MA441: Algebraic Structures I

Lecture 18

5 November 2003

Review from Lecture 17:

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

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

The proof used the map T : Aut$(\mathbb{Z}/n\mathbb{Z}) \to U(n)$
that sends $\alpha \in$ Aut$(\mathbb{Z}/n\mathbb{Z})$ to $\alpha(1)$.

Chapter 7: Cosets and Lagrange's Theorem

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

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

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

(12) and (123) are coset representatives for this coset.

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

(23) and (132) are coset representatives for this coset.

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

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

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

$1, 4, 7$ are coset representatives for this coset.

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

$2, 5, 8$ are coset representatives for this coset.

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: $aH = H$ iff $a \in H$.

Assume $aH = H$. Show $a \in H$.

Since $a = ae \in aH = H$, then $a \in H$.

(Proof of part 2 continued)

Conversely, assume $a \in H$. Show $aH = H$.

First show $aH \subseteq H$.

Since H is closed under the group operation, $aH \subseteq H$.

Next show $H \subseteq aH$.

Since $a \in H$, we have $a^{-1} \in H$.

For any $h \in H$, we know $a^{-1}h \in H$, so

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

which shows $h \in aH$.

Part 3: $aH = bH$ or $aH \cap bH = \emptyset$.

We prove this by assuming the second statement is false and showing that this implies the first statement is true.

Suppose $x \in aH \cap bH$, i.e., $aH \cap bH$ is not empty.

We wish to show $aH = bH$.

Let $x = ah_1 = bh_2$, for some $h_1, h_2 \in H$.

Then $a = bh_2 h_1^{-1}$ and $b = ah_1 h_2^{-1}$.

Then $aH = (bh_2 h_1^{-1})H = b(h_2 h_1^{-1} H)$.

Now $h_2 h_1^{-1} \in H$, so by Part 2, $h_2 h_1^{-1} H = H$.

So $aH = b(h_2 h_1^{-1} H) = bH$.

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

Assume $aH = bH$.

Multiply on the left by a^{-1}.

$aH = bH$ iff $H = a^{-1}bH$.

By Part 2, $H = a^{-1}bH$ iff $a^{-1}b \in H$.

Part 5: $|aH| = |bH|$

We will exhibit a one-to-one and onto map between aH and bH.

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.

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

Property 1 says every element is contained in a coset.

Property 3 says two cosets are identical or disjoint. That means every group element is contained in exactly one coset.

Property 5 says all the cosets are the same size.

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

$aH = Ha$ iff $(aH)a^{-1} = (Ha)a^{-1}$ iff $aHa^{-1} = H$.

We can break this down in greater detail as an exercise.

Let's consider one direction: $aH = Ha$ implies $H = aHa^{-1}$.

(The other direction will be essentially the same reasoning in reverse.)

Suppose $aH = Ha$.

First we prove $H \subseteq aHa^{-1}$.

Choose any $h \in H$. Then there is an $h' \in H$ such that $ah' = ha$. so $h = ah'a^{-1}$.

That proves $H \subseteq aHa^{-1}$.

Next we prove $aHa^{-1} \subseteq H$.

Choose any $aha^{-1} \in aHa^{-1}$, where $h \in H$. Let $g = aha^{-1}$. Then $ga = ah$. Since $aH = Ha$, g must be in H.

That proves $aHa^{-1} \subseteq H$, so $aHa^{-1} = H$.

Part 7: $aH < G$ iff $a \in H$

(That is, $aH = H$.)

Suppose aH is a subgroup of G.

Then aH contains the identity, so $aH = H$ (Part 3), which holds iff $a \in H$ (Part 2).

Conversely, if $a \in H$, then $aH = H < G$ (Part 2).

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, $|G| = r|H|$.

Definition:
The **index** of a subgroup H in G is the number of distinct left cosets of H in G and is denoted $|G : H|$ (or $[G : H]$).

We consider some implications of Lagrange's Theorem.

Corollary 1:
If G is a finite group and $H < G$, then $|G : H| = |G|/|H|$.

In the notation of the theorem, $r = |G : H| = |G|/|H|$.

Corollary 2:
In a finite group, the order of each element divides the order of the group.

For every $a \in G$, $\langle a \rangle < G$, and $|a| = |\langle a \rangle|$.

Corollary 3: Groups of Prime Order are Cyclic

A group of prime order is cyclic.

Proof:
Suppose $a \in G$, $a \neq e$. Then $|a|$ divides $|G|$, which is prime, so $|a| = |G|$. Therefore $\langle a \rangle = G$.

Corollary 4:

Let G be a finite group, and let $a \in G$. Then $a^{|G|} = e$.

Proof:
By Corollary 2, $|a|$ divides $|G|$, say $|G| = |a| \cdot k$.

Then $a^{|G|} = a^{|a|k} = e^k = e$.

Corollary 5: Fermat's Little Theorem

For every integer a and every prime p,
$a^p \equiv a \pmod{p}$.

Proof:
Consider $U(p)$. Let $a \equiv r \pmod{p}$,
where $0 \leq r < p$.

The order of $U(p)$ is $p-1$. So by Corollary 4,
$a^{p-1} = r^{p-1} = e$ in $U(p)$. Multiply by a to get
$a^p \equiv a \pmod{p}$.

Note that the converse to Lagrange's Theorem is false.

(The converse is true for cyclic groups.)

Theorem 7.2: Classification of Groups of Order $2p$

Let G be a group of order $2p$, where p is a prime greater than 2. Then G is isomorphic to either $\mathbb{Z}/2p\mathbb{Z}$ or D_p.