Grupoidy

1.) Definujme binární operaci $\circ$ na $G = \mathbb{R}\times\mathbb{R}$:

$$(a,b)\circ(c,d) = (ac,\ bc+d)$$

Je $(G,\circ)$ asociativní, nebo komutativní grupoid?

Řešení: a) $(0,1)\circ(1,1) = (0,2)$

$(1,1)\circ(0,1) = (0,1)$ $\Big\} \Rightarrow$ grupoid není komutativní

b) $(a,b)[(c,d)\circ(e,f)] = (a,b)(ce,\ de+f) = (ace,\ bce+de+f)$

$[(a,b)(c,d)]\circ(e,f) = (ac,\ bc+d)(e,f) = (ace,\ bce+de+f)$ $\Rightarrow$ grupoid je asociativní

$\Rightarrow$

2.) Definujme binární operaci $\circ$ na $\mathbb{R}-\{0\}$:

$$a\circ b = |a|\cdot b$$

Je $(\mathbb{R}-\{0\},\circ)$ asociativní, nebo komutativní?

Řešení: a) $(-1\circ 2)\circ(-3) = (|-1|\cdot 2)\circ(-3) = 2\circ(-3) = |2|(-3) = -6$

$-1\circ(2\circ(-3)) = -1\circ(|2|\cdot(-3)) = -1\circ(-6) = |-1|\cdot(-6) = -6$ $\Big\} \Rightarrow$ možná je asociativní?

obecně: $(a\circ b)\circ c = (|a|b)\circ c = ||a|b|c = |ab|c$

$a\circ(b\circ c) = a\circ(|b|c) = |a|\cdot|b|c = |ab|c$ $\Big\} \Rightarrow$ grupoid je asociativní

b) $(-1)\circ 2 = |-1|\cdot 2 = 2$ ale $2\circ(-1) = |2|(-1) = -2$ $\Rightarrow$ grupoid není ~~asociativní~~ komutativní

$\Rightarrow$ Existují grupoidy, které jsou asociativní, ale nejsou komutativní.

3.) Definujme binární operaci $*$ na $\mathbb{R}$:

$$a * b = |a-b|$$

Je $(\mathbb{R}, *)$ asociativní, nebo komutativní?

Řešení:

a) $(1*2)*3 = |1-2| * 3 = 1*3 = |1-3| = 2$
$1*(2*3) = 1*|2-3| = 1*1 = |1-1| = 0$ $\Big\}$ $\Rightarrow$ grupoid není asociativní

b) $\forall a, b \in \mathbb{R}: \quad a*b = |a-b| = |b-a| = b*a \Rightarrow$ grupoid je komutativní

$\Rightarrow$ Existují grupoidy, které nejsou asociativní, ale jsou komutativní.

4.) Určete inverzní prvky (pokud existují) všech prvků množiny $G = \{1,2,3,4\}$ v grupoidu $(G, \cdot)$, který je dán tabulkou:

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	1	1	1
3	3	1	1	4
4	4	2	3	4

$1 \cdot 1 = 1 \quad \} \Rightarrow \underline{\underline{1^{-1} = 1}}$

$\left.\begin{array}{l} 2 \cdot 2 = 1 \\ 2 \cdot 3 = 3 \cdot 2 = 1 \\ 2 \cdot 4 = 1 \text{ ale } 4 \cdot 2 \neq 1 \end{array}\right\} \Rightarrow \underline{\underline{2^{-1} = 2 \text{ a také } 2^{-1} = 3}}$

$3 \cdot 2 = 2 \cdot 3 = 1 \quad \} \Rightarrow \underline{\underline{3^{-1} = 2}}$

$2 \cdot 4 = 1$ ale $4 \cdot 2 \neq 1$ } $\Rightarrow$ $\underline{\underline{4^{-1} \text{ neexistuje}}}$

$\Rightarrow$ V grupoidu mohou existovat prvky, které inverzi nemají i prvky, které mají jediný inverzní prvek i prvky, které mají více inverzních prvků.

Př: Definujme na $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x \geq 0\}$ operaci $*$:

$$x * y = \sqrt{x^2 + y^2}$$

Určete všechny prvky grupoidu $(\mathbb{R}^+, *)$, které mají inverzi.

Řešení: Neutrálním prvkem je $e = 0$ neboť $\forall a \in \mathbb{R}^+$: $0 * a = \sqrt{0^2 + a^2} = \sqrt{a^2} = |a| = a$

$a * 0 = \sqrt{a^2 + 0^2} = \sqrt{a^2} = |a| = a$

Prvek $a \in \mathbb{R}^+$ má inverzi $\Leftrightarrow \exists x \in \mathbb{R}^+ : a * x = x * a = 0$

$$a * x = \sqrt{a^2 + x^2} = 0 \Leftrightarrow a = x = 0$$
$$x * a = \sqrt{x^2 + a^2} = 0 \Leftrightarrow a = x = 0$$

$\underline{\underline{\text{Pouze prvek } a = 0 \text{ má v } (\mathbb{R}^+, *) \text{ inverzi.}}}$

Grupy

1.) Nechť $G = \{1, -1, i, -i\}$, kde $i = \sqrt{-1}$. Dokažte, že $(G, \cdot)$, kde $\cdot$ je restrikce obvyklého násobení komplexních čísel na G, je grupa.

Řešení: Platnost axiomů grupy ověříme pomocí tabulky násobení v G:

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

1.) $\forall a,b \in G: \quad a \cdot b \in G \quad \checkmark$

2.) Násobení komplexních čísel je asociativní a $G \subseteq \mathbb{C} \Rightarrow$

$\forall a,b,c \in G: \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$

3.) $\forall a \in G: \quad a \cdot 1 = 1 \cdot a = a \quad \Rightarrow 1 \in G$ je neutrálním prvkem v G.

4.)
$$\left.\begin{aligned} 1 \cdot 1 &= 1 \\ -1 \cdot (-1) &= 1 \\ i \cdot (-i) &= (-i) i = 1 \end{aligned}\right\} \Rightarrow \left.\begin{aligned} 1^{-1} &= 1 \\ (-1)^{-1} &= -1 \\ (i)^{-1} &= -i \\ (-i)^{-1} &= i \end{aligned}\right\} \Rightarrow$$

$$\forall a \in G \; \exists a^{-1} \in G: \quad a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

$\Rightarrow$ $(G, \cdot)$ je grupa

Př.: Nechť $G = \{ z \in \mathbb{C} \mid z^8 = 1 \}$ a $\cdot$ je restrikce obvyklého násobení komplexních čísel na G. Dokažte, že $(G, \cdot)$ je grupa.

Důkaz: Víme, že $G = \{ 1 \cdot (\cos(0 + \frac{2\pi}{8}k) + i \sin(0 + \frac{2\pi}{8}k)) \mid k \in \{0,1,\dots,7\} \} =$

$$= \{ (\cos(k\tfrac{\pi}{4}) + i \sin(k\tfrac{\pi}{4})) \mid k \in \mathbb{Z} \}$$

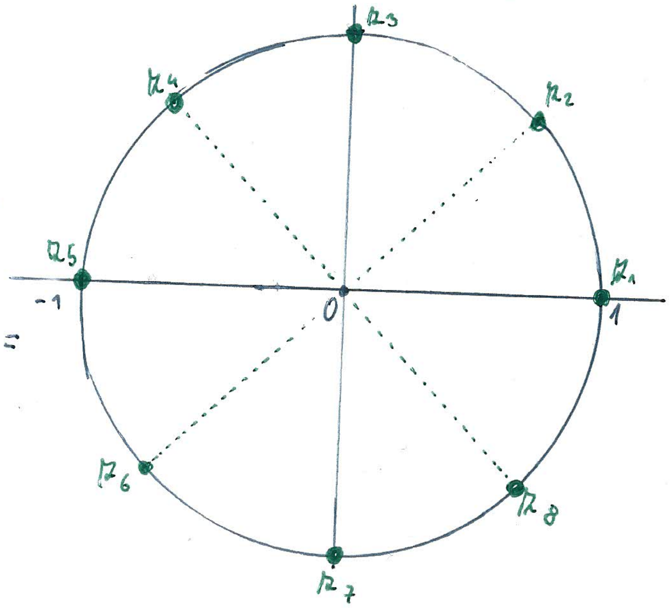
1.) $\forall z_{k_1} = (\cos(k_1\frac{\pi}{4}) + i \sin(k_1\frac{\pi}{4})) \in G$ a
$\forall z_{k_2} = (\cos(k_2\frac{\pi}{4}) + i \sin(k_2\frac{\pi}{4})) \in G$:

$$z_{k_1} \cdot z_{k_2} = (\cos((k_1+k_2)\tfrac{\pi}{4}) + i \sin((k_1+k_2)\tfrac{\pi}{4})) =$$

$$= \cos(k\tfrac{\pi}{4}) + i \sin(k\tfrac{\pi}{4}),$$

kde $k \in \{0,1,\dots,7\}$ $\Rightarrow$

$z_{k_1} \cdot z_{k_2} \in G$



2.) Asociativita $\cdot$ na G plyne z asociativity $\cdot$ na $\mathbb{C}$ a toho, že $G \subseteq \mathbb{C}$:
$\forall a,b,c \in \mathbb{C}: (a \cdot b) \cdot c = a \cdot (b \cdot c) \Rightarrow \forall a,b,c \in G: (a \cdot b) \cdot c = a \cdot (b \cdot c)$

3.) Neutrálním prvkem na G je $1 = \cos 0 + i \sin 0$:
$\forall z = \cos(k\frac{\pi}{4}) + i \sin(k\frac{\pi}{4})$: $(\cos 0 + i \sin 0) \cdot \underbrace{(\cos(k\frac{\pi}{4}) + i \sin(k\frac{\pi}{4}))}_{z} =$

$$\underbrace{(\cos(k\tfrac{\pi}{4}) + i \sin(k\tfrac{\pi}{4}))}_{z} \cdot (\cos 0 + i \sin 0) = z$$

4.) $\forall z = \cos(k\frac{\pi}{4}) + i \sin(k\frac{\pi}{4}) \in G \ \exists z^{-1} = \cos((8-k)\frac{\pi}{4}) + i \sin((8-k)\frac{\pi}{4}) \in G$:

$$z^{-1} \cdot z = z \cdot z^{-1} = \cos(k\tfrac{\pi}{4} + (8-k)\tfrac{\pi}{4}) + i \sin(k\tfrac{\pi}{4} + (8-k)\tfrac{\pi}{4}) =$$

$$= \cos(8\tfrac{\pi}{4}) + i \sin(8\tfrac{\pi}{4}) = \cos 0 + i \sin 0 = 1$$

$\square$

2.) Nechť $G = \{ a + b\sqrt{2} \in \mathbb{R} - \{0\} \mid a, b \in \mathbb{Q} \}$ a $\cdot$ je restrikce obvyklého násobení reálných čísel na G. Dokažte, že $(G, \cdot)$ je grupa.

1.) Uzavřenost:

$\forall (a_1 + b_1\sqrt{2}), (a_2 + b_2\sqrt{2}) \in G$:

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = \underbrace{a_1 a_2 + b_1 b_2 2}_{\in \mathbb{Q}} + \underbrace{(b_1 a_2 + a_1 b_2)}_{\in \mathbb{Q}}\sqrt{2} \in G$$

2.) Asociativnost:

Násobení reálných čísel je asociativní a $G \subseteq \mathbb{R}$. Proto i násobení v G je asociativní.

3.) Neutrální prvek:

$1 = 1 + 0 \cdot \sqrt{2} \in G$ a $\forall a + b\sqrt{2} \in G$: $1(a + b\sqrt{2}) = (a + b\sqrt{2}) \cdot 1 = a + b\sqrt{2}$

$\Rightarrow$ 1 je neutrálním prvkem v G.

4.) Inverzní prvky:

$\forall a + b\sqrt{2} \in G$:

$$\underbrace{(a + b\sqrt{2})}_{\neq 0}\underbrace{(a - b\sqrt{2})}_{\neq 0} = \underbrace{a^2 - 2b^2}_{\neq 0} \qquad / : (a^2 - 2b^2) \neq 0$$

$$(a + b\sqrt{2})\left(\frac{a - b\sqrt{2}}{a^2 - 2b^2}\right) = 1$$

$$(a + b\sqrt{2})\left(\underbrace{\frac{a}{a^2 - 2b^2}}_{\in \mathbb{Q}} + \underbrace{\frac{-b}{a^2 - 2b^2}}_{\in \mathbb{Q}}\sqrt{2}\right) = 1$$

(navíc násobení je komutativní)

$$\Rightarrow \exists (a + b\sqrt{2})^{-1} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \in G$$

$\Rightarrow$ $(G, \cdot)$ je grupa

3.) Na množině $\mathbb{Z}_4 = \{0,1,2,3\}$ definujme operaci $\oplus$ následovně:

$$a \oplus b = \begin{cases} a+b \iff a+b<4 \\ a+b-4 \iff a+b \geq 4 \end{cases}$$

(+ je obvyklé sčítání celých čísel)

Zjistěte, zda $(\mathbb{Z}_4, \oplus)$ je grupa.

Řešení: Platnost axiomů grupy ověříme pomocí tabulky

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

1.) Uzavřenost: $\forall a,b \in \mathbb{Z}_4 : a \oplus b \in \mathbb{Z}_4$

2.) Asociativnost: $\forall a,b,c \in \mathbb{Z}_4 :$ $a \oplus b = a+b-k_1 4$, kde $k_1 \in \{0,1\}$

$b \oplus c = b+c-k_2 4$, kde $k_2 \in \{0,1\}$

$$a \oplus (b \oplus c) = a+b+c+k_1^* 4$$
$$(a \oplus b) \oplus c = a+b+c+k_2^* 4$$

(chceme dokázat, že $k_1^* = k_2^*$)

kde $k_1^*, k_2^* \in \mathbb{Z}$ splňují:

$$0 \leq a+b+c+k_1^* 4 < 4$$
$$0 \leq a+b+c+k_2^* 4 < 4 \quad / \cdot (-1)$$

$$0 \leq a+b+c+k_1^* 4 < 4$$
$$-4 < -a-b-c-k_2^* 4 \leq 0 \quad / \text{sečteme}$$

$$-4 < \underbrace{(k_1^* - k_2^*)}_{\in \mathbb{Z}} 4 < 4$$

(jediný násobek čtyřky splňuje, že je mezi -4 a 4 : nula násobek)

$$k_1^* - k_2^* = 0 \Rightarrow k_1^* = k_2^*$$

3. Neutrální prvek: $e = 0$

3. Inverzní prvky: $0^{-1} = 0$, $1^{-1} = 3$, $2^{-1} = 2$, $3^{-1} = 1$ Obvykle zapisujeme $-0=0$, $-1=3$, $-2=2$, $-3=1$

$\Rightarrow$ $\underline{\underline{(\mathbb{Z}_4, \oplus) \text{ je grupa}}}$

($(\mathbb{Z}_4 - \{0\}, \odot)$ ← násobení modulo 4; grupa není

$\odot$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

1.) není uzavřená

2.) 2 nemá inverzi)

Examples of groups of numbers

Example 1: *The additive group of integers.*

I. Let Z be the set of integers.

II. Let $+$ be the binary operation of addition in Z.

III. $n+0 = n = 0+n$ for every $n \in Z$. Thus $(Z,+)$ has an identity element.

IV. If l, m, n are integers,

$$(l+m)+n = l+(m+n)$$

i.e. $(Z,+)$ is a semigroup.

V. If $n \in Z$, then $-n$ in Z has the property

$$n+(-n) = 0 = (-n)+n$$

i.e. $-n$ is an inverse of n in $(Z,+)$.

Thus we have shown that the groupoid $(Z,+)$ is a group. This group is usually referred to as the *additive group of integers.*

Example 2: *The additive group of rationals.*

I. Let Q be the set of rational numbers.

II. Let $+$ be the binary operation of addition in Q.

III. $a+0 = a = 0+a$ for every $a \in Q$, so 0 is an identity element for $(Q,+)$.

IV. If $a, b, c \in Q$, then $(a+b)+c = a+(b+c)$.

V. If $a \in Q$, then $-a$ in Q has the property $a+(-a) = 0 = (-a)+a$.

Example 3: *The additive group of complex numbers.*

The description of this group is left to the reader.

Example 4: *The multiplicative group of nonzero rationals.*

I. Let Q^* be the set of nonzero rational numbers.

II. Let $\cdot$ be the binary operation of multiplication, i.e. the usual multiplication of rational numbers.

III. The rational number 1 is clearly an identity in the groupoid $(Q^*, \cdot)$.

IV. If $a, b, c \in Q^*$, then

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

V. If $z \in Q^*$, so is $1/a$ and

$$a \cdot \frac{1}{a} = 1 = \frac{1}{a} \cdot a$$

Thus every element of Q^* has an inverse.

Example 5: *The multiplicative group of nonzero complex numbers.*

This group is very similar to that in Example 4. We shall go through the usual five stages in setting up and describing the group.

I. Let C^* be the set of all nonzero complex numbers. Thus

$$C^* = \{x \mid x = a+ib \text{ where } x \neq 0+i0 \text{ and } a, b \in R\}$$

Recall that $i^2 = -1$.

II. We define multiplication of complex numbers as follows:

$$(a+ib)(c+id) = (ac-bd)+i(ad+bc)$$

This is a binary operation in C^* since $(ac-bd)+i(ad+bc)$ is a unique element in C^* (not both $ac-bd$ and $ad+bc$ can be zero).

III. $1+i \cdot 0 = 1 \in C^*$ and it is clearly an identity in $(C^*, \cdot)$.

IV. Suppose $a+ib,\ c+id,\ e+if \in C^*$. Then

$$\begin{aligned}[(a+ib)(c+id)](e+if) &= [(ac-bd)+i(bc+ad)](e+if)\\ &= [(ac-bd)e-(bc+ad)f] + i[(bc+ad)e+(ac-bd)f]\end{aligned}$$

On the other hand,

$$\begin{aligned}(a+ib)[(c+id)(e+if)] &= (a+ib)[(ce-df)+i(de+cf)]\\ &= [a(ce-df)-b(de+cf)] + i[b(ce-df)+a(de+cf)]\end{aligned}$$

It follows from these two computations that

$$(a+ib)[(c+id)(e+if)] = [(a+ib)(c+id)](e+if)$$

V. We have to check the existence of inverses. Thus suppose $a+ib \in C^*$; then not both a and b are zero. Hence $a^2+b^2 \neq 0$ and so

$$\frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2} \in C^*$$

Moreover,

$$\left(\frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}\right)(a+ib) = 1 = (a+ib)\left(\frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}\right)$$

Thus we have proved $(C^*,\cdot)$ is a group and we term this group the multiplicative group of nonzero complex numbers.

Problems

3.1. Is $(S,\circ)$ a group if

(i) $S=Z$ and $\circ$ is the usual multiplication of integers?

(ii) $S=Q$ and $\circ$ is the usual multiplication in Q?

(iii) $S=\{q \mid q\in Q \text{ and } q>0\}$ and $\cdot$ is the usual multiplication of rational numbers?

(iv) $S=\{z \mid z\in Z \text{ and } z=\sqrt{2}\}$ and $\circ$ is the usual multiplication in Z?

(v) $S=R$ and $\circ$ is the usual addition of real numbers?

(vi) $S=Z$ and $\circ$ is defined by $a\circ b=0$ for all a,b in Z?

Solutions:

(i) The identity element is the integer 1. $(S,\circ)$ is not a group because $5\in Z$ but there is no *integer* z in Z such that $z\circ 5 = 5\circ z = 1$.

(ii) Again the identity is the number 1. There is no $q\in Q$ such that $q\circ 0=1$. Hence $(S,\circ)$ is not a group.

(iii) $(S,\cdot)$ is a group. Clearly $S\neq\emptyset$ and $\cdot$ is a binary operation on S. $q\cdot 1 = 1\cdot q = q$ for all $q\in S$; hence 1 is an identity. Multiplication of rational numbers is associative and every element in S has an inverse; for if $q\in S$, then $\frac{1}{q}\in S$ and $\frac{1}{q}\cdot q = 1 = q\cdot\frac{1}{q}$.

(iv) $S=\emptyset$ since $\sqrt{2}\notin Z$. Therefore $(S,\circ)$ is not a group.

(v) $(S,\circ)$ is a group. $S\neq\emptyset$ and addition is an associative binary operation on S. $r+0=0+r=r$ and $r+(-r)=0=(-r)+r$ for all $r\in S$.

(vi) $(S,\circ)$ is not a group because there is no identity element in S.

3.2. Let S be the set of even integers. Show that S is a group under addition of integers.

Solution:

Let $a=2a_1$ and $b=2b_1$ be any two elements in S. $a+b=2(a_1+b_1)$ is a unique element in S; thus addition is a binary operation on S. Associativity of addition in S follows from the associativity of addition in Z. $0=2\cdot 0$ is an identity element in S. If $a\in S$, then $-a\in S$ since $a=2a_1$ implies $-a=2(-a_1)$. Hence a has an inverse in S, as $a+(-a)=(-a)+a=0$.

3.3. Let S be the set of real numbers of the form $a+b\sqrt{2}$ where $a,b\in Q$ and are not simultaneously zero. Show that S becomes a group under the usual multiplication of real numbers.