Group Theory

Definition & Examples

Def A group is a pair (G, m) of a set G together with a map $m : G \times G \to G$ satisfying

i) $m(a, m(b,c)) = m(m(a,b),c) \quad \forall a,b,c \in G$ (associativity)

ii) $\exists e \in G$ called a unit element satisfying
$m(e,a) = a = m(a,e) \quad \forall a \in G$ (unit)

iii) $\forall a \in G \; \exists b \in G$ st. $m(a,b) = e = m(b,a)$ (inverses)

Rmk: · We usually write $m(a,b) = a*b = a \cdot b = ab$
so that eg. i) becomes $a(bc) = (ab)c$

· We write $a^{-1} = b$ for the element assumed to exist in iii)

We write $G = (G,m)$.

Examples 0) $G = \{e\}$, $m(e,e) = e$ "trivial group"

1) $(\mathbb{Z}, +)$ where $e = 0$, $a^{-1} = -a$

2) $(\mathbb{Q}, +)$

3) $(\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}, *)$ $e = 1$, $a^{-1} = \frac{1}{a}$

$\left.\right\}$ F any field $(F,+)$ $(F^\times = F \setminus \{0\}, *)$ are groups

4) $GL(n,\mathbb{R}) = \{ A \text{ } n{\times}n\text{-matrix with entries in } \mathbb{R} \mid \det A \neq 0 \}$
"general linear group" $e = I$, $A^{-1} = A^{-1}$

5) $S(X) = \{ f : X \to X \mid f \text{ bijection} \}$
$e = id_X$, $f^{-1} = f^{-1}$

Def A group G is called abelian if
$ab = ba \quad \forall a,b \in G$

Ex 1), 2), 3) are abelian
4), 5) generally not ($n \geq 2$ in 4) and $|X| \geq 3$ in 5))

Rem In abelian groups we often write $a+b$ instead of $a \cdot b$.

Prop i) the unit is unique

ii) for each $a \in G$, a^{-1} is uniquely determined

iii) $(a^{-1})^{-1} = a$

iv) $(ab)^{-1} = b^{-1}a^{-1}$

v) for any $a_1, \dots, a_n$ the value of $a_1 \cdot \ldots \cdot a_n$ is independent on how the expression is bracketed.

Proof i) Suppose e' and e are units, then

$$e = e'e = e'$$

ii) Given a, suppose b_1 and b_2 satisfy $b_1 a = e = ab_2$
$b_2 a = e = ab_2$

then $b_1 = b_1 e = b_1(ab_2) = (b_1 a)b_2 = e b_2 = b_2$.

iii) By ii) to show that $b = (a^{-1})^{-1}$ it suffices to show that b is an inverse to a^{-1}, i.e. $ba^{-1} = e = a^{-1}b$ (*)
But $b = a$ satisfies (*).

iv) We compute
$$\begin{aligned}(b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}(ab)) \\ &= b^{-1}((a^{-1}a)b) \\ &= b^{-1}(eb) \\ &= b^{-1}b \\ &= e\end{aligned}$$

and similarly for $(ab)(b^{-1}a^{-1}) = e$
to conclude that $b^{-1}a^{-1}$ is an inverse of ab.

v) We show: let $f(a_1, \dots, a_n)$ be a bracketing of $a_1, \dots, a_n$
then $f(a_1, \dots, a_n) = (a_1(a_2(\dots(a_{n-1}a_n)\dots)$
$=: m_n(a_1, \dots, a_n)$

Induction on n:

$n = 1, 2$: ✓ $\quad (m_1(a_1) = a_1, \quad m_2(a_1, a_2) = m(a_1, a_2))$

$n \geq 3$: $\quad f = m(f_1(a_1, \dots, a_k), f_2(a_{k+1}, \dots, a_n))$

by ind hyp $f_1 = m_k$, $f_2 = m_{n-k}$

It remains to show $m(m_k, m_{n-k}) = m_n \quad \forall k$

$k=1$: $m(a_1, m_{n-1}(a_2,\dots,a_n)) = m_n(a_1,\dots,a_n)$

$k>1$: $m(m_k(a_1,\dots a_k), m_{n-k}(a_{k+1},\dots,a_n))$

$$= m(m(a_1, m_{k-1}(a_2,\dots,a_k)), m_{n-k}(a_{k+1},\dots,a_n))$$

$$\overset{assoc}{=} m(a_1, \underbrace{m(m_{k-1}(a_2,\dots,a_k), m_{n-k}(a_{k+1},\dots,a_n))}_{= m_{n-1} \text{ by ind hyp}})$$

$$= m_n(a_1,\dots,a_n)$$

Rmk In ii) either one of $ab=e$ or $ba=e$ uniquely characterize $b=a^{-1}$.

Prop Left and right cancellation holds in any group i.e.

i) $ax=ay \Rightarrow x=y$

ii) $xa=ya \Rightarrow x=y$

Proof multiply with a^{-1} from left / right.

Exercise / Remark Let (G,m), $m: G\times G \to G$ satisfy

i) $m(a,m(b,c)) = m(m(a,b),c)$ assoc

ii) $\exists e$ s.t. $m(e,a)=a$ $\forall a\in G$ left-unit

iii) $\forall a\in G$ $\exists b\in G$ s.t. $m(b,a)=e$ left-inverse

then (G,m) is a group.

Notation: $x^n = \underbrace{x\cdot\ldots\cdot x}_{n}$, $x^{-n} = \underbrace{x^{-1}\cdot\ldots\cdot x^{-1}}_{n}$

($n\cdot x = x+\dots+x$, $(-n)\cdot x = -x+-x+\dots+-x$ if G is abelian)

Def The order of $x\in G$ is the smallest positive integer n s.t. $x^n=e$. We write $|x|=n$.

Ex $\cdot$ $G=\mathbb{C}^\times$, $x=i$, $|x|=4$

$\cdot$ $G=GL(2,\mathbb{R})$, $x=\begin{pmatrix}0&-1\\1&1\end{pmatrix}$, $|x|=6$