Monoids, groups, rings and fields

Examples:

1) $(\mathbb{N},+)$ comm. monoid, ~~group~~; $\mathbb{N}^*$ closed in $(\mathbb{N},+)$

$(\mathbb{N}^*,+)$ ~~monoid~~ $a+b=b \Rightarrow a=0$

$(\mathbb{N},\cdot)$ comm. monoid, ~~group~~; $\mathbb{N}^*$ is closed in $\mathbb{N}$ w.r.t. $\cdot$

$(\mathbb{N}^*,\cdot)$ comm. monoid

"$\cdot$" is distributive w.r.t. "+" $(\mathbb{N},+,\cdot)$ ~~ring~~

2) $(\mathbb{Z},+)$ Abelian group; $\mathbb{Z}^*$ is not closed in $(\mathbb{Z},+)$

$(\mathbb{Z},\cdot)$ comm. monoid; $1+(-1)=0\notin\mathbb{Z}^*$

~~group~~; units: $-1, 1$;

$(\mathbb{Z}^*,\cdot)$ comm. monoid; ~~group~~

$(\mathbb{Z},+,\cdot)$ comm. ring, unitary, $0\neq 1$, has no zero divisors = = integral domain, ~~field~~

3) $(\mathbb{Q},+)$ Abelian group

$(\mathbb{Q},\cdot)$ comm. monoid; units: $\mathbb{Q}^*$; $(\mathbb{Q}^*,\cdot)$ Abelian group

"$\cdot$" is distr. w.r.t. "+" $\Longrightarrow (\mathbb{Q},+,\cdot)$ field

4) $(\mathbb{R},+)$ Abelian group,

$(\mathbb{R},\cdot)$ comm. monoid; units: $\mathbb{R}^*$, $(\mathbb{R}^*,\cdot)$ Abelian group;

$\Longrightarrow (\mathbb{R},+,\cdot)$ field;

5) $(\mathbb{C},+)$ Abelian group;

$(\mathbb{C},\cdot)$ comm. monoid; units: $\mathbb{C}^*$; $(\mathbb{C}^*,\cdot)$ Abelian group

$\Longrightarrow (\mathbb{C},+,\cdot)$ field.

6) $\underline{\mathbb{R}\setminus\mathbb{Q}}$ is not closed in $(\mathbb{R},+)$, nor in $(\mathbb{R},\cdot)$

$\sqrt{2}+(-\sqrt{2})=0\in\mathbb{Q}$; $\sqrt{2}\cdot\sqrt{2}=2\in\mathbb{Q}$.

$(a+\sqrt{b})(a-\sqrt{b}) \in \mathbb{Q}$, $\quad a+\sqrt{b}+a-\sqrt{b}=2a\in\mathbb{Q}$

$a, b \in \mathbb{Q}$, $\sqrt{b} \notin \mathbb{Q}$

Ex1: Let $(M,\cdot)$ be a monoid.

$$U(M)=\{x\in M \mid \exists x^{-1}\in M : x^{-1}x=1=x\cdot x^{-1}\}.$$

Show that $U(M)$ is closed in $(M,\cdot)$ and that $(U(M),\cdot)$ group. (ind. op.)

(called the group of units of M).

Solution: Let $x,y\in M$ invertible, xy has an inverse

$$(xy)^{-1}=y^{-1}x^{-1}. \checkmark$$

Indeed, $(xy)(y^{-1}x^{-1})=x(yy^{-1})x^{-1}=xx^{-1}=1$

$(y^{-1}x^{-1})(xy) = \quad \dots \quad =1$

Moreover, $\underline{1\in U(M)}$ and $\underline{(x^{-1})^{-1}=x} \to x^{-1}\in U(M)$

$U(M)$ is closed in $(M,\cdot)$

$(U(M),\cdot)$

Applications: 1) $(\mathbb{Z},\cdot)$ comm. monoid, $U(\mathbb{Z})=\{-1,1\}=U_2$

$(U_2,\cdot)$ Abelian group.

2) Let M be a set, $M^M=\{f \mid f:M\to M\}$.

$a \longmapsto f(a) \longmapsto g(f(a))$

$$A \xrightarrow{f} B \xrightarrow{g} C, \qquad A \xrightarrow{g\circ f} C$$

$B^A=\{f \mid f:A\to B\}$

$\circ : \underline{C^B}\times \underline{B^A} \longrightarrow \underline{C^A}$

$\circ$ is an operation on M^M and $\underline{(M^M,\circ)}$ monoid

$1_M : M\to M$, $1_M(x)=x$ identity mapping.

the identity element in $(M^M,\circ)$

$$M \xrightarrow{1_M} M \xrightarrow{f} M, \qquad M \xrightarrow{f} M$$

$$f\circ 1_M = f \overset{?}{=} 1_M\circ f \quad \leftarrow \text{homework.}$$

$x \longmapsto x \longmapsto f(x)$

$U(M^M)=\{f:M\to M \mid \exists g:M\to M \text{ s.t. } f\circ g=1_M=g\circ f\}=$

$=\{f\in M^M \mid f \text{ bijective}\}=S_M$ and $(S_M,\circ)$ group.

The symmetric group $(S_n, \circ)$

Let $n \in \mathbb{N}^*$, M be a set, $|M| = n$

$S_M = S_n$, $(S_n, \circ)$ is called the symmetric group of degree n.

$M = \{1, 2, \dots, n\}$, $\sigma \in S_n$, $\left\{ \sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \right.$

$|S_n| = n!$ permutation of M

Ex 2: Show that for any $n \geq 3$, $(S_n, \circ)$ noncommutative group.

Solution:

$n = 3$, $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$; $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$\nparallel$

$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Let $n \geq 3$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix}$; $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix}$

$\sigma\tau \neq \tau\sigma$.

Def: Let $\sigma \in S_n$, $1 \leq i < j \leq n$.

A pair (i, j) is called inversion of σ if $\sigma(i) > \sigma(j)$.

$Inv(\sigma)$ = the number of the inversions of σ

$\varepsilon(\sigma) = (-1)^{Inv(\sigma)}$ - the signature (sign) of σ

$\left\{ \varepsilon : S_n \to \{-1, 1\},\ \sigma \mapsto \varepsilon(\sigma) \right.$
the signature

σ is odd if $\varepsilon(\sigma) = -1$
(even) $(+1)$

$e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$ the identity permutation, $\varepsilon(e) = 1$

Let $n \in \mathbb{N}$, $n \geq 2$, $1 \leq i < j \leq n$, the permutation

$$\begin{pmatrix} 1 & 2 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & n \\ 1 & 2 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & n \end{pmatrix}$$

is called transposition $((i\,j) = (j\,i))$.

$\operatorname{Inv}(i\,j) = (j-i) + (j-i-1) = 2(j-i)-1 \longrightarrow \varepsilon((i\,j)) = -1.$

$(\cancel{\ ,i}), (\cancel{j,\ })$

$(i,i+1), (i,i+2), \dots, (i,j) \leftarrow j-i$ inversions

$\cancel{(i,j)}, (i+1,j), \dots, (j-1,j) \leftarrow j-i-1$ —"—

<u>Remark:</u> The transpositions are odd permutations.

—

(i,j) inversion $\Longrightarrow \dfrac{\sigma(i)-\sigma(j)}{i-j} < 0 \Longleftarrow$

$$(*) \quad \varepsilon(\sigma) = \prod_{1\le i<j\le n} \frac{\sigma(i)-\sigma(j)}{i-j}. \checkmark$$

—

<u>Ex 3.</u> Show $\varepsilon : S_n \longrightarrow \{-1,1\} = U_2$ is a surjective group morphism from $(S_n,\circ)$ into $(U_2,\cdot)$, for any $n\in\mathbb{N}$, $n\geq 2$.

<u>Solution:</u> $\varepsilon(e) = 1$, $\varepsilon((i\,j)) = -1 \Longrightarrow \varepsilon$ is surjective.

$$\forall \sigma,\tau\in S_n, \quad \varepsilon(\sigma\circ\tau) \overset{?}{=} \varepsilon(\sigma)\cdot\varepsilon(\tau)$$

$$\varepsilon(\sigma\circ\tau) \overset{(*)}{=} \prod_{1\le i<j\le n} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{i-j} =$$

$$= \prod_{1\le i<j\le n} \frac{\sigma(\overset{k}{\overbrace{\tau(i)}})-\sigma(\overset{l}{\overbrace{\tau(j)}})}{\tau(i)-\tau(j)} \cdot \prod_{1\le i<j\le n} \frac{\tau(i)-\tau(j)}{i-j} = \varepsilon(\sigma)\cdot\varepsilon(\tau)$$