

8. HOMOMORFISMY

8.1. Homomorfismy a izomorfismy grup

8.1.1. Homomorfismy grup

Definice 8.1.1. Budte $(X, *, e_X, {}^{-1})$, $(Y, \diamond, e_Y, {}^{-1})$ grupy. Zobrazení $f: X \rightarrow Y$ je *homomorfismus grup*, jestliže

- (i) pro každé $x_1, x_2 \in X$ platí $f(x_1 * x_2) = f(x_1) \diamond f(x_2)$,
- (ii) $f(e_X) = e_Y$,
- (iii) pro každé $x \in X$ platí $f(x^{-1}) = (f(x))^{-1}$.

Značí se $f: (X, *, e_X, {}^{-1}) \rightarrow (Y, \diamond, e_Y, {}^{-1})$.

Příklad. (1) $f_2: (\mathbb{Z}, +, 0, -) \rightarrow (\mathbb{Z}, +, 0, -)$, $n \mapsto 2n$, je homomorfismus grup.

(2) Buď X grupa, $\tilde{X}$ faktorová grupa. Potom zobrazení $X \rightarrow \tilde{X}$, $x \mapsto [x]$ (faktorová projekce) je homomorfismus grup.

(3) Budte $X = \{0, 1, 2, 3\}$ a $Y = \{0, 1\}$ s binárními operacemi $+$ takovými, že

$+$	0	1	2	3		$+$	0	1
0	0	1	2	3	a	0	0	1
1	1	2	3	0		0	0	1
2	2	3	0	1		1	1	0
3	3	0	1	2				

Potom množiny X a Y s těmito operacemi jsou grupy. Zobrazení $X \rightarrow Y$, $0 \mapsto 0$, $1 \mapsto 1$, $2 \mapsto 0$, $3 \mapsto 1$, je homomorfismus těchto grup. $\square$

Tvrzení 8.1.1. Budte $(X, *, e_X, {}^{-1})$, $(Y, \diamond, e_Y, {}^{-1})$ grupy. Buď $f: X \rightarrow Y$ zobrazení takové, že pro každé $x_1, x_2 \in X$ platí $f(x_1 * x_2) = f(x_1) \diamond f(x_2)$. Pak f je homomorfismus grup $(X, *, e_X, {}^{-1}) \rightarrow (Y, \diamond, e_Y, {}^{-1})$.

Důkaz. Podmínka (i) z definice homomorfismu grup je podle předpokladu splněna.

Ukažme, že $f(e_X) = e_Y$.

$$\begin{aligned}
 f(e_X) &= f(e_X) \diamond e_Y = \\
 &= f(e_X) \diamond f(e_X) \diamond (f(e_X))^{-1} = \\
 &= f(e_X * e_X) \diamond (f(e_X))^{-1} = \\
 &= f(e_X) \diamond (f(e_X))^{-1} = \\
 &= e_Y.
 \end{aligned}$$

Ukažme, že $f(x^{-1}) = (f(x))^{-1}$ pro každé $x \in X$.

$$\begin{aligned}
 f(x^{-1}) \diamond f(x) &= f(x^{-1} * x) = f(e_X) = e_Y, \\
 f(x) \diamond f(x^{-1}) &= f(x * x^{-1}) = f(e_X) = e_Y.
 \end{aligned}$$

Takže $f(x^{-1})$ je inverze k $f(x)$. $\square$

Cvičení. Buď $f: X \rightarrow Y$ homomorfismus grup. Označme

$$\text{Im } f = \{f(x) \mid x \in X\}.$$

Pak $\text{Im } f$ je podgrupa v Y . □

Tvrzení 8.1.2. Buďte $f: X \rightarrow Y$ a $g: Y \rightarrow Z$ homomorfismy grup. Pak jejich složení $g \circ f: X \rightarrow Z$ je homomorfismus grup.

Důkaz. Buďte $(X, *, e_X, {}^{-1}), (Y, \diamond, e_Y, {}^{-1}), (Z, \cdot, e_Z, {}^{-1})$ grupy. Pro každé $x_1, x_2 \in X$ platí

$$\begin{aligned} (g \circ f)(x_1 * x_2) &= g(f(x_1 * x_2)) = \\ &= g(f(x_1) \diamond f(x_2)) = \\ &= g(f(x_1)) \cdot g(f(x_2)) = \\ &= (g \circ f)(x_1) \cdot (g \circ f)(x_2). \end{aligned}$$

Zbytek vyplývá z předchozího tvrzení. □

8.1.2. Izomorfismy grup

Definice 8.1.2. Bijektivní homomorfismus grup je *izomorfismus grup*.

Tvrzení 8.1.3. Buď $f: X \rightarrow Y$ izomorfismus grup. Pak $f^{-1}: Y \rightarrow X$ je izomorfismus grup.

Důkaz. Buďte $(X, *, e_X, {}^{-1}), (Y, \diamond, e_Y, {}^{-1})$ grupy. Inverzní zobrazení je bijektivní. Pro libovolné $y_1, y_2 \in Y$ označme $x_1 = f^{-1}(y_1)$ a $x_2 = f^{-1}(y_2)$. Takže $f(x_1) = y_1$ a $f(x_2) = y_2$. Potom

$$\begin{aligned} f^{-1}(y_1 \diamond y_2) &= f^{-1}(f(x_1) \diamond f(x_2)) = f^{-1}(f(x_1 * x_2)) = x_1 * x_2 = \\ &= f^{-1}(y_1) * f^{-1}(y_2). \end{aligned}$$

Zbytek vyplývá z Tvrzení 8.1.1. □

Příklad. (1) Každá identita je izomorfismus.

(2) Označme $\mathbb{R}_+$ množinu všech kladných reálných čísel. Pak $(\mathbb{R}_+, \cdot, 1, {}^{-1})$ je grupa (cvičení). Zobrazení $\exp: (\mathbb{R}, +, 0, -) \rightarrow (\mathbb{R}_+, \cdot, 1, {}^{-1}), x \mapsto e^x$ je homomorfismus grup, protože pro libovolná $x, y \in \mathbb{R}$ platí $\exp(x + y) = e^{x+y} = e^x e^y = (\exp x) \cdot (\exp y)$. Tento homomorfismus je bijektivní, tedy i izomorfismus.

Inverzní izomorfismus je logaritmus

$$\ln: (\mathbb{R}_+, \cdot, 1, {}^{-1}) \rightarrow (\mathbb{R}, +, 0, -). \quad \square$$

Definice 8.1.3. Grupy X, Y jsou *izomorfní*, jestliže existuje izomorfismus $X \rightarrow Y$. Zapisujeme $X \cong Y$.

Tvrzení 8.1.4. Pro libovolné grupy X, Y, Z platí

- (i) $X \cong X$ (reflexivita),
- (ii) jestliže $X \cong Y$, pak $Y \cong X$ (symetrie),
- (iii) jestliže $X \cong Y$ a $Y \cong Z$, pak $X \cong Z$ (tranzitivita).

Důkaz. Cvičení. □

Příklad. $(\mathbb{R}, +, 0, -) \cong (\mathbb{R}_+, \cdot, 1, ^{-1})$. Pro libovolné $a \in \mathbb{R}_+, a \neq 1$, zobrazení $\mathbb{R} \rightarrow \mathbb{R}_+, x \mapsto a^x$ je izomorfismus $(\mathbb{R}, +, 0, -) \rightarrow (\mathbb{R}_+, \cdot, 1, ^{-1})$. Ověřte. $\square$

Cvičení. Buď $h: X \rightarrow Y$ homomorfismus grup.

- (1) Ukažte, že relace $\sim$ zadaná předpisem

$$x_1 \sim x_2 \Leftrightarrow h(x_1) = h(x_2)$$

je kongruence na grupě X .

- (2) Ukažte, že faktorová grupa $\tilde{X}$ podle kongruence $\sim$ je izomorfní podgrupě $\text{Im } h$.

Návod: $\tilde{X} \rightarrow \text{Im } h, [x] \mapsto h(x)$. $\square$

8.2. Homomorfismy a izomorfismy polí

Definice 8.2.1. Buďte P, Q pole. Zobrazení $f: P \rightarrow Q$ je *homomorfismus polí*, jestliže

- (i) pro každé $p_1, p_2 \in P$ platí $f(p_1 + p_2) = f(p_1) + f(p_2)$,
- (ii) $f(0) = 0$,
- (iii) pro každé $p \in P$ platí $f(-p) = -f(p)$,
- (iv) pro každé $p_1, p_2 \in P$ platí $f(p_1 \cdot p_2) = f(p_1) \cdot f(p_2)$,
- (v) $f(1) = 1$,
- (vi) pro každé $p \in P, p \neq 0$, platí $f(p^{-1}) = (f(p))^{-1}$.

O zobrazeních polí platí následující tvrzení obdobné Tvrzení 8.1.1 o zobrazeních grup.

Tvrzení 8.2.1. Buďte P, Q pole. Buď $f: P \rightarrow Q$ zobrazení takové, že pro každé $p_1, p_2 \in P$ platí

- (i) $f(p_1 + p_2) = f(p_1) + f(p_2)$,
- (ii) $f(p_1 \cdot p_2) = f(p_1) \cdot f(p_2)$,
- (iii) $f(1) \neq 0$.

Pak f je homomorfismus polí $P \rightarrow Q$.

Důkaz. Cvičení. $\square$

Definice 8.2.2. Bijektivní homomorfismus polí je *izomorfismus polí*. Pole jsou *izomorfní*, jestliže mezi nimi existuje izomorfismus.

Příklad. Dvoupvkové pole $\{0, 1\}$ je izomorfní s polem $\mathbb{Z}_2$. Izomorfismem je zobrazení $0 \mapsto [0]_2, 1 \mapsto [1]_2$. $\square$

8.3. Izotonní zobrazení, homomorfismy a izomorfismy svazů

8.3.1. Izotonní zobrazení a izomorfismy uspořádaných množin

Definice 8.3.1. Buďte $(X, \leq), (Y, \leq)$ uspořádané množiny. Zobrazení $f: X \rightarrow Y$ je *izotonní*, jestliže platí implikace

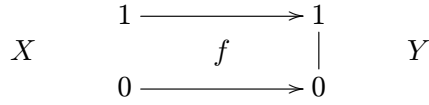
$$x \leq y \Rightarrow f(x) \leq f(y).$$

Je-li zobrazení f bijektivní a f i f^{-1} jsou izotonní, pak f je *izomorfismus uspořádaných množin* a uspořádané množiny $(X, \leq), (Y, \leq)$ jsou *izomorfní*.

Příklad. Identické zobrazení $\text{id}: (\mathbb{N}, |) \rightarrow (\mathbb{N}, \leq)$ je izotonní. Skutečně, jestliže $a \mid b$, pak $b = na$ pro nějaké $n \in \mathbb{N}$, ale $n \geq 1$, a proto $b = na \geq a$.

Inverzní zobrazení $\text{id}: (\mathbb{N}, \leq) \rightarrow (\mathbb{N}, |)$ není izotonní, protože neplatí implikace $x \leq y \Rightarrow x \mid y$ (například $2 \leq 3$, ale $2 \nmid 3$). $\square$

Příklad. Buďte $X = Y = \{0, 1\}$ s uspořádáními a zobrazením f podle obrázku:



Tedy $f: X \rightarrow Y$ je identické zobrazení. Pak f je izotonní bijekce, jejíž inverze f^{-1} není izotonní. $\square$

Cvičení. Složení izotonních zobrazení je izotonní zobrazení. $\square$

8.3.2. Homomorfismy a izomorfismy svazů

Definice 8.3.2. Buďte $(X, \wedge, \vee)$, $(Y, \wedge, \vee)$ svazy. Zobrazení $f: X \rightarrow Y$ je *homomorfismus svazů*, jestliže pro každé $x_1, x_2 \in X$

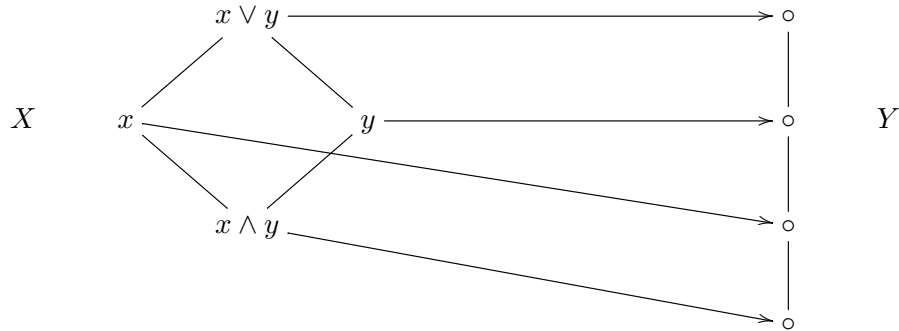
$$\begin{aligned}
 f(x_1 \wedge x_2) &= f(x_1) \wedge f(x_2) \\
 f(x_1 \vee x_2) &= f(x_1) \vee f(x_2).
 \end{aligned}$$

Tvrzení 8.3.1. Každý homomorfismus svazů je izotonní zobrazení.

Důkaz. Buďte $(X, \wedge, \vee)$, $(Y, \wedge, \vee)$ svazy, $f: X \rightarrow Y$ homomorfismus a $x_1, x_2 \in X$ takové, že $x_1 \leq x_2$, tedy $x_1 \wedge x_2 = x_1$. Potom $f(x_1) \wedge f(x_2) = f(x_1 \wedge x_2) = f(x_1)$, tedy $f(x_1) \leq f(x_2)$. $\square$

Izotonní zobrazení svazů však nemusí být homomorfismus svazů:

Příklad. Buď f zobrazení podle obrázku:



Pak f je izotonní zobrazení svazů, ale není homomorfismus svazů, protože

$$f(x) \vee f(y) = f(y) \neq f(x \vee y).$$

$\square$

Definice 8.3.3. Bijektivní homomorfismus svazů je *izomorfismus svazů*.

Cvičení. Buď f zobrazení svazů. Dokažte, že následující výroky jsou ekvivalentní:

- (1) f je izomorfismus uspořádaných množin;
- (2) f je izomorfismus svazů.

$\square$

9. VEKTOROVÉ PROSTORY

9.1. Definice, příklady, základní vlastnosti

Vektor je běžně znázorňován v rovině nebo v prostoru jako orientovaná úsečka (šipka), která má počáteční bod a koncový bod. Pokud je možné jeden takový vektor převést na druhý takový vektor rovnoběžným posunutím, říká se, že tyto dva vektory jsou totožné nebo ekvivalentní, nebo že jsou to dvě umístění jednoho vektoru. Takové vektory se sčítají pomocí pravidla rovnoběžníku a násobí se reálným číslem tak, že šipka se příslušně prodlouží nebo zkrátí a při násobení záporným číslem navíc změní směr na opačný.

Obecně definujeme vektor jako prvek vektorového prostoru a vektorový prostor nad nějakým polem jako množinu s operací sčítání a s násobením prvků množiny prvky pole s takovými vlastnostmi, které umožňují představu vektoru jako šipky a představu sčítání vektorů a násobení vektoru prvkem pole, jak je uvedeno v předchozím odstavci.

Definice 9.1.1. Buď V neprázdná množina, P pole. *Vektorový prostor V nad polem P* je množina V spolu s binární operací $+: V \times V \rightarrow V$, $(u, v) \mapsto u + v$, a zobrazením $\cdot: P \times V \rightarrow V$, $(p, v) \mapsto p \cdot v$, takovými, že

- (1) pro každé $u, v, w \in V$ platí $(u + v) + w = u + (v + w)$,
- (2) existuje $0 \in V$ takový, že pro každé $v \in V$ platí $v + 0 = v$,
- (3) pro každé $v \in V$ existuje $-v \in V$ takové, že $v + (-v) = 0$,
- (4) pro každé $u, v \in V$ platí $u + v = v + u$,
- (5) pro každé $v \in V$ platí $1 \cdot v = v$,
- (6) pro každé $p, q \in P$ a $v \in V$ platí $(p \cdot q) \cdot v = p \cdot (q \cdot v)$,
- (7) pro každé $p, q \in P$ a $v \in V$ platí $(p + q) \cdot v = (p \cdot v) + (q \cdot v)$,
- (8) pro každé $p \in P$ a $u, v \in V$ platí $p \cdot (u + v) = (p \cdot u) + (p \cdot v)$.

Prvky množiny V jsou *vektory*, prvky pole P jsou *skaláry*. Binární operace $+$ je *sčítání*, zobrazení $\cdot$ je *násobení skalárem*, vektor $0 \in V$ je *nulový vektor* nebo *nula*, vektor $-v$ je *opačný vektor* k vektoru v .

Podmínky (1)–(8) jsou *axiomy vektorového prostoru*. Podmínky (1)–(4) znamenají, že V s operací $+$ je komutativní grupa.

Jelikož každá binární operace má nejvýše jeden neutrální prvek, ve vektorovém prostoru existuje jediný nulový vektor. Obdobně, jelikož každý prvek má vzhledem k asociativní binární operaci nejvýše jeden inverzní prvek, ke každému vektoru existuje jediný opačný vektor.

Násobení skalárem $\cdot: P \times V \rightarrow V$, $(p, v) \mapsto p \cdot v$, není binární operace (není-li $P = V$), ale nazývá se *vnější operace*, a místo $p \cdot v$ se často píše jen pv . Binární operace se někdy nazývá *vnitřní operace*.

Vektorový prostor nad polem $\mathbb{R}$, nebo $\mathbb{C}$ je *reálný*, resp. *komplexní* vektorový prostor.

Příklad. (1) Vektorový prostor Eukleidovské geometrie, dvojrozměrné i trojrozměrné, kde vektor je třída ekvivalentních šipek a je reprezentován jednotlivými šípkami, jak je uvedeno v prvním odstavci této kapitoly.

Nulový vektor je reprezentován degenerovanou úsečkou nulové délky. Vektorový prostor v rovině resp. prostoru značíme E^2 resp. E^3 .

(2) Buď V jednoprvková množina, P pole. Jediný prvek množiny V označme 0 a položme $0 + 0 = 0$, $-0 = 0$ a $p \cdot 0 = 0$ pro každé $p \in P$. Dostáváme vektorový prostor nazývaný *nulový prostor* nebo *triviální prostor*.

(3) Každé pole je vektorový prostor nad sebou samým. Položíme-li v definici vektorového prostoru $V = P$, budou všechny axiomy vektorového prostoru důsledky axiomů

pole (ověřte). Získáváme tak například vektorový prostor $\mathbb{R}$ nad $\mathbb{R}$, vektorový prostor $\mathbb{C}$ nad $\mathbb{C}$, vektorový prostor $\mathbb{Q}$ nad $\mathbb{Q}$ a vektorový prostor $\mathbb{Z}_2$ nad $\mathbb{Z}_2$.

(4) Každé pole je vektorový prostor nad libovolným svým podpolem. Jediný rozdíl oproti předchozímu příkladu spočívá v tom, že násobení skalárem je dovoleno jen pro skaláry z podpole.

(5) Buď $n \in \mathbb{N}$, P pole. Na množině P^n všech uspořádaných n -tic prvků P zavedme sčítání a násobení skalárem předpisem

$$(u_1, u_2, \dots, u_n) + (v_1, v_2, \dots, v_n) = (u_1 + v_1, u_2 + v_2, \dots, u_n + v_n),$$

$$p(u_1, u_2, \dots, u_n) = (pu_1, pu_2, \dots, pu_n).$$

Vzniká vektorový prostor P^n nad polem P (ověřte). Například řádky a sloupky matic jsou prvky takových vektorových prostorů.

(6) Vektorový prostor P^n nad podpolem $Q \subset P$.

(7) Vektorový prostor matic typu $m \times n$ nad polem P s operacemi sčítání a násobení skalárem. Značí se $P^{m \times n}$ nebo $\mathcal{M}_{m \times n}(P)$ (resp. $\mathcal{M}_m(P)$ nebo $\text{gl}(m, P)$ v případě čtvercových matic).

(8) Vektorový prostor polynomů stupně nejvýše n nad polem P s operacemi sčítání a násobení skalárem.

(9) Vektorový prostor polynomů nad polem P s operacemi sčítání a násobení skalárem.

(10) Vektorový prostor všech řešení homogenní soustavy rovnic.

(11) Buď X množina, P pole. Na množině P^X všech zobrazení $X \rightarrow P$ zavedme sčítání a násobení skalárem předpisem

$$(u + v)(x) = u(x) + v(x),$$

$$(pu)(x) = p \cdot u(x).$$

Vzniká vektorový prostor P^X nad polem P (ověřte). Speciální případy jsou množina všech funkcí z $\mathbb{R}$ do $\mathbb{R}$, množina všech spojitých funkcí na $\mathbb{R}$, množina diferencovatelných funkcí na $\mathbb{R}$, množina všech spojitých funkcí na intervalu $[a, b]$. $\square$

Tvrzení 9.1.1. Buď V vektorový prostor nad polem P . Pak pro každé $u, v \in V$, $p, q \in P$ platí

- (i) $0 \cdot v = 0$,
- (ii) $(-1) \cdot v = -v$,
- (iii) $(p - q) \cdot v = p \cdot v - q \cdot v$,
- (iv) $p \cdot (u - v) = p \cdot u - p \cdot v$,
- (v) Je-li $p \cdot v = 0$, pak buď $p = 0$ nebo $v = 0$.

Důkaz. Cvičení. $\square$