MA441: Algebraic Structures I

Lecture 19

10 November 2003

Review from Lecture 18:

We proved several properties of cosets of $H < G$ from the Lemma, including

- Every element is contained in a coset,
- Two cosets are either disjoint or identical,
- Two cosets with representatives a and b are the same iff $a^{-1}b \in H$ (or $b^{-1}a \in H$),
- Any two cosets have the same size,
- The only coset of H that is actually a subgroup of G is H itself.

We learned that the cosets of H partition G.

This fact is the basis for one of the most important theorems in the theory of finite groups, Lagrange's Theorem.

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 $|G|/|H|$.

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,

$$|G| = |a_1 H| + |a_2 H| + \cdots + |a_r H|.$$

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

Therefore,

$$r = |G : H| = |G|/|H|.$$

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

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

Corollary 3:

A group of prime order is cyclic.

Proof:
Suppose $a \in G$, $a \neq e$. Then $|a|$ divides $|G|$.

Since $|G|$ is prime, its only divisors are 1 and $|G|$. But $|a| \neq 1$ since a is not the identity. So $|a| = |G|$ and $\langle a \rangle = G$.

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 $a^{|G|} = a^{|a| \cdot k} = e^k = e$.

Corollary 5 is really a corollary of Corollary 4, with $G = U(p)$, for p prime.

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 $a^p \equiv a \pmod{p}$.

Example/Application:

Is $n = 2^{257} - 1$ prime?

$2^{n-1} \equiv 1 \pmod{n}$.

Does this mean n is prime?

$$10^{n-1} \equiv \underbrace{4122...5616}_{\text{77 digits}} \pmod{n}.$$

If n were prime, then this would have to be 1.

So n is composite.

Consider the following two statements:

1) G has a subgroup H of order d.

and

2) d divides n.

Lagrange's Theorem says 1) implies 2). However, the converse is not necessarily true.

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.

Proof:

If G has an element of order $2p$, then G must be cyclic of order $2p$.

Let us assume that G does not have an element of order $2p$. We will show $G \approx D_p$.

By Lagrange's Theorem, the order of every element divides the order of G, so any non-identity element has order either 2 or p.

We will show there is an element of order p.

By way of contradiction, assume all non-identity elements have order 2.

This allows us to show that there is a subgroup of order 4, which does not divide the order of G, and gives a contradiction.

Let a be an element of order p.

Consider the cosets of $\langle a \rangle < G$.

Choose $b \notin \langle a \rangle$.

Then G is the disjoint union of $\langle a \rangle$ and $b\langle a \rangle$.

(Are there any other cosets?)

Claim: $|b| = 2$.

Consider $b^2\langle a \rangle$.

This must be either $\langle a \rangle$ or $b\langle a \rangle$.

It can't be $b\langle a \rangle$, so $b^2\langle a \rangle = \langle a \rangle$.

Thus $b^2 \in \langle a \rangle$.

What does Lagrange's Theorem say about the order of b^2?

The order of b^2 must be either 1 or p.

The order of b^2 can not be p, because then $|b| = 2p$.

Thus any element not in $\langle a \rangle$ has order 2.

Compare this to the dihedral group, where a is the rotation R.

What are the elements not in $\langle R \rangle$?

Consider ab. Can ab be in $\langle a \rangle$?

The order of ab is 2.

$ab = (ab)^{-1} = b^{-1}a^{-1} = ba^{-1}$.

In the geometric representation, this would be $RF = FR^{-1}$.

This relation is enough to determine the group structure, because with $|a| = p$, $|b| = 2$, and $ab = ba^{-1}$, we can complete the multiplication table for the group.

(See Gallian, page 140, for further discussion.)

Definition: Stabilizer of a Point

Let G be a group of permutations of a set S. For each i in S, let

$$\mathrm{Stab}_G(i) = \{\phi \in G : \phi(i) = i\},$$

(or alternatively,

$$\mathrm{Stab}_G(i) = \{a \in G : ia = i\},$$

where $ia = i \cdot a$ denotes the action of a on i on the right.)

We call $\mathrm{Stab}_G(i)$ the **stabilizer of i in G**.

We have alrady verified that the stabilizer of a point is a subgroup (Exercise 5.31).

Definition: The Orbit of a Point

Let G be a group of permutations of a set S. For each $i \in S$, let

$$\mathrm{Orb}_G(s) = \{\phi(s) : \phi \in G\},$$

(or alternatively,

$$\mathrm{Orb}_G(s) = \{sa : a \in G\},$$

where $sa = s \cdot a$ denotes the action of a on s on the right.)

The set $\mathrm{Orb}_G(s)$ is a subset of S called the **orbit of s under G**.

We write $|\,\mathrm{Orb}_G(s)|$ for the number of elements in $\mathrm{Orb}_G(s)$.

Theorem 7.3: Orbit-Stabilizer Theorem

Let G be a finite group of permutations of a set S. Then for any i in S,

$$|G| = |\,\mathsf{Stab}_G(i)| \cdot |\,\mathsf{Orb}_G(i)|.$$

Homework Assignment 10

Reading Assignment:

Chapter 7

Chapter 8: pages 150–153

Homework Problems:

Chapter 6: 35, 36, 40

Chapter 7: 4, 7, 8, 10, 15, 16, 17, 22

Chapter 8: 1