31/1/23 5 Groups: definition and examples

<u>Definition 5.1:</u> If A and B are sets, the Cartesian product $A \times B = \{(a,b) \mid a \in A,\ b \in B\}$.

Example: $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x,y) \mid x \in \mathbb{R},\ y \in \mathbb{R}\}$

Note: the pairs are <u>ordered</u>, i.e. $(a,b) \neq (b,a)$ unless $a=b$

Example: $A = \{1,2\}$ $B = \{1,2,3\}$ then

$A \times B = \{$

Remark: If A, B both finite then $|A \times B| = |A| \times |B|$

<u>Definition 5.4:</u> A <u>binary operation</u> on a set A is a map $\omega: A \times A \longrightarrow A$ (so we have a map

$(a,b) \longmapsto \omega(a,b) = a * b \in A)$

Examples: Let $A = \mathbb{Z}$. Define $\omega_1, \omega_2, \omega_3 : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ as

$\omega_1(m,n) = m+n$

$\omega_2(m,n) = m-n$

$\omega_2(m,n) = mn$

Note: $\omega(m,n) = \frac{m}{n}$ is not an operation on $\mathbb{Z}$ (even on $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$) as $m/n \notin \mathbb{Z}$ in general.

Remark 5.5: We usually write $a * b$ instead of $\omega(a,b)$.

Thus, for $*: A \times A \longrightarrow A$ to be an operation we must have $\underline{\underline{a * b}} \in A$ $\forall a,b \in A$ (closure axiom)

Examples (not interesting). $* : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$:

(1) $a * b = ab + 2$

(2) $a * b = a + 5$

(3) $a * b = 6$

Definition 5.6 (main): A *group* is a set G together with a binary operation $*: G \times G \longrightarrow G$ satisfying:

(G1) (closure) $x * y \in G \ \forall x, y \in G$

(G2) (associativity) $x * (y * z) = (x * y) * z \ \forall x, y, z \in G$

(G3) (identity) $\exists e \in G$ s.t. $e * x = x * e = x \ \forall x \in G$

(G4) (inverses) $\forall x \in G \ \exists y \in G$ s.t. $x * y = y * x = e$.

Definition 5.7: A group G is *abelian* (or *commutative*) if

(G5) $x * y = y * x \ \forall x, y \in G$

Remark: "abelian" in honour of Niels Abel

Remarks: (1) e in (G3) is called the *identity element*. It is unique.

(2) The element y in (G4) is the *inverse* of x. It is unique.

(3) We usually use *multiplicity notation* for $*$, i.e. write xy instead $x * y$; $e = 1$; x^{-1} for inverse

But if G is abelian, we can use sometimes *additive notation*: $x + y$, $e = 0$, $(-x)$ for inverse

(4) Even though G is a set with operation, we will normally speak about "group G".

(5) Associativity in (G2) means we don't need brackets in $xyzt$...

Examples: (1) $G = \mathbb{R} \setminus \{0\}$ under $\times$ is a group.

(G1) $xy \in G \ \forall x\,y \in G$ ✓

(G2) $x(yz) = (xy)z \ \forall x\,y\,z \in G$ ✓

(G3) take $e = 1$. then $1 \cdot x = x \cdot 1 = x \ \forall x \in G$ ✓

(G4) let $x \in G = \mathbb{R} \setminus \{0\}$ Then $x^{-1} = \frac{1}{x}$ is inverse ✓

(Note: $(\mathbb{R}, *)$ is not a group! as 0^{-1} doesn't exists (if $a = 0^{-1}$ then $\underbrace{a \cdot 0}_{0} = e = 1$ ↯))

set $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. then $(\mathbb{R}^*, \times)$ is a group.

similarly. $\mathbb{C}^*$, $\mathbb{Q}^*$, $\mathbb{F}^*$ (for any field $\mathbb{F}$) are groups under $\times$.

(2) $\mathbb{Z}$ is a group under $+$; $e = 0$; inverse is $(-x)$

similarly $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ are groups under $+$.