The Bright Side of Mathematics

Algebra - Part 5

Group: G together with binary operation $\circ$ and:

(G1) associativity $a\circ(b\circ c) = (a\circ b)\circ c$ for all $a,b,c\in G$

(G2) unique identity $e\in G$: $e\circ a = a = a\circ e$ for all $a\in G$

(G3) all inverses exist: $\forall a\in G\ \exists b\in G:\ b\circ a = e = a\circ b$

$a^{-1} := b$ (common notation)

Uniqueness of inverses:

$(S,\circ)$ semigroup with identity $e\in S$.

If $a\in S$ is a left invertible with x $(x\circ a = e)$ and right invertible with y, $(a\circ y = e)$

then $x = y$.

Proof: $x = x\circ e = x\circ(a\circ y) = (x\circ a)\circ y = e\circ y = y$ $\square$

Examples: (a) $G = \{e\}$ with $e\circ e = e$, $e^{-1} = e$

(b) $G = \{e, a\}$

$\circ$	e	a
e	e	a
a	a	e

$a^{-1} = a$

(c) $(\mathbb{Z}, +)$ with identity 0 and inverses $3+(-3) = 0$

$(\mathbb{Q}\setminus\{0\}, \cdot)$ with identity 1 and inverses $\frac{1}{4}\cdot\left(\frac{1}{4}\right)^{-1} = 1$

$(\mathbb{C}^{n\times n}, +)$ with identity $\begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$

$(\{A\in\mathbb{C}^{n\times n} \mid \det(A)\neq 0\}, \cdot)$ with identity $\begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$

General example: Let $(S,\circ)$ be a semigroup with identity $e\in S$.

$S^* := \{a\in S \mid a \text{ is invertible}\}$

a^{-1} exists

Then $(S^*, \circ)$ is a group.

Proof: (1) $e\circ e = e \Rightarrow e\in S^*$ with $e^{-1} = e \Rightarrow$ (G2) ✓

(2) $a\in S^* \Rightarrow \begin{matrix} a^{-1}\circ a = e \\ a\circ a^{-1} = e \end{matrix} \Rightarrow a^{-1}\in S^* \Rightarrow$ (G3) ✓

(3) $a,b\in S^* \Rightarrow (b^{-1}\circ a^{-1})\circ(a\circ b) \overset{\text{associativity in } S}{=} b^{-1}\circ\underbrace{(a^{-1}\circ a)}_{e}\circ b = e$

$(a\circ b)\circ(b^{-1}\circ a^{-1}) \overset{\text{associativity in } S}{=} a\circ(b\circ b^{-1})\circ a^{-1} = e$

$\Rightarrow (S^*, \circ)$ is a well-defined semigroup $\square$