MA441: Algebraic Structures I

Lecture 13

20 October 2003

Review from Lecture 12:

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.

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.

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.

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.

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.

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 $(n!)/2$.

Chapter 6: Isomorphisms

We have seen that the dihedral group D_4 can be represented three different ways.

1: The symmetries of a square

We let R denote a counterclockwise rotation by 90 degrees and let F denote a flip about the vertical axis of a square.

2: A permutation group

Consider permutations acting on $\{1, 2, 3, 4\}$. Let $R = (1432)$ and $F = (12)(34)$. Then D_4 is the subgroup $\langle R, F \rangle$ of S_4.

3: A matrix group

Consider four points in $\mathbb{R}^2$ that form a square: $(-1, 1)$, $(1, 1)$, $(1, -1)$, and $(-1, -1)$. Let

$$R = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

and

$$F = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

These are each three different realizations of the abstract group D_4.

In a certain sense, these three groups are the same. This notion of sameness can be precisely captured by the concept of **isomorphism**.

Isomorphism comes from the Greek and means "same form".

Definition:
An **isomorphism** ϕ from a group G_1 to a group G_2 is a one-to-one mapping (or function) from G_1 onto G_2 that preserves the group operation. That is, for every $a, b \in G_1$,

$$\phi(ab) = \phi(a)\phi(b).$$

To distinguish the two different group operations, let $\odot_1$ and $\odot_2$ denote the group operations on G_1 and G_2, respectively. Then we can write

$$\phi(a \odot_1 b) = \phi(a) \odot_2 \phi(b).$$

If there is an isomorphism from G_1 onto G_2, then we say that G_1 and G_2 are **isomorphic** and write $G_1 \approx G_2$ (or $G_1 \cong G_2$).

There are four steps to show that two groups are isomorphic:

Step 1: Mapping
Define a function from G_1 to G_2 that is a candidate for an isomorphism.

Step 2: One-to-one
Prove that ϕ is one-to-one (injective). That is, for any $a, b \in G_1$, show that $\phi(a) = \phi(b)$ in G_2 implies $a = b$.

Step 3: Onto
Prove that ϕ is onto (surjective). That is, for any $g_2 \in G_2$, there is a $g_1 \in G_1$ such that $\phi(g_1) = g_2$.

Step 4: Preserves Operation
Prove that ϕ preserves group operations (i.e., ϕ is operation-preserving). That is, show that $\phi(ab) = \phi(a)\phi(b)$ for any $a, b \in G_1$.

Later on, we'll see that you can have the first and fourth properties without necessarily having the mapping be one-to-one and onto. This more general notion is called **homomorphism**.

We'll refer to the fourth property as the **homomorphism property**.

The inverse test for isomorphisms

If ϕ is a homomorphism from G_1 to G_2 and ψ is a homomorphism from G_2 to G_1 such that

$$\phi \circ \psi = \psi \circ \phi = 1 \text{ (identity)},$$

that is, ϕ has an inverse ψ, then ϕ and ψ are isomorphisms.

The one-to-one and onto properties are satisfied for ϕ:

one-to-one: if $\phi(a) = \phi(b)$, then apply ψ to both sides:

$$\psi(\phi(a)) = \psi(\phi(b))$$

implies $a = b$.

onto: if $g_2 \in G_2$, then let $g_1 = \psi(g_2)$.
Then $\phi(g_1) = g_2$.

The same reasoning shows ψ is an isomorphism (switching ϕ with ψ).

Example 1:

Let G_1 be $(\mathbb{R}, +)$, the real numbers under addition.

Let G_2 be $(\mathbb{R}^+, \cdot)$, the positive real numbers under multiplication.

Then G_1 and G_2 are isomorphic under the map $\phi(x) = 2^x$.

Check the four properties:

1) ϕ clearly maps G_1 to G_2.

2, 3) ϕ is one-to-one and onto because we have the logarithm (base 2) as an inverse.

4) $\phi(x + y) = 2^{x+y} = 2^x \cdot 2^y = \phi(x)\phi(y)$.

Example 2:

Any infinite cyclic group is isomorphic to $\mathbb{Z}$.

The finite cyclic group $\langle a \rangle$ generated by a of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Let us show there is an isomorphism in the finite case.

Let ϕ map a^k to k.

Clearly ϕ is one-to-one by Theorem 4.1 which says that $a^i = a^j$ iff n divides $i - j$. Certainly ϕ is onto, since for any k in $\mathbb{Z}/n\mathbb{Z}$, we have that a^k maps to it.

The homomorphism property is satisfied:

$$\phi(a^r a^s) = \phi(a^{r+s}) = r + s = \phi(a^r) + \phi(a^s),$$

where addition on the right is modulo n.

For instance, $U(43)$ and $U(49)$ are both cyclic of order 42, hence they are both isomorphic to $\mathbb{Z}/42\mathbb{Z}$.

(Non)Example 3:

The mapping from $(\mathbb{R}, +)$ to itself that sends x to $\phi(x) = x^3$ is not an isomorphism because $(x+y)^3 \neq x^3 + y^3$. The homomorphism property is not satisfied.

(Non)Example 5:

$U(10) \not\approx U(12)$.

Note that $U(12) = \{1, 5, 7, 11\}$, and all elements have order 2.

On the other hand, $U(10) = \{1, 3, 7, 9\}$, and it is cyclic.

The orders of the elements are $1, 4, 4, 2$ respectively.

This difference in the orders of elements shows that the groups can not be isomorphic. We will use this discrepancy to show that any candidate function is not an isomorphism.

Suppose that ϕ is an isomorphism from $U(10)$ to $U(12)$. Then

$$\phi(9) = \phi(3 \cdot 3) = \phi(3) \cdot \phi(3) = 1,$$

since all elements of $U(12)$ have order 2.

However

$$\phi(1) = \phi(1 \cdot 1) = \phi(1) \cdot \phi(1),$$

so $\phi(1) = 1$.

This map ϕ violates the one-to-one condition, because both 9 and 1 map to 1.

Theorem 6.1: Cayley's Theorem

Every group is isomorphic to a group of permutations.

Proof:
Let G be any group. We will show that G can be viewed as a group of permutations acting on its own elements.

For any $g \in G$, let T_g denote the function

$$T_g(x) = gx \quad (\forall x \in G),$$

that is, T_g is left multiplication by g.

T_g is a permutation on the set of elements of G. (See Exercise 6.21.)

The set $\{T_g : g \in G\}$ forms a group under composition, where T_e is the identity and $T_{g^{-1}}$ is the inverse of T_g. (See Exercise 6.8.)

Let ϕ map g to T_g. We will show it is an isomorphism.

It is one-to-one. If $T_g = T_h$, then we apply them both to the identity and get
$T_g(e) = T_h(e)$, so $ge = he$ (left multiplication) and $g = h$.

It is clearly onto, since g maps to T_g.

The homomorphism property holds because

$$\phi(xy) = T_{xy} = T_x T_y = \phi(x)\phi(y).$$

Therefore G is isomorphic to the group $\{T_g : g \in G\}$.

We call this group of permutations the **left regular representation** of G.

Homework Assignment 7

Reading Assignment:

Chapter 6: pages 118–129

Homework Problems:

Chapter 4: 53, 60

Chapter 5: 13, 16, 21, 26, 40

Chapter 6: 1, 2, 3, 4, 5