MA441: Algebraic Structures I

Lecture 25

8 December 2003

Review from Lecture 24:

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

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 $H_1, H_2, \ldots, H_n$.

Example: (p. 185) Let $m = n_1 n_2 \cdots n_k$, where the n_i are relatively prime to each other. Previously we saw that

$$U(m) \approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k).$$

This external direct product is also an internal direct product:

$$U(m) \approx U_{m/n_1}(m) \times U_{m/n_2}(m) \times \cdots \times U_{m/n_k}(m).$$

For example,

$$\begin{aligned} U(105) &\approx U(7) \oplus U(15) \\ &= U_{15}(105) \times U_{7}(105) \\ &= \{1, 16, 31, 46, 61, 76\} \times \\ &\quad \{1, 8, 22, 29, 43, 64, 71, 92\} \end{aligned}$$

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 $a, b \in G$,

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

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 $\mathrm{Ker}\,\phi$.

Examples:
The kernel of the determinant map from $\mathrm{GL}(2, \mathbb{R})$ to $\mathbb{R}^*$ is the subgroup of matrices with determinant 1 is $\mathrm{SL}(2, \mathbb{R})$. (This is called the **special linear group**).

The kernel of the derivative map on polynomials is the subgroup of constant polynomials.

Theorem 10.1
Let $\phi : G_1 \to G_2$ be a homomorphism.
Let g be in G_1. Then

1. ϕ sends the identity of G_1 to the identity of G_2.
   A homomorphism preserves identity.

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

3. If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$.
The homomorphic image of an element has an order that divides the order of that element.

4. Ker $\phi < G$.
The kernel of a homomorphism is a subgroup.

5. If $\phi(g_1) = g_2$, then
$\phi^{-1}(g_2) = \{x \in G_1 | \phi(x) = g_2\} = g_1 \cdot \text{Ker}\,\phi$.
The homomorphic preimage of an element is a coset of the kernel.

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.
   The homomorphic image of a subgroup is a subgroup, or
   A homomorphism preserves the property of being a subgroup.

2. If H is cyclic, then $\phi(H)$ is cyclic.
   The homomorphic image of a cyclic group is cyclic, or
   A homomorphism preserves the property of being cyclic.

3. If H is Abelian, then $\phi(H)$ is Abelian. **The homomorphic image of an Abelian group is Abelian, or**
   A homomorphism preserves the property of being Abelian.

4. If $H \lhd G_1$, then $\phi(H) \lhd \phi(G_1)$.
   The homomorphic image of a normal subgroup of a group is normal in the image of that group.

5. If $|\operatorname{Ker}\phi| = n$, then ϕ is an n-to-one mapping from G_1 onto $\phi(G_1)$.
   Every element in the homomorphic image of a group has the same number of preimages as the identity.

6. If $|H| = n$, then $|\phi(H)|$ divides n.
   The homomorphic image of a subgroup has an order that divides the order of that subgroup.

7. If $K < G_2$, then $\phi^{-1}(K) < G_1$.
   The inverse image of a subgroup is a subgroup.

8. If $K \lhd G_2$, then $\phi^{-1}(K) \lhd G_1$.
   The inverse image of a normal subgroup is normal.

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

Let's review the proof of 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 specialized this part to get an important corollary.

Corollary: $\mathrm{Ker}\,\phi \lhd G_1$.
A kernel is a normal subgroup.

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,

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

Proof:
Let ψ denote the correspondence
$g_1 \operatorname{Ker} \phi \mapsto \phi(g_1)$.

We need to prove that this correspondence is a well-defined function, that it is one-to-one, is onto, and preserves the group operation.

Suppose $x \operatorname{Ker} \phi = y \operatorname{Ker} \phi$. We want to show their images are the same, that is, $\phi(x) = \phi(y)$.

From $x \operatorname{Ker} \phi = y \operatorname{Ker} \phi$, we have $y^{-1}x \in \operatorname{Ker} \phi$.

So $\phi(y^{-1}x) = e = \phi(y^{-1})\phi(x) = \phi(y)^{-1}\phi(x)$, which implies $\phi(y) = \phi(x)$.

Next, we show ψ is one-to-one.

Suppose $\phi(x) = \phi(y)$. We will show x and y represent the same coset of the kernel.

From $\phi(x) = \phi(y)$, we have $(\phi(y))^{-1}\phi(x) = e$.

This implies $\phi(y^{-1})\phi(x) = \phi(y^{-1}x) = e$, so $y^{-1}x \in \operatorname{Ker}\phi$, therefore $x \operatorname{Ker}\phi = y \operatorname{Ker}\phi$.

It's clear that ψ is onto, because any element of the image $\phi(G_1)$ equals $\phi(x)$ $(\exists x \in G_1)$ and ψ maps $x \operatorname{Ker} \phi$ to $\phi(x)$.

Finally, we show ψ preserves the group operation.

$\psi(x \operatorname{Ker} \phi \cdot y \operatorname{Ker} \phi) = \psi((xy) \operatorname{Ker} \phi) = \phi(xy)$.

We also have
$\psi(x \operatorname{Ker} \phi \cdot y \operatorname{Ker} \phi) = \psi(x \operatorname{Ker} \phi)\, \psi(y \operatorname{Ker} \phi) = \phi(x)\phi(y)$, which equals $\phi(xy)$.

Example 13:

Consider the map from $\mathbb{Z}$ to $\mathbb{Z}_n$ that reduces the integers modulo n. The kernel of the map is $\langle n \rangle$, and we have

$$\mathbb{Z}/\langle n \rangle \approx \mathbb{Z}_n.$$

Example 14:

Consider the map from $\mathbb{R}$ under addition to the unit circle in $\mathbb{C}$ under multiplication (the circle group) via $x \mapsto \exp(ix) = \cos(x) + i \cdot \sin(x)$.

The kernel of this map is $\langle 2\pi \rangle$, and we have that $\mathbb{R}/\langle 2\pi \rangle$ is isomorphic to the circle group.

Theorem 10.4:
Normal Subgroups are Kernels
Every normal subgroup of a group G is the kernel of a homomorphism of G. In particular, a normal subgroup $N \lhd G$ is the kernel of the mapping $g \mapsto gN$ from G to the quotient group G/N.

Proof:
Let $\gamma : G \to G/N$ be the map $\gamma(g) = gN$.

We call this map the **natural** (or **canonical**) **homomorphism**.

If we can show that this map is in fact a homomorphism and that N is its kernel, then we are done.

The map γ preserves the group operation: $\gamma(xy) = (xy)N = xN \cdot yN = \gamma(x) \cdot \gamma(y)$.

The kernel of γ is exactly N because $\gamma(x) = xN = N$ iff $x \in N$.

From the corollary above, we know that a kernel is a normal subgroup.

Let's define a few more basic concepts. (See pages 89 and 395 and Example 15 on page 203.)

Definition:
Two elements a, b in a group G are **conjugate** in G if for some $x \in G$, $b = xax^{-1}$. We say b is a conjugate of a (and vice-versa).

The **conjugacy class** of a, denoted cl(a) is the set of all conjugates of a, that is,

$$\text{cl}(a) = \{xax^{-1} | x \in G\}.$$

Conjugacy is an equivalence relation, and the conjugacy classes partition a group.

Definition:
The **normalizer** of $H < G$ is denoted $N(H)$ and defined as

$$N(H) = \{x \in G | xHx^{-1} = H\}.$$

Even if H is not normal in G, $H \lhd N(H)$, and the normalizer is the largest subgroup of G that contains H as a normal subgroup.

Definition:
The **centralizer** of $H < G$ is denoted $C(H)$ and defined as

$$C(H) = \{x \in G | xhx^{-1} = h, \forall h \in H\}.$$

The centralizer of H is the subgroup consisting of all elements that commute with elements of H.

Reading Assignment:

Chapter 10

Chapter 11: pages 211–213

Chapter 24: pages 395–400
(Read up through Cauchy's theorem and skip the proofs.)