MA441: Algebraic Structures I

Lecture 20

12 November 2003

Review from Lecture 19:

We proved five corollaries of Lagrange's Theorem.

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

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

Corollary 3:

A group of prime order is cyclic.

Corollary 4:

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

Corollary 5: Fermat's Little Theorem

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

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.

The proof relied on considering

- whether there was an element of order $2p$ or not,
- whether all (non-identity) elements had order 2 or whether there was an element a of order p,
- analyzing the cosets of the cyclic subgroup of order p and finding an element b of order 2, and
- proving the relation $ab = b^{-1}a$.

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,

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

The idea of the proof is to show that $|G : \mathsf{Stab}_G(i)| = |G|/|\,\mathsf{Stab}_G(i)|$ equals $|\,\mathsf{Orb}_G(i)|$ by showing there is a bijection between the left cosets of $\mathsf{Stab}_G(i) < G$ and $\mathsf{Orb}_G(i)$.

Let $H = \text{Stab}_G(i)$.

For any $\phi \in G$, let T be the correspondence that sends cosets of H to the orbit $\text{Orb}_G(i)$ via $\phi H \mapsto \phi(i)$.

First, we show that T is well-defined, that is, the image of a coset under T does not depend on which representative we choose.

Suppose $\alpha H = \beta H$. Then $\alpha^{-1}\beta \in H$. So $\alpha^{-1}\beta(i) = i$ and thus $\alpha(i) = \beta(i)$.

Second, we show that T is one-to-one. If $\alpha(i) = \beta(i)$, then by reversing the steps, we see $\alpha H = \beta H$.

Third, we show that T is onto. If $j \in \text{Orb}_G(i)$, then there is some ϕ such that $j = \alpha(i)$. Then $\alpha H \mapsto j$ under T.

Since T is a bijection, $|G : H| = |\,\text{Orb}_G(i)|$, which proves the theorem.

Chapter 8:
External Direct Products

(page 150)

Definition:
Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The **external direct product** of these groups, written as

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n,$$

is the set of all n-tuples for which the i-th component is an element of G_i and the group operation on the set of n-tuples is the componentwise operation, where i-th components are composed in the group G_i.

In symbols,

$$G_1 \oplus \cdots \oplus G_n = \{(g_1, \ldots, g_n) : g_i \in G_i\}$$

where the composition law is

$$(g_1, \ldots, g_n) \cdot (g_1', \ldots, g_n') = (g_1 g_1', \ldots, g_n g_n').$$

The composition $g_i g_i'$ is formed according to the group operation of G_i.

Let e_i denote the identity element of G_i.

The identity of $G_1 \oplus \cdots \oplus G_n$ is $(e_1, \ldots, e_n)$, which we shorten to $(e, \ldots, e)$.

The inverse of $(g_1, \ldots, g_n)$ is $(g_1^{-1}, \ldots, g_n^{-1})$.

Theorem:
The external direct product $G_1 \oplus \cdots \oplus G_n$ is a group.

Proof:
(Exercise 8.1)

Example:
The two-dimensional vector space over the reals, $\mathbb{R}^2$, taken as an additive group, is the external direct product of two copies of $\mathbb{R}$. We write

$$\mathbb{R}^2 = \mathbb{R} \oplus \mathbb{R}.$$

The group operation is componentwise addition.

Example 1: $U(8) \oplus U(10)$

$U(8) \oplus U(10) = \{(1,1), (1,3), (1,7), (1,9), (3,1), \ldots$
$\ldots, (7,7), (7,9)\}$

$(3,7)(7,9) = (5,3)$

Theorem 8.1: Order of an element in a Direct Product

The order of an element in a direct product of a finite number of finite groups is the least common multiple (LCM) of the orders of the components of the element. In symbols,

$$|(g_1, g_2, \ldots, g_n)| = \text{lcm}(|g_1|, |g_2|, \ldots, |g_n|)\}.$$

Compare this to the result by Ruffini (Theorem 5.3) that the order of a permutation written in disjoint cycle notation is the LCM of the cycle lengths.

Proof:

We treat only the case $n = 2$. The general case can be done by induction. (Exercise 8.2)

Let (g_1, g_2) be an arbitrary element of $G_1 \oplus G_2$.

Let

$$s = \text{lcm}(|g_1|, |g_2|)$$

and

$$t = |(g_1, g_2)|.$$

We will show that s and t divide each other.

We know that t divides s, because

$$(g_1, g_2)^s = (g_1^s, g_2^s) = (e, e).$$

Conversely,

$$(g_1, g_2)^t = (e, e) = (g_1^t, g_2^t),$$

so $|g_1|$ and $|g_2|$ divide t, meaning s divides t.

Therefore $s = t$.