MA441: Algebraic Structures I

Lecture 4

15 September 2003

The Pigeonhole Principle:

Let n be a positive integer.

If you place $n + 1$ balls in n bins, then some bin must have more than one ball.

(From Chapter 0, page 14)

Mathematical Induction

Theorem 0.4:
First Principle of Mathematical Induction

Let S be a set of integers containing a.

Suppose that S has the property that whenever some integer $n \geq a$ belongs to S, then the integer $n + 1$ belongs to S. ($n \in S$ implies $(n + 1) \in S$, for $n \geq a$.)

Then S contains every integer greater than or equal to a.

In particular, to prove that a property $P(n)$ holds for every positive integer n, you can use induction:

Step 1 (base case):
Show that $P(1)$ holds.

Step 2 (induction hypothesis):
Assume that $P(n)$ holds.

Step 3 (induction step):
Prove that $P(n+1)$ holds.

There is also a second principle of induction called "strong" induction. (Step 2: $P(k)$ holds for all $k \leq n$.)

Lemma: Let G be an Abelian group. Then for any $a, b \in G$, $(ab)^n = a^n b^n$ ($n \geq 1$).

Case $n = 1$: $(ab)^1 = ab$. (Base case)

Assume $(ab)^n = a^n b^n$. (Induction hypothesis)

Prove $(ab)^{n+1} = a^{n+1} b^{n+1}$.

$(ab)^{n+1} = (ab)^n \cdot ab$.

Use the induction hypothesis:

$(ab)^n \cdot ab = a^n b^n ab$,

and since G is Abelian,

$a^n b^n ab = a^n a \cdot b^n b = a^{n+1} b^{n+1}$.

Review from Lecture 3:

We defined

- the order $|G|$ of a group G,
- the order $|g|$ of an element $g \in G$,
- when a subset H is a subgroup of G, $H \leq G$.

We also stated 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 $a \in H$.

Example 4':

Let G be an Abelian group and H the subset of elements of order dividing 3, i.e., $\{x \in G : x^3 = e\}$.
Show that H forms a subgroup of G.

Let a, b be in H.
Closure: $(ab)^3 = a^3b^3 = e$ (since G is Abelian).
Inverses: Show $(a^{-1})^3 = e$. Since $a^3 = e$,

$$(a^{-1})^3 \cdot a^3 = (a^{-1})^3 \cdot e = e.$$

Question: Do the elements of order exactly equal to 3 form a subgroup?

Example:
$\{e, F\}$ and $\{e, R, R^2, R^3\}$ are subgroups of D_4.

Example:

Let A, B be two matrices in $\mathrm{GL}(2, \mathbb{R})$:

$$A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

and

$$B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

A and B generate the subgroup $\langle A,\, B \rangle$.

It suffices to check for identity and inverses. We then have closure automatically since $\langle A,\, B \rangle$ contains any sequence of products of A and B.

(From Chapter 3, page 62)

Theorem 3.3: Finite Subgroup Test

Let H be a nonempty finite subset of a group G. Then H is a subgroup of G if H is closed under the operation of G.

Proof:
It suffices to show that H contains inverses. Choose any a in G. If $a = e$, then it is its own inverse. If $a \neq e$, then consider the sequence $a, a^2, \ldots$. This sequence is contained in H by the closure property.

By the Pigeonhole Principle, since H is finite, there are distinct i, j such that $a^i = a^j$. Suppose $i > j$. Then a^{i-j} is in the sequence and must equal e because

$$a^i = a^j \cdot a^{i-j} = a^j.$$

We have that $aa^{i-j-1} = a^{i-j} = e$, so
$a^{-1} = a^{i-j-1}$.

Then $a = a^1 \neq e$ implies $i - j > 1$, so
$a^{-1} = a^{i-j-1} \in H$.

Definition:
For any $a \in G$, let $\langle a \rangle$ denote the set $\{a^n : n \in \mathbb{Z}\}$.

Theorem:
Let G be a group and a any element in G. Then $\langle a \rangle$ is a subgroup of G.

Proof:
For any n, m, $a^n a^m = a^{n+m}$. For any a^n, a^{-n} is in $\langle a \rangle$ as well.

Definition:
We refer to $\langle a \rangle$ as the **cyclic subgroup generated by** a. In the case that $G = \langle a \rangle$, we say that G is **cyclic** (or G is a **cyclic** group), and that a is a generator of G (or G is generated by a).

Note that since

$$a^i a^j = a^{i+j} = a^{j+i} = a^j a^i,$$

every cyclic group is Abelian.

Example 7:
In $U(10)$, $\langle 3 \rangle = \{3, 9, 7, 1\}$, that is, $U(10)$ is generated by 3.

$3^2 = 9$, $3^3 \equiv 7 \pmod{10}$, $3^4 \equiv 1 \pmod{10}$.

Example 8:
In $\mathbb{Z}/10\mathbb{Z}$ (under addition mod 10), $\langle 2 \rangle = \{2, 4, 6, 8, 0\}$ is a subgroup.

Reading Assignment:

Chapter 0: pages 14–17 on mathematical induction and 20–22 on functions.

All of Chapter 3.

Chapter 4: Properties of Cyclic Groups, pages 73–78.

Homework Assignment 2:

Chapter 2: 2, 5, 7, 14, 15, 30

Chapter 3: 1, 4, 10, 15, 16, 19

Chapter 4: 1, 2