MA441: Algebraic Structures I

Lecture 11

13 October 2003

Review from Lecture 10:

Permutations:

- Cycle notation
- Composition
- Inversion

Theorem 4.4:
If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.

Corollary:
In a finite group the number of elements of order d is divisible by $\phi(d)$.

The Lattice of Subgrooups

We can represent all subgroups of a group by a diagram that shows how the subgroups are contained in each other.

Given a group G, we begin by writing G at the top of the diagram and $\langle e \rangle$ at the bottom. Given two subgroups $H, K < G$, if $H < K$, then we write H below K and connect them.

If you know some graph theory, this lattice is a directed acyclic graph.

There is no unique way to write this graph on a sheet of paper. What is important are the containment relationships that it encodes.

Examples: $\mathbb{Z}/30\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $U(8)$

Subgroup lattices are a helpful way to visualize the structure of groups.

Chapter 5: Permutation Groups

Definition:
A **permutation** of a set A is a function from A to A that is both one-to-one and onto. A **permutation group of a set** A is a set of permutations of A that forms a group under function composition.

We will consider only permutations of finite sets.

Definition:
Let $A = \{1, 2, \ldots, n\}$. The set of all permutations of A is called the **symmetric group of degree** n (or the symmetric group on n letters) and is denoted S_n.

There are $n!$ elements of S_n, i.e., $|S_n| = n!$.

We can count the permutations on n letters by counting the possible images of each letter. The first letter can be mapped to any letter, so there are n possibilities. The second letter can be mapped to any letter except for the image of the first, so there are $n-1$ possibilities. We can continue this until we are down to the last letter, which has only one place left where it can be mapped to. So the number of possible permutations is

$$n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 2 \cdot 1 = n!$$

Theorem 5.1: Products of Disjoint Cycles

Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Idea of Proof:
Pick an element of the set and find its cycle under the permutation. The cycle has to be finite since the set is finite. If there are any elements not in that cycle, then pick one and find its cycle. It can't overlap with the first cycle because then it would be contained in the first cycle.

Proof:
Let α be a permutation on $A = \{1, 2, \ldots, n\}$. To write α in disjoint cycle form, we start by choosing any member of A, say a_1, and let

$$a_2 = a_1\alpha, \quad a_3 = a_2\alpha = a_1\alpha^2,$$

and so on, until we arrive at $a_1 = a_1\alpha^m$, for some m.

Claim: Such an m exists.

We know such an m exists, because this sequence of images is finite. Because A is finite, by the Pigeonhole Principle, there must be two images that coincide, that is, $a_1\alpha^i = a_1\alpha^j$, for some i, j with $i < j$. We take $m = j - i$. Then $a_1 = a_1\alpha^m$.

We can write the permutation α as

$$\alpha = (a_1 a_2 \ldots a_m) \cdots ,$$

where the three dots at the end indicate that there may be other elements of A not accounted for.

If there are no other elements outside the $\{a_i\}$, then we are done. Otherwise, we choose a b_1 outside this set and find its cycle $(b_1 b_2 \ldots b_k)$, for some k, as before.

This cycle must have no elements in common with the first cycle. If there were an overlap, say $a_1\alpha^i = b_1\alpha^j$, for some i, j with $i \leq j$, then we would have

$$a_1\alpha^{j-i} = b_1,$$

and then b_1 would be contained in the first cycle of the $\{a_i\}$.

This contradicts how we chose b_1.

We can continue this process until every element of A has been included in a cycle. Then we can write α in the form

$$\alpha = (a_1 a_2 \ldots a_m)(b_1 b_2 \ldots b_k) \cdots (c_1 c_2 \ldots c_s).$$

Theorem 5.2: Disjoint Cycles Commute

If the pair of cycles $\alpha = (a_1 a_2 \ldots a_m)$ and $\beta = (b_1 b_2 \ldots b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.

Proof:
Let S be written

$$S = \{a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n, c_1, \ldots c_k\}.$$

Note that α acts only on the $\{a_i\}$, and β acts only on the $\{b_i\}$.

For any element $x \in S$, we note

- If $x \notin \{a_i\}$, then $x\alpha = x$.

  Then $(x\alpha)\beta = x\beta = (x\beta)\alpha$.

- If $x \notin \{b_i\}$, then $x\beta = x$.

  Then $(x\alpha)\beta = x\alpha = (x\beta)\alpha$.

(The case $x \in \{c_i\}$ is subsumed by the above two cases, in fact, $x\alpha\beta = x = x\beta\alpha$.)

Theorem 5.3: The Order of a Permutation

The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.

Idea of Proof:

The disjoint cycles commute with each other. Therefore if we have a permutation α written as

$$\alpha = (a_1a_2\dots a_m)(b_1b_2\dots b_k)\cdots(c_1c_2\dots c_s),$$

then

$$\alpha^n = (a_1a_2\dots a_m)^n(b_1b_2\dots b_k)^n\cdots(c_1c_2\dots c_s)^n.$$

When n is the LCM of m, k, s, and the other cycle lengths, that is the lowest power of α that equals the identity.

Homework Assignment 6

Reading Assignment:

Chapter 5: pages 93–106

Homework Problems:

Chapter 4: 9, 29, 33, 34, 46, 52

Chapter 5: 2, 3, 8, 11, 12, 20