MA441: Algebraic Structures I

Lecture 23

1 December 2003

Review from Lecture 22:

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

We denote this by $H \lhd G$.

Theorem 9.1: Normal Subgroup Test

A subgroup H of G is normal in G iff $xHx^{-1} \subseteq H$ for all $x \in G$.

Definition:
For $H \lhd G$, the set of left (or right) cosets of H in G is a group called the **quotient group** (or **factor group**) of G by H.

We denote this group by G/H.

Theorem 9.2:
Let $H \lhd G$. The set G/H is a group under the operation $(aH)(bH) = abH$.

Example 11:
Let $G = U(32) = \{1, 3, 5, 7, \ldots, 27, 29, 31\}$.

Let $H = U_{16}(32) = \{1, 17\}$. ($17 \equiv 1 \pmod{16}$)

G/H is abelian of order $16/2 = 8$.

In Chapter 11, we'll learn about the Fundamental Theorem of Abelian Groups. This theorem tells us that an abelian group of order 8 must be isomorphic to Z_8, $Z_4 \oplus Z_2$, or $Z_2 \oplus Z_2 \oplus Z_2$.

Which of these three direct products is isomorphic to G/H?

We will determine the elements of G/H and their orders.

$1H = \{1, 17\}$, $3H = \{3, 19\}$, $5H = \{5, 21\}$
$7H = \{7, 23\}$, $9H = \{9, 25\}$, $11H = \{11, 27\}$
$13H = \{13, 29\}$, $15H = \{15, 31\}$.

We can rule out $Z_2 \oplus Z_2 \oplus Z_2$, because $(3H)^2 = 9H$, so $|3H| \geq 4$.

Now $(7H)^2 = (9H)^2 = H$, so these are two distinct elements with order 2. This rules out Z_8, which has only one element of order 2.

Therefore, $U(32)/U_{16}(32) \approx Z_4 \oplus Z_2$, which is isomorphic to $U(16)$.

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

Proof:
Let $g \in G$ be such that $gZ(G)$ generates $G/Z(G)$.

For any $a, b \in G$, let

$$aZ(G) = (gZ(G))^i = g^i Z(G),$$

and let

$$bZ(G) = (gZ(G))^j = g^j Z(G).$$

Then $a = g^i x$ and $b = g^j y$, $\exists x, y \in Z(G)$.

Since x, y commute with everything, and g^i commutes with g^j, we see that
$ab = (g^i x)(g^j y) = g^{i+j} xy = (g^j y)(g^i x) = ba$.

Since the a, b were arbitrary, we have that G is abelian.

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

Proof:
Define the map $T : G/Z(G) \to \text{Inn}(G)$ via $gZ(G) \mapsto \phi_g$.

(We'll use Gallian's definition of inner automorphism: $\phi_g(x) = gxg^{-1}$.)

We need to show that T is a well-defined function, that is one-to-one, onto, and preserves the group operation.

To show that T is well-defined, suppose $gZ(G) = hZ(G)$. We'll show that both cosets map to the same inner automorphism.

Now $gZ(G) = hZ(G)$ implies $h^{-1}g \in Z(G)$. Then for all $x \in G$, $h^{-1}gx = xh^{-1}g$.

By multiplying on the left by h and on the right by g^{-1}, we have $gxg^{-1} = hxh^{-1}$.

Therefore $\phi_g = \phi_h$.

One-to-one: reverse the argument. $\phi_g = \phi_h$ implies $gZ(G) = hZ(G)$.

Onto: by definition of T. For any ϕ_g, the coset $gZ(G)$ is a preimage under T.

Group operation:
$T(gZ(G) \cdot hZ(G)) = T(ghZ(G)) = \phi_{gh}$.
$T(gZ(G)) \circ T(hZ(G)) = \phi_g \circ \phi_h = \phi_{gh}$.

(Recall: $\phi_g \circ \phi_h(x) = \phi_g(hxh^{-1}) = (gh)x(gh)^{-1}$.)

Example 14:
Consider D_6. The center $Z(D_6) = \{R_0, R_{180}\}$ has order 2. Thus $|D_6/Z(D_6)| = 12/2 = 6$.

By Theorem 7.2 (classification of groups of order $2p$), we know $\text{Inn}(D_6) \approx D_3$ or $\approx Z_6$.

If $\text{Inn}(D_6) \approx Z_6$, then D_6 would have to be abelian.

So $\text{Inn}(D_6)$ must be isomorphic to D_3.

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.

Proof:
Apply strong induction on the order of G.

This is clearly true for the $|G| = 2$.

Assume that the theorem is true for all groups with fewer elements than G. We will show the theorem is true for G.

G has elements of prime order. Choose any $x \in G$. Suppose $|x| = m = qn$, for q prime. Then $|x^n| = q$.

Let x be an element of prime order q.
If $q = p$, then we're done. Otherwise, consider the cyclic subgroup $\langle x \rangle$, which is normal in G since G is abelian.

The factor group $G/\langle x \rangle$ is abelian, and has order $|G|/q$. Since p divides $|G|/q$, we can apply induction to get a $y\langle x \rangle \in G/H$ of order p.

Now apply Exercise 57 to get an element of G 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 $H \cap K = \{e\}$.

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 $H_1, H_2, \ldots, H_n$.

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 $a, b \in G$,

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

Homework Assignment 13

Reading Assignment

Chapter 9: all

Chapter 10: 194–198

Homework Problems:

Chapter 8: 29

Chapter 9: 15, 18, 31, 57, 58

Chapter 10: 1, 2, 3, 4