Algebra 2

slidy k přednáškám

KMI/ALG2

Zpracováno podle přednášek prof. Jiřího Rachůnka a podle přednášek prof. Ivana Chajdy.

Vytvořeno za podpory projektu FRUP_2017_052: Tvorba a inovace výukových opor vybraných matematických předmětů katedry informatiky

Obsah

Obsah

Obsah

Definice

Nechť G je neprázdná množina a $n \in \mathbb{N}_0$. Pak **n-ární operací na G** rozumíme každé zobrazení $f : G^n \to G$.

Definice

Neprázdná množina G spolu s neprázdnou množinou $\{f_\alpha; \alpha \in I\}$ operací na G se nazývá **algebraická struktura** (nebo stručněji **algebra**). Označení: $\mathscr{G} = (G; f_\alpha, \alpha \in I)$.

Definice

Algebraická struktura $\mathscr{G} = (G; \cdot)$, kde „$\cdot$“ je binární operace na $G \neq \emptyset$, se nazývá **grupoid**.

Definice

- Grupoid $\mathscr{G} = (G; \cdot)$ se nazývá **komutativní**, platí-li

$$\forall a, b \in G;\ ab = ba.$$

- Grupoid $\mathscr{G} = (G; \cdot)$ se nazývá **pologrupa**, platí-li

$$\forall a, b, c \in G;\ a(bc) = (ab)c,$$

  tj. jeho operace je asociativní.
- Grupoid $\mathscr{G} = (G; \cdot)$ má **jednotkový prvek** e, platí-li

$$\exists e \in G \quad \forall a \in G; \quad ae = a = ea.$$

- Pologrupa v níž existuje jednotkový prvek, se nazývá **monoid**.

Věta

Nechť $\mathscr{G} = (G; \cdot)$ je pologrupa, $a_1, a_2, \ldots, a_n \in G$ $(n \geq 3)$. Pak pro všechna uzávorkování při násobení těchto prvků zapsaných v daném pořadí dostaneme stejný výsledný prvek.

Důkaz. Na přednášce.

Poznámka. Při násobení prvků v libovolné pologrupě proto nemusíme používat závorky.

Definice

Nechť $\mathscr{G} = (G; \cdot)$ je pologrupa, $a \in G$. Pak **n-tou přirozenou mocninou** $n \in \mathbb{N}$ prvku a rozumíme prvek $a^n \in G$ takový, že $a^1 = a$, $a^{n+1} = a^n \cdot a$.

Věta

Jsou-li a, b prvky pologrupy $(G; \cdot)$ a $m, n \in \mathbb{N}$, pak platí

(a) $a^m \cdot a^n = a^{m+n}$

(b) $(a^m)^n = a^{mn}$

(c) jestliže $ab = ba$, pak $(ab)^n = a^n b^n$.

Důkaz. Na přednášce.

Poznámka. Je-li $(G; \cdot)$ monoid s jednotkovým prvkem e, pak pro každý prvek $a \in G$ definujeme nultou mocninu vztahem $a^0 = e$. Je zřejmé, že rovnosti (a), (b), (c) z předchozí věty platí i pro případ, kdy je některé z čísel m, n rovno 0.

Poznámka. Při studiu vektorových prostorů a jejich vzájemných vztahů jsme viděli zvláštní význam homomorfismů a izomorfismů vektorových prostorů, tedy zobrazení, která „zachovávaji“ operace ve vektorových prostorech. Analogické typy zobrazení zavedeme i pro libovolné algebraické struktury.

Definice

(a) Jsou-li $\mathscr{G} = (G; \cdot)$ a $\mathscr{H} = (H; \star)$ grupoidy, pak se zobrazení $f : G \to H$ nazývá **homomorfismus** grupoidu $\mathscr{G}$ do grupoidu $\mathscr{H}$, platí-li

$$\forall a, b \in G;\ f(ab) = f(a) \star f(b).$$

(b) Jestliže f je navíc bijektivní, pak se nazývá **izomorfismus** grupoidu $\mathscr{G}$ na grupoid $\mathscr{H}$.

(c) Řekneme, že grupoid $\mathscr{H}$ je **homomorfním obrazem** grupoidu $\mathscr{G}$, existuje-li surjektivní homomorfismus $\mathscr{G}$ na $\mathscr{H}$.

(d) Řekneme, že grupoid $\mathscr{H}$ je izomorfní s grupoidem $\mathscr{G}$, existuje-li izomorfismus $\mathscr{G}$ na $\mathscr{H}$.

Poznámka. Jestliže f je homomorfismus grupoidu $\mathscr{G}$ do grupoidu $\mathscr{H}$ a g je homomorfismus grupoidu $\mathscr{H}$ do grupoidu $\mathscr{K}$, pak je zřejmé, že jejich složení $f \circ g$ je homomorfismus $\mathscr{G}$ do $\mathscr{K}$. Podobně složení dvou izomorfismů grupoidů je opět izomorfismem. Navíc id_G je izomorfismem $\mathscr{G}$ na $\mathscr{G}$ a inverzní zobrazení f^{-1} k izomorfismu f grupoidu $\mathscr{G}$ na grupoid $\mathscr{H}$ je izomorfismem $\mathscr{H}$ na $\mathscr{G}$.
Relace „být izomorfní s“ je tedy ekvivalencí na třídě všech grupoidů, a proto indukuje rozklad třídy všech grupoidů na třídy navzájem izomorfních grupoidů. Grupoidy, které patří do téže třídy rozkladu, mají stejné algebraické vlastnosti.

Poznámka. Protože relace „být izomorfní s“ je symetrická, můžeme v případě, kdy grupoid $\mathscr{H}$ je izomorfní s grupoidem $\mathscr{G}$, říkat také, že grupoidy $\mathscr{G}$ a $\mathscr{H}$ jsou (navzájem) izomorfní.
Označení: $\mathscr{G} \cong \mathscr{H}$.

Příklad

Uvažujme grupoidy $\mathscr{N} = (\mathbb{N}; +)$ a $2\mathscr{N} = (2\mathbb{N}; +)$. Pak zobrazení $f : \mathbb{N} \to \mathbb{N}$ takové, že $\forall a \in \mathbb{N}; f(a) = 2a$, je homomorfismus $\mathscr{N}$ do $2\mathscr{N}$, který není surjektivní.
Označme $\bar{f} : \mathbb{N} \to 2\mathbb{N}$ zobrazení, v němž opět platí, že $\forall a \in \mathbb{N}; \bar{f}(a) = 2a$. Pak platí, že $\bar{f}$ je izomorfismus $\mathscr{N}$ na $2\mathscr{N}$, tedy $\mathscr{N}$ a $2\mathscr{N}$ jsou izomorfní.

Příklad

Ukažme, že grupoid $\mathscr{A} = (\{-1, 1\}; \cdot)$ je homomorfním obrazem grupoidu $\mathscr{Z} = (\mathbb{Z}; +)$. Uvažujme zobrazení $f : \mathbb{Z} \to \{-1, 1\}$ takové, že

$$\forall a \in 2\mathbb{Z}; f(a) = 1, \quad \forall a \in 2\mathbb{Z} + 1; \quad f(a) = -1.$$

Snadno lze ověřit, že f je homomorfismus $\mathscr{Z}$ na $\mathscr{A}$. Přitom je zřejmé, že $\mathscr{Z}$ a $\mathscr{A}$ nejsou izomorfní.

Příklad

Uvažujme grupoidy $\mathscr{R} = (\mathbb{R}; +)$ a $\mathscr{R}_1 = (\mathbb{R}; \oplus)$, kde $\forall a, b \in \mathbb{R}$; $a \oplus b = a + b + 1$. Grupoidy $\mathscr{R}$ a $\mathscr{R}_1$ jsou izomorfní, protože například zobrazení $f : \mathbb{R} \to \mathbb{R}$ takové, že $\forall a \in \mathbb{R}$; $f(a) = a - 1$, je izomorfismem $\mathscr{R}$ na $\mathscr{R}_1$.

Příklad

Sporem ověříme, že grupoidy $\mathscr{N}_1 = (\mathbb{N}; \cdot)$ a $2\mathscr{N}_1 = (2\mathbb{N}; \cdot)$ nejsou izomorfní. Nechť f je izomorfismus $\mathscr{N}_1$ na $2\mathscr{N}_1$ a nechť $f(1) = 2x$. Pak

$$2x = f(1) = f(1 \cdot 1) = f(1) \cdot f(1) = 2x \cdot 2x = 4x^2,$$

což ale neplatí pro žádné $x \in \mathbb{N}$, spor. Proto izomorfismus f neexistuje.

Definice

Nechť grupoid $\mathscr{G} = (G; \cdot)$ má jednotkový prvek e a $a \in G$. Pak se prvek $b \in G$ nazývá **inverzní** k prvku a, platí-li $ab = e = ba$.

Poznámka. V monoidu má každý prvek a nejvýše jeden inverzní prvek, který označujeme a^{-1}.

Věta

(a) Homomorfní obraz komutativního grupoidu je komutativním grupoidem.

(b) Homomorfní obraz pologrupy je pologrupou.

(c) Homomorfní obraz grupoidu s jednotkovým prvkem je grupoidem s jednotkovým prvkem.

(d) Homomorfní obraz monoidu je monoidem.

(e) Jestliže f je homomorfismus grupoidu $\mathscr{G}$ s jednotkovým prvkem na grupoid $\mathscr{H}$ a má-li prvek $a \in G$ inverzní prvek v $\mathscr{G}$, pak jeho obraz $f(a)$ má inverzní prvek v $\mathscr{H}$.

Důkaz. Na přednášce.

Poznámka. Tedy při homomorfismu f grupoidu $\mathscr{G}$ na grupoid $\mathscr{H}$ se jednotkový prvek e zobrazí na jednotkový prvek $f(e)$ a v případě monoidů plati $f(a^{-1}) = (f(a))^{-1}$.

Příklad

Žádné tvrzení z předchozí věty nelze obrátit. Například označme $\mathscr{G} = (\mathbb{C}; \circ)$, kde $\forall a, b \in \mathbb{C};\ a \circ b = a\overline{b}$, $\mathscr{H} = (\mathbb{R}_0^+; \cdot)$. Nechť $f : \mathbb{C} \to \mathbb{R}_0^+$ je takové zobrazení, že $\forall a \in \mathbb{C};\ f(a) = |a|$. Pak

$$f(a \circ b) = f(a\overline{b}) = |a\overline{b}| = |a| \cdot |\overline{b}| = |a| \cdot |b| = f(a) \cdot f(b),$$

tedy f je homomorfismus $\mathscr{G}$ do $\mathscr{H}$, který je navíc zřejmě surjektivní. Přitom $\mathscr{H}$ je komutativní monoid, v němž každý prvek (vyjma 0) má inverzní prvek, ale $\mathscr{G}$ nemá žádnou z uvedených vlastností.

Obsah

Definice

Grupou nazýváme každý monoid, v němž má každý jeho prvek inverzní prvek. Komutativní grupu $(G;\cdot)$, tedy takovou, v níž platí $\forall a,b \in G;\ ab = ba$, budeme také nazývat **abelovská grupa**.

Poznámka. Podle uvedené definice tedy platí, že grupoid $(G;\cdot)$ je grupou právě tehdy, když

1. $\forall a,b,c \in G;\ a(bc) = (ab)c$
2. $\exists e \in G\ \forall a \in G;\ ae = ea = a$
3. $\forall a \in G\ \exists a^{-1} \in G;\ aa^{-1} = a^{-1}a = e$.

Z podmínky 3 je zřejmé, že $\forall a \in G;\ (a^{-1})^{-1} = a$. Dále, jsou-li $a,b \in G$, pak

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = e,$$

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = e,$$

odkud $\forall a,b \in G;\ (ab)^{-1} = b^{-1}a^{-1}$.

Definice

Jestliže $\mathscr{G} = (G; \cdot)$ je taková grupa, že G má n prvků ($n \in \mathbb{N}$), pak řekneme, že grupa $\mathscr{G}$ má **konečný řád** n. Je-li G nekonečná, pak je grupa $\mathscr{G}$ **nekonečného řádu**.

Věta

Pologrupa $\mathscr{G}$ je grupou právě tehdy, když pro každé $a, b \in G$ jsou v $\mathscr{G}$ řešitelné rovnice $ax = b$, $ya = b$.

Důkaz. Na přednášce.

Poznámka. Předchozí věta nám dává užitečné kritérium pro určování, zdali je konečný grupoid grupou. Je-li totiž dána Cayleyova tabulka grupy konečného řádu, pak se v každém řádku a v každém sloupci musí vyskytovat všechny její prvky. Uvědomme si však, že tato podmínka je nutná, ale není postačující, protože například nezaručuje asociativnost operace.

Definice

Řekneme, že v grupoidu $(G;\cdot)$ platí **pravidlo o krácení**, jestliže pro každé prvky $a,b,c,d \in G$ platí

$$ca = cb \Rightarrow a = b, \quad ad = bd \Rightarrow a = b.$$

Věta

V každé grupě platí pravidlo o krácení.

Důkaz. Na přednášce.

Důsledek

Rovnice $ax = b$ a $ya = b$ jsou v každé grupě řešitelné jednoznačně.

Důkaz. Na přednášce.

Poznámka. Vzhledem k tomu, že grupa $\mathscr{G} = (G; \cdot)$ má právě jeden jednotkový prvek e a že ke každému jejímu prvku a v ní existuje právě jeden inverzní prvek a^{-1}, můžeme na G zavést nulární operaci „e“ a unární operaci „$^{-1}$“ tak, že $e : G^0 \to G$, $e : \emptyset \mapsto e$, $^{-1} : G \to G$, $^{-1} : a \mapsto a^{-1}$ pro každý $a \in G$. Grupu $\mathscr{G}$ pak můžeme uvažovat jako algebraickou strukturu $\mathscr{G} = (G; \cdot, e, ^{-1})$ s jednou binární, jednou nulární a jednou unární operací, pro které platí:

1. $\forall a, b, c \in G;\ a(bc) = (ab)c$
2. $\forall a \in G;\ ae = ea = a$
3. $\forall a \in G;\ aa^{-1} = a^{-1}a = e$.

Obsah

Definice

Nechť $(G;\cdot)$ je grupa, $\emptyset \neq A \subseteq G$. Řekneme, že podmnožina A **je uzavřená vzhledem k operaci** „$\cdot$“, platí-li $\forall a, b \in A;\ ab \in A$.

Poznámka. Nebude-li nebezpečí nedorozumění, budeme stručněji říkat, že A je uzavřená podmnožina v $\mathscr{G}$. Jestliže $A \neq \emptyset$ je uzavřená podmnožina v $\mathscr{G}$, pak restrikce operace $\cdot : G^2 \to G$ na A^2 je binární operací na množině A. Budeme ji nazývat **indukovanou operací** na množině A a k jejímu označení budeme používat také symbol $\cdot$.
Je-li $f : X \to Y$ zobrazení a je-li $Z \subseteq X$, pak **restrikcí** f na Z rozumíme zobrazení $\overline{f} : Z \to Y$ takové, že $\forall z \in Z;\ \overline{f}(z) = f(z)$.

Příklady

(a) Množina $\mathbb{N}$ je uzavřenou podmnožinou grupy $(\mathbb{Z};+)$.

(b) Množina $\{-1,1\}$ je uz. podmnožinou grupy $(\mathbb{Q}\setminus\{0\};\cdot)$.

(c) Množina $\mathbb{Z}_n = \{0,1,\ldots,n-1\}$ pro $1 < n \in \mathbb{N}$ není uzavřenou podmnožinou v grupě $(\mathbb{Z};+)$.

Definice

Nechť je dána grupa $\mathscr{G} = (G;\cdot)$ a nechť $\emptyset \neq A \subseteq G$. Pak $\mathscr{A} = (A;\cdot)$ se nazývá **podgrupou grupy** $\mathscr{G}$, je-li A uzavřenou podmnožinou v $\mathscr{G}$ a je-li $\mathscr{A}$ grupou vzhledem k indukované operaci. Skutečnost, že $\mathscr{A}$ je podgrupou grupy $\mathscr{G}$, budeme označovat $\mathscr{A} \leq \mathscr{G}$.

Příklady

(a) $(\mathbb{N};+) \not\leq (\mathbb{Z};+)$.

(b) $(\{-1,1\};\cdot) \leq (\mathbb{Q}\setminus\{0\};\cdot)$.

(c) Přestože $\mathscr{Z}_6 = (\mathbb{Z}_6;\oplus)$ je grupou vzhledem ke sčítání modulo 6, neplatí $(\mathbb{Z}_6;+) \leq (\mathbb{Z};+)$.

Věta

Struktura $(A;\cdot)$ je podgrupou grupy $(G;\cdot)$, právě tehdy, když platí:

1. $\forall a, b \in A;\ ab \in A$
2. $e \in A$
3. $\forall a \in A;\ a^{-1} \in A$.

Důkaz. Na přednášce.

Poznámka. Zřejmě vždy $(\{e\};\cdot) \leq (G;\cdot)$ a $(G;\cdot) \leq (G;\cdot)$. Podgrupu $(\{e\};\cdot)$ budeme nazývat **jednotkovou**. Jednotková podgrupa a celá grupa $(G;\cdot)$ se společně nazývají **triviální podgrupy** grupy $(G;\cdot)$.

Poznámka. Předpokládáme-li v předchozí větě, že $A \neq \emptyset$, pak podmínku 2 můžeme vynechat, protože jí lze v tomto případě odvodit z podmínek 1 a 3.

Poznámka. Víme, že grupu $\mathscr{G} = (G; \cdot)$ můžeme uvažovat jako algebraickou strukturu $\mathscr{G} = (G; \cdot, e, ^{-1})$. V tom případě pak dle předchozí věty platí, že $(A; \cdot)$ je podgrupou grupy $(G; \cdot)$, právě když je A uzavřená vzhledem ke všem operacím „$\cdot$“, „e“, „$^{-1}$“.

Další věta ukazuje, že podmínky z předchozí věty můžeme v případě neprázdné podmnožiny nahradit jedinou podmínkou.

Věta

Jestliže je $(G; \cdot)$ grupa, $\emptyset \neq A \subseteq G$, pak $(A; \cdot) \leq (G; \cdot)$ právě tehdy, když platí $\forall a, b \in A;\ ab^{-1} \in A$.

Důkaz. Na přednášce.

Věta

Průnik libovolného systému podgrup grupy $\mathscr{G} = (G; \cdot)$ je také podgrupou v $\mathscr{G}$.

Důkaz. Na přednášce.

Předchozí věta ukazuje na korektnost následující definice.

Definice

(a) Nechť $\mathscr{G} = (G; \cdot)$ je grupa, $M \subseteq G$. Pak podgrupu v $\mathscr{G}$, která je průnikem všech podgrup v $\mathscr{G}$ obsahujících M, nazveme **podgrupou v $\mathscr{G}$ generovanou množinou M** a označíme ji $\langle M \rangle$. Pro $M = \{a_1, a_2, \ldots, a_n\}$ píšeme také $\langle M \rangle = \langle a_1, a_2, \ldots, a_n \rangle$.

(b) Jestliže $\langle M \rangle = \mathscr{G}$, pak se M nazývá **množina generátorů** grupy $\mathscr{G}$ (nebo říkáme, že M **generuje** grupu $\mathscr{G}$).

(c) Jestliže $a \in G$, pak $\langle a \rangle$ se nazývá **cyklická podgrupa v $\mathscr{G}$ generovaná prvkem a**.

(d) Grupa $\mathscr{G}$ se nazývá **cyklická**, existuje-li v ní prvek a takový, že $\langle a \rangle = \mathscr{G}$.

Vidíme, že podgrupa generovaná podmnožinou grupy se definuje analogicky jako lineární obal podmnožiny vektorového prostoru. Přitom je známo, že lineární obal neprázdné podmnožiny se skládá právě ze všech lineárních kombinací vektorů z této podmnožiny. Ukážeme si, že podobně přehledným způsobem lze charakterizovat i prvky podgrupy generované podmnožinou grupy. Nejprve rozšíříme pojem mocniny prvku. Připomeňme, že jsme definovali přirozené mocniny prvků pologrupy a celé nezáporné mocniny prvků monoidu. Pro prvky grupy můžeme zavést i celé záporné mocniny.

Definice

Nechť $\mathscr{G} = (G; \cdot)$ je grupa a nechť $a \in G$. Jestliže $n \in \mathbb{N}$, pak $(-\mathbf{n})$**-tou mocninou prvku a** rozumíme prvek $a^{-n} \in G$ takový, že $a^{-n} = (a^n)^{-1}$.

Poznámka. Pro každé $n \in \mathbb{N}$ platí $a^{-n} = (a^{-1})^n$.

Věta

Jestliže jsou a, b prvky grupy $(G; \cdot)$ a $m, n \in \mathbb{Z}$, pak platí

(a) $a^m \cdot a^n = a^{m+n}$

(b) $(a^m)^n = a^{mn}$

(c) jestliže $ab = ba$, pak $(ab)^n = a^n b^n$.

Důkaz. Na přednášce.

Poznámka. Na základě bodu (a) předchozí věty je zřejmé, že množina $\{a^n; n \in \mathbb{Z}\}$ spolu s indukovanou operací je podgrupou grupy $\mathscr{G} = (G; \cdot)$ a že a je prvkem této podgrupy. Přitom každá podgrupa v $\mathscr{G}$, která obsahuje a, musí obsahovat také všechny celé mocniny prvku a. Platí tedy, že $\langle a \rangle = (\{a^n; n \in \mathbb{Z}\}; \cdot)$. Zřejmě je $\langle a \rangle$ abelovská.

Definice

Jsou-li všechny celé mocniny prvku $a \in G$ navzájem různé, pak řekneme, že **a má nekonečný řád**. V opačném případě říkáme, že prvek **a je konečného řádu**.

Poznámka. Nechť prvek $a \in G$ je konečného řádu. Pak existují $k, l \in \mathbb{Z}$, $k > l$, taková, že $a^k = a^l$. Platí tedy $a^{k-l} = e$, kde $k - l > 0$. Pro a proto existují mocniny s přirozenými exponenty, které jsou rovny e.

Definice

Je-li prvek $a \in G$ konečného řádu, pak jeho **řádem** rozumíme nejmenší číslo $n \in \mathbb{N}$ takové, že $a^n = e$.

Věta

Řád prvku a je roven řádu cyklické podgrupy $\langle a \rangle$.

Důkaz. Na přednášce.

Nyní už můžeme řešit otázku charakterizace prvků podgrupy $\langle M \rangle$ grupy $(G;\cdot)$ generované libovolnou podmnožinou $M \subseteq G$.

Věta

Nechť $\mathscr{G} = (G;\cdot)$ je grupa a $M \subseteq G$.

(a) Jestliže $M = \emptyset$, pak $\langle M \rangle = (\{e\};\cdot)$ (jednotková grupa).

(b) Jestliže $M \neq \emptyset$, pak
$\langle M \rangle = \{a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n};\ n \in \mathbb{N},\ a_i \in M,\ \varepsilon_i = \pm 1,\ i = 1, \dots n\}$.

Důkaz. Na přednášce.

Tedy, jestliže $M \neq \emptyset$ je množinou generátorů grupy $(G;\cdot)$, pak lze každý prvek z G vyjádřit ve tvaru součinu konečného počtu prvků z M a prvků inverzních k prvkům z M.

Příklad

Každá z množin $\{2,3\}$, $\{1\}$, $\{-1\}$ je množinou generátorů grupy $\mathscr{Z} = (\mathbb{Z};+)$. (Tedy $\mathscr{Z}$ je cyklická grupa.) Množina $\{2\}$ není množinou generátorů této grupy.

Operaci násobení prvků v libovolném grupoidu nyní rozšíříme na násobení podmnožin.

Definice

Nechť $(G;\cdot)$ je grupoid a $A, B \subseteq G$. **Součinem** AB rozumíme podmnožinu v G takovou, že

$$AB = \{ab;\ a \in A, b \in B\}.$$

Jestliže $a \in G$, $B \subseteq G$, pak místo $\{a\}B$ píšeme stručně aB a místo $B\{a\}$ píšeme Ba.

Příklad

Uvažujme grupu $\mathscr{Z}_6 = (\mathbb{Z}_6; \oplus)$ a její podmnožiny $A = \{1,3,4\}$, $B = \{2,5\}$. Pak $A \oplus B = \{3,0,5,2\}$

Definice

Jestliže $\mathscr{H} = (H; \cdot)$ je podgrupa grupy $\mathscr{G} = (G; \cdot)$, $a \in G$, pak **levou třídou** (resp. **pravou třídou**) **prvku a podle** $\mathscr{H}$ nazýváme množinu aH (resp. Ha).

Věta

Systém všech levých tříd prvků grupy $\mathscr{G} = (G; \cdot)$ podle podgrupy $\mathscr{H} = (H; \cdot)$ je rozkladem množiny G.

Důkaz. Na přednášce.

Definice

Rozklad $\{aH;\, a \in G\}$ nazýváme **levý rozklad grupy** $\mathscr{G}$ **podle podgrupy** $\mathscr{H}$ a značíme jej $G/_l H$.

Poznámka. Protože $eH = H$, platí, že $H \in G/_l H$.

Také systém všech pravých tříd prvků grupy $\mathscr{G} = (G; \cdot)$ podle podgrupy $\mathscr{H} = (H; \cdot)$ je rozkladem na G. Rozklad $\{Ha;\, a \in G\}$ nazýváme **pravý rozklad grupy $\mathscr{G}$ podle podgrupy $\mathscr{H}$** a značíme jej $G/_pH$. Opět platí, že $H \in G/_pH$.

Věta

Nechť $\mathscr{H} = (H; \cdot)$ je podgrupa $\mathscr{G} = (G; \cdot)$, nechť $a, b \in G$. Pak

(a) $aH = bH \Leftrightarrow b^{-1}a \in H$

(b) $Ha = Hb \Leftrightarrow ab^{-1} \in H$.

Důkaz. Na přednášce.

Poznámka. Připomeňme si, že dvě množiny A a B se nazývaji **ekvivalentní**, existuje-li alespoň jedno bijektivní zobrazení jedné z nich na druhou. Je zřejmé, že vztah „být ekvivalentní s“ je relací ekvivalence. Pro dvě konečné množiny platí, že jsou ekvivalentní, právě když mají stejný počet prvků.

Věta

Pro libovolnou podgrupu $(H;\cdot)$ grupy $(G;\cdot)$ platí, že rozklady $G/_l H$ a $G/_p H$ jsou ekvivalentní.

Důkaz. Na přednášce.

Definice

Mají-li rozklady $G/_l H$ a $G/_p H$ nekonečný počet tříd, pak řekneme, že podgrupa $(H;\cdot)$ má **nekonečný index**. Jestliže rozklady $G/_l H$ a $G/_p H$ mají konečný počet tříd, pak řekneme, že $(H;\cdot)$ má **konečný index**. Počet tříd každého z uvedených rozkladů se nazývá **index podgrupy** $(H;\cdot)$.

Věta

Nechť $(H;\cdot) \leq (G;\cdot)$, $a, b \in G$. Pak levá třída aH je ekvivalentní s pravou třídou Hb. (Tedy v případě konečné podgrupy $(H;\cdot)$ má každá levá třída a každá pravá třída podle H stejný počet prvků jako H.)

Důkaz. Na přednášce.

Věta Lagrangeova

Nechť $\mathscr{G} = (G; \cdot)$ je konečná grupa řádu n, $\mathscr{H} = (H; \cdot)$ její podgrupa řádu k a nechť index $\mathscr{H}$ je roven i. Pak platí $n = k\dot{i}$.

Důkaz. Na přednášce.

Poznámka. Lagrangeova věta má mimo jiné velký praktický význam při hledání podgrup konečné grupy. Podle této věty totiž řád podgrupy dělí řád grupy, a tedy můžeme předem eliminovat všechny podmnožiny s počty prvků, které nedělí řád grupy.

Důsledek

Jestliže $\mathscr{G} = (G; \cdot)$ je konečná grupa a $a \in G$, pak řád prvku a dělí řád grupy $\mathscr{G}$.

Příklad

Grupa $(\mathbb{Z}_p; \oplus)$, kde p je prvočíslo nemá netriviální podgrupy. Proto řád každého prvku $a \neq 0$ je roven číslu p.

Ke každé podgrupě $\mathscr{H} = (H; \cdot)$ grupy $\mathscr{G} = (G; \cdot)$ jsme sestrojili dva rozklady, $G/_l H$ a $G/_p H$. Je zřejmé, že v abelovské grupě vždy platí $G/_l H = G/_p H$. Zde dokonce pro každý prvek $a \in G$ platí $aH = Ha$. V nekomutativní grupě však pro podgrupu $\mathscr{H}$ může platit, že $G/_l H$ a $G/_p H$ jsou různé rozklady.

Příklad

Nechť S_3 je množina všech permutací na množině $\{1,2,3\}$. Pak $\mathscr{S}_3 = (S_3; \circ)$, kde „$\circ$“ je operace skládání permutací, je nekomutativní grupa. Pro množinu $H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$ platí $(H; \circ) \leq \mathscr{S}_3$, přičemž $S_3/_l H \neq S_3/_p H$.

Definice

Řekneme, že podgrupa $\mathscr{H} = (H; \cdot)$ grupy $\mathscr{G} = (G; \cdot)$ je **normální** v $\mathscr{G}$, jestliže $G/_l H = G/_p H$.

Poznámka. Místo názvu „normální podgrupa“ se někdy používá také označení „normální dělitel“ nebo „invariantní podgrupa“. V případě normální podgrupy $(H;\cdot)$ budeme společný levý a pravý rozklad označovat také stručněji G/H.

Věta

Jestliže $\mathscr{H} = (H;\cdot)$ je podgrupa grupy $\mathscr{G} = (G;\cdot)$, pak jsou následující podmínky ekvivalentní:

1. $\mathscr{H}$ je normální v $\mathscr{G}$
2. $\forall a \in G;\ aH = Ha$
3. $\forall a \in G,\ h \in H;\ aha^{-1} \in H$.

Důkaz. Na přednášce.

Poznámka. Nechť $(G;\cdot)$ je grupa a $c, d \in G$. Pak se prvek d nazývá **konjugovaný** s prvkem c, existuje-li prvek $x \in G$ takový, že $d = xcx^{-1}$. Podle předchozí věty tedy platí, že podgrupa $(H;\cdot)$ je normální v $(G;\cdot)$ právě tehdy, obsahuje-li s každým svým prvkem také všechny prvky s ním konjugované.

Poznámka. Skutečnost, že je $\mathscr{H} = (H; \cdot)$ je normální podgrupa v $\mathscr{G} = (G; \cdot)$ budeme označovat $\mathscr{H} \trianglelefteq \mathscr{G}$. Zřejmě pro každou grupu $\mathscr{G}$ platí, že $(\{e\}; \cdot) \trianglelefteq \mathscr{G}$ a $\mathscr{G} \trianglelefteq \mathscr{G}$.

Věta

Jestliže podgrupa $\mathscr{H} = (H; \cdot)$ grupy $\mathscr{G} = (G; \cdot)$ má index 2, pak platí $\mathscr{H} \trianglelefteq \mathscr{G}$.

Důkaz. Na přednášce.

Definice

Nechť $\mathscr{G} = (G; \cdot)$ je grupa $\mathscr{H} \leq \mathscr{G}$, $\mathscr{K} \leq \mathscr{G}$. Pak **spojením** $\mathscr{H} \vee \mathscr{K}$ těchto podgrup rozumíme nejmenší podgrupu v $\mathscr{G}$ obsahující obě podgrupy $\mathscr{H}$ a $\mathscr{G}$. (Pomocí dříve zavedené symboliky tedy $\mathscr{H} \vee \mathscr{K} = \langle H \cup K \rangle$.)

Už víme, jak obecně vyjádřit prvky, které patří do podgrupy $\langle M \rangle$ generované neprázdnou podmnožinou $M \subseteq G$. Pro případ spojení dvou podgrup můžeme toto vyjádření zjednodušit.

Věta

Jestliže $\mathscr{H} \leq \mathscr{G}$, $\mathscr{K} \leq \mathscr{G}$, pak

$$\mathscr{H} \vee \mathscr{K} = (\{a_1 b_1 a_2 b_2 \dots a_m b_m;\ a_i \in H,\ b_i \in K, i = 1, 2, \dots, m\}; \cdot).$$

Důkaz. Na přednášce.

Ukažme si nyní, že v případě normálních podgrup můžeme tento výsledek ještě zjednodušit.

Věta

Jestliže $\mathscr{H} \trianglelefteq \mathscr{G}$, $\mathscr{K} \trianglelefteq \mathscr{G}$, pak $\mathscr{H} \vee \mathscr{K} = (HK; \cdot) = (KH; \cdot)$.

Důkaz. Na přednášce.

Definice

Jestliže $\mathscr{H}_\alpha \leq \mathscr{G}$ $(\alpha \in I)$, pak **spojením** podgrup $\mathscr{H}_\alpha$ rozumíme podgrupu $\langle \bigcup_{\alpha\in I} \mathscr{H}_\alpha \rangle$ v $\mathscr{G}$, kterou označíme $\bigvee_{\alpha\in I} \mathscr{H}_\alpha$. V případě konečného počtu podgrup $\mathscr{H}_1, \ldots, \mathscr{H}_n$ používáme označení (podobně jako pro dvě podgrupy) $\mathscr{H}_1 \vee \cdots \vee \mathscr{H}_n$.

Věta

(a) Průnik libovolného systému normálních podgrup grupy $\mathscr{G}$ je normální podgrupou v $\mathscr{G}$.

(b) Spojení konečného počtu normálních podgrup grupy $\mathscr{G}$ je normální podgrupou v $\mathscr{G}$.

Důkaz. Na přednášce.

Věta

Nechť $\mathscr{G} = (G; \cdot)$ a $\mathscr{N} = (N; \cdot)$ její normální podgrupa. Pro libovolné prvky $a, b \in G$ položme $aN \cdot bN = abN$. Pak platí, že „$\cdot$“ je binární operace na faktorové množině G/N a $\mathscr{G}/\mathscr{N} = (G/N; \cdot)$ je grupa.

Důkaz. Na přednášce.

Definice

Grupa $\mathscr{G}/\mathscr{N}$ z předchozí věty se nazývá **faktorová** (nebo **podílová**) **grupa** grupy $\mathscr{G}$ podle normální podgrupy $\mathscr{N}$.

Příklad

Uvažujme podgrupu $4\mathscr{Z} = (4\mathbb{Z}; +)$ grupy $\mathscr{Z} = (\mathbb{Z}; +)$, kde $4\mathbb{Z} = \{4a; a \in \mathbb{Z}\}$. Zřejmě $4\mathscr{Z} \trianglelefteq \mathscr{Z}$, neboť $\mathscr{Z}$ je abelovská grupa. Pro faktorovou grupu $\mathscr{Z}/4\mathscr{Z} = (\mathbb{Z}/4\mathbb{Z}; \oplus)$ platí, že $\mathbb{Z}/4\mathbb{Z} = \{4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\}$ a že sčítání je dáno tabulkou:

$\oplus$	$4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$4\mathbb{Z}$	$4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$1+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4\mathbb{Z}$
$2+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4\mathbb{Z}$	$1+4\mathbb{Z}$
$3+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$

Poznámka. Požadavek normálnosti podgrupy $\mathscr{N}$ v poslední větě je nutný, protože v opačném případě bychom nedefinovali operaci násobení tříd (např. levých) korektně a výsledek by závisel na výsledku výběru reprezentantů z těchto tříd.

Obsah

Definice

Nechť $\mathscr{G} = (G; \cdot)$ a $\mathscr{G}' = (G'; \star)$ jsou grupy a $f : G \to G'$ zobrazení. Pak se f nazývá **homomorfismus grupy $\mathscr{G}$ do grupy $\mathscr{G}'$**, jestliže pro každé $a, b \in G$ platí $f(a \cdot b) = f(a) \star f(b)$. Je-li homomorfismus f bijektivní, pak se nazývá **izomorfismus $\mathscr{G}$ na $\mathscr{G}'$**.

Poznámka. Homomorfismus grupy $\mathscr{G}$ do grupy $\mathscr{G}'$ se definuje stejně jako homomorfismus grupoidu $\mathscr{G}$ do grupoidu $\mathscr{G}'$, tedy, že se pro něj vyžaduje jen přenášení binární operace násobení. Grupu však můžeme chápat také jako algebraickou strukturu s jednou binární, jednou nulární a jednou unární operací. Je tedy otázka, zda je použitá definice homomorfismu dostatečná. Pozitivní odpověď je obsažena v následující větě.

Věta

Nechť f je homomorfismus grupy $\mathscr{G}$ do grupy $\mathscr{G}'$ a nechť e je jednotkový prvek grupy $\mathscr{G}$ a e' je jednotkový prvek grupy $\mathscr{G}'$. Pak

(a) $f(e) = e'$

(b) $\forall a \in G;\ f(a^{-1}) = (f(a))^{-1}$.

Důkaz. Na přednášce.

Definice

Nechť f je homomorfismus grupy $\mathscr{G}$ do grupy $\mathscr{G}'$ a nechť e' je jednotkový prvek v $\mathscr{G}'$. Pak množinu $\mathrm{Ker} f = \{a \in G;\ f(a) = e'\}$ nazýváme **jádro homomorfismu** f.

Věta

Homomorfismus f grupy $\mathscr{G}$ do grupy $\mathscr{G}'$ je injektivní právě tehdy, když $\mathrm{Ker} f = \{e\}$.

Důkaz. Na přednášce.

Podle definice je $\mathrm{Ker} f$ podmnožinou v G. Ukažme, že jádra homomorfismů mají v grupě $\mathscr{G}$ důležité postavení.

Věta

Nechť f je homomorfismus grupy $\mathscr{G}$ do grupy $\mathscr{G}'$. Pak $\mathrm{Ker} f$ je normální podgrupou v $\mathscr{G}$.

Důkaz. Na přednášce.

Ukážeme nyní, že také obráceně, každá normální podgrupa grupy $\mathscr{G}$ je jádrem homomorfismu grupy $\mathscr{G}$ do některé grupy.

Věta

Jestliže $\mathscr{N} = (N; \cdot)$ je normální podgrupa grupy $\mathscr{G} = (G; \cdot)$, pak zobrazení $\nu : G \to G/N$ takové, že $\nu(a) = aN$ pro každý prvek $a \in G$, je homomorfismem grupy $\mathscr{G}$ na faktorovou grupu $\mathscr{G}/\mathscr{N}$. Přitom platí, že $\mathrm{Ker}\nu = N$.

Důkaz. Na přednášce.

Definice

Homomorfismus ν z předchozí věty se nazývá **přirozený homomorfismus** grupy $\mathscr{G}$ na faktorovou grupu $\mathscr{G}/\mathscr{N}$.

Poznámka. Připomeňme si, že grupoidy $\mathscr{G}$ a $\mathscr{G}'$ se nazývají izomorfní (označení $\mathscr{G} \cong \mathscr{G}'$), existuje-li alespoň jeden izomorfismus jednoho z nich na druhý. Přitom relace „být izomorfní“ je relací ekvivalence na třídě všech grupoidů. Grupoidy, které patří do téže třídy odpovídajícího rozkladu, mají stejné algebraické vlastnosti. Pro grupy jsme definovali pojem izomorfismu stejně jako pro grupoidy, proto také každá grupa jednoznačně patří do některé třídy uvedeného rozkladu a platí, že všechny grupoidy, které jsou izomorfní s danou grupou, jsou také grupami.

Příklad

Uvažujme grupy $(\mathbb{R}^+;\cdot)$ a $(\mathbb{R};+)$ a zobrazení $\log : \mathbb{R}^+ \to \mathbb{R}$ takové, že $\log : x \mapsto \log x$. Je zřejmé, že log je bijektivní zobrazení $\mathbb{R}^+$ na $\mathbb{R}$, a je známo, že pro každé $x, y \in \mathbb{R}^+$ platí $\log(xy) = \log x + \log y$. Tedy $(\mathbb{R}^+;\cdot) \cong (\mathbb{R};+)$.

Věta o homomorfismu grup

Nechť f je surjektivní homomorfismus grupy $\mathscr{G}$ na grupu $\mathscr{G}'$. Pak je grupa $\mathscr{G}'$ izomorfní s faktorovou grupou $\mathscr{G}/\mathrm{Ker}f$. Přitom platí, že existuje právě jeden izomorfismus g grupy $\mathscr{G}'$ na faktorovou grupu $\mathscr{G}/\mathrm{Ker}f$ takový, že $f \circ g$ je přirozeným homomorfismem $\mathscr{G}$ na $\mathscr{G}/\mathrm{Ker}f$.

Důkaz. Na přednášce.

Poznámka. Nechť $\mathscr{A}$ je některá třída grup. Jestliže platí, že danou vlastnost mají právě všechny grupy z třídy $\mathscr{A}$ a všechny grupy, které jsou izomorfní s některou grupou z $\mathscr{A}$, pak říkáme, že tuto vlastnost „**mají, až na izomorfismus**“, právě grupy z třídy $\mathscr{A}$. Předchozí věta říká, že homomorfními obrazy grupy $\mathscr{G}$ jsou, až na izomorfismus, právě všechny faktorové grupy podle normálních podgrup grupy $\mathscr{G}$.

Příklad

Určete všechny homomorfní obrazy grupy $\mathscr{Z} = (\mathbb{Z}; +)$. Protože $\mathscr{Z}$ je abelovská grupa, je každá její podgrupa normální. Přitom platí, že podgrupami grupy $\mathscr{Z}$ jsou právě všechny struktury $n\mathscr{Z} = (n\mathbb{Z}; +)$, kde $n\mathbb{Z} = \{na; a \in \mathbb{Z}\}$. (Speciálně $0\mathbb{Z} = \{0\}$, $1\mathbb{Z} = \mathbb{Z}$.) Faktorová grupa $\mathscr{Z}/n\mathscr{Z}$ je izomorfní s grupou $\mathscr{Z}_n = (\mathbb{Z}_n; \oplus)$ čísel $\{0, 1, \ldots, n-1\}$ se sčítáním modulo n. Podle předchozí věty tedy platí, že homomorfními obrazy grupy $\mathscr{Z}$ jsou, až na izomorfismus, právě všechny grupy $\mathscr{Z}_n$, $(n > 0)$.

Věta

Jestliže f je homomorfismus grupy $\mathscr{G}$ do grupy $\mathscr{G}'$, pak $\mathrm{Im}f = \{f(x); x \in G\} \leq \mathscr{G}'$ a navíc je $\mathrm{Im}f$ izomorfní s faktorovou grupou $\mathscr{G}/\mathrm{Ker}f$.

Důkaz. Na přednášce.

Obsah

Úloha vytvořit homomorfní obrazy dané algebraické struktury se vyskytuje v algebře (ale i v dalších matematických disciplínách a jejich aplikacích) velmi často. Přitom nejjednodušším řešením je vždy konstrukce odpovídajících faktorových algebraických struktur.

V případě grup k tomu postačuje nalezení všech normálních podgrup. V obecném případě ale analogické podstruktury (až na výjimky – např. pro okruhy) neexistují. Proto je nutné ke konstrukci faktorových struktur v obecnosti užít univerzálnější metodu založenou na pojmu kongruence. Ukážeme si tento přístup na grupoidech. Pro grupy, které jsou speciálním případem grupoidů, jsou však obě konstrukce faktorových grup (tj. pomocí normálních podgrup a pomocí kongruencí) ekvivalentní.

Definice

Nechť $\mathscr{G} = (G; \cdot)$ je grupoid. Pak **kongruencí** grupoidu $\mathscr{G}$ rozumíme každou relaci ekvivalence ρ na G, pro kterou je splněna podmínka

$$\forall a, b, c, d \in G; (\langle a, b\rangle \in \rho \wedge \langle c, d\rangle \in \rho) \Rightarrow \langle ac, bd\rangle \in \rho.$$

Příklad

Jestliže $n \in \mathbb{N}$, pak relace kongruence podle modulu n je grupoidovou kongruencí na grupoidu $\mathscr{Z}' = (\mathbb{Z}; \cdot)$. Vskutku, nechť $a, b, c, d \in \mathbb{Z}$, $a \equiv b (mod\, n)$, $c \equiv d (mod\, n)$. Pak existují $x, y \in \mathbb{Z}$ taková, že $a - b = nx$, $c - d = ny$. Tedy

$$ac - bd = ac - ad + ad - bd = a(c - d) + (a - b)d =$$

$$= any + nxd = n(ay + xd),$$

a proto $ac \equiv bd (mod\, n)$.

Věta o homomorfismu grup

Jestliže ρ je kongruence grupoidu $\mathscr{G} = (G; \cdot)$ a jestliže pro libovolné $a, b \in G$ položíme $[a]_\rho \cdot [b]_\rho = [a \cdot b]_\rho$, pak $(G/\rho; \cdot)$ je grupoid.

Důkaz. Na přednášce.

Definice

Grupoid $\mathscr{G}/\rho = (G/\rho; \cdot)$ z předchozí věty se nazývá faktorový grupoid grupoidu $\mathscr{G}$ podle kongruence ρ.

Příklad

Uvažujeme grupoid $\mathscr{Z}' = (\mathbb{Z}; \cdot)$ a kongruenci podle modulu n ($n \in \mathbb{N}$). Pak faktorovým grupoidem $\mathscr{Z}'$ podle této kongruence je množina všech zbytkových tříd podle modulu n. Přitom např. pro $n = 4$ je Cayleyova tabulka pro násobení ve faktorovém grupoidu následující:

$\otimes$	$4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$4\mathbb{Z}$	$4\mathbb{Z}$	$4\mathbb{Z}$	$4\mathbb{Z}$	$4\mathbb{Z}$
$1+4\mathbb{Z}$	$4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$2+4\mathbb{Z}$	$4\mathbb{Z}$	$2+4\mathbb{Z}$	$4\mathbb{Z}$	$2+4\mathbb{Z}$
$3+4\mathbb{Z}$	$4\mathbb{Z}$	$3+4\mathbb{Z}$	$2+4\mathbb{Z}$	$1+4\mathbb{Z}$

Definice

Jestliže $\mathscr{G} = (G; \cdot)$ je grupa, pak **grupovou kongruencí** grupy $\mathscr{G}$ rozumíme právě každou kongruenci grupoidu $(G; \cdot)$. (Proto přívlastek „grupová“ můžeme vynechávat.)

Věta

Nechť ρ je kongruence grupy $\mathscr{G}$ a nechť $a, b \in G$. Pak platí:

$$\langle a, b \rangle \in \rho \Rightarrow \langle a^{-1}, b^{-1} \rangle \in \rho .$$

Důkaz. Na přednášce.

Věta

Nechť $\mathscr{H} = (H; \cdot)$ je podgrupa grupy $\mathscr{G} = (G; \cdot)$. Pak ekvivalence ρ_H na G odpovídající levému rozkladu $\mathscr{G}/_l\mathscr{H}$ grupy $\mathscr{G}$ podle $\mathscr{H}$ je kongruencí grupy $\mathscr{G}$ právě tehdy, když $\mathscr{H}$ je normální podgrupou.

Důkaz. Na přednášce.

Věta

Binární relace ρ na G je kongruencí grupy $\mathscr{G} = (G; \cdot)$ právě tehdy, když existuje normální podgrupa $\mathscr{N} = (N; \cdot)$ grupy $\mathscr{G}$ taková, že

$$\forall a, b \in G; \langle a, b \rangle \in \rho \Leftrightarrow b^{-1}a \in N.$$

V takovém případě je relace ρ ekvivalencí indukovanou rozkladem G/N.

Důkaz. Na přednášce.

Poznámka. Vidíme tedy, že existuje vzájemně jednoznačná korespondence mezi normálními podgrupami grupy $\mathscr{G}$ a kongruencemi této grupy, která je dána vztahy z předchozích vět. Odpovídající si kongruence ρ a normální podgrupa $\mathscr{N}$ přitom určují stejnou faktorovou strukturu, kterou proto můžeme označovat $\mathscr{G}/\rho$ nebo $\mathscr{G}/\mathscr{N}$. (Mimo jiné odtud dostáváme, že faktorový grupoid grupy je vždy grupou.)

Obsah

Dále se zaměříme na vlastnosti cyklických grup a dokážeme, že libovolnou grupu lze interpretovat jako některou grupu permutací. Připomeňme, že grupa $\mathscr{G} = (G; \cdot)$ se nazývá cyklická právě tehdy, existuje-li prvek $a \in G$ takový, že $\mathscr{G} = \langle a \rangle$. Příklady cyklických grup jsou $\mathscr{Z} = (Z; +)$, kde $\mathscr{Z} = \langle 1 \rangle = \langle -1 \rangle$, popř. $\mathscr{Z}_n = (\mathbb{Z}_n; \oplus)$ $(n \in \mathbb{N})$, kde vždy $\mathscr{Z}_n = \langle 1 \rangle$. Existují tedy cyklické grupy nekonečného řádu i libovolného konečného řádu.

Věta

Každá nekonečná cyklická grupa je izomorfní s grupou $\mathscr{Z} = (Z; +)$. Každá konečná cyklická grupa řádu n je izomorfní s grupou $\mathscr{Z}_n = (\mathbb{Z}_n; \oplus)$.

Důkaz. Na přednášce.

Poznámka. Vidíme tedy, že, až na izomorfismus, existuje jediná cyklická grupa nekonečného řádu, a to $\mathscr{Z} = (Z; +)$. Podobně pro libovolné $n \in \mathbb{N}$ existuje cyklická grupa konečného řádu n která je také, až na izomorfismus, určena jednoznačně.

Věta

(a) Každá podgrupa a každý homomorfní obraz cyklické grupy je cyklickou grupou.

(b) Každá podgrupa nekonečné cyklické grupy různá od jednotkové grupy je nekonečnou cyklickou grupou.

Důkaz. Na přednášce.

Věta

(a) Cyklická grupa $\mathscr{Z} = (Z; +)$ má právě dva generátory 1 a -1.

(b) Jestliže $\mathscr{G} = \langle a \rangle$ je konečná cyklická grupa řádu n a $k \in \mathbb{N}$, pak $\langle a^k \rangle = \mathscr{G}$ právě tehdy, když jsou čísla k a n nesoudělná.

Důkaz. Na přednášce.

Věta

Každá grupa prvočíselného řádu je cyklická.

Důkaz. Na přednášce.

Důsledek

Pro každé prvočíslo p existuje, až na izomorfismus, právě jedna grupa řádu p.

Důkaz. Na přednášce.

Definice

Víme, že pro libovolnou konečnou neprázdnou množinu M je množina všech permutací na M uvažovaná spolu s operací skládání permutací grupou. Označujeme ji $\mathscr{S}(M)$ a nazýváme **symetrická grupa** množiny M. Všechny sudé permutace na M spolu s operací skládání permutací tvoří podgrupu $\mathscr{A}(M) \leq \mathscr{S}(M)$, kterou nazýváme **alternující grupa** množiny M.

Věta

Jestliže M je konečná neprázdná množina, pak alternující grupa $\mathscr{A}(M)$ je normální podgrupou symetrické grupy $\mathscr{S}(M)$.

Důkaz. Na přednášce.

Ukažme si nyní, že grupy permutací mají v teorii grup zcela obecný význam, protože v sobě obsahují, samozřejmě až na izomorfismus, jakoukoliv grupu. Abychom se o tom přesvědčili, rozšiřme pojem permutace i na nekonečné množiny.

Definice

Jestliže M je libovolná neprázdná množina, pak **permutací** na M budeme rozumět libovolné bijektivní zobrazení množiny M na množinu M.

Poznámka. Je zřejmé, že označíme-li $S(M)$ množinu všech permutací na M, pak $S(M)$ tvoří spolu se skládáním permutací grupu, kterou budeme také označovat $\mathscr{S}(M) = (S(M); \circ)$ a nazývat symetrickou grupou množiny M.

Cayleyova věta

Každá grupa je izomorfní s některou podgrupou symetrické grupy některé množiny.

Důkaz. Na přednášce.

Obsah

Obsah

V této části se budeme věnovat algebraickým strukturám se dvěma binárními operacemi. Připomeneme základní definice.

Definice

Algebraická struktura $\mathscr{M} = (M; +, \cdot)$ se nazývá **okruh**, platí-li, že $(M; +)$ je abelovská grupa, $(M; \cdot)$ je pologrupa a násobení je distributivní zleva i zprava vzhledem ke sčítánít, tj.

$$\forall a, b, c \in M;\ a(b+c) = ab + ac, \quad (b+c)a = ba + ca.$$

Poznámka. Jestliže $a, b \in M$, označme $a - b = a + (-b)$. Je zřejmé, že odčítání je také binární operací na M. Víme, že násobení je distributivní také vzhledem k odčítání, tedy že

$$\forall a, b, c \in M;\ a(b-c) = ab - ac, \quad (b-c)a = ba - ca.$$

Nulový prvek okruhu M (tj. nulový prvek aditivní grupy $(M; +)$) budeme označovat o. Platí $\forall a \in M;\ ao = o = oa$, což se někdy vyjadřuje formulací, že o je **agresivní prvek** pologrupy $(M; \cdot)$. Dále platí, že $\forall a, b \in M;\ a(-b) = (-a)b = -ab$.

Definice

(a) Jestliže pro okruh $\mathscr{M} = (M; +, \cdot)$ platí, že pologrupa $(M; \cdot)$ je komutativní, pak se i **okruh** $\mathscr{M}$ nazývá **komutativní**.

(b) Je-li $(M; \cdot)$ monoid s jednotkovým prvkem e, pak se e nazývá **jednotkový prvek okruhu** $\mathscr{M}$.

Příklady

(a) $\mathscr{Z} = (\mathbb{Z}; +, \cdot)$ je komutativní okruh s jednotkovým prvkem 1.

(b) $\mathscr{Z}_n = (\mathbb{Z}; \oplus, \otimes)$, kde operace „$\oplus$“ a „$\otimes$“ jsou sčítání a násobení modulo n, je komutativní okruh s jednotkovým prvkem 1.

(c) $2\mathscr{Z} = (2\mathbb{Z}; +, \cdot)$ je komutativní okruh, který nemá jednotkový prvek.

Příklady

(a) Množina všech polynomů jedné proměnné nad $\mathscr{R}$ (popř. nad libovolným číselným tělesem $\mathscr{T}$) je vzhledem ke sčítání a násobení polynomů komutativním okruhem, v němž je jednotkovým prvkem konstatní polynom 1.

(b) Množina $M_n(\mathscr{T})$ všech čtvercových matic stupně $n \geq 2$ nad číselným tělesem $\mathscr{T}$ tvoří okruh vzhledem ke sčítání a násobení matic. Tento okruh není komutativní, ale má jednotkový prvek (kterým je jednotková matice stupně n).

Definice

Jestliže $\mathscr{M} = (M; +, \cdot)$ je okruh a $\emptyset \neq A \subseteq M$, pak se A nazývá **uzavřená podmnožina**, je-li uzavřená vzhledem k oběma binárním operacím okruhu, tj. platí-li

$$\forall a, b \in A;\ a + b \in A,\ ab \in A.$$

Poznámka. Na uzavřené podmnožině A můžeme uvažovat restrikce „$+_A$“, „$\cdot_A$“ operací „$+$“ a „$\cdot$“ okruhu $\mathscr{M}$. Budeme je ovšem bez nebezpečí z nedorozumění označovat také symboly „$+$“ a „$\cdot$“.

Definice

Nechť $\mathscr{M} = (M; +, \cdot)$ je okruh a $\emptyset \neq A \subseteq M$ je uzavřená podmnožina. Pak $\mathscr{A} = (A; +, \cdot)$ nazveme **podokruh** okruhu $\mathscr{M}$ (označení: $\mathscr{A} \leq \mathscr{M}$), jestliže je $\mathscr{A}$ okruhem vzhledem k indukovaným operacím.

Poznámka. Zřejmě vždy platí, že $(\{o\}; +, \cdot) \leq (M; +, \cdot) = \mathscr{M}$ a $\mathscr{M} \leq \mathscr{M}$. Podokruh $(\{o\}; +, \cdot)$ budeme nazývat **nulovým** a oba podokruhy $(\{o\}; +, \cdot)$ a $\mathscr{M}$ nazveme **triviálními podokruhy** okruhu $\mathscr{M}$.

Věta

Jestliže $\mathscr{M} = (M; +, \cdot)$ je okruh a $A \subseteq M$, pak $\mathscr{A} = (A; +, \cdot) \leq \mathscr{M}$ právě tehdy, jsou-li splněny následující podmínky:

1. $\forall a, b \in A;\ a + b \in A$
2. $o \in A$
3. $\forall a \in A;\ -a \in A$
4. $\forall a, b \in A;\ ab \in A$.

Důkaz. Na přednášce.

Poznámka. Jestliže navíc předpokládáme, že $A \neq \emptyset$, pak platí $\mathscr{A} \leq \mathscr{M}$ právě tehdy, když jsou splněny podmínky 1, 3 a 4 z předchozí věty. Je-li totiž $a \in A$, pak $o = a + (-a) \in A$.

Poznámka. Analogicky jako v případě grup, můžeme okruh uvažovat jako algebraickou strukturu $\mathscr{M} = (M; +, o, -(.), \cdot)$ se dvěma binárními operacemi „$+$“ a „$\cdot$“, s jednou nulární operací „o“ a s jednou unární operací „$-(.)$“, pro které platí

- $\forall a, b, c \in M;\ a + (b + c) = (a + b) + c$
- $\forall a \in M;\ a + o = o + a = a$
- $\forall a \in M;\ a + (-a) = (-a) + a = o$
- $\forall a, b, c \in M;\ a(bc) = (ab)c$.

Pak $\mathscr{A} = (A; +, \cdot)$ je podokruhem okruhu $\mathscr{M} = (M; +, o, -(.), \cdot)$ právě tehdy, když A je uzavřená vzhledem ke všem čtyřem jeho operacím.

Věta

Nechť $\emptyset \neq A \subseteq M$ a $\mathscr{M} = (M; +, \cdot)$ je okruh. Pak $(A; +, \cdot) \leq \mathscr{M}$ právě tehdy, když

1. $\forall a, b \in A;\ a - b \in A$
2. $\forall a, b \in A;\ ab \in A$.

Důkaz. Na přednášce.

Definice

(a) Okruh $\mathscr{J} = (J; +, \cdot)$ se nazývá **obor integrity**, jestliže je komutativní, má jednotkový prvek $e \neq o$ a nemá **netriviální dělitele nuly**, tj.

$$\forall a, b \in J;\ ab = o,\ a \neq o \Rightarrow b = o.$$

(b) Každý alespoň dvouprvkový okruh $\mathscr{T} = (T; +, \cdot)$ takový, že $(T \setminus \{o\}; \cdot)$ je grupa, se nazývá **těleso**.

Poznámka. Podle definice tělesa je zřejmé, že je-li $\mathscr{T} = (T; +, \cdot)$ těleso, pak ke každému nenulovému prvku $a \in T$ existuje inverzní prvek $a^{-1} \in T$, který je také nenulový. Proto v rovnostech můžeme multiplikativně krátit nenulovými prvky zleva i zprava. Tedy, pro libovolné prvky $a, b, c \in T$ platí, že jestliže $ab = ac$, $a \neq o$, pak $b = c$, a také z $ba = ca$, $a \neq o$ plyne $b = c$. Odtud je také vidět, že každé komutativní těleso je oborem integrity.

Definice

Podokruh okruhu $\mathscr{M}$, který je vzhledem k indukovaným operacím oborem integrity (popř. tělesem), budeme nazývat **podoborem integrity** (popř. **podtělesem**) okruhu $\mathscr{M}$.

Poznámka. Podoobor integrity (popř. podtěleso) mohou být podokruhem okruhu $\mathscr{M}$, který není ani oborem integrity ani tělesem.

Příklad

Uvažujme okruh $\mathscr{Z}_n = (\mathbb{Z}_n; \oplus, \otimes)$, kde $n \in \mathbb{N}$ je složené číslo takové, že $n = ab$, $1 < a, b < n$, $a, b \in \mathbb{N}$. Pak v $\mathscr{Z}_n$ platí $a \otimes b = 0$, tzn., že obě čísla a, b jsou netriviálními děliteli nuly. V takovém případě tedy platí, že $\mathscr{Z}_n$ je komutativní okruh s jednotkovým prvkem 1, který není oborem integrity.

Příklad

Uvažujme okruh $\mathscr{Z}_n = (\mathbb{Z}_n; \oplus, \otimes)$, kde $n \in \mathbb{N}$ je prvočíslo, $k, a \in \mathbb{N}$, $0 < k, a < n$, $k \otimes a = 0$. Pak existuje $x \in \mathbb{N}$ tak, že $ka = nx$, tedy $n|ka$. Protože n je prvočíslo, platí $n|k$ nebo $n|a$, což je spor s volbou čísel k a a. Tedy $k \otimes a \neq 0$ pro každá $0 < k$, $a < n$, a proto „$\otimes$“ je binární operace na $\mathbb{Z}_n \backslash \{0\}$. Ukažme, že $(\mathbb{Z}_n \backslash \{0\}; \otimes)$ je grupa. Samozřejmě $1 \in \mathbb{Z}_n \backslash \{0\}$. Zbývá tedy dokázat, že ke každému prvku $a \in \mathbb{Z}_n \backslash \{0\}$ existuje v $\mathbb{Z}_n \backslash \{0\}$ inverzní prvek a^{-1}. Nechť $a, k, l \in \mathbb{N}$, $0 < a, k, l < n$, $k \geq l$, $k \otimes a = l \otimes a$. To ovšem znamená, že $ka \equiv la (mod\, n)$, proto $ka - la = nx$, kde $x \in \mathbb{Z}$. Tedy $(k-l)a = nx$, a protože n je prvočíslo, musí platit $n|(k-l)$. Ovšem pak podle volby čísel k a l dostáváme, že $k - l = 0$, odkud $k = l$. Proto jsou všechna čísla $1 \otimes a, 2 \otimes a, \ldots, (n-1) \otimes a$ navzájem různá, a vzhledem k tomu, že všechna patří do $\mathbb{Z}_n \backslash \{0\}$, platí, že $\mathbb{Z}_n \backslash \{0\} = \{1 \otimes a, 2 \otimes a, \ldots, (n-1) \otimes a\}$. Proto musí existovat $k \in \mathbb{Z}_n \backslash \{0\}$ takové, že $k \otimes a = 1$, tzn. $a^{-1} = k$. Platí tedy, že je-li $n \in \mathbb{N}$ prvočíslo, pak je $\mathscr{Z}_n$ komutativním tělesem (a tedy i oborem integrity).

Příklad

Označme A množinu všech zobrazení z $\mathbb{R}$ do $\mathbb{R}$ a definujme pro libovolná $f, g \in A$ zobrazení $f+g$ a $f \cdot g$ takto:

$$\forall x \in \mathbb{R};\ (f+g)(x) = f(x)+g(x),\ (f \cdot g)(x) = f(x) \cdot g(x).$$

Je zřejmé, že $f+g$ a $f \cdot g$ jsou opět zobrazeními z $\mathbb{R}$ do $\mathbb{R}$ a že $\mathscr{A} = (A; +, \cdot)$ je okruhem. Tento okruh je navíc komutativní a má jednotkový prvek, kterým je konstantní zobrazení 1 takové, že $1 : x \mapsto 1$ pro každé $x \in \mathbb{R}$. Okruh $\mathscr{A}$ ale není oborem integrity. Např. pro $f, g \in A$ takové, že

$$\forall x < 0;\ f(x) = -x,\ g(x) = 0, \quad \forall x \geq 0;\ f(x) = 0,\ g(x) = x,$$

platí $f \cdot g = 0$, ale $f \neq 0$ a $g \neq 0$. (Zde 0 označuje konstantní zobrazení, v němž jsou obrazy všech reálných čísel rovny číslu 0.)
Dále, množina B všech konstantních zobrazení z $\mathbb{R}$ do $\mathbb{R}$ je podokruhem okruhu $\mathscr{A}$, který je izomorfní s tělesem $\mathscr{R}$, a proto $(B; +, \cdot)$ je podtělesem okruhu $\mathscr{A}$.

Příklad

Nechť $\mathscr{T}$ je libovolné číselné těleso a $T[x]$ je množina všech polynomů jedné proměnné nad $\mathscr{T}$. Pak $T[x]$ je spolu s operacemi sčítání a násobení polynomů oborem integrity $\mathscr{T}[x]$, který není tělesem, a přitom množina všech konstantních polynomů (tj. polynomů stupně 0 a s nulovým polynomem) spolu s operacemi sčítání a násobení polynomů je podtělesem v $\mathscr{T}[x]$.

Obsah

V teorii grup jsme mezi všemi podgrupami dané grupy vyčlenili normální podgrupy, jejichž význam se ukázal např. při konstrukci faktorových grup a ve větě o homomorfismu grup. Analogickým pojmem k normální podgrupě je v teorii okruhů pojem (oboustranného) ideálu okruhu.

Definice

Neprázdná podmnožina I okruhu $\mathscr{M} = (M; +, \cdot)$ se nazývá **ideál** okruhu $\mathscr{M}$ (označení: $I \trianglelefteq \mathscr{M}$), platí-li

1. $\forall a, b \in I;\ a - b \in I$
2. $\forall a \in I,\ r \in M;\ ra \in I,\ ar \in I$.

Příklad

Ideálem oboru integrity $\mathscr{Z} = (\mathbb{Z}; +, \cdot)$ je například množina všech sudých celých čísel $2\mathbb{Z}$.

Poznámka. Někdy se používají i pojmy jednostranných (tj. levých a pravých) ideálů. Neprázdná množina I se pak nazývá **levý** (popř. **pravý**) **ideál** v $\mathscr{M}$, platí-li podmínka 1 z definice ideálu a platí-li pro každé $a \in I$ a $r \in M$, že $ra \in I$ (popř., že $ar \in I$). V takovém případě se pak ideál podle původní definice nazývá **oboustranný ideál**.

Poznámka. Je-li I ideál okruhu $\mathscr{M} = (M; +, \cdot)$, pak zřejmě $(I; +, \cdot)$ je podokruhem okruhu $\mathscr{M}$. Přitom ale podokruh nemusí být ideálem v $\mathscr{M}$.

Příklad

Uvažujme znovu okruh $\mathscr{A} = (A; +, \cdot)$ všech zobrazení z $\mathbb{R}$ do $\mathbb{R}$ spolu s operacemi sčítání a násobení reálných funkcí jedné reálné proměnné. Snadno vidíme, že množina C všech omezených funkcí z A spolu s operacemi sčítání a násobení reálných funkcí jedné reálné proměnné je podokruhem v $\mathscr{A}$, který není ideálem v $\mathscr{A}$.

Definice

Jestliže $\mathscr{M} = (M; +, \cdot)$ je okruh a $A, B \subseteq M$, pak **součtem podmnožin** A a B budeme rozumět množinu $A + B \subseteq M$ takovou, že

$$A + B = \{a + b; a \in A, b \in B\}.$$

Jestliže $A = \{a\}$, pak místo $\{a\} + B$ píšeme $a + B$. Podobně můžeme definovat **rozdíl** a **součin podmnožin** A a B okruhu $\mathscr{M}$:

$$A - B = \{a - b; a \in A, b \in B\},$$

$$AB = \{ab; a \in A, b \in B\}.$$

Poznámka. V případě podmnožin okruhu nezaměňujme jejich rozdíl $A - B$ ve smyslu teorie okruhů s množinovým rozdílem.

Poznámka. Definice podokruhu $\mathscr{A}$ a ideálu I okruhu $\mathscr{M} = (M; +, \cdot)$ můžeme přeformulovat. Nechť $A \neq \emptyset \neq I$. Pak $\mathscr{A} = (A; +, \cdot) \leq \mathscr{M}$ právě tehdy, když $A - A \subseteq A$, $AA \subseteq A$ a $I \trianglelefteq \mathscr{M}$ právě tehdy, když $I - I \subseteq I$, $MI \subseteq I$, $IM \subseteq I$.

Definice

Nechť $\mathscr{M} = (M; +, \cdot)$ je okruh, $\mathscr{A} = (A; +, \cdot) \leq \mathscr{M}$, $x \in M$. Pak **třídou prvku x vzhledem k podokruhu** $\mathscr{A}$ rozumíme množinu $x + A$, tj. (levou) třídu prvku x v aditivní grupě $(M; +)$ vzhledem k její podgrupě $(A; +)$.

Poznámka. Vzhledem k tomu, že $(M; +)$ je abelovská grupa, je každá její podgrupa normální (a tedy také levé a pravé třídy prvků splývají). Proto faktorová množina M/A je (abelovskou) grupou vzhledem k operaci „$+$“, kde

$$\forall x, y \in M; (x + A) + (y + A) = (x + y) + A.$$

Nulovým prvkem v $(M/A; +)$ je podokruh A, opačným prvkem ke třídě $x + A$ je třída $(-x) + A$.

Věta

Nechť I je ideál okruhu $\mathscr{M}$. Jestliže pro libovolné prvky $x, y \in M$ položíme $(x + I) \cdot (y + I) = xy + I$, pak je „$\cdot$“ binární operace na M/I.

Důkaz. Na přednášce.

Věta

Jestliže I je ideál okruhu $\mathscr{M}$, pak $\mathscr{M}/I = (M/I; +, \cdot)$ je okruh.

Důkaz. Na přednášce.

Definice

Okruh $\mathscr{M}/I$ se nazývá **faktorový okruh** okruhu $\mathscr{M}$ podle ideálu I.

Definice

(a) Nechť $\mathscr{M}_1 = (M_1; +_1, \cdot_1)$ a $\mathscr{M}_2 = (M_2; +_2, \cdot_2)$ jsou okruhy a nechť f je zobrazení z množiny M_1 do množiny M_2. Pak se f nazývá **homomorfismus okruhu $\mathscr{M}_1$ do okruhu $\mathscr{M}_2$**, platí-li

$$\forall a, b \in M_1;\ f(a +_1 b) = f(a) +_2 f(b),\ f(a \cdot_1 b) = f(a) \cdot_2 f(b),$$

tedy f je současně homomorfismem grupy $(M_1; +_1)$ do grupy $(M_2; +_2)$ a homomorfismem pologrupy $(M_1; \cdot_1)$ do pologrupy $(M_2; \cdot_2)$.

(b) Řekneme, že okruh $\mathscr{M}_2$ je **homomorfním obrazem** okruhu $\mathscr{M}_1$, existuje-li alespoň jeden surjektivní homomorfismus $\mathscr{M}_1$ na $\mathscr{M}_2$.

(c) Bijektivní homomorfismus okruhu $\mathscr{M}_1$ na $\mathscr{M}_2$ se nazývá **izomorfismus**.

(d) Okruhy $\mathscr{M}_1$ a $\mathscr{M}_2$ se nazývají **izomorfní**, existuje-li alespoň jeden izomorfismus jednoho z těchto okruhů na druhý.

Poznámka. Podobně jako v případě grup platí, že identické zobrazení je izomorfismem okruhu $\mathscr{M}_1$ na okruh $\mathscr{M}_2$, že složení dvou izomorfismů okruhů je opět izomorfismem okruhů, a že je-li f izomorfismus okruhu $\mathscr{M}_1$ na okruh $\mathscr{M}_2$, pak inverzní zobrazení f^{-1} je izomorfismem okruhu $\mathscr{M}_2$ na okruh $\mathscr{M}_1$. Proto relace „být izomorfní s“ je ekvivalencí na třídě všech okruhů, a proto rozkládá tuto třídu na třídy navzájem izomorfních okruhů, které mají stejné algebraické vlastnosti. To znamená, že i zde můžeme používat formulaci, že „danou vlastnost mají, až na izomorfimus, právě jisté okruhy“.

Definice

Jestliže f je homomorfismus okruhu $\mathscr{M}_1$ do okruhu $\mathscr{M}_2$, pak **jádrem** f budeme rozumět množinu $\mathrm{Ker} f \subseteq M_1$ takovou, že $\mathrm{Ker} f = \{x \in M_1 ; f(x) = o_2\}$, kde o_2 je nulový prvek okruhu $\mathscr{M}_2$.

Věta

Jestliže f je homomorfismus okruhu $\mathscr{M}_1$ do okruhu $\mathscr{M}_2$, pak $\mathrm{Ker} f \trianglelefteq \mathscr{M}_1$.

Důkaz. Na přednášce.

Věta

Jestliže $\mathscr{M} = (M; +, \cdot)$ je okruh a $I \trianglelefteq \mathscr{M}$, pak zobrazení $\nu : M \to M/I$ takové, že $\nu : x \mapsto x + I$ pro každý $x \in M$, je homomorfismem $\mathscr{M}$ na faktorový okruh $\mathscr{M}/I$, přičemž $\mathrm{Ker}\nu = I$.

Důkaz. Na přednášce.

Definice

Zobrazení ν z předchozí věty se nazývá **přirozený homomorfismus** okruhu $\mathscr{M}$ na faktorový okruh $\mathscr{M}/I$.

Věta o homomorfismu okruhů

Nechť f je surjektivní homomorfismus okruhu $\mathscr{M} = (M; +, \cdot)$ na okruh $\mathscr{M}' = (M'; +, \cdot)$. Pak je okruh $\mathscr{M}'$ izomorfní s faktorovým okruhem $\mathscr{M}/\mathrm{Ker}f$ a přitom existuje právě jeden izomorfismus g okruhu $\mathscr{M}$ na okruh $\mathscr{M}/\mathrm{Ker}f$ takový, že $f \circ g = \nu$, kde ν je přirozený homomorfismus $\mathscr{M}$ na $\mathscr{M}/\mathrm{Ker}f$.

Důkaz. Na přednášce.

Poznámka. Platí, že jádry homomorfismů okruhu $\mathscr{M}$ do dalších okruhů jsou právě všechny ideály okruhu $\mathscr{M}$. Přitom je faktorový okruh okruhu $\mathscr{M}$ podle jeho libovolného ideálu I homomorfním obrazem okruhu $\mathscr{M}$ a jedním z homomorfismů $\mathscr{M}$ na $\mathscr{M}/I$ je odpovídající přirozený homomorfismus. Předcházející věta říká, že (až na izomorfismus) neexistují jiné homomorfní obrazy okruhu $\mathscr{M}$ než jeho faktorové okruhy a že každý homomorfismus okruhu $\mathscr{M}$ na některý jeho homomorfní obraz pak může být nahrazen přirozeným homomorfismem.

Poznámka. Máme-li za úkol určit všechny homomorfní obrazy daného okruhu $\mathscr{M}$, pak jej můžeme vyřešit tak, že najdeme všechny ideály okruhu $\mathscr{M}$ a pak sestrojíme faktorové okruhy okruhu $\mathscr{M}$ podle těchto ideálů. Tím je daný úkol, až na izomorfismus, zcela vyřešen. Tzn., že homomorfními obrazy okruhu $\mathscr{M}$ jsou právě všechny jeho faktorové okruhy a okruhy s nimi izomorfní.

Poznámka. Připomeňme si, že pro algebraické struktury s jednou binární operací platí například, že homomorfní obraz pologrupy je opět pologrupou, homomorfní obraz grupy je také grupou, atd. U algebraických struktur se dvěma binárními operacemi, kterým se věnujeme, je ale situace složitější. Například homomorfní obraz oboru integrity nemusí být oborem integrity. K tomu stačí uvažovat okruhy $\mathscr{Z}$ a $\mathscr{Z}_4$ a zobrazeni $f : \mathbb{Z} \to \mathbb{Z}_4$ takové, že je-li $a \in \mathbb{Z}$, pak $f : a \mapsto r_a$, kde r_a je nejmenší nezáporný zbytek při dělení čísla a číslem 4. Platí, že f je homomorfismus $\mathscr{Z}$ na $\mathscr{Z}_4$ a přitom $\mathscr{Z}$ je obor integrity, zatímco $\mathscr{Z}_4$ má netriviální dělitele nuly.

Poznámka. Na druhé straně ale homomorfní obraz oboru integrity, který není tělesem, může být tělesem. Například stačí uvažovat obor integrity $\mathscr{Z}$ a těleso $\mathscr{Z}_5$ a použít pro ně analogický homomorfismus $\mathscr{Z}$ na $\mathscr{Z}_5$ jako v předchozím případě.

Poznámka. Nechť $\mathscr{M} = (M; +, \cdot)$ je libovolný okruh a nechť I a J jsou jeho ideály. Pak $(I \cap J; +)$ a $(I + J; +)$ jsou podle vět o (normálních) podgrupách grup podgrupami aditivní grupy $(M; +)$. Dále pro libovolný prvek $a \in I \cap J$ a libovolný prvek $x \in M$ platí, že $ax \in I \cap J$ a $xa \in I \cap J$. Konečně pro libovolný $b \in I + J$, kde $b = b_1 + b_2$, $b_1 \in I$, $b_2 \in J$, a libovolný $y \in M$ platí $by = (b_1 + b_2)y = b_1 y + b_2 y \in I + J$ a také analogicky $yb \in I + J$. Tedy $I \cap J$ a $I + J$ jsou ideály okruhu $\mathscr{M}$.

Příklad

Uvažujme okruh $\mathscr{Z}$. Snadno se můžeme přesvědčit, že ideály tohoto okruhu jsou právě všechny množiny $n\mathbb{Z}$, kde $0 \leq n \in \mathbb{Z}$. Proto libovolný okruh, který je homomorfním obrazem okruhu $\mathscr{Z}$, je izomorfní s některým faktorovým okruhem $\mathscr{Z}/n\mathbb{Z}$ okruhu $\mathscr{Z}$ podle některého ideálu $n\mathbb{Z}$.
Pak je například okruh $\mathscr{Z}_3$ izomorfní s faktorovým okruhem $\mathscr{Z}/3\mathbb{Z}$, který má následující tabulky operací:

$\oplus$	$3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$3\mathbb{Z}$	$3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$1+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$	$3\mathbb{Z}$
$2+3\mathbb{Z}$	$2+3\mathbb{Z}$	$3\mathbb{Z}$	$1+3\mathbb{Z}$

$\otimes$	$3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$3\mathbb{Z}$	$3\mathbb{Z}$	$3\mathbb{Z}$	$3\mathbb{Z}$
$1+3\mathbb{Z}$	$3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$2+3\mathbb{Z}$	$3\mathbb{Z}$	$2+3\mathbb{Z}$	$1+3\mathbb{Z}$

Podle věty o homomorfismu okruhů je každý homomorfní obraz daného okruhu izomorfní s faktorovým okruhem toho okruhu podle některého z jeho ideálů. Ukažme si proto některé vztahy mezi vlastnostmi ideálů a odpovídajících faktorových okruhů, a to pro případ komutativních okruhů s jednotkovými prvky.

Definice

Nechť $\mathscr{M} = (M; +, \cdot)$ je okruh a nechť $I \trianglelefteq M$, $I \neq M$. Pak se I nazývá

(a) **maximální ideál** v $\mathscr{M}$, jestliže pro každý $J \trianglelefteq \mathscr{M}$ takový, že $I \subseteq J \subseteq M$, platí $J = I$ nebo $J = M$.

(b) **prvoideál** v $\mathscr{M}$, jestliže $\forall a, b \in M$; $ab \in I \Rightarrow a \in I$ nebo $b \in I$.

Věta

Nechť $\mathscr{M} = (M; +, \cdot)$ je netriviální okruh s jednotkovým prvkem e a nechť $I \trianglelefteq \mathscr{M}$, $I \neq M$. Pak

(a) $\mathscr{M}/I$ je obor integrity právě tehdy, když I je prvoideál.

(b) $\mathscr{M}/I$ je komutativní těleso právě tehdy, když I je maximální ideál.

Důkaz. Na přednášce.

Důsledek

Jestliže $\mathscr{M}$ je komutativní okruh s jednotkovým prvkem, pak každý maximální ideál v $\mathscr{M}$ je prvoideálem v $\mathscr{M}$.

Důkaz. Na přednášce.

Poznámka. Obrácená implikace obecně neplatí.

Obsah

V další části se budeme věnovat pojmu charakteristika okruhu, k jejímuž zavedení budeme pracovat s řády prvků okruhu vzhledem k jeho aditivní grupě. Znamená to tedy, že je-li $\mathscr{M} = (M; +, \cdot)$ okruh, pak budou pro nás podstatné řády prvků z M v grupě $(M; +)$. Protože se jedná o aditivní symboliku, budeme používat celé násobky prvků. Připomeňme si, že jestliže $a \in M$, $n \in N$, pak

$$1 \times a = a, (n+1) \times a = (n \times a) + a,$$

$$0 \times a = o, (-n) \times a = -(n \times a) = n \times (-a).$$

Definice

Nechť $\mathscr{M} = (M; +, \cdot)$ je okruh. Pak řád prvku $a \in M$ je definován takto:

(a) Jestliže pro každé $n \in \mathbb{N}$ platí $n \times a \neq o$, pak a má **nekonečný řád**.

(b) Jestliže existují přirozená čísla n_i taková, že $n_i \times a = o$, pak **řádem prvku** a je nejmenší z těchto čísel n_i.

Věta

Jestliže okruh $\mathscr{M} = (M; +, \cdot)$ nemá netriviální dělitele nuly, pak všechny nenulové prvky z M mají stejný řád.

Důkaz. Na přednášce.

Poznámka. Jestliže okruh $\mathscr{M} = (M; +, \cdot)$ má netriviální dělitele nuly, pak jeho různé nenulové prvky mohou mít různé řády.

Příklad

(a) V okruhu $\mathscr{Z}_5 = (\mathbb{Z}_5; \oplus, \otimes)$ mají nenulové prvky řád 5.

(b) V okruhu $\mathscr{Z}_6 = (\mathbb{Z}_6; \oplus, \otimes)$ mají čísla 1 a 5 řád 6, čísla 2 a 4 mají řád 3 a číslo 3 má řád 2.

Definice

Okruh $\mathscr{M} = (M; +, \cdot)$ **má charakteristiku k**, jestliže k je nejmenší přirozené číslo takové, že $k \times a = o$ pro všechny prvky $a \in M$. Jestliže takové přirozené číslo k neexistuje, pak říkáme, že $\mathscr{M}$ je **nekonečné charakteristiky** (nebo že **má charakteristiku 0**).

Věta

Má-li okruh $\mathscr{M} = (M; +, \cdot)$ jednotkový prvek e, pak je charakteristika okruhu $\mathscr{M}$ rovna řádu prvku e.

Důkaz. Na přednášce.

Poznámka. Právě dokázaná věta velice podstatně zjednodušuje určování charakteristiky okruhu $\mathscr{M} = (M; +, \cdot)$, pokud má $\mathscr{M}$ jednotkový prvek. Podle původní definice totiž musíme hledat (pokud existuje) nejmenší přirozené číslo k splňující $k \times a = o$ pro každý prvek $a \in M$, tzn., že nalezení konečného řádu některého z nenulových prvků dává jen částečnou informaci o charakteristice okruhu. Pro okruh $\mathscr{M}$ s jednotkovým prvkem e však stačí k určení charakteristiky okruhu $\mathscr{M}$ nalézt řád jediného prvku, a to prvku e. Podobně pro charakteristiku okruhu bez netriviálních dělitelů nuly stačí určit řád kteréhokoliv z nenulových prvků toho okruhu.

Poznámka. Podle předchozí věty můžeme snadno ověřit, že každé přirozené číslo n je charakteristikou některého okruhu. Stačí k tomu uvažovat okruh $\mathscr{Z}_n = (\mathbb{Z}_n; \oplus, \otimes)$. Protože $\mathscr{Z}_n$ má jednotkový prvek 1, je jeho charakteristika rovna řádu čísla 1, tj. je rovna n.
Pro charakteristiky oborů integrity a těles však platí podstatná omezení, jak je popsáno v následující větě.

Věta

Nechť $\mathscr{M} = (M; +, \cdot)$ je nenulový okruh bez netriviálních dětitelů nuly. Pak $\mathscr{M}$ je buď nekonečné charakteristiky nebo jeho charakteristikou je prvočíslo.
Tedy každý obor integrity a každé těleso má buď nekonečnou nebo prvočíselnou charakteristiku.

Důkaz. Na přednášce.

Věta

Nechť $\mathscr{M} = (M; +, \cdot)$ je okruh a A_α ($\alpha \in I$) jsou podokruhy okruhu $\mathscr{M}$. Pak $A = \bigcap_{\alpha \in I} A_\alpha$ je také podokruhem okruhu $\mathscr{M}$.

Důkaz. Na přednášce.

Definice

Jestliže $\mathscr{M} = (M; +, \cdot)$ je okruh a $B \subseteq M$, pak průnik všech podokruhů okruhu $\mathscr{M}$, které obsahují B, se nazývá **podokruh v $\mathscr{M}$ generovaný množinou B**. Označíme jej $\langle B \rangle$.

Poznámka. $\langle B \rangle$ je tedy nejmenší podokruh okruhu $\mathscr{M}$ obsahující B, tzn., že je obsažen v každém podokruhu okruhu $\mathscr{M}$, který obsahuje B.
Jestliže $B = \{b\}$, pak místo $\langle \{b\} \rangle$ budeme stručněji psát $\langle b \rangle$.

Věta

Nechť $\mathscr{M} = (M; +, \cdot)$ je okruh bez dělitelů nuly, který má jednotkový prvek e.

(a) Jestliže má $\mathscr{M}$ nekonečnou charakteristiku, pak obsahuje podokruh izomorfní s oborem integrity $\mathscr{Z}$.

(b) Jestliže má $\mathscr{M}$ konečnou (tj. prvočíselnou) charakteristiku p, pak obsahuje podokruh izomorfní s tělesem $\mathscr{Z}_p$.

Důkaz. Na přednášce.

Definice

Jestliže má okruh $\mathscr{M} = (M; +, \cdot)$ jednotkový prvek e, pak podokruh $\langle e \rangle$ se nazývá **prvookruh** okruhu $\mathscr{M}$.

Poznámka. Podle předchozí věty mj. platí, že je-li $\mathscr{M}$ obor integrity, pak jeho prvookruh je izomorfní buď s oborem integrity $\mathscr{Z}$ (pokud je $\mathscr{M}$ nekonečné charakteristiky) nebo s tělesem $\mathscr{Z}_p$, kde p je prvočíslo (pokud má $\mathscr{M}$ konečnou charakteristiku p).

Věta

Jestliže je $\mathscr{T}$ těleso, a jestliže A_α ($\alpha \in I$) jsou podtělesa tělesa $\mathscr{T}$, pak $A = \bigcap_{\alpha \in I} A_\alpha$ je také podtěleso tělesa $\mathscr{T}$.

Důkaz. Na přednášce.

Protože každá podmnožina tělesa $\mathscr{T}$ je obsažena alespoň v jednom podtělese tělesa $\mathscr{T}$, můžeme pro tělesa zavést pojem analogický s pojmem prvookruhu okruhu.

Definice

Jestliže $\mathscr{T} = (T; +, \cdot)$ je těleso a $B \subseteq T$, pak průnik všech podtěles tělesa $\mathscr{T}$ obsahujících podmnožinu B se nazývá, **podtěleso tělesa** $\mathscr{T}$ **generované** B. Značíme jej $\overline{\langle B \rangle}$. Jestliže $b \in T$, pak místo $\overline{\langle \{b\} \rangle}$ píšeme $\overline{\langle b \rangle}$.

Věta

Nechť $\mathscr{T} = (T; +, \cdot)$ je komutativní těleso.

(a) Má-li $\mathscr{T}$ konečnou charakteristiku p, pak $\mathscr{T}$ obsahuje podtěleso izomorfní s tělesem $\mathscr{Z}_p$.

(b) Má-li $\mathscr{T}$ nekonečnou charakteristiku p, pak $\mathscr{T}$ obsahuje podtěleso izomorfní s tělesem $\mathscr{Q}$.

Důkaz. Na přednášce.

Definice

Podtěleso $\overline{\langle e \rangle}$ tělesa $\mathscr{T}$ se nazývá **prvotěleso** tělesa $\mathscr{T}$.

Poznámka. Na základě předchozí věty tedy platí, že je-li $\mathscr{T}$ komutativní těleso, pak prvotěleso tělesa $\mathscr{T}$ je izomorfní buď s tělesem racionálních čísel $\mathscr{Q}$ (pokud má $\mathscr{T}$ nekonečnou charakteristiku) nebo s tělesem $\mathscr{Z}_p$, kde p je prvočíslo (pokud má $\mathscr{T}$ konečnou charakteristiku p).

Dosud jsme pracovali s komutativními tělesy nekonečné charakteristiky (např. s číselnými tělesy) nebo v případě těles konečné charakteristiky s tělesy $\mathscr{Z}_p$, kde p je prvočíslo. Dále ukážeme dvě obecné vlastnosti libovolných konečných těles.

Věta

Má-li konečné komutativní těleso $\mathscr{T}$ charakteristiku p, pak počet prvků, v $\mathscr{T}$ je roven některé mocnině čísla p.

Důkaz. Na přednášce.

Poznámka. Z teorie grup víme, že pro každé přirozené číslo n existuje alespoň jedna grupa řádu n. Podobně každé $n \in \mathbb{N}$ je počtem prvků některého okruhu. Ovšem podle předchozí věty obdobná situace nenastane pro komutativní tělesa, protože počet prvků libovolného konečného komutativního tělesa je roven mocnině některého prvočísla, takže např. neexistuje žádné komutativní těleso, které by mělo právě šest prvků. (Ve skutečnosti nemůže existovat vůbec žádné těleso, jehož počet prvků by nebyl mocninou některého prvočísla, protože se dá dokázat, že každé konečné těleso je komutativní.)

Věta

Má-li konečné komutativní těleso $\mathscr{T} = (T; +, \cdot)$ q prvků, pak pro každý prvek $a \in T$ platí $a^q = a$.

Důkaz. Na přednášce.

Obsah

Dále se budeme věnovat vztahům mezi obory integrity a tělesy. V oboru integrity, na rozdíl od tělesa, nemusí ke každému nenulovému prvku existovat jeho inverzní prvek, tedy zde obecně neexistují operace dělení. Na druhé straně ale mají obory integrity a tělesa hodně společných vlastností: například v nich neexistují netriviální dělitelé nuly (a je tedy možno v nich krátit při násobení nenulovými prvky), jejich charakteristika je buď nekonečná nebo prvočíselná, atd. Ukážeme, že každý obor integrity $\mathscr{J}$ můžeme přirozeným způsobem rozšířit na komutativní těleso $\overline{\mathscr{J}}$, které má pro $\mathscr{J}$ analogický význam, jako má těleso $\mathscr{Q}$ pro obor integrity $\mathscr{Z}$.

Definice

Nechť $\mathscr{J} = (J; +, \cdot)$ je obor integrity. **Zlomkem nad** $\mathscr{J}$ rozumíme každou uspořádanou dvojici $\langle a, b \rangle$, kde $a, b \in J$, $b \neq o$. Na množině $\mathscr{J}^* = J \times (J \setminus \{o\})$ všech zlomků nad $\mathscr{J}$ zavedeme binární relaci $\equiv$ takto:

$$\forall a, a_1, b, b_1 \in J, b \neq o \neq b_1 ; \langle a, b \rangle = \langle a_1, b_1 \rangle \Leftrightarrow ab_1 = a_1 b.$$

Věta

Relace $\equiv$ je relací ekvivalence na množině J^*.

Důkaz. Na přednášce.

Nechť $\langle a,b\rangle, \langle c,d\rangle \in J^*$. Definujme $\langle a,b\rangle + \langle c,d\rangle = \langle ad+bc, bd\rangle$, $\langle a,b\rangle \cdot \langle c,d\rangle = \langle ac, bd\rangle$. Protože $\mathscr{J}$ je obor integrity a protože $b \neq o \neq d$, platí $bd \neq o$ a tedy „$+$“ a „$\cdot$“ jsou binární operace na J^*.
Označme $\overline{J} = J^*/\equiv$. Jestliže $\langle a,b\rangle \in J^*$, pak označíme $[\langle a,b\rangle]$ třídu rozkladu (tj. prvek faktorové množiny $\overline{J}$), indukovanou ekvivalencí „$\equiv$“, v níž leží prvek $\langle a,b\rangle$. Na $\overline{J}$ nyní zavedeme dvě binární operace, které budeme také značit „$+$“ a „$\cdot$“. Jestliže $[\langle a,b\rangle], [\langle c,d\rangle] \in \overline{J}$, pak položíme

$$[\langle a,b\rangle] + [\langle c,d\rangle] = [\langle a,b\rangle + \langle c,d\rangle],$$

$$[\langle a,b\rangle] \cdot [\langle c,d\rangle] = [\langle a,b\rangle \cdot \langle c,d\rangle].$$

Věta

Jestliže $\mathscr{J} = (J; +, \cdot)$ je obor integrity, pak operace „$+$“ a „$\cdot$“ jsou na J definovány korektně a platí, že $\overline{\mathscr{J}} = (\overline{J}; +, \cdot)$ je komutativní těleso, které obsahuje podobor integrity, izomorfní s oborem integriy $\mathscr{J}$.

Důkaz. Na přednášce.

Definice

Těleso $\overline{\mathscr{J}}$ se nazývá **podílové těleso** oboru integrity $\mathscr{J}$.

Definice

Nechť $\mathscr{M}$ a $\mathscr{M}'$ jsou okruhy. Řekneme, že $\mathscr{M}$ lze **izomorfně vnořit** do $\mathscr{M}'$ existuje-li injektivní homomorfismus okruhu $\mathscr{M}$ do $\mathscr{M}'$. Takový homomorfismus nazýváme **vnoření** $\mathscr{M}$ do $\mathscr{M}'$.

Důsledek

Každý obor integrity lze vnořit do jeho podílového tělesa.

Ukážeme nyní možnost jednoduchého vyjádření prvků z podílového tělesa pomocí prvků z $\mathscr{J}$ (které také odůvodňuje volbu názvu pro toto těleso).

Věta

Nechť $\mathscr{J}$ je obor integrity. Pak platí:

(a) Každý prvek podílového tělesa $\overline{\mathscr{J}}$ lze vyjádřit jako podíl dvou prvků z J.

(b) Jestliže ψ je vnoření oboru integrity J do libovolného komutativního tělesa $\mathscr{T}$, pak lze ψ rozšířit na vnoření $\overline{\psi}$ tělesa $\overline{\mathscr{J}}$ do tělesa $\mathscr{T}$.

Důkaz. Na přednášce.

Poznámka. Podle části b) předchozí věty tedy platí, že podílové těleso je nejmenší ze všech komutativních těles, která obsahují podobory integrity izomorfní s $\mathscr{J}$, neboli do nichž lze $\mathscr{J}$ izomorfně vnořit.

Obsah

Obsah

Budeme se zabývat otázkami souvisejícími s relací dělitelnosti v libovolném oboru integrity, zejména otázkami existence či neexistence největších společných dělitelů daných prvků a možnostmi určování těchto největších společných dělitelů standardními metodami (např. algoritmy).

Definice

Nechť $\mathscr{J} = (J; +, \cdot)$ je obor integrity a $a, b \in J$. Řekneme, že **prvek a dělí prvek b** (značíme $a \mid b$), existuje-li prvek $c \in J$ takový, že $b = ac$. V opačném případě budeme říkat, že **a nedělí b** (označení $a \nmid b$).

Definice

Nechť $\mathscr{J} = (J; +, \cdot)$ je obor integrity a $a, b \in J$. Nechť platí současně $a \mid b$ a $b \mid a$, pak říkáme, že prvky a a b jsou **asociované** (značíme $a \parallel b$). V opačném případě použijeme označení $a \nparallel b$.

Úmluva

Dále bude $\mathscr{J}$ označovat obor integrity $(J; +, \cdot)$, přičemž jeho jednotkový prvek budeme označovat e.

Definice

(a) Prvek $a \in J$ se nazývá **jednotka** oboru integrity $\mathscr{J}$, platí-li $a \parallel e$.

(b) Prvek $a \in J$, který není jednotkou v $\mathscr{J}$, se nazývá **vlastním dělitelem** prvku b, když $a \mid b$ a $a \nparallel b$. **Nevlastními děliteli** prvku b rozumíme všechny jednotky v $\mathscr{J}$ a všechny prvky asociované s b.

Věta

Nechť $a, b, c, x, y \in J$. Pak platí:

(a) $a \mid a$, $e \mid a$, $a \mid o$

(b) $(a \mid b, b \mid c) \Rightarrow a \mid c$

(c) $(a \mid b, a \mid c) \Rightarrow a \mid (bx + cy)$

(d) $a \mid b \Rightarrow ac \mid bc$

(e) $o \mid a \Leftrightarrow a = o$

(f) a je jednotka v $\mathscr{J}$ právě tehdy, když k prvku a existuje inverzní prvek v $(J; \cdot)$

(g) $a \parallel b$ právě tehdy, když existuje jednotka $j \in J$ taková, že $b = aj$

Důkaz. Na přednášce.

Poznámka. Binární relace „být asociován s“ je relací ekvivalence na J. Symetričnost je obsažena přímo v definici asociovaných prvků a reflexivnost s tranzitivností vyplývají z částí (a) a (b) předchozí věty. Proto tato relace indukuje rozklad množiny J na třídy navzájem asociovaných prvků.

Příklad

V oboru integrity $\mathscr{Z}$ jsou jednotkami právě čísla 1 a -1. Jestliže $x \in \mathbb{Z}$, pak s ním asociované prvky jsou právě x a $-x$.

Příklad

Nechť $\mathscr{T}$ je komutativní těleso. Víme, že jestliže $a \in T$, pak v $\mathscr{T}$ existuje inverzní prvek a^{-1} k prvku a, právě tehdy, když $a \neq o$. Proto jsou jednotkami v $\mathscr{T}$ právě všechny jeho nenulové prvky. Nechť $a, b \in T$, $a \neq o \neq b$. Pak $a = (ab^{-1})b$, a tedy $b \mid a$. Podobně dokážeme, že $a \mid b$, a proto $a \parallel b$. To ovšem znamená, že otázky dělitelnosti v komutativních tělesech jsou triviální a že má proto smysl se dělitelností zabývat jen v takových oborech integrity, které nejsou tělesy.

Příklad

Nechť $\mathscr{T}$ je číselné těleso a $\mathscr{T}[x]$ je obor integrity polynomů jedné proměnné nad $\mathscr{T}$. Pak jednotkami v $\mathscr{T}[x]$ jsou právě všechny polynomy stupně 0, tj. všechny nenulové konstantní polynomy. Je-li proto $f(x) \in \mathscr{T}[x]$, pak $g(x) \in \mathscr{T}[x]$ je asociovaný s $f(x)$ právě tehdy, když $g(x) = a \cdot f(x)$, kde $0 \neq a \in T$.

Příklad

Nechť $\mathbb{Z}[i] = \{a + bi;\, a, b \in \mathbb{Z}\}$. Pak $\mathscr{Z}[i] = (\mathbb{Z}[i]; +, \cdot)$ je číselný obor integrity, který se nazývá **obor integrity Gaussových celých čísel**. Jednotkami v $\mathscr{Z}[i]$ jsou právě čísla 1, -1, i, $-i$.

Definice

(a) Nechť $a_1, a_2, \ldots, a_n \in J$. Prvek $c \in J$ se nazývá **společný dělitel** prvků $a_1, a_2, \ldots, a_n$, platí-li $c \mid a_i$ pro každé $i = 1, 2, \ldots, n$.

(b) Prvek $d \in J$ se nazývá **největší společný dělitel** prvků $a_1, a_2, \ldots, a_n$, jestliže je jejich společným dělitelem a jestliže pro každý společný dělitel c těchto prvků platí $c \mid d$. Největší společný dělitel prvků $a_1, a_2, \ldots, a_n$ budeme označovat $D(a_1, a_2, \ldots, a_n)$.

(c) Prvky $a_1, a_2, \ldots, a_n$ nazýváme **nesoudělné**, platí-li $D(a_1, a_2, \ldots, a_n) = e$.

Poznámka. Nechť prvky $a_1, a_2, \ldots, a_n$ mají aspoň jeden největší společný dělitel a nechť prvky d a d_1 jsou největšími společnými děliteli těchto prvků. Pak $d \mid d_1$ a $d_1 \mid d$, tedy $d \parallel d_1$. Obráceně, nechť $D(a_1, a_2, \ldots, a_n) = d$ a nechť $d_1 \parallel d$. Jelikož $d_1 \mid d$ a $d \mid a_i$ pro každé $i = 1, 2, \ldots, n$, je d_1 společným dělitelem prvků $a_1, a_2, \ldots, a_n$. Nechť c je libovolný společný dělitel prvků $a_1, a_2, \ldots, a_n$. Pak $c \mid d$, a protože $d \mid d_1$, dostáváme $c \mid d_1$. Tedy d_1 je také největším společným dělitelem prvků $a_1, a_2, \ldots, a_n$. Znamená to tedy, že pokud největší společný dělitel daných prvků existuje, pak dalšími největšími společnými děliteli těchto prvků jsou právě všechny prvky s ním asociované. Můžeme proto také říci, že největší společný dělitel daných prvků (pokud existuje) je určen jednoznačně až na asociovanost.

Věta

Jestliže v oboru integrity $\mathscr{J}$ existuje ke každým dvěma prvkům jejich největší společný dělitel, pak také k libovolnému konečnému počtu prvků z J existuje jejich největší společný dělitel v $\mathscr{J}$.

Důkaz. Nechť $a_1, a_2, \ldots, a_n \in J$. Důkaz provedeme indukcí podle počtu prvků n. Pro $n = 1$ je tvrzení triviální, protože $D(a_1) = a_1$. Pro $n = 2$ platí podle předpokladu. Nechť $n > 2$ a nechť pro $n-1$ je už pravdivost tvrzení ověřena. Pak tedy existují $u = D(a_1, a_2, \ldots, a_{n-1})$ a $d = D(u, a_n)$. Ukážeme, že $d = D(a_1, a_2, \ldots, a_n)$. Platí $u \mid a_i$ $(i = 1, 2, \ldots, n-1)$, $d \mid u$, $d \mid a_n$. Odkud, s využitím tranzitivnosti relace dělitelnosti, dostáváme $d \mid a_i$, pro každé $i = 1, 2, \ldots, n$, tj. d je společným dělitelem prvků $a_1, a_2, \ldots, a_n$. Nechť $d_1 \mid a_i$ $(i = 1, 2, \ldots, n)$. Pak $d_1 \mid u$ a $d_1 \mid a_n$, proto $d_1 \mid d$, tedy vskutku d je největším společným dělitelem prvků $a_1, a_2, \ldots, a_n$.

Poznámka. Uvedený důkaz dává také návod, jak určit $D(a_1, a_2, \ldots, a_n)$, pokud v $\mathscr{J}$ existuje největší společný dělitel pro libovolnou dvojici prvků z J. Můžeme jej totiž najít např. takto:

$$D(a_1, a_2, \ldots, a_n) = D(D(a_1, a_2, \ldots, a_{n-1}), a_n).$$

Speciálně pro $n = 3$ dostáváme

$$D(a_1, a_2, a_3) = D(D(a_1, a_2), a_3),$$

ale také např.

$$D(a_1, a_2, a_3) = D(a_1, D(a_2, a_3)).$$

Věta

Nechť $a, b, c \in J$ a nechť v $\mathscr{J}$ existují $D(a, b)$ a $D(ca, cb)$. Pak $D(ca, cb) = c \cdot D(a, b)$.

Důkaz. Na přednášce.

Věta

Nechť $a_1, a_2 \in J$, nechť existuje $d = D(a_1, a_2)$ a nechť $a_1 = db_1$, $a_2 = db_2$. Pak jsou prvky b_1 a b_2 nesoudělné.

Důkaz. Na přednášce.

Dále zavedeme duální pojmy k pojmům společný dělitel a největší společný dělitel daných prvků.

Definice

(a) Nechť $a_1, a_2, \ldots, a_n \in J$. Prvek $v \in J$ se nazývá **společný násobek** prvků $a_1, a_2, \ldots, a_n$, platí-li $a_i \mid v$ pro každé $i = 1, 2, \ldots, n$.

(b) Prvek $u \in J$ se nazývá **nejmenší společný násobek** prvků $a_1, a_2, \ldots, a_n$, je-li jejich společným násobkem a platí-li pro každý společný násobek v těchto prvků, že $u \mid v$. Nejmenší společný násobek prvků $a_1, a_2, \ldots, a_n$ budeme označovat $n(a_1, a_2, \ldots, a_n)$.

Poznámka. Podobně jako pro největší společné dělitele bychom mohli ověřit, že pokud $n(a_1, a_2, \ldots, a_n)$ existuje, pak je určen jednoznačně až na asociovanost. Platí také, že existuje-li nejmenší společný násobek ke každým dvěma prvkům z J, pak existuje nejmenší společný násobek také ke každé konečné podmnožině prvků oboru integrity $\mathscr{J}$.

Ukážeme nyní, jaké jsou vztahy mezi existencí největších společných dětitelů a nejmenších společných nasobků prvků z oboru integrity $\mathscr{J}$.

Věta

Nechť v oboru integrity $\mathscr{J}$ k libovolným dvěma prvkům existuje jejich největší společný dělitel. Pak k libovolným dvěma prvkům z $\mathscr{J}$ existuje také jejich nejmenší společný násobek.

Důkaz. Na přednášce.

Poznámka. Dále budeme hledat podmínky pro existenci největších společných dělitelů. Podle předchozí věty se ovšem v takových případech nebudeme muset zvlášť věnovat analogickému hledání podmínek pro existenci nejmenších společných násobků.

Následující věta dává metodu výpočtu nejmenšího společného násobku pomocí největšího společného dělitele.

Věta

Nechť k libovolným dvěma prvkům z J existuje v $\mathscr{J}$ jejich největší společný dělitel. Pak pro každé prvky $a, b \in J$ platí

$$D(a,b) \cdot n(a,b) = ab.$$

Speciálně, jestliže $D(a,b) = e$, pak $n(a,b) = ab$.

Důkaz. Na přednášce.

Obsah

Dále budeme studovat některé typy oborů integrity, v nichž bude zaručena existence největších společných dělitelů, popř. navíc i existence algoritmů pro výpočet největších společných dělitelů (a tedy i nejmenších společných násobků).

Věta

Jestliže $\mathscr{M}$ je okruh a $I_\alpha \trianglelefteq \mathscr{M}$ $(\alpha \in \Gamma)$, pak $I = \bigcap_{\alpha\in\Gamma} I_\alpha$ je také ideálem okruhu $\mathscr{M}$.

Důkaz. Na přednášce.

Definice

Nechť $\mathscr{M} = (M; +, \cdot)$ je okruh a $B \subseteq M$. Pak průnik všech ideálů okruhu $\mathscr{M}$, které obsahují B, nazveme **ideál generovaný množinou** B a budeme jej označovat $[B]$. Jestliže $B = \{a_1, \ldots, a_n\}$, budeme psát stručněji $B = [a_1, \ldots, a_n]$ místo $B = [\{a_1, \ldots, a_n\}]$.

Poznámka. Podle předchozí věty je $[B]$ ideál v $\mathscr{M}$. Můžeme jej charakterizovat jako nejmenší ideál v $\mathscr{M}$ obsahujici B.
Speciálně pro $B = \emptyset$ platí $[B] = \{o\}$. Často je ovšem třeba rozhodovat o prvku z M, zdali patří nebo nepatří do ideálu $[B]$ pro některou danou neprázdnou podmnožinu $B \subseteq M$.
V následující větě ukážeme, jak lze o odpovědi na tuto otázku rozhodnout v okruzích s jednotkovým prvkem.

Věta

Nechť má okruh $\mathscr{M}$ jednotkový prvek e. Pak pro libovolnou podmnožinu $\emptyset \neq B \subseteq M$ platí, že

$$[B] = \left\{ \sum_{i=1}^{k} x_i a_i y_i;\ a_i \in B,\ x_i, y_i \in M,\ k \in \mathbb{N} \right\}.$$

Důkaz. Na přednášce.

Definice

Jestliže $\mathscr{M} = (M; +, \cdot)$ je okruh a $a \in M$, pak se $[a]$ nazývá **hlavní ideál v $\mathscr{M}$ generovaný prvkem a.**

Příklady

(a) Nechť má okruh $\mathscr{M} = (M; +, \cdot)$ jednotkový prvek e, $a \in M$ a $b \in [a]$. Pak lze b vyjádřit ve tvaru $b = \sum_{i=1}^{k} x_i a y_i$. Přitom jsou-li $x, y \in M$, pak $xay \in [a]$. Podle poslední věty tedy platí, že $[a] = \{xay;\, x, y \in M\}$.

(b) Můžeme snadno ověřit, že v oboru integrity celých čisel $\mathscr{Z}$ platí pro libovolné $n \in \mathbb{Z}$, že $n\mathbb{Z}$ je ideálem v $\mathscr{Z}$ a že platí $n\mathbb{Z} = [n]$.

Definice

Obor integrity $\mathscr{J}$ se nazývá **oborem integrity hlavních ideálů**, je-li každý ideál v $\mathscr{J}$ hlavní.

Příklad

$\mathscr{Z}$ je obor integrity hlavních ideálů.

Věta

Nechť $\mathscr{J}$ je obor integrity hlavních ideálů a nechť $a_1, a_2, \ldots, a_n \in J$. Pak existují prvky $x_1, x_2, \ldots, x_n \in J$ takové, že $\sum_{i=1}^{n} a_i x_i$ je největším společným dělitelem prvků $a_1, a_2, \ldots, a_n$.

Důkaz. Na přednášce.

Důsledek

Jestliže $\mathscr{J}$ je obor integrity hlavních ideálů, pak k libovolnému konečnému počtu prvků z J existuje v $\mathscr{J}$ jejich největší společný dělitel.

Poznámka. Existují ovšem také obory integrity v nichž některé konečné množiny prvků nemají největší společný dělitel. Podle předchozí věty pak ale musí platit, že v těchto oborech integrity existují i ideály, které nejsou hlavní.

Příklad

Uvažujme množinu $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5};\, a, b \in \mathbb{Z}\}$. Platí, že $\mathscr{Z}[i\sqrt{5}]$ je číselný obor integrity, v němž jsou jednotkami právě čísla 1 a -1. Uvažujme čísla 9 a $6 + 3i\sqrt{5}$, která patří do $\mathbb{Z}[i\sqrt{5}]$. Můžeme se přesvědčit, že jejich společnými děliteli jsou právě čísla $\pm 1, \pm 3, \pm(2 + i\sqrt{5})$. Přitom ale žádné z těchto čísel není největším společným dělitelem čísel 9 a $6 + 3i\sqrt{5}$. Proto v tomto oboru integrity existují i ideály, které nejsou hlavními.

Obsah

Definice

Obor integrity $\mathscr{J}$ se nazývá **eukleidovský obor integrity**, jestllže existuje zobrazení v množiny $J \setminus \{o\}$ do množiny všech celých nezáporných čísel takové, že platí

1. $\forall a, b \in J; (a \mid b, b \neq o) \Rightarrow v(a) \leq v(b)$
2. $\forall a, b \in J, a \neq o \neq b \; \exists q, r \in J; a = bq + r$ a $r = o$ nebo $v(r) < v(b)$.

Obraz $v(a)$ prvku $a \in J$ budeme nazývat **norma prvku** a.

Věta

Jestliže $\mathscr{J}$ je eukleidovský obor integrity, $a, b \in J$, $a \neq o \neq b$, pak platí:

(a) $a \parallel b \Rightarrow v(a) = v(b)$

(b) $(a \mid b, v(a) = v(b)) \Rightarrow a \parallel b$

(c) jestliže $a \mid b$, pak a je vlastním dělitelem prvku b právě tehdy, když prvek a není jednotka v $\mathscr{J}$ a $v(a) < v(b)$

(d) jestliže k je nejmenší číslo v množině $\{v(a); o \neq a \in J\}$, pak $b \in J$ je jednotka v $\mathscr{J}$ právě tehdy, když $v(b) = k$.

Důkaz. Na přednášce.

Věta

Každý eukleidovský obor integrity je oborem integrity hlavních ideálů.

Důkaz. Na přednášce.

Poznámka. Podle předchozích vět platí, že každá konečná podmnožina eukleidovského oboru integrity $\mathscr{J}$ má v $\mathscr{J}$ největší společný dělitel. V následující větě ukážeme, že pro eukleidovské obory integrity existuje jednotný algoritmus pro nalezení největšího společného dělitele dvou, a tedy také následně libovolného konečného počtu prvků.

Věta – Eukleidův algoritmus

Nechť $\mathscr{J}$ je eukleidovský obor integrity, $a, b \in J$, $a \neq o \neq b$. Pak v J existují prvky $q_0, q_1, \ldots q_n, r_1, r_2, \ldots, r_n$, přičemž $r_n = D(a, b)$ a

$$\begin{aligned}
a &= bq_0 + r_1, \quad v(r_1) < v(b) \\
b &= r_1 q_1 + r_2, \quad v(r_2) < v(r_1) \\
&\vdots \\
r_{i-1} &= r_i q_i + r_{i+1}, \quad v(r_{i+1}) < v(r_i) \\
&\vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, \quad v(r_n) < v(r_{n-1}) \\
r_{n-1} &= r_n q_n.
\end{aligned}$$

Příklad

Platí, že $\mathscr{Z}$ je eukleidovský obor integrity. K tomu, abychom to ověřili, stačí pro každé nenulové číslo $a \in \mathbb{Z}$ položit $v(a) = |a|$. Obě podmínky z definice normy eukleidovského oboru integrity jsou zde splněny, přičemž druhá z nich využívá známé možnosti dělení celých čísel se zbytkem.

Příklad

Obor integrity Gaussových celých čísel $\mathscr{Z}[i]$, který se skládá právě z komplexních čísel tvaru $a+bi$, kde $a, b \in \mathbb{Z}$ je eukleidovský obor integrity.

Příklad

Nechť $\mathscr{T}$ je číselné těleso. Pak polynomy jedné proměnné x nad $\mathscr{T}$ tvoří obor integrity $\mathscr{T}[x]$. Pro libovolný nenulový polynom $f(x) \in \mathscr{T}[x]$ položíme $v(f(x))$ rovno stupni polynomu $f(x)$. Pak je v zobrazení, které má vlastnosti normy, a proto $\mathscr{T}[x]$ je eukleidovský obor integrity.

Obsah

Dále budeme z pohledu dělitelnosti studovat další typy oborů integrity. K tomu bude užitečné všimnout si prvků majících vlastnosti analogické těm, které mají v oboru integrity $\mathscr{Z}$ právě všechna prvočísla (a čísla k nim opačná).

Definice

Nechť $\mathscr{J}$ je libovolný obor integrity, $p \in J$, $p \neq o$, $p \nmid e$. Pak se prvek p nazývá

(a) **ireducibilní**, jestliže má pouze nevlastní dělitele (tj. jen jednotky a prvky asociované s p)

(b) **prvočinitel**, platí-li pro libovolné prvky $a, b \in J$, že pokud $p \mid ab$, pak $p \mid a$ nebo $p \mid b$.

Poznámka. Vlastnosti „být ireducibilní“ a „být prvočinitelem“ vždy má nebo nemá každý prvek z třídy vzájemně asociovaných prvků.

Věta

Jestliže $\mathscr{J}$ je obor integrity, pak každý prvočinitel v $\mathscr{J}$ je také ireducibilní v $\mathscr{J}$.

Důkaz. Na přednášce.

Poznámka. Obrácená implikace ale obecně neplatí, tzn. existují takové obory integrity, v nichž pojmy prvočinitele a ireducibilního prvku nesplývají.

Příklad

Uvažujme obor integrity $\mathscr{Z}[i\sqrt{5}]$. Platí, že číslo 3 je ireducibilním prvkem v $\mathscr{Z}[i\sqrt{5}]$, že $3 \mid 9$ a že $9 = (2+i\sqrt{5})(2-i\sqrt{5})$. Avšak $3 \nmid (2+i\sqrt{5})$ a $3 \nmid (2-i\sqrt{5})$. Tedy v $\mathscr{Z}[i\sqrt{5}]$ ireducibilní prvek 3 není prvočinitelem.

Víme, že v oboru integrity celých čísel $\mathscr{Z}$ jsou ireducibilními prvky i prvočiniteli právě všechna prvočísla a čísla k nim opačná. V následující větě ukážeme, že analogickou vlastnost (tj., že ireducibilní prvky a prvočinitelé jsou tytéž) zaručuje pro širokou třídu oborů integrity jednoduchá postačující podmínka.

Věta

Jestliže v oboru integrity $\mathscr{J}$ existuje ke každým dvěma prvkům jejich největší společný dělitel, pak každý ireducibilní prvek z J je také prvočinitelem v $\mathscr{J}$.

Důkaz. Na přednášce.

Důsledek

Jestliže $\mathscr{J}$ je eukleidovský obor integrity a $a \in J$, pak a je v $\mathscr{J}$ ireducibilní právě tehdy, když a je prvočinitelem v $\mathscr{J}$.

Nyní se budeme věnovat možnostem rozložitelnosti prvků daného oboru integrity na součiny ireducibilních prvků. Víme, že např. v oboru integrity $\mathscr{Z}$ jsou takové rozklady velmi praktické při určování největších společných dělitelů a nejmenších společných násobků dvou i více celých čísel.

Definice

Řekneme, že obor integrity $\mathscr{J}$ **splňuje podmínku konečnosti řetězců vlastních dělitelů** (KD), jestliže pro každou posloupnost $a_1, a_2, \ldots a_n$ prvků z J takovou, že $a_{i+1} \mid a_i$ pro každé $i = 1, 2, \ldots$, existuje index $n \in N$ takový, že $a_n \parallel a_{n+1}$, $a_n \parallel a_{n+2}$, $\ldots$.

Věta

Každý eukleidovský obor integrity splňuje podmínku (KD).

Důkaz. Na přednášce.

Věta

Jestliže obor integrity $\mathscr{J}$ splňuje podmínku (KD), pak každý jeho nenulouý prvek a, který není jednotkou, je možno rozložit na součin konečného počtu ireducibilních prvků v $\mathscr{J}$.

Důkaz. Na přednášce.

Následující věta je bezprostředním důsledkem předchozích dvou vět.

Věta

Jestliže $\mathscr{J}$ je eukleidovský obor integrity a jestliže a je nenulový prvek z J, který není jednotkou v $\mathscr{J}$, pak a je v $\mathscr{J}$ rozložitelný na součin konečného počtu ireducibilních prvků.

Důkaz. Na přednášce.

Při otázkách rozložitelnosti prvků daného oboru integrity na součiny ireducibilních prvků se jedná nejenom o existenci takových rozkladů, ale také o jejich jednoznačnost.

Příklad

(a) V oboru integrity $\mathscr{Z}$ platí např.

$$60 = 2 \cdot 2 \cdot 3 \cdot 5 = (-3) \cdot 2 \cdot (-5) \cdot 2.$$

(b) V oboru integrity $\mathscr{Z}[i\sqrt{5}]$ např. platí

$$9 = 3 \cdot 3 = (2 + i\sqrt{5}) \cdot (2 - i\sqrt{5}).$$

Definice

Nechť $\mathscr{J}$ je obor integrity, nechť $p_1, p_2, \ldots, p_n$, $q_1, q_2, \ldots, q_m$ jsou ireducibilní prvky v $\mathscr{J}$ a nechť

$$a = p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_m.$$

Pak řekneme, že tyto dva rozklady prvku $a \in J$ **jsou spolu asociovány**, jestliže $n = m$ a po vhodném očíslování prvků $q_1, q_2, \ldots, q_n$ platí $p_i \parallel q_i$ pro každé $i = 1, 2, \ldots, n$.

Příklad

V předchozím příkladě jsou v části (a) rozklady čísla 60 spolu asociovány, zatimco v části (b) uvedené dva rozklady čísla 9 asociovány nejsou.

Definice

Obor integrity $\mathscr{J}$ se nazývá **Gaussův obor integrity** (nebo také **obor integrity s jednoznačným rozkladem**), jestliže pro každý prvek $o \neq a \in J$, $a \nmid e$, existuje jeho rozklad na součin ireducibilních prvků a jestliže každé dva takové rozklady prvku a jsou spolu asociovány.

Příklad

Obor integrity $\mathscr{Z}[i\sqrt{5}]$ není Gaussův.

Věta

Jestliže obor integrity $\mathscr{J}$ splňuje podmínku (KD) a jestliže ke každým jeho dvěma prvkům existuje v $\mathscr{J}$ jejich největší společný dělitel, pak $\mathscr{J}$ je Gaussův obor integrity.

Důkaz. Na přednášce.

Věta

Každý eukleidovský obor integrity je Gaussův obor integrity.

Důkaz. Na přednášce.

Poznámka. Obrácená věta neplatí, o čemž se lze přesvědčit na příkladě oboru integrity $\mathscr{Z}[x]$ polynomů jedné proměnné nad oborem integrity $\mathscr{Z}$.

Nechť $\mathscr{J}$ je Gaussův obor integrity, $o \neq a \in J$, $a \nmid e$, a nechť $a = q_1 q_2 \dots q_m$ je rozklad prvku a na součin ireducibilních prvků. Upravíme tento rozklad tak, že sdružíme vždy všechny navzájem asociované činitele. Pak můžeme zapsat prvek a ve tvaru $a = j p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$, kde j je jednotka v $\mathscr{J}$, $p_1, p_2, \dots, p_n$ jsou vzájemně neasociované ireducibilní prvky z původního rozkladu prvku a, $k_1, k_2, \dots, k_n \in \mathbb{N}$ a $k_1 + k_2 + \dots k_n = m$. Rozklad $a = j p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$ se nazývá **kanonický rozklad prvku a**.

Nechť $a, b \in J$, $a \neq o \neq b$, $a \nmid e$, $b \nmid e$, a nechť $p_1, p_2, \ldots, p_n$ jsou právě všechny vzájemně neasociované ireducibilní prvky z J, které dělí aspoň jeden z prvků a, b. Pak kanonické rozklady prvků a a b můžeme rozšířit na tvar $a = jp_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$, $b = j' p_1^{l_1} p_2^{l_2} \ldots p_n^{l_n}$, kde j a j' jsou jednotky v $\mathscr{J}$, $k_i \geq 0$, $l_i \geq 0$ $(i = 1, 2, \ldots, n)$. Uvedené rozklady nazýváme **zobecněné kanonické rozklady prvků a a b**.

Věta

Nechť $\mathscr{J}$ je Gaussův obor integrity, $a, b \in J$, $a \neq o \neq b$, $a \nmid e$, $b \nmid e$, a nechť $a = jp_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$ a $b = j' p_1^{l_1} p_2^{l_2} \ldots p_n^{l_n}$ jsou jejich zobecněné kanonické rozklady. Pak platí:

(a) prvek b je dělitelem prvku a právě tehdy, když $l_i \leq k_i$ pro každé $i = 1, 2, \ldots, n$.

(b) označíme-li $r_i = \min(k_i, l_i)$ a $s_i = \max(k_i, l_i)$, $i = 1, 2, \ldots, n$, pak $D(a, b) = p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}$, $n(a, b) = p_1^{s_1} p_2^{s_2} \ldots p_n^{s_n}$.

Důkaz. Na přednášce.

Předchozí věta umožňuje určit přímo největší společné dělitele nejenom pro dvojice prvků Gaussových oborů integrity, ale i pro libovolný konečný počet prvků těchto oborů integrity. K tomu postačí sestavit zobecněné kanonické rozklady současně pro všechny uvažované prvky.

Příklad

V oboru integrity $\mathscr{Z}$ určíme největší společný dělitel trojice čísel 4500, 1176 a 5292. Nejdříve sestavíme zobecněné kanonické rozklady:

$$4500 = 2^2 \cdot 3^2 \cdot 5^3 \cdot 7^0,\ 1176 = 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^2,\ 5292 = 2^2 \cdot 3^3 \cdot 5^0 \cdot 7^2.$$

Podle předchozí věty pak platí

$$D(4500, 1176, 5292) = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 = 12,$$

$$n(4500, 1176, 5292) = 2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 = 1323000.$$

Implikace v jedné z předchozích vět je ve skutečnosti ekvivalencí.

Věta

Obor integrity $\mathscr{J}$ je Gaussovým oborem integrity právě tehdy, když $\mathscr{J}$ splňuje podmínku (KD) a ke každým dvěma prvkům z J existuje v $\mathscr{J}$ jejich největší společný dělitel.

Důkaz. Na přednášce.

Obsah

Obsah

Uspořádání a kvaziuspořádání

Definice

Nechť A je neprázdná množina. **Binární relací na A** rozumíme každou podmnožinu kartézského součinu $A \times A$. Řekneme, že relace R na A je

- **reflexivní**, jestliže $\forall x \in A$ platí: $\langle x, x \rangle \in R$
- **symetrická**, jestliže $\forall x, y \in A$ platí: $\langle x, y \rangle \in R \Rightarrow \langle y, x \rangle \in R$
- **tranzitivní**, jestliže $\forall x, y, z \in A$ platí: $(\langle x, y \rangle \in R \wedge \langle y, z \rangle \in R) \Rightarrow \langle x, z \rangle \in R$
- **antisymetrická**, jestliže $\forall x, y \in A$ platí: $(\langle x, y \rangle \in R \wedge \langle y, x \rangle \in R) \Rightarrow x = y$.

Relaci na množině A, která je reflexivní a tranzitivní, nazveme **kvaziuspořádání**. Relaci, která je reflexivní, tranzitivní a antisymetrická, nazveme **uspořádání**. Relaci, která je reflexivní, symetrická a tranzitivní, nazveme **ekvivalence**.

Tedy uspořádání je antisymetrické kvaziuspořádání, ekvivalence je symetrické kvaziuspořádání.

Je-li R uspořádání na A, pak pro zápis této relace zpravidla používáme symbol $\leq$ a místo $\langle x, y \rangle \in R$ zapisujeme $x \leq y$ nebo také $y \geq x$. Je-li $x \leq y$ a $x \neq y$, zapisujeme $x < y$ nebo $y > x$. Je-li $\leq$ uspořádání na A, a jestliže pro dva prvky $x, y \in A$ neplatí ani $x \leq y$ ani $y \leq x$, zapisujeme $x \parallel y$ a říkáme, že prvky x a y jsou **nesrovnatelné**.

Příklady

(1) Relace $\leq$ na množině všech čísel celých (resp. racionálních, resp. reálných) je uspořádání.

(2) Relace dělitelnosti na množině všech čísel přirozených je uspořádání.

(3) Relace inkluze $\subseteq$ na množině *ExpM* všech podmnožin neprázdné množiny M je uspořádání.

(4) Relace dělitelnosti na množině všech čísel celých je kvaziuspořádání, které není uspořádáním, neboť např. 3 dělí -3, a -3 dělí 3, ale $-3 \neq 3$.

(5) Nechť F je množina všech reálných funkcí jedné reálné proměnné na intervalu (a, b). Položme $f \leq g$ pro $f, g \in F$, právě když $\forall x \in (a, b)$ platí $f(x) \leq g(x)$ (pro čísla $f(x), g(x) \in \mathbb{R}$). Pak takto zavedená relace je uspořádání na F.

Je-li $\leq$ uspořádání na množině A, dvojici $(A, \leq)$ nazveme **uspořádaná množina**. Jestliže $\leq$ je uspořádání na A takové, že $\forall x, y \in A$ platí buď $x \leq y$ nebo $y \leq x$, pak se $\leq$ nazývá **úplné uspořádání** a A se nazývá **úplně uspořádaná množina** neboli **řetězec**. Je-li $\leq$ uspořádání na A takové, že $\forall x, y \in A$, $x \neq y$ platí $x \parallel y$, pak se $(A, \leq)$ nazývá **antiřetězec**.
Množiny z příkladu (1), tj. $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$ jsou řetězce, uspořádané množiny z příkladů (2), (3), (5) nejsou řetězce (v příkladu (3) je $(M, \subseteq)$ řetězec, právě když je M jednoprvková).

Věta (Princip duality)

Nechť $\leq$ je uspořádání na množině A. Pak inverzní relace, tj. $\leq^{-1}$ (označení $\geq$), je opět uspořádání na A.

Důkaz. Je ihned zřejmé, že z reflexivity, antisymetrie a tranzitivity relace $\leq$ plyne, že tyto vlastnosti má i relace $\geq$. $\square$

Je-li $(A, \leq)$ konečná uspořádaná množina, pak ji lze snadno (pro $|A| \leq 10$) znázornit v rovině i s relací uspořádání. Zavedeme následující pojem: Nechť $x, y \in A$, $x < y$. Řekneme, že prvek y **kryje** prvek x, neboli x **je pokrýván** prvkem y, jestliže $\forall z \in A$ splňující $x \leq z \leq y$ platí $x = z$ nebo $z = y$. Zapisujeme $x \prec y$. Relaci $\prec$ nazveme **relace pokrytí**.

Nyní popíšeme znázornění konečné uspořádané množiny diagramem: Nechť $(A, \leq)$ je konečná. Representujme každý prvek z A bodem v rovině a to tak, že je-li $a, b \in A$, $a < b$, pak bod b znázorníme nad bodem a (posunutí do strany tuto situaci neovlivní). Je-li $x \prec y$, pak body x, y spojíme úsečkou. Vzniklou konfiguraci nazveme **diagram uspořádané množiny** $(A, \leq)$, nebo **Hasseův diagram**.

Příklad

Nechť $A = \{a, b, c, d, e, f, g\}$ a relace $\leq$ je na A dána takto: $a \leq c$, $b \leq c$, $c \leq d$, $a \leq d$, $b \leq d$, $e \leq f$, $e \leq g$, a $\forall x \in A$ je $x \leq x$. Pak $(A, \leq)$ má diagram:

Obr. 1

Příklad (speciální případy uspořádaných množin)

(a) Je-li $(A, \leq)$ řetězec, pak je diagram znázorněn na Obr. 2.

(b) Je-li $(A, \leq)$ antiřetězec, pak je diagram znázorněn na Obr. 3.

(c) Je-li $(A, \leq)$ konečná uspořádaná množina a $\geq$ je inverzní uspořádání, pak dle principu duality je $(A, \geq)$ rovněž uspořádaná množina, jejíž diagram je „vzhůru nohama“ obrácený diagram množiny $(A, \leq)$.

Obr. 2

Obr. 3

Obsah

Definice

Nechť $(A, \leq)$ je uspořádaná množina. Prvek $a \in A$ se nazývá

- **minimální**, jestliže $x \leq a \Rightarrow x = a$
- **nejmenší**, jestliže $\forall x \in A$ platí $a \leq x$
- **maximální**, jestliže $a \leq x \Rightarrow x = a$
- **největší**, jestliže $\forall x \in A$ platí $x \leq a$.

Je ihned zřejmé, že má-li $(A, \leq)$ největší prvek, pak je jediný; má-li $(A, \leq)$ nejmenší prvek, pak je jediný. Na Obr. 1 je uspořádaná množina, která nemá ani nejmenší, ani největší prvek, avšak a, b, e jsou minimální prvky, d, f, g jsou maximální prvky v $(A, \leq)$.
Má-li $(A, \leq)$ největší prvek, pak tento prvek je maximální a jiné maximální prvky v $(A, \leq)$ neexistují; duálně, má-li $(A, \leq)$ nejmenší prvvek, pak je tento prvek minimální a jiné minimální prvky v $(A, \leq)$ neexistují. Každý konečný řetězec má největší a nejmenší prvek. Antiřetězec (se dvěma a více prvky) nemá ani největší, ani nejmenší prvek, ale každý jeho prvek je současně minimální i maximální.

Definice

Nechť $(A, \leq)$ je uspořádaná množina a $M \subseteq A$. Označme symbolem

$$U(M) = \{x \in A;\ y \leq x \text{ pro každé } y \in M\}$$
$$L(M) = \{x \in A;\ x \leq y \text{ pro každé } y \in M\}.$$

Množina $U(M)$ se nazývá **horní kužel množiny M**, množina $L(M)$ se nazývá **dolní kužel množiny M**. Má-li $U(M)$ nejmenší prvek, pak se tento prvek nazývá **supremum M** a značí se $\sup M$; má-li $L(M)$ největší prvek, pak se tento prvek nazývá **infimum M** a značí se $\inf M$.

Jelikož v uspořádané množině může být nejvýše jediný největší (nejmenší) prvek, je zřejmé, že pro každou $M \subseteq A$ buď $\sup A$ ($\inf A$) neexistuje, nebo je jediné. Je-li $M = \{a_1, \ldots, a_n\}$, pak místo $\sup(\{a_1, \ldots, a_n\})$ píšeme $\sup(a_1, \ldots, a_n)$, místo $\inf(\{a_1, \ldots, a_n\})$ píšeme $\inf(a_1, \ldots, a_n)$.

Zřejmě, je-li $a \leq b$, je $\sup(a,b) = b$, $\inf(a,b) = a$. Je-li $(A, \leq)$ konečná uspořádaná množina, $a, b \in A$, a platí-li $a||b$, pak v diagramu $(A, \leq)$ nalezneme $\sup(a,b)$ (pokud existuje) jako nejmenší prvek, který je spojen s prvky a, b a leží nad nimi; $\inf(a,b)$ (pokud existuje) je pak největší prvek, který je spojen s a, b, a leží pod nimi. Např. na diagramu množiny A (na Obr. 1) je $\sup(a,b) = c$, $\inf(f,g) = e$.

Příklad

Ověřte, že pro každou uspořádanou množinu $(A, \leq)$ a pro každé dvě její podmnožiny X, Y platí:

(i) $U(\emptyset) = A$, $L(\emptyset) = A$

(ii) $X \subseteq Y \Rightarrow L(Y) \subseteq L(X)$ a $U(Y) \subseteq U(X)$

(iii) má-li A největší prvek a, pak $U(A) = \{a\}$, nemá-li A největší prvek, pak $U(A) = \emptyset$; duálně, má-li A nejmenší prvek b, pak $L(A) = \{b\}$, nemá-li A nejmenší prvek, pak $L(A) = \emptyset$

(iv) $L(U(A)) = A$, $U(L(A)) = A$.

Definice

Polosvazem nazýváme komutativní idempotentní pologrupu, tj. takový grupoid $(G, \circ)$, kde pro každé tři prvky $a, b, c \in G$ platí tyto identity:

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

(k) komutativita: $a \circ b = b \circ a$

(i) idempotence: $a \circ a = a$.

Věta P1

Nechť $(G, \circ)$ je polosvaz. Relace $\leq$ definovaná na G předpisem:

$$a \leq b \text{ právě když } a \circ b = b$$

je uspořádání, přičemž v uspořádané množině $(G, \leq)$ existuje $\sup(a, b)$ pro každé $a, b \in G$ a platí $\sup(a, b) = a \circ b$.

Důkaz. Z idempotence ihned plyne $a \leq a$ pro každé $a \in G$, tedy $\leq$ je reflexivní. Je-li $a \leq b$, $b \leq c$ pro $a, b, c \in G$, pak $a \circ b = b$, $b \circ c = c$, odkud z asociativity dostáváme
$a \circ c = a \circ (b \circ c) = (a \circ b) \circ c = b \circ c = c$, tedy $a \leq c$, tj. $\leq$ je tranzitivní. Nechť $a \leq b$ a $b \leq a$. Vzhledem ke komutativitě dostáváme
$b = a \circ b = b \circ a = a$, tedy $\leq$ je antisymetrická, tj. $\leq$ je uspořádání v G. Z asociativity, komutativity a idempotence plyne $a \circ (a \circ b) = a \circ b$, $b \circ (a \circ b) = a \circ b$, tedy $a \leq a \circ b$, $b \leq a \circ b$, tj. $a \circ b \in U(a, b)$. Nechť $c \in U(a, b)$, pak $a \leq c$, $b \leq c$, tedy $a \circ c = c$, $b \circ c = c$, tudíž $(a \circ b) \circ c = (a \circ b) \circ (c \circ c) = (a \circ c) \circ (b \circ c) = c \circ c = c$, tj. $a \circ b \leq c$. Je tedy $a \circ b$ nejmenší prvek v $U(a, b)$, tj. $a \circ b = \sup(a, b)$. □

Věta P2

Nechť $(G, \leq)$ je uspořádaná množina a pro každé $a, b \in G$ existuje $\sup(a, b)$. Označme $a \circ b = \sup(a, b)$, pak $(G, \circ)$ je polosvaz.

Důkaz. Jelikož $\sup(a, a) = a$, $\sup(a, b) = \sup(b, a)$, $\sup(a, \sup(b, c)) = \sup(a, b, c) = \sup(\sup(a, b), c)$, je ihned zřejmé, že operace $\circ$ je idempotentní, komutativní a asociativní. □

Poznámka. Zaměníme-li uspořádání za tzv. duální, tj. $\geq$, pak, dle principu duality, pojem suprema v duálním uspořádaní $\geq$ je infimem v uspořádání $\leq$. Definujeme-li v polosvazu uspořádání předpisem:

$$a \leq b \text{ právě když } a \circ b = a,$$

pak pro každé $a, b \in G$ existuje $\inf(a, b)$ a platí $\inf(a, b) = a \circ b$ (viz věta P1). Obráceně, je-li $(G, \leq)$ uspořádaná množina, kde pro každé $a, b \in G$ existuje $\inf(a, b)$, pak $(G, \circ)$, kde $a \circ b = \inf(a, b)$ je polosvaz (srovnej s větou P2).

Příklady

(1) Nechť $M \neq \emptyset$, pak v $(ExpM, \subseteq)$ existuje pro každé A, B supremum a platí $\sup(A, B) = A \cup B$. Tedy $(ExpM, \cup)$ je polosvaz. Duálně, $\inf(A, B) = A \cap B$, tedy $(ExpM, \cap)$ je opět polosvaz.

(2) Na množině všech přirozených čísel $\mathbb{N}$ zaveďme relaci dělitelnosti: $a|b$ právě když a dělí b. Pak $|$ je uspořádání na $\mathbb{N}$ a $\forall a, b \in \mathbb{N}$ je $\sup(a, b) =$ nejmenší společný násobek čísel a, b, $\inf(a, b) =$ největší společný dělitel čísel a, b; označujeme $n(a, b)$, $D(a, b)$. Tedy $(\mathbb{N}, n)$ a $(\mathbb{N}, D)$ jsou polosvazy.

Tvrzení. Nechť $(G, \circ)$ je polosvaz a $(H, \circ)$ je podgrupoid grupoidu $(G, \circ)$. Pak $(H, \circ)$ je opět polosvaz, tzv. **podpolosvaz polosvazu** $(G, \circ)$.

Obsah

Definice

Nechť L je neprázdná množina, nechť $\vee, \wedge$ jsou dvě binární operace na L takové, že $(L; \wedge)$ a $(L; \vee)$ jsou polosvazy a pro každé $a, b \in L$ platí tzv. **zákony absorpce**:

(ab) $a \wedge (a \vee b) = a, \quad a \vee (a \wedge b) = a.$

Pak se $(L, \vee, \wedge)$ nazývá **svaz**, přičemž operaci $\vee$ nazýváme **spojení** a operaci $\wedge$ nazyváme **průsek**.

Tedy svaz je množina se dvěmi binárními operacemi, které jsou asociativní, komutativní, idempotentní a splňují zákony absorpce.

Lemma

Nechť $L \neq \emptyset$ je množina se dvěmi binárními operacemi, které jsou asociativní, komutativní a splňují zákony absorpce. Pak $\vee, \wedge$ jsou idempotentní, tj. $(L; \vee, \wedge)$ je svaz.

Důkaz. Nechť $a, b \in L$. Označme $a \wedge b = c$. Dle absorpce obdržíme $a = a \vee (a \wedge b)$, tedy $a \wedge a = a \wedge (a \vee (a \wedge b)) = a \wedge (a \vee c) = a$, tj. operace $\wedge$ je idempotentní. Duálně pro operaci $\vee$. □

Věta

Nechť $(L; \vee, \wedge)$ je svaz. Definujme relaci $\leq$ na L takto:

$$a \leq b \text{ právě když } a \vee b = b.$$

Pak platí:

(i) $\leq$ je uspořádání na L (tzv. **indukované uspořádání**)

(ii) $a \vee b = \sup(a, b)$

(iii) $a \leq b$ právě když $a \wedge b = a$

(iv) $a \wedge b = \inf(a, b)$.

Důkaz. Tvrzení (i) a (ii) plynou přímo z věty P1. Dále, nechť $a \leq b$. Tato relace je ekvivalentní s $a \vee b = b$, což dle absorpce dává $a \wedge b = a \wedge (a \vee b) = a$, tedy platí (iii). Z duality plyne ihned (iv). □

Věta

Nechť $(L, \leq)$ je uspořádaná množina, kde pro každé $a, b \in L$ existuje $\sup(a, b)$, $\inf(a, b)$. Označme $\sup(a, b) = a \vee b$, $\inf(a, b) = a \wedge b$. Pak $(L; \vee, \wedge)$ je svaz.

Důkaz. Z věty P2 plyne, že stačí dokázat zákony absorpce pro operace $\vee, \wedge$. Jelikož

$$a \wedge b = \inf(a, b) \leq a \leq \sup(a, b) = a \vee b,$$

platí zřejmě

$$a \vee (a \wedge b) = \sup(a, \inf(a, b)) = a,$$

$$a \wedge (a \vee b) = \inf(a, \sup(a, b)) = a.$$

□

Příklady

(1) Každý řetězec je svaz, kde zřejmě $a \vee b = \max(a, b)$, $a \wedge b = \min(a, b)$.

(2) Nechť $M \neq \emptyset$, pak $(ExpM; \cup, \cap)$ je svaz.

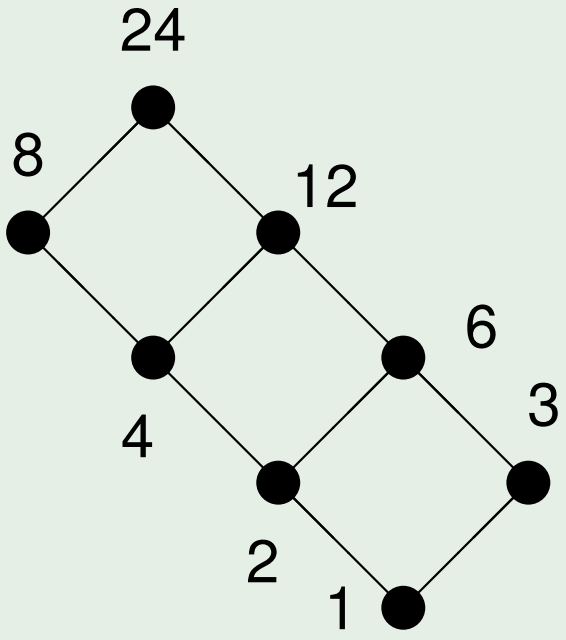
(3) Nechť $\mathbb{N}$ je množina přirozených čísel, $a \vee b$ je $n(a, b)$, $a \wedge b$ je $D(a, b)$. Pak $(\mathbb{N}; \vee, \wedge)$ je svaz.

(4) Nechť $(G, \cdot)$ je grupa. Pak množina všech normálních podgrup tvoří svaz, přičemž $A \wedge B = A \cap B$, $A \vee B = A \cdot B$, kde A, B jsou normální podgrupy.

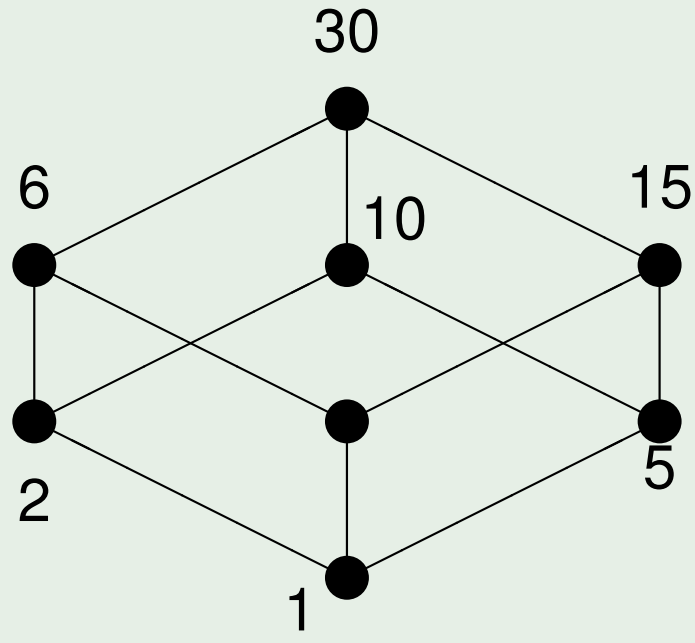
(5) Nechť $(R, +, \cdot)$ je okruh. Množina K všech ideálů okruhu R je svaz, kde pro $I, J \in K$ je $I \wedge J = I \cap J$, $I \vee J$ je ideál, generovaný množinou $I \cup J$.

Příklad

Nechť n je přirozené číslo, $P(n)$ je množina všech přirozených dělitelů čísla n. Pak $(P(n); n, D)$ je svaz. Pro $n = 24$ resp. $n = 30$ je tento svaz znázorněn diagramem na Obr. 4, resp Obr. 5 (kde uspořádání je zřejmě relace dělitelnosti).



Obr. 4



Obr. 5

Poznámka. Princip duality se ve svazech uplatní tímto způsobem: Nahradíme-li v platném tvrzení o svazu všude symbol $\vee$ symbolem $\wedge$ a symbol $\wedge$ symbolem $\vee$, resp. symbol $\leq$ symbolem $\geq$ a naopak, dostaneme opět platné tvrzení, tzv. **duální tvrzení**. Proto v důkazech dokazujeme zpravidla jen jedno tvrzení, neboť duální z něj získáme dle principu duality výše uvedeným postupem.

Definice

Nechť $(L; \vee, \wedge)$ je svaz, nechť $\emptyset \neq A \subseteq L$. A se nazývá **podsvaz** svazu $(L; \vee, \wedge)$, jestliže $\forall a, b \in A$ platí $a \vee b \in A$, $a \wedge b \in A$.

Věta

Nechť $(L; \vee, \wedge)$ je svaz, A_i pro $i \in I$ jeho podsvazy. Je-li $\cap\{A_i;\ i \in I\} \neq \emptyset$, pak je $\cap\{A_i;\ i \in I\}$ podsvazem svazu $(L; \vee, \wedge)$.

Důkaz. Nechť $A = \cap\{A_i;\ i \in I\} \neq \emptyset$, nechť $a, b \in A$. Pak $a, b \in A_i\ \forall i \in I$, přičemž A_i je podsvaz, tedy i $a \vee b \in A_i$, $a \wedge b \in A_i\ \forall i \in I$, tedy $a \vee b \in A$, $a \wedge b \in A$, tj. A je podsvaz. □

Definice

Nechť $(L; \vee, \wedge)$ je svaz a $\leq$ je indukované uspořádání. Má-li $(L; \leq)$ nejmenší prvek, nazýváme jej **nula svazu** a značíme 0; má-li $(L; \leq)$ největší prvek, nazýváme jej **jednotka svazu** a značíme 1.

Věta

Má-li svaz $(L; \vee, \wedge)$ prvek 0, pak pro každé $x \in L$ platí

$$x \wedge 0 = 0, \qquad x \vee 0 = x.$$

Má-li svaz $(L; \vee, \wedge)$ prvek 1, pak pro každé $x \in L$ platí

$$x \wedge 1 = x, \qquad x \vee 1 = 1.$$

Důkaz. Je zřejmý. □

Definice

Nechť $(A; \leq)$ je uspořádaná množina, $a, b \in A$ a platí $a \leq b$. Množina $[a, b] = \{x \in A;\ a \leq x \leq b\}$ se nazývá **interval v A.**

Věta

Nechť $(L; \vee, \wedge)$ je svaz. Pak platí:

(i) každý interval svazu $(L; \vee, \wedge)$ je jeho podsvaz

(ii) pro každý prvek $a \in L$ je $\{a\}$ podsvaz svazu $(L; \vee, \wedge)$

(iii) má-li L prvky 0 a 1, pak $L = [0, 1]$.

Důkaz.
(i): Nechť $\leq$ je indukované uspořádání, $a, b \in L$ a platí $a \leq b$. Nechť $x, y \in [a, b]$. Pak $a \leq x \leq b$, $a \leq y \leq b$, tedy také $a \leq \inf(x, y) \leq \sup(x, y) \leq b$ tj. $x \vee y \in [a, b]$, $x \wedge y \in [a, b]$, tedy $[a, b]$ je podsvaz svazu $(L; \vee, \wedge)$.
(ii): Jelikož $a \leq a$ pro každé $a \in L$, je $\{a\} = [a, a]$, tedy také $\{a\}$ je podsvaz svazu $(L; \vee, \wedge)$.
(iii): Má-li L prvky 0 a 1, pak vzhledem k indukovanému uspořádání $\leq$ je $0 \leq x \leq 1$ pro každé $x \in L$. □

Věta

Nechť $(L;\vee,\wedge)$ je konečný svaz (tj. L je konečná množina). Pak v $(L;\vee,\wedge)$ existují prvky 0 a 1.

Důkaz. Je-li L konečná množina, tj. $L=\{a_1,a_2,\ldots,a_n\}$, položme $a=a_1\wedge a_2\wedge\cdots\wedge a_n$, $b=a_1\vee a_2\vee\cdots\vee a_n$. Zřejmě $a\leq a_i\leq b$ pro každý prvek $a_i\in L$, tedy a je nula a b je jednotka svazu $(L;\vee,\wedge)$. □

Věta

Nechť $(A;\vee,\wedge)$ je svaz, $\leq$ je indukované uspořádání. Pak pro každé prvky $a,b,c,d\in A$ platí:

(i) $a\wedge b\leq a\leq a\vee b$

(ii) jestliže $a\leq b$, $c\leq d$, pak $a\wedge c\leq b\wedge d$, $a\vee c\leq b\vee d$.

Důkaz.
(i): Je zřejmé, neboť $\inf(a,b)\leq a\leq\sup(a,b)$.
(ii): Jestliže $a\leq b$, $c\leq d$, pak $a\wedge b=a$, $c\wedge d=c$. Tedy

$$a\wedge c=(a\wedge b)\wedge c=(a\wedge b)\wedge(c\wedge d)=(a\wedge c)\wedge(b\wedge d),$$

odkud $a\wedge c\leq b\wedge d$. Duálně lze dokázat druhou nerovnost. □

Definice

Nechť $(A;\vee,\wedge)$ a $(B;\vee,\wedge)$ jsou svazy. Zobrazení $h : A \to B$ se nazývá **homomorfismus**, jestliže pro každé $a, b \in A$ platí:

$$h(a \vee b) = h(a) \vee h(b), \quad h(a \wedge b) = h(a) \wedge h(b).$$

Bijektivní homomorfismus se nazývá **izomorfismus**.

Definice

Ekvivalence θ na množině L se nazývá **kongruence svazu** $(L;\vee,\wedge)$, jestliže pro každé $a, b, c, d \in L$ platí implikace:

$$\langle a, b\rangle \in \theta, \langle c, d\rangle \in \theta \Rightarrow \langle a \vee c, b \vee d\rangle \in \theta, \langle a \wedge c, b \wedge d\rangle \in \theta.$$

Úmluva. Pokud nehrozí nebezpečí nedorozumění, budeme místo zápisu: $(L;\vee,\wedge)$ je svaz, psát pouze: L je svaz; v tomto případě budou vždy operace svazu L označeny $\vee$ a $\wedge$.

Věta

Buďte A, B, C svazy, $f : A \to B$, $g : B \to C$ homomorfismy (resp. izomorfismy). Pak složené zobrazení $f \circ g$ je opět homomorfismus (izomorfismus) $A \to C$. Je-li $f : A \to B$ izomorfismus, je i $f^{-1} : B \to A$ izomorfismus. Identické zobrazení $id(x) = x$ je izomorfismem svazu A. Je-li h homomorfismus svazu A do B, $a, b \in A$ a platí $a \leq b$ vzhledem k indukovanému uspořádání na A, pak $h(a) \leq h(b)$ vzhledem k indukovanému uspořádání na B.

Důkaz. Nechť $a, b \in A$, pak $f \circ g(a \vee b) = g(f(a \vee b)) = g(f(a) \vee f(b)) = g(f(a)) \vee g(f(b)) = f \circ g(a) \vee f \circ g(b)$, duálně pro operaci $\wedge$, tedy složení dvou homomorfismů je homomorfismus. Jelikož složení dvou bijekcí je bijekce, je složení dvou izomorfismů izomorfismem.
Je-li $f : A \to B$ izomorfismus, $x, y \in B$, pak, jelikož f je surjekce, existují $a, b \in A$ tak, že $f(a) = x, f(b) = y$. Odkud $f^{-1}(x \vee y) = f^{-1}(f(a) \vee f(b)) = f^{-1}(f(a \vee b)) = a \vee b = f^{-1}(x) \vee f^{-1}(y)$, duálně pro operaci $\wedge$, tedy inverzní zobrazení k izomorfismu je izomorfismus. Identita je zřejmě bijekcí a platí $id(x \vee y) = x \vee y = id(x) \vee id(y)$, duálně pro $\wedge$, tedy je izomorfismem.
Nechť $a, b \in A$, $a \leq b$. Pak $a \wedge b = a$, a pro homomorfismus h platí $h(a) = h(a \wedge b) = h(a) \wedge h(b)$, tedy $h(a) \leq h(b)$. □

Označení. Jestliže existuje izomorfismus svazu A na svaz B, říkáme, že A, B jsou **izomorfní**, což zapisujeme $A \cong B$.

Poznámka. Vzhledem k předchozí větě platí: jsou-li A, B, C svazy, pak

$$A \cong A,$$
$$A \cong B \Rightarrow B \cong A,$$
$$(A \cong B \text{ a } B \cong C) \Rightarrow A \cong C,$$

tedy relace „býti izomorfní“ je ekvivalencí na třídě všech svazů.

Poznámka. Bijekce svazu A na svaz B je izomorfismus tehdy a jen tehdy, jestliže $a \leq b$ právě když $h(a) \leq h(b)$.

Věta o homomorfismu

(1) Nechť A, B jsou svazy a $h : A \to B$ je surjektivní homomorfismus. Definujme relaci θ_h na A takto:

$$\langle a, b \rangle \in \theta_h \text{ právě když } h(a) = h(b).$$

Pak θ_h je kongruence na A a $A/\theta_h \cong B$.

(2) Nechť θ je kongruence na svazu L. Pro $a \in L$ označme $[a]_\theta$ tu třídu L/θ, která obsahuje prvek a. Pak zobrazení $h_\theta : L \to L/\theta$ dané předpisem

$$h_\theta(a) = [a]_\theta$$

je surjektivní homomorfismus svazu L na L/θ.

Důkaz. Na přednášce.

Obsah

Víme, že svazem je každá uspořádaná množina $(A, \leq)$, ve které existují $\sup(a, b)$ a $\inf(a, b)$ pro každé dva prvky $a, b \in A$. Indukcí lze snadno dokázat, že je-li $(A, \leq)$ svazem, pak existují sup a inf pro každou konečnou podmnožinu $B \subseteq A$. Nelze odtud však odvodit žádné tvrzení o sup a inf nekonečných podmnožin. Například ve svazu $(\mathbb{N}; n, D)$ pro žádnou nekonečnou podmnožinu $M \subseteq \mathbb{N}$ zřejmě $\sup M$ neexistuje.

Avšak existují svazy, ve kterých sup a inf existují i pro nekonečné podmnožiny, např. svaz $(ExpM; \cup, \cap)$ pro nekonečnou množinu M. Zavedeme proto následující pojem.

Definice

Uspořádaná množina $(L, \leq)$ se nazývá **úplný svaz**, jestliže pro každou $S \subseteq L$ existuje $\sup S$ a $\inf S$ v L.

Je zřejmé, že každý úplný svaz je svazem, neboť podle této definice existují sup a inf i pro dvouprvkové podmnožiny. Navíc každý úplný svaz $(L;\leq)$ má vždy největší a nejmenší prvek, jsou to prvky $1 = \sup L$ a $0 = \inf L$. Dále, v úplném svazu lze předpokládat existenci jen jednoho z prvků sup a inf pro libovolnou podmnožinu; druhý prvek pak již lze zkonstruovat.

Věta

Nechť $(L;\leq)$ je uspořádaná množina, ve které existuje $\inf S$ pro každou $S \subseteq L$. Pak $(L;\leq)$ je úplný svaz.

Důkaz. Nechť $S \subseteq L$ a nechť $U(S)$ je horní kužel množiny S. Zřejmě $U(S) \neq \emptyset$, neboť $1 = \inf \emptyset$, $1 \in U(S)$. Označme $x = \inf U(S)$. Zřejmě $s \leq x$ pro každé $s \in S$ a dále, je-li $s \leq y$ pro každé $s \in S$, pak $y \in U(S)$, tedy $x = \inf U(S) \leq y$, tedy $x = \sup S$. □

Poznámka. Dle principu duality lze předchozí větu vyslovit i ve tvaru: má-li každá podmnožina S uspořádané množiny $(L; \leq)$ supremum, pak je $(L; \leq)$ úplný svaz.

Příklad

Nechť $M \neq \emptyset$ je množina (např. nekonečná). Pak množina všech ekvivalencí na M uspořádaná množinovou inkluzí je úplný svaz. Dle předchozí věty totiž stačí dokázat, že pro libovolnou množinu I a libovolnou množinu ekvivalencí E_i $(i \in I)$ na M je $\cap\{E_i;\ i \in I\}$ opět ekvivalence.
Analogicky se dokáže, že množina všech kongruencí $ConA$ na grupoidu (grupě, okruhu, svazu) A uspořádaná vzhledem k $\subseteq$ je úplný svaz.

Definice

Nechť $(A, \leq)$, $(B, \leq)$ jsou dvě uspořádané množiny. Zobrazení $f : A \to B$ se nazývá **izotonní zobrazení**, jestliže pro každé $a, b \in A$ platí: jestliže $a \leq b$, pak $f(a) \leq f(b)$.

Věta o pevném bodu

Nechť $(L, \leq)$ je úplný svaz a nechť f je izotonní zobrazení L do L. Pak existuje prvek $x \in L$ takový, že $f(x) = x$ (tzv. **pevný bod zobrazení f**).

Důkaz. Nechť $(L, \leq)$ je úplný svaz a $f : L \to L$ je izotonní zobrazení. Nechť $S = \{v \in L;\, v \leq f(v)\}$. Zřejmě $S \neq \emptyset$, neboť nejmenší prvek $0 \in S$. Položme $x = \sup S$. Pak pro každé $s \in S$ je $s \leq x$, tedy $s \leq f(s) \leq f(x)$. Tedy $f(x)$ je větší nebo rovno každému $s \in S$, je tedy větší nebo rovno i $\sup S = x$, tj. $x \leq f(x)$. Ale f je izotonní zobrazení, tedy $f(x) \leq f(f(x))$, tj. $f(x) \in S$. Ale $x = \sup S$, tedy $f(x) \leq x$. Odtud $f(x) = x$. □

Dokážeme, že každý svaz je možné považovat za podsvaz úplného svazu. Nejprve definujme:

Definice

Nechť $(L;\vee,\wedge)$ je svaz, $\emptyset \neq I \subseteq L$. Množina I se nazývá **ideál svazu** $(L;\vee,\wedge)$, pokud splňuje následující podmínky:

(i) jestliže $x, y \in I$, pak $x \vee y \in I$

(ii) jestliže $x \in I$, $a \in L$, pak $x \wedge a \in I$.

Věta

Nechť $(L;\vee,\wedge)$ je svaz, J_0 je množina všech ideálů svazu L a $J = J_0 \cup \{\emptyset\}$. Pak $(J,\subseteq)$ je úplný svaz.

Důkaz. Nechť $K \subseteq J_0$, tj. K je některá množina ideálů svazu L. Je-li $\cap K = \emptyset$, pak $\cap K \in J$. Nechť $\cap K \neq \emptyset$, označme $\cap K = J$. Nechť $x, y \in J$, $a \in L$. Pak $\forall I \in K$ je $x, y \in I$, tudíž $x \vee y \in I$ a $x \wedge a \in I$ pro každé $I \in K$, tedy i $x \vee y \in \cap K = J$, $x \wedge a \in J$, tj. J je ideál, tedy $\cap K = J \in J_0 \subseteq J$. Tedy pro každou $K \subseteq J$ je $\inf K = \cap K$ prvkem J, tj. $(J,\subseteq)$ úplný svaz. □

Lemma

Nechť L je svaz, $a \in L$. Pak $I(a) = \{x \in L;\, x \leq a\}$ je ideál svazu L.

Důkaz. Nechť $x, y \in I(a)$. Pak $x \leq a$, $y \leq a$, tedy $x \vee y \leq a \vee a = a$, tj. $x \vee y \in I(a)$. Je-li $b \in L$, pak $x \wedge b \leq x \leq a$, tedy $x \wedge b \in I(a)$, tj. $I(a)$ je ideál svazu L. □

Poznámka. Je-li svaz L konečný, I jeho ideál, pak zřejmě $I = I(a)$, kde $a = \sup I$. Tedy $(\{I(a);\, a \in L\}, \subseteq)$ je svaz všech ideálů konečného svazu L, tj. zobrazení $f : a \to I(a)$ je izomorfismus L na $(J; \subseteq)$. Množina $I(a)$ se nazývá **hlavní ideál svazu** L. U konečného svazu je tedy každý ideál hlavní.

Věta

Každý svaz je izomorfní s podsvazem úplného svazu.

Důkaz. Nechť L je svaz. Definujme zobrazení f svazu L do množiny všech ideálů J svazu L takto: $f(a) = I(a)$. Pak zřejmě f je injekce, neboť $I(a) = I(b) \Rightarrow a = b$. Tedy f je bijekce na množinu $\{I(a);\, a \in L\} \subseteq J$. Dokážeme, že f je svazový homomorfismus. Pro každé $a, b \in L$ zřejmě platí $a \wedge b \in I(a)$, $a \wedge b \in I(b)$, tedy $a \wedge b \in I(a) \cap I(b) \Rightarrow I(a \wedge b) \subseteq I(a) \cap I(b)$. Jestliže $x \in I(a) \cap I(b)$, pak $x \leq a$, $x \leq b$, tedy $x \leq a \wedge b \Rightarrow x \in I(a \wedge b)$, tedy $I(a) \cap I(b) \subseteq I(a \wedge b)$. Dohromady dostáváme

$$f(a \wedge b) = I(a \wedge b) = I(a) \cap I(b) = f(a) \cap f(b).$$

Dle důkazu předchozí věty je $I(a) \vee I(b)$ rovno průniku všech ideálů z J, obsahujících $I(a) \cup I(b)$. Avšak $I(a) \subseteq I(a \vee b)$, $I(b) \subseteq I(a \vee b)$, tj. $I(a) \cup I(b) \subseteq I(a \vee b)$, tedy i $I(a) \vee I(b) \subseteq I(a \vee b)$. Je-li však $I \in J$ takový, že $I(a) \cup I(b) \subseteq I$, pak $a \in I$, $b \in I$, tedy i $a \vee b \in I$, tj. $I(a \vee b) \subseteq I$. Neboli $I(a) \vee I(b) = I(a \vee b)$, odkud

$$f(a \vee b) = I(a \vee b) = I(a) \vee I(b) = f(a) \vee f(b),$$

tedy f je homomorfismus L do úplného svazu $(J; \subseteq)$, neboli f je izomorfismus L na podsvaz $\{I(a);\, a \in L\}$. □

Obsah

Věta

Nechť L je svaz. Pak pro každé $a, b, c \in L$ platí tzv. **distributivní nerovnosti**, tj.

$$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c), \quad (a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c).$$

Pro každé $a, b, c \in L$ splňující $a \leq c$ platí tzv. **modulární nerovnost**, tj.

$$a \vee (b \wedge c) \leq (a \vee b) \wedge c.$$

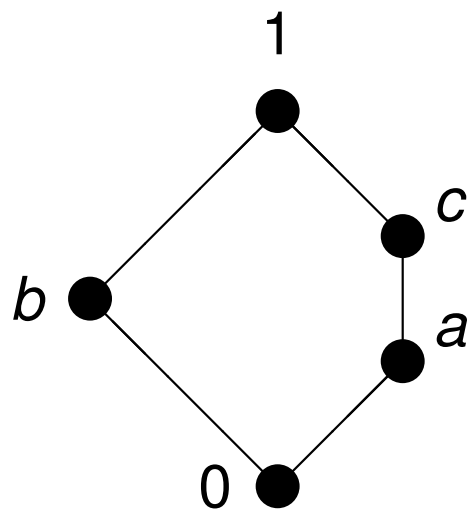
Důkaz. Jelikož $a \leq a \vee b$, $a \leq a \vee c$, je také $a \leq (a \vee b) \wedge (a \vee c)$. Dále $b \wedge c \leq b \leq a \vee b$, $b \wedge c \leq c \leq a \vee c$, tedy $b \wedge c \leq (a \vee b) \wedge (a \vee c)$. Odtud již dostaneme nerovnost

$$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c).$$

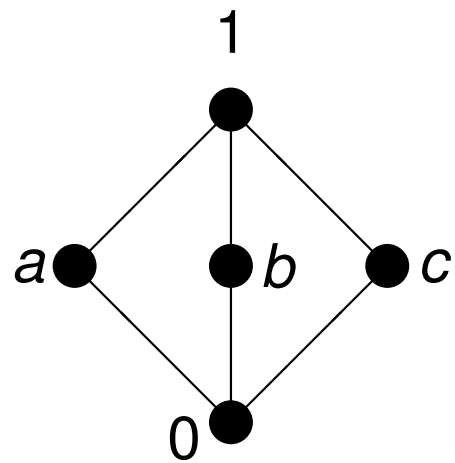
Duálně se dokáže druhá distributivní nerovnost.
Nechť nyní $a \leq c$. Jelikož $a \leq a \vee b$, dostaneme $a \leq (a \vee b) \wedge c$.
Podobně $b \wedge c \leq b \leq a \vee b$, $b \wedge c \leq c$ implikují $b \wedge c \leq (a \vee b) \wedge c$, tedy dohromady

$$a \vee (b \wedge c) \leq (a \vee b) \wedge c.$$

Poznámka. Obrácené nerovnosti obecně ve svazu neplatí. Je-li např. $L = N_5$ (viz Obr. 6), tzv. **pentagon**, pak $a \leq c$, ale $a \vee (b \wedge c) = a \vee 0 = a$, prvek a však není větší než prvek $c = (a \vee b) \wedge c$, tedy nerovnost obrácená k modulární nerovnosti v tomto svazu neplatí. Je-li $L = M_3$ (viz Obr. 7), tzv. **diamant**, pak $a \vee (b \wedge c) = a$ není větší než $1 = (a \vee b) \wedge (a \vee c)$, dále $(a \wedge b) \vee (a \wedge c) = 0$ není větší než $a = a \wedge (b \vee c)$, tedy ani jedna z nerovností obrácených k distributivním nerovnostem v tomto svazu neplatí.



Obr. 6



Obr. 7

Definice

Svaz L se nazývá **distributivní**, jestliže pro každé $a, b, c \in L$ platí

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c). \tag{D}$$

Svaz L se nazývá **modulární**, jestliže pro každé $a, b, c \in L$ splňující $a \leq c$ platí

$$a \vee (b \wedge c) = (a \vee b) \wedge c. \tag{M}$$

Věta

Svaz L je distributivní, právě když pro každé $a, b, c \in L$ platí rovnost duální k rovnosti (D), tj.

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

Důkaz. Nechť L je distributivní. Pak platí:
$(a \vee b) \wedge (a \vee c) = ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) = a \vee ((a \wedge c) \vee (b \wedge c)) =$
$= (a \vee (a \wedge c)) \vee (b \wedge c) = a \vee (b \wedge c)$.
Obrácené tvrzení lze dokázat duálně. □

Věta

Každý distributivní svaz je modulární.

Důkaz. Nechť L je distributivní, $a, b, c \in L$ a platí $a \leq c$. Pak

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c.$$

□

Poznámka. Každý podsvaz a každý homomorfní obraz distributivního svazu je distributivní svaz.

Příklady distributivních (a modulárních) svazů

(1) Každý řetězec je distributivní svaz.

(2) Nechť $M \neq \emptyset$, pak $(Exp\ M; \cup, \cap)$ je distributivní svaz.

(3) Svaz všech podgrup cyklické grupy je distributivní.

ad důkaz (3). Každá podgrupa cyklické grupy je normální, tedy pro dvě podgrupy A, B cyklické grupy $(G, \circ)$ platí $A \wedge B = A \cap B$, $A \vee B = A \circ B$. Stačí ověřit platnost inkluze $A \cap (B \circ C) \subseteq (A \cap B) \circ (A \cap C)$. □

Příklady modulárních svazů, které nejsou distributivní

(a) Svaz všech normálních podgrup libovolné grupy $(G, \circ)$ je modulární.

(b) Množina všech ideálů okruhu R tvoří modulární svaz.

Důkaz (a). Nechť A, B, C jsou normální podgrupy grupy $(G, \circ)$ a nechť $A \subseteq C$. (Zřejmě $A \wedge B = A \cap B$, $A \vee B = A \circ B$.) Stačí ověřit, že $(A \circ B) \cap C \subseteq A \circ (B \cap C)$. Nechť $a \in (A \circ B) \cap C$. Pak $a \in C$ a existují $d \in A$, $b \in B$ tak, že $a = d \circ b$. Tedy $d \in A \subseteq C$, ale C je podgrupa, tedy $d^{-1} \in C$, tj. $b = d^{-1} \circ a \in C$. Tedy $b \in B \cap C$, tj. $a = d \circ b \in A \circ (B \cap C)$. □

Důkaz (b). Zřejmě pro dva ideály I, J okruhu R je $I \cap J = \inf(I, J)$ vzhledem k uspořádání inkluzí, a dále $I + J = \{i + j;\ i \in I, j \in J\}$ je nejmenší ideál okruhu R, obsahující současně I i J, tedy $I + J$ je $\sup(I, J)$. Tedy množina všech ideálů je svaz, kde $\vee = +$, $\wedge = \cap$. Nechť I, J, K jsou ideály okruhu R takové, že $I \subseteq K$, a nechť $k \in (I + J) \cap K$. Pak $k \in K$, $k = i + j$, kde $i \in I$, $j \in J$. Ale $I \subseteq K$, tedy $i \in K$, a také $j = k - i \in K$, tedy $j \in J \cap K$. Odtud $k = i + j \in I + (J \cap K)$. Dokázali jsme inkluzi $(I + J) \cap K \subseteq I + (J \cap K)$. Jelikož obrácená inkluze platí vždy, je svaz všech ideálů okruhu R modulární. □

Věta

Svaz L je modulární, právě když pro každé $a, b, c \in L$ platí

$$a \vee (b \wedge (a \vee c)) = (a \vee b) \wedge (a \vee c).$$

Důkaz. Nechť L je modulární. Jelikož $a \leq a \vee c = c'$, platí dle (M)

$$a \vee (b \wedge (a \vee c)) = a \vee (b \wedge c') = (a \vee b) \wedge c' = (a \vee b) \wedge (a \vee c).$$

Obráceně, nechť pro libovolné $a, b, c \in L$ platí identita $a \vee (b \wedge (a \vee c)) = (a \vee b) \wedge (a \vee c)$ a nechť $a \leq c$. Pak $a \vee c = c$, a tato identita přechází ihned v axiom (M). □

Poznámka. Tedy i modulární svazy lze charakterizovat pouze identitami. Nyní však ukážeme, že jak distributivní, tak i modulární svazy lze charakterizovat pomocí tzv. **zakázaných podsvazů**.

Věta

Svaz L je modulární, právě když neobsahuje podsvaz izomorfní s N_5. Svaz L je distributivní, právě když neobsahuje podsvaz izomorfní s N_5 nebo M_3 (viz Obr. 6 a Obr. 7).

Důkaz. Na přednášce.

Důsledek

Svaz L je modulární tehdy a jen tehdy, když pro každé $x, y, z \in L$, $x \leq y$ platí:

$$\text{jestliže } x \wedge z = y \wedge z \text{ a } x \vee z = y \vee z, \text{ pak } x = y. \qquad (\star)$$

Svaz L je distributivní tehdy a jen tehdy, když pro každé $x, y, z \in L$ platí $(\star)$.

Důkaz. Je-li L modulární, $x, y, z \in L$ a neplatí $(\star)$, pak $\{x \wedge y \wedge z, x, y, z, x \vee y \vee z\}$ tvoří N_5 – spor. Jestliže L není modulární, pak obsahuje podsvaz izomorfní s N_5, jehož prvky nesplňují $(\star)$. Je-li L distributivní, $x, y, z \in L$ a neplatí $(\star)$, pak $\{x \wedge y \wedge z, x, y, z, x \vee y \vee z\}$ tvoří N_5 nebo M_3, jehož prvky však nesplňují $(\star)$, jak se lze snadno přesvědčit. □

Věta

Nechť L je modulární svaz. Nechť $a, b \in L$. Pak intervaly $[a, a \vee b]$, $[a \wedge b, b]$ jsou izomorfní podsvazy.

Důkaz. Definujme zobrazení $f : [a, a \vee b] \to [a \wedge b, b]$ předpisem $f(x) = x \wedge b$. Pak pro každé $y \in [a \wedge b, b]$ je $a \leq a \vee y \leq a \vee b$, tj. $a \vee y \in [a, a \vee b]$, přičemž dle (M) platí

$$f(a \vee y) = (y \vee a) \wedge b = y \vee (a \wedge b) = y.$$

Tedy f je surjekce. Nechť $x, x' \in [a, a \vee b]$. Jestliže $f(x) = f(x')$, pak $x \wedge b = x' \wedge b$, tedy dle (M) dostaneme

$$x = (a \vee b) \wedge x = a \vee (b \wedge x) = a \vee (b \wedge x') = (a \vee b) \wedge x' = x',$$

tedy f je injekce. Platí

$$f(x \wedge x') = x \wedge x' \wedge b = (x \wedge b) \wedge (x' \wedge b) = f(x) \wedge f(x').$$

Dále, jelikož $x \wedge b \leq b$, $a \leq x$, $a \leq x' \leq a \vee b$, dostaneme opakovaným použitím modulární identity (M):
$f(x) \vee f(x') = (x \wedge b) \vee (x' \wedge b) = ((x \wedge b) \vee x') \wedge b = ((x \wedge b) \vee a \vee x') \wedge b =$
$(((a \vee b) \wedge x) \vee x') \wedge b = (x' \vee x) \wedge (a \vee b) \wedge b = (x \vee x') \wedge b = f(x \vee x')$.
Tedy f je bijektivní homomorfismus, tj. izomorfismus. □

Definice

Nechť L je svaz s 0 a 1. Prvek $b \in L$ se nazývá **komplement** prvku $a \in L$, jestliže $a \vee b = 1$, $a \wedge b = 0$. Svaz L s 0 a 1 se nazývá **komplementární**, má-li každý prvek alespoň jeden komplement.
Nechť L je svaz, $a, b \in L$, $a \leq b$. Nechť $c \in [a, b]$. Prvek $d \in [a, b]$ se nazývá **relativní komplement** prvku c v intervalu $[a, b]$, jestliže platí $c \vee d = b$, $c \wedge d = a$. Svaz L se nazývá **relativně komplementární**, má-li každý prvek $c \in [a, b]$ pro libovolné $a, b \in L$, $a \leq b$, alespoň jeden relativní komplement v $[a, b]$.

Je-li tedy L svaz s 0 a 1 relativně komplementární, je i komplementární, neboť $L = [0, 1]$ a komplement prvku $a \in L$ je tudíž relativní komplement prvku a v intervalu [0,1]. Existují však relativně komplementární svazy, které nemají 0 resp. 1.

Příklady na komplementaritu

(1) Nechť L je svaz s 0 a 1. Pak 0 je komplementem prvku 1, a obráceně 1 je komplementem prvku 0.

(2) Je-li ve svazu L prvek a komplementem prvku b, pak b je komplementem a; říkáme tedy, že a, b jsou (vzájemně) **komplementární**.

(3) Nechť C_n je n-prvkový řetězec, tj. C_n obsahuje prvky $0 < a_1 < a_2 < \cdots < a_{n-2} < 1$. Pak $0, 1$ jsou jediné prvky svazu C_n, které mají komplement.

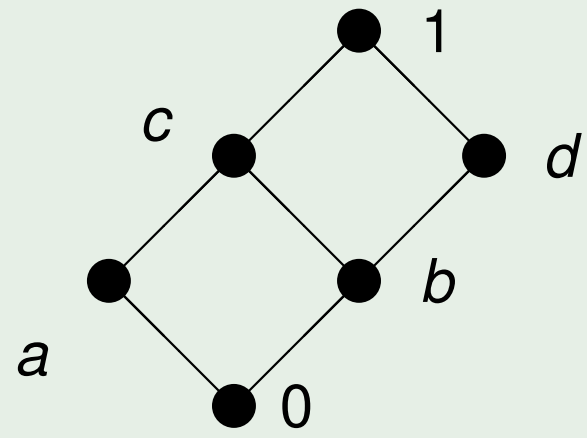
(4) Ve svazu L na Obr. 5 má každý prvek právě jeden komplement.

(5) Ve svazu N_5 na Obr. 6 má prvek b dva komplementy, a to prvky a, c; prvek c má jediný komplement b; prvek a má rovněž jediný komplement b.

(6) Ve svazu M_3 na Obr. 7 má a dva komplementy b, c; prvek b má dva komplementy a, c; prvek c má dva komplementy a, b.

Příklad

Ve svazu na Obr. 8 jsou a, d komplementární, $0, 1$ jsou komplementární, ale prvky b, c nemají komplementy.



Obr. 8

O vztazích mezi komplementy a relativními komplementy, a o podmínce pro jednoznačnou komplementaci, vypovídají následující věty.

Věta

Nechť L je distributivní svaz s 0 a 1. Pak každý prvek $a \in L$ má nejvýše jeden komplement.

Důkaz. Nechť $b, c \in L$ jsou komplementy prvku $a \in L$. Pak

$$b = b \wedge 1 = b \wedge (a \vee c) = (b \wedge a) \vee (b \wedge c) = 0 \vee (b \wedge c) = b \wedge c,$$

$$c = c \wedge 1 = c \wedge (a \vee b) = (c \wedge a) \vee (c \wedge b) = 0 \vee (c \wedge b) = b \wedge c,$$

tedy $b = c$. □

Definice

Svaz L s 0 a 1 se nazývá **jednoznačně komplementární**, má-li každý prvek $a \in L$ právě jeden komplement.

V jednoznačně komplementárním svazu budeme komplement prvku x označovat symbolem x'.
Zřejmě tedy svaz L na Obr. 5 je jednoznačně komplementární.

Důsledek

Každý komplementární distributivní svaz je jednoznačně komplementární.

Poznámka. Naskýtá se otázka, zda lze tento důsledek obrátit, tj. zda platí tvrzení, že každý jednoznačně komplementární svaz je distributivní. Toto obrácené tvrzení obecně neplatí, což je ale obtížné dokázat; takový svaz totiž není konečný a jeho konstrukce je složitá. Pro konečné svazy však lze dokázat obrácené tvrzení. Zaveďme následující pojmy:

Definice

Prvek a svazu L s 0 se nazývá **atom**, jestliže $0 < a$, a pro každé $x \in L$ splňující $0 < x \leq a$ platí $x = a$. Jinými slovy, atom je prvek, který kryje 0. Svaz L s 0 se nazývá **atomický**, jestliže pro každý prvek $b \in L$, $b \neq 0$ existuje atom $a \in L$ tak, že $a \leq b$.

Věta

Každý jednoznačně komplementární atomický svaz je distributivní.

Důkaz. Nechť L je jednoznačně komplementární svaz. Označme A množinu všech atomů v L, a pro $x \in L$ označme $A(x)$ množinu všech atomů, které jsou $\leq x$. Snadno nahlédneme, že $x \leq y \Rightarrow A(x) \subseteq A(y)$. Předpokládejme, že $x \neq y$, avšak $A(x) = A(y)$. Nechť x' je komplement (jednoznačný) prvku x. Pak bude platit

$$A(0) = \emptyset = A(x) \cap A(x'),$$

$$A(1) = A = A(x) \cup A(x').$$

Je-li tedy $A(x) = A(y)$, plyne odtud, že také x' je komplement k y, tj. $x' = y'$. Avšak $(x')' = x$, $(y')' = y$, tedy $x' = y' \Rightarrow x = y$, což je spor. Je tedy pro $x \neq y$ také $A(x) \neq A(y)$. Nechť $f : L \to A$ takové, že $f(x) = A(x)$. Pak, jak bylo výše ukázáno, f zachovává uspořádání a je bijekcí, tj. f je izomorfismus, neboli

$$f(x \vee y) = A(x) \cup A(y),$$

$$f(x \wedge y) = A(x) \cap A(y).$$

Tedy f je izomorfismus $(L; \vee, \wedge)$ na svaz $(ExpA, \cup, \cap)$, který je distributivní.

Důsledek

Každý konečný jednoznačně komplementární svaz je distributivní.

Důkaz. Je-li L konečný svaz, $0 < x \in L$, pak je buď x atom, nebo existuje jen konečně mnoho prvků $z_1, \ldots, z_n$ tak, že $0 \prec z_1 \prec z_2 \prec \cdots \prec z_n \prec x$. Pak z_1 je atom. Tedy L je atomický a důsledek plyne z předchozí věty. □

Definice

Nechť L je jednoznačně komplementární svaz. Řekneme, že v L platí **De Morganovy zákony**, jestliže pro každé $x, y \in L$:

$$\begin{aligned} (x \vee y)' &= x' \wedge y', \\ (x \wedge y)' &= x' \vee y'. \end{aligned}$$

Věta

Nechť L je jednoznačně komplementární svaz. Pak je ekvivalentní

(a) pro každé $x, y \in L$ platí: $x \leq y \Rightarrow x' \geq y'$

(b) v L platí De Morganovy zákony.

Důkaz. (a) $\Rightarrow$ (b): Nechť $x, y \in L$. Pak dle (a) platí:

$$x \leq x \vee y \Rightarrow x' \geq (x \vee y)'$$

$$y \leq x \vee y \Rightarrow y' \geq (x \vee y)',$$

tedy $x' \wedge y' \geq (x \vee y)'$. Dále

$$\left.\begin{array}{l} x' \geq x' \wedge y' \Rightarrow x = (x')' \leq (x' \wedge y')' \\ y' \geq x' \wedge y' \Rightarrow y = (y')' \leq (x' \wedge y')' \end{array}\right\} \Rightarrow x \vee y \leq (x' \wedge y')',$$

což implikuje $(x \vee y)' \geq x' \wedge y'$. Dohromady tedy $x' \wedge y' = (x \vee y)'$. Duálně se dokáže druhý De Morganův zákon.
(b) $\Rightarrow$ (a): Nechť $x \leq y$. Pak $y = x \vee y$, dle De Morganova zákona platí $y' = (x \vee y)' = x' \wedge y'$, tedy $y' \leq x'$. □

Definice

Komplementární distributivní svaz nazveme **booleovský**.

Poznámka. Každý booleovský svaz je jednoznačně komplementární. A každý konečný jednoznačně komplementární svaz booleovský.

Věta

V každém booleovském svazu platí De Morganovy zákony.

Důkaz. Nechť L je booleovský svaz, $a, b \in L$, $a \leq b$. Pak

$$a \wedge b' = (a \wedge b) \wedge b' = a \wedge (b \wedge b') = a \wedge 0 = 0,$$

tedy

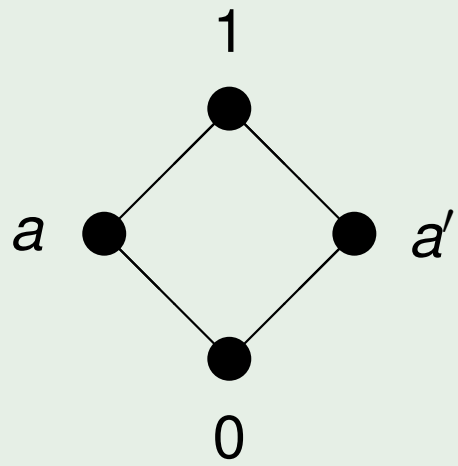
$$a' = 0 \vee a' = (a \wedge b') \vee a' = (a \vee a') \wedge (b' \vee a') = 1 \wedge (b' \vee a') = b' \vee a',$$

tj. $a' \geq b'$. Odkud, dle předchozí věty, platí ve svazu L De Morganovy zákony. □

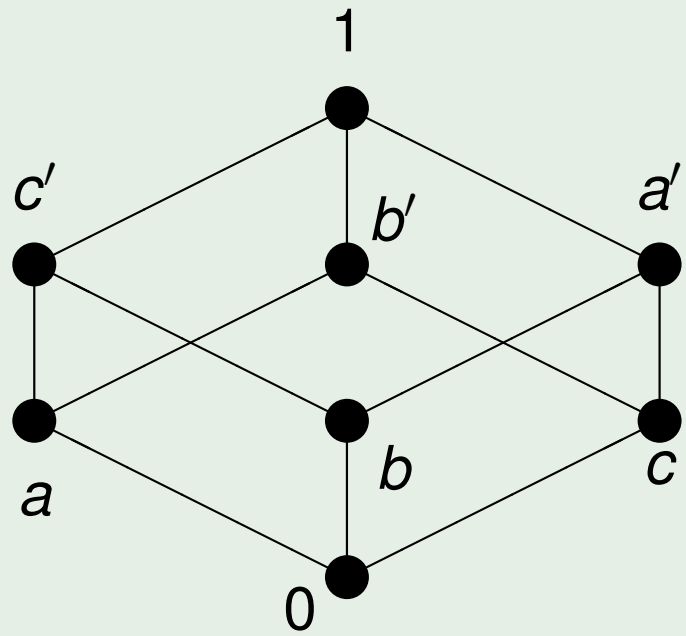
Příklady booleovských svazů

(1) Svaz $(Exp\, M, \cup, \cap)$ pro $M \neq \emptyset$, kde pro každou $X \subseteq M$ je $X' = M \setminus X$.

(2) Svazy na Obr. 9 a Obr. 10.



Obr. 9



Obr. 10

Nyní ukážeme souvislost komplementarity s relativní komplementaritou pro modulární svazy.

Věta

Nechť L je komplementární modulární svaz. Pak L je relativně komplementární.

Důkaz. Nechť $x, y \in L$, $x \leq y$, $a \in [x, y]$. Nechť b je komplement prvku a v L. Položme

$$c = (y \wedge b) \vee x.$$

Z modularity a ze vztahu $x \leq y$ plyne $c = y \wedge (b \vee x)$, a dále

$$c \wedge a = [(x \vee b) \wedge y] \wedge a = (x \vee b) \wedge (y \wedge a) = (x \vee b) \wedge a = x \vee (b \wedge a) = x,$$

$$c \vee a = [(y \wedge b) \vee x] \vee a = (y \wedge b) \vee (x \vee a) = (y \wedge b) \vee a = y \wedge (b \vee a) = y,$$

tedy c je relativní komplement prvku a v intervalu $[x, y]$. □

Důsledek

Každý booleovský svaz je relativně komplementární.

Nyní ukážeme, že pomocí relativních komplementů lze dokonce charakterizovat distributivitu a modularitu.

Věta

Svaz L je distributivní tehdy a jen tehdy, když každý prvek $a \in L$ má v libovolném intervalu nejvýše jeden relativní komplement.
Svaz L je modulární tehdy a jen tehdy, jestliže žádný prvek $a \in L$ nemá v libovolném intervalu dva srovnatelné relativní komplementy.

Důkaz. Plyne ihned z věty o zakázaných podsvazech, neboť $a \in L$ má v některém $[x, y] \subseteq L$ dva relativní komplementy b, c, $b \neq c$, právě když $\{x, a, b, c, y\}$ tvoří podsvaz M_3; dále $b \in L$ má v $[x, y] \subseteq L$ dva srovnatelné relativní komplementy $a \leq c$, právě když $\{x, a, b, c, y\}$ tvoří N_5 (viz Obr. 6 a Obr. 7). □

Obsah

Již jsme definovali kongruenci na svazu a zavedli jsme pojem svazového ideálu. Zajímáme se, zda existuje analogie vzájemného vztahu mezi ideálem a kongruencí, jaký je znám pro okruhy.

Definice

Nechť L je svaz s 0, nechť θ je kongruence na L. Množinu $K_\theta = \{x \in L; \langle x, 0\rangle \in \theta\}$ nazveme **jádro kongruence** θ.

Věta

Nechť L je svaz s 0 a θ je kongruence na L. Pak jádro K_θ je ideál svazu L.

Důkaz. Nechť $a, b \in K_\theta$. Pak $\langle a, 0\rangle \in \theta$, $\langle b, 0\rangle \in \theta$, tedy $\langle a \vee b, 0\rangle = \langle a \vee b, 0 \vee 0\rangle \in \theta$. Odtud $a \vee b \in K_\theta$. Nechť $a \in K_\theta$, $x \in L$. Pak $\langle a, 0\rangle \in \theta$ a z reflexivity plyne $\langle x, x\rangle \in \theta$, tedy $\langle a \wedge x, 0\rangle = \langle a \wedge x, 0 \wedge x\rangle \in \theta$, tj. $a \wedge x \in K_\theta$. Tedy K_θ je ideál svazu L. □

Poznámka.

(1) Je-li I ideál svazu L, $a \in I$ a $x \in L$, přičemž $x \leq a$, pak $x = a \wedge x \in I$.

(2) Je-li L svaz s 0 a $\theta = \omega$, pak $K_\theta = \{0\}$. Je-li $\theta = L \times L$, pak $K_\theta = L$.

Věta

Nechť L je svaz s 0. Pak je ekvivalentní:

(1) Každý ideál svazu L je jádrem alespoň jedné kongruence na L.

(2) L je distributivní.

Důkaz. Na přednášce.

Poznámka. Na rozdíl od okruhů, v distributivním svazu nemusí být ideál jádrem jediné kongruence.

Nyní budeme řešit problém, kdy je každý ideál jádrem nejvýše jedné kongruence.

Věta

Nechť θ je kongruence na svazu L a $x, y \in L$. Pak $\langle x, y \rangle \in \theta$, právě když $\langle x \vee y, x \wedge y \rangle \in \theta$.

Důkaz. Nechť $\langle x, y \rangle \in \theta$. Pak ze symetrie relace θ je také $\langle y, x \rangle \in \theta$ a z reflexivity θ je $\langle x, x \rangle \in \theta$ a $\langle y, y \rangle \in \theta$. Odkud

$$\left.\begin{array}{l} \langle x, x \wedge y \rangle = \langle x \wedge x, x \wedge y \rangle \in \theta \\ \langle y, x \wedge y \rangle = \langle y \wedge y, y \wedge x \rangle \in \theta \end{array}\right\} \overset{\vee}{\Rightarrow} \langle x \vee y, x \wedge y \rangle \in \theta.$$

Obráceně, nechť $\langle x \vee y, x \wedge y \rangle \in \theta$. Pak

$$\langle x, x \wedge y \rangle = \langle x \wedge (x \vee y), x \wedge (x \wedge y) \rangle \in \theta,$$

$$\langle y, x \wedge y \rangle = \langle y \wedge (x \vee y), y \wedge (x \wedge y) \rangle \in \theta,$$

odkud ze symetrie a tranzitivity relace θ plyne $\langle x, y \rangle \in \theta$. □

Věta

Nechť L je relativně komplementární svaz s 0. Pak každý ideál svazu L je jádrem nejvýše jedné kongruence.

Důkaz. Na přednášce.

Následující věta charakterizuje svazy, pro které je analogie vztahu ideálů a kongruencí pro okruhy úplná.

Věta

Nechť L je svaz s 0. Pak je ekvivalentní:

(1) Každý ideál svazu L je jádrem právě jedné kongruence na L.

(2) Svaz L je relativně komplementární distributivní svaz.

Důkaz. Na přednášce.

V závěru této části zavedeme významné druhy svazových ideálů.

Definice

Ideál I svazu L nazveme

- **prvoideál**, jestliže pro každé $a, b \in L$ platí implikace:

$$a \wedge b \in I \Rightarrow a \in I \text{ nebo } b \in I.$$

- **maximální**, jestliže $I \neq L$, a je-li J ideál svazu L, $J \neq I$ a platí-li $I \subseteq J \subseteq L$, pak $J = L$.
- **vlastní**, je-li $I \neq L$.

Lemma

Nechť L je svaz s 0 a 1, I je vlastní ideál svazu L, $a \in L$. Nechť b je komplement prvku a. Jestliže $a \in I$, pak $b \notin I$.

Důkaz. Jestliže $a \in I$ a také $b \in I$, pak $a \vee b \in I$. Ale b je komplement prvku a, tedy $a \vee b = 1$, tj. $1 \in I$. Zřejmě odtud plyne $I(1) \subseteq I$. Avšak $I(1) = L$, tedy $I = L$, spor. □

Zavedeme další pojem, duální k pojmu ideál:

Definice

Nechť L je svaz, $\emptyset \neq F \subseteq L$. Množinu F nazveme **filtr svazu** L, jestliže pro každé $a, b \in F$ a libovolné $x \in L$ platí: $a \wedge b \in F$, $a \vee x \in F$.

Analogicky jako pro ideály lze dokázat, že množina všech filtrů svazu L spolu s $\emptyset$ tvoří úplný svaz.

Lemma

Nechť L je svaz, I jeho ideál. Pak I je prvoideál právě když $L \setminus I$ je filtr.

Důkaz. Na přednášce. □

Věta

Nechť L je distributivní svaz.

- Pak každý jeho maximální ideál je prvoideál.
- Nechť I je ideál a F filtr svazu L, a platí $I \cap F = \emptyset$. Pak existuje prvoideál P tak, že $I \subseteq P$ a $P \cap F = \emptyset$.
- Nechť $x, y \in L$, $x \not\geq y$. Pak existuje prvoideál P obsahující x a neobsahující y.

Důkaz. Na přednášce.

Obsah

Definice.

Nechť $A \neq \emptyset$. **Booleovou algebrou** nazveme šestici $(A; \vee, \wedge, ', 0, 1)$ takovou, že $0 \neq 1$ a

(i) $(A; \vee, \wedge)$ je distributivní svaz,

(ii) 0 resp. 1 je nejmenší resp. největší prvek tohoto svazu,

(iii) symbol $'$ označuje operaci komplementace, tj. pro každé $a \in A$ je a' komplement prvku a ve svazu $(A; \vee, \wedge)$.

Nechť A je booleovský svaz. Je-li 0 resp. 1 nejmenší resp. největší prvek tohoto svazu a' označuje komplementaci v A, pak $(A; \vee, \wedge, ', 0, 1)$ je Booleova algebra. Na Obr. 9 resp. 10 je diagram čtyřprvkové resp. osmiprvkové Booleovy algebry.

Příklady

(1) Pro každou $M \neq \emptyset$ je $(ExpM; \cup, \cap, \setminus, \emptyset, M)$ Booleova algebra, přičemž symbol $\setminus$ označuje pro $X \subseteq M$ podmnožinu $M \setminus X$, tj. komplement v množinovém svazu.

(2) Nechť $P(x)$ je množina všech dělitelů přirozeného čísla x, pak $(P(30); n, D, \frac{30}{y}, 1, 30)$ je Booleova algebra (viz Obr. 5), kde pro $y \in P(30)$ označuje $\frac{30}{y}$ aritmetický podíl.

(3) Každý dvouprvkový svaz (tj. dvouprvkový řetězec) $(\{a, b\}, \vee, \wedge)$ lze chápat jako Booleovu algebru. Je-li $a < b$, pak tato Booleova algebra je $(\{a, b\}; \vee, \wedge, ', a, b)$, kde $a' = b$, $b' = a$, $x \vee y = \max(x, y)$, $x \wedge y = \min(x, y)$.

Definice

Nechť $\mathscr{A} = (A; \vee, \wedge, ', 0, 1)$ je Booleova algebra, $\emptyset \neq B \subseteq A$. Jestliže pro každé $a, b \in B$ platí:

(i) $a \vee b \in B$, $a \wedge b \in B$

(ii) $a' \in B$

(iii) $0 \in B$, $1 \in B$,

pak se B nazývá **podalgebra Booleovy algebry** $\mathscr{A}$.

Nechť $\mathscr{C} = (C; \vee, \wedge, ', 0, 1)$ je také Booleova algebra a $h : A \to C$ je zobrazení splňující $h(a \vee b) = h(a) \vee h(b)$, $h(a \wedge b) = h(a) \wedge h(b)$, $h(a') = h(a)'$, $h(0) = 0$, $h(1) = 1$. Pak h se nazývá **homomorfismus Booleových algeber**. Je-li h navíc bijekcí, nazývá se **izmorfismus Booleových algeber**.

Relace θ na Booleově algebře $\mathscr{A}$ je **kongruence**, je-li kongruencí na svazu $(A; \vee, \wedge)$, tj. je-li ekvivalence, a pro každé $a, b, c, d \in \mathscr{A}$ platí:
$(\langle a, b \rangle \in \theta, \langle c, d \rangle \in \theta) \Rightarrow (\langle a \vee c, b \vee d \rangle \in \theta, \langle a \wedge c, b \wedge d \rangle \in \theta)$.

Poznámka. Nechť $\mathscr{A} = (L; \vee, \wedge, ', 0, 1)$ je Booleova algebra, a nechť θ je kongruence na svazu $(L; \vee, \wedge)$. Pak θ je kongruence na Booleově algebře $\mathscr{A}$. Nechť platí $\langle a, b\rangle \in \theta$. Pak z reflexivity θ plyne $\langle a', a'\rangle \in \theta$, $\langle b', b'\rangle \in \theta$, a tedy také

$$\langle a', a' \wedge b'\rangle = \langle a' \wedge 1, 0 \vee (a' \wedge b')\rangle = \langle a' \wedge (b \vee b'), a' \wedge (a \vee b')\rangle \in \theta$$

$$\langle b', a' \wedge b'\rangle = \langle b' \wedge 1, 0 \vee (b' \wedge a')\rangle = \langle b' \wedge (a \vee a'), b' \wedge (b \vee a')\rangle \in \theta,$$

a ze symetrie a tranzitivity relace θ plyne $\langle a', b'\rangle \in \theta$. Neboli, každá kongruence svazu $(L; \wedge, \vee)$ má substituční podmínku i vzhledem k operaci komplementace. Proto nezavádíme nový pojem „booleovské kongruence“.

Poznámka. Nechť L je booleovský svaz, nechť $\mathscr{A} = (L; \vee, \wedge, ', 0, 1)$ je odpovídající Booleova algebra. Pak každá podalgebra Booleovy algebry $\mathscr{A}$ je zřejmě podsvazem svazu L, avšak obrácené tvrzení neplatí. Je-li např. $L = \{0, a, a', 1\}$ svaz (viz Obr. 9), pak $(L; \vee, \wedge, ', 0, 1)$ je Booleova algebra. Pak $S = \{0, a, 1\}$ je podsvaz svazu L, avšak není podalgebrou Booleovy algebry $(L; \vee, \wedge, ', 0, 1)$, neboť $a' \notin S$. Také $A = \{0, a\}$ je podsvaz svazu L, ovšem není podalgebrou této Booleovy algebry, neboť $1 \notin A$.

Dále zobrazení $h : L \to L$ dané předpisem $h(1) = a$, $h(a') = 0$, $h(a) = a$, $h(0) = 0$ je svazový homomorfismus, ale není homomorfismem Booleových algeber, jelikož $h(1) \neq 1$, $h(a') = 0 \neq a' = h(a)'$.

Věta

Každá konečná Booleova algebra $(L;\vee,\wedge,',0,1)$ je izomorfní s Booleovou algebrou $(ExpM;\cup,\cap,\setminus,\emptyset,M)$, kde M je množina všech atomů svazu $(L;\vee,\wedge)$.

Důkaz. Nechť $\mathscr{A}=(L;\vee,\wedge,',0,1)$ je konečná Booleova algebra a nechť M je množina atomů svazu $(L;\vee,\wedge)$. Pro každý prvek $a\in L$ označme $A(a)=\{p\in M;\, p\leq a\}$. Zřejmě platí $A(a\vee b)\supseteq A(a)$, $A(a\vee b)\supseteq A(b)$, tedy $A(a\vee b)\supseteq A(a)\cup A(b)$. Obráceně, nechť $c\in A(a\vee b)$. Pak $c=c\wedge(a\vee b)=(c\wedge a)\vee(c\wedge b)$. Jelikož c je atom, plyne odtud $c=c\wedge a$ nebo $c=c\wedge b$, tj. $c\leq a$ nebo $c\leq b$, odtud $c\in A(a)$ nebo $c\in A(b)$, a tedy $c\in A(a)\cup A(b)$. Dokázali jsme $A(a\vee b)=A(a)\cup A(b)$. Rovnost $A(a\wedge b)=A(a)\cap A(b)$ vyplývá z faktu, že $c\leq a\wedge b$ právě když $c\leq a$ a současně $c\leq b$. Tedy zobrazení $L\to ExpM$ dané předpisem $a\mapsto A(a)$ je homomorfismus. Jestliže $a,b\in L$ a platí $A(a)=A(b)$, pak vzhledem ke konečnosti množin $A(a)$, $A(b)$ platí $a=\bigvee A(a)$, $b=\bigvee A(b)$, tedy $a=\bigvee A(a)=\bigvee A(b)=b$, tj. zobrazení $a\mapsto A(a)$ je injektivní homomorfismus. Zbývá dokázat, že toto zobrazení je surjekce. Nechť $B\subseteq M$. Jelikož B je konečná, existuje $b=\bigvee B$, tedy $B=A(b)$, neboli $b\mapsto B$. Dokázali jsme, že toto zobrazení je hledaný izomorfismus. □

Důsledek.

(1) Nechť $\mathscr{A}$ je konečná Booleova algebra. Pak existuje přirozené číslo n tak, že $\mathscr{A}$ má 2^n prvků.

(2) Jsou-li $\mathscr{A}$, $\mathscr{B}$ dvě konečné Booleovy algebry se stejným počtem prvků, pak jsou izomorfní.

Důkaz.

(1) Je-li $\mathscr{A}$ konečná, pak je dle předchozí věty izomorfní s $(ExpM; \cup, \cap, \setminus, ', \emptyset, M)$, kde M je množina atomů Booleovy algebry $\mathscr{A}$. Jelikož $\mathscr{A}$ je konečná, je i M konečná; nechť $|M| = n$. Pak $|ExpM| = 2^n$, tudíž i $\mathscr{A}$ má 2^n prvků.

(2) Mají-li konečné Booleovy algebry $\mathscr{A}$, $\mathscr{B}$ stejný počet prvků, např. 2^n, pak $\mathscr{A} \cong (ExpM; \cup, \cap, ', \emptyset, M)$, $\mathscr{B} \cong (ExpM; \cup, \cap, ', \emptyset, M)$, kde M je n-prvková množina, a tedy i $\mathscr{A} \cong \mathscr{B}$. □

Věta

Nechť $\mathscr{A}$ je konečná Booleova algebra, která má 2^n prvků. Pak $\mathscr{A}$ je izomorfní s Booleovou algebrou $\mathscr{B}$ všech n-tic $(a_1, \ldots, a_n)$, kde $a_i \in \{0, 1\}$, přičemž nulou je v $\mathscr{B}$ prvek $o = (0, \ldots, 0)$, jednotkou je prvek $j = (1, \ldots, 1)$, komplementem $a = (a_1, \ldots, a_n)$ je prvek $a' = (a'_1, \ldots, a'_n)$, kde $0' = 1$, $1' = 0$ a operace $\vee, \wedge$ jsou v $\mathscr{B}$ definovány takto:

$$(a_1, \ldots, a_n) \vee (b_1, \ldots, b_n) = (a_1 \vee b_1, \ldots, a_n \vee b_n),$$

$$(a_1, \ldots, a_n) \wedge (b_1, \ldots, b_n) = (a_1 \wedge b_1, \ldots, a_n \wedge b_n).$$

Důkaz. Nechť L je množina všech n-tic $(a_1, \ldots, a_n)$, jejichž prvky jsou 0 a 1. Zřejmě $|L| = 2^n$. Snadno ověříme, že $\mathscr{B} = (L; \vee, \wedge, ', o, j)$ je Booleova algebra. Jelikož $\mathscr{A}, \mathscr{B}$ mají stejný počet prvků, jsou dle předchozího důsledku izomorfní. □

Poznámka. Víme, že nejmenší Booleova algebra má právě dva prvky, a to 0 a 1, přičemž $0' = 1$, $1' = 0$, $0 \vee 0 = 0$, $1 \vee 0 = 0 \vee 1 = 1 \vee 1 = 1$, $0 \wedge 1 = 1 \wedge 0 = 0$. Tato Booleova algebra je izomorfní s Booleovou algebrou pravdivostních hodnot výrokové logiky, kde 1 je pravd. hodnota pravdivého výroku, 0 je pravd. hodnota nepravdivého výroku a operace $\vee$ resp. $\wedge$ lze interpretovat jako disjunkci resp. konjunkci, operaci $'$ jako negaci. Jsou-li $A_1, \ldots, A_n$ výroky, pro které chceme zjistit pravdivostní hodnotu některé logické funkce těchto výroků, pak, jak známe z výrokové logiky, interpretujeme jejich pravdivostní hodnoty pomocí m n-tic 0 a 1 (kde $m = 2^n$). Jelikož je množina všech těchto n-tic Booleovou algebrou (která má 2^n prvků), lze dle předchozí věty operace $\vee, \wedge$ interpretovat jako disjunkci a konjunkci (neboť jsou prováděny po souřadnicích a dle výše uvedeného lze tyto interpretovat v každé souřadnici jako disjunkci a konjunkci), komplement $'$ lze interpretovat jako negaci, tedy na logické operace s konečnou množinou výroků lze nahlížet jako na konečnou Booleovu algebru. To byla původní myšlenka, se kterou přišel v r. 1847 George Boole při výzkumu formalizace matematické logiky.

Věta

Nechť $\mathscr{A} = (L; \vee, \wedge, ', 0, 1)$ je Booleova algebra. Zaveďme operaci $\oplus$ na L takto:

$$x \oplus y = (x \wedge y') \vee (x' \wedge y).$$

Pak $(L; \oplus)$ je abelovská grupa.

K důkazu. Z definice je zřejmé, že operace $\oplus$ je komutativní. Rutinně se dá se ověřit asociativnost operace $\oplus$. Pro každé $x \in L$ je $x \oplus 0 = (x \wedge 0') \vee (x' \wedge 0) = x \wedge 1 = x$, tedy 0 je jednotkou v $(L; \oplus)$. Dále pro každé $x \in L$ je $x \oplus x = (x \wedge x') \vee (x' \wedge x) = 0 \vee 0 = 0$, odkud x je inverzní prvek k sobě samému. Tedy $(L; \oplus)$ je abelovská grupa. □

Poznámka. Je-li $\mathscr{A} = (L; \vee, \wedge, ', 0, 1)$ Booleova algebra, pak

(i) $(L; \vee, \wedge)$ distributivní svaz,

(ii) $(L; \oplus)$ abelovská grupa.

Booleovy algebry jsou tedy takové algebraické struktury, které sjednocují vlastnosti (distributivních) svazů a (abelovských) grup.
Nyní objasníme další zajímavý vztah Booleových algeber k okruhům.

Definice

Okruh $(R; +, \cdot)$ s alespoň dvěma prvky, jehož každý prvek je idempotentní (tj. pro každé $a \in R$ platí $a \cdot a = a$), se nazývá **booleovský**.

Věta

Každý booleovský okruh je komutativní a má charakteristiku 2.

Důkaz. Nechť $(R;+,\cdot)$ je booleovský okruh. Pak pro každé $x, y \in R$ platí $x+y = (x+y)(x+y) = x^2+xy+yx+y^2 = x+xy+yx+y$, tedy $xy+yx = 0$. Položme $x = y$ a dostaneme $0 = x^2+x^2 = x+x$, tedy R je charakteristiky 2. Dále, jestliže jsme dokázali $xy+yx = 0$ pro každé $x, y \in R$, pak

$$xy = xy+0 = xy+xy+yx = 0+yx = yx,$$

neboť R je charakteristiky 2, tedy R je komutativní. □

Příklad

Dvouprvkový booleovský okruh je okruh zbytkových tříd mod 2.

Věta

Nechť $\mathscr{A} = (L; \vee, \wedge, ', 0, 1)$ je Booleova algebra. Definujme

$$\begin{aligned} x \oplus y &= (x \wedge y') \vee (x' \wedge y), \\ x \cdot y &= x \wedge y. \end{aligned}$$

Pak $\mathscr{R} = (L; \oplus, \cdot)$ je booleovský okruh s jednotkou 1.

K důkazu. Víme, že $(L; \oplus)$ abelovská grupa. Operace $\cdot$ je zřejmě asociativní, neboť $\wedge$ je asociativní. Z distributivních zákonů pro operace $\vee, \wedge$ lze odvodit distributivní zákon $x \cdot (y \oplus z) = (x \cdot y) \oplus (x \cdot z)$. Tedy $\mathscr{R} = (L; \oplus, \cdot)$ je okruh. Jelikož pro každé $x \in L$ je $x \cdot x = x \wedge x = x$, je $\mathscr{R}$ booleovský okruh. Dále, $1 \cdot x = x \cdot 1 = x \wedge 1 = x$, tedy 1 je jednotkou v $\mathscr{R}$. □

Věta

Nechť $\mathscr{R} = (A; +, \cdot)$ je booleovský okruh s 1. Definujme $x \vee y = x + y + x \cdot y$, $x \wedge y = x \cdot y$, $x' = 1 + x$. Pak $\mathscr{A} = (A; \vee, \wedge, ', 0, 1)$, kde 0 je nulou okruhu $\mathscr{R}$, je Booleova algebra.

Důkaz. Z komutativity a asociativity operací $+, \cdot$ lze odvodit asociativitu a komutativitu operací $\vee, \wedge$. Dále,

$$x \vee (x \wedge y) = x + xy + x^2 y = x + xy + xy = x,$$

$$x \wedge (x \vee y) = x(x + y + xy) = x^2 + xy + x^2 y = x + xy + xy = x,$$

tedy $(A; \vee, \wedge)$ je svaz. Dále, $0 \vee x = 0 + x + 0 \cdot x = x$, $0 \wedge x = 0 \cdot x = 0$, $1 \vee x = 1 + x + 1 \cdot x = 1 + x + x = 1$, $1 \wedge x = 1 \cdot x = x$. Konečně

$$x \wedge x' = x(1 + x) = x + x^2 = x + x = 0,$$

$$x \vee x' = x + (1 + x) + x(1 + x) = x + 1 + x + 0 = 1,$$

tedy x' je komplement prvku x. Ověříme distributivitu svazu $(A; \vee, \wedge)$:

$$(x \wedge y) \vee (x \wedge z) = xy + xz + xyxz = xy + xz + xyz = x(y + z + yz) = x \wedge (y \vee z).$$

Tedy $(A; \vee, \wedge, ', 0, 1)$ je Booleova algebra. □

Věta

Nechť $(L; \vee, \wedge)$ je relativně komplementární distributivní svaz, nechť $a, b \in L$, $a < b$. Pak $I(a, b) = ([a, b]; \vee, \wedge, ^*, a, b)$ je Booleova algebra, kde symbol * označuje relativní komplement v intervalu $[a, b]$.

Důkaz. Nechť $(L; \vee, \wedge)$ je relativně komplementární distributivní svaz, $a < b$, $a, b \in L$. Uvažujme interval $[a, b]$. Pak $[a, b]$ je podsvaz svazu $(L; \vee, \wedge)$, přičemž a je nejmenší a b je největší prvek v $[a, b]$. Pro $x \in [a, b]$ označme x^* relativní komplement prvku x v intervalu $[a, b]$. Jelikož L je distributivní, je i $[a, b]$ distributivní svaz, tedy komplementace je jednoznačná. Tedy $([a, b]; \vee, \wedge)$ je booleovský svaz, tj. $I(a, b) = ([a, b]; \vee, \wedge, ^*, a, b)$ je Booleova algebra. □

Závěrem

Použitá literatura

1. Jiří Rachůnek: Grupy a okruhy. VUP Olomouc, 2005.
2. Ivan Chajda: Algebra III. VUP Olomouc, 1998.

Podpora

Tyto slidy vznikly za podpory projektu FRUP_2017_052: Tvorba a inovace výukových opor vybraných matematických předmětů katedry informatiky.