Math342: *Abstract Algebra I*
2010-2011
Lecture 5: *Cyclic Groups*

Review

•we are mainly concerned with finite groups, that is, groups with a finite number of elements.

•The o*rder* of a group, ***|G|***, is the number of elements in the group. The order of a group may be finite or infinite.

•The o*rder* of an element, *|a|*, is the *smallest positive* integer *n* such that $a^n = e$.

•The order of an element may likewise be finite or infinite.

•Note*: if |a|=2 then* $a=a^{-1}$*. If |a|=1 then a=e.*

- A *subgroup* ***H*** of a group ***G*** is a subset of ***G*** together with the group operation, such that ***H*** is also a group.

That is, ***H*** is closed under the operation, and includes inverses and identity.

Note: ***H*** must use the same group operation as ***G***.

One step subgroup test

*Suppose **G** is a group and **H** is a non-empty subset of **G**.*
If, whenever a and b are in **H**,
$a*b^{-1}$ is also in **H**,
then **H** is a subgroup of **G**.

Or, in additive notation:
If, whenever a and b are in **H**,
$a - b$ is also in **H**,
then **H** is a subgroup of **G**.

To apply this test:

- Note that **H** is a non-empty subset of **G**.
- Show that for any two elements a and b in **H**, $a*b^{-1}$ is also in **H**.
- Conclude that **H** is a subgroup of **G**.

Exercise: Show that the even integers are a subgroup of the Integers.

Two step subgroup test

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

To apply this test:

- Note that **H** is nonempty .
- Show that **H** is closed with respect to the group operation.
- Show that **H** is closed with respect to inverses.
- Conclude that **H** is a subgroup of **G**.

Example: Let G be an Abelian group and $H = \{ x \in G : x^3 = e \}$. Show that H is a subgroup of G.

We note that e is in H, since $e^3 = e$. So H is not empty.
Let a, b be in H, then $a^3 = e$ and $b^3 = e$. Now $(ab)^3 = b^3 a^3 = a^3 b^3 = e$, therefore ab is in H.
Since $a^3 = e$, $(a^{-1})^3 = (a^{-1})^3 e = (a^{-1})^3 a^3 = (a^{-1} a)^3 = e$.

Finite subgroup test

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

To Use the Finite Subgroup Test:

If we know that ***H*** is finite and non-empty, all we need to do is show that ***H*** is closed under the group operation. Then we may conclude that ***H*** is a subgroup of ***G.***

Examples of Subgroups

Let **G** be a group, and *a* an element of **G**.

Let $<a> = \{a^n$, where *n* is an integer}, that is, all powers of a

Or, in additive notation

let $<a>=\{na$, where *n* is an integer}, that is, all multiples of *a*

Then $<a>$ is a subgroup of **G**.

For, in multiplicative notation, $a^0 = 1$is the identity; while $0a=0$ is the identity in additive notation.

Thus $<a>$ includes the identity.

Also note that the integers less than 0 are included here, so $<a>$ includes all inverses.

For example:

- *In **R***, <2>, the powers of 2, form a subgroup of **R***.*
- In **Z**, <2>, the even numbers, form a subgroup.
- In $\mathbf{Z}_8$, the integers mod 8,
  <2>={2,4,6,0} is a subgroup of $\mathbf{Z}_8$.

Cyclic Groups

A group G is cyclic if there is an element a in G such that $G = \{ a^n \mid n \in Z\}$.

a is called a generator of G and we write

$G = < a >.$

Note That:

In a group G, for $x \in G$, we define the powers x^n of x for $n \in Z$ as

- $x^0 = e$, *where e is the identity of G.*
- $x^n = x.x.x....x \qquad n > 0$
- $x^{-n} = (x^{-1})^n = (x^{-1}).(x^{-1}).(x^{-1})........(x^{-1}) \qquad n > 0$

Theorem 4.1

Let G be a group, and let a belong to G. If a has infinite order, then $a^i = a^j$ *if and only if* $i = j$.

If a has finite order, say n, then

$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j$ *if and only if* n *divides* $i-j$.

Corollary 1

For any group element a, $|a| = |\langle a \rangle|$

Corollary 2

Let G be a group and let a be an element of order n in G. If $a^k = e$, then n divides k.

Note That

1. Multiplication in $<a>$ works the same as addition in Z_n whenever $|a| = n$, no matter what group G is or how the element a is chosen.

$$\text{If } (i+j) \bmod n = k, \text{ then } a^i a^j = a^k$$

2. If *a* has infinite order, then multiplication in <*a*> works the same as addition in *Z.*

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

(A simple method of computing $|a^k|$ knowing only $|a|$)

Theorem 4.2

Let a be an element of order n in a group and let k be a positive integer. Then $\langle a^k \rangle = \langle a^{gcd(n, k)} \rangle$ and $|a^k| = n/gcd(n, k)$.

Corollaries

1. In a finite cyclic group, the order of an element divides the order of the group.
2. Let $|a|=n$. Then

   $$\langle a^i \rangle = \langle a^j \rangle \text{ iff } \gcd(n, i) = \gcd(n, j), \text{ and}$$

   $$|a^i| = |a^j| \text{ iff } \gcd(n, i) = \gcd(n, j).$$

3. $\langle a \rangle = \langle a^j \rangle$ *iff* $\gcd(n, j) = 1$ *and* $|a| = |\langle a^j \rangle|$ *iff* $\gcd(n, j) = 1$.
4. An integer k in Z_n is a generator of Z_n *iff* $\gcd(n, k) = 1$

How many subgroups a finite cyclic group has and how to find them?

<u>Fundamental theorem of cyclic groups</u>

<u>Theorem 4.3</u>

Every subgroup of a cyclic group is cyclic. Moreover, if $|a| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n and for each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k, $\langle a^{n/k} \rangle$.

Corollary (Subgroups of Z_n)

For each positive divisor *k* of n, the set $\langle n/k \rangle$ is the unique subgroup of Z_n of order *k*; moreover, these are the only subgroups of Z_n .

We can count the number of elements of each order in a finite cyclic group.

The Euler phi function:

Define $\varphi(1) = 1$, and for any integer $n>1$,

define $\varphi(n)$ to be the number of positive integers less than n and relatively prime to n.

For example, in the group $U(n)$ *what is* $\varphi(n)$?

It is impractical to determined the number of positive integers less than n and relatively prime to n by examining them one by one.

However, the following properties of the φ function simplify things.

- For any prime p, $\varphi(p^n) = p^n - p^{n-1}$
- For a relatively prime m and n,

$$\varphi(mn) = \varphi(m)\ \ \varphi(n).$$

For example, $\varphi(40) = \varphi(8)\ \varphi(5) = 4.4 = 16$,

$\varphi(75) = \varphi(5^2)\ \varphi(3) = (25 - 5).2 = 40.$

Theorem 4.4 (number of elements of each order in a cyclic group)

If *d* is a positive divisor of *n*, the number of elements of order *d* in a cyclic group of order *n is φ(d).*

Note that

there is no formula for the number of elements of each order for arbitrary finite group, though we still can have the next result.

Corollary (Number of elements of order d in a finite group)

In a finite group, the number of elements of order d is divisible by $\phi(d)$.

The relationships between the various subgroups of a group can be illustrated by a subgroup lattice of the group.