MA441: Algebraic Structures I

Lecture 22

24 November 2003

Review from Lecture 21:

Theorem 8.2: Criterion for $G \oplus H$ to be Cyclic

Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic iff $|G|$ and $|H|$ are relatively prime.

Corollary 1:
An external direct product $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ is cyclic iff $|G_i|$ and $|G_j|$ are relatively prime for $i \neq j$.

Theorem 8.3: $U(n)$ as an External Direct Product

Suppose s and t are relatively prime. Then $U(st)$ is isomorphic to the external direct product of $U(s)$ and $U(t)$, that is,

$$U(st) \approx U(s) \oplus U(t).$$

Moreover, $U_s(st)$ is isomorphic to $U(t)$ and $U_t(st)$ is isomorphic to $U(s)$.

To prove this, we defined a map

$$U(st) \to U(s) \oplus U(t)$$

that sends

$$x \mapsto (x \text{ mod } s, \, x \text{ mod } t).$$

We found c, d such that $cs \equiv 1 \pmod t$ and $dt \equiv 1 \pmod s$.

For any (a, b), $x = acs + bdt \in U(st)$ maps to (a, b).

Corollary:
Let $m = n_1 \cdot n_2 \cdots n_k$, where gcd$(n_i, n_j) = 1$ for $i \neq j$. Then

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

Chapter 9: Normal Subgroups and Factor Groups

(page 172)

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 $x \in G$.

Proof:
If $H \lhd G$, then for any $x \in G, h \in H$, there is an $h' \in H$ such that $xh = h'x$.

Thus $xhx^{-1} = h' \in H$, so $xHx^{-1} \subseteq H$.

Conversely, suppose $xHx^{-1} \subseteq H$. We want to show that $aH = Ha$ for any $a \in G$.

Letting $x = a$, we have $aHa^{-1} \subseteq H$, so $aH \subseteq Ha$.

By letting $x = a^{-1}$, we have $a^{-1}Ha \subseteq H$, so $Ha \subseteq aH$.

Therefore $aH = Ha$.

Example 1:

Every subgroup of an Abelian group is normal. In fact, $ah = ha$ for any $a \in G$, any $h \in H$.

Example 2:

$Z(G) \lhd G$ by the same reasoning.

Example 3:

$A_n \lhd S_n$. Let β be an odd permutation. Then $\beta A_n = A_n \beta$ are both equal to the coset of all odd permutations. For example,
(12)(123) $\in$ (12)A_3 equals (132)(12) $\in$ A_3(12).

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 $(aH)(bH) = abH$.

Proof:
We must show that

1. the operation is well-defined,

2. G/H is closed under the operation,

3. G/H has an identity,

4. G/H has inverses, and

5. the operation is associative.

We must show that the map from $G/H \times G/H \to G/H$ via $(aH, bH) \mapsto abH$ is a well-defined function.

That is, the image abH is the same no matter how we pick coset representatives for the cosets aH and bH.

Suppose $aH = a'H$ and $bH = b'H$.

Then $a' = ah_1$ and $b' = bh_2$.

$a'b'H = (ah_1)(bh_2)H = (ah_1)bH$ by absorbing h_2.

Since $H \lhd G$, $bH = Hb$.

$(ah_1)bH = (ah_1)Hb = aHb$ by absorbing h_1.

Then again by normality,
$aHb = abH$. So the function is well-defined.

Clearly G/H is closed under the group operation since abH is again a coset of H.

$eH = H$ is the identity.

$a^{-1}H$ is the inverse of aH. Check $(aH)(a^{-1}H) = (a^{-1}H)(aH) = aa^{-1}H = H$

To show associativity, consider a product of three cosets aH, bH, and cH.

$(aHbH)cH = (abH)(cH) = (ab)(HcH) = (ab)(cH) = ((ab)c)H = abcH$.

$aH(bHcH) = aH(bcH) = a(H(bc)H) = a(bc)H = abcH$.

Essentially, we're using normality to bring the elements a, b, c together, and then applying the associativity of the group operation of G.

Example 7:
Let $4\mathbb{Z} = \{0, \pm 4, \pm 8, \ldots\}$.

The cosets are $0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}$.

$\mathbb{Z}/4\mathbb{Z} \approx Z_4$.

More generally, $\mathbb{Z}/n\mathbb{Z} \approx Z_n$.

Note: Let $H \lhd G$.

$|aH|$ could mean the size of the coset aH, the number of elements it contains. It could also mean the order of aH in the quotient group G/H. The meaning should always be clear from context.

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

Then $ab = (g^i x)(g^j y) = g^{i+j} xy = ba$.

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

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.

Homework Assignment 12

Reading Assignment

Chapter 9: all

Homework Problems:

Chapter 8: 14, 15, 22

Chapter 9: 1, 3, 4, 7, 12