Math 342: *Abstract Algebra I*

2010-2011

Lecture 3: *Finite Groups and Subgroups*

Review:

We defined the following groups:

- Z_n ; the group of integers *modulo* n under addition *modulo n,*
- *GL(2, R);* the general linear group of 2-by- 2 matrices over the real numbers,
- *U(n);* the group of positive integers less than n and relatively prime to n under multiplica-tion.

A group has a unique identity element, and every Element has a unique inverse.

Finite Groups; Subgroups

Finite groups (groups have finitely many elements) have interesting arithmetic properties.

We will give some notions and terminology first.

Order of a Group

The number of elements of a group (finite or infinite) is its order and is denoted by $|G|$.

Sometimes it is denoted by $O(G)$.

Examples:

- The group

$$U(10) = \{1, 3, 7, 9\}$$

under multiplication modulo 10 has order 4.

- The group Z of integers under addition has infinite order.

Order of an element

The order of an element g in a group G is the smallest positive integer n such that

$$g^{n} = e.$$

In additive notation, this would be

$$n\,g = 0.$$

We denote the order of g by |g|.

If there is no such integer exists, we say that g has infinite order.

Note that

- To find the order of g, you need to compute the sequence of products

$$g, g^2, g^3, \ldots$$

until you reach the identity for the first time. The exponent of this product (the coefficient in addition) is the order of g.

- If no identity appears in the sequence, then g has infinite order.

Example 1

$U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ under multiplication modulo 15.

What is $|U(15)|$?

What is $|7|, |11|, |1|, |2|, |4|, |8|, |13|$ and $|14|$?

Hint: rather than computing the sequence

$$13^1, 13^2, 13^3, \ldots$$

We use the observation that $13 = -2 \bmod 15$, so $(13)^2 = (-2)^2 = 4$ and so on.

Example 2

Consider Z_{10} under addition modulo 10.

Find the order of its elements.

Hint: for instant 2+2 is treated as 2*2

And 2+2+2 as 3*2 and so on.

Example 3

What would be the order of the elements in Z under the ordinary addition?

Study the sequence a, 2a, 3a,... for nonzero a in Z

Some groups are subsets of the other with the same binary operation. For instance, the group SL(2, **R**) is a subset of the group GL(2, **R**).

Subgroups

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 and we denote it by $H \leq G$.

Proper subgroup

If H is a subgroup of G and is not equal to G, we write $H<G$.

- {e} is the trivial subgroup of G.

- A subgroup that is not {e} is called a nontrivial subgroup of G.

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

Example:

Z_n under addition modulo n is not a subgroup of Z under addition.

While the elements {0, 1, . . . , n – 1} may be regarded as a subset of the integers, the group operation of addition modulo n is different than the operation on Z.

In order to test whether a subset *H* of a group *G* is a subgroup, we check the four steps:

1. Identify a condition that defines *H*.
2. prove that the identity satisfies this condition, so the identity is in *H*.
3. For any *a, b* in *H*, prove that *ab* satisfies this condition and is therefore in *H*.
4. For any *a* in *H,* prove that a^{-1} satisfies the defining condition and is therefore in *H* as well.

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

Subgroup Test

To determined whether a subset H of a group G is a subgroup, we apply any of the following tests instead of verifying the group axioms.

Theorem 3.1 (One-step subgroup test)

Let G be a group and H a nonempty subset of G. If $ab^{-1} \in H$ whenever a and b are in H, then H is a subgroup of G.

(In additive notation, if a-b is in H whenever a, b are in H, then H is a subgroup of G.)

Steps to apply Theorem 3.1

1. Identify a defining condition P (say) on H.
2. prove that the identity has condition P (that is to say H is nonempty).
3. Assume that two elements a and b have condition P.
4. Show that ab^{-1} has condition P using that a and b have condition P.

Example 4

Let G be an abelian group with identity e. Let $H = \{x \in G \mid x^2 = e\}$. Show that H is a subgroup of G.

Example 5

Let G be an abelian group under multiplication with identity e. Show that $H = \{x^2 \mid x \in G\}$ is a subgroup of G. H is the set of all squares.

Theorem 3.2 (Two-step Subgroup Test)

Let G be a group and H be a nonempty subset of G. If ab in H whenever a and b are in H (i.e H is closed under the operation) and a^{-1} is in H whenever a is in H (i.e H is closed when taking inverses), then H is a subgroup of G.

To apply Theorem 3.2

Use the assumption that *a* and *b* have condition *P* (say) to prove that

1. *ab* has condition *P* and
2. a^{-1} has condition *P* as well.

How do you prove that a subset of a group is not a subgroup?

Do one of the three possible ways

1. show that the identity is not in the set.
2. find an element of the set whose inverse is not in the set.
3. find two elements in the set whose product is not in the set.

Example 6

Let G be the group of nonzero real numbers under multiplication,

$H = \{x \in G \mid x = 1 \text{ or } x \text{ is irrational}\}$ and

$K = \{x \in G \mid x \geq 1\}$. Show that H and K are not subgroups of G.

Theorem 3.3 (Finite subgroup Test)

Easier to use with finite groups

Let H be a nonempty finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.