MA441: Algebraic Structures I

Lecture 17

3 November 2003

Review from Lecture 16:

Theorem 6.2: Properties of Isomorphisms Acting on Elements

Suppose that $\phi : G_1 \to G_2$ is an isomorphism.

(Part 5)
Then for a fixed integer k and a fixed group element b in G_1, the equation $x^k = b$ has the same number of solutions in G_1 as does the equation $x^k = \phi(b)$ in G_2.

Theorem 6.3: Properties of Isomorphisms Acting on Groups

Suppose that $\phi : G_1 \to G_2$ is an isomorphism. Then the following properties hold.

1. G_1 is Abelian iff G_2 is Abelian.

2. G_1 is cyclic iff G_2 is cyclic.

3. ϕ^{-1} is an isomorphism from G_2 to G_1.

4. If $K \leq G_1$ is a subgroup, then $\phi(K) = \{\phi(k) | k \in K\}$ is a subgroup of G_2.

Definition:
Let G be a group, and let $a \in G$.
The function ϕ_a defined by

$$\phi_a(x) = a^{-1}xa,$$

for all $x \in G$, is called the **inner automorphism** of G **induced by** a.

The set of inner automorphisms is denoted $\mathrm{Inn}(G)$.

Theorem 6.4: $\mathrm{Aut}(G)$ **and** $\mathrm{Inn}(G)$ **are groups**

The set of automorphisms $\mathrm{Aut}(G)$ of a group G and the set of inner automorphisms $\mathrm{Inn}(G)$ of a group are both groups under the operation of function compositions.

Example 13:
$\mathrm{Aut}(\mathbb{Z}/10\mathbb{Z})$ is isomorphic to $U(10)$.

Theorem 6.5: $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \approx U(n)$

For every positive integer n, $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ is isomorphic to $U(n)$.

Proof:
Consider the map $T : \text{Aut}(\mathbb{Z}/n\mathbb{Z}) \to U(n)$ that sends $\alpha \in \text{Aut}(\mathbb{Z}/n\mathbb{Z})$ to $\alpha(1)$.

First we show that T does indeed map $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ to $U(n)$.

Recall from Example 13 that $\alpha(k) = k \cdot \alpha(1)$ by the homomorphism property.

Since α is onto, there is an $m \in \mathbb{Z}/n\mathbb{Z}$ such that $\alpha(m) = 1 \in \mathbb{Z}/n\mathbb{Z}$. Since $\alpha(m) = m \cdot \alpha(1) = 1$, the multiplicative inverse of $\alpha(1)$ is m modulo n. So $\alpha(1) \in U(n)$.

Second, we show that T is one-to-one.

Suppose that $\alpha, \beta \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$.

If $\alpha(1) = \beta(1)$, then

$$\alpha(k) = k \cdot \alpha(1) = k \cdot \beta(1) = \beta(k),$$

for all $k \in \mathbb{Z}/n\mathbb{Z}$, so α and β are the same.

Third, we show that T is onto.

Let $r \in U(n)$ and consider the map
$\alpha : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ via $s \mapsto rs \pmod{n}$.

Exercise 17 shows that α is an automorphism.

Then $T(\alpha) = \alpha(1) = r$ shows that we have a pre-image for r and that T is onto.

The fourth and final property to show is that T preserves the group operation (the homomorphism property).

Let α, β be in Aut$(\mathbb{Z}/n\mathbb{Z})$. Then

$$T(\alpha \circ \beta) = (\alpha \circ \beta)(1) = \alpha(\beta(1)).$$

Now $\alpha(k) = k\alpha(1) = \alpha(1)k$, so

$$\alpha(\beta(1)) = \alpha(1)\beta(1) = T(\alpha)T(\beta).$$

Chapter 7:
Cosets and Lagrange's Theorem

(page 134)

Definition:
Let G be a group and H a subset of G. For any $a \in G$, the set

$$\{ah : h \in H\}$$

is denoted aH. Analogously,

$$Ha = \{ha : h \in H\}.$$

When H is a subgroup of G,
aH is the **left coset of G containing a** and Ha is the **right coset of G containing a**.

We say that a is a coset representative of aH or Ha. We write $|aH|$ and $|Ha|$ to denote the number of elements in the respective sets.

Example 1:
Let $G = S_3$ and $H = \{(1), (13)\}$. Then the left cosets of H in G are

$(1)H = H = (13)H$

$(12)H = \{(12)(1), (12)(13)\} = \{(12), (123)\} = (123)H$

$(23)H = \{(23)(1), (23)(13)\} = \{(23), (132)\} = (132)H$

Example 3:
Let $H = \{0, 3, 6\}$ in $(\mathbb{Z}/9\mathbb{Z}, +)$.

We use $a + H$ as additive notation for cosets.

The cosets of H in $\mathbb{Z}/9\mathbb{Z}$ are

$0 + H = H = \{0, 3, 6\} = 3 + H = 6 + H$

$1 + H = \{1, 4, 7\} = 4 + H = 7 + H$

$2 + H = \{2, 5, 8\} = 5 + H = 8 + H$

Lemma: Properties of Cosets

Let H be a subgroup of G and $a, b \in G$. Then

1. $a \in aH$,

2. $aH = H$ iff $a \in H$,

3. $aH = bH$ or $aH \cap bH = \emptyset$,

4. $aH = bH$ iff $a^{-1}b \in H$,

5. $|aH| = |bH|$,

6. $aH = Ha$ iff $H = aHa^{-1}$,

7. $aH < G$ iff $a \in H$.

Proof:

Part 1: $a = ae \in aH$.

Part 2: Assume $aH = H$. Since $a = ae \in aH$, then $a \in H$. Conversely, assume $a \in H$. Then $aH \subseteq H$ because H is closed under addition. Now $H \subseteq aH$ because for any $h \in H$, we know $a^{-1}h \in H$, so

$$h = eh = (aa^{-1})h = a(a^{-1}h) \in aH.$$

Part 3: Suppose $x \in aH \cap bH$. We wish to show $aH = bH$. Let $x = ah_1 = bh_2$. Then $a = bh_2h_1^{-1}$ and $b = ah_1h_2^{-1}$. Now any $ah \in aH$ can be rewritten as $b(h_2h_1^{-1}h) \in bH$. Conversely, any $bh \in bH$ can be rewritten as $a(h_1h_2^{-1}h) \in aH$.

Part 4: $aH = bH$ iff $H = a^{-1}bH$. Apply property 2.

Part 5: The map that sends $ah \mapsto bh$ is clearly onto. It is one-to-one because of cancellation. If $ah_1 = ah_2$, then $h_1 = h_2$. This shows the sets have the same size.

We'll delay the proof of 6 and 7.

Note that properties 1, 3, and 5 show that the left cosets of a subgroup $H < G$ partition G into blocks of equal size.

Theorem 7.1: Lagrange's Theorem

If G is a finite group and $H < G$ is a subgroup, then $|H|$ divides $|G|$. Moreover, the number of distinct left (or right) cosets of H in G is $|G|/|H|$.

Proof:
Let $a_1H, a_2H, \ldots, a_rH$ denote a complete set of distinct left cosets of H in G.

Since the cosets partition G, we have

$$G = a_1H \cup a_2H \cup \cdots \cup a_rH,$$

and then

$$|G| = |a_1H| + |a_2H| + \cdots + |a_rH|.$$

Since all cosets have the same size, $|G| = r|H|$.

Homework Assignment 9

Reading Assignment:

Chapter 7: 134–144

Homework Problems:

Chapter 6: 12, 14, 15, 17, 19, 20, 23, 24, 29, 32

Chapter 7: 1, 2, 3, 7