MA441: Algebraic Structures I

Lecture 3

10 September 2003

Review:

By repeatedly using the division algorithm for two positive integers a, b, we can compute their greatest common divisor gcd(a, b).

When a, b are relatively prime, we can compute the inverse of a in $U(b)$ (and vice-versa).

The Cayley table of a group represents the composition law: the (a, b) table entry equals ab.

We defined what it means for a set of elements to generate a group.

We defined the following groups:

- $\mathbb{Z}/n\mathbb{Z}$: the group of integers modulo n under addition modulo n;

- GL$(2, \mathbb{R})$: the general linear group of 2-by-2 matrices over the reals;

- $U(n)$: the group of positive integers less than n that are relatively prime to n under multiplication (the group of units mod n)

A group has a unique identity element.

Every element in a group has a unique inverse.

We defined a permutation of a set as a rearrangement (a one-to-one and onto mapping) and introduced notation that represents the rearrangement as a table.

Finite Groups and Subgroups

(From Chapter 3, page 58)

Definition: Order of a Group
The number of elements of a group (finite or infintite) is called its **order**. We will use $|G|$ (or sometimes $\#G$) to denote the order of G.

Example:
The group D_4 and the group $\mathbb{Z}/8\mathbb{Z}$ (under addition) both have order 8. The integers $\mathbb{Z}$, rationals $\mathbb{Q}$, or reals $\mathbb{R}$ (under addition) have infinite order.

Definition: Order of an Element
The **order** of an element g in a group G is the smallest positive integer n such that $g^n = e$. If no such integer exists, then we say that g has **infinite** order. We denote the order of an element g by $|g|$.

Note: in additive notation, we would write $ng = 0$ when the order of g is n.

To find the order of a group element g, it suffices to compute $g, g^2, g^3, \ldots$. If the first time you reach the identity in this sequence is when $g^n = e$, then the order of g is n.

Examples

In D_4, the order of R is 4, and the order of F is 2.

In $U(7) = (\mathbb{Z}/7\mathbb{Z})^*$, the order of 2 is 3. $2^2 = 4$ and $2^3 \equiv 1 \pmod 7$.

Example 3: Any nonzero a in the integers $\mathbb{Z}$ (under addition) has infinite order because the sequence $a, 2a, 3a, \ldots$ never contains the identity zero.

Definition: Subgroup
If a subset H of a group G is itself a group under the operation of G, then we say that H is a **subgroup** of G.

We denote this by writing $H \leq G$, or $H < G$ if we want to indicate that $H \neq G$.

The subgroup $\{e\}$ containing only the identity is called the **trivial subgroup**. Any other subgroup is a **nontrivial subgroup**.

A subset of a group under a different group operation is not a subgroup.

Example:
$\mathbb{Z}/n\mathbb{Z}$ under addition modulo n is not a subgroup of the integers $\mathbb{Z}$ under addition. While the elements $\{0, 1, \ldots, n-1\}$ may be regarded as a subset of the integers (under a natural inclusion), the group operation of addition modulo n is different than the operation on $\mathbb{Z}$

We can test whether a subset H of G is a subgroup in four steps.

Subgroup Test

1. Identify a condition (say, property P) that defines H.

2. Prove that the identity satisfies this defining condition. (Identity)

3. For any two elements a, b in H, prove that ab satisfies the defining condition and is therefore again in H. (Closure)

4. For any a in H, prove that a^{-1} satisfies the defining condition and is therefore again in H. (Inverses)

Note that because the group operation on H must be the same as the group operation on G, associativity follows automatically.

To show that a subset is not a subgroup, it suffices to show that at least one of the three properties (Identity, Closure, or Inverses) is not satisfied.

Example 6:
Let $G = \mathbb{R}^*$ (nonzero reals under multiplication). Let H be the subset of irrational numbers union with $\{1\}$. Then H is not a subgroup since $\sqrt{2}\sqrt{2} = 2$ is not in H and the Closure property is not satisfied.

We can rewrite the subgroup conditions more succinctly as follows.

Theorem 3.2 The Two-Step Subgroup Test

Let G be a group and H a nonempty subset of G. Then $H \leq G$ if $ab \in H$ for any $a, b \in H$ and if $a^{-1} \in H$ for any $a \in H$.

Note that the Inverse and Closure properties imply $e \in H$ since $aa^{-1} = e$.

Gallian also states a One-Step Subgroup Test that simply combines the closure and inverse steps.