MA441: Algebraic Structures I

Lecture 2

8 September 2003

Review:

A group G is a set with a binary operation that satisfies four properties:

- Closure
- Associativity
- Identity
- Inverses

Note:

The associativity property lets us write a composition without parentheses:

$abc = a(bc) = (ab)c$.

For a positive integer n, we write a^n for the product of a taken n times.

When n is negative, we mean $(a^{-1})^n$.

We take $a^0 = e$.

(From Chapter 0, page 5)

Division Algorithm

Let a, b be integers with $b > 0$. Then there exist unique integers q, r with the property that

$$a = qb + r,$$

where $0 \leq r < b$.

Example:

Let $a = 17$ and $b = 5$. Then $a = 3b + 2$ $(q = 3, r = 2)$.

Definition:
The **greatest common divisor** of two nonzero integers a and b is the largest of all common divisors of a and b. We denote this integer by $\gcd(a, b)$.

When $\gcd(a, b) = 1$, we say that a and b are **relatively prime**.

Fact: GCD is a linear combination
For any nonzero integers a, b, there exist integers s and t such that $\gcd(a, b) = as + bt$. Moreover, $\gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

By repeatedly applying the division algorithm to two nonzero integers a and b, we can compute $\gcd(a, b)$ and the linear combination $\gcd(a, b) = as + bt$.

Example:
$a = 17, b = 5$

$$\begin{aligned} 17 &= 3 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1. \end{aligned}$$

We can work backwards to write

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ 2 &= 17 - 3 \cdot 5 \\ 1 &= 5 - 2(17 - 3 \cdot 5) \\ &= 7 \cdot 5 - 2 \cdot 17. \end{aligned}$$

Note:

Let a, b be two relatively prime integers.

We can find s, t such that $as + bt = 1$.

Then $as \equiv 1 \pmod{b}$ and we say that a has a multiplicative inverse modulo b.

Likewise, $bt \equiv 1 \pmod{a}$ and we say that b has a multiplicative inverse modulo a.

(From Chapter 1, page 33)

Definition:
Let G be a group of n elements.
A **Cayley table** (or **operation table**) is a table with n rows, indexed by the elements of G, and n columns, also indexed by G, such that the table entry corresponding to (a, b) is the product (or composition) ab in G.

Example
The dihedral group of an equilateral triangle, D_3, has 6 elements corresponding to rotation by 0, 120, and 240 degrees and reflection about an axis going through each vertex.

(Chapter 2, page 49)

Definition:
Let S be a subset of a group G. We say that S **generates** G if every element of G can be written as a product of elements of S or their inverses.

In other words, for any g in G, there are x_i $(i = 1 \ldots n)$ such that either x_i or x_i^{-1} is in S and

$$g = x_1 x_2 \cdots x_n.$$

We say that S is a set of **generators** for G.

Example:

The dihedral group D_4 is generated by a rotation and a flip. For example, let $R = R_{90}$ and $F = V$ be the flip about the vertical axis.

Compute $R, R^2, R^3, R^4 = e$. Then apply F to these four elements to get RF, R^2F, R^3F, F.

(From Chapter 2, page 43 on)

Examples

Example 1
The set of integers $\mathbb{Z}$, the set of rational numbers $\mathbb{Q}$, and the set of real numbers $\mathbb{R}$ are all groups under ordinary addition. In each case, the identity is 0 and the inverse of a is $-a$.

Example 4
The set of positive rationals $\mathbb{Q}^+$ is a group under multiplication. The inverse of a is $1/a$.

Example 7
The set of integers modulo n $\{0, 1, \ldots, n-1\}$, denoted $\mathbb{Z}/n\mathbb{Z}$ (often shortened to $\mathbb{Z}_n$) is a group under addition modulo n. The inverse of j is $n - j$.

Example 9

The 2-by-2 matrices with real coefficients and nonzero determinant form a group under multiplication called the **general linear group** of 2-by-2 matrices over $\mathbb{R}$, denoted $\mathrm{GL}(2, \mathbb{R})$.

Example 11

An integer a has a multiplicative inverse modulo n iff a and n are relatively prime. For each $n > 1$, we define $U(n)$ to be the set of positive integers that are less than n and that are relatively prime to n. Then $U(n)$ is a group under multiplication.

In particular, when n is a prime p, $\mathbb{Z}/p\mathbb{Z}$ is the set $\{1, 2, \ldots, p-1\}$. We sometimes write $(\mathbb{Z}/p\mathbb{Z})^*$ for this group.

(From Chapter 2, page 50)

Theorem 2.1:
In a group G, there is only one identity element.

Proof:
Suppose there are two identities e and e' such that for any $a \in G$, $ae = ea = a$ and $ae' = e'a = a$. Then

$$e = ee' = e'.$$

Theorem 2.3:
For each element a in a group G, there is a unique inverse b in G such that $ab = ba = e$.

Proof:
Suppose that b and c are inverses of a. Then $ab = ac = e$. Multiply on the left by b and apply the associativity and inverse rules.

$$\begin{aligned} ab &= ac \\ b(ab) &= b(ac) \\ (ba)b &= (ba)c \\ b &= c. \end{aligned}$$

(From Chapter 5, page 93)

A **permutation** of a set is a mapping that exchanges or rearranges the elements of the set.

Definition:
A **permutation** of a set A is a function from A to A that is both one-to-one and onto. A **permutation group of a set** A is a set of permutations of A that forms a group under function composition.

Example:
Let A be the set $\{1, 2, 3, 4\}$. Let α be a permutation defined by $\alpha(1) = 2,\ \alpha(2) = 3,\ \alpha(3) = 1,\ \alpha(4) = 4$.

We can write α in a table format as follows:

$$\alpha = \left[\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{array} \right]$$

We can represent the dihedral group D_4 as a permutation group. Take generators $R = R_{90}$ and F the vertical flip.

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

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

We compose RF to get

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

Reading Assignment

Chapter 0, pages 3–8

All of Chapter 1 and Chapter 2

Chapter 5, pages 93–96

Homework

Chapter 0: 1, 2, 3, 4

Chapter 1: 2, 3, 4

Chapter 2: 1, 4, 16, 18, 24

As permutations, compute the composition $FRFR$. Show the intermediate steps FR, FRF.