MA441: Algebraic Structures I

Lecture 15

27 October 2003

Correction for Lecture 14:
I should have used multiplication on the right for Cayley's theorem.

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 for 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:

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

For emphasis, I may write $(x)T_g$ for xT_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
$(e)T_g = (h)T_g$ so $eg = eh$ (right multiplication) and $g = h$.

It is clearly onto, since g maps to T_g.

The homomorphism property holds because

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

We check this by applying $\phi(xy)$ to any $g \in G$:

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

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:

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

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:

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

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).

Consider the composition $R \cdot D1 = D3 = (12)$.

Multiply $D3 = (12)$ on the right by every element of D_3:

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

In labels, this is the permutation

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

which is the permutation (16)(25)(34).

In the group D_3, $R \cdot D1 = D3$ can be represented in permutations as

$$(132)(23) = (12).$$

Applying the isomorphism $\phi : g \mapsto T_g$, we can represent the operation as permutations in S_6 as

$$(123)(456) \cdot (14)(26)(35) = (16)(25)(34).$$

Let's summarize how we transform the group operation from D_3 to its right regular representation in S_6.

$$\phi(R \cdot D1) = \phi\,((132)(23)) = \phi((132))\,\phi((23))$$

$$\phi((132))\,\phi((23)) = (123)(456) \cdot (14)(26)(35)$$

$$(123)(456) \cdot (14)(26)(35) = (16)(25)(34)$$

$$(16)(25)(34) = \phi((12)) = \phi(D3).$$

Theorem 6.2: Properties of Isomorphisms Acting on Elements

Suppose that $\phi : G_1 \rightarrow G_2$ 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 3: a and b commute iff $\phi(a)$ and $\phi(b)$ commute.

We know that for a and b to commute means $ab = ba$.

Apply ϕ to the left and right and apply the homomorphism property.

Part 4: isomorphisms preserve orders.

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

(Non)example: $\mathbb{C}^*$ is not isomorphic to $\mathbb{R}^*$ because the equation $x^4 = 1$ has a different number of solutions in each group.

Theorem 6.3: Properties of Isomorphisms Acting on Groups

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

1. G_1 is Abelian iff G_2 is Abelian.

2. G_1 is cyclic iff G_2 is cyclic.

3. ϕ^{-1} is an isomorphism from G_2 to G_1.

4. If $K \leq G_1$ is a subgroup, then $\phi(K) = \{\phi(k) | k \in K\}$ is a subgroup of G_2.

Definition:
An isomorphism from a group G onto itself is called an **automorphism** of G. The set of automorphisms is denoted Aut(G).

Example 9:
Complex conjugation is an automorphism of $\mathbb{C}$ under addition and $\mathbb{C}^*$ under multiplication.

Example 10:
In $\mathbb{R}^2$, $\phi(a, b) = (b, a)$ is an automorphism of $\mathbb{R}^2$ under componentwise addition.

Correction: Last time I should not have defined an inner automorphism to be $\phi_a(x) = axa^{-1}$ as Gallian does. To compose from left to right, we need the following definition.

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.

The set of inner automorphisms is denoted Inn(G).

Theorem 6.4: Aut(G) **and** Inn(G) **are groups**

The set of automorphisms of a group G and the set of inner automorphisms of a group are both groups under the operation of function compositions.

Proof:
(Exercise 15)

Example 13: Aut($\mathbb{Z}/10\mathbb{Z}$) is isomorphic to $U(10)$.

Homework Assignment 8

Reading Assignment

Chapter 6: review

Chapter 7: pages 134–138

Homework Exercises

Chapter 5: 19, 28, 31, 44

Chapter 6: 2, 6, 7, 8, 10, 11

Note: in 6.8, $T_g(x) = xg$ is right multiplication, and in 6.11, $\phi_g(x) = g^{-1}xg$.