MA441: Algebraic Structures I

Lecture 16

29 October 2003
Review from Lecture 15:

**Theorem 6.1: Cayley’s Theorem**

Every group is isomorphic to a group of permutations.

**Example:**
\[
\phi(R \cdot D1) = \phi((132)(23)) = \phi((132)) \phi((23)) \\
\phi((132)) \phi((23)) = (123)(456) \cdot (14)(26)(35) \\
(123)(456) \cdot (14)(26)(35) = (16)(25)(34) \\
(16)(25)(34) = \phi((12)) = \phi(D3).
\]
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. $\phi$ 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 5:
Apply the isomorphism \( \phi \) to the equation \( x^k = b \) to get \( \phi(x^k) = \phi(x)^k = \phi(b) \).

Let’s rename the variable \( x \) to \( y \) in the second equation and write \( y^k = \phi(b) \).

For every solution \( x \in G_1 \) to the first equation, we get a solution \( y \in G_2 \) to the second equation. Because \( \phi \) is one-to-one, there are at least as many \( y \) as \( x \).
Suppose \( y \in G_2 \) is a solution to \( y^k = \phi(b) \). Since \( \phi \) is onto, there is an \( x \in G_1 \) such that \( \phi(x) = y \).

Now \( y^k = \phi(x)^k = \phi(x^k) = \phi(b) \). Since \( \phi \) is one-to-one, we know \( x^k = b \).

Therefore we have at least as many \( x \) as \( y \), and the number of solutions of the two equations are equal.

(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. \( \phi^{-1} \) 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 \( G_2 \).
Proof:

Part 1: follows from part 3 of Theorem 6.2, which shows that isomorphisms preserve commutativity.

Part 2: follows from part 4 of Theorem 6.2, which shows that isomorphisms preserve order and by noting that if $G_1 = \langle a \rangle$, then $G_2 = \langle \phi(a) \rangle$. 
Part 3: Since $\phi$ is one-to-one and onto, for every $y \in G_2$, there is a unique $x \in G_1$ such that $\phi(x) = y$. Define $\phi^{-1}(y)$ to be this $x$.

Clearly, $\phi^{-1}$ is one-to-one and onto, since $\phi$ is.

In fact, $\phi \circ \phi^{-1}$ is the identity map on $G_2$, and $\phi^{-1} \circ \phi$ is the identity map on $G_1$.

We need to show the homomorphism property for $\phi^{-1}$:

$$\phi^{-1}(ab) = \phi^{-1}(a) \phi^{-1}(b).$$
Let $\phi(x) = a$ (so $\phi^{-1}(a) = x$) and let $\phi(y) = b$ (so $\phi^{-1}(b) = y$).

Then substituting for $a$ and $b$,

$$\phi^{-1}(ab) = \phi^{-1}(\phi(x)\phi(y)) = \phi^{-1}(\phi(xy)) = xy = \phi^{-1}(a) \phi^{-1}(b).$$

Therefore $\phi^{-1} : G_2 \to G_1$ is an isomorphism.
Definition:
An isomorphism from a group $G$ onto itself is called an automorphism of $G$. The set of automorphisms is denoted $\text{Aut}(G)$.

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:** Previously I defined an inner automorphism to be of the form \( \phi_a(x) = axa^{-1} \), as Gallian does. To compose from left to right, we need instead the following definition.

**Definition:**

Let \( G \) be a group, and let \( a \in G \).

The function \( \phi_a \) 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 \( \text{Inn}(G) \).
Theorem 6.4: $\text{Aut}(G)$ and $\text{Inn}(G)$ are groups

The set of automorphisms $\text{Aut}(G)$ of a group $G$ and the set of inner automorphisms $\text{Inn}(G)$ of a group are both groups under the operation of function compositions.

Proof:
(Exercise 15)

$\text{Inn}(G)$ is closed under composition:

$$x\phi_a\phi_b = (a^{-1}xa)\phi_b = b^{-1}(a^{-1}xa)b = x\phi_{ab}.$$ 

$\text{Inn}(G)$ is closed under inversion:

$$x\phi_a\phi_{a^{-1}} = (a^{-1}xa)\phi_{a^{-1}} = x.$$
Example 13:

Aut(\(\mathbb{Z}/10\mathbb{Z}\)) is isomorphic to \(U(10)\).

An automorphism \(\alpha \in \text{Aut}(\mathbb{Z}/10\mathbb{Z})\) is determined by \(\alpha(1)\) because

\[
\alpha(k) = \alpha(\underbrace{1 + 1 \cdots + 1}_{k}) = k\alpha(1).
\]

Since 1 has order 10 in \(\mathbb{Z}/10\mathbb{Z}\), Theorem 6.2 tells us that \(\alpha(1)\) must also have order 10.

There are four elements of \(\mathbb{Z}/10\mathbb{Z}\) with order 10: 1, 3, 7, 9, hence \(\alpha(1)\) must be one of the four.
Let $\alpha_1$, $\alpha_3$, $\alpha_7$, and $\alpha_9$ be maps for which $\alpha_1(1) = 1$, $\alpha_3(1) = 3$, $\alpha_7(1) = 7$, and $\alpha_9(1) = 9$.

These are the only possible automorphisms. We can easily check that they are in fact automorphisms.

Consider $\alpha_3$. Since 3 generates $\mathbb{Z}/10\mathbb{Z}$, the map is onto.

The map $\alpha_3$ is also one-to-one. If $3a = 3b$, then $a = b$, because 3 is invertible mod 10.

The homomorphism property holds since $\alpha_3(a + b) = 3(a + b) = 3a + 3b = \alpha_3(a) + \alpha_3(b)$. 
**Theorem 6.5:** $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong U(n)$

For every positive integer $n$, $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ is isomorphic to $U(n)$.

The proof follows the reasoning of Example 13.
Chapter 7: 
Cosets and Lagrange’s Theorem

(page 134)

Definition:
Let $G$ be a group and $H$ a subset of $G$. For any $a \in G$, the set

$$\{ah : h \in H\}$$

is denoted $aH$. Analogously,

$$Ha = \{ha : h \in H\}.$$

When $H$ is a subgroup of $G$, $aH$ is the left coset of $G$ containing $a$ and $Ha$ is the right coset of $G$ containing $a$.

We say that $a$ is a coset representative of $aH$ or $Ha$. We write $|aH|$ and $|Ha|$ to denote the number of elements in the respective sets.
Theorem 7.1: Lagrange’s Theorem

If $G$ is a finite group and $H < G$ is a subgroup, then $|H|$ divides $|G|$. Moreover, the number of distinct left (or right) cosets of $H$ in $G$ is $|G|/|H|$. 