Finite Groups, Subgroups

Def Order of a Group

The number of elements of a group (finite or infinite) is called its order. We will use $|G|$ to denote the order of G.

Examples: $(\mathbb{Z}, +)$ has infinite order

$U(10) = \{1, 3, 7, 9\}$ under multiplication modulo 10 has order 4.

Def Order of an Element

The order of an element g of a group G is the smallest positive integer n such that $g^n = e$. (In additive notation $ng = e$.) If no such integer exists, we say g has infinite order. We denote the order of g by $|g|$.

Example :

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

  $7^1 = 7$, $7^2 = 49 = 4 \bmod 15$, $7^3 = 13$, $7^4 = 1$, so $|7| = 4$ in this case.

- Consider $\mathbb{Z}$ under ordinary addition. Every $z \in \mathbb{Z}$ with $z \neq 0$ has infinite order as $nz \neq 0$ if $z \neq 0$ and $n \geq 1$.

Def Subgroup

If a subset H of a group G is itself a group under the operation of G, we say H is a subgroup of G.

We write $H \leq G$. If $H \neq G$, we write $H < G$ (proper subgroup).

$\{e\} < G$ is called the trivial subgroup.

If $H \leq G$ and $H \neq \{e\}$ it is called nontrivial subgroup.

Thm One-Step Subgroup Test

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

Proof:

- The operation of H is associative since it is the same operation as in G.
- We show $e \in H$. Pick $x \in H$. Then $xx^{-1} = e \in H$.
- Existence of inverse: Pick $x \in H$, then $e \cdot x^{-1} = x^{-1} \in H$.
- We need to show closure: Namely that for $x, y \in H$, we have $xy \in H$. Let $x, y \in H$, we know that $y^{-1} \in H$. Then $xy = x(y^{-1})^{-1} \in H$

$\square$

Example: Let G be an Abelian group. $H = \{x \in G \mid x^2 = e\}$ is a subgroup of G.

<u>Proof:</u> $e \in H$, so H is nonempty.

Let $a, b \in H$, so $a^2 = e$ and $b^2 = e$.

We need to show $ab^{-1} \in H$, so $(ab^{-1})^2 = e$.

Proof: $(ab^{-1})^2 = (ab^{-1})(ab^{-1})$

$= a^2 (b^{-1})^2 = a^2 (b^2)^{-1} = ee^{-1} = e$ $\square$

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

Examples:
- The identity is not in the set.
- An element does not have an inverse in the set.
- The product of two elements is not in the set.

<u>Example</u>: Let G be the group of nonzero real numbers under multiplication

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

$K = \{x \in G \mid x \geq 1\}$

H is not a subgroup as $\sqrt{2} \in H$, but $\sqrt{2} \cdot \sqrt{2} = 2 \notin H$.
K is not a subgroup as $2 \in K$, but $2^{-1} \notin K$.

Thm Two-Step Subgroup Test
Let G be a group, H a nonempty subset of G. Then, H is a subgroup of G if H is closed under the operation and closed under inverse.

Proof: If $a, b \in H$, it follows that $ab^{-1} \in H$ $\square$

Thm 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: We only need to show that for $a \in H$, we also have $a^{-1} \in H$.

Consider $a \in H$. If $a = e$, then $a^{-1} = e \in H$. Otherwise, consider the sequence

$K = \{a, a^2, a^3, \dots\}$ Since H is finite and closed under the operation, $K \subseteq H$ and K is finite. So there exist i, j with $a^i = a^j$ and $i > j$, hence $a^i = a^j a^{i-j}$, so $a^{i-j} = e$.

$e = a^{i-j} = a \cdot a^{i-j-1}$, so $a^{i-j-1} = a^{-1} \in H$ $\square$

More Examples of Subgroups

Def $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ for $a \in G$ (group)

Thm $\langle a \rangle$ is a subgroup.

Proof: $a^n, a^m \in \langle a \rangle \Rightarrow a^n (a^m)^{-1} = a^{n-m}$ and $a^{n-m} \in \langle a \rangle$

$\square$

$\langle a \rangle$ is called cyclic subgroup of G generated by a.

MTH 339

Example: In $\mathbb{Z}_{10}$, $\langle 2 \rangle = \{2, 4, 6, 8, 0\}$

(Remember a^n means na when we use addition)

Def Center of a Group

The center $Z(G)$ of a group G is the subset of elements in G that commute with every element of G.

$$Z(G) = \{a \in G \mid ax = xa \text{ for all } x \in G\}$$

Def Centralizer of a in G

Let $a \in G$ (group), and define $C(a)$ as the set of all $g \in G$ that commute with a, so

$$C(a) = \{g \in G \mid ga = ag\}$$

MTH 339 - Do now

- Show that $|8| = 4$ in $U(15)$.
  What is $|4|$?

- Consider $\mathbb{Z}_{10}$ under addition modulo 10.
  Show that $|5| = 2$ and $|6| = 5$.
  What is $|7|$?

- 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

- Show that, in $U(10)$ we have $\langle 3 \rangle = \{3, 9, 7, 1\} = U(10)$.

MTH 339 - HW

1./ Define the set of complex roots of unity (solutions to $z^n - 1 = 0$) as

$$G_n = \left\{ \cos\left(\frac{k \cdot 360}{n}\right) + i \sin\left(\frac{k \cdot 360}{n}\right) \;\middle|\; k = 0, 1, 2, \dots n-1 \right\}$$

(a) Show that G_n is a group under multiplication.

(b) Show that G_4 is a subgroup of G_8. Sketch the elements of both groups on the complex plane.

2/ Prove that the center of a group G is a subgroup of G.

3/ Prove that the centralizer $C(a)$ is a subgroup.

4/ Prove that $Z(G) = \bigcap_{a \in G} C(a)$.

5/ Consider $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL(2, \mathbb{R})$. Find $|A|$.

Consider $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL(2, \mathbb{Z}_p)$, p prime.

MTH 339 - HW

Find $|A|$ in this case.

6/ Let $G = GL(2,\mathbb{R})$, and

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \,\middle|\, a, b \text{ are nonzero integers} \right\}$$

Prove or disprove that H is a subgroup of G.

7/ Let $G = GL(2,\mathbb{R})$

(a) Find $C\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right)$

(b) Find $C\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)$

(c) Find $Z(G)$.