Lecture Notes Math 371: Algebra (Fall 2006)

by Nathanael Leedom Ackerman

September 7, 2006

0.1 TALK SLOWLY AND WRITE NEATLY!!

0.2 Introduction

Before Class

(1) Write my name, office and office hours on the board.

(2) Write name of teaching assistant.

(3) Write the course web address

(1) Introduce myself and tell about my office hours.

(2) Introduce the TA

(3) Explain structure of the grading and exams.

- Give dates of take home midterms.
- Give break up of Homeworks (50%), In Class Midterm (20%), Take Home Midterm (30%)
- Say that homeworks will be posted on the webpage on Tuesdays and are due one week later in

class.

- The way homeworks will be graded is that two problems will randomly be selected and graded.
- Each student will be allowed to drop his lowest homework grade.
- We will try and post solution sets on the web after all homeworks are turned in.
- Homeworks can be done in groups (and I would encourage you to form groups to work on the problems). However, each person should write up the solutions themselves and they should write on the homework the names of all the people they collaborated with.

(4) Give a brief outline of the course.

(5) Say that we are going to be covering a lot of material, so it is important to stay on top of it. And if at any

point during the lecture something is unclear, please ask about it. Because if something doesn't make sense to you, then it probably doesn't make sense to others as well.

0.3 Review

As you guys have had an entire summer to think about anything but Algebra, lets start with a little review today and the go into some easy stuff

0.3.1 Definitions

Definition 0.3.1.1. We say that $\langle G, *, e\rangle$ is a group if

- G is a set.
- $* : G \times G \to G$
- $e \in G$
- (Associativity) $(\forall a, b, c \in G)(a * b) * c = a * (b * c)$
- (Identity) $(\forall x) x * e = e * x = x$

- (Inverse) $(\forall x)(\exists y)x * y = y * x = e$

0.3.2 Examples

Some examples of groups I am sure you are familiar with

are

- $\langle \mathbb{Z}, +, 0 \rangle$
- $\langle \mathbb{R} - 0, \times 1 \rangle$
- $\langle \{f : n \rightarrow n \text{ a bijection}\}, \circ, \text{ID} \rangle$

Now this last one is an important one as it consists of all permutations an n element set. It is called the Symmetric Group on n e
(S_n).

One way to think about it is to imagine we have a collection of n pebbles all in a row each labelled with a different number. An element of S_n is a way to put the pebbles in a different ordering. Draw 4 dots labelled with the numbers 1 to 4 and then draw a rearrangement of them. This is a group because no matter how you rearrange them you can always put them back in the original order. And, because when rearranging them it doesn't matter the order in which you do the rearranging operations. Maybe have it be a homework to confirm S_n is a group group

0.3.3 Theorems

Recall that

Definition 0.3.3.1. The Order of a group G is the number of its elements ($|G|$). The order of an element $x \in G$ is the size of the cyclic group generated by that element. I.e. $|\{e, x, x + x, x + x + x, \cdots\}|$.

Theorem 0.3.3.2 (Lagrange)**.** *Let G be a finite group and let H be a subgroup of G. The order of H divides the order of G.*

Proof. In order to prove this, recall the definition of a left coset.

Definition 0.3.3.3. Let G be a group and let H be a subgroup of G. A left coset of H is of the form $aH =$

$\{a + h : h \in H\}$. The number of left cosets is called the <u>index of H in G</u> ($[G : H]$)

We then have the following results.

Lemma 0.3.3.4. *Let H be a subgroup of G. If $aH \cap bH \neq \emptyset$ then $aH = bH$.*

Proof. -Let $x \in aH \cap bH$.

-We then know $x = ah$ and $x = bh'$. So in particular $b = xh^{-1} = ahh'^{-}1 \in aH$. So $bH \subseteq aH$.

-And similarly $aH \subseteq bH$. □

Lemma 0.3.3.5. *Let H be a subgroup of G. Then $|aH| = |H|$.*

Proof. -To see this observe that the map $h \longrightarrow ah$ is a bijection from H to aH with inverse $x \longrightarrow a^{-1}x$ (a map from aH to H) □

-We therefore have that $G = \bigsqcup_{a \in G} aH$ (which is a disjoint union).

-So $|G| = \Sigma_{aH}|aH|\Sigma_{aH}|H| = |H|[G : H]$ □

0.4 Group Actions

0.4.1 Definitions

Definition 0.4.1.1. Let $\langle G, *, e\rangle$ be a group and let X be a set. Let $\circ : G \times X \to X$. We will write $\circ(g, x)$ as $g \circ x$. We then say $\circ$ is a Group Action of G on X if

(1) $(\forall x \in X)e \circ x = x$

(2) $(\forall x \in X, g, g' \in G)(g * g') \circ x = g \circ (g' \circ x)$

In this context we say $(X, \circ)$ is a G-Set

Definition 0.4.1.2. Let $(X, \circ)$ be a G-Set. If $x \in X$ we define the Stabilizer of x to be $G_x = \{g \in G : g \circ x = x\}$. We also call the set $O_x = \{x : (\exists g \in G)g \circ y = x\}$ the Orbit of x under G.

0.4.2 Examples

0.4.2.1 General Linear Group

We have seen several examples of group actions so far. The first example we will consider is the group $GL_n(\mathbb{R})$ action on $\mathbb{R}^n$ dimensional real vectors. The operation we want is $\circ : GL_n(\mathbb{R}) \times R^n \rightarrow \mathbb{R}^n$ where $\circ$ is just matrix multiplication. To see that this is in fact a group operation we need to check:

$(\forall \overrightarrow{x} \in \mathbb{R}^n), ID \circ \overrightarrow{x} = \overrightarrow{x}$

$(\forall \overrightarrow{x} \in \mathbb{R}^n, A, B \in GL_n(\mathbb{R}) A \circ_{GL_n} B) \circ \overrightarrow{x} = A \circ (B \circ \overrightarrow{x})$.

The first of these is true by the definition of ID and the second is true because matrix multiplication (when it is defined) is associative

0.4.2.2 Left Group Action

Let $\langle G, *, e \rangle$ be a group. We want to consider the action of G on itself by left multiplication. To be specific we want to consider

$$* : G \times G \to G$$

$$(g, g') \rightsquigarrow g * g'$$

. Then checking that this is a group action amounts to checking that

$e * g = g$ for all $g \in G$

$(g * g') * h = g * (g' * h)$

Which is immediate from the definition of group.

0.4.2.3 Permutation Group (ONLY USE IF LOTS OF TIME)

Let $P_n = \{\langle i_1, \cdots i_n \rangle$ such that $\{i_1, \cdots i_n\} \subseteq \{1, \cdots n\}$ and $i_j = i_k \to j = k\}$. So P_n is the collection possible ways we can list the numbers $1 \cdots n$. Now let $\diamondsuit : S_n \times P_n$ be the function such that

If $f : \{1, \cdots n\} \to \{1, \cdots n\}$ is an automorphism (so that $f \in S_n$)

If $\langle i_1, \cdots i_n \rangle \in P_n$

Then define $f \Diamond \langle i_1, \cdots i_n \rangle = \langle f(i_1), \cdots f(i_n) \rangle$

For example to see how this works, say we have a function $f : \{1, \cdots 6\}$ such that

- $f(6) = 1$
- $f(i) = i + 1$ if $i \leq 5$

Now lets work out what $f \Diamond \langle 2, 4, 6, 1, 3, 5 \rangle$ is.
Well this is going to go to $\langle f(2), f(4), f(6), f(1), f(3), f(5) \rangle = \langle 3, 5, 1, 2, 4, 6 \rangle$.
Now that we know what the operation is applied we still need to show that it is a group operation of S_n on P_n. Well that involves checking that

- $e_{S_n} \Diamond \langle i_1, \cdots, i_n \rangle$.
- $f \Diamond (g \Diamond \langle i_1, \cdots, i_n \rangle) = (f \circ g) \Diamond \langle i_1, \cdots, i_n \rangle$

However the first of these is obviously true because e_{S_n} is just the identity and the second one is how composition in S_n is defined.

0.4.3 Theorems

We now have the following

Theorem 0.4.3.1 (Cayley's Theorem)**.** *If G is a finite group of order n then it is isomorphic to a subgroup of S_n.*

Proof. Lets label the elements of the group $\{1, \cdots, n\}$. Then each element $g \in G$ can be applied to $\langle 1, \cdots, n \rangle$ to get $\langle g * 1, \cdots, g * n \rangle = \langle i^g(1), \cdots, i^g(n) \rangle \subseteq \{1, \cdots, n\}$.

Further, because g has an inverse so does $i^g : \{1, \cdots, n\} \to \{1, \cdots, n\}$.

But that means $i^g \in S_n$ and we further have $i^{g*h}(t) = i^g \circ i^h(g)$ and so $g \rightsquigarrow i^g$ is an isomorphism. $\square$

0.4.4 Group actions on sets

Definition 0.4.4.1. Whenever we have a group action $\circ : G \times X \to X$ it induces a group action on $P(X)$ the powerset of X given by

$$g \circ \{x_i : i \in I, x_i \in X\} = \{g \circ x_i : i \in I, x_i \in X\}$$

If $Y \subseteq X$ then the set $\{g \circ Y : g \in G\}$ is called the Orbit of Y.

We have already run into one of these induced group actions before although we didn't put it in those terms. Specifically if G is a group and H is a subgroup then $H \subseteq G$ and the collection of left cosets of H is just the orbit of H under the action of left multiplication.

0.5 Counting Formula

0.5.1 Background Theorems

Let $(S, \circ)$ be a G-Set.

Theorem 0.5.1.1. *If $s \in S$ and let H be the stabilizer of s while $O_s \subseteq S$ is the orbit of s. Then there is a* *bijection*

$$\varphi : G/H \to O_s$$

defined by

$$aH \rightsquigarrow as$$

and further $\varphi(gC) = g \circ \varphi(C)$ *for every coset and every element* $g \in G$*.*

Proof. We need to show 4 things.

(1) φ does in fact define a map.

(2) $\varphi(gC) = g \circ \varphi(C)$

(3) φ is injective

(4) φ is surjective.

$\underline{(1)}$ In order to show this map is well defined we need to show that if $aH = bH$ then $a \circ s = b \circ s$. But we know that $b \in aH$ and so $b = ah$ for some $h \in H$. So we know that

$$b \circ s = (ah) \circ s = a(h \circ s) = a \circ s$$

because H is the stabilizer of s.

(2) This is true by the definition.

(3) Suppose $a \circ s = b \circ s$ and $aH \neq bH$. Then $(b^{-1}a) \circ s = s$ and so $b^{-1}a \in H$ the stabilizer of of s. but then $a \in bH$ and so $aH = bH$ by a previous theorem. $\Rightarrow\Leftarrow$ (4) Suppose $g \circ s \in O_s$. Well we know that $s = \varphi(H)$ and so, by (2) we know that $g \circ s = \varphi(gH)$. □

Corollary 0.5.1.2 (Counting Theorem)**.** *Let $(S, \circ)$ be a G-Set. If $s \in S$ then we have*

(order of G) = (order of stabilizer of s)(order of orbit of s)

$$|G| = |G_s||O_s|$$

Or equivalently $|O_s| = [G : G_s]$

Proof. This is because $|O_s| = [G : G_s]$ by the previous theorem. □

Lemma 0.5.1.3.

$$|S| = \Sigma_i |O_i|$$

where each O_i occurs exactly once.

Proof. We know that $S = \bigcup_{s \in S} O_s$ and so it suffices to show that $O_s \cap O_t \neq \emptyset \to O_s = O_t$ (i.e. that the orbits are disjoint).

But this is true because if $r \in O_s \cap O_t$ then we know $r = g \circ s = h \circ t$. But then $s = (h^{-1}g) \circ t$ and so $O_s \subseteq O_t$. (and we get the other direction the same way). □

0.5.2 Conjugation

Definition 0.5.2.1. Let $\langle G, *, e \rangle$ be a group. The group action which takes

$$\circ : G \times G \to G$$

$$(g, x) \rightsquigarrow gxg^{-1}$$

is called Conjugation

Theorem 0.5.2.2. *Conjugation is a group action.*

Proof. Checking this is a group action amounts to checking that

$e * g * e = g$ for all $g \in G$

$(g * g') \circ h = g \circ (g' \circ h)$

The first is obvious and the second is true because $(g * g') \circ h = (g * g') * h * (g * g')^{-1} = g * (g' * h * g'^{-1}) * g^{-1} = g \circ (g' \circ h)$ □

Definition 0.5.2.3. The stabilizer for a an element x under conjugation is called the Centralizer of x and denoted $Z(x)$. So

$$Z(x) = \{g \in G : gxg^{-1} = x\} = \{g \in g : gx = xg\}$$

and the centralizer of x is the collection of elements which commute with x.

Definition 0.5.2.4. We define the Center of a group G to be

$$Z = \{g \in G : (\forall x \in G) gx = xg\}$$

i.e those elements which commute with everything.

Notice that it is not hard to see that Z is a subgroup of G

0.5.3 Class Equation

Definition 0.5.3.1. If we apply the counting theorem to conjugation we see that

$$|G| = \Sigma_{\text{Conjugacy Classes C}} |C|$$

This is called the Class Equation for a finite group G.

This equation turns out to be very useful. As a simple example we will prove the following theorem.

Theorem 0.5.3.2. *Let $|G| = p^e$. Then the center of G has order > 1.*

Proof. The first thing to notice is by the previous theorem $|G| = |Z(x)| * |C_x|$ where C_x is the conjugacy class of x. So in particular, every conjugacy class divides $|G| = p^e$.

But, if $|C_x| = 1$ then that means that $C_x = \{gxg^{-1} : g \in G\} = \{x\}$ and so

$$(\forall g \in G) gx = xg$$

and hence $x \in Z$.

Now lets assume to get a contradiction that $|Z| = 1$.

Then we have by the class equation

$$|G| = p^e = 1 + \Sigma_i |C_i|$$

where each $|C_i| = p^{k_i}$ where $k_i > 0$.

$\Rightarrow\Leftarrow$

So we must have $|Z| > 1$. □