MA441: Algebraic Structures I

Lecture 12

15 October 2003

Review from Lecture 11:

We showed how to organize a list of the subgroups of a group into a diagram called the **lattice of subgroups.**

We reviewed the definition of a permutation.

We defined the group of permutations of degree n, denoted S_n, and showed that it has order $n!$.

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.

Theorem 5.2: Disjoint Cycles Commute

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

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

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

then

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

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.

Proof:
First, observe that a cycle of length n has order n. (Exercise 5.2)

Next, suppose that α and β are disjoint cycles of lengths m and n, respectively.

Let k be the LCM of m and n.
Then $(\alpha\beta)^k = \alpha^k\beta^k = e$.

Let t be the order of $\alpha\beta$, that is, $t = |\alpha\beta|$.

By Corollary 2 to Theorem 4.1, we know that t divides k.

By definition of t,

$$(\alpha\beta)^t = e = \alpha^t\beta^t,$$

so $\alpha^t = \beta^{-t}$.

Since α and β are assumed to be disjoint cycles, it is also true that α^t and β^t are disjoint cycles.

Therefore α^t and β^t must both be the identity, since they are inverses, yet any element is fixed by either α^t or β^t since they are disjoint.

$\alpha^t = e$ implies $m|t$.
$\beta^t = e$ implies $n|t$.
So t equals the LCM of m and n.

We can extend the argument to more than two disjoint cycles by similar reasoning.

We can prove this by induction, treating the above argument as the base case. We assume the result is true for n disjoint cycles, then show it is true for $n+1$ disjoint cycles by treating the first n cycles as the permutation α and the $(n+1)$-th cycle as β.

The LCM of the lengths of the cycles is the same, no matter how you group them.

Definition:
A cycle of length 2, i.e., of the form (ab) is called a **transposition** or 2-cycle.

Theorem 5.4: Product of 2-cycles

Every permutation in S_n, $n > 1$, is a product of 2-cycles.

Proof:
Note that the identity can be written as (12)(12).

A k-cycle $(a_1 a_2 \dots a_k)$ can be written as

$$(a_1 a_2 \dots a_k) = (a_1 a_2)(a_1 a_3) \cdots (a_1 a_{k-1})(a_1 a_k).$$

Since any permutation can be written as a product of disjoint cycles, we can decompose any permutation into a product of transpositions by decomposing each disjoint cycle in the product.

Examples:

$(12345) = (12)(13)(14)(15)$.

$(1632)(457) = (16)(13)(12)(45)(47)$.

Note that our order is the reverse of Gallian's because we compose from left to right.

Note that decomposing a permutation into a product of transpositions is not unique.

$(12345) = (12)(13)(14)(15)$.

$(12345) = (13)(23)(25)(12)(25)(45)$.

While the number of transpositions may vary, we will see that the parity of the number does not.

Lemma:
If $\beta_1\beta_2\cdots\beta_{r-1}\beta_r = e$ in S_n (for some n), where the β_i are transpositions, then r is even.

Proof:
Clearly $r \neq 1$, since a single transposition is not the identity.

When $r = 2$, we are done.

We proceed by (strong) induction.
Suppose that the theorem is true for any integer less than r, $r > 2$. We will show it holds for r.

Sketch: Rewrite the permutation in such a way that we shift the last occurrence of an integer a as far left as possible until we eventually remove a from the permutation.

Proof:
The last pair of transpositions must be one of these four cases:

1. $e = (ab)(ab)$,

2. $(ab)(bc) = (ac)(ab)$,

3. $(ac)(cb) = (bc)(ab)$,

4. $(ab)(cd) = (cd)(ab)$.

If a occurs in the last transposition, then we can rewrite the last pair so that a no longer occurs in the last transposition.

Successively rewrite $\beta_{r-1}\beta_r$, then $\beta_{r-2}\beta_{r-1}$, $\beta_{r-3}\beta_{r-2}$, and so on, as long as the integer a still occurs in the permutation.

Eventually, we will reach the first case above, $(ab)(ab)$, where we can cancel out two transpositions.

If we don't, then the left-most transposition β_1 will have the only occurrence of a. This would contradict the assumption that the permutation is the identity, because if only one transposition contains a, then the permutation does not fix a.

Once we cancel the two transpositions, then there are only $r-2$ transpositions in the permutation, and we can apply our induction hypothesis.

Theorem 5.5: Always Even or Odd

If a permutation α can be expressed as a product of an even number of transpositions, then every decomposition of α into a product of transpositions must have an even number of transpositions. In symbols, if

$$\alpha = \beta_1\beta_2\cdots\beta_r = \gamma_1\gamma_2\cdots\gamma_s,$$

where the $\{\beta_i\}$ and $\{\gamma_i\}$ are transpositions, then r and s are both even or both odd.

Proof:

Write the identity as

$$\begin{aligned} \alpha\alpha^{-1} &= (\gamma_1\gamma_2\cdots\gamma_s)\cdot(\beta_1\beta_2\cdots\beta_r)^{-1} \\ e &= \gamma_1\gamma_2\cdots\gamma_s\beta_r^{-1}\cdots\beta_2^{-1}\beta_1^{-1} \\ e &= \gamma_1\gamma_2\cdots\gamma_s\beta_r\cdots\beta_2\beta_1. \end{aligned}$$

Note that a transposition is its own inverse. By our previous lemma, $r+s$ is even. So r and s are either both even or both odd.

Definition:
A permutation that can be expressed as a product of an even number of transpositions is called an **even** permutation. A permutation that can be expressed as a product of an odd number of transpositions is called an **odd** permutation.

Theorem 5.6: Even Permutations Form a Group

The set of even permutations in S_n forms a subgroup of S_n.

(See exercise 5.13.)

Definition:
The group of even permutations on n symbols is denoted A_n and is called **the alternating group of degree** n.

Theorem 5.7

For $n > 1$, the order of A_n is $(n!)/2$.

Proof:
For each odd permutation α, the permutation $(12)\alpha$ is even. Let β be any other odd permutation ($\beta \neq \alpha$). Then $(12)\alpha \neq (12)\beta$. So the number of even permutations is greater than or equal to the number of odd permutations.

The same argument holds when we take α, β odd to show that there are at least as many odd permutations as even ones.

Therefore, there are as many even permutations as odd permutations, so A_n has half the order of S_n.