MA441: Algebraic Structures I

Lecture 5

17 September 2003

Review from Lecture 4:

The Pigeonhole Principle

Mathematical induction, $(ab)^n = a^n b^n$

Finite Subgroup Test

We defined the cyclic subgroup generated by $a \in G$ to be

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\}.$$

We said that G is cyclic if $G = \langle a \rangle$.

We previewed the concept of **isomorphism** by looking at D_4 in three different ways: geometric group, permutation group, and matrix group.

(From Chapter 3, page 64.)

Definition:
We say two elements a, b of a group **commute** if $ab = ba$.

Note: all elements of an Abelian group commute.

Definition: Center of a Group

The **center** $Z(G)$ of a group G is the subset of elements of G that commute with every element of G. We can express this formally as

$$Z(G) = \{a \in G : ax = xa, \text{ for all } x \in G\}.$$

Theorem 3.5: The center is a subgroup.

Proof:
Identity: $e \in Z(G)$ since the identity commutes with all elements.
Closure: suppose $a, b \in Z(G)$. We have

$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab).$

Inverses: given $ax = xa$, we can multiply on the left and right by a^{-1} to get

$$a^{-1}axa^{-1} = a^{-1}xaa^{-1},$$

which yields

$$xa^{-1} = a^{-1}x.$$

So a^{-1} commutes with x.

Definition: The centralizer of a in G

Let a be a fixed element of G.
The **centralizer of a in G**, which we denote $C(a)$ (or sometimes $C_a(G)$) is the set of elements of G that commute with a.

We can write this formally as

$$C(a) = \{g \in G : ga = ag\}.$$

Note that $C(a)$ contains $Z(G)$.

Example 12:
Consider D_4, where R_n denotes rotation by n degrees, H denotes reflection about the horizontal axis, V denotes reflection about the vertical axis.

(Notation: $R_0 = e$, $R_{90} = R$, and $V = F$.)

$C(R_0) = D_4 = C(R_{180})$.

$C(R_{90}) = \{R_0, R_{90}, R_{180}, R_{270}\} = C(R_{270})$.

$C(H) = \{R_0, H, R_{180}, V\} = C(V)$.

Since $R = R_{90}$ and $F = V$ generate D_4, it suffices to test relationships on these two generators.

Chapter 4: Cyclic Groups

(From Chapter 4, page 73)

Consider a cyclic group $G = \langle a \rangle$.

We say that G is generated by a or that a generates G.

Example 1:
The set of integers $\mathbb{Z}$ under addition is generated by 1. The additive inverse of 1 is -1.

When $n > 0$, we have $n = 1 + \cdots + 1$ (n times).
When $n < 0$, $n = (-1) + \cdots + (-1)$ (n times).

Example 3:
$\mathbb{Z}/8\mathbb{Z}$ under addition is cyclic generated by either 1, 3, 5, or 7. Let's check that 7 is a generator.

$$\begin{aligned} 1 \cdot 7 &= 7 \pmod 8 \\ 2 \cdot 7 &\equiv 6 \pmod 8 \\ 3 \cdot 7 &\equiv 5 \pmod 8 \\ &\cdots \end{aligned}$$

and so on, because $7 \equiv -1 \pmod 8$.

Nonexample 1:
$\mathbb{Z}/8\mathbb{Z}$ under addition is not generated by 4, since $\langle 4 \rangle = \{4, 0\}$.

Nonexample 2:
The dihedral group D_4 is not cyclic because all elements are either rotations or reflections and have orders 1, 2, or 4. A generator would have to have order 8.

Nonexample 3:
$U(8) = \{1, 3, 5, 7\}$ is not cyclic since 3, 5, 7 have order 2:

$$\begin{aligned} 3^2 &\equiv 1 \pmod{8} \\ 5^2 &\equiv 1 \pmod{8} \\ 7^2 &\equiv 1 \pmod{8} \end{aligned}$$

A generator would have to have order 4.

Theorem 4.1: Criterion for $a^i = a^j$

Let G be a group, and let a belong to G. If a has infinite order, then all distinct powers of a are distinct group elements. If a has finite order, say, n, then

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$$

and $a^i = a^j$ if and only if n divides $i - j$.

Proof:

If a has infinite order, then there is no non-zero n such that $a^n = e$. Since $a^i = a^j$ implies that $a^{i-j} = e$, it follows that $i - j = 0$, so $i = j$. That proves the first statement of the theorem.

Now assume that a has order n, i.e., $|a| = n$.

We will prove that $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.

Certainly these n elements are distinct. If $a^i = a^j$ with $0 \leq j < i \leq n-1$, then $a^{i-j} = e$ with $0 < i-j \leq n-1$. But by the definition of the order of an element, $i - j = 0$.

Now suppose that a^k is an arbitrary element of $\langle a \rangle$. We wish to show that a^k is in $\{e, a, \ldots, a^{n-1}\}$.

By the division algorithm, there exist integers q, r such that $k = qn + r$ with $0 \leq r < n$. Then

$$a^k = a^{qn+r} = a^{qn} \cdot a^r = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r.$$

This proves that $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$.

Next we prove that $a^i = a^j$ if and only if (iff) n divides $i - j$.

Suppose $a^i = a^j$. We show $n|(i - j)$.

Apply the division algorithm again to obtain q, r integers for which $i-j = qn+r$, with $0 \leq r < n$.

Since $a^i = a^j$, we know $a^{i-j} = e$ and

$$e = a^{i-j} = a^{qn+r} = (a^n)^q \cdot a^r = a^r.$$

Since the order of a is n and $0 \leq r < n$, we have $r = 0$, so n divides $i - j$.

Conversely, if $n|(i-j)$, say, $i - j = qn$, then $a^{i-j} = a^{qn} = e$.

This proves the last statement.