MA441: Algebraic Structures I

Lecture 8

29 September 2003

Homework 2

Chapter 2, Problem 14:

Let G be a group with the following property:

> If a, b, and c belong to G and $ab = ca$,
> then $b = c$.

Prove that G is Abelian.

Please include this in Homework 4.

Review from Lecture 7:

Corollary 2 to Theorem 4.1:
Let G be a group and let $a \in G$ have order n. If $a^k = e$, then $|a| = n$ divides k.

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

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

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

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 $\gcd(n, k) = 1$.

Theorem 4.3: Fundamental Theorem of Cyclic Groups

Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k, namely, $\langle a^{n/k} \rangle$.

We proved last time:

Claim 1:
Every subgroup of a cyclic group is cyclic.

Proof of Theorem 4.3:

Claim 2: if $|\langle a\rangle| = n$, then the order of any subgroup of $\langle a\rangle$ is a divisor of n.

Let H be any subgroup of $\langle a\rangle$.

We've shown that $H = \langle a^m\rangle \leq \langle a\rangle$ for some $m > 0$.

We know $(a^m)^n = (a^n)^m = e^m = e$.

What can we say about the order of a^m?
(Consider Corollary 2 to Theorem 4.1)

This corollary tells us that $|a^m|$ divides n.

Therefore the order of H, $|H| = |a^m|$, is a divisor of n.

Claim 3: For each positive divisor k of n, the group $\langle a \rangle$ has a subgroup of order k.

What is the logical choice for such a subgroup?

Why does it have order k?

The subgroup $\langle a^{n/k} \rangle$ has order k:

$$(a^{n/k})^k = a^n = e.$$

Why does this have order exactly equal to k?

From Theorem 4.2,

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

Since k divides n, so does n/k. Therefore the order is $n/(n/k) = k$.

Claim 4: $\langle a^{n/k} \rangle$ is the unique subgroup of order k in $\langle a \rangle$.

Suppose H is any subgroup of order k, $H \leq \langle a \rangle$.

Then by the first Claim, $H = \langle a^s \rangle$ for some s that divides n.

Then $s = \gcd(n, s)$ and $|H| = n/s$.

What can we say about s and k?

By assumption, $|H| = k$, which equals n/s.

So $s = n/k$, which means $H = \langle a^{n/k} \rangle$.

Since any subgroup of order k is equal to this one, it is the unique subgroup of order k.

Corollary: Subgroups of $\mathbb{Z}/n\mathbb{Z}$

For each positive divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order k; moreover, these are the only subgroups of $\mathbb{Z}/n\mathbb{Z}$.

Definition:
We define the **Euler phi function** $\phi(n)$ to be the number of positive integers less than n and relatively prime to n $(n > 1)$.

Special case: for $n = 1$, we set $\phi(1) = 1$.

Note:
$\phi(n) = |U(n)|$.

Examples:
$\phi(3) = 2$, $\phi(12) = 4$.
Let p be prime. Then $\phi(p) = p - 1$.

Theorem 4.4:
If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.

(From Chapter 5, page 96)

Cycle Notation

We have seen how to specify a permutation as a two-row table. A different, more compact notation for a permutation is **cycle notation**.

Definition:
Suppose a permutation α acts on a set $A = \{1, 2, \ldots, n\}$. A **cycle** of α is a list $(a_1, a_2, \ldots, a_m)$ such that the $\{a_i\}$ are a subset of A and
$a_{i+1} = a_i\alpha$ (or $\alpha(a_i)$) for $0 \le i \le m-1$, and
$a_1 = a_m\alpha$ (or $\alpha(a_m)$).

We say that we write a permutation in **cycle notation** when we write it as a sequence of all its cycles.

Examples:

Let A be the set $\{1, 2, 3, 4\}$. Let α be the permutation

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}$$

In cycle notation, $\alpha = (123)(4)$.

Consider the permutations R and F.

$$R = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$$

In cycle notation, $R = (1234)$.

$$F = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}$$

In cycle notation, $F = (12)(34)$.

Homework Assignment 4

Reading Assignment:

Review chapters 1–4 and the first part of 5.

Homework problems:

Chapter 2: 8, 14, 17, 20, 36

Chapter 3: 11, 14, 17, 18, 24

Chapter 4: 7, 16, 19, 22, 39