MA441: Algebraic Structures I

Lecture 14

22 October 2003

Review from Lecture 13:

We looked at how the dihedral group D_4 can be viewed as

1. the symmetries of a square,

2. a permutation group, and

3. a matrix group.

This is an example of an **isomorphism** between groups.

Example 1:

The group $(\mathbb{R}, +)$, the real numbers under addition, is isomorphic to the group $(\mathbb{R}^+, \cdot)$, the positive real numbers under multiplication.

The isomorphism mapping is the exponential map $\phi(x) = 2^x$.

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 $\mathbb{Z}/n\mathbb{Z}$.

The isomorphism mapping sends
$a^k \in \langle a \rangle$ to $k \in \mathbb{Z}/n\mathbb{Z}$.

(Non)Example 3:

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

(Non)Example 5:

$U(10)$ is not isomorphic to $U(12)$.

Although both groups have order four, $U(10)$ is cyclic and therefore has an element of order four. On the other hand, all non-identity elements of $U(12)$ have order 2.

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 $a, b \in G_1$,

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

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 $a, b \in G_1$.

Definition:
A mapping from G_1 to G_2 that satisfies the fourth property is called a **homomorphism**.

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

$$T_g : G \to G \text{ via } x \mapsto xg,$$

that is, T_g is right multiplication by g.

Note: Gallian uses left multiplication T_g since he composes group operations from right to left. We compose from left to right, so we use right multiplication for T_g.

Write xT_g or $T_g(x)$ for the image of x under T_g:

$$xT_g = T_g(x) = xg.$$

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
$T_g(e) = T_h(e)$ $(eT_g = hT_g)$ so $eg = eh$ (right 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 **right regular representation** of G.

Example:

We form the right regular representation of D_3.

We label the elements of D_3 and write each in geometric and permutation notation:

Label	Geom.	Perm.
1	e	()
2	R	(132)
3	R^2	(123)
4	$D1$	(23)
5	$D2$	(13)
6	$D3$	(12)

Let us multiply $R = (132)$ on the right by every element of D_3:

$$\begin{array}{lcl} e \cdot R & = & R \\ R \cdot R & = & R^2 \\ R^2 \cdot R & = & e \\ D1 \cdot R & = & D2 \\ D2 \cdot R & = & D3 \\ D3 \cdot R & = & D1 \end{array}$$

In labels, this is the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix},$$

which is the permutation (123)(456).

Let us multiply $D1 = (23)$ on the right by every element of D_3:

$$
\begin{array}{lcl}
e \cdot D1 & = & D1 \\
R \cdot D1 & = & D3 \\
R^2 \cdot D1 & = & D2 \\
D1 \cdot D1 & = & e \\
D2 \cdot D1 & = & R^2 \\
D3 \cdot D1 & = & R
\end{array}
$$

In labels, this is the permutation

$$
\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 1 & 3 & 2 \end{pmatrix},
$$

which is the permutation (14)(26)(35).

Theorem 6.2: Properties of Isomorphisms Acting on Elements

Suppose that $\phi : G_1 \to G_2$ is an isomorphism. Then the following properties hold.

1. ϕ sends the identity of G_1 to the identity of G_2.

2. For every integer n and for every group element a in G_1, $\phi(a^n) = (\phi(a))^n$.

3. For any elements $a, b \in G_1$, a and b commute iff $\phi(a)$ and $\phi(b)$ commute.

4. The order of a, $|a|$ equals $|\phi(a)|$ for all $a \in G_1$ (isomorphisms preserve orders).

5. For a fixed integer k and a fixed group element b in G_1, the equation $x^k = b$ has the same number of solutions in G_1 as does the equation $x^k = \phi(b)$ in G_2.

Proof:

Part 1: $\phi(e_1) = e_2$, where e_1, e_2 are the identity elements of G_1, G_2, respectively.

Since $e_1 = e_1 e_1$,

$$\phi(e_1) = \phi(e_1 e_1) = \phi(e_1)\phi(e_1),$$

by the homomorphism property. By cancelling $\phi(e_1)$ from both sides, we have $e_2 = \phi(e_1)$.

Part 2: When n is positive,

$$\phi(a^n) = \phi(\overbrace{a \cdot a \cdots a}^{n}) = \overbrace{\phi(a) \cdots \phi(a)}^{n} = \phi(a)^n.$$

The inverse of an element is preserved under an isomorphism:

$$\phi(e_1) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1}) = e_2.$$

Then $\phi(g^{-1})$ is the inverse of $\phi(g)$, that is,

$$\phi(g^{-1}) = \phi(g)^{-1}.$$

Part 4: isomorphisms preserve orders.

Note $a^n = e_1$ iff $\phi(a)^n = e_2$.

Definition:
An isomorphism from a group G onto itself is called an **automorphism** of G.

Definition:
Let G be a group, and let $a \in G$. The function ϕ_a defined by $\phi_a(x) = a^{-1}xa$ for all $x \in G$, is called the **inner automorphism** of G **induced by** a.