Poznámky - Algebra II

Petr Chmel, LS 2019/20

Definice 1 (Částečně uspořádaná množina, nejmenší, největší, minimální, maximální prvky, supremum, infimum)**.** Pro M množinu, $\leq$ relaci na M: $(M, \leq)$ je částečně uspořádaná množina, pokud $\leq$ je reflexivní, slabě antisymetrická a tranzitivní. TODO: prvky

Supremum/infimum množiny A je nejmenší/největší prvek množiny $\{m \in M : \forall a \in A : a \leq m\}/\{m \in M : \forall a \in A : a \geq m\}$.

Definice 2 (Svaz, úplný svaz)**.** Částečně uspořádaná množina $(M, \leq)$ js *svaz*, pokud v M existuje $\sup\{a, b\}, \inf\{a, b\}$ pro libovolné $a, b \in M$ a zároveň $M \neq \emptyset$. Pak píšeme „a spojení b“ jako $a \vee b = \sup\{a, b\}$ a „a průsek b“ jako $a \wedge b = \inf\{a, b\}$.

Navíc, pokud existuje $\sup A, \inf A$ pro všechny $A \subseteq M$, mluvíme o *úplném svazu*.

Definice 3 (Pokrytí, Hasseův diagram)**.** Buď $(M, \leq)$ částečně uspořádaná množina. Řekneme, že $a \in M$ pokrývá $b \in M$, psáno $b \prec a$, pokud $b \leq a \wedge b \neq a \wedge \forall c \in M : (b \leq c \wedge c \leq a) \Rightarrow (b = c \vee c = a)$.

Věta 1 (Vlastnosti svazu)**.** 1. Je-li $(M, \leq)$ svaz, pak $\forall a, b, c \in M$ platí:

S1 $a \vee b = b \vee a, a \wedge b = b \wedge a$

S2 $a \wedge a = a = a \vee a$

S3 $(a \vee b) \vee c = a \vee (b \vee c)$

S4 $a \vee (b \wedge a) = a = (a \vee b) \wedge a$ (*absorpční zákon*)

2. Nechť $M(\wedge, \vee)$ je algebra, kde $\wedge, \vee$ jsou binární operace splňující S1-S4. Definujeme na M binární relaci $\leq$: $a \leq b \overset{\text{def}}{\Leftrightarrow} b = a \vee b$. Pak platí: $a \leq b \Leftrightarrow a = a \wedge b$, $(M, \leq)$ je svaz, $\sup_{\leq}\{a, b\} = a \vee b, \inf_{\leq}\{a, b\} = a \wedge b$.

Důkaz. 1: S1, S2 zjevně z definice.

S3: ukážeme $\sup_{\leq}\{a, b, c\} = (a \vee b) \vee c$, zbytek plyne komutativitou z S1: Nechť $e \in M : a, b, c \leq e$. Pak $a \vee b \leq e$, a tedy i $(a \vee b) \vee c \leq e$, pro $e = \sup\{a, b, c\}$ máme také $e \geq (a \vee b) \vee c$, $\wedge$ analogicky.

S4: stačí jedna rovnost, druhá se ukáže duálně. Z $a \leq a, b \wedge a \leq a$ máme $a \vee (b \wedge a) \leq a$, navíc $a \leq a \vee (b \wedge a)$, protože $a \leq a \vee \gamma$ pro libovolné γ. Rovnost pak plyne ze slabé antisymetrie.

2: $\leq$ je uspořádání: z S2: $a = a \vee a \Rightarrow a \leq a$ a máme reflexivitu.

Nechť $a \leq b, b \leq c$, tedy $b = a \vee b, c = b \vee c$. Pak $c = (a \vee b) \vee c \overset{S3}{=} a \vee (b \vee c) = a \vee c$, tedy $a \vee c$ a máme tranzitivitu.

Pro $a \leq b, b \leq a$ máme $b = a \vee b \overset{S1}{=} b \vee a = a$ a máme slabou antisymetrii.

Ekvivalence uspořádání a průseku: ať $b = a \vee b$, pak $a \wedge b = a \wedge (a \vee b) = a \wedge (b \vee a) = a$. Duálně pro $a = a \wedge b$ a $b = a \vee b$.

$(M, \leq)$ je svaz: Vztah pro supremum: $a \vee b$ je horní závora pro $\{a, b\}$, pak $a \wedge (a \vee b) = a \wedge (b \vee a) = a$, tedy $a \leq a \vee b$. Dále $b \wedge (a \vee b) = b \Rightarrow b \leq a \vee b$. Nechť nyní $c \in M$ takový, že $a, b \leq c$, tedy $c = a \vee c = b \vee c$. Pak $c = a \vee (b \vee c) = (a \vee b) \vee c \Rightarrow a \vee b \leq c$. Infimum duálně. ⊞

Důsledek 1 (Pohledy na svaz)**.** Na svaz se můžeme dívat dvěma způsoby: jako na uspořádanou množinu se supremy a infimy pro $\{a, b\}$ nebo jako na algebru $M(\wedge, \vee)$ splňující (a)-(d).

Definice 4 (Monotónní zobrazení a homomorfismus svazů)**.** Ať $(A, \leq), (B, \leq)$ jsou svazy. Zobrazení $f\colon A \to B$ se nazývá

- *monotónní*, pokud $\forall x, y \in A : x \leq y \Rightarrow f(x) \leq f(y)$
- homomorfismus svazů, pokud f je homomorfismus algeber $A(\wedge, \vee)$ a $B(\wedge, \vee)$.

Definice 5 (Podsvaz)**.** Podsvazem svazu $(A, \leq)$ budeme rozumět každou podalgebru algebry $A(\wedge, \vee)$.

Tvrzení 1 (Homomorfismus svazů je monotónní)**.** Homomorfismus svazů je monotónní.

Důkaz. $x \leq y \Leftrightarrow y = x \vee y \Rightarrow f(y) = f(x \vee y) \overset{f \text{ homom.}}{=} f(x) \vee f(y) \leftrightarrow f(x) \leq f(y)$ ⊞

Věta 2 (Charakterizace isomorfismu svazů)**.** Bijekce $f : A \to B$ svazů $(A, \leq), (B, \leq)$ je isomorfismus, právě když f i f^{-1} jsou monotónní.

Důkaz. „⇒“: Plyne z monotonie homomorfismů.

„⇐“: Stačí ukázat, že f je homomorfismus, f^{-1} získáme otočením role A a B. Tedy $\forall x, y \in A : f(x \vee y) = f(x) \vee f(y), f(x \wedge y) = f(x) \wedge f(y)$.

Pro $\vee$: $x, y \leq x \vee y \overset{\text{iso}}{\Rightarrow} f(x), f(y) \leq f(x \vee y) \Rightarrow f(x) \vee f(y) \leq f(x \vee y)$.

Na druhou stranu: $f(x), f(y) \leq f(x) \vee f(y) \overset{f^{-1}\ \text{iso}}{\Rightarrow} x, y \leq f^{-1}(f(x) \vee f(y)) \Rightarrow x \vee y \leq f^{-1}(f(x) \vee f(y)) \overset{f\ \text{mono}}{\Rightarrow} f(x \vee y) \leq f(x) \leq f(y) \Rightarrow f(x \vee y) = f(x) \vee f(y)$, a tedy f je homomorfismus.

TODO: pro $\wedge$. ⊞

Definice 6 (Distributivní svaz, atom, koatom, komplement)**.** Nechť $S(\wedge, \vee)$ je svaz. Řekneme, že S je distributivní svaz, pokud $\forall a, b, c \in S : (a \vee b) \cap (a \vee c) = a \vee (b \wedge c)$.

Pokud jako nejmenší prvek svazu označíme 0, největší 1, pak *atomem* svazu $S(\wedge, \vee)$ rozumíme každé $a \in S$ pokrývající prvek 0 (tj. $O \prec a$). Duálním pojmem je *koatom*, tedy prvek svazu, který je pokrytý 1.

Dále *komplementem* prvku $a \in S$ nazveme $a' \in S$ takový, že $a \vee a' = 1, a \wedge a' = 0$.

Tvrzení 2 (O distributivních svazech)**.**

1. Svaz $S(\wedge, \vee)$ je distributivní, právě když $\forall a, b, c \in S : a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.
2. Každý prvek distributivního svazu má nejvýše jeden komplement.

Důkaz. 1: Stačí jedna implikace, druhá se ukáže duálně - „⇒“: mějme $a, b, c \in S$ libovolné. Pak $(a \wedge b) \vee (a \wedge c) = ((a \wedge b) \vee a) \wedge ((a \wedge b) \vee c) = a \wedge ((a \wedge b) \vee c) = a \wedge (c \vee (a \wedge b)) = a \wedge ((c \vee a) \wedge (c \vee b)) = (a \wedge (c \vee a)) \wedge (c \vee b) = a \wedge (c \vee b)$.

2: pro $a \in S$, nechť $b_1, b_2 \in S$ jsou komplementy k a. Pro libovolné $i, j \in \{1, 2\} : b_i = b_i \cap 1 = b_i \cap (a \vee b_j) = (b_i \wedge a) \vee (b_i \wedge b_j) = 0 \vee (b_i \wedge b_j) = b_i \wedge b_j \Rightarrow b_i \leq b_j$ Tedy ze slabé antisymetrie $b_i = b_j$. ⊞

Definice 7 (Booleova algebra)**.** Booleovou algebrou nazveme algebru $S(\wedge, \vee, 0, 1, ')$ takovou, že:

- $S(\wedge, \vee)$ je distributivní svaz
- 0 je jeho nejmenší prvek
- 1 je jeho největší prvek
- pro libovolné $a \in S$ je a' komplement a.

Tvrzení 3 (O Booleově algebře)**.** Ať $S(\wedge, \vee, 0, 1, ')$ je Booleova algebra. Pak pro každé $a, b \in S$ platí:

1. $(a')' = a$
2. $1' = 0, 0' = 1$
3. $(a \vee b)' = a' \wedge b'$
4. $(a \wedge b)' = a' \vee b'$

Důkaz. 1,2: snadno

3: $(a \vee b) \wedge (a' \wedge b') = (a \wedge a' \wedge b') \vee (b \wedge a' \wedge b') = (0 \wedge b') \vee (0 \wedge a') = 0$

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

4 symetricky ⊞

Věta 3 (Charakterizace konečných Booleových algeber)**.** Nechť $S(\wedge, \vee, 0, 1, ')$ je konečná Booleova algebra. Označme $A = \{a \in S : 0 \prec a\}$ množinu atomů v S. Potom zobrazení $\varphi\colon \mathcal{P}(A) \to S$ definované vztahem $\varphi(B) = \sup B$ je izomorfismus Booleových algeber $\mathcal{P}(A)(\cap, \cup, \emptyset, A, ')$ a $S(\wedge, \vee, 0, 1, ')$.

Důkaz. Pro $T \subseteq S : \bigvee T = \sup T, \bigwedge T = \inf T$. Pro $T = \emptyset : \bigvee \emptyset = 0, \bigwedge \emptyset = 1$. Položíme $\psi\colon S \to \mathcal{P}(A) : \psi(s) = \{a \in A : a \leq s\}$. Z definice jsou φ, ψ monotónní, navíc $\varphi(\emptyset) = 0, \psi(0) = \emptyset$. Ukážeme, že obě složení jsou identity.

Prvně $\psi \circ \varphi = id_{\mathcal{P}(A)}$: mějme libovolné $B \subseteq A$. Pak $\psi(\varphi(B)) = \psi(\bigvee B) = \{a \in A : a \leq \bigvee B\} \stackrel{?}{=} B$.

$B \subseteq \psi(\bigvee B) : b \in B : b \leq \bigvee B$, jelikož $b \in B$, navíc $b \in A$, tedy $b \in \psi(\bigvee B)$.

$B \supseteq \psi(\bigvee B) : c \in \psi(\bigvee B) : c \neq 0, c = c \wedge (\bigvee B) = \bigvee_{b \in B}(c \wedge b)$, a jelikož $c \wedge b$ jsou atomy, máme $c \in B$, jinak by průsek byl nulový.

Zadruhé: $\varphi \circ \psi = id_S$: mějme $s \in S$ libovolné, položme $t = \varphi(\psi(s)) = \bigvee \psi(s)$, tedy $t \leq s \Rightarrow t \subseteq s$. Pro spor nechť $t < s$. Z distributivitiy: $s = s \cap 1 = s \cap (t \vee t') = (s \cap t) \vee (s \cap t') = t \vee (s \cap s') \Rightarrow s \cap t' \neq 0$. Ať $a \in A$ je nějaký, že $a \leq s \cap t'$. Pak $a \leq t', a \leq t$ (druhé protože $a \in \psi(s)$), což je spor, neboť pak $a \leq t \cap t' = 0$.

Z charakterizace izomorfismu svazů máme φ, ψ vzájemně inverzní monotónní bijekce, tedy jsou izomorfismy. Dále $\varphi(\emptyset) = 0, \varphi(A) = 1$, a díky tomu máme slučitelnost s komplementem. ⊞

Definice 8 (Modulární svaz)**.** O svazu $S(\wedge, \vee)$ řekneme, že je *modulární*, pokud $\forall a, b, c \in S : (a \leq c \Rightarrow (a \vee b) \wedge c = a \vee (b \wedge c))$. Této implikaci říkáme *modulární zákon pro svazy.*

Tvrzení 4 (O modulárních svazech)**.** 1. Každý distributivní svaz je modulární.

2. Svaz $S(\wedge, \vee)$ je modulární, právě když $\forall a, b, c \in S : ((a \wedge c) \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$.

Důkaz. 1: Ať $a \leq c, a, b, c \in S$ libovolné. Pak $(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c) = a \vee (b \wedge c)$.

2: „⇒“: $S(\wedge, \vee)$ je modulární, tedy $((a \wedge c) \vee b) \wedge c \stackrel{mod}{=} (a \wedge c) \vee (b \wedge c)$.

„⇐“: Ať $a \leq c$. Pak $(a \vee b) \wedge c = ((a \wedge c) \vee b) \wedge c = (a \wedge c) \vee (b \wedge c) = a \vee (b \wedge c)$. ⊞

Věta 4 (Charakterizace modulárních svazů)**.** Svaz $S(\wedge, \vee)$ je modulární, právě když $S(\wedge, \vee)$ neobsahuje podsvaz izomorfní $N_5(\wedge, \vee)$.

Důkaz. „⇒“ obměnou: ať v $S(\wedge, \vee)$ existuje takový podsvaz, pak ani v S nemůže platit modularita.

„⇐“ obměnou: Ať S není modulární. Pak existují $x, y, z \in S : x \leq z \wedge (x \vee y) \wedge z > x \vee (y \wedge z)$. Položme $a := x \vee (y \wedge z), b := y, c := (x \vee y) \wedge z$. Tvrdíme, že jediná možná situace je N_5, kde v levé větvi je b a a je pod c v pravé větvi: musíme ukázat $b \wedge c = b \wedge a, b \vee a = b \vee c$.

$y \wedge z \stackrel{\text{abs}}{=} y \wedge (x \vee y) \wedge z = b \wedge c \geq a \wedge b = y \wedge (x \vee (y \wedge z)) = y \wedge (y \wedge z) = y \wedge z$

$x \vee y = y \vee x \vee (y \wedge z) = b \vee a \leq c \vee b = y \vee ((x \vee y) \wedge z) \leq y \vee (x \vee y) = x \vee y.$ ⊞

Věta 5 (Modulární svazy a zobrazení)**.** Nechť $S(\wedge, \vee)$ je svaz, $a, b \in S$, $a \not\leq b, b \not\leq a$.

Zadefinujeme $[a \wedge b, b] := \{s \in S : a \wedge b \leq s \leq b\}$, $[a, a \vee b] := \{s \in S : a \leq s \leq a \vee b\}$. Položíme $f_a\colon [a \wedge b, b] \to [a, a \vee b]$ tak, že $f_a(x) = a \vee x$ a $g_b\colon [a, a \vee b] \to [a \wedge b, b]$ tak, že $g_b(y) = b \wedge y$.

Pak svaz $S(\wedge, \vee)$ je modulární, právě když $\forall a, b \in S : a \not\leq b \ \& \ b \not\leq a \Rightarrow f_a, g_b$ jsou vzájemně inverzní bijekce.

Důkaz. „⇐“ obměnou: Nechť $S(\wedge, \vee)$ není modulární. Uvažujme jeho podsvaz izomorfní N_5. Pak $g_b(c) = b \wedge c = a \wedge b = g_b(a)$, tedy g_b není bijekce.

„⇒“: buď $S(\wedge, \vee)$ modulární, prvky $a \not\leq b, b \not\leq a$ jsou libovolné.

Ať $c \in [a \wedge b, b]$ libovolné. Pak $g_b(f_a(c)) = b \wedge (a \vee c)) \stackrel{mod}{=} (b \wedge a) \vee c = c$.

Ať $d \in [a, a \vee b]$ libocolné. Pak $f_a(g_b(d)) = a \wedge (b \vee d) \stackrel{mod}{=} (a \wedge b) \vee d = d$.

Tím jsme ověřili vzájemnou inverznost (a navíc i monotonii) bijekcí. ⊞

Důsledek 2 (Modularita svazu normálních podgrup)**.** Svaz normálních podgrup (či kongruencí) dané grupy G je modulární.

Poznámka (3. věta o izomorfismu)**.** Buď $G(\cdot)$ grupa, $H \trianglelefteq G, K \leq G$. Pak $H \cap K \trianglelefteq K$ a platí $HK/H \simeq K/H \cap K$.

Tvrzení 5 (O distributivních svazech a prohození průseku a spojení)**.** Svaz $S(\wedge, \vee)$ je distributivní, právě když $\forall x, y, z \in S : LS := (x \wedge y) \vee (x \wedge z) \vee (y \wedge z) = (x \vee y) \wedge (y \vee z) \wedge (z \vee x) =: PS$.

Důkaz. „⇒“: $LS \overset{distr}{=} (x \vee ((x \wedge z) \vee (y \wedge z))) \wedge (y \vee ((x \wedge z) \vee (y \wedge z))) = (x \vee (y \wedge z)) \wedge (y \vee (x \wedge z)) \overset{distr}{=} (x \vee y) \wedge (x \vee z) \wedge (y \vee x) \wedge (y \vee z) = (x \vee y) \wedge (x \vee z) \wedge (y \vee z) = PS$.

„⇐“: modularita S: mějme $x, y, z \in S, x \leq z$. Pak $(x \vee y) \wedge z = (x \vee y) \wedge (x \vee z) \wedge (y \vee z) \overset{\text{předp.}}{=} (x \vee y) \wedge (y \vee z) \wedge (z \vee x) = x \vee (y \wedge z)$.

Použijeme větu o modulárních svazech a zobrazeních pro $x, y \wedge z$. Pak $f_{y \wedge z} : [x \wedge y \wedge z, x] \to [y \wedge z, x \vee (y \wedge z)] : a \mapsto a \vee (y \wedge z), g_x : b \mapsto b \wedge x$.

Pak $x \wedge z \wedge z \leq (x \wedge y) \vee (x \wedge z) \leq x$. $f_{y \wedge z}((x \wedge y) \vee (x \wedge z)) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z) \overset{\text{předp.}}{=} (x \vee y) \wedge (x \vee z) \wedge (y \vee z)$ a dále $(x \wedge y) \vee (x \wedge z) = g_x((x \vee y) \wedge (x \vee z) \wedge (y \vee z)) = x \wedge (y \vee z)$, což je distributivita. ⊞

Věta 6 (Charakterizace distributivních svazů)**.** Svaz $S(\wedge, \vee)$ je distributivní, právě když neobsahuje jako podsvaz N_5 ani M_3.

Důkaz. „⇒“ obměnou: pokud S obsahuje jako podsvaz N_5, pak není modulární, a tedy ani distributivní. Pokud obsahuje jako podsvaz M_3, ten není distributivní (a má dva různé komplementy), a tedy ani S není distributivní.

„⇐“ obměnou: Ať $S(\wedge, \vee)$ není distributivní. Není-li modulární, obsahuje N_5 a máme hotovo. Buď tedy S modulární. Pak existuje x, y, z taková, že $(x \wedge y) \vee (x \wedge z) \vee (y \wedge z) \neq (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$. Konkrétně musí platit $LS < PS$, protože vždy $LS \leq PS$. Označme $u := LS, v := PS$ a položíme $a = (u \vee x) \wedge v \overset{mod}{=} u \vee (x \wedge v) = u \vee (x \wedge (y \vee z)) = (y \wedge z) \vee (x \wedge (y \vee z)) \overset{mod}{=} ((y \wedge z) \vee x) \wedge (y \vee z), b = (a \vee y) \wedge v = u \vee (y \wedge v), c = (u \vee z) \wedge v = u \vee (z \wedge v)$. Ukážeme $a \wedge b = u : a \wedge b = (y \vee z) \wedge ((y \wedge z) \vee x) \wedge ((x \wedge z) \vee y) \wedge (x \vee z) = ((y \wedge z) \vee x) \wedge ((x \wedge z) \vee y) \overset{mod}{=} [((y \wedge z) \vee x) \wedge y] \vee (x \wedge z) = (y \wedge z) \vee (x \wedge z) \vee (x \wedge z) = u$. Podobně $a \vee b = v$, stejně tak pro další dvojice, čímž ukážeme, že $S(\wedge, \vee)$ obsahuje M_3. ⊞

Věta 7 (Krácení v distributivních svazech)**.** Svaz $S(\wedge, \vee)$ je distributivní, právě když $\forall a, b, c \in S : a \wedge b = c \wedge b \;\&\; a \vee b = c \vee b \Rightarrow a = c$.

Důkaz. „⇒“: Mějme $a, b, c \in S : a \wedge b = c \wedge b \& a \vee b = c \vee b$. Pak $c = c \vee (c \wedge b) = c \vee (a \wedge b) = (c \vee a) \wedge (c \wedge b) = (c \vee a) \wedge (a \vee b) = a \vee (c \wedge v) = a \vee (a \wedge b) = a$.

„⇐“ obměnou: Ať $S(\wedge, \vee)$ není distributivní: pak obsahuje M_3 nebo N_5, a tam to neplatí pro typické volby a, b, c. ⊞

Definice 9 (Kompaktní prvek, algebraický svaz)**.** Buď $S(\wedge, \vee)$ úplný svaz. Prvek $k \in S$ je *kompaktní*, pokud $\forall A \subseteq S$, kdykoliv $k \leq \bigvee A (= \bigvee_{a \in A} a)$, potom existuje konečná $F \subseteq A$ taková, že $k \leq \bigvee F$.

Úplný svaz nazveme *algebraický*, pokud lze každý jeho prvek vyjádřit jako spojení (ne nutně konečně mnoha) kompaktních prvků.

Pozorování (Konečné spojení zachovává kompaktnost)**.** Spojení konečně mnoha kompaktních prvků je opět kompaktní prvek.

Tvrzení 6 (Svaz poduniverz algebry je algebraický)**.** Nechť $\mathcal{A} = A(\alpha_i, i \in I)$ je algebra. Svaz $\mathrm{Sub}(\mathcal{A})(\bigcap, \vee)$ všech jejích poduniverz je algebraický. Kompaktními prvky jsou právě konečně generovaná poduniverza.

Důkaz. Každé poduniverzum je spojením svých konečně generovaných poduniverz, stačí tedy dokázat tvrzení o kompaktních prvcích.

„⊆“: Buď K kompaktní prvek svazu $\mathrm{Sub}(\mathcal{A})$. Pak $K = \bigvee_{a \in K} \langle a \rangle$, kde $\langle a \rangle$ je poduniverzum univerza K generované prvkem a. Z kompaktnosti existuje $F \subseteq K$ takový, že $K = \bigvee_{a \in F} \langle a \rangle = \langle F \rangle$, tedy K je konečně generované.

„⊇“: Stačí ukázat, že $\forall a \in A : \langle a \rangle$ je kompaktní prvek ve svazu $\mathrm{Sub}(\mathcal{A})$. Předpokládejme, že $\langle a \rangle \subseteq \bigvee_{j \in J} U_j$. Pak $B = \{b \in A : \text{existuje konečná } F \subset J : b \in \bigvee_{j \in F} U_j\}$ je poduniverzum algebry A. Tedy $B = \bigvee_{j \in J} U_j$, a tedy $a \in B \Rightarrow \langle a \rangle \subseteq \bigvee_{j \in F} U_j$ pro nějakou konečnou $F \subseteq J$. ⊞

Věta 8 (Oprávněné pojmenování algebraických svazů)**.** Buď $S(\wedge, \vee)$ algebraický svaz. Pak $S \simeq \mathrm{Sub}(\mathcal{A})$ pro nějakou algebru $\mathcal{A}$.

Důkaz. Označme množinu všech kompaktních prvků svazu S jako A Na A zavedeme algebru $\mathcal{A}(0, \vee, o_k, k \in A)$, kde $0 \in A$ je nejmenší prvek svazu S (ten je jistě kompaktní) a $o_k(a) = k$ pro $k \vee a = a$ a a jinak. Zadefinujeme $\iota : S \to \mathrm{Sub}(\mathcal{A})$ vztahem $\iota : s \mapsto \{a \in A : a \leq s\}$, tedy $\iota(s) \in \mathrm{Sub}(\mathcal{A})$, je to „dolní množina" pod s, a tedy vše respektuje. Dále definujeme $\mu : \mathrm{Sub}(\mathcal{A}) \to S$ takovou, že $\mu(B) = \bigvee B$.

Obě zobrazení jsou zjevně monotónní, ukážeme vzájemně inverzní bijekci.

Pro $s \in S : s = \bigvee \iota(s)$ z algebraičnosti S.

Pro $B \in \mathrm{Sub}(\mathcal{A}) : B \subseteq \iota(\bigvee B)$ triviálně. Pokud dále $a \in \iota(\bigvee B)$, pak $a \leq \bigvee B$. Protože a je kompaktní ve svazu S, existuje konečná $F \subseteq B$ taková, že $a \leq \bigvee F$. Ovšem $\bigvee F \subseteq B$, neboť B je uzavřená na konečná spojení (z $B \in \mathrm{Sub}(\mathcal{A})$). Tedy i $a = o_a(\bigvee F) \in B$, a tedy $B = \iota(\bigvee B)$, čímž máme vzájemně jednoznanou inverzní bijekčnost. ⊞

Definice 10 (Term)**.** Buď fixovaný typ $\Omega : I \to \mathbb{N}_0$, $X \neq \emptyset$ taková, že $I \cap X = \emptyset$. Pak *term* nad X je definován rekurzivně následovně:

1. $\forall x \in X : x$ je term nad X
2. $\forall i \in I, n = \Omega(i), t_1, \ldots, t_n$ termy nad X, pak $(i, t_1, \ldots, t_n)$ je term nad X.

Definice 11 (Algebra termů)**.** *Algebrou termů* nad X typu Ω: $I \to \mathbb{N}_0$ rozumíme algebru $\mathcal{T}_X = T_X(a_i, i \in I)$ typu Ω, kde T_X je množina všech termů nad X a $\forall i \in I, n = \Omega(i)$ je $a_i(t_1, \ldots, t_n) = (i, t_1, \ldots, t_n)$.

Definice 12 ($\mathcal{K}$-volná algebra)**.** Fixujme typ Ω, nechť $\mathcal{K}$ značí nějakou třídu algeber typu Ω. Řekneme, že algebra $\mathcal{A} \in \mathcal{K}$ je *$\mathcal{K}$-volná nad množinou X* pro $X \subseteq A$ takovou, že X generuje $\mathcal{A}$ a pro každou $\mathcal{B} \in \mathcal{K}$ a zobrazení $f : X \to B$ existuje homomorfismus $g : \mathcal{A} \to \mathcal{B}$ takový, že $g \restriction X = f$.

Definice 13 (Absolutně volná algebra)**.** Řekneme, že $\mathcal{A}$ je *absolutně volná nad X*, pokud je $\mathrm{Alg}(\Omega)$-volná nad X, kde $\mathrm{Alg}(\Omega)$ je třída všech algeber typu Ω.

Tvrzení 7 (Absolutní volnost algebry termů)**.** Algebra termů je absolutně volná.

Důkaz. Buď $\mathcal{B} = B(\alpha_i, i \in I)$ typu Ω, zobrazení $f : X \to B$.
Definujeme $g : T_x \to B$ rekurzivně následovně: $g(t) = f(t)$ pro $t \in X$, jinak $g((i, t_1, \ldots, t_n)) = \alpha_i(g(t_1), \ldots, g(t_n))$.
Snadno ukážeme, že g je homomorfismus. (TODO) ⊞

Definice 14 (Kvaziprimitivní (netriviální) třída, varieta)**.** *Kvaziprimitivní třídou typu Ω* rozumíme $\mathcal{K} \subseteq \mathrm{Alg}(\Omega)$, která je uzavřená na součiny, podalgebry a izomorfismy. Pokud je $\mathcal{K}$ navíc uzavřená na homomorfní obrazy, tj. je-li $g : \mathcal{A} \to \mathcal{B}$ homomorfismus algeber typu Ω, pak $A \in \mathcal{K} \Rightarrow Im(g) \in \mathcal{K}$, nazýváme $\mathcal{K}$ *varietou typu Ω*.

Kvaziprimitivní třídu nazveme *netriviální*, obsahuje-li alespoň jednu alespoň dvouprvkovou algebru.

Tvrzení 8 (Existence $\mathcal{K}$-volné algebry)**.** Je-li $\mathcal{K}$ netriviální kvaziprimitivní třída, pak pro každou $X \neq \emptyset$ existuje $\mathcal{K}$-volná algebra nad X.

Důkaz. Položme $\mathcal{A} := \mathcal{T}_X$. Uvažme $S = \{r \in \mathrm{Con}(\mathcal{A}) : \mathcal{A}/r \in \mathcal{K}\}$. Tvrdíme, že $\bigcap S \in S$.

Zadefinujeme homomorfismus $F : \mathcal{A} \to \prod_{r \in S} \mathcal{A}/r$. vztahem $F(a)(r) = [a]_r$, kde r probíhá přes S. Pak $\ker F = \bigcap S$ a dle první věty o izomorfismu $\mathcal{K} \ni Im(F) \simeq \mathcal{A}/ker(F)$. Tedy $\bigcap S \in S$.

Dále nechť $I := Im(f)$. Z věty o homomorfismu plyne, že pro libovolný homomorfismus $g : \mathcal{A} \to \mathcal{B}$, kde $\mathcal{B} \in \mathcal{K}$ existuje právě jedno $h : I \to \mathcal{B}$ takové, že $g = h \circ F$ (zde využíváme $\bigcap S \subseteq \ker(g), IM(g) \in \mathcal{K}$).

Stačí ukázat, že I je volná nad $Y = F(X) = \{F(x) : x \in X\}$ a že $F \restriction X$ je prosté. Z netriviality $\mathcal{K}$ existuje $\mathcal{B} \in \mathcal{K}$, jejíž nosič má mohutnost aspoň $|X|$. Tedy existuje prosté zobrazení $f : X \to B$. To lze rozšířit do homomorfismu z $\mathcal{A}$ do $\mathcal{B}$, jelikož $\mathcal{A}$ je absolutně volná nad X. Tedy $F \restriction X$ je prosté.

Dále I je jistě generovaná množinou Y - uvažme libovolnou $\mathcal{B} \in \mathcal{K}$ a zobrazení $f : Y \to \mathcal{B}$. Chceme f rozšířit do homomorfismu z $\mathcal{I}$ do $\mathcal{B}$. Nejprve díky absolutní volnosti $\mathcal{A}$ najdeme homomorfismus $g : \mathcal{A} \to \mathcal{B}$ takový, že $g \restriction X = f \circ (F \restriction X)$. Dále díky větě o homomorfismu obdržíme $h : \mathcal{I} \to \mathcal{B}$ takové, že $g = h \circ F$. Homomorfismu h zjevně rozšiřuje zobrazení f. ⊞

Definice 15 (Splnění atomické formule)**.** Atomická formule $s = t$ je splněna v $\mathcal{A}$, právě když $\forall$homomorfismus$f : \mathcal{T}_X \to \mathcal{A}$ platí $f(s) = f(t)$. Ekvivalentně, $(s, t) \in \bigcap\{\ker(f) : f : \mathcal{T}_X \to \mathcal{A}\}$.

Definice 16 (Eq a Mod)**.** Nechť $\mathcal{K} \subseteq Alg(\Omega)$. Označíme $Eq(\mathcal{K}) = \{(s,t) \in T_X^2 : (\forall B \in \mathcal{K}) s = t \text{ je splněna v } B\}$.

Duálně pro $R \subseteq T_X^2$ položíme $Mod(R) = \{B \in Alg(\Omega) : (s,t) \in R \Rightarrow s = t \text{ je splněna v } B\}$.

Lemma 1 (O termech a Eq)**.** Nechť A je neprázdná množina, $\mathcal{T}_A$ algebra termů typu Ω. Mějme dané $(u,v) \in T_A^2$. Pak existuje $(s,t) \in \mathcal{T}_X^2$ takové, že pro každou $\mathcal{K} \subseteq Alg(\Omega)$ platí $(u,v) \in \bigcap\{\ker(f) : f : T_A \to B : B \in \mathcal{K}\} \Leftrightarrow (s,t) \in Eq(\mathcal{K})$.

Důkaz. Buď C nějaká konečná podmnožina množiny A taková, že u, v jsou termy nad C. Zvolme libovolně zobrazení $z \to A \to X$, tak, aby $z \restriction C$ bylo prosté a definujeme $Y := \{z(c) : c \in C\}$. Víme, že $\mathcal{T}_A$ je absolutně volná nad A, takže existuje (právě jeden) homomorfismus $g : \mathcal{T}_A \to \mathcal{T}_X$ takový, že $g \restriction A = z$.

Položme $s = g(u), t = g(v)$ a zpozorujeme, že $g \restriction T_c$ je izomorfismus algeber $\mathcal{T}_C$ a $\mathcal{T}_Y$. Nechť g' je izomorfismus inverzní k $g \restriction T_c$.

Mějme $(u,v) \in \bigcap\{\ker(f) : f : \mathcal{T}_A \Rightarrow \mathcal{B}, \mathcal{B} \in \mathcal{K}\}$ a $h : \mathcal{T}_X \to \mathcal{B}$ je libovolná, že $\mathcal{B} \in \mathcal{K}$. Pak $(u,v) \in ker(h \circ g)$, a tedy $(s,t) = (g(u), g(v)) \in ker(h)$, tedy i $(s,t) \in Eq(\mathcal{K})$.

Naopak, mějme $(s,t) \in Eq(\mathcal{K})$ a buď $f : \mathcal{T}_A \to \mathcal{B}$ libovolně, že $\mathcal{B} \in \mathcal{K}$. Pak $(u,v) \in T_C$ a $f \restriction T_C = f \circ g \circ (g \restriction T_C)$. Homomorfismus $f \circ g' : \mathcal{T}_Y \to \mathcal{B}$ rozšíříme libovolně na homomorfismus $h : \mathcal{T}_X \to \mathcal{B}$. To uděláme tak, že $f \circ g'$ nejdříve zúžíme na konečnou množinu Y, pak libovolně dodefinujeme na $X \setminus Y$ a nakonec jednoznačně rozšíříme na h, neboť $\mathcal{T}_X$ je absolutně volná nad X. Máme $(s,t) \in ker(h) \Rightarrow (s,t) \in ker(f \circ g')$.

V důsledku $f(u) = f(g'(g(u))) = f(g'(s)) = f(g'(t)) = f(g'(g(v))) = f(v)$, tedy $u, v \in ker(f)$.

⊞

Věta 9 (Birkhoffova)**.** Nechť $\mathcal{K} \subseteq Alg(\Omega)$. Pak $\mathcal{K}$ je varietou, právě když lze $\mathcal{K}$ axiomatizovat atomickými formulemi, tedy $\mathcal{K} = Mod(Eq(\mathcal{K}))$.

Důkaz. „⇐“: Nechť platí $\mathcal{K} = Mod(Eq(\mathcal{K}))$. Uvažujme libovolnou $(s,t) \in Eq(\mathcal{K})$ a $\mathcal{A} \in \mathcal{K}$. Je-li $\mathcal{B}$ podalgebra algebry $\mathcal{A}$, pak z definice dostáváme, že $s = t$ je splněno v $\mathcal{B}$, a tedy $\mathcal{K}$ je uzavřena na podalgebry.

Dále ať je $h : \mathcal{A} \to \mathcal{C}$ surjektivní homomorfismus a $g : \mathcal{T}_X \to \mathcal{C}$ libovolný homomorfismus. Pro každé $x \in X$ vybereme jedno $a_x \in A$ tak, že $h(a_x) = g(x)$. Definujeme zobrazení $f : X \to A$ vztahem $f(x) = a_x$ a rozšíříme do homomorfismu $F : \mathcal{T}_X \to \mathcal{A}$. Pak $h \circ F = g$, neboť oba homomorfismy se rovnají na X, která generuje $\mathcal{T}_X$. Z $\mathcal{A} \in \mathcal{K}$ plyne $F(s) = F(t)$, a proto musí být i $g(s) = h \circ F(s) = h \circ F(t) = g(t)$. Tedy jsme ukázali, že $\mathcal{K}$ je uzavřeno na homomorfní obrazy.

„⇒“: Prvně, pokud je $\mathcal{K}$ triviální vareta (obsahuje jen jednoprvkové algebry), pak je axiomatizovaná formulí $x = y$, kde x, y jsou různé proměnné. (Všechny jednoprvkové algebry jsou izomorfní a $\mathcal{K}$ je uzavřená na izomorfismy.)

Nechť $\mathcal{K}$ je netriviální, jistě $\mathcal{K} \subseteq Mod(Eq(\mathcal{K}))$. Uvažme dále libovolnou $\mathcal{A} \in Mod(Eq(\mathcal{K}))$, chceme $\mathcal{A} \in \mathcal{K}$. Buď $h : \mathcal{T}_A \to \mathcal{A}$ homomorfismus takový, že $h(a) = a \forall a \in A$. Pak h je surjektivní. Dále uvažme $\mathcal{I} \in \mathcal{K}$ takové, že je $\mathcal{K}$-volná nad A. Taková existuje a $\mathcal{I} \simeq \mathcal{T}_A/r_0$, kde $r_0 = \bigcap\{r \in Con(\mathcal{T}_A) : \mathcal{T}_A/r \in \mathcal{K}\}$.

Ukážeme, že $r_0 \subseteq ker(h)$. Nechť $(u,v) \in r_0 \subseteq T_A^2$ je libovolné. Z předchozího lemmatu získáme $(s,t) \in T_X^2$. Pro každý homomorfismus $f : \mathcal{T}_A \to \mathcal{C}$, kde $\mathcal{C} \in \mathcal{K}$, máme $\mathcal{T}_A/ker(f) \simeq Im(f) \in \mathcal{K}$, a tedy $(u,v) \in r_0 \subseteq ker(f)$.

Z jedné implikace $(s,t) \in Eq(\mathcal{K})$, a tedy $s = t$ je splněna v $\mathcal{A}$. (Jinak řečeno, $(s,t) \in Eq(\{\mathcal{A}\})$, z čehož z druhé implikace plyne $(u,v) \in ker(h)$.) Tedy máme $r_0 \subseteq ker(h)$.

Z věty o homomorfismu máme $g : \mathcal{T}_A/r_0 \to \mathcal{A}$ takové, že $g([u]_{r_0}) = h(i)$ platí pro každ= $u \in T_A$. Jelikož h je surjekce, i g musí být surjekce.

Nakonec, jelikož $\mathcal{T}_A/r_0 = \mathcal{I} \in \mathcal{K}$ a $\mathcal{K}$ je uzavřená na homomorfní obrazy, máme $\mathcal{A} \in \mathcal{K}$. ⊞

Definice 17 (Komutativní okruh s jednotkou, obor integrity, těleso, podobor)**.** Komutativní okruh s jednotkou R je množina R s operacemi $+, -, \cdot$ a konstantami $0 \neq 1$ splňující $a, b, c \in R$ následující podmínky: $a+(b+c) = (a+b)+c, a+b = b+a, a+0 = a, a+(-a) = 0, a(bc) = (ab)c, ab = ba, a \cdot 1 = a, a(b+c) = ab+ac$.

Platí-li navíc podmínka $a, b \neq 0 \to ab \neq 0$, nazýváme R obor integrity.

Platí-li navíc podmínka $\forall a \neq 0 \exists b : ab = 1$, nazýváme R těleso, značíme $b = a^{-1}$.

Pro $S \subseteq R$ takovou, že $0, 1 \in S$, a kdykoliv $a, b \in S$, pak i $-a \in S, a + b \in S, ab \in S$, pak S s restrikcemi operací nazveme podoborem.

Definice 18 (Rozšíření podoboru)**.** Buď R podobor oboru S a $a_1, a_2, \ldots, a_n \in S$. Definujeme $R[a_1, \ldots, a_n]$ jako nejmenší podobor oboru S obsahující množinu R i prvky $a_1, \ldots, a_n$.

Definice 19 (Dělitelnost a invertibilita)**.** Řekneme, že a dělí b v oboru R, pokud $\exists c \in R : b = ac$, píšeme $a|b$.

Řekneme, že prvky a a b jsou asociované, pokud $a|b$ a $b|a$, píšeme $a||b$.

Prvek a nazveme invertibilní, pokud $a||1$.

Tvrzení 9 (Asiociovanost a invertibilita)**.** Dva prvky a, b jsou asociované, právě když existuje invertibilní prvek q takový, že $a = bq$.

Důkaz. „⇐“: $a = bq \Rightarrow b|a$, z invertibility q máme $b = aq^{-1}$, a tedy $a|b$.

„⇒“: $b|a \Rightarrow a = bu$, $a|b \Rightarrow b = av$, tedy $a = bu = avu$, krácením: $vu = 1$, tedy $u, v||1$ a navíc $u = v^{-1}$. ⊞

Pozorování (Čum na oboru)**.** $||$ je ekvivalence na R. Můžeme tedy zadefinovat $\overline{R} = R/||$, pak $(\overline{R}, |)$ je částečně uspořádaná množina.

Definice 20 (NSD, NSN)**.** Řekneme, že $c = NSD(a, b)$, pokud $c|a \wedge c|b \wedge$ kdykoliv $d|a \wedge d|b$, pak $d|c$.

Řekneme, že $c = NSN(a, b)$, pokud $c \cdot NSD(a, b) = ab$.

Definice 21 (Ireducibilní prvek)**.** Neinvertibilní prvek a nazveme ireducibilní, pokud nemá vlastní dělitele, tj. pro každý rozklad $a = bc$ platí $b||1$ nebo $c||1$.

Definice 22 (Gaussovský obor)**.** Obor integrity nazveme gaussovský, pokud má každý jeho neinvertibilní nenulový prvek jednoznačný rozklad na ireducibilní činitele.

Tvrzení 10 (Gaussovský obor a dělitelnost vzhledem k rozkladu)**.** Buď R gaussovský obor, $a \in R$ a mějme rozklad $a = a_1^{k_1} \cdot \dots \cdot a_n^{k_n}$ na ireducibilní činitele, kde $a_i \not|| a_j$ pro $i \neq j$. Pak $b|a \Leftrightarrow b||a_1^{l_1} \cdot \dots \cdot a_n^{l_n}$ pro nějaká $0 \leq l_i \leq k_i$.

Důkaz. „⇐“: $a_1^{l_1} \cdot \dots \cdot a_n^{l_n} | a_1^{k_1} \cdot \dots \cdot a_n^{k_n}$, protože $a||b \cdot (a_1^{k_1 - l_1} \cdot \dots \cdot a_n^{k_n - l_n})$.

„⇒“: Nechť $b|a = a_1^{k_1} \cdot \dots \cdot a_n^{k_n}$. Tedy $a = bc$ pro nějaké $c \in R$. Označme $b = b_1 \cdot \dots \cdot b_r$, $c = c_1 \cdot \dots \cdot c_s$ ireducibilní rozklady. Pak $a = a_1^{k_1} \cdot \dots \cdot a_n^{k_n} = b_1 \dots \dots \cdot b_r \cdot c_1 \cdot \dots \cdot c_s$ jsou dva rozklady prvku a a z jednoznačnosti plyne, že pro každé $i \in [r]$ existuje j tak, že $b_i||a_j$, a navíc pro každé j existuje nejvýše k_J indexů takových, že $a_j||b_i$. Tedy $b||a_1^{l_1} \cdot \dots \cdot a_n^{l_n}$ pro nějaké $0 \leq l_i \leq k_i$. ⊞

Tvrzení 11 (Gaussovský obor a dělitelnost ireducibilních prvků)**.** Buď R gaussovský obor a $p \in R$ ireducibilní prvek. Platí-li $p|a \cdot b$, pak $p|a$ nebo $p|b$.

Důkaz. Mějme $a = a_1 \cdot \dots \cdot a_m, b = b_1 \cdot \dots \cdot b_n$ ireducibilní rozklady. Neboť $p|a_1 \cdot \dots \cdot a_m \cdot b_1 \cdot \dots \cdot b_n$, musí mít z předchozího tvrzení nějaký rozklad, obsahující některé z $a_1, \dots, a_m, b_1, \dots, b_n$. Protože p je ireducibilní, musí být $p||a_i$ nebo $p||b_i$, a tedy $p|a$ nebo $p|b$. ⊞

Poznámka (Prvočinitel)**.** Prvek splňující $p|ab \Rightarrow p|a \vee p|b$ nazýváme prvnočinitel.

Tvrzení 12 (Gaussovské obory a NSD)**.** V gaussovských oborech existuje NSD všech prvků.

Důkaz. Nechť $a||c_1^{k_1} \cdot \dots \cdot c_n^{k_n}, b||c_1^{l_1} \cdot \dots \cdot c_n^{l_n}$ jsou ireducibilní rozklady a, b a $c_i \not|| c_j$ pro $i \neq j$. Pak $c := c_1^{\min(k_1, l_1)} \cdot \dots \cdot c_n^{\min(k_n, l_n)}$, ukážeme $NSD(a, b) = c$. Z věty o dělitelnosti vzhledem k rozkladu gaussovských oborů máme, že d je společný dělitel a a b, právě když $d||c_1^{r_1} \cdot \dots \cdot c_n^{r_n}$ pro nějaká $r_1, \dots, r_n \geq 0$ taková, že $r_i \leq k_i, r_i \leq l_i$ pro všechna i. Největší je zjevně takové, že $r_i = \min(k_i, l_i)$. ⊞

Lemma 2 (Obor integrity a násobení s NSD)**.** Buď R obor integrity, $a, b, c \in R$ takové, že existují $NSD(a, b), NSD(ac, bc)$. Pak $NSD(ac, bc) = c \cdot NSD(a, b)$.

Důkaz. NSD je definován až na asiociovanost. Stačí ukázat, že levá strana dělí pravou a naopak. Mějme $u := NSD(ac, bc)$. (Pro $c = 0$ triviální, nechť tedy $c \neq 0$.) Prvně $u|x \cdot NSD(a, b)$. $u|ac, u|bc \Rightarrow \exists x : ac = ux, \exists y : bc = uy$. Protože $u = NSD(ac, bc)$, máme $c|u$, tedy $\exists z : u = cz$. Pak $ac = czx, bc = czy$ a z krácení máme $a = zx, b = zy$ a z je společný dělitel a, b, tedy $z|NSD(a, b)$, a tedy $u = cz|c \cdot NSD(a, b)$.

Druhak: $NSD(a, b)|a, NSD(a, b)|b \Rightarrow NSD(a, b) \cdot c|ac, NSD(a, b) \cdot c|bc$, tedy $c \cdot NSD(a, b)|NSD(ac, bc)$. ⊞

Lemma 3 (Existence všech NSD implikuje prvočinitelnost ireducibilních prvků)**.** Nechť v oboru R existuje NSD všech dvojic prvků a $p \in R$ je ireducibilní. Pak $p|ab \Rightarrow p|a \vee p|b$.

Důkaz. Nechť $p \not| a$. Pak $NSD(a,p) = 1$ z ireducibility p, tedy $NSD(pb, ab) = b \cdot NSD(a,p) = b$. Ovšem p je společným dělitelem pb, ab, a tedy $p|NSD(pb,ab) = b$. ⊞

Věta 10 (Charakterizace gaussovských oborů)**.** Nechť R je obor integrity. Pak R je gaussovský, právě když

1. existuje NSD všech dvojic prvků,
2. neexistuje posloupnost $a_1, a_2, \ldots \in R$ taková, že $a_{i+1}|a_i$ a $a_i \not| a_{i+1}$.

Důkaz. „⇒“: Buď R gaussovsky. 1 plyne z tvrzení o NSD v gaussovských oborech, zbývá 2.

Pro spor nechť taková posloupnost existuje, buď $a_1 = b_1^{k_1^1} \cdot \cdots \cdot b_n^{k_n^1}$ ireducibilní rozklad a_1. Máme $a_i|a_1$ pro všechna $i > 1$, a také $a_i || b_1^{k_1^i} \cdot \cdots \cdot b_n^{k_n^i}$ pro nějaká k_j^i, kde $k_1^1 \geq k_1^2 \geq \ldots$ atd. Neboť $a_{i+1} \not| a_i$, musí se aspoň jeden k_j^i snížit, a to nemůže jít až do nekonečna.

„⇐“: 1. každý prvek má ireducibilní rozklad: ať $a \neq 0, a \not| 1$ takový rozklad nemá. Pak indukcí zkontruujeme posloupnost, která protiřečí 2: $a_1 = a$, mějme $a_i \not| 1$. a_i také sám není ireducibilní, tedy $a_i = bc$ pro $b, c \not| 1$. Kdyby b i c měly ireducibilní rozuklad, pak by ho měl i a, búno b ho nemá a $a_{i+1} := b$.

2. jednoznačnost rozkladu: pro spor a prvek, který má více rozkladů a jeho rozklad je ze všech sporných nejkratší $a := a_1 \cdot \cdots \cdot a_n$ nejkratší a $a = b_1 \cdot \cdots \cdot b_m$ další rozklad. a_1 je ireducibilní, z lemmatu o dělitelnosti a ireducibilitě máme nějaké $b_i : a_1 || b_i$ (máme dělitelnost + b_i je ireducibilní). Tedy $a' = a_2 \cdot \cdots \cdot a_n || b_1 \cdot \cdots \cdot b_{i-1} \cdot b_{i+1} \cdot \cdots \cdot b_m$ je prvek s kratším rozkladem, což je spor. ⊞

Definice 23 (Eukleidovská norma, obor)**.** Eukleidovskou normou na oboru R rozumíme zobrazení $\nu : R \to \mathbb{N} \cup \{0\}$ splňující:

0. $\nu(0) = 0$
1. $a|b \neq 0 \Rightarrow \nu(a) \leq \nu(b)$
2. $\forall a, b \in R : b \neq 0 : \exists q, r \in R : a = bq + r, \nu(r) < \nu(b)$.

Obor se nazývá eukleidovský, pokud na něm existuje eukleidovská norma.

Algoritmus 1 (Eukleidův)**.** IN: $a, b \in R, \nu(a) \geq \nu(b)$.
OUT: $NSD(a,b), u, v \in R : NSD(a,b) = ua + vb$.
$a_0 = a, u_0 = 1, v_0 = 0, a_1 = b, u_1 = 0, v_1 = 1$
$a_{i+1} = r, u_{i+1} = u_{i-1} - u_i q, v_{i+1} = v_{i-1} - v_i q$, kde $a_{i-1} = a_i q + r$ a $\nu(r) < \nu(a_i)$.
Pokud $a_{i+1} = 0$ vrať a_i, u_i, v_i.

Věta 11 (Eukleidův algoritmus je korektní)**.** Eukleidův algoritmus nalezne v eukleidovském oboru R pro jakýkoliv vstup $a, b \in R$ hodnotu $NSD(a,b)$ a $uv \in R : NSD(a,b) = ua + vb$.

Důkaz. $\nu(a_0) \geq \nu(a_1) > \nu(a_2) > \ldots \geq 0$, tedy musí v konečném čase zastavit. Chceme $NSD(a,b) = a, k = u_k a + v_k b$. Neboť $NSD(a_k, 0) = a_k$, stačí ukázat, že NSD dvou po sobš jdouvích prvků posloupnosti a_i se nemění, tedy $\forall i \in [k] : NSD(a_{i-1}, a_i) = NSD(a_i, a_{i+1})$ a $\forall i \in [k] \cup \{0\} : a_i = u_i a + v_i b$. Oboje plyne z $a_{i-1} = a_i q + a_{i+1}$. ⊞

Lemma 4 (O dělitelnosti a eukleidovské normě)**.** Buď R eukleidovský obor. $a, b \in R, a, b \neq 0$.

1. $a||b \Rightarrow \nu(a) = \nu(b)$
2. $a|b \wedge b \not| a \Rightarrow \nu(a) < \nu(b)$.

Důkaz. 1. $a||b \Rightarrow a|b \wedge b|a \to \nu(a) \leq \nu(b) \wedge \nu(b) \leq \nu(a) \Rightarrow \nu(a) = \nu(b)$.

2. Jistě $\nu(a) \leq \nu(b)$, pro spor nechť $\nu(a) = \nu(b)$. Tedy $b = au$ pro nějaké $u \in R$, $a = bq + r$ pro nějaké $q, r \in R$, $\nu(r) < \nu(b) = \nu(a)$. Jelikož $b \not| a$, máme $r \neq 0$. Pak $r = a - bq = a - auq = a(1 - uq) \Rightarrow a|r \Rightarrow \nu(a) \leq \nu(r) \Rightarrow$ spor.

⊞

Důsledek 3 (Eukleidovské obory jsou gaussovské)**.** Eukleidovské obory jsou gaussovské.

Důkaz. Existence NSD z předchozí věty (máme Eukleidův algoritmus), neexistence nekonečné posloupnosti dělitelů plyne z druhé části předchozího lemmatu - při dělení se snižuje norma. ⊞

Definice 24 (Ideál, hlavní ideál)**.** Ideálem v oboru R rozumíme libovolnou podmnožinu $I \subseteq R$ splňující $0 \in I, \forall a, b \in U, \forall u \in R : -a \in I \wedge a + b \in I \wedge au \in I$.

Hlavním ideálem v oboru R rozumíme podmnožinu $aR = \{ar : r \in R\} = \{u \in R : a|u\}$ pro libovolné $a \in R$.

Věta 12 (Ideály v eukleidovských oborech)**.** V eukleidovských oborech je každý ideál hlavní.

Důkaz. Buď I ideál v eukleidovském oboru R. Pokud $I = \{0\}$, máme $I = 0R$.

Jinak označíme a prvek ideálu, který má nejmenší nenulovou eukleidovskou normu. (Je-li jich více, volíme libovolně). Ukážeme $I = aR$. Zjevně $aR \subseteq I$, tedy pro spor nechť $b \in I \setminus aR$. Zvolme q, r splňující $b = aq + r$ a $\nu(r) < \nu(a)$. Jistě $r \neq 0$, a neboť b není dělitelná a, máme $a < \nu(r) < \nu(a)$. Ale $r = b - aq$, kde $b, aq \in I$, a tedy i $r \in I$. Tím máme spor s výběrem a jako prvku s nejmenší kladnou normou. ⊞

Definice 25 (Obor integrity hlavních ideálů)**.** Řekneme, že R je obor integrity hlavních ideálů, pokud je v R každý ideál hlavní.

Pozorování (Eukleidovskost implikuje OIHI)**.** Každý eukleidovský obor je obor integrity hlavních ideálů.

Věta 13 (Obory integrity hlavních ideálů jsou gaussovské)**.** Obory integrity hlavních ideálů jsou gaussovské.

Důkaz. Buď R OIHI. Stačí ukázat existenci NSD a neexistenci nekonečné posloupnosti vlastních dělitelů.

NSD: Mějme $a, b \in R$ libovolně. buď I nejmenší ideál obsahující množinu $aR \cup bR$. Pak existuje $c : I = cR$. Víme, že $aR \subset cR, bR \subset cR \Rightarrow c|a \wedge c|b$. Dále pro d společný dělitel a a b: $aR \subset dR, bR \subset dR \Rightarrow cR \subset dR \Rightarrow d|c$, tedy $c = NSD(a, b)$.

Dělitele: nechť taková posloupnost $a_1, a_2, \ldots$ existuje. Pak $a_1R \subset a_2R \subset a_3R \subset \ldots$ a navíc nikde neplatí rovnost. Buď $I = \bigcup_{i=1}^{\infty} a_iR$. Tato množina tvoří ideál. a tedy $I = bR$ pro nějaké $b \in R$. A jelikož $b \in I$, musí eixostvat nějaké $i : b \in a_iR$, a tedy $bR = a_iR = a_{i+1}R$, což je náš spor. ⊞

Poznámka (Obory $\mathbb{Z}$ rozšířené $\sqrt{s}$, a ν)**.** Obory $\mathbb{Z}[\sqrt{s}]$ uvažujeme pro s, jež není dělitelné druhou mocninou žádného prvočísla a ν značí zobrazení $\mathbb{Z}[\sqrt{s}] \to \mathbb{N} \cup \{0\}$, kde $a + b\sqrt{s} \mapsto |a^2 - sb^2|$.

Tvrzení 13 (O ν v $\mathbb{Z}$ rozšířené $\sqrt{s}$)**.** Pro každá $u, v \in \mathbb{Z}[\sqrt{s}]$ platí

1. $\nu(uv) = \nu(u) \cdot \nu(v)$.
2. $\nu(u) = 1 \Leftrightarrow u$ je invertibilní.

Důkaz. 1: $u = a+b\sqrt{s}, v = c+d\sqrt{s}$. Pak $\nu(uv) = \nu((ac+sbd)+(ad+bc)\sqrt{s})) = |a^2-sb^2|\cdot|c^2-sd^2| = \nu(u)\cdot\nu(v)$.

2: $\nu(a + b\sqrt{s}) = |a^2 - sb^2| = 1 \Rightarrow s^2 - sb^2 = (a - b\sqrt{s})(a + b\sqrt{s}) = \pm 1 \Rightarrow a + b\sqrt{s} || 1$. Opačná implikace plyne z 1, neboť $u||1 \Rightarrow \exists v : uv = 1 \Rightarrow 1 = \nu(1) = \nu(uv) = \nu(u) \cdot \nu(v) \Rightarrow \nu(u) = \nu(v) = 1$. ⊞

Tvrzení 14 (ν a $\mathbb{Z}$ rozšířené o i)**.** Zobrazení ν je euklidovská norma na $\mathbb{Z}[i]$.

Důkaz. 0: Zjevně

1: Plyne z předchozího tvrzení (pro $s = -1$)

2: Mějme $a, b \in \mathbb{Z}[i], b \neq 0$ a $z = \frac{a}{b} \in \mathbb{C}$. Buď q nejbližší prvek $\mathbb{Z}[j]$ k z (minimalizujeme $|z - q|$); je-li jich více, zvolíme libovolně. Položme $r = a - bq$. Pak zjevně $a + bq + r$ a zbývá ukázat $\nu(r) < \nu(b)$. Jistě $|z - q| \leq \frac{\sqrt{2}}{2} < 1 \Rightarrow \nu(r) = |r|^2 = |a - bq|^2 = |b^2| \cdot |\frac{a}{b} - q|^2 = |b|^2 \cdot |z - q|^2 < |b|^2 = \nu(b)$. ⊞

Definice 26 (Obsah polynomu, primitivní část polynomu, primitivní polynom)**.** Buď $f = \sum_{i=0}^{n} a_i x^i$ polynom. Pak

- obsahem polynomu f rozumíme $ct(f) = NSD(a_0, a_1, \ldots, a_n)$
- primitivní částí polynomu f rozumíme $pp(f) = \sum_{i=0}^{n} \frac{a_i}{ct(f)} x^i$

- polynom f nazýváme primitivní, jestliže $ct(f) = 1$.

Věta 14 (O ireducibilitě polynomu ($!\delta$))**.** Buď R gaussovský obor, Q jeho podílové těleso a f polynom z $R[x]$. Pak f je ireducibilní v $R[x]$, právě když:

- deg $f = 0$ a f je ireducibilní v R nebo
- deg $f > 0$, f je primitivní a ireducibilní v $Q[x]$.

Věta 15 (Gaussova ($!\delta$))**.** Buď R gaussovský obor a X libovolná neprázdná množina. Pak $R[X]$ je také gaussovský obor.

Tvrzení 15 (Eisensteinovo kritérium)**.** Buď R gaussovský obor, $f = \sum_{i=0}^{n} a_i x^i$ primitivní polynom z $[X]$. Pokud existuje ireducibilní prvek $p \in R$ splňující $p|a_0, p|a_1, \ldots, p|a_{n-1}$ a $p^2 \nmid a_0$, pak je f ireducibilní v $R[x]$.

Důkaz. Uvažme rozklad $f = gh : g = \sum_{i=0}^{k} b_i x^i, h = \sum_{i=0}^{l} c_i x^i$ polynomy z $R[X]$ stupně alespoň 1. Pak $p|a_0 = b_0 c_0$, tedy $p|b_0$ nebo $p|c_0$, ale určitě ne oboje zároveň. Bez újmy na obecnosti nechť $p|b_0 \wedge p \nmid c_0$. Pak $p|a_1 = b_0 c_1 + b_1 c_0$, z předchozího nutně $p|b_1$. Takto pokračujeme a získáme $p|b_i \forall i \in [k]$. Tím získáváme $p|f$, což je spor s primitivitou f. ⊞

Definice 27 (Kořen polynomu)**.** Prvek $a \in R$ se nazývá kořen polynomu $f \in R[x]$, pokud $f(a) = 0$.

Tvrzení 16 (Obor integity a kořeny)**.** Buď R obor integrity, $f \in R[x], a \in R$. Pak a je kořenem f, právě když $x - a|f$.

Důkaz. „⇐“: $x - a|f$, tedy $f = (x - a)g$, načež je snadno vidět $f(a) = 0$.
„⇒“: Nechť $f = q(x - a) + r$. Pak $0 = f(a) = q(a)(x - a)(a) + r(a) = 0 + r = r$, a tedy $x - a|f$. ⊞

Věta 16 (Obor integrity a počet kořenů polynomu)**.** Buď R obor integrity, $0 \neq f \in R[x]$ a deg $f = n$. Pak má f nejvýše n kořenů.

Důkaz. Indukcí podle n. Pro $n = 0$ – mám nenulový konstantní polynom, vše v pořádku.
Pro $n \geq 1$ – buď f nemá kořen, nebo jej má (buď $a \in R$), pak $f = (x - a)g$ a z IP máme, že f má nejvýše $1 + n - 1 = n$ kořenů. ⊞

Definice 28 (Algebraické a transcendentní číslo)**.** Reálné číslo se nazývá algebraické, pokud existuje nenulový polynom $f \in \mathbb{Z}[x]$ takový, že $f(a) = 0$. V opačném případě se nazývá transcendentní.

Tvrzení 17 (Spočetnost algebraických reálných čísel)**.** Množina algebraických reálných ísel je spočetná.

Důkaz. Definujeme index polynomu f jako $|a_0| + \ldots + |a_n| + n$. Každého indexu existuje jen konečné mnoho polynomů, tak je můžeme nějak seřadit, a kořeny k nim nějak přidáme. ⊞

Tvrzení 18 (Nespočetnost reálných čísel)**.** $\mathbb{N} \not\approx \mathbb{R}$.

Důkaz. Diagonální metoda. ⊞

Tvrzení 19 (Obor integrity, podílové těleso a kořen)**.** Buď R obor integrity, Q jeho podílové těleso. Má-li polynom $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ kořen $r/s \in Q$ s r, s nesoudělnými, pak $r|a_0$ a $s|a_n$.

Důkaz. $0 = f(r/s) = \sum_{i=0}^{n} a_i (r/s)^i$. Toto přenásobíme s^n a získáme $a_0 s^n + a_1 r s^{n-1} + \ldots + a_{n-1} r^{n-1} s + a_n r^n = 0$. s dělí vše krom posledního členu, tak musí dělit i ten, r naopak. ⊞

Věta 17 (O interpolaci)**.** Buď T těleso a uvažujme po dvou různé body $a_1, \ldots, a_n \in T$ a libovolné hodnoty $u_1, \ldots, u_n \in T$. Pak existuje právě jeden polynom $f \in T[x]$ stupně $< n$ splňující $f(a_i) = u_i$ pro každé $i \in [n]$.

Důkaz. Řešení: Langrangeův interpolační polynom $f = \sum_{i=1}^{n} (u_i \cdot \prod_{j \neq i} \frac{x - a_j}{a_i - a_j})$. Pak $f(a_k) = 0 + \ldots + 0 + u_k \cdot 1 + 0 + \ldots + 0 = u_k$.
Jednoznačnost: $f, g : f \neq g, f(a_i) = g(a_i) = u_i \forall i \in [n], h := f - g$. $h(a_i) = 0 \forall i$, tedy $x - a_i | h \forall i$, tedy $(x - a_1) \cdots (x - a_n) | h$. Neboť deg$(h) < n$, musí být $h = 0$ a tedy $f \equiv g$. ⊞

Důsledek 4 (Funkce a polynomy v konečném tělese)**.** Buď T konečné těleso. Pak pro každou funkci $f : T \to T$ existuje právě jeden polynom g stupně $< |T|$ takový, že $f(a) = g(a) \forall a \in T$.

Důkaz. Interpolujeme. ⊞

Definice 29 (n-násobný kořen)**.** Řekneme, že $a \in R$ je n-násobný kořen polynomu $f \in R[x]$, pokud $(x-a)^n | f$ a $(x-a)^{n+1} \nmid f$.

Definice 30 (Derivace polynomu)**.** Derivace polynomu $f = \sum_{i=0}^{n} a_i x^i$ je $f' = \sum_{i=0}^{n-1} (i+1) a_{i+1} x^i$.

Derivace vyšších řádů definujeme induktivně: $f^{(0)} = f, f^{(n+1)} = (f^{(n)})'$.

Lemma 5 (Derivace a operace na polynomech)**.** Buď R obor integrity, $f, g \in R[x], n \in \mathbb{N}$. Pak

1. $(f+g)^{(n)} = f^{(n)} + g^{(n)}$
2. $(fg)^{(n)} = \sum_{i=0}^{n} \binom{n}{i} f^{(i)} g^{(n-i)}$ (Leibnizova formule)
3. $(f^n)' = n \cdot f^{n-1} \cdot f'$

Důkaz. 1. rozepsat + indukce

2. rozepsat + indukce

3. indukce za pomoci 2

⊞

Věta 18 (Derivace a násobnost kořene)**.** Buď R obor integrity, $0 \neq f \in R[x], a \in R$ a nechť charakteristika R je buď 0 nebo větší než $\deg f$. Pak jsou následující ekvivalentní:

1. a je n-násobný kořen polynomu f
2. $f^{(0)}(a) = \ldots = f^{(n-1)}(a) = 0, f^{(n)}(a) \neq 0$.

Důkaz. $1 \Rightarrow 2$: $f = (x-a)^n \cdot g : g(a) \neq 0$, dosadit do Leibnizovy formule.

$2 \Rightarrow 1$: $f^{(0)}(a) = f(a) = 0$, tedy a je kořen, a musí být n-násobný pro nějaké m, a z $1 \Rightarrow 2$ máme $m = n$. ⊞

Definice 31 (Podokruh, generovaný podokruh)**.** Buď R okruh. Pak $S \subseteq R$ tvoří podokruh okruhu R, pokud je uzavřená na všechny operace, tj. $0 \in S, -a \in S, a+b \in S, ab \in S$. Píšeme $S \leq R$, podokruhy R a $\{0\}$ nazýváme nevlastní.

Nejmenší podokruh okruhu R obsahující danou množinu X zveme podokruh generovaný X a značíme $\langle X \rangle_R$. Pro R okruh, $S \leq R$ a $a_1, \ldots, a_n \in R$, $S[a_1, \ldots, a_n] = \langle S \cup \{a_1, \ldots, a_n\} \rangle_R$ a hovoříme o rozšíření S o prvky $a_1, \ldots, a_n$.

Tvrzení 20 (Rozšíření okruhu a funkční hodnoty)**.** Buď R komutativní okruh, S jeho vlastní podokruh a $a_1, \ldots, a_n \in R$. Pak $S[a_1, \ldots, a_n] = \{f(a_1, \ldots, a_n) : f \in S[x_1, \ldots, x_n]\}$.

Důkaz. Označíme $M = \{f(a, 1, \ldots, a_n) : f \in S[x_1, \ldots, x_n]\}$. Musíme ukázat:

1. $S \cup \{a_1, \ldots a_n\} \subseteq M$
2. všechny prvky M lze nagenerovat z $S \cup \{a_1, \ldots, a_n\}$
3. M je uzavřená na všechny operace.

1: prvky S jsou konstantní polynomy, prvky a_i – polynom x_i.

2: Je-li $f \in S[x_1, \ldots, x_n]$, pak $f(a_1, \ldots, a_n)$ je prvek podokruhu $S[a_1, \ldots, a_n]$ - konstanty jsou v S a dosazení je v $\langle \{a_1, \ldots, a_n\} \rangle_R$.

3: máme díky polynomům. ⊞

Definice 32 (Prvotěleso, rozšíření tělesa)**.** Prvotěleso je nejmenší podtěleso (musí obsahovat 1).

Rozšířením tělesa T rozumíme libovolné nadtěleso $S \geq T$ a značíme $T(a_1, \ldots, a_n)$ pro nejmenší podtěleso S obsahující T i $a_1, \ldots, a_n$.

Poznámka (Prvotělesa a rozšíření + stupeň rozšíření)**.** Každé těleso obsahuje prvotěleso izomorfní buď $\mathbb{Q}$ nebo $\mathbb{Z}_p$.

$S \geq T$ lze považovat na vektorový prostor nad T, kde násobení $S \times S \to S$ redukujeme na $T \times S$ a máme násobení skalárem. Značíme $S_T(S, +, -, 0, a\cdot : a \in T)$, dimenzi S_T nazýváme stupněm rozšíření $T \leq S$ a značíme $[S : T] = \dim S_T$.

Definice 33 (Algebraický, transcendentní prvek a algebraické rozšíření)**.** Buď $T \leq S$ rozšíření tělesa a $a \in S$. Řekneme, že a je algebraický nad T, pokud existuje polynom z $T[x]$, jehož je a kořenem. V opačném případě nazveme prvek transcendentní nad T. Je-li každý prvek tělesa S algebraický nad T, hovoříme o algebraickém rozšíření.

Tvrzení 21 (Rozšíření konečného stupně jsou algebraická)**.** Rozšíření konečného stupně jsou algebraická.

Důkaz. $n := [S : T]$ a uvažme $a \in S$, ukážeme algebraičnost. Prvky $1, a, a^2, \ldots, a^n$ jsou lineárně závislé, tedy $\exists b_i : \sum_{i=0}^{n} b_i a^i = 0$, tedy máme nenulový polynom, jehož je a kořenem. ⊞

Definice 34 (Minimální polynom)**.** Buď $T \leq S$ rozšíření tělesa a $a \in S$ algebnraický prvek nad T. Pak minimálním polynomem prvku a nad T rozumíme monický polynom $m_{a,T} \in T[x]$ splňující $m_{a,T}(a) = 0$ a kdykoliv monický polynom $f \in T[x]$ splňuje $f(a) = 0$, pak $m_{a,T} | f$.

Tvrzení 22 (Rozšíření tělesa a podokruhu algebraickým prvkem je totéž)**.** Buď $T \leq S$ rozšíření těles a $a \in S$ algebraický prvek nad T. Pak $T(a) = T[a]$.

Důkaz. Víme, že $T[a] = \{f(a) : f \in T[x]\}$ je podokruh S Nalezneme inverzy k nenulovým prvkům a tím získáme podtělesovost. Buď $0 \neq f(a) \in T[a]$, hledáme polynom $g \in T[x]$ takový, že $f(a)g(a) = 1$. Jelikož $f(a) \neq 0$, máme $m_{a,T} \not| f$. Z ireducibility $m_{a,T}$ plyne $NSD(m_{a,T}, f) = 1$ a z Bézoutovy rovnost existují polynomy $u, f \in T[x] : 1 = um_{a,T} + gf$. Dosazením máme $1 = u(a) \cdot 0 + g(a)f(a) = g(a)f(a)$. ⊞

Tvrzení 23 (Stupeň rozšíření je stupeň minimálního polynomu)**.** Buď $T \leq S$ rozšíření těles a $a \in S$ algebraický prvek nad T. Pak $[T(a) : T] = \deg m_{a,T}$.

Důkaz. Položíme $n := \deg m_{a,T}$. Ukážeme, že $1, a, \ldots, a^{n-1}$ jsou báze $T(a)_T$. Kdyby byly lineárně závislé, pak $\exists b_i : \sum_{i=0}^{n-1} b_i a^i = 0$, čímž jsme našli stupněm menší nenulový polynom, což je spor s minimalitou.

Generujícnost: $f(a) \in T(a) = T[a]$, tedy $q, r \in T[x]$ t.ž. $f = qm_{a,T} + r, \deg r < \deg m_{a,T} = n$. Pak $f(a) = q(a) \cdot m_{a,T}(a) + r(a) = r(a)$. Potom $f(a) = r(a) = \sum_{i=0}^{n-1} b_i a^i$, kde $b_i \in T$ jsou koeficienty polynomu. ⊞

Tvrzení 24 (O stupních rozšíření těles)**.** Nuď $T \leq S \leq U$ rozšíření těles. Pak $[U : T] = [U : S] \cdot [S : T]$.

Důkaz. Jen pro konečnou dimenzi: $m := [U : S], n := [S : T]$, zvolme bázi A vektorového prostoru S_Ta bázi b vektorového prostoru U_S. Ukážeme, že $a_1 b_1 \ldots a_1 b_m, b_2 a_1, \ldots, a_n b_m$ tvoří bázi U_T.

Generujícnost: $u \in Z : u = \sum_i s_i b_i$ pro $s_i \in S$. Pak $s_i = \sum_j t_{ij} a_j$, tedy $u = \sum_i (\sum_j t_{ij} a_j) b_i = \sum_{i,j} t_{ij} \cdot a j_b i$, čímž máme generování.

Nezávislost: Nechť $\sum_{i,j} t_{ij} \cdot a_j b_i = 0$ pro nějaká t_{ij}. Pak $0 = \sum_{i,j} t_{ij} a_j b_i = \sum_j (\sum_i t_{ij} a_i) b_j \Rightarrow \sum_i t_{ij} a_i = 0 \Rightarrow t_{ij} = 0 \forall i, j$. ⊞

Věta 19 (Charakterizace konečnosti stupně rozšíření)**.** Rozšíření $T \leq S$ má konečný stupeň, právě když $S = T(a_1, \ldots, a_n)$ pro nějaké prvky $a_1, \ldots, a_n \in S$ algebraické nad T.

Důkaz. „$\Leftarrow$“: Uvažme postupná rozšíření $T \leq T(a_1) \leq \ldots, \leq T(a_1, \ldots, a_n)$. Pak $[T(a_1, \ldots, a_n) : T] = [T(a_1) : T] \cdot \cdots \cdot [T(a_1, \ldots, a_n) : T(a_1, \ldots, a_{n-1})]$. Všechny stupně jsou konečné, neboť odpovídají stupni minimálních polynomů.

„$\Rightarrow$“: Indukcí podle $k = [S : T]$. Pro $k = 1 : S = T$. Indukční krok: $a \in S \setminus T$: $T < T(a) \leq S$. Máme $[S : T] = [S : T(a)] \cdot [T(a) : T]$. Z IP: $S = (T(a))(b_1, \ldots, b_n) = T(a, b_1, \ldots, b_n)$ pro nějaké prvky $b_1, \ldots, b_n$. Rozšíření je konečného stupně z předpokladu, takže prvky jsou algebraické. ⊞

Definice 35 (Kořenové nadtěleso)**.** Řekneme, že $S \geq T$ je kořenové nadtěleso polynomu $f \in T[x]$, pokud má polynom f v tělese S kořen a a navíc $S = T(a)$.

Definice 36 (T-izomorfismus)**.** T-izomorfismus je izomorfismus $U \to V$, jehož restrikce na T je identita.

Věta 20 (O kořenovém nadtělesu)**.** Buď T těleso a $f \in T[x]$ stupně alespoň 1. Pak

1. existuje kořenové nadtěleso polynomu f,

2. je-li polynom f ireducibilní v $T[x]$, pak jsou každá dvě kořenová nadtělesa polynomu f T-izomorfní.

Důkaz. 1: Buď g nějaký ireducibilní dělitel polynomu f a položme $I = gT[x]$. Toto je maximální ideál v $T[x]$, a tedy $S = T[x]/I$ je těleso. Uvažme homomorfismus $\psi : T \to S : a \mapsto [a]$. Je prostý, neboť prvky tělesa T nejsou v I, takže můžeme ztotožnit T a $Im(\psi)$ a uvážíme $T \leq S$.

Dosadíme-li do polynomu $g = \sum_{i=0}^{n} a_i x^i$ prvek $b = fx]$, máme $g(b) = [g] = [0]$. Prvek b je tedy kořenem g, tedy i kořenem f v tělese S a navíc $S = T(b)$, protože $T[x]$ je generován $T \cup \{x\}$.

2: Uvažme $T \leq T(a), T \leq T(b)$ kořenová nadtělesa. Máme $T(a) = \{g(a) : g(\in T[x])\}, T(b) = \{g(b) : g \in T[x]\}$. Uvažujme tedy zobrazení $\varphi : T(a) \to T(b), g(a) \mapsto g(b)$.

Uvědomíme si, že $f = m_{a,T} = m_{b,T}$, a tedy $g(a) = h(a) \Leftrightarrow (g-h)(a) = 0 \Leftrightarrow f|g-h \Leftrightarrow (g-h)(b) = 0 \Leftrightarrow g(b) = h(b)$. Tedy φ je opravdu zobrazení, navíc je prosté. Z toho výše jistě zachovává všechny operace, máme tedy izomorfismus. ⊞

Definice 37 (Rozkladové nadtěleso)**.** Řekneme, že $S \geq T$ je rozkladové nadtěleso polynomu $f \in T[x]$, pokud se polynom f rozkládá v S na lineární činitele, a navíc, kdykoliv $T \leq U \leq S$, pak se polynom f v $U[x]$ na lineární činitele nerozkládá.

Tvrzení 25 (O rozkladovém nadtělesu)**.** Buď T těleso a $f \in T[x]$ je stupně ≥ 1. Pak

1. existuje rozkladové nadtěleso polynomu f,

2. každá dvě rozkladová nadtělesa f jsou T-izomorfní.

Důkaz. 1: indukcí podle stupně f. Pro stupeň 1 máme $S = T$. Jinak uvažme kořenové nadtěleso $T(a) \geq T$ polynomu f a $g \in T(a)[x]$ takové, že $f = g \cdot (a - x)$. Z $\deg g < \deg f$ a IP máme rozkladové nadtěleso S nad $T(a)$. Také se tam rozkládá f na lineární činitele, tedy $g = g(x-a) = (\ldots) \cdots (x-a)$. Navíc je nejmenší takové: kdyby bylo menší, rozkládal by se v něm i g, což je spor.

2: Dokážeme obecnější tvrzení:

Buďte T_1, T_2 nadtělesa T, $\varphi : T_1 \to T_2$ T-izomorfismus, $f = \sum a_i x^i$ polynomu z $T_1[x]$, $\varphi(f) = \sum \varphi(a_i) x^i$ polynom z $T_2[x]$ a označme S_1 rozkladové nadtěleso f nad T_1, S_2 rozkladové nadtěleso $\varphi(f)$ nad T_2. Pak S_1 a S_2 jsou T-izomorfní.

Naše tvrzení pak plyne dosazením $T_1 = T_2 = T, \varphi = \mathrm{id}$. Budeme postupovat indukcí podle $\deg f$. Pro stupeň 1 máme $S_1 = T_1, S_2 = T_2$ a máme hotovo. Pro stupeň > 1: uvažme ireducibilní dělitel g polynomu f a jeho kořen a v S_1. Pak $\varphi(g)$ je ireducibilní dělitel polynomu $\varphi(f)$, a $\varphi(a) \in S_2$ je jeho kořen, a tak podobně jako v předchozí větě máme T-izomorfismu $T_1(a)$ a $T_2(\varphi(a))$, označíme jej ψ. Dále z IP: $h \in T_1(a)[x]$ je polynom: $f = (x-a)h$, tedy $\psi(f) = (x - \psi(a)) \cdot \psi(h)$, pak rozkladové nadtěleso S_1 polynomu h nad $T_1(a)$ a rozkladové nadtěleso S_2 polynomu $\varphi(h)$ nad $T_2(\varphi(a))$ jsou T-izomorfní z IP. ⊞

Věta 21 (O rozkladovém nadtělese polynomu $x^{p^n} - x$)**.** Buď p prvočíslo, $n \in \mathbb{N}$ a S rozkladové nadtěleso polynomu $f = x^{p^n} - x \in \mathbb{Z}_p$. Pak $|S| = p^n$.

Důkaz. Uvažme $M = \{a \in s : f(a) = 0\} = \{a \in S : a^{p^n} = a\}$. Prvně $f' = p^n x^{p^n - 1} - 1 = -1$, neboť $\mathbb{Z}_p$ má charakteristiku p. Derivace f' tedy nemá s f společná žádný kořen, neboť je konstantní -1, tedy $|M| = p^n$ a všechny kořeny jsou jednoduché.

Ukážeme, že M je podtělesem $S : 0, 1 \in M$ jistě. Dále $(a^{-1})^{p^n} = (a^{p^n})^{-1} = a^{-1}$, $(ab)^{p^n} = a^{p^n} b^{p^n} = ab$, $(a+b)^p = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} = a + b$, neboť $\binom{p}{k}$ je dělitelné p pro každé $k : 0 < k < p$. Pak $(a+b)^{p^n}$ použijeme n-násobnou aplikaci.

Tím máme M podtěleso S. Navíc jde o rozkladové nadtěleso f, jelikož obsahuje právě všechny kořeny polynomu f, a tedy $M = S$. ⊞

Tvrzení 26 (O existenci ireducibilního polynomu stupně n)**.** Pro každé prvočíslo p a $n \in \mathbb{N}$ existuje polynom $g \in \mathbb{Z}_p[x]$ stupně n, který je ireducibilní nad $\mathbb{Z}_p$. Navíc pro g v $\mathbb{Z}_p[x]$ platí $g | x^{p^n} - x$.

Důkaz. Ze ZS: Pokud je S konečné (komutativní) těleso, pak $S^*(\cdot,^{-1},1)$ je cyklická grupa. Z předchozí věty máme těleso S mající p^n prvků, kde S je rozkladové nadtěleso polynomu $x^{p^n}-x \in \mathbb{Z}_p[x]$. Uvažme libovolný generátor $\alpha \in S^*$ multiplikativní grupy S^*. Pak jistě $\mathbb{Z}_p(\alpha) = S$. Jako g nyní vezmeme minimální polynom $\alpha \in S$ nad $\mathbb{Z}_p$, tedy $g = m_{\alpha,\mathbb{Z}_p}$. Víme, že $n = [S:\mathbb{Z}_p] = [\mathbb{Z}_p(\alpha):\mathbb{Z}_p] = \deg g$ a g je ireducibilní nad $\mathbb{Z}_p$. Dále, jelikož α je kořenem $x^{p^n}-x$, plyne z minimality g, že v $\mathbb{Z}_p[x]$ platí $g|x^{p^n}-x$. ⊞

Seznam témat

1 Definice (Částečně uspořádaná množina, nejmenší, největší, minimální, maximální prvky, supremum, infimum) . . . 1
2 Definice (Svaz, úplný svaz) . . . 1
3 Definice (Pokrytí, Hasseův diagram) . . . 1
1 Věta (Vlastnosti svazu) . . . 1
1 Důsledek (Pohledy na svaz) . . . 1
4 Definice (Monotónní zobrazení a homomorfismus svazů) . . . 1
5 Definice (Podsvaz) . . . 1
1 Tvrzení (Homomorfismus svazů je monotónní) . . . 1
2 Věta (Charakterizace isomorfismu svazů) . . . 2
6 Definice (Distributivní svaz, atom, koatom, komplement) . . . 2
2 Tvrzení (O distributivních svazech) . . . 2
7 Definice (Booleova algebra) . . . 2
3 Tvrzení (O Booleově algebře) . . . 2
3 Věta (Charakterizace konečných Booleových algeber) . . . 2
8 Definice (Modulární svaz) . . . 3
4 Tvrzení (O modulárních svazech) . . . 3
4 Věta (Charakterizace modulárních svazů) . . . 3
5 Věta (Modulární svazy a zobrazení) . . . 3
2 Důsledek (Modularita svazu normálních podgrup) . . . 3
Poznámka (3. věta o izomorfismu) . . . 3
5 Tvrzení (O distributivních svazech a prohození průseku a spojení) . . . 3
6 Věta (Charakterizace distributivních svazů) . . . 4
7 Věta (Krácení v distributivních svazech) . . . 4
9 Definice (Kompaktní prvek, algebraický svaz) . . . 4
Pozorování (Konečné spojení zachovává kompaktnost) . . . 4
6 Tvrzení (Svaz poduniverz algebry je algebraický) . . . 4
8 Věta (Oprávněné pojmenování algebraických svazů) . . . 4
10 Definice (Term) . . . 5
11 Definice (Algebra termů) . . . 5
12 Definice ($\mathcal{K}$-volná algebra) . . . 5
13 Definice (Absolutně volná algebra) . . . 5
7 Tvrzení (Absolutní volnost algebry termů) . . . 5
14 Definice (Kvaziprimitivní (netriviální) třída, varieta) . . . 5
8 Tvrzení (Existence $\mathcal{K}$-volné algebry) . . . 5
15 Definice (Splnění atomické formule) . . . 5
16 Definice (Eq a Mod) . . . 6
1 Lemma (O termech a Eq) . . . 6
9 Věta (Birkhoffova) . . . 6
17 Definice (Komutativní okruh s jednotkou, obor integrity, těleso, podobor) . . . 6
18 Definice (Rozšíření podoboru) . . . 6
19 Definice (Dělitelnost a invertibilita) . . . 7
9 Tvrzení (Asiociovanost a invertibilita) . . . 7

Pozorování (Čum na oboru) . . . 7
20 Definice (NSD, NSN) . . . 7
21 Definice (Ireducibilní prvek) . . . 7
22 Definice (Gaussovský obor) . . . 7
10 Tvrzení (Gaussovský obor a dělitelnost vzhledem k rozkladu) . . . 7
11 Tvrzení (Gaussovský obor a dělitelnost ireducibilních prvků) . . . 7
Poznámka (Prvočinitel) . . . 7
12 Tvrzení (Gaussovské obory a NSD) . . . 7
2 Lemma (Obor integrity a násobení s NSD) . . . 7
3 Lemma (Existence všech NSD implikuje prvočinitelnost ireducibilních prvků) . . . 8
10 Věta (Charakterizace gaussovských oborů) . . . 8
23 Definice (Eukleidovská norma, obor) . . . 8
1 Algoritmus (Eukleidův) . . . 8
11 Věta (Eukleidův algoritmus je korektní) . . . 8
4 Lemma (O dělitelnosti a eukleidovské normě) . . . 8
3 Důsledek (Eukleidovské obory jsou gaussovské) . . . 9
24 Definice (Ideál, hlavní ideál) . . . 9
12 Věta (Ideály v eukleidovských oborech) . . . 9
25 Definice (Obor integrity hlavních ideálů) . . . 9
Pozorování (Eukleidovskost implikuje OIHI) . . . 9
13 Věta (Obory integrity hlavních ideálů jsou gaussovské) . . . 9
Poznámka (Obory $\mathbb{Z}$ rozšířené $\sqrt{s}$, a ν) . . . 9
13 Tvrzení (O ν v $\mathbb{Z}$ rozšířené $\sqrt{s}$) . . . 9
14 Tvrzení (ν a $\mathbb{Z}$ rozšířené o i) . . . 9
26 Definice (Obsah polynomu, primitivní část polynomu, primitivní polynom) . . . 9
14 Věta (O ireducibilitě polynomu (!δ)) . . . 10
15 Věta (Gaussova (!δ)) . . . 10
15 Tvrzení (Eisensteinovo kritérium) . . . 10
27 Definice (Kořen polynomu) . . . 10
16 Tvrzení (Obor integity a kořeny) . . . 10
16 Věta (Obor integrity a počet kořenů polynomu) . . . 10
28 Definice (Algebraické a transcendentní číslo) . . . 10
17 Tvrzení (Spočetnost algebraických reálných čísel) . . . 10
18 Tvrzení (Nespočetnost reálných čísel) . . . 10
19 Tvrzení (Obor integrity, podílové těleso a kořen) . . . 10
17 Věta (O interpolaci) . . . 10
4 Důsledek (Funkce a polynomy v konečném tělese) . . . 11
29 Definice (n-násobný kořen) . . . 11
30 Definice (Derivace polynomu) . . . 11
5 Lemma (Derivace a operace na polynomech) . . . 11
18 Věta (Derivace a násobnost kořene) . . . 11
31 Definice (Podokruh, generovaný podokruh) . . . 11
20 Tvrzení (Rozšíření okruhu a funkční hodnoty) . . . 11
32 Definice (Prvotěleso, rozšíření tělesa) . . . 11
Poznámka (Prvotělesa a rozšíření + stupeň rozšíření) . . . 12
33 Definice (Algebraický, transcendentní prvek a algebraické rozšíření) . . . 12
21 Tvrzení (Rozšíření konečného stupně jsou algebraická) . . . 12
34 Definice (Minimální polynom) . . . 12
22 Tvrzení (Rozšíření tělesa a podokruhu algebraickým prvkem je totéž) . . . 12
23 Tvrzení (Stupeň rozšíření je stupeň minimálního polynomu) . . . 12
24 Tvrzení (O stupních rozšíření těles) . . . 12
19 Věta (Charakterizace konečnosti stupně rozšíření) . . . 12
35 Definice (Kořenové nadtěleso) . . . 12
36 Definice (T-izomorfismus) . . . 12

20 Věta (O kořenovém nadtělesu) 13
37 Definice (Rozkladové nadtěleso) 13
25 Tvrzení (O rozkladovém nadtělesu) 13
21 Věta (O rozkladovém nadtělese polynomu $x^{p^n} - x$) 13
26 Tvrzení (O existenci ireducibilního polynomu stupně n) 13