$\phi^{-1}(g_2) = \{x \in G_1 | \phi(x) = g_2\} = g_1 \cdot \operatorname{Ker} \phi$.

Proof:
Parts 1 and 2 are the same as we proved before for isomorphisms.

Part 3: $|\phi(g)|$ divides $|g|$.

Let $n = |g|$. Then $\phi(g)^n = \phi(g^n) = e$.

Part 4: $\mathrm{Ker}\,\phi < G$.

We know the kernel is not empty since it contains the identity.

Two-step subgroup test:
For any $a, b \in \mathrm{Ker}\,\phi$, we have $\phi(ab) = \phi(a)\phi(b) = ee = e$, so $ab \in \mathrm{Ker}\,\phi$.
For inverses, we have $e = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) = e\phi(a^{-1})$, so $\phi(a^{-1}) = e$ and $a^{-1} \in \mathrm{Ker}\,\phi$.

Part 5: If $\phi(g_1) = g_2$, then
$\phi^{-1}(g_2) = \{x \in G_1 | \phi(x) = g_2\} = g_1 \cdot \text{Ker}\,\phi$.

We will show containment in both directions.

First, $\phi^{-1}(g_2) \subseteq g_1 \cdot \text{Ker}\,\phi$.

Let $x \in \phi^{-1}(g_2)$, so $\phi(x) = g_2 = \phi(g_1)$. $\phi(g_1^{-1}x) = g_2^{-1}g_2 = e$. Then $g_1^{-1}x \in \text{Ker}\,\phi$, so $x \in g_1 \,\text{Ker}\,\phi$.

Second, $g_1 \cdot \text{Ker}\,\phi \subseteq \phi^{-1}(g_2)$.

Let $x \in g_1 \cdot \text{Ker}\,\phi$, that is, $x = g_1 k$, for some $k \in \text{Ker}\,\phi$. Then $\phi(x) = \phi(g_1 k) = \phi(g_1)\phi(k) = g_2 \cdot e = g_2$, so $x \in \phi^{-1}(g_2)$.

Theorem 10.2:
Let $\phi : G_1 \to G_2$ be a homomorphism and let $H < G_1$. We have the following properties:

1. $\phi(H) = \{\phi(h) | h \in H\}$ is a subgroup of G_2.

2. If H is cyclic, then $\phi(H)$ is cyclic.

3. If H is Abelian, then $\phi(H)$ is Abelian.

4. If $H \lhd G_1$, then $\phi(H) \lhd \phi(G_1)$.

5. If $|\,\text{Ker}\,\phi| = n$, then ϕ is an n-to-one mapping from G_1 onto $\phi(G_1)$.

6. If $|H| = n$, then $|\phi(H)|$ divides n.

7. If $K < G_2$, then $\phi^{-1}(K) < G_1$.

8. If $K \lhd G_2$, then $\phi^{-1}(K) \lhd G_1$.

9. If ϕ is onto and $\text{Ker}\,\phi = \{e\}$, then ϕ is an isomorphism.

Proof:

Parts 1, 2, 3 are similar to what we have proved before for isomorphisms.

Part 4: If $H \lhd G_1$, then $\phi(H) \lhd \phi(G_1)$.

We know $xHx^{-1} \subseteq H$ $(\forall x \in G_1)$.

Any element g in $\phi(G_1)$ has a preimage x, $\phi(x) = g$.

Choose any $\phi(h) \in \phi(H)$. $\phi(x)\phi(h)\phi(x)^{-1} = \phi(xhx^{-1}) = \phi(h') \in \phi(H)$.

So $\phi(H) \lhd \phi(G_1)$.

(We'll skip parts 5, 6.)

Part 7: If $K < G_2$, then $\phi^{-1}(K) < G_1$.

Clearly the identity is in $\phi^{-1}(K)$.

Closure: for any $a, b \in \phi^{-1}(K)$, $\phi(ab) = \phi(a)\phi(b) \in K$, so $ab \in \phi^{-1}(K)$.

Inverses: $\phi(a^{-1}) = \phi(a)^{-1} \in K$.

Part 8: If $K \lhd G_2$, then $\phi^{-1}(K) \lhd G_1$.

Choose any $a \in \phi^{-1}(K)$. For any $x \in G_1$, $\phi(xax^{-1}) = \phi(x)\phi(a)\phi(x)^{-1} \in K$ since $K \lhd G_2$, so $xax^{-1} \in \phi^{-1}(K)$.

(We'll skip part 9.)

Corollary: $\mathrm{Ker}\,\phi \lhd G_1$.

Proof:
Apply part 8 with $K = \{e\} < G_2$.

Theorem 10.3:
The First Isomorphism Theorem
(Jordan, 1870)

Let $\phi : G_1 \to G_2$ be a homomorphism. Then the mapping

$$G_1/(\text{Ker}\,\phi) \to \phi(G_1)$$

given by

$$g_1 \, \text{Ker}\,\phi \mapsto \phi(g_1)$$

is an isomorphism, that is,

$$G_1/(\text{Ker}\,\phi) \approx \phi(G_1).$$