4. Grupy, okruhy, pole Verze 335.

Dostáváme se k nejjednodušším algebraickým strukturám. Nejprve studujeme *Grupu* množinu s jednou operací, dále její podgrupy a *homomorfismy* — zobrazení zachovávající grupové operace. Zmiňujeme nejdůležitější příklady grup a jejich podgrup.

Dále se zmiňujeme o *okruhu*, a na závěr je zařazen odstavec věnující se *poli*, složitější avšak přirozené algebraické struktuře.

Binární operací na množině M rozumíme každé zobrazení z $M \times M$ do M. Je-li $\circ$ relace na M, její hodnotu na prvcích $x, y \in M$ značíme $x \circ y$. Operace $\circ$ se nazývá *komutativní*, jestliže pro každé $x, y \in M$ platí

$$x \circ y = y \circ x, \qquad \text{(komutativita)} \tag{4.1}$$

asociativní, jestliže pro každé $x, y, z \in M$ platí

$$(x \circ y) \circ z = x \circ (y \circ z). \qquad \text{(asociativita)} \tag{4.2}$$

Nechť $+$ a $\circ$ jsou dvě operace na M, řekneme, že operace $\circ$ je *distributivní* vzhledem k operaci $+$, jestliže pro každé $x, y, z \in M$ platí

$$\begin{aligned} x \circ (x + z) &= (x \circ y) + (x \circ z), \\ (x + y) \circ z &= (x \circ z) + (y \circ z). \end{aligned} \qquad \text{(distributivita)} \tag{4.3}$$

Podmnožina $A \subset M$ se nazývá *uzavřená* vzhledem k operaci f na M, jestliže zúžení $f|_{A\times A}$ je operace na A.[1)]

4.1 Grupa. Nejjednodušší struktura, o které se zde zmíníme, je grupa. Nechť G je množina a $\circ$ operace na ní. Množině G s touto operací říkáme *grupa*, jestliže
1) operace $\circ$ je asociativní;
2) existuje *neutrální prvek* tedy $e \in G$ takové, že pro každé $x \in G$ platí[2)]

$$x \circ e = e \circ x = x; \qquad \text{(neutralita } e\text{)} \tag{4.4}$$

3) pro každé $x \in G$ existuje prvek $x^{-1} \in G$ takový, že

$$x \circ x^{-1} = x^{-1} \circ x = e. \qquad \text{(inverzní prvek)} \tag{4.5}$$

Prvek x^{-1} se nazývá *inverze* prvku x.

Věta 4.1. *1. V každé grupě existuje jediný neutrální prvek.*
2. Inverzní prvek k prvku x je určen jednoznačně.
D ů k a z. 1. Předpokládejme, že existují dva neutrální prvky e_1 a e_2. Využitím neutrality e_1 a e_2 spolu s asociativitou operace $\circ$ máme

[1)] Zde se jedná o to, zda platí $f(A \times A) \subset A$. Pokud ano je možné udělat zúžení definičního oboru na $A \times A$ a zúžení oboru hodnot na A. Tím dostaneme operaci na A.

[2)] Pro následující podmínku potřebujeme jednoznačnost neutrálního prvku. To nám zaručuje věta 4.1.

$$e_1 = e_1 \circ (e_2 \circ e_2) = (e_1 \circ e_2) \circ e_2 = e_2.$$

Tedy $e_1 = e_2$. Neutrální prvek je tedy jedinečný.

2. Podobně jako v předchozím tvrzení předpokládejme, že y a z jsou dvě inverze prvku x.

$$y = y \circ e = y \circ (x \circ z) = (y \circ x) \circ z = e \circ z = z.$$

Dostali jsme, že $y = z$, což znamená jednoznačnost inverze x.

Jen díky platnosti tvrzení 2. předchozí věty jsme si mohli dovolit uvést značení x^{-1} pro inverzní prvek k x. Kdyby tomu tak nebylo, nebylo by jasné, který z inverzních prvků x^{-1} označuje.

Příkladem grupy je $\mathbb{R}$ spolu s operací $+$, samozřejmě že neutrálním prvkem je 0 a inverzí k x je opačný prvek tedy $-x$. Tuto grupu nazýváme *aditivní grupa reálných čísel*.

Dalším příkladem grupy je *multiplikativní grupa reálných čísel*, jedná se o množinu $\mathbb{R} \setminus \{0\}$ na níž uvažujeme operaci $\cdot$ (násobení). Neutrálním prvkem (v tomto případě častěji užíváme pojem *jednotkový prvek*) je zde 1 a inverzním prvkem k x je převrácená hodnota $1/x$.

Snadno se přesvědčíme, že jsme z multiplikativní grupy reálných čísel museli vyloučit 0. Jinak by totiž k ní v $\mathbb{R}$ musel existovat inverzní prvek, což by dost dobře nešlo.

Zaveďme na množině $\mathbb{R}^2$ operaci sčítání (označme ji $+$) tak že $(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$ (*sčítání po složkách*). Množina $\mathbb{R}^2$ vybavena touto operací tvoří také grupu. Jednotkovým prvkem zde bude $(0, 0)$ a opačným prvkem k prvku (x_1, x_2) je samozřejmě $(-x_1, -x_2)$. Obdobně můžeme přirozeným způsobem zavést strukturu grupy na $\mathbb{R}^n$ pro libovolné přirozené n.

Grupa se nazývá *komutativní* (*Abelova*) je-li její operace komutativní.

Množina všech regulárních matic typu n/n nad polem $\mathbb{R}$ (případně nad $\mathbb{C}$) s operací násobení matic je grupa. Nazveme ji *obecná lineární grupa*. Označujeme ji $\mathrm{GL}(n, \mathbb{R})$ (případně $\mathrm{GL}(n, \mathbb{C})$). Tato grupa na rozdíl od všech výše uvedených je nekomutativní (přesvědčte se).

Věta 4.2. *Necht'G s $\circ$ je grupa, e její neutrální prvek. Potom platí*
1. $e^{-1} = e$.
2. Pro libovolné $x, y \in G$ *je* $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$.
3. $(x^{-1})^{-1} = x$.
D ů k a z. 1. Pro e^{-1} platí:

$$e^{-1} = e^{-1} \circ e = e.$$

2. Ověříme, že prvek $y^{-1} \circ x^{-1}$ je inverzním prvkem k $x \circ y$. Tedy

$$(x \circ y) \circ (y^{-1} \circ x^{-1}) = (x \circ (y \circ y^{-1})) \circ x^{-1} = (x \circ e) \circ x^{-1} = x \circ x^{-1} = e.$$

a

$$(y^{-1} \circ x^{-1}) \circ (x \circ y) = (y^{-1} \circ (x^{-1} \circ x)) \circ y = (y^{-1} \circ e) \circ y) = y^{-1} \circ y) = e.$$

3. Musíme prověřit, že x je inverzním prvkem k x^{-1}. To je ale evidentní.

Věta 4.3. *Je-li G grupa,* $a, b \in G$ *libovolné prvky. Potom rovnice* $a \circ x = b$, $y \circ a = b$ *mají v G jednoznačné řešení vzhledem k* x, y.
D ů k a z. Dokážeme větu pro rovnici $a \circ x = b$, druhý případ se udělá obdobně. Hledaným prvkem grupy, který splňuje danou rovnici je $x = a^{-1} \circ b$. Protože $a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = b$.

Nyní předpokládejme, že existují dva prvky $x_1, x_2 \in G$ splňující naši rovnici. Tedy platí jednak $a \circ x_1 = b$ a jednak $a \circ x_2 = b$. To znamená, že se rovnají levé strany těchto rovnic.

$$\begin{aligned} a \circ x_1 &= a \circ x_2 \\ a^{-1} \circ (a \circ x) &= a^{-1} \circ (a \circ x) \\ x_1 &= x_2 \end{aligned}$$

Tedy naše rovnice má jediné řešení.

Je-li G Abelova grupa zavádíme operaci, která prvkům x, y přiřadí prvek $x \circ y^{-1}$. (*Odčítání*, případně *dělení*). Podmnožina A grupy G se nazývá *podgrupa* jestliže A je grupa vzhledem k operaci na G.

Věta 4.4. *Podmnožina $A \subset G$ je podgrupa grupy G s operací $\circ$, jestliže je uzavřená vzhledem k operaci $\circ$ a inverzi. (Tedy pokud pro každé $x, y \in A$ platí $x \circ y \in A$ a $x^{-1} \in A$).*
D ů k a z. Stačí ověřit, že A splňuje podmínky grupy. To je ale jednoduché.

Věta 4.5. *1. Jestliže je G' podgrupa G a G'' je podgrupa G', pak je G'' podgrupou G.*
2. Průnikem libovolného systému podgrup grupy G je opět podgrupa G.
3. Podgrupa Abelovy grupy je Abelova.
D ů k a z. Body 1. a 3. jsou triviální.

2. Nechť S je systém podgrup grupy G s operací $\circ$. Vezměme si libovolná $x, y \in \cap S$, dokážeme, že $x \circ y \in \cap S$. Protože $x, y \in \cap S$ leží $x, y \in G'$, pro každé $G' \in S$. Podgrupa G' je uzavřená vzhledem k operaci $\circ$, proto $x \circ y \in G'$. To znamená $x \circ y \in \cap S$.

Obdobně pro x^{-1}. Mějme $x \in \cap S$, to znamená, že $x \in G'$, pro každé $G' \in S$. Podgrupa G' ale musí obsahovat x^{-1}. To znamená, že jej obsahují všechny prvky z S. Proto $x^{-1} \in \cap S$.

4.2 Homomorfismus. Nechť G_1 s operací $\circ$ je grupa a G_2 s operací $*$ je grupa. Zobrazení $f: G_1 \to G_2$ se nazývá *homomorfismus*, jestliže pro každé $a, b \in G_1$ platí

$$f(a \circ b) = f(a) * f(b). \tag{4.6}$$

Bijektivní homomorfismus se nazývá *izomorfismus*. Množinu

$$\ker f = \{x \in G_1 \mid f(x) = e_2\}, \tag{4.7}$$

kde e_2 označuje jednotkový prvek v G_2, nazýváme *jádro homomorfismu* f. Zopakujme pojem obraz zobrazení, je to množina

$$\operatorname{Im} f = f(G_1) = \{x' \in G_2 \mid \text{existuje } x \in G_1, \text{ tak, že } f(x) = x'\} = \{f(x) \mid x \in G_1\}.$$

Je-li f homomorfismus, pak Im f říkáme *obraz homomorfismu* f.

Buďte G_1, G_2 dvě grupy a e_2 nechť označuje jednotkový prvek v G_2. Definujeme zobrazení $f: G_1 \to G_2$ tak, že položíme $f(x) = e_2$ pro všechna $x \in G_1$. Toto zobrazení je homomorfismus, skutečně

$$f(x \circ y) = e_2,$$

stejně jako

$$f(x) * f(y) = e_2 * e_2 = e_2.$$

V tomto případě je $\ker f = G_1$ a Im $f = \{e_2\}$.

Uvažujme aditivní grupu reálných čísel $\mathbb{R}$ a grupu $\mathbb{R}^+$ s operací násobení (ověřte, že se skutečně jedná o grupu). Exponenciální funkce $\exp: \mathbb{R} \to \mathbb{R}^+$ je homomorfismus těchto grup. Skutečně, platí

$$\exp(x + y) = \exp(x) \cdot \exp(y).$$

A jelikož je exp bijektivní jedná se o izomorfismus těchto grup.

Označme $\mathcal{M}_2$ množinu matic $2/2$ s prvky z množiny $\mathbb{R}$. To že $\mathcal{M}_2$ je se sčítáním matic grupa je snad jasné. Na

této množině definujeme zobrazení $f: \mathcal{M} \to \mathbb{R}^4$ tak, že položíme $f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = (a, b, c, d)$. Již víme, že $\mathbb{R}^4$ se sčítáním „po složkách“ je grupa. Není těžké ověřit, že právě definované f je izomorfismus těchto grup.

Věta 4.6. *Bud' $f: G_1 \to G_2$ homomorfismus grup G_1 a G_2.*
1. Obrazem jednotkového prvku z grupy G_1 při f je jednotkový prvek v G_2.
2. Obrazem inverzního prvku $x^{-1} \in G_1$ je inverzní prvek k prvku $f(x)$ v G_2. To znamená, že

$$f(x^{-1}) = (f(x))^{-1}.$$

D ů k a z. Označme e_1 jednotkový prvek v G_1 a e_2 jednotkový prvek G_2.

1. Z definice jednotkového prvku je nutné ověřit, že pro každý prvek $x_2 \in G_2$ platí $x_2 * f(e_1) = f(e_1) * x_2 = x_2$. Z jedinečnosti neutrálního prvku v G_2 vyplyne $e_2 = f(e_1)$. Platí

$$f(e_1) = f(e_1 \circ e_1) = f(e_1) * f(e_1) \tag{4.8}$$

a tím pádem

$$x_2 * f(e_1) = x_2 * (f(e_1) * f(e_1)). \qquad \text{(podle (4.8))}$$

Odtud

$$(x_2 * f(e_1)) * (f(e_1))^{-1} = (x_2 * f(e_1)) * (f(e_1) * (f(e_1))^{-1})$$

a tedy

$$x_2 = x_2 * f(e_1).$$

Důkaz rovnosti $x_2 = f(e_1) * x_2$ je obdobný a proto jej vynecháme.

2. Ověřme, že $f(x)$ je inverze k $f(x^{-1})$ v grupě G_2.

$$\begin{aligned} f(x) * f(x^{-1}) &= f(x \circ x^{-1}) = && \text{(homomorfismus)} \\ &= f(e_1) = e_2. && \text{(bod 1. této věty)} \end{aligned}$$

Rovnost $f(x^{-1}) * f(x) = e_2$ se dokáže obdobně.

Věta 4.7. *Jádro homomorfismu $f: G_1 \to G_2$ je podgrupa v G_1 a obraz homomorfismu f je podgrupa v G_2.*
D ů k a z. Nejprve dokážeme, že $\ker f$ je podgrupa v G_1. Podle věty 4.4 musíme ověřit, že pro každé $x, y \in \ker f$ je $x \circ y \in \ker f$ a $x^{-1} \in \ker f$. To, že $x, y \in \ker f$, znamená, že $f(x) = e_2$ a $f(y) = e_2$. Počítejme

$$f(x \circ y) = f(x) * f(y) = e_2 \circ e_2 = e_2.$$

To znamená, že $x \circ y \in \ker f$. Nyní ověříme, že $x^{-1} \in \ker f$.

$$\begin{aligned} f(x^{-1}) &= (f(x))^{-1} = && \text{(věta 4.6)} \\ &= e_2^{-1} = e_2. \end{aligned}$$

Proto $x^{-1} \in \ker f$.

Nyní dokážeme, že $\operatorname{Im} f$ je podgrupa G_2. Zvolme libovolně $f(x)$, $f(y) \in \operatorname{Im} f$, obdobně jako v první polovině důkazu dokážeme, že $f(x) * f(y) \in \operatorname{Im} f$ a $(f(x))^{-1} \in \operatorname{Im} f$. Zobrazení f je homomorfismus, tudíž

$$f(x) * f(y) = f(x \circ y).$$

Tedy na prvek $f(x) * f(y)$ se zobrazí $x \circ y \in G_1$, proto $f(x) * f(y) \in \operatorname{Im} f$.

$$(f(x))^{-1} = f(x^{-1}). \qquad \text{(opět věta 4.6)}$$

To znamená, že se na $(f(x))^{-1}$ zobrazí $x^{-1} \in G_1$, a proto $(f(x))^{-1} \in \operatorname{Im} f$.

Věta 4.8. *Složení homomorfismů je homomorfismus.*
D ů k a z. Nechť $f: G_1 \to G_2$ je homomorfismus grupy G_1 s operací $\circ$ a grupy G_2 s operací $*$, dále $h: G_2 \to G_3$ je homomorfismus G_2 a grupy G_3 s operací $\cdot$. Dokážeme, že $g \circ f$ je homomorfismus.

Ukážeme, že pro libovolné prvky $x, y \in G_1$ platí $(g \circ f)(x \circ y) = (g \circ f)(x) \cdot (g \circ f)(y)$.

$$\begin{aligned}
&(g \circ f)(x \circ y) = g(f(x \circ y)) = && \text{(definice složeného zobrazení)}\\
&\quad = g(f(x) * f(y)) = && (f \text{ je homeomorfismus})\\
&\quad = g(f(x)) \cdot g(f(x)) = && (g \text{ je homeomorfismus})\\
&\quad = (g \circ f)(x) \cdot (g \circ f)(y). && \text{(opět definice složeného zobrazení)}
\end{aligned}$$

Důsledek 4.9. *Složení izomorfismů je izomorfismus.*
D ů k a z. Plyne z předchozí věty a z toho, že složení bijekcí je bijekce (pro důkaz viz větu 1.6 v [2]).

O dvou grupách G_1, G_2 řekneme, že jsou izomorfní, jestliže existuje izomorfismus $f: G_1 \to G_2$. Tuto skutečnost značíme $G_1 \approx G_2$.

Věta 4.10. *Relace $\approx$ na množině všech grup je relace ekvivalence.*
D ů k a z. Nejprve ověříme, že $\approx$ je reflexivní. Je-li G grupa, pak $\mathrm{id}_G: G \to G$ (identita na G) je izomorfismus (ověřte!).

Nyní symetrie $\approx$. Jsou-li G_1, G_2 izomorfní, tedy existuje-li izomorfismus $f: G_1 \to G_2$, pak jeho inverze je izomorfismus G_2 a G_1. Stačí ověřit (proč?), že f^{-1} je homomorfismus G_2 a G_1. Zvolme $y_1, y_2 \in G_2$, $\circ$ je operace na G_1 a $*$ je operace na G_2. Máme

$$\begin{aligned}
&f^{-1}(y_1 * y_1) = f^{-1}(f(f^{-1}(y_1)) * f(f^{-1}(y_2))) =\\
&\quad = f^{-1}(f(f^{-1}(y_1) \circ f^{-1}(y_2))) = && (f \text{ je homomorfismus})\\
&\quad = f^{-1}(y_1) \circ f^{-1}(y_2). && (f^{-1} \circ f = \mathrm{id}_{G_1})
\end{aligned}$$

Nakonec tranzitivita $\approx$. Nechť $G_1 \approx G_2$ a $G_2 \approx G_3$. Tedy existují izomorfismy $f: G_1 \to G_2$ a $g: G_2 \to G_3$. Hledaným izomorfismem, který ukáže, že $G_1 \approx G_3$, je zobrazení $f \circ g$. To je izomorfismus podle důsledku 4.9.

Uvažujme množinu $\mathbb{Z}$ a na ní operaci sčítání. Snadno se ověří, že spolu tvoří Abelovu grupu.

Dále pro pevné $n \in \mathbb{N}$ označme $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ na této množině definujeme sčítání $x + y \pmod n$. Stejně tak definujeme na $\mathbb{Z}_n$ i násobení. Například pro $\mathbb{Z}_3$ vypadají tabulky pro sčítání a násobení modulo 3 následovně.

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	2	2	1

Grupa $\mathbb{Z}_3$, stejně jako ostatní $\mathbb{Z}_n$ grupy, ale není podgrupou $\mathbb{Z}$, je sice podmnožinou $\mathbb{Z}$, ovšem operace na nich se liší.

Podgrupy obecné lineární grupy $\mathrm{GL}(n, \mathbb{R})$

Ortogonální grupa $\mathrm{O}(n) = \{A \in \mathrm{GL}(n, \mathbb{R}) \mid A \cdot A^\top = E\}$, matice splňující podmínku $A^{-1} = A^\top$ se nazývají *ortogonální matice*. Jelikož $\det A = \det A^\top$, je jasné, že pro ně platí $\det A = \pm 1$.

Speciální lineární grupa $\mathrm{SL}(n,\mathbb{R}) = \{A \in \mathrm{GL}(n,\mathbb{R}) \mid \det A = 1\}$. Tato grupa je také podgrupou ortogonální grupy.

Podgrupy obecné lineární grupy $\mathrm{GL}(n,\mathbb{C})$

Unitární grupa $\mathrm{U}(n) = \{A \in \mathrm{GL}(n,\mathbb{C}) \mid A \cdot A^{\top *} = E\}$, matice splňující podmínku $A^{-1} = A^{\top *}$ se nazývají *unitární matice*. Jelikož $\det A = \det A^{\top}$, platí, že $|\det A| = 1$. To znamená, že $\det A$ leží na jednotkové kružnici v komplexní rovině.

Speciální lineární grupa $\mathrm{SL}(n,\mathbb{C}) = \{A \in \mathrm{GL}(n,\mathbb{C}) \mid \det A = 1\}$. Tato grupa je také podgrupou unitární grupy.

Vztahy těchto grup ilustruje následující diagram.

$$\begin{array}{ccccc} \mathrm{SL}(n,\mathbb{R}) & \subset & \mathrm{O}(n) & \subset & \mathrm{GL}(n,\mathbb{R}) \\ \cap & & \cap & & \cap \\ \mathrm{SL}(n,\mathbb{C}) & \subset & \mathrm{U}(n) & \subset & \mathrm{GL}(n,\mathbb{C}) \end{array}$$

Zobrazení determinant z grupy $\mathrm{GL}(n,\mathbb{R})$ do multiplikativní grupy reálných čísel $\mathbb{R} \setminus \{0\}$ s operací násobení je homomorfismus těchto grup. Skutečně, platí $\det(A \cdot B) = \det A \cdot \det B$. Jeho jádro je podgrupa $\mathrm{SL}(n,\mathbb{R})$.

4.3 Okruh. Na množině R je dána struktura *okruhu*, jsou-li dány dvě operace. S první z nich, většinou ji nazýváme *sčítání* (označujeme $+$), tvoří R Abelovu grupu (*neutrální prvek* označujeme 0, *opačný prvek* k x značíme $-x$). Druhá operace, které říkáme *násobení* (označujeme $\cdot$), musí se sčítáním splňovat *distributivní zákon*

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c), \\ (a + b) \cdot c &= (a \cdot c) + (b \cdot c). \end{aligned}$$

Je-li násobení komutativní operace mluvíme o *komutativním okruhu*, je-li násobení asociativní řekneme, že jde o *asociativní okruh*. Existuje-li jednotkový prvek vzhledem k násobení, kterému říkáme *jednotka* (označujeme 1), jedná se o *okruh s jednotkou*.

Prvek $x \in R$ se nazývá *invertibilní*, jestliže existuje prvek x^{-1} takový, že $x \cdot x^{-1} = x^{-1} \cdot x = 1$. Jestliže existují prvky $a, b \in R \setminus \{0\}$ takové, že $a \cdot b = 0$, říkáme, že R má *dělitele nuly*. *Triviální okruh* je okruh obsahující pouze nulu ($R = \{0\}$).

Množina polynomů s reálnými koeficienty s operací sčítání polynomů a násobení polynomů tvoří komutativní asociativní okruh s jednotkou (o čemž se čtenář jistě rád přesvědčí). Značíme jej $P[x]$.

Množina čtvercových matic řádu n s operací sčítání a násobení matic tvoří asociativní nekomutativní okruh s jednotkou. Tento okruh má dělitele nuly (najděte je!).

4.4 Pole. Netriviální komutativní asociativní okruh s jednotkou, jehož každý nenulový prvek má inverzi je *pole*.

Uvedenou definici si trochu rozebereme. Je-li P pole, pak P spolu se *sčítáním* (označujeme $+$) tvoří Abelovu grupu (*opačný* $-x$, *neutrální prvek* 0); pro libovolné $x, y, z \in P$ platí

$$\begin{aligned} &x + y = y + x, \\ &(x + y) + z = x + (y + z), \\ &x + 0 = 0 + x = x, \\ &x + (-x) = (-x) + x = 0. \end{aligned}$$

P s operaci *násobení* tvoří Abelovu grupu (*inverze* x^{-1}, *neutrální* prvek 1); pro libovolné $x, y, z \in P$ platí

$$\begin{aligned} &x \cdot y = y \cdot x, \\ &(x \cdot y) \cdot z = x \cdot (y \cdot z), \\ &x \cdot 1 = 1 \cdot x = x, \end{aligned}$$

$$x \cdot x^{-1} = x^{-1} \cdot x = 1.$$

P s oběma operacemi tvoří okruh, tedy splňují distributivní zákon; pro libovolné $x, y, z \in P$ platí

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z),$$
$$(x + y) \cdot z = (x \cdot z) + (y \cdot z).$$

Tyto rovnice jsou někdy označovány za *axiomy pole*.

Jelikož je operace sčítání asociativní vynecháváme ve vyraze $(x + y) + z$ závorky a píšeme prostě $x + y + z$, stejně tak i u násobení. Pro ještě větší pohodlí zavádíme přednost násobení před sčítáním, proto by distributivní zákon mohl být zapsán $x \cdot (y + z) = x \cdot y + x \cdot z$. Dále místo přičítání opačného prvku zavádíme operaci *odčítání*, tedy $x + (-y) = (-y) + x = x - y$ a *dělení* pro násobení inverzním prvkem $x \cdot y^{-1} = y^{-1} \cdot x = \frac{x}{y}$. Pokud to nebudou vyžadovat okolnosti, budeme vynechávat znak $\cdot$ pro násobení.

Množina $\mathbb{R}$ s operacemi sčítání a násobení je příkladem pole. Dalšími poli se stejnými operacemi jsou $\mathbb{Q}$ a $\mathbb{C}$. Poli, které je podmnožinou pole komplexních čísel, se říká *číselné pole*.

Okruh polynomů není pole jelikož vzhledem k násobení neexistuje ke každému polynomu inverze. Například kdyby k polynomu x, jehož stupeň je roven 1, existoval inverzní polynom $f(x)$ stupně n, muselo by platit $x \cdot f(x) = 1$. Pro stupně by pak platilo $1 + n = 0$ a to není možné.

Rovněž okruh reálných funkcí není pole také proto, že neexistuje inverze vzhledem k násobení. „Problematickými“ funkcemi jsou ty, které nabývají nulové hodnoty.

Okruh čtvercových matice není pole, jelikož násobení matic není komutativní.

Ani množina $\mathbb{R}^n$ pro $n > 1$ vybavena sčítáním a násobením n-tic „po složkách“ není pole jelikož má dělitele nuly (například $(0, 1)$ a $(1, 0)$) a tyto prvky nemají inverzi vzhledem k násobení.[3)]

Grupa $\mathbb{Z}_3 = \{0, 1, 2\}$ s operací sčítání modulo 3 a násobení modulo 3 je pole (Ověřte!). Kdežto $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ s obdobnými operacemi pole není. (Ověřte, že 2 nemá vzhledem k násobení v $\mathbb{Z}_4$ inverzi[4)]).

[3)] Poznamenejme, že zde jednotkou je uspořádaná dvojice $(1, 1)$. Rovnice $(0, 1) \cdot (x, y) = (1, 1)$ nemá řešení.

[4)] V $\mathbb{Z}_3$ byla inverzí 2 vzhledem k násobení 2, skutečně $2 \cdot 2 \pmod 3 = 4 \pmod 3 = 1$. Vyzkoušíme-li v $\mathbb{Z}_4$ všechny prvky inverzi se nám najít nepodaří.

Rejstřík

Značení

$+$	Operace sčítání v grupě, 13
$\approx$	Relace izomorfnosti grup, 17
$\circ$	Operace v grupě, 13
$\mathrm{GL}(n, \mathbb{C})$	Obecná lineární grupa, 14
$\mathrm{GL}(n, \mathbb{R})$	Obecná lineární grupa, 14
$\mathrm{Im}\ f$	Obraz homomorfismu f, 15
$\mathcal{M}_2$	Množina matic 2/2, 15
$\mathrm{O}(n)$	Ortogonální grupa, 17
$\mathbb{R}$	Aditivní grupa reálných čísel, 14
$\mathbb{R}^+$	Multiplikativní grupa kladných reálných čísel, 15
$\mathbb{R} \setminus \{0\}$	Multiplikativní grupa reálných čísel, 14
$\mathrm{SL}(n, \mathbb{C})$	Speciální lineární grupa, 18
$\mathrm{SL}(n, \mathbb{R})$	Speciální lineární grupa, 18
$\mathrm{U}(n)$	Unitární grupa, 18
$\mathbb{Z}$	Grupa celých čísel, 17
$\mathbb{Z}_n$	Grupa zbytkových tříd, 17
e	Neutrální prvek grupy, 13
exp	Exponenciální zobrazení, 15
$\ker f$	Jádro homomorfismu f, 15
x^{-1}	Inverzní prvek v grupě, 13

Literatura

[1] H. J. Bartsch, *Matematické vzorce*, Praha, SNTL, 1983.

[2] M. Krupka, M. Malek, *Matematická anlýza I,II*, Pomocný učební text, Slezská univerzita, Opava 2006.

[3] K. Rektorys a kol., *Přehled užité matematiky*, Prometheus, 1995