1 prvy priklad

Priklad 1.1. *Rozhodni a dokaz, ci* $(\mathbb{R}^+ \times \mathbb{R}, \oplus)$ *je grupa, pricom*

$$(a, b) \oplus (c, d) = (2ac, b + d).$$

Je operacia $\oplus$ *komutativna?*

Proof. $\oplus$ je binarna operacia na $\mathbb{R}^+ \times \mathbb{R}$: ak a, c su kladne cisla, tak aj $2ac$ je kladne. je jasne, ze $b+d$ je realne cislo ak b, d su realne. takze ak $(a, b), (c, d)$ su z $\mathbb{R}^+ \times \mathbb{R}$, tak aj $(a, b) \oplus (c, d) = (2ac, b + d)$ je z $\mathbb{R}^+ \times \mathbb{R}$.

operacia $\oplus$ je asociativna:

$$((a, b) \oplus (c, d)) \oplus (e, f) = (2ac, b + d) \oplus (e, f) = (4ace, b + d + f)$$

$$(a, b) \oplus ((c, d) \oplus (e, f)) = (a, b) \oplus (2ce, d + f) = (4ace, b + d + f)$$

pre neutralny prvok musi platit, ze $(a, b) \oplus (e_1, e_2) = (2ae_1, b + e_2) = (a, b)$. z toho dostaneme, ze $2ae_1 = a$ a $b + e_2 = b$. prvu rovnost mozeme vydelit $2a$ (a je z $\mathbb{R}^+$, teda je nenulove a mozeme nim delit). dostaneme $e_1 = \frac{1}{2}$. z druhej rovnosti mame $e_2 = 0$. neutralny prvok je teda $(\frac{1}{2}, 0)$.
este najdeme inverzne prvky. oznacme (c, d) inverzny prvok k (a, b). ma platit $(a, b) \oplus (c, d) = (2ac, b + d) = (\frac{1}{2}, 0)$. z toho vidime, ze $2ac = \frac{1}{2}$ a $b + d = 0$. prvu rovnost mozeme zase vydelit $2a$ a dostaneme, ze $c = \frac{1}{4a}$. z druhej vidime, ze $d = -b$. nasli sme inverzny prvok k (a, b) – je to $(\frac{1}{4a}, -b)$. takze $(\mathbb{R}^+ \times \mathbb{R}, \oplus)$ je grupa.
este sa pytame, ci je operacia $\oplus$ komutativna. je, lebo $(a, b) \oplus (c, d) = (2ac, b + d) = (2ca, d + b) = (c, d) \oplus (a, b)$. □

Priklad 1.2. *Rozhodni a dokaz, ci* $(\mathbb{Q} \setminus \{0\}, \oplus)$ *je grupa, pricom*

$$a \oplus b = ab - a.$$

Je operacia $\oplus$ *komutativna?*

Proof. $(\mathbb{Q} \setminus \{0\}, \oplus)$ nie je grupa, lebo $\oplus$ nie je binarna operacia na mnozine $\mathbb{Q} \setminus \{0\}$: ak za b zoberieme 1 (a moze byt lubovolne), dostaneme $a \oplus 1 = a - a = 0 \notin \mathbb{Q} \setminus \{0\}$. □

Priklad 1.3. *Rozhodni a dokaz, ci* $(G, \oplus)$ *je grupa, pricom*

$$G = \{a + i\sqrt{3}\ b \mid a, b \in \mathbb{Q}\}$$
$$a \oplus b = a + ab + b.$$

Je operacia $\oplus$ *komutativna?*

Proof. neutralny prvok je 0, lebo $a \oplus 0 = a + a0 + 0 = a$ a $0 \oplus a = 0 + 0a + a = a$. skusme teraz najst inverzne prvky. pre inverzny prvok musi platit

$$a \oplus a^{-1} = a + aa^{-1} + a^{-1} = 0$$

z toho dostaneme

$$aa^{-1} + a^{-1} = -a$$
$$(a + 1)a^{-1} = -a$$
$$a^{-1} = \frac{-a}{a + 1}$$

pre $a = -1$ ten zlomok nema zmysel, takze k -1 neexistuje inverzny prvok. $(G, \oplus)$ teda nie je grupa. este sa pytame, ci je operacia $\oplus$ komutativna. je, lebo $a \oplus b = a + ab + b = b + ba + a = b \oplus a$ □

Priklad 1.4. *Rozhodni a dokaz, ci* $(G, .)$ *je grupa, pricom*

$$G = \{a + b\sqrt{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}.$$

Operacia . je obycajne nasobenie.

Ak $(G, .)$ *je grupa, je komutativna?*

Proof. zoberme si prvky $a + b\sqrt{2} + c\sqrt[3]{4}$ a $d + e\sqrt{2} + f\sqrt[3]{4}$ z G.

$$(a + b\sqrt{2} + c\sqrt[3]{4})(d + e\sqrt{2} + f\sqrt[3]{4}) =$$

$$= ad + ae\sqrt{2} + af\sqrt[3]{4} + bd\sqrt{2} + 2be + bf\sqrt{2}\sqrt[3]{4} + cd\sqrt[3]{4} + ce\sqrt{2}\sqrt[3]{4} + cf\sqrt[3]{16} =$$
$$= (ad + 2de) + (ae + bd)\sqrt{2} + (af + cd)\sqrt[3]{4} + (bf + ce)\sqrt{2}\sqrt[3]{4} + cf\sqrt[3]{16}$$

toto cislo sa neda vyjadrit v tvare $x + y\sqrt{2} + z\sqrt[3]{4}$ (kvoli clenom $(bf + ce)\sqrt{2}\sqrt[3]{4}$ a $cf\sqrt[3]{16}$), takze nepatri do G. nasobenie nie je binarna operacia na G, takze $(G, .)$ nie je grupa. □

Priklad 1.5. *Nech*

$$M_1 = \{f : \mathbb{Z} \to \mathbb{Z} \mid f \text{ je bijekcia}\}$$

- teda mnozina vsetkych bijekcii na mnozine celych cisel. Rozhodni a dokaz, ci $(M_2, \circ)$ *je grupa, pricom*

$M_2 = \{f : \mathbb{Z} \to \mathbb{Z} \mid f \in M_1 \wedge f(n) = n$ *pre vsetky cele cisla az na konecny pocet*$\}$

$a \circ$ *je operacia skladania zobrazeni. Je operacia* $\circ$ *komutativna?*

Proof. najskor ukazeme, ze $\circ$ je binarna operacia na M_2. zadanie nam vlastne hovori, ze do M_2 patria tie zobrazenia f, pre ktore je $f(n) \neq n$ iba pre konecny pocet celych cisel. ak teda mame zobrazenia $f, g \in M_2$, tak $f(n) \neq n$ pre k cisel a $g(n) \neq n$ pre l cisel. Ak mame take cislo n, ze $f(n) = n$ aj $g(n) = n$, tak aj $f \circ g(n) = f(g(n)) = f(n) = n$. takze $f \circ g(n)$ sa moze lisit od n maximalne v $k+l$ pripadoch (ked $f(n) \neq n$ alebo $g(n) \neq n$), a to je konecny pocet. takze zlozene zobrazenie $f \circ g$ tiez patri do mnoziny M_2. asociativnost overovat nemusime, lebo vieme ze skladanie zobrazeni je asociativne. neutralny prvok je identicke zobrazenie, teda take zobrazenie f, ze $f(n) = n$ pre vsetky n. toto zobrazenie splna podmienku zo zadania, teda patri do M_2. Este zostava najst inverzne prvky. ak f je z M_2 existuje k nemu inverzne zobrazenie, lebo f je bijekcia. otazka je, ci toto inverzne zobrazenie patri do M_2. zo zadania vieme, ze $f(n) = n$ pre vsetky cele cisla az na konecny pocet. ale ak $f(n) = n$, tak aj $f^{-1}(n) = n$. teda aj $f^{-1}(n) = n$ pre vsetky cele cisla az na konecny pocet, a preto aj f^{-1} patrí do M_2. $(M_2, \circ)$ je teda grupa.

druha otazka je, ci je operacia $\circ$ komutativna. zoberme si zobrazenia z $\mathbb{Z}$ do $\mathbb{Z}$:

$$f(n) = \begin{cases} 2 & \text{ak } n = 1 \\ 1 & \text{ak } n = 2 \\ n & \text{inak} \end{cases}$$

$$g(n) = \begin{cases} 3 & \text{ak } n = 1 \\ 1 & \text{ak } n = 3 \\ n & \text{inak} \end{cases}$$

obidve patria do M_2 a $f \circ g(1) = 3 \neq 2 = g \circ f(1)$. operacia $\circ$ teda komutativna nie je. □

Priklad 1.6. *Nech*

$$M_1 = \{f : \mathbb{Z} \to \mathbb{Z} \mid f \text{ je bijekcia}\}$$

- teda mnozina vsetkych bijekcii na mnozine celych cisel. Rozhodni a dokaz, ci $(M_2, \circ)$ *je grupa, pricom*

$M_2 = \{f : \mathbb{Z} \to \mathbb{Z} \mid f \in M_1 \ \wedge \ f(n) = n \text{ len pre konecny pocet celych cisel}\}$

$a \circ$ *je operacia skladania zobrazeni. Je operacia* $\circ$ *komutativna?*

Proof. trochu trikovy priklad ... vzdy je dobre sa nad prikladom najprv trochu zamysliet. v tomto pripade si staci uvedomit co je neutralnym prvkom operacie skladania bijekcii ... zrejme taka bijekcia, ktora vsetky prvky necha na mieste ... inymi slovami take zobrazenie f, ze $f(n) = n$ pre vsetky n.

mame taketo zobrazenie v mnozine M_2? ... nemame, lebo v M_2 su len take zobrazenia f, ze $f(n) = n$ len pre konecny pocet "'eniek"' ... ale mnozina $\mathbb{Z}$ je nekonecna ... teda $(M_2, \circ)$ nie je grupou.

este sa pytame, ci je operacia $\circ$ komutativna ... uz sme si na cviceniach ukazali, ze skladanie zobrazeni vo vseobecnosti komutativne nie je ... teda asi sa budeme snazit dokazat aj teraz, ze ani v tomto pripade komutativna nie je.

premyslite si, ze zobrazenia z $\mathbb{Z}$ do $\mathbb{Z}$:

$$f(n) = \begin{cases} n+1 & \text{ak } n = 2k \\ n-1 & \text{ak } n = 2k+1 \end{cases}$$

a $g(n) = n + 1$ patria do M_2. pritom $f(g(2)) = 2 \neq 4 = g(f(2))$. □

2 druhy priklad

Priklad 2.1. *Nech* $\circ$ *je binarna operacia na mnozine* A*, taka, ze pre kazde* $a, b, c \in A$ *plati*

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

a nech $\circ$ *ma neutralny prvok. Dokazte, ze operacia* $\circ$ *je komutativna a asociativna.*

Proof. podla predpokladov ma operacia $\circ$ neutralny prvok, oznacme ho e. potom

$$e \circ (b \circ c) = (e \circ c) \circ b$$

a teda

$$b \circ c = c \circ b$$

co dokazuje komutativnost. dalej

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

pouzijeme uz dokazanu komutativnost (vo vnutri zatvoriek)

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

dalej pouzijeme vlastnost $\circ$ zo zadania

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

nakoniec pouzijeme dva krat komutativnost ... najprv na zatvorku a potom na cely vyraz

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

cim sme dokazali aj asociativnost. □

Priklad 2.2. *Nech $(G, \circ)$ je grupa. Dokazte, ze ak $x \circ x = x$, potom $x = e$ (teda x je neutralnym prvkom).*

Proof. ak $x \in G$, potom ku x musi v grupe G existovat inverzny prvok x^{-1}. potom uz jednoducho z predpokladu odvodime co mame:

$$x \circ x = x$$

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

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

tu sme pouzili asociativnost a zaverom dostavame

$$x = e.$$

□

Priklad 2.3. *Dokazte, ze v lubovolnom poli F plati*

$$-0 = 0$$
$$(a - b)c = ac - bc.$$

Proof. v prvom rade si treba uvedomit, ze ona 0 nemusi byt ta 0, ktoru poznate z celych cisel. v tomto pripade znak 0 oznacuje neutralny prvok pola $(F, +, .)$ pre operaciu $+$. vo svetle povedaneho potom tvrdenie $-0 = 0$ nehovori nic ine ako to, ze neutralny prvok je sam sebe inverzny. toto by malo byt uz intuitivne jasne kazdemu, kto vie definiciu grupy. pre pochybovacov vsak predsa

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

pricom sme vyuzili neutralitu 0.

v druhom priklade si opat staci uvedomit, ze operaciu $-$ v poli nepozname ... sluzi nam iba na skratenie zapisu $a + (-b)$ na $a - b$. potom teda

$$(a - b)c = (a + (-b))c = ac + (-b)c$$

este by sa nam hodilo ukazat, ze $(-b)c = -(bc)$

$$(-b)c + bc = (-b + b)c = 0c$$

pozrime sa na vyraz $0c$

$$0c = (0 + 0)c = 0c + 0c$$

preto $0 = 0c$. teda dostali sme

$$(-b)c + bc = 0$$
$$((-b)c + bc) + (-(bc)) = 0 + (-(bc))$$
$$(-b)c = -(bc)$$

co je to co sme chceli ukazat. mozeme sa teda vratit k prvej rovnici

$$(a - b)c = (a + (-b))c = ac + (-b)c = ac + (-(bc)) = ac - bc.$$

□

Priklad 2.4. *Dokazte, ze v lubovolnom poli F plati*

$$-(a+b) = -a - b$$
$$1 \neq 0.$$

Teda ze neutralny prvok pre operaciu . sa nerovna neutralnemu prvku pre operaciu +.

Proof. podobne ako v predoslom priklade, zadanie je skratenym zapisom

$$-(a+b) = (-a) + (-b).$$

vieme, ze

$$-(a+b) + (a+b) = 0$$

vyuzijuc asociativitu operacie + dostaneme

$$(-(a+b) + a) + b = 0$$

nasledne pripocitame najprv $-b$ a potom $-a$ a zaverom pouzijeme komutativnost +

$$-(a+b) = (-b) + (-a) = (-a) + (-b).$$

co by sa stalo, keby operacie + a . mali rovnaky neutralny prvok v poli $(F, +, .)$? minimalne by potom $(F - \{0\}, .)$ nebola grupou, lebo by nemala neutralny prvok. iny dovod (nie nutne posledny) : v predoslom priklade sme ukazali, ze pre vsetky $a \in F$ plati

$$0a = 0$$

a zaroven, kedze 1 je neutralny prvok pre operaciu . , plati

$$1a = a$$

ak by sme predpokladali, ze $0 = 1$, potom by sme dostali

$$a = 1a = 0a = 0$$

co je spor. este by niekto mohol namietat, ze mozeme mat jednoprvkovu mnozinu $F = \{0\}$ a teda pole len s jednym prvkom ... $(\{0\}, +, .)$ ... rozmyslite si, preco je tento argument zly (hint: pozrite si poriadne definiciu pola a grupy). □

Priklad 2.5. *Dokazte, ze v lubovolnom poli F plati*

$$aa = 1 \Leftrightarrow a = 1 \vee a = -1$$
$$a(b_1 + ... + b_n) = ab_1 + ... + ab_n.$$

Proof. prve tvrdenie hovori, ze ak je prvok v poli $(F, +, .)$ inverzny sam k sebe, potom tento prvok je 1 alebo -1. zrejme 1, neutralny prvok operacie . , je inverzny sam k sebe, lebo $1.1 = 1$.

dalej, v predoslych prikladoch sme uz ukazali, ze $(-b)c = -(bc)$. pouzijuc tento poznatok dvakrat mozeme pisat

$$(-1)(-1) = -(1.(-1)) = -(-(1.1)) = -(-1) = 1$$

v poslednej rovnosti sme pouzili (dufam, ze uz vsetkym zname tvrdenie z grup), ze $(a^{-1})^{-1} = a$.

teda zatial sa nam podarilo ukazat, ze pre a rovne 1 aj -1 plati $aa = 1$. k dokonceniu dokazu este treba ukazat, ze pre ziadne ine prvky pola F rovnost neplati. pozrime sa, co by pre taky prvok muselo platit.

$$a(a + 1) = aa + a = 1 + a = a + 1$$

kedze $(a + 1) \neq 0$ (lebo $a \neq -1$), tento prvok patri do grupy $(F - \{0\}, .)$, a teda mozeme pouzit zakony o krateni. dostavame, ze $a = 1$, co je spor s predpokladom $a \neq 1$ ani -1. teda naozaj, rovnica $aa = 1$ je splnena prave vtedy, ked a je bud 1 alebo -1.

druha cast je typicky priklad na indukciu. z definicie pola vieme, ze tvrdenie plati pre $n = 2$

$$a(b_1 + b_2) = ab_1 + ab_2.$$

predpokladajme, ze tvrdenie plati pre n a dokazme, ze plati aj pre $n + 1$.

$$a(b_1+b_2+...+b_n+b_{n+1}) = a(b_1+b_2+...+b_n)+ab_{n+1} = ab_1+ab_2+...+ab_n+ab_{n+1}$$

pricom sme v prvej rovnosti pouzili asociativitu ... $a(b_1 + b_2 + ... + b_n + b_{n+1})$ sme napisali ako $a((b_1 + b_2 + ... + b_n) + b_{n+1})$. nasledne sme pouzili distributivny zakon a v druhej rovnosti nakoniec indukcny predpoklad. □

Priklad 2.6. *Nech $(G, \circ)$ je grupa. Dokazte, ze zobrazenie $f : G \to G$ definovane ako $f(a) = a^{-1}$ je bijekcia.*

Proof. staci si spomenut na to, co vieme o grupach. v prvom rade to, ze ku kazdemu prvku existuje prave jeden inverzny prvok. tento poznatok nas opravnuje hovorit o f ako o zobrazeni.

dalej si spomenme, ze byt inverznym prvkom je symetricka relacia ... teda ak a^{-1} je inverzny prvok ku a, potom aj a je inverzny prvok ku a^{-1}. tato vlastnost zaruci injektivnost f ... naozaj, keby dva prvky a_1 a a_2 mali rovnaky inverzny prvok a, potom prvok a by mal dva rozne inverzne prvky ... co nemoze byt.

keby bola mnozina G konecna, mohli by sme pouzit predchadzajuci vysledok hovoriaci, ze pre zobrazenie $f : G \to G$ su pojmy byt injekciou, byt surjekciou, byt bijekciou ekvivalentne. vo vseobecnosti vsak mnozina G konecna byt nemusi.

aj tak je surjektivnost jednoducha ... ku kazdemu prvku existuje inverzny ... teda ak $g \in G$ potom existuje $g^{-1} \in G$ pricom plati $f(g^{-1}) = g$ ... opat a stale dookola vyuzivame, ze $(g^{-1})^{-1} = g$.

□