MA441: Algebraic Structures I

Lecture 21

17 November 2003

Review from Lecture 20:

Let G be a group of permutations of a set S.

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

We defined $\mathrm{Orb}_G(s)$, the **orbit of s under G**.

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 was to consider the correspondence that maps cosets of $\mathsf{Stab}_G(i)$ to the orbit $\mathsf{Orb}_G(i)$ via $\phi\,\mathsf{Stab}_G(i) \mapsto \phi(i)$.

We defined the **external direct product**

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

to be 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.

The external direct product of groups is a group.

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,

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

Example 3:
We count the number of elements in $\mathbb{Z}/25\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ of order 5.

We want to find elements of the form (a, b) with $a \in \mathbb{Z}/25\mathbb{Z}$ and $b \in \mathbb{Z}/5\mathbb{Z}$ such that $\text{lcm}(|a|, |b|) = 5$.

Question: how many elements of order 5 are there in $\mathbb{Z}/25\mathbb{Z}$?

There are 4 elements of order 5 ($\phi(5) = 4$).

Case 1: $|a| = |b| = 5$
There are 4 choices for a and 4 choices for b, total 16.

Case 2: $|a| = 5, |b| = 1$
There are 4 choices for a, and $b = 0$, total 4.

Case 3: $|a| = 1, |b| = 5$
There are 4 choices for b, and $a = 0$, total 4.

Grand total: 24 elements of order 5.

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.

Proof:
Let $|G| = m$ and $|H| = n$, so $|G \oplus H| = mn$.

Assume $G \oplus H$ is cyclic. Show the orders are relatively prime.

Let $d = \text{gcd}(m, n)$ and let (g, h) be a generator for $G \oplus H$. $|(g, h)| = mn$.

Consider $(g,h)^{mn/d} = ((g^m)^{n/d}, (h^n)^{m/d}) = (e,e)$.

Then $mn = |(g,h)| \leq mn/d$, so $d = 1$.

Conversely, suppose m and n are relatively prime. We'll show $G \oplus H$ is cyclic.

Choose generators g for G and h for H. That is, $G = \langle g \rangle$ and $H = \langle h \rangle$.

Since $\gcd(m,n) = 1$, $\text{lcm}(m,n) = mn$. Then by Theorem 8.1,

$$|(g,h)| = \text{lcm}(m,n) = mn = |G \oplus H|,$$

so $G \oplus H$ is cyclic.

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 $i \neq j$.

Proof:
By induction, using Theorem 8.2.

Corollary 2:
Let $m = n_1 \cdot n_2 \cdots n_k$. Then

$$\mathbb{Z}/m\mathbb{Z} \approx \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}$$

iff n_i and n_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 $U(s)$.

Recall that $U_k(n)$ is the subgroup of $U(n)$ consisting of elements congruent to 1 modulo k.

Proof:

Consider the map $U(st) \to U(s) \oplus U(t)$ that sends $x \mapsto (x \bmod s, x \bmod t)$.

Let us verify that this map is an isomorphism.

Well-defined: If x is relatively prime to st, then it is relatively prime to both s and t.

We can choose c, d such that $cs \equiv 1 \pmod{t}$ and $dt \equiv 1 \pmod{s}$.

Onto: For any (a, b), let $x = acs + bdt$.

Then $x \bmod t = acs = a$ and
$x \bmod s = bdt = b$.

(This is a special case of the
Chinese Remainder Theorem.)

One-to-one: suppose x and y both map to (a, b). Then xy^{-1} maps to $(1, 1)$.

So $xy^{-1} \equiv 1 \pmod{s}$ and $xy^{-1} \equiv 1 \pmod{t}$.

That means $xy^{-1} - 1$ is divisible by s and t, so it must be 1. So $x = y$.

The homomorphism property is clear:

$(xy \bmod s, xy \bmod t) =$
$(x \bmod s, y \bmod s) \cdot (x \bmod t, y \bmod t)$.

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

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

Example:
$U(105) \approx U(7) \oplus U(15)$
$U(105) \approx U(21) \oplus U(5)$
$U(105) \approx U(3) \oplus U(5) \oplus U(7)$

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 $H \triangleleft G$.

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 $aH = Ha$.

Homework Assignment 11

Reading Assignment

Chapter 8

Chapter 9: 172–174

Homework Problems:

Chapter 8: 2, 4, 5, 10

Chapter 9: 1, 3