MA441: Algebraic Structures I

Lecture 10

6 October 2003

Review from Lecture 8:

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, $\langle a^{n/k}\rangle$.

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 $\phi(1) = 1$.

Cycle notation for permutations

The cycle $(a_1, \ldots, a_m)$ denotes a mapping that sends a_i to a_{i+1} for $1 \leq i \leq m - 1$ and sends a_m to a_1.

We say such a cycle has length m.

When a permutation fixes an element (the element forms a cycle of length 1), we can drop it from the cycle notation.

It's easy to compose permutations written in cycle notation.

Example:
Consider $R = (1234)$, $F = (12)(34)$.

$R^2 = (1234)(1234) =?$

$R^2 = (13)(24)$.

$RF = (1234)(12)(34) =?$

$RF = (1)(24)(3) = (24).$ (diagonal flip)

$FR = (12)(34)(1234) =?$

$FR = (13)(2)(4) = (13).$ (diagonal flip)

$(FR)^2 = (13)(13) = e.$

To invert a permutation, simply reverse the direction of the mapping.

Examples:

$(1234)^{-1} = (1432)$

$[(123)(45)]^{-1} = (132)(45)$

Definition:
The group of permutations on n objects (or letters, numbers, etc.) is denoted S_n, for the **symmetric group** on n letters.

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 $\phi(d)$.

Proof:
By Theorem 4.3, there is exactly one subgroup of order d, say $\langle a \rangle$.

Every element of order d also generates $\langle a \rangle$.

By Corollary 2 of Theorem 4.2, an element a^k generates $\langle a \rangle$ iff $\gcd(k, d) = 1$, that is, k is relatively prime to d. There are exactly $\phi(d)$ such k.

Corollary:
In a finite group the number of elements of order d is divisible by $\phi(d)$.

Idea of proof:
Find all copies of the cyclic group of order d that sit inside the finite group. These copies must have no elements of order d in common, and they each have $\phi(d)$ elements of order d.

Proof:
Let G be a finite group.

If G has no elements of order d, then the statement is true because any integer divides zero.

Now suppose that $a \in G$ and has order d. By Theorem 4.4, we know that $\langle a \rangle$ has $\phi(d)$ elements of order d.

If all elements of order d in G are in $\langle a \rangle$, then we are done.

Otherwise, choose $b \in G$ of order d such that $b \notin G$.

Can the two cyclic subgroups $\langle a \rangle$ and $\langle b \rangle$ meet in an element of order d?

Suppose c has order d and is contained in both cyclic subgroups.

Since c has order d and is contained in $\langle a \rangle$, then $\langle c \rangle = \langle a \rangle$.

The same is true for $\langle b \rangle$, which also equals $\langle c \rangle$.

So $\langle a \rangle = \langle b \rangle$, which contradicts our choice of b not being in $\langle a \rangle$.

Since all cyclic subgroups of order d each have $\phi(d)$ elements of order exactly equal to d and have no such elements in common, the number of elements of order d in a finite group is a multiple of $\phi(d)$.

Homework Assignment 5

No reading assignment (review for midterm).

Homework Problems:

Chapter 4: 5, 18, 24, 25, 49