MA441: Algebraic Structures I

Lecture 6

22 September 2003

Review from Lecture 5:

We defined

- the **center** $Z(G)$ of a group G

- the **centralizer** $C(a)$ of an element $a \in G$

We also proved an important theorem about the structure of cyclic groups.

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 $i - j$.

We have two immediate consequences of this theorem.

The first corollary states that the order of an element equals the order of the subgroup generated by that element.

Corollary 1:
For any group element a,

$$|a| = |\langle a \rangle|.$$

Corollary 2:
Let G be a group and let $a \in G$ have order n. If $a^k = e$, then n divides k.

Multiplication (composition) of elements in a cyclic group of order n is accomplished by addition modulo n.

In fact, $\mathbb{Z}/n\mathbb{Z}$ is a prototype for all cyclic groups.

(A cyclic group $\langle a \rangle$ of order n is **isomorphic** to $\mathbb{Z}/n\mathbb{Z}$, where a plays the role of 1.)

Theorem 4.2:

Let a be an element of order n in a group and let k be a positive integer. Then

$$\langle a^k \rangle = \langle a^{\text{gcd}(n,k)} \rangle$$

and

$$|a^k| = \frac{n}{\text{gcd}(n,k)}.$$

Proof:
Let $d = \text{gcd}(n,k)$ and $k = dr$.

Since $a^k = (a^d)^r$, we have $\langle a^k \rangle \subseteq \langle a^d \rangle$.

Using the Euclidean algorithm, we can find s, t such that $d = ns + kt$. Then

$$a^d = a^{ns+kt} = (a^n)^s \cdot (a^k)^t = (a^k)^t,$$

so $\langle a^k \rangle \supseteq \langle a^d \rangle$ and the two sets are equal.

We prove the second part of the theorem by showing that $|a^d| = n/d$ for any $d|n$.

Clearly, $(a^d)^{n/d} = a^n = e$, so $|a^d| \leq n/d$.

Suppose i is a positive integer less than n/d. Then $i \cdot d < n$ and therefore $(a^d)^i \neq e$. So the order of a^d is n/d.

Now apply this to a^k.

Since $|a^k| = |\langle a^k \rangle|$, $|a^d| = |\langle a^d \rangle|$, and $\langle a^k \rangle = \langle a^d \rangle$, we have that the order of a^k is n/d, that is,

$$|a^k| = n/\operatorname{gcd}(n, k).$$

Corollary 1:
Let $|a| = n$. Then $\langle a^i \rangle = \langle a^j \rangle$ iff $\text{gcd}(n, i) = \text{gcd}(n, j)$.

Proof:
By Theorem 4.2, we have that $\langle a^i \rangle = \langle a^{\text{gcd}(n,i)} \rangle$ and $\langle a^j \rangle = \langle a^{\text{gcd}(n,j)} \rangle$.

We need to prove $\langle a^{\text{gcd}(n,i)} \rangle = \langle a^{\text{gcd}(n,j)} \rangle$ iff $\text{gcd}(n, i) = \text{gcd}(n, j)$.

Clearly $\gcd(n,i) = \gcd(n,j)$ implies $\langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle$.

Suppose that $\langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle$.

This means $|\langle a^{\gcd(n,i)} \rangle| = |\langle a^{\gcd(n,j)} \rangle|$, so $|a^{\gcd(n,i)}| = |a^{\gcd(n,j)}|$.

By the second part of Theorem 4.2, on the LHS $|a^{\gcd(n,i)}| = n/\gcd(n,i)$ and on the RHS $|a^{\gcd(n,j)}| = n/\gcd(n,j)$. Therefore,

$$\frac{n}{\gcd(n,i)} = \frac{n}{\gcd(n,j)},$$

so $\gcd(n,i) = \gcd(n,j)$.

Here are two special cases of Corollary 1.

Corollary 2:
Let $G = \langle a \rangle$ be a cyclic group of order n. Then $G = \langle a^k \rangle$ iff $\gcd(n, k) = 1$.

Corollary 3:
An integer k in $\mathbb{Z}/n\mathbb{Z}$ is a generator of $\mathbb{Z}/n\mathbb{Z}$ iff $\gcd(n, k) = 1$.

(Compare this to exercises 1, 2 of Chapter 4.)

Example:
Find all generators of $U(50)$. We're given that 3 generates $U(50)$ and has order 20.

The positive integers k less than 20 that are relatively prime to 20, i.e., $\gcd(20, k) = 1$, correspond to the powers of 3 that generate $U(50)$, by Corollary 2.

These integers are $\{1, 3, 7, 9, 11, 13, 17, 19\}$.

So $3 = 3^1$, $27 = 3^3$, $37 \equiv 3^7 \pmod{50}$, and so on, generate $U(50)$.

Caution: Notation for composition

In a group of functions, it is standard in group theory literature to compose from left to right (in the order in which you write symbols). To write ab means to first consider a, then b.

However, Gallian wishes to maintain consistency with the notation for composition of functions, where fg means $f(g) = f \circ g$. In this notation, fg means to first consider g then f.

We will consistently follow left to right composition. This may cause confusion with Gallian's notation for permutations.

Reading Assignment:

Chapter 4: pages 78–82

Chapter 5: pages 93–100

Homework Assignment 3

Chapter 2: 33, 34, 35

Chapter 3: 6, 7, 13, 22 (why?), 32

Chapter 4: 3, 10, 14, 17