Introduction to Groups

Contents

1 Basic Axioms and Examples

Definition. ***(Binary Operation)***

1. ***(binary operation)*** *$\star$ on a set G is a function $\star : G \to G$. write $a \star b$ instead of $\star(a, b)$*
2. ***(associative $\star$)*** *A binary operation on G is associative if for all $a, b, c \in G$ $a \star (b \star c) = (a \star b) \star c$*
3. ***(commutative $\star$)*** *A binary operation on G is commutative if for all $a, b \in G$, $a \star b = b \star a$*
4. ***(closed under $\star$)*** *$\star$ is a binary operation on G and $H \subset H$, if $\star|_H$ is a binary operation on H, i.e. for all $a, b \in H$, $a \star b \in H$, then H is closed under $\star$. Associativity/Commutativity of $\star$ is inherited on H*

- *(examples)*
  1. *$+$ on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ is a commutative binary operation*
  2. *$\times$ on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ is a commutative binary operation*
  3. *$-$ is not commutative on $\mathbb{Z}$ ($a - b \neq b - a$ usually)*
  4. *$-$ is not commutative on $\mathbb{Z}^+$ ($1, 2 \in \mathbb{Z}^+$, but $1 - 2 = -1 \notin \mathbb{Z}^+$)*

Definition. ***(Group)***

1. ***(group)*** *A group is an ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G satisfying*
   (a) *(associative) $\forall\, a, b, c \in G$, $(a \star b) \star c = a \star (b \star c)$*
   (b) *(identity) $\exists\, e \in G\ \ \forall\, a \in G\ \ a \star e = e \star a = a$ (e is an identity of G)*
   (c) *(inverse) $\forall\, a \in G\ \ \exists\, a^{-1} \in G$, $a \star a^{-1} = a^{-1} \star a = e$ (a^{-1} is an inverse of a)*
2. ***(abelian group)*** *A group if abelian/commutative if $a \star b = b \star a$ for all $a, b \in G$*
3. ***(finite group)*** *G is a finite group if G is a finite set*
4. ***(direct product)*** *If $(A, \star)$ and $(B, \circ)$ are groups, a new group $A \times B$ called direct product are defined as*

$$A \times B = \{(a, b) \mid a \in A \ \ b \in B\}$$

with binary operation defined component-wise

$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \circ b_2)$$

- *(examples)*
  - *$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are groups under $+$ ($e = 0$, $a^{-1} = -a$, associativity by axioms of $+$)*
  - *$\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}, \mathbb{C} - \{0\}, \mathbb{Q}^+, \mathbb{R}^+$ are gorups under $\times$ ($e = 1$, $a^{-1} = 1/a$, associativity by $\times$))*
  - *$(\mathbb{Z} - \{0\}, \times)$ is not a group ($2^{-1} = 1/2 \notin \mathbb{Z} - \{0\}$)*
  - *$(V, +)$ is an abelian group, where V is a vector space (commutativity by axioms of a vector space)*
  - *$(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian group ($e = \overline{1}$, $a^{-1} = \overline{-a}$)*
  - *$((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ is abelian group ($e = \overline{1}$, a^{-1} exists by definition of $(\mathbb{Z}/n\mathbb{Z})^\times$)*
- ***(theorem)*** *direct product of two groups is a group*
- ***(proposition)*** *identity/inverse are unique*
  1. *identity of G is unique*
  2. *inverse a^{-1} of any a in G is unique*
  3. *$(a^{-1})^{-1} = a$ for all a in G*