MTH 339

More examples (definition of group)

Example: $\mathbb{Z}$ with ordinary multiplication is not a group. E.g. $5 \in \mathbb{Z}$ does not possess an inverse.

Example: $\{1, -1, i, -i\}$ is a group under multiplication.

Example: $\mathbb{Q}^+$ of positive rationals is a group under ordinary multiplication.

Example: $\mathbb{Z}_n = \{0, 1, \ldots n-1\}$ for $n \geq 1$ is a group under addition mod n.

For any $j \in \mathbb{Z}_n$ the inverse of j is $n-j$ as $(n-j) + j = n$, so $(n-j+j) \bmod n = 0$.

Example: $GL(2,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{R},\ ad-bc \neq 0 \right\}$

forms a group under matrix multiplication. For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$,

$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. $GL(2,\mathbb{R})$ is non-Abelian.

Example: $U(n)$: set of all integers larger 0 and relatively prime to n.
$U(n)$ is a group under multiplication modulo n.

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

mod 10	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Example: For a fixed point $(a,b) \in \mathbb{R}^2$, define $T_{a,b} : \mathbb{R}^2 \to \mathbb{R}^2$ by $(x,y) \to (x+a, y+b)$. Then $T(\mathbb{R}^2) = \{ T_{a,b} \mid a, b \in \mathbb{R} \}$ is a group under composition. Its elements are called translations.

Note: $T_{a,b} T_{c,d} = T_{a+c} T_{b+d}$ and therefore $T_{0,0}$ is the neutral element, $T_{-a,-b}$ the inverse of $T_{a,b}$.

Example: The set of all 2x2 matrices with determinant 1 and entries from $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}_p$ (p prime) is a non-Abelian group under matrix multiplication called the special linear group, e.g. $SL(2, \mathbb{Z}_5)$

Note: For $SL(2, \mathbb{Z}_5)$ we use modulo p arithmetic.

$A = \begin{pmatrix} 3 & 4 \\ 4 & 4 \end{pmatrix} \in SL(2, \mathbb{Z}_5)$, then

$\det(A) = 3 \cdot 4 - 4 \cdot 4 = -4 = 1 \bmod 5$

$A^{-1} = \begin{pmatrix} 4 & -4 \\ -4 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 1 \\ 1 & 3 \end{pmatrix}$. Indeed

$$\begin{pmatrix} 3 & 4 \\ 4 & 4 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 16 & 15 \\ 20 & 16 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Example: $\{1, 2, \ldots, n-1\}$ is a group under multiplication modulo n if and only if n is prime.

Elementary Properties of Groups:

Thm Uniqueness of the Identity

In a group, there is only one identity element.

Proof: Assume e and e' are identities.

$$\left.\begin{array}{l} ae = a \Rightarrow e'e = e' \\ e'a = a \Rightarrow e'e = e \end{array}\right\} \Rightarrow e' = e$$

$\square$

Thm Cancellation

(*) $ba = ca$ implies $b = c$

(**) $ab = ac$ implies $b = c$

Proof: Let a^{-1} be inverse of a.

$$\begin{aligned} ba = ca &\Rightarrow (ba)a^{-1} = (ca)a^{-1} \\ &\Rightarrow b(aa^{-1}) = c(aa^{-1}) \\ &\Rightarrow be = ce \\ &\Rightarrow b = c \end{aligned}$$

(**) similar

$\square$

Thm **Uniqueness of Inverses**

For each element a in a group G, there is a unique element b in G such that $ab = ba = e$.

Proof: Suppose b and c are inverses of a.

$ab = e \quad ac = e \Rightarrow ab \Rightarrow ac$

$\Rightarrow b = c$ (use cancellation)

$\square$

MTH 339 - Do Now

1./ Show that $\{1, -1, i, -i\}$ is a group under multiplication.

2./ Write the Cayley table for $\mathbb{Z}_4$.

3./ Show that $A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

MTH 339 - HW

1./ Let n and a be positive integers and let $d = \gcd(a, n)$. Show that the equation $ax = 1 \mod n$ has a solution if and only if $d = 1$.

2./ Construct a Cayley table for $U(12)$.

3./ Show that $\{1, 2, 3\}$ under multiplication modulo 4 is not a group, but that $\{1, 2, 3, 4\}$ under multiplication modulo 5 is a group.

4./ Let $a, b \in G$, G Abelian group. Prove $(ab)^n = a^n b^n$. Is this true for non-Abelian groups?

5./ Prove that G is Abelian if and only if $(ab)^{-1} = a^{-1} b^{-1}$ for all $a, b \in G$.