Základy obecné algebry

Ústav matematiky, Fakulta strojního inženýrství VUT v Brně, 2013

Obsah

Kapitola 1

Algebraické struktury

1.1 Operace a zákony

Definice 1.1. Buď A množina, $n \in \mathbb{N}_0$. Potom zobrazení $\omega : A^n \to A$ se nazývá *n-ární operace* na A . Tedy pro $n \in \mathbb{N}$:

$$\omega : \begin{cases} A^n \to A \\ (x_1, \ldots, x_n) \mapsto \omega x_1 \ldots x_n, \end{cases}$$

pro $n = 0$:

$$\omega : \begin{cases} A^0 = \{\emptyset\} \to A \\ \emptyset \mapsto \omega\emptyset =: \omega. \end{cases}$$

Nejdůležitější případ: $n = 2$. 2-ární neboli binární operace je zobrazení

$$\omega : \begin{cases} A^2 \to A \\ (x, y) \mapsto \omega xy =: x\omega y. \end{cases}$$

Většinou označujeme binární operace nějakým grafickým symbolem, např. $\circ$, namísto symbolu ω, tedy

$$\circ : \begin{cases} A^2 \to A \\ (x, y) \mapsto x \circ y. \end{cases}$$

Užijeme-li k označení binární operace symbolu $\cdot$, mluvíme o multiplikativním značení (a píšeme xy místo $x \cdot y$). Užijeme-li symbolu $+$, mluvíme o aditivním značení.

Příklad(y) 1.2. 1) $+$ a $\cdot$ jsou binární operace na $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}^+$, $\mathbb{R}$, $\mathbb{R}^+$ a $\mathbb{C}$, $-$ je binární operace na $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{C}$, $\div$ je binární operace na $\mathbb{Q}^+$, $\mathbb{R}^+$, $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$.

2) Operace $+$ a $\cdot$ (v běžném smyslu) jsou binární operace na množině $M_n(\mathbb{C})$ všech čtvercových matic řádu n nad $\mathbb{C}$ (podobně pro $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ místo $\mathbb{C}$).

3) Nechť M, N jsou množiny a $N^M := \{f \mid f : M \to N\}$. Pro $M = N$ je binární operace $\circ$ na M^M definována takto: $(f \circ g)(x) := f(g(x))$ pro všechna $x \in M$ (jde o známou operaci skládání funkcí). Obdržíme tedy:

$$\circ : \begin{cases} (M^M)^2 \to M^M \\ (f, g) \mapsto f \circ g. \end{cases}$$

4) Buď M množina a $\mathcal{P}(M) := \{T \mid T \subseteq M\}$ množina všech podmnožin množiny M. Operace $\cap, \cup$ jsou binární operace na $\mathcal{P}(M)$.

Další důležitý příklad: $n = 1$. 1-ární neboli unární operace na množině A je zobrazení

$$\omega : \begin{cases} A \to A \\ x \mapsto \omega x. \end{cases}$$

Příklad(y) 1.3. 1) $- : \begin{cases} \mathbb{C} \to \mathbb{C} \\ x \mapsto -x \end{cases}$ je unární operace na $\mathbb{C}$.

2) $-$ je unární operace na $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $M_n(\mathbb{C})$.

3) $x \mapsto 1/x$ je unární operace na $\mathbb{Q} \setminus \{0\}$, $\mathbb{Q}^+$, $\mathbb{R} \setminus \{0\}$, $\mathbb{R}^+$, $\mathbb{C} \setminus \{0\}$.

4) $T \mapsto M \setminus T =: T'$ je unární operace na množině všech podmnožin $\mathcal{P}(M)$ množiny M.

Definice 1.4. Buď A množina, $n \in \mathbb{N}_0$, $D \subseteq A^n$. Potom zobrazení $\omega : D \to A$ se nazývá *n-ární parciální operace* na A.

Příklad(y) 1.5. 1) $-$ je binární parciální operace na $\mathbb{N}$.

2) $x \mapsto 1/x$ je unární parciální operace na $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ($D = \mathbb{Q} \setminus \{0\}, \ldots$).

Buď $A = \{a_1, \ldots, a_n\}$ konečná množina a $\circ$ binární operace na A. Pak $\circ$ lze zadat pomocí tzv. *Cayleyovy tabulky* . Tabulka má v průsečíku i-tého řádku s j-tým sloupcem prvek $a_i \circ a_j$.

Definice 1.6. Buď A množina, I množina (indexů). Pro $i \in I$ buď ω_i n_i-ární operace na A, $n_i \in \mathbb{N}_0$. Potom $\mathcal{A} := (A, (\omega_i)_{i \in I})$ označuje (*univerzální*) *algebru* s *nosnou množinou* A a *souborem operací* $(\omega_i)_{i \in I} =: \Omega$.

Často bývá I konečná, např. $I = \{1, \ldots, n\}$. V takovémto případě píšeme

$$(A, \Omega) = (A, (\omega_i)_{i \in \{1, \ldots, n\}}) =: (A, \omega_1, \ldots, \omega_n).$$

Soubor $(n_i)_{i \in I}$ se nazývá *typ* algebry (A, Ω).

Příklad(y) 1.7. $(\mathbb{Z}, +, -, 0)$ je algebra typu $(2, 1, 0)$, $(\mathbb{Z}, +, -, 0, \cdot, 1)$ je algebra typu $(2, 1, 0, 2, 0)$.

Definice 1.8. Buď A množina, $\circ$ binární operace na A. Prvek $e \in A$ se nazývá a) *levý neutrální prvek* vzhledem k $\circ :\Leftrightarrow \forall x \in A : e \circ x = x$, b) *pravý neutrální prvek* vzhledem k $\circ :\Leftrightarrow \forall x \in A : x \circ e = x$, c) *neutrální prvek* vzhledem k $\circ :\Leftrightarrow \forall x \in A : e \circ x = x \circ e = x$.

Poznámka 1.9. Rovnice, které mají tvar $t_1(x, y, z, \ldots) = t_2(x, y, z, \ldots)$ s vhodnými termy t_1, t_2 a musejí být splněny pro všechny prvky nosné množiny uvažované algebry (např. „$\forall x \in A : e \circ x = x$“), se nazývají *zákony* .

Příklad(y) 1.10. 1) $A = \mathbb{C}$, $\circ = +$, 0 je neutrální prvek; $A = \mathbb{C}$, $\circ = \cdot$, 1 je neutrální prvek.

2) $A = M_n(\mathbb{C})$, $\circ = +$, $\begin{pmatrix} 0 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 0 \end{pmatrix}$ je neutrální prvek; $A = M_n(\mathbb{C})$, $\circ = \cdot$, $\begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}$ je neutrální prvek.

3) $A = M^M$, $\circ =$ složení, id_M (identické zobrazení) je neutrální prvek.

4) $A = \mathcal{P}(M)$, $\circ = \cap$, M je neutrální prvek; $A = \mathcal{P}(M)$, $\circ = \cup$, $\emptyset$ je neutrální prvek.

Věta 1.11. *Buď $\circ$ binární operace na A, e_1 levý neutrální prvek a e_2 pravý neutrální prvek. Potom platí: $e_1 = e_2$, a $e_1 (= e_2)$ je neutrální prvek.*

Důsledek 1.12. *Existuje nejvýše jeden neutrální prvek.*

Neutrální prvek se v případě multiplikativního značení obvykle nazývá *jednotkovým prvkem* a značí symbolem 1. V případě aditivního značení se neutrální prvek obvykle nazývá *nulovým prvkem* a značí symbolem 0.

Definice 1.13. Buď A množina, $\circ$ binární operace, e neutrální prvek, $x \in A$. Potom nazýváme prvek $y \in A$ a) *levým inverzním prvkem* k $x :\Leftrightarrow y \circ x = e$, b) *pravým inverzním prvkem* k $x :\Leftrightarrow x \circ y = e$, c) *inverzním prvkem* k $x :\Leftrightarrow x \circ y = y \circ x = e$.

Příklad(y) 1.14.

Množina	Operace	Prvek	Inverzní prvek
$\mathbb{C}$	$+$	x	$-x$
$\mathbb{C}$	$\cdot$	$x \neq 0$	$1/x$
$M_n(\mathbb{C})$	$+$	(a_{ij})	$(-a_{ij})$
$M_n(\mathbb{C})$	$\cdot$	(a_{ij}) s $\det(a_{ij}) \neq 0$	$(a_{ij})^{-1}$
M^M	$\circ$	bijektivní f	f^{-1}
$\mathcal{P}(M)$	$\cap$	M	M
$\mathcal{P}(M)$	$\cup$	$\emptyset$	$\emptyset$
$\mathbb{Z}$	$\cdot$	± 1	± 1

Definice 1.15. Prvek x se nazývá *invertibilní* $:\Leftrightarrow$ existuje inverzní prvek k x.

Definice 1.16. Buď A množina, $\circ$ binární operace na A. $\circ$ se nazývá *asociativní* $:\Leftrightarrow \forall x, y, z \in A : (x \circ y) \circ z = x \circ (y \circ z)$ (*asociativní zákon*) .

Příklad(y) 1.17. Operace $+, \cdot$ na $\mathbb{C}$ a $M_n(\mathbb{C})$ jsou asociativní, stejně tak $\circ$ na M^M a $\cap, \cup$ na $\mathcal{P}(M)$. Naproti tomu operace $-, \div$ obecně *nejsou* asociativní!

Věta 1.18. *Buď $\circ$ asociativní binární operace na A, $x \in A$, y_1 levý inverzní prvek k x, y_2 pravý inverzní prvek k x. Potom platí $y_1 = y_2$.*

Důkaz. $y_2 = e \circ y_2 = (y_1 \circ x) \circ y_2 = y_1 \circ (x \circ y_2) = y_1 \circ e = y_1$. □

Důsledek 1.19. *Je-li operace asociativní, existuje ke každému prvku nejvýše jeden inverzní prvek.*

Způsob označení pro inverzní prvek k x: x^{-1} při multiplikativním značení a $-x$ při aditivním značení (při aditivním značení se místo pojmu inverzní prvek používá také pojem *opačný* prvek).

Definice 1.20. Binární operace $\circ$ se nazývá *operací s dělením* na $A :\Leftrightarrow \forall (a, b) \in A^2 \; \exists (x, y) \in A^2 : a \circ x = b$ (*levý zákon o dělení*) $\wedge \; y \circ a = b$ (*pravý zákon o dělení*).

Věta 1.21. *Buď $A \neq \emptyset$ a $\circ$ asociativní binární operace na A. Potom jsou následující tvrzení ekvivalentní:*

a) $\circ$ je operace s dělením na A.

b) Existuje neutrální prvek e (vzhledem k $\circ$) a každý prvek $x \in A$ je invertibilní, tzn. $\exists y \in A : x \circ y = y \circ x = e$.

Důkaz. b) $\Rightarrow$ a): Pro $x \in A$ nechť x^{-1} značí prvek inverzní k prvku x a nechť $a, b \in A$. Potom platí $a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b$ a $(b \circ a^{-1}) \circ a = b \circ (a^{-1} \circ a) = b \circ e = b$.

a) $\Rightarrow$ b): Nechť $a \in A$ je libovolné ale pevné. Potom platí: $\exists e_1, e_2 \in A : e_1 \circ a = a = a \circ e_2$ (položme $b = a, y = e_1, x = e_2$). Pro libovolné $b \in A$ pak platí:

$$\exists x \in A : b = a \circ x \Rightarrow e_1 \circ b = e_1 \circ (a \circ x) = (e_1 \circ a) \circ x = a \circ x = b,$$
$$\exists y \in A : b = y \circ a \Rightarrow b \circ e_2 = (y \circ a) \circ e_2 = y \circ (a \circ e_2) = y \circ a = b.$$

Tedy je e_1 levý jednotkový prvek, e_2 pravý jednotkový prvek, a proto $e_1 = e_2 =: e$ jednotkový prvek.

Nyní ještě musíme ukázat, že ke každému $x \in A$ existuje inverzní prvek y. Jelikož je $\circ$ operace s dělením, platí:

$$\exists y_1, y_2 \in A : x \circ y_1 = e \wedge y_2 \circ x = e.$$

Tedy je y_1 pravý inverzní prvek a y_2 levý inverzní prvek k x, odkud plyne $y_1 = y_2 =: y$. Proto je y inverzní prvek k x. □

Poznámka 1.22. Je-li $\circ$ asociativní binární operace s dělením na neprázdné množině, pak podle předchozí věty mají rovnice $a \circ x = b$ a $y \circ a = b$ právě jedno řešení x, y. Ze vztahu $a \circ x_1 = b = a \circ x_2$ plyne totiž $a^{-1} \circ (a \circ x_1) = a^{-1} \circ (a \circ x_2)$ a odtud (pomocí asociativního zákona) $x_1 = x_2$. Analogicky pro druhou rovnici.

Definice 1.23. Binární operace $\circ$ na A se nazývá *operací s krácením* $:\Leftrightarrow \forall a, x_1, x_2, y_1, y_2 \in A : (a \circ x_1 = a \circ x_2 \Rightarrow x_1 = x_2)$ (*levý zákon o krácení*) $\wedge (y_1 \circ a = y_2 \circ a \Rightarrow y_1 = y_2)$ (*pravý zákon o krácení*) .

Rovnice $a \circ x = b$ a $y \circ a = b$ mají tedy při operaci $\circ$ s krácením *nejvýše* jedno řešení a při asociativní operaci $\circ$ s dělením *přesně* jedno řešení.

V tabulce operace: s krácením $\Leftrightarrow$ každý řádek (sloupec) obsahuje každý prvek *nejvýše* jedenkrát, s dělením $\Leftrightarrow$ každý řádek (sloupec) obsahuje každý prvek *nejméně* jednou.

Pro konečnou množinu A platí: $\circ$ je operace s dělením $\Leftrightarrow$ $\circ$ je operace s krácením (Cvičení).

Podle výše uvedené poznámky platí: $\circ$ je asociativní operace s dělením $\Rightarrow$ $\circ$ je operace s krácením.

Příklad(y) 1.24. Operace $+, \cdot$ na $\mathbb{N}$ jsou s krácením, ale *nikoliv* s dělením.

Definice 1.25. Binární operace $\circ$ na A se nazývá *komutativní* $:\Leftrightarrow \forall x, y \in A : x \circ y = y \circ x$ (*komutativní zákon*) .

Příklad(y) 1.26. Následující operace *nejsou* komutativní: $-$ na $\mathbb{C}$, $\div$ na $\mathbb{C} \setminus \{0\}$, $\cdot$ na $M_n(\mathbb{C})$ pro $n \geq 2$, $\circ$ na M^M pro $|M| \geq 2$.

Definice 1.27. Pokud jsou $+, \cdot$ binární operace na A, potom se $\cdot$ nazývá *distributivní nad* $+ :\Leftrightarrow \forall x, y, z \in A : x \cdot (y + z) = x \cdot y + x \cdot z$ (*levý distributivní zákon*) $\wedge$ $(y + z) \cdot x = y \cdot x + z \cdot x$ (*pravý distributivní zákon*) .

Poznámka 1.28. Kvůli úspoře závorek se řídíme konvencí, při které výpočet operace $\cdot$ se provede před výpočtem operace $+$.

Příklad(y) 1.29. Operace $\cdot$ je distributivní nad $+$ v $\mathbb{C}$, $M_n(\mathbb{C})$. V $\mathcal{P}(M)$ je $\cup$ distributivní nad $\cap$ a $\cap$ je distributivní nad $\cup$.

1.2 Některé důležité typy algeber

Definice 1.30. Algebra $(A, \cdot)$ typu (2) se nazývá *grupoid* .

Definice 1.31. Grupoid $(H, \cdot)$ se nazývá *pologrupa* $:\Leftrightarrow$ $\cdot$ je asociativní.

Příklad(y) 1.32. $(M^M, \circ)$ je pologrupa, tzv. *symetrická* pologrupa nad M.

Definice 1.33. a) Pologrupa $(H, \cdot)$ se nazývá *monoid* typu (2) $:\Leftrightarrow$ existuje neutrální prvek e.

b) Algebra $(H, \cdot, e)$ typu $(2, 0)$ se nazývá *monoid* typu $(2, 0) :\Leftrightarrow$ platí následující zákony pro všechna $x, y, z \in H$:

1) $x(yz) = (xy)z$,

2) $ex = x$, $xe = x$.

Definice 1.34. a) Monoid $(G, \cdot)$ s neutrálním prvkem e se nazývá *grupa* typu (2) $:\Leftrightarrow$ každý prvek $x \in G$ je invertibilní, tj., $\forall x \in G\ \exists x^{-1} \in G : xx^{-1} = x^{-1}x = e$.

b) Algebra $(G, \cdot, e, {}^{-1})$ typu $(2, 0, 1)$ se nazývá *grupa* typu $(2, 0, 1) :\Leftrightarrow$ platí následující zákony pro všechna $x, y, z \in G$:

1) $x(yz) = (xy)z$,
2) $ex = x$, $xe = x$,
3) $xx^{-1} = e$, $x^{-1}x = e$.

c) Grupa $(G, \cdot)$, resp. $(G, \cdot, e, {}^{-1})$ se nazývá *komutativní* nebo *abelovská* $:\Leftrightarrow \forall x, y \in G : xy = yx$.

Poznámka 1.35. $(G, \cdot)$ je grupa $\Leftrightarrow G \neq \emptyset$ a $\cdot$ je asociativní operace s dělením.

Definice 1.36. a) Algebra $(R, +, \cdot)$ typu $(2, 2)$ se nazývá *okruh* typu $(2, 2) :\Leftrightarrow$

1) $(R, +)$ je abelovská grupa,
2) $(R, \cdot)$ je pologrupa,
3) $\cdot$ je distributivní nad $+$.

b) Algebra $(R, +, 0, -, \cdot)$ typu $(2, 0, 1, 2)$ se nazývá *okruh* typu $(2, 0, 1, 2) :\Leftrightarrow$

1) $(R, +, 0, -)$ je abelovská grupa,
2) $(R, \cdot)$ je pologrupa,
3) $\cdot$ je distributivní nad $+$.

Prvek 0 se nazývá „nulový prvek“ okruhu. Budeme psát $x - y := x + (-y)$.

Lemma 1.37. *Buď $(R, +, 0, -, \cdot)$ okruh. Potom platí pro všechna $x, y, z \in R$:*

a) $x0 = 0 = 0x$,

b) $x(-y) = (-x)y = -(xy)$,

c) $(-x)(-y) = xy$,

d) $x(y-z) = xy - xz$, $(x-y)z = xz - yz$.

Důkaz. a) $0 = 0 + 0 \Rightarrow x0 = x(0+0) = x0 + x0 \Rightarrow x0 - x0 = x0 + x0 - x0 \Rightarrow 0 = x0$. Analogicky pro $0 = 0x$.

b) $y + (-y) = 0 \Rightarrow xy + x(-y) = x0 = 0 \Rightarrow xy + (-(xy)) + x(-y) = 0 + (-(xy)) \Rightarrow x(-y) = -(xy)$. Analogicky pro $(-x)y = -(xy)$.

c) Plyne z b) a $-(-x) = x$.

d) $x(y-z) = x(y+(-z)) = xy + x(-z) = xy + (-(xz)) = xy - xz$ podle b). Analogicky pro $(x-y)z = xz - yz$. □

Příklad(y) 1.38. $(\mathbb{Z}, +, 0, -, \cdot)$ a $(M_n(\mathbb{C}), +, 0, -, \cdot)$ jsou okruhy.

Definice 1.39. a) Algebra $(R, +, 0, -, \cdot, 1)$ typu $(2, 0, 1, 2, 0)$ se nazývá *okruh s jednotkovým prvkem* $:\Leftrightarrow$

1) $(R, +, 0, -, \cdot)$ je okruh,
2) 1 je neutrální prvek vzhledem k $\cdot$, tj. $\forall x \in R : 1 \cdot x = x \cdot 1 = x$ (1 se nazývá *jednotkový prvek* okruhu).

b) Okruh $(R, +, 0, -, \cdot)$ se nazývá *komutativní* $:\Leftrightarrow \forall x, y \in R : xy = yx$.

c) Algebra $(R, +, 0, -, \cdot, 1)$ se nazývá *komutativní okruh s jednotkovým prvkem* $:\Leftrightarrow$

1) $(R, +, 0, -, \cdot)$ je komutativní okruh,
2) 1 je neutrální prvek vzhledem k $\cdot$.

Příklad(y) 1.40. $(\mathbb{Z}, +, 0, -, \cdot, 1)$ je komutativní okruh s jednotkovým prvkem; stejně tak kažzdé pole (viz níže).

Definice 1.41. Komutativní okruh s jednotkovým prvkem $(R, +, 0, -, \cdot, 1)$ se nazývá *obor integrity* $:\Leftrightarrow$

1) $R \setminus \{0\} \neq \emptyset$ (tj. $0 \neq 1$),
2) $\forall x, y \in R : x \neq 0 \wedge y \neq 0 \Rightarrow xy \neq 0$ (tj. neexistují dělitelé nuly).

Lemma 1.42. *Je-li* $(R, +, 0, -, \cdot, 1)$ *obor integrity, potom je* $\cdot$ *operace s krácením na* $R \setminus \{0\}$.

Důkaz. Buďte $x, y, z \neq 0$. Potom platí: $xy = xz \Rightarrow xy - xz = 0 \Rightarrow x(y-z) = 0 \Rightarrow y - z = 0 \Rightarrow y = z$. □

Poznámka 1.43. V oboru integrity je $(R \setminus \{0\}, \cdot, 1)$ komutativní monoid.

Příklad(y) 1.44. $(\mathbb{Z}, +, 0, -, \cdot, 1)$ je obor integrity.

Definice 1.45. a) Okruh s jednotkovým prvkem $(R, +, 0, -, \cdot, 1)$ se nazývá *těleso* $:\Leftrightarrow$

1) $0 \neq 1$,
2) $(R \setminus \{0\}, \cdot)$ je grupa.

b) Komutativní těleso se nazývá *pole* .

Tedy komutativní okruh s jednotkovým prvkem $(R, +, 0, -, \cdot, 1)$ je pole $\Leftrightarrow$

1) $0 \neq 1$,

2) $(R \setminus \{0\}, \cdot)$ je abelovská grupa.

Příklad(y) 1.46. 1) $(\mathbb{Q}, +, 0, -, \cdot, 1)$, $(\mathbb{R}, +, 0, -, \cdot, 1)$, $(\mathbb{C}, +, 0, -, \cdot, 1)$ jsou pole.

2)) Bez důkazu: každé konečné těleso je pole (věta Wedderburnova) .

3) Je-li p prvočíslo, potom je $(\mathbb{Z}_p, +, 0, -, \cdot, 1)$ pole (s p prvky). (K přesnější definici okruhu zbytkových tříd $(\mathbb{Z}_n, +, 0, -, \cdot, 1)$ modulo n viz odstavec 2.4.)

Poznámka 1.47. $\mathbb{Z}_n$ je pole $\Leftrightarrow$ n je prvočíslo $\Leftrightarrow$ $\mathbb{Z}_n$ je obor integrity (viz odstavec 2.4).

Věta 1.48. *Každé pole je obor integrity. Každý konečný obor integrity je pole.*

Důkaz. Nechť $x \neq 0$, $y \neq 0$ a $xy = 0$. Pak $x^{-1}(xy)y^{-1} = 1 = 0$, což je spor.

Buď nyní $R = \{a_1, \ldots, a_n\}$ konečný obor integrity. Pak $\cdot$ je asociativní operace s krácením na konečné množině $R \setminus \{0\}$. Proto je $\cdot$ operace s dělením, tedy $(R \setminus \{0\}, \cdot)$ je abelovská grupa. □

Definice 1.49. Buď $(K, +, 0, -, \cdot, 1)$ pole, $I = \{a, b, c\} \cup K$, kde $a, b, c \notin K$, a, b, c po dvou různé. Algebra $(V, (\omega_i)_{i \in I})$ typu $(2, 0, 1, (1)_{\lambda \in K})$ se nazývá *vektorový prostor nad* K :$\Leftrightarrow$

1) $(V, \omega_a, \omega_b, \omega_c) =: (V, +, 0, -)$ je abelovská grupa,

2) $\forall x, y \in V, \lambda, \mu \in K$:
$\omega_\lambda(x + y) = \omega_\lambda(x) + \omega_\lambda(y)$,
$\omega_{\lambda+\mu}(x) = \omega_\lambda(x) + \omega_\mu(x)$,
$\omega_{\lambda\mu}(x) = \omega_\lambda(\omega_\mu(x))$,
$\omega_1(x) = x$.

V dalším textu polžíme $\omega_\lambda =: \lambda$ a budeme zapisovat vektorový prostor jako $(V, +, 0, -, K)$. Zákony uvedené v bodě 2) pak mají tvar: $\lambda(x + y) = \lambda x + \lambda y$, $(\lambda + \mu)x = \lambda x + \mu x$, $(\lambda\mu)x = \lambda(\mu x)$, $1x = x$.

Definice 1.50. Algebra $(V, \cap, \cup)$ typu $(2, 2)$ se nazývá *svaz* :$\Leftrightarrow$ pro všechna $a, b, c \in V$ platí:

1) $a \cap b = b \cap a$, $a \cup b = b \cup a$,

2) $a \cap (b \cap c) = (a \cap b) \cap c$, $a \cup (b \cup c) = (a \cup b) \cup c$,

3) $a \cap (a \cup b) = a$, $a \cup (a \cap b) = a$.

Podle 1) a 2) jsou $\cap$ a $\cup$ kommutativní a asociativní, tj. $(V, \cap)$ a $(V, \cup)$ jsou komutativní pologrupy. Zákony uvedené v bodě 3) se nazývají *absorbční zákony* .

Příklad(y) 1.51. $(\mathcal{P}(M), \cap, \cup)$ je svaz.

Poznámka 1.52. $(V, \cap, \cup)$ je svaz $\Leftrightarrow$ $(V, \cup, \cap)$ je svaz. Zákony jsou symetrické v $\cap$ a $\cup$ – tzv. *princip duality* pro svazy .

Definice 1.53. Svaz $(V, \cap, \cup)$ se nazývá *distributivní* $:\Leftrightarrow$ pro všechna $a, b, c \in V$ platí:

4) $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$, $a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$

(tj. $\cap$ je distributivní nad $\cup$ a $\cup$ je distributivní nad $\cap$).

Poznámka 1.54. $(V, \cap, \cup)$ je distributivní svaz $\Leftrightarrow$ $(V, \cup, \cap)$ je distributivní svaz (princip duality). Dokonce platí, že $\cap$ je distributivní nad $\cup$, právě když $\cup$ je distributivní nad $\cap$.

Příklad(y) 1.55. $(\mathcal{P}(M), \cap, \cup)$ je distributivní svaz.

Definice 1.56. Buď $(V, \cap, \cup)$ svaz. Prvek $0 \in V$ se nazývá *nulový prvek* svazu $V :\Leftrightarrow \forall a \in V : a \cup 0 = a$ (tj. 0 je neutrální vzhledem k $\cup$). Prvek $1 \in V$ se nazývá *jednotkový prvek* svazu $V :\Leftrightarrow \forall a \in V : 1 \cap a = a$ (tj. 1 je neutrální vzhledem k $\cap$).

Poznámka 1.57. Buďte $b, c \in V$, libovolné prvky. Pak platí $\forall a \in V : a \cup b = a \Leftrightarrow \forall a \in V : a \cap b = b$, $\forall a \in V : c \cap a = a \Leftrightarrow \forall a \in V : c \cup a = c$.

Definice 1.58. Algebra $(V, \cap, \cup, 0, 1)$ typu $(2, 2, 0, 0)$ se nazývá *ohraničený svaz* $:\Leftrightarrow$

1) $(V, \cap, \cup)$ je svaz,

2) 0 je nulový prvek svazu V,

3) 1 je jednotkový prvek svazu V.

Příklad(y) 1.59. $(\mathcal{P}(M), \cap, \cup, \emptyset, M)$ je ohraničený svaz.

Definice 1.60. Ohraničený svaz $(V, \cap, \cup, 0, 1)$ se nazývá *komplementární* $:\Leftrightarrow \forall a \in V\ \exists a' \in V : a \cap a' = 0 \wedge a \cup a' = 1$. Prvek a' se nazývá *komplement* prvku a.

Příklad(y) 1.61. $(\mathcal{P}(M), \cap, \cup, \emptyset, M)$ je komplementární svaz, přičemž pro $A \subseteq M$ je komplement dán vztahem $A' = M \setminus A$.

Definice 1.62. Distributivní a komplementární svaz $(V, \cap, \cup, 0, 1)$ se nazývá *Booleův svaz* .

Příklad(y) 1.63. $(\mathcal{P}(M), \cap, \cup, \emptyset, M)$ je Booleův svaz.

Věta 1.64. *Je-li* $(V, \cap, \cup, 0, 1)$ *Booleův svaz, pak existuje ke každému* $a \in V$ *přesně jeden komplement* a'.

Důkaz. Buďte a' a a^* komplementy prvku a. Pak platí $a \cup a' = 1 = a \cup a^*$, $a \cap a' = 0 = a \cap a^*$, a tudíž $a' = a' \cup 0 = a' \cup (a \cap a^*) = (a' \cup a) \cap (a' \cup a^*) = 1 \cap (a' \cup a^*) = a' \cup a^* = a^* \cup a' = \ldots = a^*$. □

Definice 1.65. Algebra $(B, \cap, \cup, 0, 1, ')$ typu $(2, 2, 0, 0, 1)$ se nazývá *Booleova algebra* $:\Leftrightarrow$

1) $(B, \cap, \cup, 0, 1)$ je ohraničený distributivní svaz,

2) $\forall a \in B : a \cap a' = 0 \wedge a \cup a' = 1$.

Poznámka 1.66. $(B, \cap, \cup, 0, 1, ')$ je Booleova algebra $\Rightarrow$ $(B, \cap, \cup, 0, 1)$ je Booleův svaz. Pokud naopak $(B, \cap, \cup, 0, 1)$ je Booleův svaz a a' (jednoznačně určený) komplement prvku a, pak je $(B, \cap, \cup, 0, 1, ')$ Booleova algebra.

Příklad(y) 1.67. $(\mathcal{P}(M), \cap, \cup, \emptyset, M, ')$ je Booleova algebra.

1.3 Základní pojmy teorie grup

Definice 1.68. Buď $(G, \cdot)$ grupoid, $a_1, \ldots, a_n \in G$ $(n \in \mathbb{N})$. Potom je *součin* $a_1 \cdots a_n$ definován indukcí vztahem $a_1 \cdots a_n := (a_1 \cdots a_{n-1})a_n$.

Příklad(y) 1.69. $a_1a_2a_3a_4 = (a_1a_2a_3)a_4 = ((a_1a_2)a_3)a_4$.

Definice 1.70. Buď $(G, \cdot)$ grupoid, $a \in G$. Potom jsou *mocniny* prvku a definovány takto: $a^1 := a$, $a^{n+1} := (a^n)a$ $(n \in \mathbb{N})$.

Poznámka 1.71. 1) Při počítání se součiny v pologrupě je možno libovolně závorkovat (Cvičení).

2) V komutativní pologrupě platí: $a_1 \cdots a_n = a_{\pi(1)} \cdots a_{\pi(n)}$, přičemž π je libovolná permutace množiny $M = \{1, \ldots, n\}$.

Věta 1.72. *Buď $(G, \cdot, e, {}^{-1})$ grupa, $a, b \in G$. Potom platí $(ab)^{-1} = b^{-1}a^{-1}$.*

Důkaz. $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1} = e$. □

Důsledek 1.73. $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$.

Důkaz. Indukcí podle n. □

Definice 1.74. Buď $(G, \cdot, e, {}^{-1})$ grupa, $a \in G$. Pro $n \in \mathbb{N}$ buď a^n jak je definováno výše. Dále klademe $a^0 := e$ a $a^{-n} := (a^{-1})^n$, $n \in \mathbb{N}$.

Věta 1.75. *(Pravidla pro počítání s mocninami v grupách) Pro všechna $a, b \in G$, $n, m \in \mathbb{Z}$ platí:*

1) $a^n a^m = a^{n+m}$,

2) $(a^m)^n = a^{mn}$,

3) $(ab)^n = a^n b^n$, *pokud je $\cdot$ komutativní.*

Důkaz. Rozlišíme jednotlivé případy. Např. 2) pro $n > 0$:

$$(a^m)^n = \underbrace{a^m \cdots a^m}_{n\text{-krát}} = a^{\overbrace{m+\cdots+m}^{n\text{-krát}}} = a^{nm}.$$

□

Poznámka 1.76. Tato pravidla platí pro $m, n \in \mathbb{N}$ také v pologrupách.

Definice 1.77. Buď $(G, \cdot, e, {}^{-1})$ grupa, $a \in G$. Potom se kardinální číslo

$$\mathrm{o}(a) := |\{a^0 = e, a^1, a^{-1}, a^2, a^{-2}, \ldots\}| = |\{a^k \mid k \in \mathbb{Z}\}|$$

nazývá *řád* prvku a.

Poznámka 1.78. $\mathrm{o}(a) \in \mathbb{N}$ nebo $\mathrm{o}(a) = |\mathbb{N}| = \aleph_0 (= \infty)$.

Příklad(y) 1.79. 1) V $(\mathbb{Z}, +, 0, -)$ píšeme (stejně tak ve všech grupách s aditivním značením) na místo a^n. Výše uvedená pravidla pak mají následující tvar: (i) $ma + na = (m + n)a$, (ii) $n(ma) = (mn)a$, (iii) $n(a+b) = na+nb$. Platí $\mathrm{o}(0) = 1$, $\mathrm{o}(k) = \infty$ pro všechna $k \in \mathbb{Z}$, $k \neq 0$. (V každé grupě platí $\mathrm{o}(e) = 1$.)

2) V grupě $(\mathbb{C} \setminus \{0\}, \cdot, 1, ^{-1})$ platí: $\mathrm{o}(1) = 1$, $\mathrm{o}(-1) = 2$, $\mathrm{o}(i) = \mathrm{o}(-i) = 4$.

Definice 1.80. Buď $(G, \cdot, e, ^{-1})$ grupa. Potom se $|G|$ (mohutnost množiny G) nazývá *řád* této grupy. Obecně se pro algebru $(A, (\omega_i)_{i\in I})$ mohutnost $|A|$ nazývá *řád* této algebry.

Pro všechna $a \in G$ platí: $\mathrm{o}(a) \leq |G|$.

Lemma 1.81. *(Dělení se zbytkem)* $\forall k, l \in \mathbb{Z}, l \neq 0\ \exists q, r \in \mathbb{Z} : 0 \leq r < |l| \wedge k = lq + r$.

Důkaz. Případ 1: $k \geq 0$. Určitě existuje $n \in \mathbb{N}$ tak, že $|l|n \geq k$ (Archimedův axiom pro $\mathbb{R}$). Buď $q^* := \max\{n \in \mathbb{N}_0 \mid |l|n \leq k\}$ a $q := q^*$ pro $l > 0$, $q := -q^*$ pro $l < 0$. Potom je $k = lq + r$, kde $0 \leq r < |l|$.

Případ 2: $k < 0$ – důkaz se provede podobně. □

Definice 1.82. Pro $n \in \mathbb{N}$, $r, s \in \mathbb{Z}$ je $r \equiv s \bmod n$ („r je kongruentní s s modulo n“) :$\Leftrightarrow$ $n|(r - s)$ (n dělí $(r - s)$).

Platí:

1) $r \equiv s \bmod n \Leftrightarrow r = s + kn$, $k \in \mathbb{Z} \Leftrightarrow r, s$ mají stejný zbytek při dělení číslem n.

2) $\equiv \bmod n$ je relace ekvivalence (viz později).

Věta 1.83. *Buď $(G, \cdot, e, ^{-1})$ grupa, $a \in G$.*

a) Je-li $\mathrm{o}(a) = \infty$, pak jsou mocniny prvku a navzájem různé.

b) Je-li $\mathrm{o}(a) = n \in \mathbb{N}$, potom platí $n = \min\{m \in \mathbb{N} \mid a^m = e\}$ a $\{a^k \mid k \in \mathbb{Z}\} = \{a^0 = e, a^1, \ldots, a^{n-1}\}$. Dále je $a^r = a^s \Leftrightarrow r \equiv s \bmod n$.

Důkaz. a) Buď $\mathrm{o}(a) = \infty$ a předpokládejme, že $\exists r, s \in \mathbb{Z} : r > s \wedge a^r = a^s$. Pro $m := r-s \in \mathbb{N}$ pak platí $a^m = e$. Buď $k \in \mathbb{Z}$. Potom je $k = mq + l$, $q \in \mathbb{Z}$, $l \in \mathbb{N}_0$ a $0 \leq l < m$. Odtud plyne $a^k = a^{mq+l} = (a^m)^q a^l = e^q a^l = a^l$, tedy $\{a^k \mid k \in \mathbb{Z}\} = \{e, a, \ldots, a^{m-1}\}$. To je spor, neboť $\mathrm{o}(a) = \infty$.

b) Je-li $\mathrm{o}(a) = n \in \mathbb{N}$, potom podle a) existuje $m \in \mathbb{N}$ takové, že $a^m = e$, což dává $\{a^k \mid k \in \mathbb{Z}\} = \{e, a, \ldots, a^{m-1}\}$. Buď $n_0 = \min\{m \in \mathbb{N} \mid a^m = e\}$. Potom je $a^{n_0} = e$ a prvky $e, a, \ldots, a^{n_0-1}$ jsou po dvou různé. Pokud by totiž tomu tak nebylo, potom by platilo $a^r = a^s$ pro $0 \leq s < r < n_0$. Tedy bychom měli $a^{r-s} = e$ pro $0 < r - s < n_0$, což je spor s minimalitou čísla n_0. Proto platí $n = n_0$. Takže máme $\{a^k \mid k \in \mathbb{Z}\} = \{e, a, \ldots, a^{n-1}\}$.

Dokážeme teď ještě, že $a^r = a^s \Leftrightarrow r \equiv s \bmod n$.

$\Rightarrow$: $a^r = a^s \Rightarrow a^{r-s} = e$, $r - s = nq + l$, $0 \leq l < n \Rightarrow e = a^{r-s} = (a^n)^q a^l = e^q a^l = a^l \Rightarrow l = 0$ $\Rightarrow r - s = nq \Rightarrow r \equiv s \bmod n$.
$\Leftarrow$: $r \equiv s \bmod n \Rightarrow r - s = nq \Rightarrow a^{r-s} = a^{nq} = (a^n)^q = e \Rightarrow a^r = a^s$. □

Příklad(y) 1.84. Buď M množina a $S_M := \{f : M \to M \mid f \text{ bijektivní}\}$. $(S_M, \circ, \mathrm{id}_M, {}^{-1})$ je grupa, která se nazývá *symetrická grupa na* M (Cvičení). Prvky množiny S_M se nazývají *permutace* množiny M. Je-li $M = \{1, 2, \ldots, n\}$, píšeme S_n místo S_M. Platí: $|S_n| = n!$. Je tedy např.

$$S_3 = \left\{ \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix} \right\},$$

používáme-li *cyklický zápis* :

$$S_3 = \{(1), (123), (132), (23), (13), (12)\}.$$

Připomeňme, že permutace $f : M \to M$ je sudá (lichá), má-li sudý (lichý) počet inverzí, tj. dvojic prvků $x, y \in M$ takových, že $x < y$ a $f(x) > f(y)$. Snadno se ukáže, že parita permutace je rovna paritě počtu jejich cyklů sudé délky. Sudé permutace tvoří tzv. *alternující* grupu A_n. V našem případě je množina sudých permutací

$$A_3 = \{(1), (123), (132)\}.$$

Řády prvků grupy S_3:

π	$\mathrm{o}(\pi)$
(1)	1
(123)	3
(132)	3
(23)	2
(13)	2
(12)	2

Platí: Každý prvek grupy S_n je možno vyjádřit jako součin (tj. složení) cyklů s různými prvky . Toto vyjádření je až na pořadí cyklů jednoznačné. Např. permutace

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 9 & 8 & 5 & 4 & 1 & 3 & 2 & 7 \end{pmatrix}$$

z grupy S_9 má cyklické vyjádření $(16)(29738)(45)$. Platí $\mathrm{o}(\pi) = 2 \cdot 5 = \mathrm{NSN}(2, 5, 2)$. Řád součinu cyklů s různými prvky je nejmenší společný násobek délek všech činitelů (tj. řádů všech činitelů, protože každý cyklus je permutací množiny všech prvků, které obsahuje, a jeho řád je stejný jako jeho délka).

Kapitola 2

Základní algebraické metody

2.1 Podalgebry

Definice 2.1. Buď A množina, $\omega : A^n \to A$ n-ární operace na A ($n \in \mathbb{N}_0$), $T \subseteq A$. Potom se množina T nazývá *uzavřená* vzhledem k $\omega :\Leftrightarrow \omega(T^n) \subseteq T$ (tj. $t_1, \ldots, t_n \in T \Rightarrow \omega t_1 \ldots t_n \in T$; v případě $n = 0$: $\omega \in T$).

Definice 2.2. Buď $\mathcal{A} = (A, (\omega_i)_{i\in I})$ algebra typu $(n_i)_{i\in I}$, $T \subseteq A$. Potom se množina T nazývá *uzavřená* vzhledem k $(\omega_i)_{i\in I} :\Leftrightarrow T$ je uzavřená vzhledem k ω_i pro všechna $i \in I$. V tomto případě se pomocí vztahu $\omega_i^* x_1 \ldots x_{n_i} := \omega_i x_1 \ldots x_{n_i}$, $(x_1, \ldots, x_{n_i}) \in T^{n_i}$, definuje n_i-ární operace ω_i^* na T, tj. $\omega_i^* = \omega_i|_{T^{n_i}}$. Algebra $(T, (\omega_i^*)_{i\in I})$ se pak nazývá *podalgebra* algebry $\mathcal{A}$. Většinou píšeme: $\omega_i^* =: \omega_i$.

Poznámka 2.3. Často také nazýváme podalgebrou algebry $\mathcal{A}$ pouze množinu T.

Podalgebry speciálních algebraických struktur

1) Buď $(H, \cdot)$ pologrupa. $T \subseteq H$ je podalgebrou algebry $(H, \cdot) \Leftrightarrow (x, y \in T \Rightarrow xy \in T)$. Pak je $\cdot = \cdot|_{T\times T}$ binární operace na T a $(T, \cdot)$ je pologrupa, neboť asociativní zákon platí v H, a tedy i v T. (Obecně: Je-li v algebře definovaná vlastnost nějaké operace pomocí nějakého *zákona*, pak má tato operace zúžená na některou podalgebru tuto vlastnost přirozeně také.)

   $(T, \cdot)$ se nazývá *podpologrupa* pologrupy $(H, \cdot)$.

2) 2) Buď $(G, \cdot)$ grupa typu (2) a $(T, \cdot)$ podpologrupa pologrupy $(G, \cdot)$. Potom *není* obecně $(T, \cdot)$ grupa!

   Příklad(y) 2.4. $(G, \cdot) = (\mathbb{Z}, +)$, $(T, \cdot) = (\mathbb{N}, +)$.

3) Buď $(G, \cdot, e, {}^{-1})$ grupa typu $(2, 0, 1)$. $T \subseteq G$ je podalgebra

$$\Leftrightarrow \left\{ \begin{array}{l} x, y \in T \Rightarrow xy \in T \\ e \in T \\ x \in T \Rightarrow x^{-1} \in T \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} T \neq \emptyset \\ x, y \in T \Rightarrow xy^{-1} \in T \end{array} \right\}.$$

   Protože zákony grupy typu $(2, 0, 1)$ platí v G, a tedy také v T, je podalgebra $(T, \cdot, e, {}^{-1})$ opět grupou a nazývá se *podgrupa* grupy $(G, \cdot, e, {}^{-1})$.

4) 4) Je-li $(R, +, 0, -, \cdot)$ okruh typu $(2, 0, 1, 2)$, potom je podalgebra $(T, +, 0, -, \cdot)$ opět okruhem a nazývá se *podokruh* okruhu $(R, +, 0, -, \cdot)$. To neplatí pro okruhy typu $(2, 2)$.

   Příklad(y) 2.5. $(\mathbb{N}, +, \cdot)$ je *podalgebrou* $(\mathbb{Z}, +, \cdot)$, ale nikoliv *podokruhem.*

5) Buď $(K, +, 0, -, \cdot, 1)$ pole typu $(2, 0, 1, 2, 0)$ a $(T, +, 0, -, \cdot, 1)$ podalgebra (tj. podokruh se stejným jednotkovým prvkem). Je-li $(T, +, 0, -, \cdot, 1)$ samotná polem, pak se nazývá *podpole* pole $(K, +, 0, -, \cdot, 1)$. Platí: T je podpole

$$\Leftrightarrow \begin{cases} x, y \in T \Rightarrow x + y \in T \\ 0 \in T \\ x \in T \Rightarrow -x \in T \\ x, y \in T \Rightarrow xy \in T \\ 1 \in T \\ x \in T, x \neq 0 \Rightarrow x^{-1} \in T. \end{cases}$$

Příklad(y) 2.6. $(\mathbb{R}, +, 0, -, \cdot, 1)$ je podpolem pole $(\mathbb{C}, +, 0, -, \cdot, 1)$, zatímco $(\mathbb{Z}, +, 0, -, \cdot, 1)$ *není.*

6) Buď $(V, +, 0, -, K)$ vektorový prostor nad K a $(T, +, 0, -, K)$ podalgebra, tj.

$$\begin{array}{l} x, y \in T \Rightarrow x + y \in T \\ 0 \in T \\ x \in T \Rightarrow -x \in T \\ \lambda \in K, x \in T \Rightarrow \lambda x \in T. \end{array}$$

Potom je také $(T, +, 0, -, K)$ vektorový prostor nad K a nazývá se *vektorový podprostor.*

Věta 2.7. *Buď (A, Ω) algebra a $(T_j)_{j \in J}$ soubor podalgeber. Potom je $\bigcap_{j \in J} T_j$ rovněž podalgebra.*

Poznámka 2.8. Průnik, který se vyskytuje v předchozí větě, se definuje pomocí vztahu $\bigcap_{j \in J} T_j := \{x \in A \mid \forall j \in J : x \in T_j\}$. Pro $J = \emptyset$ je $\bigcap_{j \in J} T_j = A$.

Důkaz. Buď $\Omega = (\omega_i)_{i \in I}$, ω_i n_i-ární operace, a $T := \bigcap_{j \in J} T_j$. Buď $i \in I$, přičemž $n_i > 0$, a buďte $x_1, \ldots, x_{n_i} \in T$. Potom platí $\forall j \in J : x_1, \ldots, x_{n_i} \in T_j$, tedy $\forall j \in J$: $\omega_i x_1 \ldots x_{n_i} \in T_j$. Proto $\omega_i x_1 \ldots x_{n_i} \in T$. Pro $n_i = 0$ platí $\forall j \in J : \omega_i \in T_j$, takže $\omega_i \in T$. □

Věta 2.9. *Buď (A, Ω) algebra a $S \subseteq A$ podmnožina. Potom je*

$$\langle S \rangle := \bigcap \{T \mid T \supseteq S,\ T \text{ je podalgebra algebry } (A, \Omega)\}$$

nejmenší podalgebra algebry (A, Ω), která S obsahuje.

Definice 2.10. $\langle S \rangle$ se nazývá *podalgebra algebry (A, Ω) generovaná množinou S* . Množina S se nazývá *systém generátorů* podalgebry $\langle S \rangle$.

Věta 2.11. *Buď $(G, \cdot, e, ^{-1})$ grupa, $x \in G$, $S = \{x\}$. Potom platí:*

$$\langle x \rangle := \langle S \rangle = \{x^k \mid k \in \mathbb{Z}\}.$$

Důkaz. Máme dokázat: $\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\} =: T$.
$\subseteq$: T je podgrupa grupy $(G, \cdot, e, ^{-1})$. Nechť $x^k, x^l \in T$, $k, l \in \mathbb{Z}$. Potom platí $x^k x^l = x^{k+l} \in T$ (jelikož $k + l \in \mathbb{Z}$), $x^0 \in T$ (protože $0 \in \mathbb{Z}$), $(x^k)^{-1} = x^{-k} \in T$ (neboť $-k \in \mathbb{Z}$). Dále platí $x = x^1 \in T$, tedy $\{x\} \subseteq T$, odkud plyne $\langle x \rangle \subseteq T$.
$\supseteq$: Buď U podgrupa grupy $(G, \cdot, e, ^{-1})$, kde $\{x\} \subseteq U$, tj. $x \in U$. Potom platí $x^n \in U$ $(n \in \mathbb{N})$, $e = x^0 \in U$, $x^{-n} = (x^n)^{-1} \in U$, takže $T \subseteq U$. Zejména tedy $T \subseteq \langle x \rangle$. □

Definice 2.12. $\langle x \rangle$ se nazývá *podgrupa grupy* $(G, \cdot, e, ^{-1})$ *generovaná prvkem* x .

Poznámka 2.13. 1) Pro vektorové prostory máme:

$$\langle \{x_1, \ldots, x_n\} \rangle = \{ \sum_{1 \leq i \leq n} \lambda_i x_i \mid \lambda_i \in K \}.$$

2) Je-li $(G, \cdot, e, ^{-1})$ *abelovská* grupa, potom platí:

$$\langle \{x_1, \ldots, x_n\} \rangle = \{x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} \mid k_i \in \mathbb{Z}\}.$$

Vyjádříme-li abelovskou grupu ve tvaru $(G, +, 0, -)$, potom platí:

$$\langle \{x_1, \ldots, x_n\} \rangle = \{k_1 x_1 + k_2 x_2 + \cdots + k_n x_n \mid k_i \in \mathbb{Z}\}.$$

3) Pro *neabelovské* grupy platí např.:

$$\langle \{x_1, x_2\} \rangle = \{x_1^{k_{11}} x_2^{k_{12}} x_1^{k_{21}} x_2^{k_{22}} \cdots x_1^{k_{n1}} x_2^{k_{n2}} \mid n \in \mathbb{N},\, k_{ij} \in \mathbb{Z}\}.$$

4) Obecně platí:

$$\langle \{x_1, \ldots, x_n\} \rangle = \{t(x_1, \ldots, x_n) \mid t \text{ je libovolný } n\text{-ární } \textit{term} \text{ v algebře } (A, \Omega)\}.$$

Definice 2.14. Grupa $(G, \cdot, e, ^{-1})$ se nazývá *cyklická* $:\Leftrightarrow \exists x \in G : G = \langle x \rangle$. Prvek x se pak nazývá *generátor* .

Z Věty 1.83 a Věty 2.11 plyne

Důsledek 2.15. *Buď* $(G, \cdot, e, ^{-1})$ *cyklická grupa a nechť* $\langle x \rangle = G$. *Potom můžeme rozlišit dva případy:*

a) Je-li $\mathrm{o}(x) = \infty$, *potom je také* G *nekonečná a platí* $G = \{e, x, x^{-1}, x^2, x^{-2}, \ldots\}$.

b) Je-li $\mathrm{o}(x) = n \in \mathbb{N}$, *potom máme* $|G| = n$, *a platí* $G = \{e, x, x^2, \ldots, x^{n-1}\}$.

V obou případech jsou uvedené mocniny v dané množině navzájem různé.

Příklad(y) 2.16. K a): pro $(\mathbb{Z}, +, 0, -)$ platí $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

K b): pro $(\mathbb{Z}_m, +, 0, -)$ (operace modulo m, viz odstavec 2.4) platí $\mathbb{Z}_m = \langle 1 \rangle = \langle k \rangle$, kde $\mathrm{NSD}(m, k) = 1$ (Cvičení).

2.2 Relace ekvivalence a rozklad na třídy ekvivalence

Definice 2.17. Je-li M množina, potom se podmnožina R množiny $M \times M$ nazývá *binární relace* na M. Místo $(x, y) \in R$ píšeme většinou xRy. Speciální relace: $\alpha_M := M \times M$ se nazývá *univerzální relace* , $\iota_M := \{(x, x) \mid x \in M\}$ se nazývá *identická relace* nebo *relace rovnosti* .

Definice 2.18. Relace $R \subseteq M \times M$ se nazývá:

1) *reflexivní* $:\Leftrightarrow \iota_M \subseteq R$, tj., $\forall x \in M : xRx$.

2) *symetrická* $:\Leftrightarrow \forall x, y \in M : xRy \Rightarrow yRx$.

3) *antisymetrická* $:\Leftrightarrow \forall x, y \in M : xRy \wedge yRx \Rightarrow x = y$.

4) *transitivní* $:\Leftrightarrow \forall x, y, z \in M : xRy \wedge yRz \Rightarrow xRz$.

Relace splňující 1), 2) a 4) se nazývá *relace ekvivalence* , relace splňující 1), 3) a 4) se nazývá *relace (částečného) uspořádání* .

Příklad(y) 2.19. α_M a ι_M jsou vždy relace ekvivalence. Relace $\leq$ na množině $\mathbb{R}$, $\subseteq$ na množině $\mathcal{P}(M)$ a $|$ (dělí) na množině $\mathbb{N}$ jsou relace uspořádání.

Definice 2.20. Buď M množina. $\mathcal{P} \subseteq \mathcal{P}(M)$ se nazývá *rozklad množiny M na třídy ekvivalence* třídy ekvivalence $:\Leftrightarrow$

1) $\bigcup_{C \in \mathcal{P}} C = M$,

2) $\emptyset \notin \mathcal{P}$,

3) $A, B \in \mathcal{P} \Rightarrow A = B \vee A \cap B = \emptyset$ (tj. množiny v $\mathcal{P}$ jsou po dvou disjunktní).

Věta 2.21. *Buď π relace ekvivalence na množině M, $a \in M$, $[a]_\pi := \{b \in M \mid b\pi a\}$ tzv. třída ekvivalence prvku a a $M/\pi := \{[a]_\pi \mid a \in M\}$ tzv. faktorová množina množiny M podle ekvivalence π. Potom je M/π rozklad množiny M na třídy ekvivalence.*

Je-li naopak $\mathcal{P}$ rozklad množiny M na třídy ekvivalence a π je definováno vztahem $a\pi b :\Leftrightarrow \exists C \in \mathcal{P} : a, b \in C$, potom je π relace ekvivalence na množině M, a platí $M/\pi = \mathcal{P}$.

$\pi \mapsto M/\pi$ je bijektivní zobrazení množiny všech relací ekvivalence na množině M na množinu všech rozkladů množiny M na třídy ekvivalence. Inverzní zobrazení je dáno výše uvedeným předpisem $\mathcal{P} \mapsto \pi$.

Důkaz. Úloha k procvičení. □

Věta 2.22. *Buďte M, N množiny, $f : M \to N$ zobrazení a $x\pi_f y :\Leftrightarrow f(x) = f(y)$. Potom platí:*

a) π_f je relace ekvivalence na M, která se nazývá jádro f .

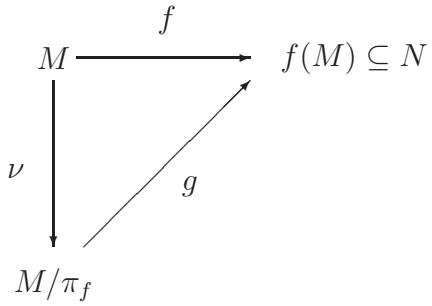
b) Zobrazení

$$\begin{cases} M/\pi_f \to f(M) := \{f(x) \mid x \in M\} \subseteq N \\ [x]_{\pi_f} \mapsto f(x) \end{cases}$$

je korektně definováno a bijektivní.

Důkaz. Úloha k procvičení. □

Poznámka 2.23. Význam zobrazení definovaného v předchozí větě je možno znázornit následujícím *komutativním diagramem* :



Zde je

$$\nu : \begin{cases} M \to M/\pi_f \\ x \mapsto [x]_{\pi_f} \end{cases}$$

kanonické neboli *faktorové* zobrazení a g zobrazení

$$\begin{cases} M/\pi_f \to f(M) \\ [x]_{\pi_f} \mapsto f(x). \end{cases}$$

Platí: $f = g \circ \nu$.

Rozklad grupy na třídy podle podgrupy

Označení: Pokud nebude moci dojít k nedorozumění, budeme dále často klást $G := (G, \cdot, e, ^{-1})$, resp. $G := (G, \cdot)$, tj. označíme grupu tímtéž symbolem jako její nosnou množinu. Podobně pro okruhy.

Věta 2.24. *Buď $(G, \cdot, e, ^{-1})$ grupa a $(H, \cdot, e, ^{-1})$ podgrupa grupy G. Buď dále $\pi \subseteq G \times G$ podmnožina definovaná pomocí vztahu $x\pi y :\Leftrightarrow x^{-1}y \in H$, $x, y \in G$. Potom je π relace ekvivalence na G.*

Důkaz. 1) π je reflexivní: $\forall x : x\pi x$, neboť $x^{-1}x = e \in H$.
2) π je symetrická: $x\pi y \Rightarrow x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} = y^{-1}x \in H \Rightarrow y\pi x$.
3) π je tranzitivní: $x\pi y$, $y\pi z \Rightarrow x^{-1}y \in H$, $y^{-1}z \in H \Rightarrow (x^{-1}y)(y^{-1}z) = x^{-1}z \in H \Rightarrow x\pi z$. □

Poznámka 2.25. Analogicky platí: pomocí vztahu $x\varrho y :\Leftrightarrow xy^{-1} \in H$ je na G rovněž definována relace ekvivalence.

Definice 2.26. Buď $(G, \cdot, e, ^{-1})$ grupa, $A, B \subseteq G$. Potom se nazývá $AB := \{ab \mid a \in A, b \in B\}$ *složený součin* A a B. Speciální případy: $A = \{a\}$: $AB =: aB = \{ab \mid b \in B\}$, $B = \{b\}$: $AB =: Ab = \{ab \mid a \in A\}$. Pro podgrupu H grupy G se nazývá aH *levá třída rozkladu* grupy G podle H a Ha se nazývá *pravá třída rozkladu* grupy G podle H ($a \in G$ pevné ale libovolné).

Věta 2.27. *Buďte π, ϱ výše definované relace ekvivalence na grupě G. Potom platí pro všechna $a \in G$: $[a]_\pi = aH$, $[a]_\varrho = Ha$.*

Důkaz. Platí $\{y \mid a^{-1}y \in H\} = aH$ ($\subseteq$: $a^{-1}y = x \in H \Rightarrow y = ax \in aH$; $\supseteq$: $y = ax \in aH \Rightarrow a^{-1}y = x \in H$). Odtud plyne $[a]_\pi = \{y \mid a\pi y\} = \{y \mid a^{-1}y \in H\} = aH$.

Důkaz vztahu $[a]_\varrho = Ha$ se provede analogicky. □

Důsledek 2.28. $\{aH \mid a \in G\}$ *je rozklad grupy* G *na třídy ekvivalence, který se nazývá* levý rozklad *grupy* G *podle* H. *Podobně se nazývá* $\{Ha \mid a \in G\}$ pravý rozklad *grupy* G *podle* H.

Příklad(y) 2.29. $G = S_3 = \{(1), (123), (132), (12), (23), (13)\}$, $H = \{(1), (23)\}$.

$$\begin{array}{ll} (1)H{=}H & H(1){=}H \\ (123)H{=}\{(123),(12)\} & H(123){=}\{(123),(13)\} \\ (132)H{=}\{(132),(13)\} & H(132){=}\{(132),(12)\} \end{array}$$

Obecně tedy platí $Ha \neq aH$! Pro $a = e$ však platí vždy $He = eH = H$. V abelovských grupách platí $Ha = aH$ pro všechna $a \in G$.

Věta 2.30. *Buď* $(G, \cdot, e, ^{-1})$ *grupa,* H *podgrupa grupy* G, $a, b \in G$. *Potom je vztahem*

$$i : \begin{cases} aH \to bH \\ ax \mapsto bx \end{cases}$$

definováno bijektivní zobrazení.

Důkaz. 1) i je korektně definováno: $ax_1 = ax_2 \Rightarrow x_1 = x_2 \Rightarrow bx_1 = bx_2$.
2) i je injektivní: $i(ax_1) = i(ax_2) \Rightarrow bx_1 = bx_2 \Rightarrow x_1 = x_2$.
3) i je surjektivní: každé $bx \in bH$ je obrazem $ax \in aH$. □

Důsledek 2.31. $\forall a, b \in G : |aH| = |bH| = |H|$. *(Analogicky:* $\forall a \in G : |Ha| = |H|$.*)*

Věta 2.32. *Vztahem* $aH \mapsto Ha^{-1}$, $a \in G$, *je definováno bijektivní zobrazení* φ *levého rozkladu na pravý rozklad grupy* G *podle* H.

Důkaz. 1) φ je korektně definováno: $aH = bH \Rightarrow a\pi b \Rightarrow a^{-1}b \in H \Rightarrow a^{-1}\varrho b^{-1} \Rightarrow Ha^{-1} = Hb^{-1}$.
2) φ je surjektivní: $\forall a \in G : \varphi(a^{-1}H) = Ha$.
3) φ je injektivní: $\varphi(aH) = \varphi(bH) \Rightarrow Ha^{-1} = Hb^{-1} \Rightarrow a^{-1}\varrho b^{-1} \Rightarrow a^{-1}b \in H \Rightarrow a\pi b \Rightarrow aH = bH$. □

Definice 2.33. Počet všech různých tříd levého rozkladu (pravého rozkladu) grupy G podle H se nazývá *index podgrupy* H *v* G , formálně: $[G : H] := |\{aH \mid a \in G\}| = |\{Ha \mid a \in G\}|$.

Věta 2.34. *(Lagrangeova) Buď* $(G, \cdot, e, ^{-1})$ *konečná grupa,* H *podgrupa* G. *Potom platí:*

$$[G : H] \cdot |H| = |G|.$$

Poznámka 2.35. Lagrangeova věta platí také pro nekonečné grupy.

Důsledek 2.36. *a) Je-li* H *podgrupa* G, *pak* $|H|$ *dělí* $|G|$.

b) $x \in G \Rightarrow \mathrm{o}(x) = |\{x^n \mid n \in \mathbb{Z}\}| = |\langle x \rangle|$ *dělí* $|G|$.

c) $|G| = p$ *prvočíslo,* H *podgrupa* $G \Rightarrow H = \{e\}$ *nebo* $H = G$. *Pro* $x \in G$, $x \neq e$, *dostáváme* $\langle x \rangle = G$, *tedy* G *je cyklická.*

2.3 Izomorfizmy a homomorfizmy

Definice 2.37. Buďte $\mathcal{A} = (A, (\omega_i)_{i\in I})$ a $\mathcal{A}^* = (A^*, (\omega_i^*)_{i\in I})$ algebry téhož typu $(n_i)_{i\in I}$. Zobrazení $f : A \to A^*$ se nazývá *homomorfizmus algebry $\mathcal{A}$ do algebry $\mathcal{A}^*$* :$\Leftrightarrow$

1) Pro $i \in I$, kde $n_i > 0$, platí $\forall x_1, \ldots, x_{n_i} \in A : f(\omega_i x_1 \ldots x_{n_i}) = \omega_i^* f(x_1) \ldots f(x_{n_i})$,

2) pro $i \in I$, kde $n_i = 0$, platí $f(\omega_i) = \omega_i^*$.

Lemma 2.38. *Buďte $(G, \cdot, e, ^{-1})$ a $(H, \cdot, e, ^{-1})$ grupy, $f : G \to H$. Potom platí: f je homomorfizmus grupy $(G, \cdot, e, ^{-1})$ do grupy $(H, \cdot, e, ^{-1}) \Leftrightarrow$ f je homomorfizmus grupy $(G, \cdot)$ do grupy $(H, \cdot)$.*

Důkaz. $\Rightarrow$: Triviální.
$\Leftarrow$: Nechť $f(xy) = f(x)f(y)$. Máme ukázat, že $f(e) = e$, $f(x^{-1}) = (f(x))^{-1}$. Platí $ee = e \Rightarrow f(e)f(e) = f(e) \Rightarrow f(e) = e$. Dále, $xx^{-1} = e \Rightarrow f(x)f(x^{-1}) = f(e) = e = f(x)(f(x))^{-1} \Rightarrow f(x^{-1}) = (f(x))^{-1}$. □

Důsledek 2.39. *1) Buďte $\mathcal{V} = (V, +, 0, -, K)$ a $\mathcal{W} = (W, +, 0, -, K)$ vektorové prostory nad tímtéž polem K a $f : V \to W$. Potom platí: f je homomorfizmus vektorového prostoru $\mathcal{V}$ do vektorového prostoru $\mathcal{W} \Leftrightarrow$ f je lineární zobrazení, tj. $\forall x, y \in V : f(x + y) = f(x) + f(y)$, $\forall \lambda \in K, x \in V : f(\lambda x) = \lambda f(x)$.*

2) Buďte $(R, +, 0, -, \cdot)$ a $(S, +, 0, -, \cdot)$ okruhy, $f : R \to S$. Potom platí: f je homomorfizmus okruhu $(R, +, 0, -, \cdot)$ do okruhu $(S, +, 0, -, \cdot) \Leftrightarrow$ f je homomorfizmus okruhu $(R, +, \cdot)$ do okruhu $(S, +, \cdot)$.

Definice 2.40. Buďte $\mathcal{A} = (A, (\omega_i)_{i\in I})$ a $\mathcal{A}^* = (A^*, (\omega_i^*)_{i\in I})$ algebry téhož typu $(n_i)_{i\in I}$ a $f : A \to A^*$ homomorfizmus algebry $\mathcal{A}$ do algebry $\mathcal{A}^*$. f se nazývá

1) *izomorfizmus* , pokud je f bijektivní (v tomto případě říkáme, že $\mathcal{A}$ je *izomorfní obraz* $\mathcal{A}^*$, a píšeme $\mathcal{A} \cong \mathcal{A}^*$),

2) *endomorfizmus* , pokud $\mathcal{A} = \mathcal{A}^*$,

3) *automorfizmus* , pokud $\mathcal{A} = \mathcal{A}^*$ a f izomorfizmus,

4) *epimorfizmus* , pokud je f surjektivní (v tomto případě se nazývá $\mathcal{A}^*$ *homomorfní obraz* $\mathcal{A}$),

5) *monomorfizmus*, pokud je f injektivní (v tomto případě se nazývá $\mathcal{A}$ *izomorfně vnořená* v $\mathcal{A}^*$).

Lemma 2.41. *a) Buďte $\mathcal{A}$, $\mathcal{A}^*$, $\mathcal{A}^{**}$ algebry téhož typu, f homomorfizmus algebry $\mathcal{A}$ do algebry $\mathcal{A}^*$, g homomorfizmus algebry $\mathcal{A}^*$ do algebry $\mathcal{A}^{**}$. Potom je $g \circ f$ homomorfizmus algebry $\mathcal{A}$ do algebry $\mathcal{A}^{**}$. Jsou-li f, g izomorfizmy, pak je také $g \circ f$ izomorfizmus.*

b) Je-li f izomorfizmus $\mathcal{A}$ do $\mathcal{A}^*$, pak je f^{-1} izomorfizmus $\mathcal{A}^*$ do $\mathcal{A}$.

Důkaz. Cvičení. □

Obrazy a (úplné) vzory podalgeber při homomorfizmech jsou opět podalgebry (Cvičení). (Je-li $f : A \to A^*$ zobrazení, $U^* \subseteq A^*$, pak se $f^{-1}(U^*) := \{x \in A \mid f(x) \in U^*\}$ nazývá *úplný vzor* U^*.)

Homomorfizmy a zákony

Věta 2.42. *Buď $(H,\cdot)$ pologrupa, $(H^*,\cdot)$ grupoid a $f : H \to H^*$ homomorfizmus. Potom je podalgebra $(f(H),\cdot)$ grupoidu $(H^*,\cdot)$ pologrupa.*

Důkaz. Buďte $x, y, z \in f(H)$. Potom existuje $a, b, c \in H$, kde $f(a) = x$, $f(b) = y$ a $f(c) = z$. Protože $(H,\cdot)$ je pologrupa, platí $a(bc) = (ab)c$, tudíž $f(a)(f(b)f(c)) = (f(a)f(b))f(c)$, tedy $x(yz) = (xy)z$. □

Poznámka 2.43. Buďte $(A,(\omega_i)_{i\in I})$ a $(A^*,(\omega_i^*)_{i\in I})$ algebry téhož typu, $f : A \to A^*$ epimorfizmus (tj. A^* je homomorfní obraz A). Platí-li pro vhodné termy t_1, t_2 v A rovnice (zákon) $\forall a, b, c, \ldots : t_1(a, b, c, \ldots) = t_2(a, b, c, \ldots)$, pak plyne ze vztahu $t_1(f(a), f(b), f(c), \ldots) = f(t_1(a, b, c, \ldots)) = f(t_2(a, b, c, \ldots)) = t_2(f(a), f(b), f(c), \ldots)$, že zákon platí též v A^*. Termy jsou přitom vytvořeny z konečného počtu proměnných a symbolů operací (pro A, resp. A^*).

Poznámka 2.44. Je-li $(A,(\omega_i)_{i\in I})$ algebra, pak nazýváme $(\omega_i)_{i\in I}$ *fundamentální* operace , příslušné termy naproti tomu nazýváme *odvozené* operace .

Interpretace věty 2.42: každý homomorfní obraz pologrupy je pologrupa. Analogicky se dá ukázat: každý homomorfní obraz
1) (abelovské) grupy je (abelovská) grupa,
2) (komutativního) okruhu je (komutativní) okruh,
3) okruhu s jednotkovým prvkem je okruh s jednotkovým prvkem,
4) svazu je svaz,
5) Booleovy algebry je Booleova algebra,
6) vektorového prostoru nad K je vektorový prostor nad K.

Buď $(A,\cdot)$ grupoid, kde $A = \{a_1, \ldots, a_n\}$, a $(A^*,\circ)$ další grupoid, kde $|A^*| = n$, $f : A \to A^*$ izomorfizmus, $A^* = \{a_1^*, \ldots, a_n^*\}$, kde $a_i^* = f(a_i)$, $1 \le i \le n$. Tabulky operací obou algeber pak vypadají následovně:

$\cdot$	a_1	$\ldots$	a_n
a_1	a_1a_1	$\ldots$	a_1a_n
$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_n	a_na_1	$\ldots$	a_na_n

$\circ$	a_1^*	$\ldots$	a_n^*
a_1^*	$a_1^* \circ a_1^*$	$\ldots$	$a_1^* \circ a_n^*$
$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_n^*	$a_n^* \circ a_1^*$	$\ldots$	$a_n^* \circ a_n^*$

Je-li v levé tabulce $a_ia_j = a_k$, pak je v pravé tabulce $a_i^* \circ a_j^* = a_k^*$. Z algebraického hlediska je proto izomorfizmus pouhé „přeznačení“. Na izomorfní algebry je nutno „pohlížet jako na stejné“.

Algebraické vlastnosti jsou takové vlastnosti, které zůstávají zachovány při izomorfizmech. Například všechny zákony jsou algebraickými vlastnostmi, protože podle výše uvedené poznámky zůstávají zachovány dokonce už při epimorfizmech.

Často je možné charakterizovat algebraické struktury „až na izomorfizmus“. Tak jsou např. všechny konečnědimenzionální vektorové prostory nad K až na izomorfizmus dány vektorovým prostorem K^n, $n \in \mathbb{N}_0$ (s obvyklými operacemi). Analogická tvrzení uvedeme pro konečná pole a konečné Booleovy algebry. Dalším výsledkem v tomto směru je následující věta:

Věta 2.45. *(Cayleyova věta o reprezentaci) Buď $(G,\cdot,e,^{-1})$ grupa. Potom je G izomorfní s podgrupou symetrické grupy $(S_G,\circ,\mathrm{id}_G,^{-1})$.* Krátce: *Každá grupa je izomorfní s nějakou grupou permutací.*

Důkaz. Zkonstruujeme vnoření (monomorfizmus) $\pi : G \to S_G$, $a \mapsto \pi_a$, následujícím způsobem:

$$\forall g \in G : \pi_a(g) := ag.$$

1) $\pi_a \in S_G$, tj., π_a je injektivní a surjektivní (injektivní: $\pi_a(g_1) = \pi_a(g_2) \Rightarrow ag_1 = ag_2 \Rightarrow g_1 = g_2$; surjektivní: $h \in G \Rightarrow h = \pi_a(a^{-1}h)$).
2) π je injektivní: $\pi_{a_1} = \pi_{a_2} \Rightarrow \pi_{a_1}(e) = \pi_{a_2}(e) \Rightarrow a_1 e = a_2 e \Rightarrow a_1 = a_2$.
3) $\pi_{ab} = \pi_a \circ \pi_b$: $\pi_{ab}(g) = (ab)g = a(bg) = \pi_a(bg) = \pi_a(\pi_b(g)) = (\pi_a \circ \pi_b)(g)$. □

Poznámka 2.46. Analogická věta platí také pro monoidy.

2.4 Relace kongruence a faktorové algebry

Definice 2.47. Buď $\mathcal{A} = (A, (\omega_i)_{i\in I})$ algebra typu $(n_i)_{i\in I}$ a π relace ekvivalence na A. π se nazývá *(relace) kongruence* na $\mathcal{A} :\Leftrightarrow$ pro všechna $i \in I$, kde $n_i > 0$, $a_1, \ldots, a_{n_i}, b_1, \ldots, b_{n_i} \in A$, platí

$$a_1 \pi b_1 \wedge \ldots \wedge a_{n_i} \pi b_{n_i} \Rightarrow \omega_i a_1 \ldots a_{n_i} \pi \omega_i b_1 \ldots b_{n_i}.$$

Příklad(y) 2.48. Buď $\mathcal{A} = (\mathbb{Z}, +, 0, -, \cdot, 1)$ obor integrity celých čísel a $n \in \mathbb{N}_0$ pevné (n se nazývá modul). Nechť binární relace π na $\mathbb{Z}$ je definována pomocí vztahu:

$$a \pi b :\Leftrightarrow \exists c \in \mathbb{Z} : a - b = cn, \qquad a, b \in \mathbb{Z}.$$

Dále budeme psát – podobně jako v odstavci 1.3 – $a \equiv b \bmod n$ místo $a\pi b$. Platí: $\equiv \mathrm{mod}\, n$ je relace kongruence neboť:
1) $\equiv \mathrm{mod}\, n$ je relace ekvivalence: $a \equiv a \bmod n$ protože $a - a = 0 = 0n$; $a \equiv b \bmod n \Rightarrow a - b = cn \Rightarrow b - a = (-c)n \Rightarrow b \equiv a \bmod n$; $a \equiv b \bmod n \wedge b \equiv c \bmod n \Rightarrow a - b = d_1 n \wedge b - c = d_2 n \Rightarrow a - c = (d_1 + d_2)n \Rightarrow a \equiv c \bmod n$.
2) Operace $+$: $a_1 \equiv b_1 \bmod n \wedge a_2 \equiv b_2 \bmod n \Rightarrow a_1 - b_1 = c_1 n \wedge a_2 - b_2 = c_2 n \Rightarrow (a_1 + a_2) - (b_1 + b_2) = (c_1 + c_2)n \Rightarrow (a_1 + a_2) \equiv (b_1 + b_2) \bmod n$.
3) Operace $-$: $a \equiv b \bmod n \Rightarrow a - b = cn \Rightarrow (-a) - (-b) = (-c)n \Rightarrow (-a) \equiv (-b) \bmod n$.
4) Operace $\cdot$: $a_1 \equiv b_1 \bmod n \wedge a_2 \equiv b_2 \bmod n \Rightarrow a_1 = b_1 + c_1 n \wedge a_2 = b_2 + c_2 n \Rightarrow a_1 a_2 = b_1 b_2 + (b_1 c_2 + b_2 c_1 + c_1 c_2 n)n \Rightarrow a_1 a_2 \equiv b_1 b_2 \bmod n$.

Příslušný rozklad na třídy: Platí $[a] = \{a + kn \mid k \in \mathbb{Z}\}$. Pro $n = 0$ máme $[a] = \{a\}$ pro všechna $a \in \mathbb{Z}$ ($\equiv \mathrm{mod}\, n$ je potom relace rovnosti). Pro $n > 0$ platí: $\mathbb{Z}_n := \mathbb{Z}/\equiv \mathrm{mod}\, n = \{[a] \mid a \in \mathbb{Z}\} = \{[0], \ldots, [n-1]\}$.

Věta 2.49. *Buď $\mathcal{A} = (A, (\omega_i)_{i\in I})$ algebra a π kongruence na $\mathcal{A}$. Potom jsou vztahy*

$$\omega_i^*[a_1]_\pi \ldots [a_{n_i}]_\pi := [\omega_i a_1 \ldots a_{n_i}]_\pi, \quad n_i > 0,\ a_1, \ldots, a_{n_i} \in A,$$
$$\omega_i^* := [\omega_i]_\pi, \quad n_i = 0,$$

definovány operace $(\omega_i^*)_{i\in I}$ na faktorové množině A/π.

Důkaz. Operace jsou korektně definovány:

$$\left.\begin{array}{c} [a_1]_\pi = [b_1]_\pi \\ \vdots \\ [a_{n_i}]_\pi = [b_{n_i}]_\pi \end{array}\right\} \Rightarrow \left\{\begin{array}{c} a_1 \pi b_1 \\ \vdots \\ a_{n_i} \pi b_{n_i} \end{array}\right\} \Rightarrow \omega_i a_1 \ldots a_{n_i} \pi \omega_i b_1 \ldots b_{n_i}.$$

Proto je $[\omega_i a_1 \ldots a_{n_i}]_\pi = [\omega_i b_1 \ldots b_{n_i}]_\pi$. □

Definice 2.50. Algebra $\mathcal{A}/\pi := (A/\pi, (\omega_i^*)_{i\in I})$ se nazývá *faktorová algebra* algebry $\mathcal{A}$ podle kongruence π. Často klademe $\omega_i := \omega_i^*$.

Příklad(y) 2.51. $\mathcal{A} = (\mathbb{Z}, +, 0, -, \cdot, 1)$, $\pi = \equiv \mathrm{mod}\, n$. Faktorová algebra $\mathcal{A}/\pi$ je potom dána pomocí vztahu $(\mathbb{Z}_n, +^*, 0^*, -^*, \cdot^*, 1^*)$, kde $[a] +^* [b] = [a+b]$, $0^* = [0]$, $-^*[a] = [-a]$, $[a] \cdot^* [b] = [ab]$, $1^* = [1]$ (tj. počítáme s „reprezentanty" tříd). Dále budeme symbol * u operací vynechávat. Platí (viz následující věta): $(\mathbb{Z}_n, +, 0, -, \cdot, 1)$ je komutativní okruh s jednotkovým prvkem, který se nazývá *okruh zbytkových tříd modulo n* .

Věta 2.52. *Buď $\mathcal{A} = (A, (\omega_i)_{i\in I})$ algebra, π kongruence na $\mathcal{A}$. Potom je zobrazení*

$$\nu : \begin{cases} A \to A/\pi \\ a \mapsto [a]_\pi \end{cases}$$

surjektivní homomorfizmus algebry $\mathcal{A}$ na $\mathcal{A}/\pi$, který se nazývá přirozený homomorfizmus .

Důkaz.

$$\nu(\omega_i a_1 \dots a_{n_i}) = [\omega_i a_1 \dots a_{n_i}]_\pi = \omega_i [a_1]_\pi \dots [a_{n_i}]_\pi = \omega_i \nu(a_1) \dots \nu(a_{n_i}), \quad n_i > 0,$$
$$\nu(\omega_i) = [\omega_i]_\pi = \omega_i, \quad n_i = 0.$$

□

Důsledek 2.53. *a) $\mathcal{A}/\pi$ je homomorfní obraz $\mathcal{A}$.*

b) Každý zákon, který platí v $\mathcal{A}$, platí také v $\mathcal{A}/\pi$. Speciálně je tedy

i) každá faktorová algebra pologrupy pologrupou,

ii) každá faktorová algebra (abelovské) grupy (abelovskou) grupou,

iii) každá faktorová algebra vektorového prostoru vektorovým prostorem,

iv každá faktorová algebra (komutativního) okruhu (komutativním) okruhem,

v) každá faktorová algebra okruhu s jednotkovým prvkem okruhem s jednotkovým prvkem,

vi) každá faktorová algebra svazu (resp. Booleovy algebry) svazem (resp. Booleovou algebrou).

Poznámka 2.54. Faktorová algebra oboru integrity nemusí být oborem integrity, jak je vidět na příkladu $(\mathbb{Z}_n, +, 0, -, \cdot, 1)$, kde $n \in \mathbb{N}$ není prvočíslo.

Věta 2.55. *(O homomorfizmu) Buďte $\mathcal{A} = (A, (\omega_i)_{i\in I})$ a $\mathcal{A}^* = (A^*, (\omega_i^*)_{i\in I})$ algebry téhož typu $(n_i)_{i\in I}$ a $f : A \to A^*$ homomorfizmus. Potom je jádro π_f kongruencí na $\mathcal{A}$ a existuje* přesně jeden *injektivní homomorfizmus g z $\mathcal{A}/\pi_f$ do $\mathcal{A}^*$ takový, že $f = g \circ \nu$ (ν je přirozené zobrazení).*

Důkaz. 1) π_f je relace ekvivalence a existuje injektivní zobrazení $g : A/\pi_f \to A^*$, kde $f = g \circ \nu$ (viz odstavec 2.2).

2) π_f je kongruence: Buď $i \in I$, $n_i > 0$. Máme:

$$\left.\begin{array}{c} a_1 \pi_f b_1 \\ \vdots \\ a_{n_i} \pi_f b_{n_i} \end{array}\right\} \Rightarrow \left\{\begin{array}{c} f(a_1) = f(b_1) \\ \vdots \\ f(a_{n_i}) = f(b_{n_i}) \end{array}\right\} \Rightarrow \omega_i^* f(a_1) \dots f(a_{n_i}) = \omega_i^* f(b_1) \dots f(b_{n_i})$$

$\Rightarrow f(\omega_i a_1 \dots a_{n_i}) = f(\omega_i b_1 \dots b_{n_i}) \Rightarrow \omega_i a_1 \dots a_{n_i} \pi_f \omega_i b_1 \dots b_{n_i}$. Jednoznačnost g je triviální: $g([a]_{\pi_f}) = g(\nu(a)) = (g \circ \nu)(a) = f(a)$.

3) g je homomorfizmus: Buď $i \in I$, $n_i > 0$, potom platí:

$$g(\omega_i [a_1]_{\pi_f} \dots [a_{n_i}]_{\pi_f}) = g([\omega_i a_1 \dots a_{n_i}]_{\pi_f}) = g(\nu(\omega_i a_1 \dots a_{n_i})) = f(\omega_i a_1 \dots a_{n_i})$$
$$= \omega_i^* f(a_1) \dots f(a_{n_i}) = \omega_i^* g(\nu(a_1)) \dots g(\nu(a_{n_i})) = \omega_i^* g([a_1]_{\pi_f}) \dots g([a_{n_i}]_{\pi_f}).$$

Analogicky pro $n_i = 0$: $g(\omega_i) = g([\omega_i]_{\pi_f}) = f(\omega_i) = \omega_i^*$. □

Důsledek 2.56. *Pro podalgebru $(f(A), (\omega_i^*)_{i \in I})$ algebry $\mathcal{A}^*$ platí $(f(A), (\omega_i^*)_{i \in I}) \cong \mathcal{A}/\pi_f$, tedy je každý homomorfní obraz algebry izomorfní s nějakou faktorovou algebrou.*

Poznámka 2.57. Relace rovnosti $\iota = \{(x, x) \mid x \in A\}$ a univerzální relace $\alpha = A \times A$ jsou vždy kongruencemi na $\mathcal{A}$ a nazývají se *triviální* kongruence na $\mathcal{A}$. Platí: $\mathcal{A}/\iota \cong \mathcal{A}$ a $|\mathcal{A}/\alpha| \leq 1$. $\mathcal{A}/\iota$ a $\mathcal{A}/\alpha$ jsou *triviální* faktorové algebry .

Definice 2.58. Algebra $\mathcal{A}$ se nazývá *prostá* , má-li pouze triviální kongruence.

Poznámka 2.59. Algebra $\mathcal{A}$ je prostá tehdy a jen tehdy, když má pouze *triviální* homomorfní obrazy (tj. pouze obrazy izomorfní s $\mathcal{A}$, resp. nejvýše jednoprvkové homomorfní obrazy).

2.5 Relace kongruence na grupách a okruzích

Věta 2.60. *Buď $(G, \cdot, e, ^{-1})$ grupa a π relace ekvivalence na G. Potom platí:*

a) π je kongruence na $(G, \cdot, e, ^{-1}) \Leftrightarrow \pi$ je kongruence na $(G, \cdot)$.

b) Je-li π kongruence na $(G, \cdot)$ a $[e]_\pi =: N$, potom platí:

i) N je podgrupa $(G, \cdot, e, ^{-1})$.

ii) $xNx^{-1} = \{xyx^{-1} \mid y \in N\} \subseteq N$ pro všechna $x \in G$.

iii) $x \pi y \Leftrightarrow x^{-1}y \in N$ pro všechna $x, y \in G$ (tj., $[x]_\pi = xN$ pro všechna $x \in G$).

Důkaz. a) $\Rightarrow$: Triviální.
$\Leftarrow$:

$$\left.\begin{matrix} x \pi y \\ x^{-1} \pi x^{-1} \end{matrix}\right\} \Rightarrow \left\{\begin{matrix} e = x x^{-1} \pi y x^{-1} \\ y^{-1} \pi y^{-1} \end{matrix}\right\} \Rightarrow y^{-1} \pi y^{-1} y x^{-1} = x^{-1}.$$

b) i) $e \in N$ protože $e \pi e$. $x, y \in N \Rightarrow x \pi e \wedge y \pi e \Rightarrow xy \pi ee = e \Rightarrow xy \in N$.
$x \in N \Rightarrow x \pi e \Rightarrow x^{-1} \pi e^{-1} = e \Rightarrow x^{-1} \in N$.
ii) $y \in N \Rightarrow y \pi e \Rightarrow xyx^{-1} \pi x e x^{-1} = e \Rightarrow xyx^{-1} \in N$.
iii) $\Rightarrow$: $x \pi y \Rightarrow e = x^{-1} x \pi x^{-1} y \Rightarrow x^{-1} y \in N$.
$\Leftarrow$: $x^{-1} y \in N \Rightarrow x^{-1} y \pi e \Rightarrow y = x x^{-1} y \pi x e = x$. □

Definice 2.61. Podgrupa N grupy $(G, \cdot, e, ^{-1})$ se nazývá *normální podgrupa* grupy G (symbolicky: $N \lhd G$) $:\Leftrightarrow xNx^{-1} \subseteq N$ pro všechna $x \in G$.

Poznámka 2.62. V abelovské grupě je každá podgrupa normální podgrupou. Pro neabelovské grupy tomu tak není. Např. existují podgrupy grupy S_3, které nejsou normálními podgrupami, totiž: $\{(1), (12)\}$, $\{(1), (13)\}$ a $\{(1), (23)\}$.

Lemma 2.63. *Pro podgrupu N grupy G jsou následující tvrzení ekvivalentní:*

a) N je normální podgrupa grupy G.

b) $\forall x \in G : xNx^{-1} = N$.

c) $\forall x \in G : Nx = xN$, tj. pravá třída rozkladu = levá třída rozkladu.

Důkaz. a) $\Rightarrow$ b): N normální podgrupa $\Rightarrow \forall x \in G : xNx^{-1} \subseteq N \Rightarrow \forall x \in G : x^{-1}Nx \subseteq N$ $\Rightarrow \forall x \in G : N = xx^{-1}Nxx^{-1} \subseteq xNx^{-1} \Rightarrow \forall x \in G : xNx^{-1} = N$.

b) $\Rightarrow$ a) je triviální.

b) $\Leftrightarrow$ c): $xNx^{-1} = N \Rightarrow xN = xNx^{-1}x = Nx$; $xN = Nx \Rightarrow xNx^{-1} = Nxx^{-1} = N$ pro všechna $x \in G$. □

Věta 2.64. *Buď $(G, \cdot, e, ^{-1})$ grupa, $N \lhd G$ a π buď binární relace na G definovaná vztahem $x\pi y :\Leftrightarrow x^{-1}y \in N$, $x, y \in G$. Potom je π relace kongruence na G, kde $[e]_\pi = N$.*

Důkaz. π je relace ekvivalence a $[x]_\pi = xN = Nx$ podle Věty 2.24 a Lemmatu 2.63. π je kongruence:

$$\left.\begin{array}{l} x_1\pi y_1 \\ x_2\pi y_2 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} x_1 = y_1n_1, \text{ kde } n_1 \in N \text{ (neboť } x_1 \in y_1N) \\ x_2 = n_2y_2, \text{ kde } n_2 \in N \text{ (neboť } x_2 \in Ny_2) \end{array}\right\} \Rightarrow$$
$$\Rightarrow x_1x_2 = y_1n_1n_2y_2 \in y_1Ny_2 = y_1y_2N \Rightarrow x_1x_2\pi y_1y_2.$$

Dále platí $[e]_\pi = eN = N$. □

Věta 2.65. *Vztahem $\pi \mapsto [e]_\pi$ je definováno bijektivní zobrazení množiny kongruencí na grupě G na množinu všech normálních podgrup grupy G. Inverzní zobrazení je dáno pomocí vztahu $N \mapsto \pi$, kde $x\pi y :\Leftrightarrow x^{-1}y \in N$.*

Důkaz. Obě přiřazení jsou navzájem inverzní: $\pi \mapsto [e]_\pi =: N \mapsto \pi_1$, kde $x\pi_1 y :\Leftrightarrow x^{-1}y \in N \Leftrightarrow x\pi y$, tj. $\pi = \pi_1$. Obráceně: $N \mapsto \pi \mapsto [e]_\pi = N$. □

Chceme-li najít všechny homomorfní obrazy – až na izomorfizmus – nějaké grupy G, můžeme tedy určit všechny normální podgrupy N grupy G a vytvořit faktorové algebry G/π pomocí odpovídajících kongruencí. Pokud normální podgrupě N odpovídá kongruence π, píšeme $G/N := G/\pi = \{xN \mid x \in G\}$. Takováto faktorová algebra se nazývá *faktorgrupa* grupy G.

Ve faktorgrupě G/N se počítá následujícím způsobem: $(xN)(yN) = (xy)N$, $eN = N$ je jednotkový prvek, $(xN)^{-1} = x^{-1}N$.

Triviálním kongruencím $\iota = \{(x, x) \mid x \in G\}$ a $\alpha = G \times G$ odpovídají tzv. *triviální* normální podgrupy $\{e\}$ a G. Odtud plyne: G je prostá $\Leftrightarrow$ G má pouze triviální normální podgrupy.

Příklad(y) 2.66. 1) Každá cyklická grupa $G = \langle x \rangle$ taková, že $o(x) = p$ (p prvočíslo), je prostá (věta Lagrangeova). Obráceně platí: Každá prostá abelovská grupa G, kde $|G| > 1$, je cyklická a má prvočíselný řád (Cvičení).

2) Alternující grupa A_n (viz Příklad 1.84) je prostá pro $n \neq 4$.

3) Symetrická grupa S_n není pro $n \geq 3$ prostá, neboť platí $A_n \lhd S_n$. Levý (pravý) rozklad S_n na třídy podle A_n je roven $\{A_n, S_n \setminus A_n\}$, tedy platí $[S_n : A_n] = 2$ (index A_n v S_n).

Věta 2.67. *Buď G grupa, U podgrupa, kde $[G:U]=2$. Potom platí $U \lhd G$.*

Důkaz. $x \in U \Rightarrow xU = Ux = U$. $x \notin U \Rightarrow xU = Ux = G \setminus U$. □

Poznámka 2.68. Také pro vektorové prostory platí podobný výsledek jako pro grupy: Vztahem $\pi \mapsto [0]_\pi$ je definováno bijektivní zobrazení množiny všech relací kongruence vektorového prostoru $(V, +, 0, -, K)$ na množinu všech podprostorů prostoru V (Důkaz podobný jako u grup).

Je-li U podprostor prostoru V, pak je $V/U = \{x+U \mid x \in V\}$ faktorový prostor s operacemi $(x+U)+(y+U) = (x+y)+U$, $0+U = U$ (neutrální prvek), $-(x+U) = (-x)+U$, $\lambda(x+U) = (\lambda x)+U$, $x, y \in V$, $\lambda \in K$.

Definice 2.69. Buď $(R, +, 0, -, \cdot)$ okruh a I podokruh okruhu R. Potom se I nazývá

- *levý ideál* okruhu $R :\Leftrightarrow \forall r \in R : rI := \{ri \mid i \in I\} \subseteq I$,
- *pravý ideál* okruhu $R :\Leftrightarrow \forall r \in R : Ir := \{ir \mid i \in I\} \subseteq I$,
- *ideál* okruhu R (formálně: $I \lhd R$) $:\Leftrightarrow \forall r \in R : rI \subseteq I \wedge Ir \subseteq I$.

Příklad(y) 2.70. 1) $\{0\}$ a R jsou vždy ideály okruhu R, tak zvané *triviální* ideály .

2) V $(\mathbb{Z}, +, 0, -, \cdot)$ je $\{nk \mid k \in \mathbb{Z}\}$, $n \in \mathbb{N}_0$, ideálem. Tím jsou vyčerpány všechny ideály v $\mathbb{Z}$.

Lemma 2.71. *Buď $(R, +, 0, -, \cdot, 1)$ okruh s jednotkovým prvkem a I ideál okruhu R. Potom platí: $1 \in I \Leftrightarrow I = R$.*

Důkaz. Je triviální. □

Věta 2.72. *Každé těleso má pouze triviální ideály.*

Důkaz. Buď I ideál tělesa $(K, +, 0, -, \cdot, 1)$ a $I \neq \{0\}$. Potom existuje $x \in I$, $x \neq 0$. Protože $1 = x^{-1}x \in x^{-1}I \subseteq I$, platí $I = K$. □

Věta 2.73. *Buď $(R, +, 0, -, \cdot, 1)$ komutativní okruh s jednotkovým prvkem, který má pouze triviální ideály. Potom je R pole nebo $R = \{0\}$.*

Důkaz. $x \in R$, $x \neq 0 \Rightarrow xR = \{xr \mid r \in R\}$ je ideál okruhu R (analogicky k $\mathbb{Z}$), kde $x = x1 \in xR \Rightarrow xR \neq \{0\} \Rightarrow xR = R \Rightarrow \exists r \in R : 1 = xr \Rightarrow x$ má inverzní prvek. □

Důsledek 2.74. *Komutativní okruh $R \neq \{0\}$ s jednotkovým prvkem je pole $\Leftrightarrow$ R má pouze triviální ideály.*

Věta 2.75. *Buď $(R, +, 0, -, \cdot)$ okruh.*

a) Je-li π kongruence na R, potom je $I := [0]_\pi$ ideál okruhu R, a platí: $R/\pi = R/I = \{x + I \mid x \in R\}$.

b) Je-li I ideál okruhu R a π binární relace na R definovaná vztahem $x\pi y :\Leftrightarrow y - x \in I$, $x, y \in R$, potom je π kongruence na R a $[0]_\pi = I$.

c) $\pi \mapsto [0]_\pi$ *definuje bijektivní zobrazení množiny všech kongruencí na* R *na množinu všech ideálů okruhu* R*. Inverzní zobrazení je dáno vztahem* $I \mapsto \pi$*, kde* π *je kongruence definovaná v b).*

Důkaz. a) $i \in I \wedge r \in R \Rightarrow i\pi 0 \wedge r\pi r \Rightarrow ir\pi 0r = 0 \wedge ri\pi r0 = 0 \Rightarrow ir, ri \in I$.

b) $x_1\pi y_1 \wedge x_2\pi y_2 \Rightarrow y_1 = x_1 + i_1 \wedge y_2 = x_2 + i_2$, $i_1, i_2 \in I \Rightarrow y_1y_2 = x_1x_2 + i$, kde $i = x_1i_2 + i_1x_2 + i_1i_2 \in I$ (I je ideál) $\Rightarrow x_1x_2\pi y_1y_2$.

c) $\pi \mapsto [0]_\pi = I \mapsto \pi$, $I \mapsto \pi \mapsto [0]_\pi = I$ (analogicky k odpovídajícímu důkazu pro normální podgrupy). □

Je-li I ideál okruhu R, potom je faktorová algebra $(R/I, +, I, -, \cdot)$ okruhem a nazývá se *faktorový okruh* nebo *okruh zbytkových tříd* okruhu R modulo I. Operace v R/I jsou: $(x + I) + (y + I) = (x + y) + I$ (je identická se součtem $A + B = \{a + b \mid a \in A,\ b \in B\}$), $(x+I)(y+I) = xy + I$ (*není* identická se součinem $AB = \{ab \mid a \in A,\ b \in B\}$), $-(x+I) = (-x) + I$, $0 + I = I$ je nulový prvek.

Příklad(y) 2.76. Nechť $\mathbb{Z}_n = \mathbb{Z}/I$, $I = \{kn \mid k \in \mathbb{Z}\}$. Pak $y - x \in I \Leftrightarrow \exists k \in \mathbb{N} : y - x = kn \Leftrightarrow x \equiv y \bmod n$. Tedy zadaný ideál I odpovídá relaci $\equiv \bmod n$, což zapíšeme jako $I =: (n)$.

Poznámka 2.77. Okruh R je prostý $\Leftrightarrow$ R má pouze triviální kongruence $\Leftrightarrow$ R má pouze triviální ideály $\{0\} =: (0)$ a R.

Věta 2.78. *Komutativní okruh* $R \neq \{0\}$ *s jednotkovým prvkem je prostý právě tehdy, když je pole.*

Příklad(y) 2.79. Každý okruh matic $M_n(K)$ nad polem K je prostý (Cvičení).

2.6 Přímé součiny algeber

Definice 2.80. Buďte $\mathcal{A}_k = (A_k, (\omega_i^{(k)})_{i\in I})$, $k \in K$, algebry téhož typu $(n_i)_{i\in I}$ a $A := \prod_{k\in K} A_k = \{(a_k)_{k\in K} \mid a_k \in A_k\}$ kartézský součin všech množin A_k. Pro všechna $i \in I$ buď operace ω_i na A definována vztahem:

$$\omega_i(a_k^{(1)})_{k\in K} \dots (a_k^{(n_i)})_{k\in K} := (\underbrace{\omega_i^{(k)} a_k^{(1)} \dots a_k^{(n_i)}}_{\in A_k})_{k\in K} \quad \text{pro } n_i > 0,$$

$$\omega_i := (\omega_i^{(k)})_{k\in K} \quad \text{pro } n_i = 0.$$

Algebra $(A, (\omega_i)_{i\in I})$ se nazývá *přímý součin* algeber $\mathcal{A}_k$ a značí se $\prod_{k\in K} \mathcal{A}_k$.

Příklad(y) 2.81. Nechť $K = \{1, 2\}$, $\mathcal{A}_1 = (A_1, \cdot, e, {}^{-1})$, $\mathcal{A}_2 = (A_2, +, 0, -)$ jsou grupy. Potom se v $\mathcal{A}_1 \times \mathcal{A}_2 = (A_1 \times A_2, \circ, (e, 0), {}')$ počítá následujícím způsobem: $(a_1, a_2) \circ (b_1, b_2) = (a_1b_1, a_2 + b_2)$, $(a_1, a_2)' = (a_1^{-1}, -a_2)$. Platí: $\mathcal{A}_1 \times \mathcal{A}_2$ je grupa. Asociativní zákon: $((a_1, a_2) \circ (b_1, b_2)) \circ (c_1, c_2) = (a_1b_1c_1, a_2 + b_2 + c_2) = (a_1, a_2) \circ ((b_1, b_2) \circ (c_1, c_2))$; $(e, 0)$ je neutrální prvek: $(e, 0) \circ (a_1, a_2) = (ea_1, 0 + a_2) = (a_1, a_2) = (a_1e, a_2 + 0) = (a_1, a_2) \circ (e, 0)$; $(a_1, a_2)'$ je inverzní prvek k (a_1, a_2): $(a_1, a_2) \circ (a_1, a_2)' = (a_1, a_2) \circ (a_1^{-1}, -a_2) = (a_1a_1^{-1}, a_2 + (-a_2)) = (e, 0)$, analogicky $(a_1, a_2)' \circ (a_1, a_2) = (e, 0)$.

Věta 2.82. *Pokud platí při vhodných termech* t_1, t_2 *zákon tvaru* $\forall x_1, \dots, x_n : t_1(x_1, \dots, x_n) = t_2(x_1, \dots, x_n)$ *ve všech algebrách* $\mathcal{A}_k$*,* $k \in K$*, potom platí také v* $\prod_{k\in K} \mathcal{A}_k$*.*

Důkaz. Indukcí podle složitosti termů t_1, t_2. □

Důsledek 2.83. *Přímé součiny pologrup (grup, vektorových prostorů, okruhů, Booleových algeber) jsou opět pologrupy (grupy, vektorové prostory, okruhy, Booleovy algebry).*

Pozor! Přímý součin (alespoň dvou) oborů integrity není *nikdy* obor integrity, neboť $(0,1) \cdot (1,0) = (0,0)$. (Všimněte si: $0 \neq 1$.)

Poznámka 2.84. Přímý součin $\prod_{k \in K} \mathcal{A}_k$ je až na izomorfizmus

a) komutativní, tj. nezávislý na pořadí činitelů, např.: $\mathcal{A}_1 \times \mathcal{A}_2 \cong \mathcal{A}_2 \times \mathcal{A}_1$,

b) asociativní, tj. je možno jej libovolně uzávorkovat, např.: $\mathcal{A}_1 \times \mathcal{A}_2 \times \mathcal{A}_3 \cong (\mathcal{A}_1 \times \mathcal{A}_2) \times \mathcal{A}_3 \cong \mathcal{A}_1 \times (\mathcal{A}_2 \times \mathcal{A}_3)$.

V následujícím textu symbolem C_n označíme cyklickou grupu řádu n.

Věta 2.85. *Grupa $C_n \times C_m$ je cyklická* $\Leftrightarrow \mathrm{NSD}(m,n) = 1$.

Důkaz. Buď $C_n = \langle x \rangle$, $C_m = \langle y \rangle$.
$\Rightarrow$ (nepřímo): $\mathrm{NSD}(n,m) > 1 \Rightarrow k := \mathrm{NSN}(n,m) < nm$ (neboť $\mathrm{NSN}(n,m) = nm/\mathrm{NSD}(n,m)$) a $(x^i, y^j)^k = (x^{ki}, y^{kj}) = (e,e)$ (protože $n|ki$ a $m|kj$) $\Rightarrow \mathrm{o}(x^i, y^j)|k < nm \Rightarrow$ řád všech prvků množiny $C_n \times C_m$ je menší než $nm = |C_n \times C_m| \Rightarrow C_n \times C_m$ není cyklická.
$\Leftarrow$: Ukážeme, že $C_n \times C_m = \langle (x,y) \rangle$. Máme $(x,y)^t = (e,e) \Rightarrow x^t = e \wedge y^t = e \Rightarrow n|t \wedge m|t$ $\Rightarrow \mathrm{NSN}(n,m) = nm|t$ (jelikož $\mathrm{NSD}(n,m) = 1$). Tedy $nm|\mathrm{o}(x,y)$. Na druhé straně platí $(x,y)^{nm} = (x^{nm}, y^{nm}) = ((x^n)^m, (y^m)^n) = (e,e)$, takže $\mathrm{o}(x,y)|mn$. Proto $\mathrm{o}(x,y) = nm$. □

Důsledek 2.86. *Je-li $n = p_1^{e_1} \cdots p_k^{e_k}$ rozklad na prvočinitele čísla $n \in \mathbb{N}$, potom platí $C_n \cong C_{p_1^{e_1}} \times \cdots \times C_{p_k^{e_k}}$.*

Věta 2.87. *(Hlavní věta o konečně generovaných abelovských grupách) Je-li $G = \langle x_1, \ldots, x_m \rangle$* abelovská *grupa generovaná prvky $x_1, \ldots, x_m$, potom platí:*

$$G \cong C_\infty^k \times C_{n_1} \times \cdots \times C_{n_r},$$

přičemž $k \geq 0$ ($C_\infty^0 := \{e\}$), $n_i \in \mathbb{N}$, $r \geq 0$. Přitom platí: G je konečná $\Leftrightarrow k = 0$.

(C_∞ označuje nekonečnou cyklickou grupu.)

Důkaz této věty zde neuvádíme. Lze jej nalézt v mnoha učebnicích o algebře a teorii grup.

Příklad(y) 2.88. 1) Všechny abelovské grupy s 12 prvky jsou – až na izomorfizmus – dány grupami C_{12} ($\cong C_3 \times C_4$) a $C_2 \times C_6$ ($\cong C_2 \times C_2 \times C_3$).

2) Všechny abelovské grupy s 8 prvky jsou – až na izomorfizmus – dány grupami C_8, $C_2 \times C_4$ a $C_2 \times C_2 \times C_2$.

Kapitola 3

Svazy a Booleovy algebry

3.1 (Částečně) uspořádané množiny

Na začátku odstavce 2.2 jsme definovali: Jestliže M je množina a R binární relace na M, kde

1) $\forall x \in M : xRx$ (reflexivita) ,

2) $\forall x, y \in M : xRy \wedge yRx \Rightarrow x = y$ (antisymmetrie) ,

3) $\forall x, y, z \in M : xRy \wedge yRz \Rightarrow xRz$ (transitivita) ,

potom se R nazývá *(částečné) uspořádání* na M a (M, R) se nazývá *(částečně) uspořádaná* množina. Platí-li navíc

4) $\forall x, y \in M : xRy \vee yRx$ (srovnatelnost) ,

potom se (M, R) nazývá *řetězec* nebo *lineárně uspořádaná* množina.

Označení: Místo R se většinou píše "$\leq$". Dále klademe

$$\begin{aligned} x \geq y &:\Leftrightarrow y \leq x, \\ x < y &:\Leftrightarrow x \leq y,\ x \neq y, \\ x > y &:\Leftrightarrow x \geq y,\ x \neq y. \end{aligned}$$

Příklad(y) 3.1. 1) $(\mathbb{R}, \leq)$ je řetězec.

2) $(\mathbb{N}_0, |)$ je uspořádaná množina, ale není řetězec.

3) $(\mathcal{P}(M), \subseteq)$ je uspořádaná množina, ale pro $|M| \geq 2$ není řetězec.

Definice 3.2. Buď $(M, \leq)$ uspořádaná množina. Potom se $k \in M$ nazývá *nejmenší* (resp. *největší*) prvek množiny $M :\Leftrightarrow \forall x \in M : k \leq x$ (resp. $k \geq x$).

Příklad(y) 3.3. 1) $(\mathbb{R}, \leq)$ nemá nejmenší, resp. největší prvek.

2) $(\mathbb{N}_0, |)$ má 1 jako nejmenší a 0 jako největší prvek.

3) $(\mathcal{P}(M), \subseteq)$ má $\emptyset$ jako nejmenší a M jako největší prvek.

Poznámka 3.4. Existuje vždy nejvýše jeden nejmenší, resp. největší prvek, neboť platí: jsou-li k_1, k_2 nejmenší prvky, potom $k_1 \leq k_2 \wedge k_2 \leq k_1$, a proto $k_1 = k_2$. Analogicky pro největší prvky.

Definice 3.5. Buď $(M, \leq)$ uspořádaná množina. Potom se $m\ in M$ nazývá *minimální* (resp. *maximální*) prvek množiny $M :\Leftrightarrow \forall x \in M : x \leq m$ (resp. $x \geq m$) $\Rightarrow x = m$.

Každý nejmenší prvek je také minimální, každý největší je také maximální.

Věta 3.6. *a) Buď $(M, \leq)$ uspořádaná množina a $N \subseteq M$. Potom je $(N, \leq)$ rovněž uspořádaná množina. Je-li $(M, \leq)$ řetězec, potom také $(N, \leq)$ řetězec. Přitom $(N, \leq)$ zkráceně označuje $(N, \leq \cap(N \times N))$.*

b) Je-li $(M, \leq)$ uspožádaná množina, potom také $(M, \geq)$ je uspořádaná množina (tzv. „princip duality pro uspožádané množiny“). .

Duální pojmy:

$\leq$	$\geq$
nejmenší prvek	největší prvek
maximální prvek	minimální prvek

Tak například platí: m je maximální v $(M, \leq) \Leftrightarrow m$ je minimální v $(M, \geq)$.

Definice 3.7. Buď $(M, \leq)$ uspořádaná množina a $N \subseteq M$. Potom se nazývá $u \in M$ *dolní závora* množiny $N :\Leftrightarrow \forall x \in N : u \leq x$. Největší prvek množiny všech dolních závor se nazývá *infimum* množiny N, formálně: $\inf N$ nebo $\bigcap N$. Prvek $v \in M$ se nazývá *horní závora* množiny $N :\Leftrightarrow \forall x \in N : x \leq v$. Nejmenší horní závora se nazývá *supremum* množiny N, formálně: $\sup N$ nebo $\bigcup N$.

Příklad(y) 3.8. 1) V množině $(\mathbb{R}, \leq)$ odpovídají právě definované pojmy pojmům běžným v analýze.

2) V množině $(\mathbb{N}_0, |)$ platí pro $T \subseteq \mathbb{N}_0$, kde $T \neq \emptyset$: $\inf T = \mathrm{NSD}(T)$ a $\sup T = \mathrm{NSN}(T)$. Dále je $\inf \emptyset = 0$ a $\sup \emptyset = 1$.

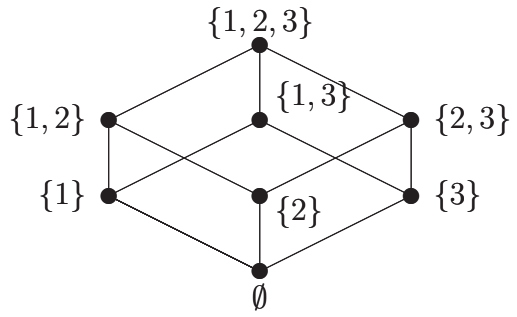
3) V množině $(\mathcal{P}(M), \subseteq)$ platí pro $\mathcal{S} \subseteq \mathcal{P}(M)$: $\inf \mathcal{S} = \bigcap \mathcal{S}$ a $\sup \mathcal{S} = \bigcup \mathcal{S}$.

Hasseův diagram. Buď $(M, \leq)$ konečná uspořádaná množina a nechť relace „sousední“ je definovaná takto:

$$a, b \text{ sousední } :\Leftrightarrow \begin{cases} 1)\ a < b \text{ nebo } b < a, \\ 2) \text{ neexistuje c takové, že } a < c < b \text{ nebo } b < c < a. \end{cases}$$

Potom je Hasseův diagram $(M, \leq)$ dán grafy relace „sousední“. (Množina uzlů je M; je-li $a < b$, nakreslí se uzel a „níže“ než uzel b a a se spojí s b hranou, pokud jsou a a b sousední.)

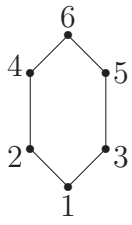
Příklad(y) 3.9. Hasseův diagram pro $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$ vypadá takto:

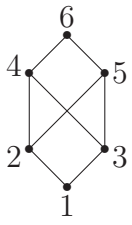


3.2 (Částečná)uspořádání a svazy

Definice 3.10. Buď $(V, \leq)$ uspořádaná množina. $(V, \leq)$ se nazývá *svazově uspořádaná* $:\Leftrightarrow$ $\sup\{a, b\}$ a $\inf\{a, b\}$ existují pro všechna $a, b \in V$.

Příklad(y) 3.11. Nechť jsou na $M = \{1, 2, 3, 4, 5, 6\}$ definovány dvě relace uspořádání $\leq$ a $\leq'$.

$(M, \leq)$: 

$(M, \leq')$: 

TexCadOptions

$(M, \leq)$ je svazově uspořádána (platí např. $\inf\{2, 3\} = 1$ a $\sup\{2, 3\} = 6$). Naproti tomu $(M, \leq')$ *není* svazově uspořádána: $\sup\{2, 3\}$ neexistuje, protože množina $\{2, 3\}$ má horní závory 4, 5 a 6, tedy nemá nejmenší horní závoru.

Lemma 3.12. *Buď $(V, \cap, \cup)$ svaz, potom platí:*

a) $\forall a \in V : a \cap a = a = a \cup a$,

b) $\forall a, b \in V : a \cap b = a \Leftrightarrow a \cup b = b$.

Důkaz. a) Na základě absorbčních zákonů platí: $a \cap a = a \cap (a \cup (a \cap a)) = a$ a $a \cup a = a \cup (a \cap (a \cup a)) = a$.

b) $\Rightarrow$: $a \cup b = (a \cap b) \cup b = b$, $\Leftarrow$: $a \cap b = a \cap (a \cup b) = a$ (rovněž podle absorpčních zákonů). □

Věta 3.13. *a) Buď $(V, \cap, \cup)$ svaz. Pokud definujeme relaci $\leq$ na V pomocí vztahu $a \leq b :\Leftrightarrow a \cap b = a$, $a, b \in V$, potom je $(V, \leq)$ svazově uspořádaná množina.*

b) Buď $(V, \leq)$ svazově uspořádaná množina. Definujeme-li na V binární operace $\cap, \cup$ pomocí vztahů $a \cap b := \inf\{a, b\}$, $a \cup b := \sup\{a, b\}$, $a, b \in V$, potom je $(V, \cap, \cup)$ svaz.

c) Přiřazení definovaná v a) a b) jsou navzájem inverzní.

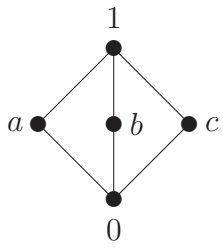
Důkaz. a) Relace $\leq$ je reflexivní ($a \leq a$ protože $a \cap a = a$), antisymetrická ($a \leq b \wedge b \leq a \Rightarrow a \cap b = a \wedge b \cap a = b \Rightarrow a = b$) a transitivní ($a \leq b \wedge b \leq c \Rightarrow a \cap b = a \wedge b \cap c = b \Rightarrow a \cap c = (a \cap b) \cap c = a \cap (b \cap c) = a \cap b = a$).
Ukážeme nyní, že $a \cap b = \inf\{a, b\}$. Platí $a \cap b \leq a, b$ ($a \cap b \cap a = a \cap b \cap b = a \cap b$); $x \leq a \wedge x \leq b \Rightarrow a \cap x = b \cap x = x \Rightarrow (a \cap b) \cap x = a \cap (b \cap x) = a \cap x = x \Rightarrow x \leq a \cap b$. Nakonec ukážeme, že platí $a \cup b = \sup\{a, b\} : a, b \leq a \cup b$ ($a \cup b \cup a = a \cup b \cup b = a \cup b$); $a, b \leq x \Rightarrow a \cup x = b \cup x = x \Rightarrow (a \cup b) \cup x = a \cup (b \cup x) = a \cup x = x \Rightarrow a \cup b \leq x$.

b) Musíme ukázat, že platí svazové zákony:
$a \cap b = \inf\{a, b\} = \inf\{b, a\} = b \cap a$.
$a \cap (b \cap c) = \inf\{a, \inf\{b, c\}\} = \ldots = \inf\{a, b, c\} = \ldots = \inf\{\inf\{a, b\}, c\} = (a \cap b) \cap c$.
$a \cap (a \cup b) = \inf\{a, \sup\{a, b\}\} = a$.
Analogicky se dokážou duální zákony.

c) $(V, \cap, \cup) \overset{\text{a)}}{\longmapsto} (V, \leq) \overset{\text{b)}}{\longmapsto} (V, \cap^*, \cup^*)$, přičemž $a \cap^* b = \inf\{a, b\} = a \cap b$ a $a \cup^* b = \sup\{a, b\} = a \cup b$.
$(V, \leq) \overset{\text{b)}}{\longmapsto} (V, \cap, \cup) \overset{\text{a)}}{\longmapsto} (V, \leq^*)$, přičemž $a \leq^* b \Leftrightarrow a \cap b = a \Leftrightarrow \inf\{a, b\} = a \Leftrightarrow a \leq b$. □

Každý konečný svaz je tak možno popsat nějakým Hasseovým diagramem.

Příklad(y) 3.14. 1)

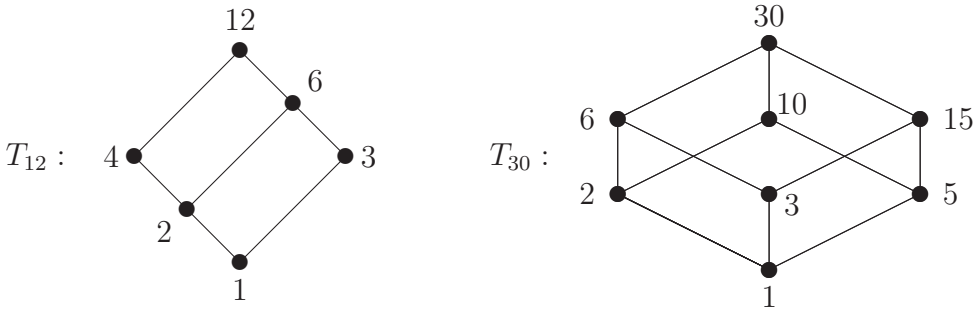


$\cap$	0	a	b	c	1
0	0	0	0	0	0
a	0	a	0	0	a
b	0	0	b	0	b
c	0	0	0	c	c
1	0	a	b	c	1

$\cup$	0	a	b	c	1
0	0	a	b	c	1
a	a	a	1	1	1
b	b	1	b	1	1
c	c	1	1	c	1
1	1	1	1	1	1

0 je nejmenší prvek a zároveň neutrální prvek pro operaci $\cup$. 1 je největší prvek a zároveň neutrální prvek pro operaci $\cap$.

2) 2) Svazy dělitelů $(T_n, \mathrm{NSD}, \mathrm{NSN})$, kde $T_n := \{t \in \mathbb{N} \mid t \text{ dělí } n\}$, $n \in \mathbb{N}$. Hasseovy diagramy



Princip duality pro svazy:

$$(V, \cap, \cup) \text{ svaz} \Leftrightarrow (V, \cup, \cap) \text{ svaz},$$
$$(V, \leq) \text{ svazově uspořádaný} \Leftrightarrow (V, \geq) \text{ svazově uspořádaný}.$$

3.3 Booleovy algebry

Na konci odstavce 1.2 jsme definovali: algebra $(B, \cap, \cup, 0, 1, ')$ typu $(2, 2, 0, 0, 1)$ se nazývá *Booleova algebra* $\Leftrightarrow$ platí následující zákony pro všechna $a, b, c \in B$:

$$\begin{aligned} a \cap b &= b \cap a & a \cup b &= b \cup a \\ a \cap (b \cap c) &= (a \cap b) \cap c & a \cup (b \cup c) &= (a \cup b) \cup c \\ a \cap (a \cup b) &= a & a \cup (a \cap b) &= a \\ a \cap (b \cup c) &= (a \cap b) \cup (a \cap c) & a \cup (b \cap c) &= (a \cup b) \cap (a \cup c) \\ 1 \cap a &= a & 0 \cup a &= a \\ a \cap a' &= 0 & a \cup a' &= 1 \end{aligned}$$

Princip duality:

$$(B, \cap, \cup, 0, 1, ') \text{ Booleova algebra} \Leftrightarrow (B, \cup, \cap, 1, 0, ') \text{ Booleova algebra}.$$

Lemma 3.15. *Buď $(V, \cap, \cup)$ svaz. Potom platí:*

a) $\forall a, b, c \in V : a \cap (b \cup c) = (a \cap b) \cup (a \cap c) \Leftrightarrow \forall a, b, c \in V : a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$,

b) $\forall a \in V : 0 \cup a = a \Leftrightarrow \forall a \in V : 0 \cap a = 0$,

c) $\forall a \in V : 1 \cap a = a \Leftrightarrow \forall a \in V : 1 \cup a = 1$,

Důkaz. a) $\Rightarrow$: $(a \cup b) \cap (a \cup c) = [\underbrace{(a \cup b) \cap a}_{a}] \cup [(a \cup b) \cap c] = \underbrace{a \cup (a \cap c)}_{a} \cup (b \cap c) = a \cup (b \cap c)$.
$\Leftarrow$: analogicky.
b) a c) plynou z $a \cap b = a \Leftrightarrow a \cup b = b$. □

Příklad(y) 3.16. $(\mathcal{P}(M), \cap, \cup, \emptyset, M, ')$, kde $A' = M \setminus A$ je Booleova algebra.

Věta 3.17. *(Věta o komplementech) Buď $(B, \cap, \cup, 0, 1, ')$ Booleova algebra. Potom platí:*

a) Jsou-li a, a^* prvky množiny B, kde $a \cup a^* = 1$ a $a \cap a^* = 0$, pak platí $a^* = a'$.

b) $(a')' = a$ pro všechna $a \in B$.

c) $0' = 1$ a $1' = 0$.

d) $(a \cup b)' = a' \cap b'$ a $(a \cap b)' = a' \cup b'$ pro všechna $a, b \in B$ (De Morganovy zákony).

Důkaz. a) bylo dokázáno na konci odstavce 1.2.

b) $a \cup a' = 1$, $a \cap a' = 0 \overset{\text{a)}}{\Longrightarrow} (a')' = a$.

c) $0 \cup 1 = 1$, $0 \cap 1 = 0 \overset{\text{a)}}{\Longrightarrow} 0' = 1$, $1' = 0$.

d) $(a \cup b) \cup (a' \cap b') = (a \cup b \cup a') \cap (a \cup b \cup b') = 1 \cap 1 = 1$, $(a \cup b) \cap (a' \cap b') = (a \cap a' \cap b') \cup (b \cap a' \cap b') = 0 \cup 0 = 0 \overset{\text{a)}}{\Longrightarrow} (a \cup b)' = a' \cap b'$. Analogicky se dokáže $(a \cap b)' = a' \cup b'$. □

Věta 3.18. *(Věta o homorfizmech) Buďte $(B, \cap, \cup, 0, 1, ')$ a $(C, \cap, \cup, 0, 1, ')$ Booleovy algebry, $\varphi : B \to C$ surjektivní zobrazení. Potom platí: φ je homomorfizmus $(B, \cap, \cup, 0, 1, ')$ do $(C, \cap, \cup, 0, 1, ') \Leftrightarrow \varphi$ je homomorfizmus $(B, \cap, \cup)$ do $(C, \cap, \cup)$ (tj. stačí, aby φ bylo konzistentní se svazovými operacemi.)*

Důkaz. $\Rightarrow$: triviální.
$\Leftarrow$: Jelikož $0 \cup a = a$, platí $\varphi(0) \cup \varphi(a) = \varphi(a)$ pro všechna $a \in B$. Protože φ je surjektivní, platí $\varphi(0) \cup c = c$ pro všechna $c \in C$. Tedy je $\varphi(0)$ neutrální prvek vzhledem k $\cup$ v C a proto $\varphi(0) = 0$. Analogicky se dokáže $\varphi(1) = 1$.
φ je kompatibilní s $'$: $a \cup a' = 1$, $a \cap a' = 0 \Rightarrow \varphi(a) \cup \varphi(a') = \varphi(1) = 1$, $\varphi(a) \cap \varphi(a') = \varphi(0) = 0$ $\Rightarrow \varphi(a') = \varphi(a)'$. □

3.4 Stoneova věta o reprezentaci

Definice 3.19. Buď $(V, \cap, \cup, 0, 1)$ svaz s nulovým a jdnotkovým prvkem. Potom se $a \in V$ nazývá *atom* $:\Leftrightarrow$

1) $0 < a$ a

2) $0 \leq b \leq a \Rightarrow b = 0 \vee b = a$

(tj. a je horním sousedním prvkem nulového prvku).

Lemma 3.20. *Buď $(B, \cap, \cup, 0, 1, ')$ konečná Booleova algebra. Potom ke každému prvku $b \in B \setminus \{0\}$ existuje atom $a \in B$, kde $a \leq b$. (Toto platí i pro libovolné konečné svazy.)*

Důkaz. Buď $b \in B \setminus \{0\}$. Je-li b atom, pak můžeme položit $a = b$. Není-li b atom, pak existuje $b_1 \in B$, kde $0 < b_1 < b$. Je-li b_1 atom, pak můžeme klást $a = b_1$. Jinak tímto postupem pokračujeme tak dlouho, až obdržíme řetězec $b > b_1 > b_2 > \ldots$, který, vzhledem k tomu, že B je konečná, musí skončit některým b_i. Potom položíme $a = b_i$. □

Věta 3.21. *(Stoneova věta) Buď $(B, \cap, \cup, 0, 1, ')$ konečná Booleova algebra a $M := \{a \in B \mid a$ atom algebry $B\}$. Potom platí:*

$$(B, \cap, \cup, 0, 1, ') \cong (\mathcal{P}(M), \cap, \cup, \emptyset, M, '),$$

přičemž vztahem $\varphi(b) := \{a \in M \mid a \leq b\}$ je dán izomorfizmus $\varphi : B \to \mathcal{P}(M)$.

Důkaz. Vzhledem k tomu, že $\varphi(b) \subseteq M$, φ je korektně definováno.

1) $\varphi(b \cup c) = \varphi(b) \cup \varphi(c)$:
$a \in \varphi(b \cup c) \Rightarrow a \leq b \cup c \Rightarrow a = a \cap (b \cup c) = (\underbrace{a \cap b}_{\leq a}) \cup (\underbrace{a \cap c}_{\leq a}) \Rightarrow a \cap b = a \vee a \cap c = a \Rightarrow$
$a \leq b \vee a \leq c \Rightarrow a \in \varphi(b) \vee a \in \varphi(c) \Rightarrow a \in \varphi(b) \cup \varphi(c)$.
$a \in \varphi(b) \cup \varphi(c) \Rightarrow a \in \varphi(b) \vee a \in \varphi(c) \Rightarrow a \leq b \vee a \leq c \Rightarrow a \leq b \cup c \Rightarrow a \in \varphi(b \cup c)$.

2) $\varphi(b \cap c) = \varphi(b) \cap \varphi(c)$:
$a \in \varphi(b \cap c) \Leftrightarrow a \leq b \cap c \Leftrightarrow a \leq b \wedge a \leq c \Leftrightarrow a \in \varphi(b) \wedge a \in \varphi(c) \Leftrightarrow a \in \varphi(b) \cap \varphi(c)$.

3) φ je surjektivní:
Buď $U \in \mathcal{P}(M)$, tj. $U \subseteq M$. Nechť $U = \{a_1, \ldots, a_r\}$ a $b := a_1 \cup \cdots \cup a_r$. Potom platí $\varphi(b) = \varphi(a_1 \cup \cdots \cup a_r) \overset{1)}{=} \varphi(a_1) \cup \cdots \cup \varphi(a_r) \overset{a_i \text{ atomy}}{=} \{a_1\} \cup \cdots \cup \{a_r\} = U$.

4) $\varphi(b') = \varphi(b)' = M \setminus \varphi(b)$, $\varphi(0) = \emptyset$, $\varphi(1) = M$ podle posledního zákona z odstavce 3.3.

5) φ je injektivní (tj. $b \neq c \Rightarrow \varphi(b) \neq \varphi(c)$):
Je-li $b \neq c$, potom platí $b \not\leq c$ nebo $c \not\leq b$. Bez újmy na obecnosti můžeme předpokládat $b \not\leq c$. Potom je $b \cap c' \neq 0$, neboť: $b \cap c' = 0 \Rightarrow b = b \cap 1 = b \cap (c \cup c') = (b \cap c) \cup (\underbrace{b \cap c'}_{0}) = b \cap c$
$\Rightarrow b \leq c$. Proto existuje $a \in M$ takové, že $a \leq b \cap c'$, tj. $a \leq b$ a $a \leq c'$, tedy $a \leq b$, ale $a \not\leq c$ (jinak by platilo $a \leq c \cap c' = 0$). Odtud plyne $a \in \varphi(b)$ a $a \notin \varphi(c)$, tj. $\varphi(b) \neq \varphi(c)$. □

Poznámka 3.22. 1) $|M| = |M_1| \Rightarrow (\mathcal{P}(M), \cap, \cup, \emptyset, M, ') \cong (\mathcal{P}(M_1), \cap, \cup, \emptyset, M_1, ')$.

2) $|M| = n \in \mathbb{N}_0 \Rightarrow |\mathcal{P}(M)| = 2^n$.

Důsledek 3.23. *Je-li B konečná Booleova algebra, potom platí $|B| = 2^n$ pro libovolné $n \in \mathbb{N}_0$. Ke každému $n \in \mathbb{N}_0$ tak existuje — až na izomorfizmus — přesně jedna Booleova algebra s 2^n prvky, totiž $\mathcal{P}(\{0, 1, \ldots, n-1\})$.*

Definice 3.24. Buď M množina. $\mathcal{K} \subseteq \mathcal{P}(M)$ se nazývá *množinový okruh* :⇔ pro všechna $A, B \in \mathcal{K}$ platí

1) $A \cup B \in \mathcal{K}$,

2) $A \cap B \in \mathcal{K}$ a

3) $A \cap B' = A \setminus B \in \mathcal{K}$.

Příklad(y) 3.25. $\mathcal{P}(M)$ je množinový okruh.

Definice 3.26. Buď $\mathcal{K} \subseteq \mathcal{P}(M)$ množinový okruh a nechť $M \in \mathcal{K}$. Potom Booleova algebra $(\mathcal{K}, \cap, \cup, \emptyset, M, ')$ se nazývá *algebra množinového okruhu* .

Algebra množinového okruhu je tedy podalgebra $(\mathcal{P}(M), \cap, \cup, \emptyset, M, ')$.

Příklad(y) 3.27. Buď $(0, 1]$ polootevřený interval číselné osy a $\mathcal{K} \subseteq \mathcal{P}((0, 1])$ množina daná vztahem $\mathcal{K} := \{\emptyset\} \cup \{\bigcup_{1 \le i \le n}(a_i, b_i] \mid 0 \le a_i < b_i \le 1,\ n \in \mathbb{N}\}$. Potom je $\mathcal{K}$ podalgebra algebry $(\mathcal{P}((0, 1]), \cap, \cup, \emptyset, (0, 1], ')$.

Následující větu uvádíme bez důkazu.

Věta 3.28. *(Stoneova věta) Každá Booleova algebra je izomorfní s nějakou algebrou množinového okruhu.*

Poznámka 3.29. $\mathcal{P}(M) \cong \{0, 1\}^M$ (potenční množina). (Každé podmnožině je přiřazena její charakteristická funkce.) Ze Stoneovy věty proto vyplývá: každá Booleova algebra B je izomorfní s nějakou podalgebrou jisté potenční množiny $\{0, 1\}^M$. Každý zákon v Booleově algebře $\{0, 1\}$ platný pro operace

$\cap$	0	1
0	0	0
1	0	1

$\cup$	0	1
0	0	1
1	1	1

$'$	
0	1
1	0

musí proto platit ve všech Booleových algebrách!

Poznámka 3.30. Analogické tvrzení platí také pro distributivní svazy. K tomu definujme: $\mathcal{V} \subseteq \mathcal{P}(M)$ se nazývá *množinový svaz* $:\Leftrightarrow$ pro všechna $A, B \in \mathcal{V}$ platí $A \cap B, A \cup B \in \mathcal{V}$. Platí potom (bez důkazu): Každý distributivní svaz je izomorfní s nějakým množinovým svazem. Odtud plyne: každý zákon, který platí v distributivním svazu $\{0, 1\}$ s výše uvedenými operacemi $\cap, \cup$, musí platit ve všech distributivních svazech.

Kapitola 4

Polynomy

4.1 Konstrukce okruhů polynomů

Definice 4.1. Buď $(R, +, 0, -, \cdot, 1)$ komutativní okruh s jednotkovým prvkem. Výraz tvaru $\sum_{k=0}^{\infty} a_k x^k$, kde $a_k \in R$ pro všechna $k \in \mathbb{N}_0$ a množina $\{k \in \mathbb{N}_0 \mid a_k \neq 0\}$ je konečná, se nazývá *polynom neurčité x nad R* . Množinu všech polynomů neurčité x nad R označíme symbolem $R[x]$. Definujme nyní operace $+, 0, -, \cdot, 1$ na $R[x]$ tak, aby $(R[x], +, 0, -, \cdot, 1)$ byl opět komutativní okruh s jednotkovým prvkem:

$$\sum_{k=0}^{\infty} a_k x^k + \sum_{k=0}^{\infty} b_k x^k := \sum_{k=0}^{\infty} (a_k + b_k) x^k, \quad 0 := \sum_{k=0}^{\infty} 0 \cdot x^k, \quad -\big(\sum_{k=0}^{\infty} a_k x^k\big) := \sum_{k=0}^{\infty} (-a_k) x^k,$$
$$\sum_{k=0}^{\infty} a_k x^k \cdot \sum_{k=0}^{\infty} b_k x^k := \sum_{k=0}^{\infty} \big(\sum_{l=0}^{k} a_l b_{k-l}\big) x^k, \quad 1 := \sum_{k=0}^{\infty} \delta_{0k} x^k.$$

Věta 4.2. *$(R[x], +, 0, -, \cdot, 1)$ je komutativní okruh s jednotkovým prvkem.*

Důkaz. Např. asociativní zákon pro násobení:

$$\big(\sum_{k=0}^{\infty} a_k x^k \sum_{k=0}^{\infty} b_k x^k\big) \sum_{k=0}^{\infty} c_k x^k = \sum_{k=0}^{\infty} \big(\sum_{l=0}^{k} a_l b_{k-l}\big) x^k \sum_{k=0}^{\infty} c_k x^k =$$
$$= \sum_{k=0}^{\infty} \big(\sum_{l=0}^{k} \big(\sum_{j=0}^{l} a_j b_{l-j}\big) c_{k-l}\big) x^k = \sum_{k=0}^{\infty} \big(\sum_{\substack{0 \le i,j,k \le k, \\ i+j+l=k}} a_i b_j c_l\big) x^k =$$
$$= \ldots = \sum_{k=0}^{\infty} a_k x^k \big(\sum_{k=0}^{\infty} b_k x^k \sum_{k=0}^{\infty} c_k x^k\big).$$

Analogicky se dokáží i ostatní zákony.

□

Polynomy neurčité x nad R, tedy prvky množiny $R[x]$, budeme značit $f(x)$, $p(x)$, ... V dalším textu budeme při zápisu polynomu $p(x) = \sum_{k=0}^{\infty} a_k x^k$ používat pravidlo, že ty členy $a_k x^k$, pro které platí $a_k = 0$, mohou být vynechány. Dále klademe $x^0 = 1$, tedy $a_0 x^0 = a_0$. Polynom $p(x)$ pak můžeme psát ve tvaru $p(x) = \sum_{k=0}^{n} a_k x^k = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$, kde $n \in \mathbb{N}_0$. Buď dále $q(x) = \sum_{k=0}^{m} b_k x^k$, $m \le n$, polynom. Kdy platí $p(x) = q(x)$? Zřejmě platí $q(x) = \sum_{k=0}^{n} b_k x^k$, přičemž $b_k = 0$ pro $m < k \le n$. Máme tedy $p(x) = q(x) \Leftrightarrow a_k = b_k$ pro $k = 0, \ldots, n$.

S polynomy budeme počítat podle zákonů komutativního okruhu $R[x]$ s jednotkovým prvkem.

Definice 4.3. Je-li $p(x) = \sum_{k=0}^{n} a_k x^k$, kde $a_n \neq 0$, pak se n nazývá *stupeň* polynomu $p(x)$ (píšeme $n = \operatorname{grad} p(x)$).

Platí: $\operatorname{grad}(p(x)+q(x)) \leq \max(\operatorname{grad} p(x), \operatorname{grad} q(x))$ a $\operatorname{grad}(p(x)q(x)) \leq \operatorname{grad} p(x)+\operatorname{grad} q(x)$, jestliže $p(x), q(x), p(x)+q(x)$ a $p(x)q(x) \neq 0$. Polynomu 0 se obecně nepřiřazuje žádný stupeň.

Každý prvek $a \in R$ můžeme ztotožnit s polynomem $p(x) = a_0 \in R[x]$, kde $a_0 = a$. Máme tedy $R \subseteq R[x]$ a $(R, +, 0, -, \cdot, 1)$ je zřejmě podokruhem okruhu $(R[x], +, 0, -, \cdot, 1)$.

Definice 4.4. Je-li $p(x) = \sum_{k=0}^{n} a_k x^k \in R[x]$, pak se prvky a_k nazývají *koeficienty* polynomu $p(x)$. $0 \in R[x]$ je *nulový polynom*, $a \in R \subseteq R[x]$ se nazývá *konstantní* polynom. Platí-li $\operatorname{grad} p(x) = n$ a $a_n = 1$, pak se $p(x)$ nazývá *normovaný* polynom. Polynomy tvaru $ax + b$, kde $a \neq 0$, se nazývají *lineární* polynomy.

Věta 4.5. *Je-li R obor integrity, potom je také $R[x]$ obor integrity, a pro $p(x), q(x) \in R[x] \setminus \{0\}$ platí* $\operatorname{grad}(p(x)q(x)) = \operatorname{grad} p(x) + \operatorname{grad} q(x)$.

Důkaz. $p(x) = \sum_{k=0}^{n} a_k x^k$, $a_n \neq 0$, $q(x) = \sum_{k=0}^{m} b_k x^k$, $b_m \neq 0 \Rightarrow p(x)q(x) = \sum_{k=0}^{n+m} c_k x^k$, kde $c_k = \sum_{j=0}^{k} a_j b_{k-j}$, speciálně tedy $c_{n+m} = a_n b_m \neq 0$. □

Poznámka 4.6. Není-li R obor integrity, pak ani $R[x]$ není obor integrity, neboť R je podokruh okruhu $R[x]$.

Polynomy n neurčitých $x_1, \ldots, x_n$

Indukcí se definuje:

$$R[x_1] := R[x], \qquad R[x_1, \ldots, x_n] := (R[x_1, \ldots, x_{n-1}])[x_n],\ n > 1.$$

Potom platí (důkaz úplnou indukcí podle n):

$$R[x_1, \ldots, x_n] = \{ \sum_{0 \leq i_1, \ldots, i_n \leq m} a_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n} \mid m \in \mathbb{N}_0,\ a_{i_1 \ldots i_n} \in R\}.$$

Např. prvek z $R[x_1, x_2]$ má obecný tvar: $p(x_1, x_2) = a_{00} + a_{10}x_1 + a_{01}x_2 + a_{20}x_1^2 + a_{11}x_1x_2 + a_{02}x_2^2 + \cdots + a_{jk}x_1^j x_2^k$.

4.2 Polynomy a funkce

Princip dosazování. Buď $(R, +, 0, -, \cdot, 1)$ komutativní okruh s jednotkovým prvkem a $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$. Pro $a \in R$ je potom $p(a) := a_n a^n + \cdots + a_1 a + a_0$ opět prvkem z R, který se nazývá *hodnota polynomu v a* . Funkce

$$\begin{cases} R \to R \\ a \mapsto p(a) \end{cases}$$

se nazývá *polynomiální funkce indukovaná polynomem* $p(x)$ a často se také označuje p.

Věta 4.7. *Zobrazení*

$$\varphi : \begin{cases} R[x] \to R \\ p(x) \mapsto p(a) \end{cases}$$

je pro pevně dané $a \in R$ surjektivní homomorfizmus $R[x]$ na R.

Důkaz. Buď $p(x) = \sum_{k=0}^{n} a_k x^k$ a $q(x) = \sum_{k=0}^{n} b_k x^k$. Potom platí

$$\varphi(p(x) + q(x)) = \sum_{k=0}^{n} (a_k + b_k) a^k = \sum_{k=0}^{n} a_k a^k + \sum_{k=0}^{n} b_k a^k = \varphi(p(x)) + \varphi(q(x)).$$

Analogicky je vidět, že $\varphi(p(x)q(x)) = \varphi(p(x))\varphi(q(x))$. Zbytek důkazu je triviální. □

Příklad(y) 4.8. Platí-li např. $f(x)^2 - g(x)h(x) + k(x) = f(x)^4 + k(x)^2$, kde $f(x), g(x), h(x), k(x) \in R[x]$, a je-li $a \in R$, pak také platí $f(a)^2 - g(a)h(a) + k(a) = f(a)^4 + k(a)^2$.

Definice 4.9. Buď $p(x) \in R[x]$ (R komutativní okruh s jednotkovým prvkem). Potom se $a \in R$ nazývá *kořen* polynomu $p(x) :\Leftrightarrow p(a) = 0$. Polynom $p(x)$ se nazývá *dělitelný* polynomem $q(x) \in R[x]$ (formálně: $q(x)|p(x)) :\Leftrightarrow p(x) = q(x)r(x)$, kde $r(x) \in R[x]$.

Věta 4.10. *Je-li a kořen polynomu $p(x)$, pak je $p(x)$ dělitelný lineárním polynom $x - a$ (a opačně).*

Důkaz. Buď $p(x) = a_n x^n + \cdots + a_1 x + a_0$. Vytvořme

$$\begin{aligned} q(x) &:= p(x) - a_n x^{n-1}(x - a) = b_{n-1}x^{n-1} + \cdots + b_1 x + b_0, \\ r(x) &:= q(x) - b_{n-1}x^{n-2}(x - a) = c_{n-2}x^{n-2} + \cdots + c_1 x + c_0, \\ s(x) &:= r(x) - c_{n-2}x^{n-3}(x - a) = d_{n-3}x^{n-3} + \cdots + d_1 x + d_0, \text{ atd.} \end{aligned}$$

Pak obdržíme $p(x) = a_n x^{n-1}(x - a) + q(x) = a_n x^{n-1}(x - a) + b_{n-1}x^{n-2}(x - a) + r(x) = a_n x^{n-1}(x - a) + b_{n-1}x^{n-2}(x - a) + c_{n-2}x^{n-3}(x - a) + s(x) = \ldots = a_n x^{n-1}(x - a) + \cdots + k_1(x - a) + k_0$. Vzhledem k tomu, že $0 = p(a) = a_n a^{n-1}(a - a) + \cdots + k_1(a - a) + k_0 = k_0$, je $k_0 = 0$ a $p(x) = (x - a)(a_n x^{n-1} + \cdots + k_1)$. Tedy $x - a$ dělí $p(x)$. (Vlastně jsme $p(x)$ podělili polynomem $x - a$ a obdrželi jsme zbytek $k_0 = 0$!) □

Dále nechť je R obor integrity (např. $R = \mathbb{Z}$ nebo R pole).

Je-li $\operatorname{grad} p(x) = n$ a platí $(x - a)^k | p(x)$, tj. $p(x) = (x - a)^k q(x)$, potom je $k + \operatorname{grad} q(x) = \operatorname{grad} p(x) = n$, z čehož plyne $k \leq n$.

Definice 4.11. Buď $p(x) \in R[x] \setminus \{0\}$ a nechť $a \in R$ je kořenem $p(x)$. Potom největší číslo $k \in \mathbb{N}$ takové, že $(x - a)^k | p(x)$, se nazývá *násobnost* kořene a. (Podle právě učiněné poznámky je $k \leq \operatorname{grad} p(x)$.)

Věta 4.12. *Nechť $a_1, \ldots, a_r$ jsou po dvou různé kořeny polynomu $p(x) \in R[x] \setminus \{0\}$ s násobnostmi $k_1, \ldots, k_r$. Potom platí:*

$$(x - a_1)^{k_1} \cdots (x - a_r)^{k_r} | p(x).$$

Důkaz. Pro $r = 1$ není co dokazovat. Pro $r > 1$ platí podle předpokladu $p(x) = (x - a_1)^{k_1} q_1(x) = (xa_2)^{k_2} q(x)$. Jelikož $p(a_2) = (a_2 - a_1)^{k_1} q_1(a_2) = 0$ a $(a_2 - a_1)^{k_1} \neq 0$, musí platit $q_1(a_2) = 0$, a proto $q_1(x) = (x - a_2)q_2(x)$. Tedy je $p(x) = (x - a_1)^{k_1}(x - a_2)q_2(x) = (x - a_2)^{k_2} q(x)$, tj. $(x - a_1)^{k_1} q_2(x) = (x - a_2)^{k_2 - 1} q(x)$. Pokud $k_2 - 1 > 0$, dostaneme analogicky $p(x) = (x - a_1)^{k_1} (x - a_2)^2 q_3(x) = (x - a_2)^{k_2} q(x)$, tj. $(x - a_1)^{k_1} q_3(x) = (x - a_2)^{k_2 - 2} q(x)$. Po k_2 krocích tak obdržíme $p(x) = (x - a_1)^{k_1}(x - a_2)^{k_2} q_{k_2+1}(x)$, tj. $(x - a_1)^{k_1}(x - a_2)^{k_2} | p(x)$. S ostatními kořeny $a_3, \ldots, a_r$ naložíme podobně a nakonec obdržíme tvrzení. □

Důsledek 4.13. *Nechť $a_1, \ldots, a_r$ jsou po dvou různé kořeny polynomu $p(x) \in R[x] \setminus \{0\}$ s násobnostmi $k_1, \ldots, k_r$. Potom platí: $k_1 + \cdots + k_r \leq \operatorname{grad} p(x)$.*

Polynom stupně n nad oborem integrity má tedy nejvýše n kořenů, přičemž každý kořen se počítá tolikrát, kolik je jeho násobnost.

Věta 4.14. *Buďte $p(x), q(x) \in R[x] \setminus \{0\}$, $\operatorname{grad} p(x), \operatorname{grad} q(x) \leq n$ a $p(b_i) = q(b_i)$ pro $n+1$ po dvou různých prvků $b_0, \ldots, b_n$ množiny R. Potom platí $p(x) = q(x)$.*

Důkaz. $(p-q)(b_i) = 0$ pro $0 \leq i \leq n \Rightarrow p - q$ má $n+1$ kořenů $\Rightarrow p - q = 0 \Rightarrow p = q$. □

Polynom nemusí mít žádné kořeny.

Příklad(y) 4.15. 1) $x^2 - 2 \in \mathbb{Q}[x]$ nemá kořeny v $\mathbb{Q}$, ale v $\mathbb{R} \supset \mathbb{Q}$ má, totiž $\pm\sqrt{2}$.

2) $x^2 + 1 \in \mathbb{R}[x]$ nemá kořeny v $\mathbb{R}$, ale v $\mathbb{C} \supset \mathbb{R}$ má, totiž $\pm i$.

Definice 4.16. Pole K se nazývá *algebraicky uzavřené* , jestliže každý polynom $p(x) \in K[x] \setminus K$ má aspoň jeden kořen.

Poznámka 4.17. Pokud má nad oborem integrity každý lineární polynom kořen, pak je tento obor integrity pole ($ax - 1$ $(a \neq 0)$ má kořen $c \Rightarrow ac = 1 \Rightarrow c = a^{-1}$).

Věta 4.18. *(Gaussova základní věta algebry) Pole $\mathbb{C}$ je algebraicky uzavřené.*

Věta 4.19. *Je-li K pole, potom jsou následující tvrzení ekvivalentní:*

a) K je algebraicky uzavřené.

b) Pro všechna $p(x) \in K[x]$, kde $\operatorname{grad} p(x) = n > 0$, platí $p(x) = c(x - b_1)^{k_1} \cdots (x - b_r)^{k_r}$, kde $b_1, \ldots, b_r, c \in K$ a $k_1 + \cdots + k_r = n$.

Důkaz. b) $\Rightarrow$ a): triviální.
a) $\Rightarrow$ b): Buď $p(x) \in K[x]$, $\operatorname{grad} p(x) > 0$. Potom existuje $a_1 \in K$ takové, že $p(a_1) = 0$, tj. $p(x) = (x - a_1)p_1(x)$. Je-li $\operatorname{grad} p_1(x) > 0$, obdržíme analogicky $p_1(x) = (x - a_2)p_2(x)$, tedy $p(x) = (x - a_1)(x - a_2)p_2(x)$. Další aplikací této úvahy nakonec obdržíme $p(x) = (x-a_1)(x-a_2)\cdots(x-a_n)c$. Pokud shrneme členy $(x-a_i)$ se stejnými mocninami dohromady, obdržíme tvar obsažený v tvrzení věty. □

Výpočet kořenů polynomů nad poli.
1) $\operatorname{grad} p(x) = 1$: triviální.
2) $\operatorname{grad} p(x) = 2$: $p(x) = ax^2 + bx + c$ $(a \neq 0)$ má kořeny $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ („2“ resp. „4“ zde označuje $1 + 1$ resp. $1 + 1 + 1 + 1$; vyjádření kořenů musí existovat a musí být $1 + 1 \neq 0$).
3) $\operatorname{grad} p(x) = 3, 4$: Cardanovy vzorce (Cardano Tartaglia).
4) $\operatorname{grad} p(x) > 4$: zde už neexistují obecné "vzorce"(vyžadující pouze základní početní postupy a odmocňování).

4.3 Interpolace pomocí polynomů

Buď K pole a $f : K \to K$ funkce.
Zadáno: $b_i = f(a_i)$ pro po dvou různá $a_i \in K$, $1 \leq i \leq n$ (např.: výsledek řady měření).
Hledá se: $p(x) \in K[x]$, kde $p(a_i) = b_i = f(a_i)$, $1 \leq i \leq n$, a $\operatorname{grad} p(x) < n$. (Existuje nejvýše jeden takový polynom $p(x)$: z $p(a_i) = q(a_i)$, $1 \leq i \leq n$, kde $\operatorname{grad} p(x), \operatorname{grad} q(x) < n$ totiž plyne $p = q$.)

Lagrangeovy interpolační vzorce:

Buď

$$q_i(x) := \prod_{\substack{1 \leq j \leq n, \\ j \neq i}} (x - a_j) = (x - a_1) \cdots (x - a_{i-1})(x - a_{i+1}) \cdots (x - a_n).$$

Potom platí:

$$q_i(a_k) = \begin{cases} 0 & \text{pro } i \neq k, \\ \displaystyle\prod_{1 \leq j \leq n, j \neq i} (a_k - a_j) \neq 0 & \text{pro } i = k. \end{cases}$$

Pro

$$p(x) := \sum_{i=1}^{n} b_i \frac{q_i(x)}{qi(a_i)}$$

platí potom $p(a_j) = b_j$, $1 \leq j \leq n$.

Důsledek 4.20. *Je-li K* konečné *pole (např. $K = \mathbb{Z}_p$, p prvočíslo), $f : K \to K$, potom existuje polynom $p(x) \in K[x]$ takový, že $f(a) = p(a)$ pro všechna $a \in K$.*

Newtonovy interpolační vzorce:

Buď K pole, $n \in \mathbb{N}$, $K_{n-1}[x] := \{p(x) \in K[x] \mid \operatorname{grad} p(x) < n\} \cup \{0\}$. Potom platí: $K_{n-1}[x] = \{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \mid a_i \in K\}$ je n-rozměrný vektorový prostor nad K s bází $\{1, x, \ldots, x^{n-1}\}$.

Snadno je vidět: Je-li $\varphi_i(x) \in K[x]$, $\operatorname{grad} \varphi_i(x) = i-1$, $1 \leq i \leq n$, potom je $\{\varphi_1(x), \ldots, \varphi_n(x)\}$ rovněž báze vektorového prostoru $K_{n-1}[x]$.

Buď nyní $f : K \to K$, $a_1, \ldots, a_n \in K$, $f(a_i) = b_i$, $1 \leq i \leq n$. Položíme-li $\varphi_1(x) := 1$ a

$$\varphi_i(x) := \prod_{j=1}^{i-1} (x - a_j), \qquad 2 \leq i \leq n,$$

pak je $\{\varphi_1(x), \ldots, \varphi_n(x)\}$ podle právě uvedené poznámky báze vektorového prostoru $K_{n-1}[x]$. Pro hledaný interpolační polynom $p(x)$ takový, že $p(a_i) = b_i$, $1 \leq i \leq n$, tedy musí platit

$$p(x) = \sum_{i=1}^{n} \lambda_i \varphi_i(x)$$

pro vhodné prvky $\lambda_i \in K$. Ty se dají vypočítat pomocí následujícího systému rovnic ve schodovitém tvaru:

$$\begin{aligned} p(a_1) &= b_1 = \lambda_1 \\ p(a_2) &= b_2 = \lambda_1 + \lambda_2(a_2 - a_1) \\ p(a_3) &= b_3 = \lambda_1 + \lambda_2(a_3 - a_1) + \lambda_3(a_3 - a_1)(a_3 - a_2) \\ &\vdots \end{aligned}$$

Výhoda této interpolační metody spočívá v tom, že přidáme-li jednu novou hodnotu $b_{n+1} = f(a_{n+1})$, zůstanou $\lambda_1, \ldots, \lambda_n$ nezměněny a je nutno pouze spočítat nové λ_{n+1}.

Kapitola 5

Obory integrity a dělitelnost

5.1 Jednoduchá pravidla dělitelnosti

Definice 5.1. Buď $(I, +, 0, -, \cdot, 1)$ obor integrity. Jsou-li $a, b \in I$, potom říkáme, že prvek a je *dělitelný* prvkem b a b se nazývá *dělitel* prvku a (b „dělí“ a, formálně: $b|a$) $:\Leftrightarrow \exists c \in I : a = bc$.

Elementární pravidla dělitelnosti:

1) $\forall a \in I : a|0$,

2) $\forall a \in I : 1|a$,

3) $\forall a \in I : a|a$,

4) $\forall a, b, c \in I : a|b \wedge b|c \Rightarrow a|c$,

5) $\forall a, b, c \in I : a|b \Rightarrow a|bc$,

6) $\forall a, b, c \in I : a|b \wedge a|c \Rightarrow a|b + c$,

7) $\forall a, b, c \in I, c \neq 0 : a|b \Leftrightarrow ac|bc$,

8) $\forall a, b, c, d \in I : a|b \wedge c|d \Rightarrow ac|bd$,

9) $\forall a, b \in I, n \in \mathbb{N} : a|b \Rightarrow a^n|b^n$.

Definice 5.2. Buď $(I, +, 0, -, \cdot, 1)$ obor integrity. Dělitel prvku 1 se nazývá *jednotka* oboru integrity I. Buď $E(I)$ množina všech jednotek I. Prvky $a, b \in I$ se nazývají *asociované* (formálně: $a \sim b$) $:\Leftrightarrow \exists e \in E(I) : a = be$.

Příklad(y) 5.3. 1) $I = \mathbb{Z}$: $E(I) = \{\pm 1\}$, tedy $a \sim b \Leftrightarrow a = \pm b$.

2) $I = K$ (K pole): $E(I) = K \setminus \{0\}$, tedy $a \sim b \Leftrightarrow a, b \neq 0 \vee a = b = 0$.

3) $I = K[x]$ (K pole): $E(I) = K \setminus \{0\}$ (jelikož $\operatorname{grad} p(x)q(x) = \operatorname{grad} p(x) + \operatorname{grad} q(x)$), platí $p(x) \sim q(x) \Leftrightarrow \exists a \in K \setminus \{0\} : p(x) = aq(x)$.

Věta 5.4. *a) $e \in I$ je jednotka oboru integrity $I \Leftrightarrow \exists f \in I : ef = 1$.*

b) $(E(I), \cdot)$ je abelovská grupa, která se nazývá grupa jednotek *oboru integrity I.*

c) $\sim$ je relace kongruence na $(I, \cdot)$.

d) $\forall a, b \in I : a \sim b \Leftrightarrow a|b \wedge b|a$.

Důkaz. a) Plyne bezprostředně z definice.

b) $1 \in E(I)$; $e_1, e_2 \in E(I) \Rightarrow \exists f_1, f_2 : e_1 f_1 = e_2 f_2 = 1 \Rightarrow (e_1 e_2)(f_1 f_2) = 1 \cdot 1 = 1 \Rightarrow e_1 e_2 \in E(I)$; $e \in E(I) \Rightarrow \exists f : ef = 1 \Rightarrow f \in E(I)$ a f je inverzní k e.

c) $a \sim a$, neboť $a = a \cdot 1$; $a \sim b \Rightarrow a = be \Rightarrow b = ae^{-1}$ $(e, e^{-1} \in E(I)) \Rightarrow b \sim a$; $a \sim b$, $b \sim c$ $\Rightarrow a = be$, $b = cf \Rightarrow a = c(ef) \Rightarrow a \sim c$ (protože $ef \in E(I)$). Tedy $\sim$ je relace ekvivalence. Dále platí: $a \sim b$, $c \sim d \Rightarrow a = be$, $c = df \Rightarrow ac = (bd)(ef) \Rightarrow ac \sim bd$.

d) $\Rightarrow$: $a \sim b \Rightarrow a = be$, $b = ae^{-1} \Rightarrow b|a \wedge a|b$.
$\Leftarrow$: $b|a \wedge a|b \Rightarrow a = bc \wedge b = ad \Rightarrow a = adc$. Pro $a = 0$ je také $b = 0$. Pro $a \neq 0$ je $1 = dc$, tedy $d, c \in E(I)$, tj. $a \sim b$. □

Příklad(y) 5.5. Třídy ekvivalence vzhledem k $\sim$:

1) $I = \mathbb{Z}$: $\{0\}$, $\{\pm 1\}, \{\pm 2\}, \ldots, \{\pm n\}, \ldots$, $n \in \mathbb{N}$.

2) $I = K$: $\{0\}, K \setminus \{0\}$.

3) $I = K[x]$: $\{0\}$, $\{ap(x) \mid a \in K \setminus \{0\},\ p(x)$ *normovaný*$\}$.

Definice 5.6. Buď $(I, +, 0, -, \cdot, 1)$ obor integrity, $a \in I$.
Triviální dělitelé prvku a jsou všechna $e \in E(I)$ a všechna b taková, že $b \sim a$.
Vlastní dělitelé prvku a jsou všechna b taková, že $b|a$, $b \notin E(I)$ a $b \not\sim a$.

Definice 5.7. Prvek $a \in I \setminus E(I)$, $a \neq 0$, se nazývá *ireducibilní prvek* $:\Leftrightarrow a$ má pouze triviální dělitele.

Příklad(y) 5.8. 1) $I = \mathbb{Z}$: $a \in I$ je ireducibilní prvek $\Leftrightarrow a = \pm p$, p prvočíslo.

2) $I = K[x]$ (K pole): Ireducibilní prvky se nazýají *ireducibilní polynomy* . Např. lineární polynom $ax + b$, $a \neq 0$ je vždy ireducibilní prvek. V algebraicky uzavřeném poli je každý ireducibilní polynom také lineární.

3) $I = \mathbb{R}[x]$: ireducibilní prvky jsou zde všechny lineární polynomy a polynomy $ax^2 + bx + c$, kde $a \neq 0$ a $b^2 - 4ac < 0$. (Ze základní věty algebry plyne, že žádné jiné neexistují.)

4) $I = K[x]$, K konečné pole: ke každému $n \in \mathbb{N}$ existuje polynom $p(x) \in K[x]$ takový, že $\operatorname{grad} p(x) = n$ a $p(x)$ je ireducibilní prvek. (viz odstavec 6.3)

Definice 5.9. $p \in I \setminus E(I)$, $p \neq 0$, se nazývá *prvočinitel* $:\Leftrightarrow p|ab \Rightarrow p|a \vee p|b$.

Příklad(y) 5.10. Pro $I = \mathbb{Z}, K[x]$ (K pole) platí: p je prvočinitel$\Leftrightarrow$ p je ireducibilní prvek (plyne z příkladů 5.8).

Poznámka 5.11. 1) a je ireducibilní prvek s $b \sim a \Rightarrow b$ je ireducibilní prvek.

2) p je prvočinitel a $q \sim p \Rightarrow q$ je prvočinitel.

3) p je prvočinitel $\Rightarrow p$ je ireducibilní prvek, neboť: $a|p \Rightarrow \exists b \in I : p = ab \Rightarrow p|ab \Rightarrow p|a \vee p|b$ a $a|p \wedge b|p$. Platí tedy $p \sim a \vee p \sim b$. V případě $p \sim b$ je $p = eb = ab$ pro některou jednotku e. Vzhledem k tomu, že $p \neq 0$, je $b \neq 0$, a proto $a = e$. Tedy v každém případě je a triviální dělitel p. (Tvrzení obrácené k tvrzení 3) obecně neplatí, protože např. 3 je ireducibilním prvkem, nikoliv však prvočinitelem, v oboru ointegrity všech komplexních čísel tvaru $a + ib\sqrt{5}$, $a, b \in \mathbb{C}$.)

5.2 Gaussovy okruhy

Definice 5.12. Obor integrity I se nazývá *Gaussův okruh* $:\Leftrightarrow$ Ke každému prvku $a \in I \setminus E(I)$, $a \neq 0$, existují prvočinitelé $p_1, \ldots, p_r$ (nikoliv nutně po dvou různí) tak, že platí $a = p_1 \cdots p_r$.

Věta 5.13. *(Jednoznačnost rozkladu na prvočinitele) Buď I Gaussův okruh, $a \in I \setminus E(I)$, $a \neq 0$, $a = p_1^{(1)} \cdots p_{r_1}^{(1)} = p_1^{(2)} \cdots p_{r_2}^{(2)}$, kde $p_i^{(1)}, p_j^{(2)}$ jsou prvočinitelé. Potom je $r_1 = r_2 =: r$ a existuje permutace π množiny $\{1, \ldots, r\}$ taková, že $p_i^{(1)} \sim p_{\pi(i)}^{(2)}$, $i = 1, \ldots, r$.*

Důkaz. Vzhledem k tomu, že $p_1^{(1)} | p_1^{(2)} \cdots p_{r_2}^{(2)}$, existuje $\pi(1)$, $1 \leq \pi(1) \leq r_2$, takové, že $p_1^{(1)} | p_{\pi(1)}^{(2)}$. Protože $p_{\pi(1)}^{(2)}$ je ireducibilní prvek, dostáváme $p_1^{(1)} \sim p_{\pi(1)}^{(2)}$. Pro vhodnou jednotku e_1 proto platí $e_1 p_2^{(1)} \cdots p_{r_1}^{(1)} = p_1^{(2)} \cdots p_{\pi(1)-1}^{(2)} p_{\pi(1)+1}^{(2)} \cdots p_{r_2}^{(2)}$. Opakovanou aplikací této úvahy nakonec obdržíme tvrzení. □

Příklad(y) 5.14. $\mathbb{Z}$ a $K[x]$ (K pole) jsou Gaussovy okruhy.

Definice 5.15. Buď I obor integrity, $a_1, \ldots, a_n \in I$.

1) $d \in I$ se nazývá *největší společný dělitel (NSD)* prvků $a_1, \ldots, a_n \in I :\Leftrightarrow$ (i) $d | a_i$, $i = 1, \ldots, n$ a (ii) $\forall t \in I : t | a_i$, $i = 1, \ldots, n \Rightarrow t | d$.

2) $v \in I$ se nazývá *nejmenší společný násobek (NSN)* prvků $a_1, \ldots, a_n \in I :\Leftrightarrow$ (i) $a_i | v$, $i = 1, \ldots, n$ a (ii) $\forall w \in I : a_i | w$, $i = 1, \ldots, n \Rightarrow v | w$.

Poznámka 5.16. Buď d NSD prvků $a_1, \ldots, a_n$ a $d_1 \in I$. Potom platí: d_1 je NSD prvků $a_1, \ldots, a_n \Leftrightarrow d_1 \sim d$. Podobné tvrzení platí i pro NSN.

Věta 5.17. *V Gaussově okruhu I je každý ireducibilní prvek prvočinitelem.*

Důkaz. $a \in I$, a ireducibilní prvek $\Rightarrow a \notin E(I)$, $a \neq 0 \Rightarrow a = p_1 \cdots p_r$, kde p_i jsou prvočinitelé $\Rightarrow p_1 | a$, $p_1 \notin E(I)$, tj. $p_1 \sim a \Rightarrow a$ je prvočinitel. □

Uvažujme faktorovou množinu $I/\sim = \{[a]_\sim \mid a \in I\}$ a nechť z každé třídy rozkladu $[a]_\sim = \{b \in I \mid b \sim a\}$ je vybrán pevný prvek $n([a]_\sim)$ (to je možné dle tzv. axiomu výběru, který užíváme), tj.

$$n : \begin{cases} I/\sim \to I \\ [a]_\sim \mapsto n([a]_\sim) \in [a]_\sim. \end{cases}$$

Prvky množiny $n(I/\sim)$ se nazývají *normované prvky* (vzhledem k n).

Každá třída $[a]_\sim$, kde a je prvočinitel, se skládá pouze z prvočinitelů. Prvky $n([a]_\sim)$, kde a je prvočinitel, se nazývají *normovaní prvočinitelé* .

Příklad(y) 5.18. 1) $I = \mathbb{Z}$, $n([a]_\sim) = n(\{\pm a\}) = |a|$.

2) $I = K[x]$, $n(\{0\}) = 0$, $n([p(x)]_\sim) = q(x)$, přičemž $p(x) = a_n x^n + \cdots + a_1 x + a_0$, $a_n \neq 0$, $q(x) = (1/a_n)p(x)$.

Věta 5.19. *Je-li I Gaussův okruh, $a \in I \setminus E(I)$, $a \neq 0$, potom platí $a = e p_1^{e_1} \cdots p_r^{e_r}$, kde $e \in E(I)$, $p_1, \ldots, p_r$ jsou normovaní navzájem různí prvočinitelé, $e_i \in \mathbb{N}$.*

Lemma 5.20. *Buď I Gaussův okruh, $a, b \in I \setminus \{0\}$, $a = fp_1^{f_1} \cdots p_r^{f_r}$, $b = gp_1^{g_1} \cdots p_r^{g_r}$ (p_j normovaní navzájem různí prvočinitelé, $f_j, g_j \in \mathbb{N}_0$, $f, g \in E(I)$). Potom platí: $a|b \Leftrightarrow f_j \leq g_j$ pro $j = 1, \ldots, r$.*

Důkaz. $a|b \Rightarrow \exists c \in I : b = ac \Rightarrow c = hp_1^{h_1} \cdots p_r^{h_r}$, $h_j \in \mathbb{N}_0$, $h \in E(I)$ (protože I je Gaussův okruh) $\Rightarrow f_j + h_j = g_j$, $j = 1, \ldots, r \Rightarrow f_j \leq g_j$, $j = 1, \ldots, r$.
Obráceně: Je-li $f_j \leq g_j$, $j = 1, \ldots, r$, pak platí pro $h_j := g_j - f_j \in \mathbb{N}_0$, $c := f^{-1}gp_1^{h_1} \cdots p_r^{h_r}$: $ac = b$, tj. $a|b$. □

Věta 5.21. *Buď I Gaussův okruh, $a_1, \ldots, a_n \in I$, $a_i \neq 0$, $a_i = e_i p_1^{e_{1i}} \cdots p_r^{e_{ri}}$, $e_i \in E(I)$, p_j navzájem různí normovaní prvočinitelé, $e_{ji} \in \mathbb{N}_0$. Potom platí:*

$$\mathrm{NSD}(a_1, \ldots, a_n) = p_1^{\min_{1 \leq i \leq n}(e_{1i})} \cdots p_r^{\min_{1 \leq i \leq n}(e_{ri})}$$

a

$$\mathrm{NSN}(a_1, \ldots, a_n) = p_1^{\max_{1 \leq i \leq n}(e_{1i})} \cdots p_r^{\max_{1 \leq i \leq n}(e_{ri})}.$$

Jsou-li některá $a_i = 0$, potom je $\mathrm{NSD}(a_1, \ldots, a_n) = \mathrm{NSD}(a_i \mid a_i \neq 0)$; jsou-li všechna $a_i = 0$, potom je $\mathrm{NSD}(a_1, \ldots, a_n) = 0$. Jsou-li některá $a_i = 0$, pak je $\mathrm{NSN}(a_1, \ldots, a_n) = 0$.

Důkaz. Buď $d := p_1^{\min_{1 \leq i \leq n}(e_{1i})} \cdots p_r^{\min_{1 \leq i \leq n}(e_{ri})}$.
(i) $\min_i(e_{ji}) \leq e_{jk}$ pro všechna $k \in \{1, \ldots, n\} \Rightarrow d|a_k$, $k = 1, \ldots, n$.
(ii) $t|a_k$ pro všechna $k \in \{1, \ldots, n\} \Rightarrow t = fp_1^{f_1} \cdots p_r^{f_r}$, kde $f \in E(I)$, $f_j \leq e_{jk}$, $k = 1, \ldots, n$, $j = 1, \ldots, r \Rightarrow f_j \leq \min_i(e_{ji})$, $j = 1, \ldots, r \Rightarrow t|d$.
Zvláštní případy (některá nebo všechna $a_i = 0$) jsou triviální.
Tvrzení o NSN se dokáží pododbně jako pro NSD. □

Věta 5.22. *Buď I Gaussův okruh a $\cap, \cup$ binární operace na $I/\sim = \{[a]_\sim \mid a \in I\}$ definované vztahy*

$$[a]_\sim \cap [b]_\sim := [\mathrm{NSD}(a, b)]_\sim, \qquad [a]_\sim \cup [b]_\sim := [\mathrm{NSN}(a, b)]_\sim.$$

Potom jsou $\cap$ a $\cup$ korektně definovány (tj. nezávisle na volbě reprezentantů) a $(I/\sim, \cap, \cup)$ je svaz s nulovým prvkem $[1]_\sim = E(I)$ a jednotkovým prvkem $[0]_\sim = \{0\}$ („svaz dělitelů“). Příslušné uspořádání $\leq$ je dáno vztahem: $[a]_\sim \leq [b]_\sim :\Leftrightarrow a|b$.

Důkaz. Důkaz této věty plyne snadno z definic. □

Příklad(y) 5.23. $(\mathbb{Z}/\sim, \cap, \cup) \cong (\mathbb{N}_0, \mathrm{NSD}, \mathrm{NSN})$.

5.3 Eukleidovy okruhy

Definice 5.24. Obor integrity I se nazývá *Eukleidův okruh* :$\Leftrightarrow$ existuje zobrazení $H : I \setminus \{0\} \to \mathbb{N}_0$ (eukleidovské ohodnocení) s následující vlastností: pro všechna $a \in I \setminus \{0\}$, $b \in I$ existují $q, r \in I$ tak, že $b = aq + r$, kde $r = 0 \vee H(r) < H(a)$ (dělení se zbytkem) .

Příklad(y) 5.25. 1) $\mathbb{Z}$ je Eukleidův okruh, kde $H(a) := |a|$ (viz odstavec 1.3).

2) Každé pole je Eukleidův okruh ($q = a^{-1}b$, $r = 0$).

Věta 5.26. *$K[x]$ (K pole) je Eukleidův okruh, kde $H(p(x)) := \operatorname{grad} p(x)$, tj. pro $p(x) \neq 0$, $p_1(x)$ libovolné, je $p_1(x) = p(x)q(x) + r(x)$, kde $r(x) = 0$ nebo $\operatorname{grad} r(x) < \operatorname{grad} p(x)$.*

Důkaz. Buď $p(x) = a_m x^m + \cdots + a_1 x + a_0$, $a_m \neq 0$, $m = \operatorname{grad} p(x)$, $p_1(x) = b_n x^n + \cdots + b_1 x + b_0$. Pro $n < m$ lze zvolit $q(x) = 0$ a $r(x) = p_1(x)$. Pro $n \geq m$ nechť $p_2(x) := p_1(x) - b_n a_m^{-1} x^{n-m} p(x)$. Platí $p_2(x) = c_k x^k + \cdots + c_1 x + c_0$, kde $k \leq n-1$. Pro $k < m$ lze zvolit $q(x) = b_n a_m^{-1} x^{n-m}$ a $r(x) = p_2(x)$. Pro $k \geq m$ nechť $p_3(x) := p_2(x) - c_k a_m^{-1} x^{k-m} p(x)$. Platí $p_3(x) = d_l x^l + \cdots + d_1 x + d_0$, kde $l \leq k-1$. Pro $l < m$ lze zvolit $q(x) = b_n a_m^{-1} x^{n-m} + c_k a_m^{-1} x^{k-m}$ a $r(x) = p_3(x)$. Pro $l \geq m$ v postupu pokračujeme a po konečném počtu kroků obdržíme polynom $p_t(x)$ takový, že $p_t(x) = 0$ nebo $\operatorname{grad} p_t(x) < m$. □

Důsledek 5.27. *Pro libovolný polynom $p(x) \in K[x]$ a libovolný prvek $a \in K$ existuje $q(x) \in K[x]$ tak, že $p(x) = (x-a)q(x) + p(a)$.*

Důkaz. Buď $p(x) \in K[x]$ a $a \in K$. Podle předchozí věty existuje $q(x) \in K[x]$ a $r \in K$ tak, že $p(x) = (x-a)q(x) + r$. Zřejmě platí $p(a) = r$. □

Poznámka 5.28. Ukážeme způsob, jak určit $q(x)$ a $p(a)$ z předchozího důsledku. Je-li $p(x) = p \in K$, pak $q(x) = 0$ a $p(a) = p$. Nechť tedy $\operatorname{grad} p(x) = n > 0$, $p(x) = \sum_{k=0}^{n} a_k x^k$. Potom zřejmě $\operatorname{grad} q(x) = n-1$. Nechť $q(x) = \sum_{k=0}^{n-1} b_k x^k$. Pak máme $a_n = b_{n-1}$, $a_{n-1} = b_{n-2} - ab_{n-1}$, $\ldots$, $a_i = b_{i-1} - ab_i$, $\ldots$, $a_0 = p(a) - ab_0$. Odtud $b_{n-1} = a_n$, $b_{n-2} = a_{n-1} + ab_{b-1}$, $\ldots$, $b_{i-1} = a_i + ab_i$, $\ldots$, $b_0 = a_1 + ab_1$, $p(a) = a_0 + ab_0$. Koeficienty polynomu $q(x)$ a prvek $p(a)$ lze tedy určit pomoí tzv. Hornerova schématu

a_n	a_{n-1}	a_{n-2}	$\ldots$	a_1	a_0
0	ab_{n-1}	ab_{n-2}	$\ldots$	ab_1	ab_0
b_{n-1}	b_{n-2}	b_{n-3}	$\ldots$	b_0	$p(a)$

Ve schématu se nejprve napíše první řádek, pak se postupuje zleva po sloupcích a v každém sloupci se doplní prvek ležící ve druhém a třetím řádku - kažký prvek ve třetím řádku se obdrží součtem obou prvků, které leží ve stejném sloupci nad ním, je-li poslední prvek ve třetím řádku tabulky 0, pak je a kořenem polynomu $p(x)$.

Příklad(y) 5.29. Buď $p(x) = 4x^4 - x^2 + 2x + 5$, $a = -3$. Pomocí Hornerova schématu určíme polynom $q(x)$ a $p(a) \in \mathbb{Z}$ s vlastností $p(x) = (x-a)q(x) + p(a)$:

-3	4	0	-1	2	5
	4	-12	35	-103	314

Tedy $q(x) = 4x^3 - 12x^2 + 35x - 103$, $p(a) = 314$, tj.

$$4x^4 - x^2 + 2x + 5 = (x+3)(4x^3 - 12x^2 + 35x - 103) + 314.$$

Následující větu uvádíme bez důkazu.

Věta 5.30. *Každý Eukleidův okruh je Gaussův okruh.*

Eukleidův algoritmus pro výpočet NSD v Eukleidových okruzích.

Buď I Eukleidův okruh a $a, b \in I$. Pro $a = b = 0$ je $\mathrm{NSD}(a, b) = 0$. Nechť bez újmy na obecnosti $a \neq 0$.

$$\begin{array}{rcl} \text{Pak} & \exists q_1, r_1 \in I : b = aq_1 + r_1,\ r_1 = 0 \vee H(r_1) < H(a), \\ \text{pro } r_1 \neq 0 & \Rightarrow & \exists q_2, r_2 \in I : a = r_1 q_2 + r_2,\ r_2 = 0 \vee H(r_2) < H(r_1), \\ \text{pro } r_2 \neq 0 & \Rightarrow & \exists q_3, r_3 \in I : r_1 = r_2 q_3 + r_3,\ r_3 = 0 \vee H(r_3) < H(r_2), \\ & \vdots & \\ \text{obecně:} & & \\ \text{pro } r_i \neq 0 & \Rightarrow & \exists q_{i+1}, r_{i+1} \in I : r_{i-1} = r_i q_{i+1} + r_{i+1},\ r_{i+1} = 0 \vee H(r_{i+1}) < H(r_i). \\ & & \text{(Přitom je třeba dosadit } a = r_0 \text{ a } b = r_{-1}.) \end{array}$$

Po konečném počtu kroků (vzhledem k tomu, že $H(a) = H(r_0) > H(r_1) > H(r_2) > \ldots$) obdržíme k takové, že $r_k = 0$ a $r_{k-1} \neq 0$. Nyní dokážeme, že $r_{k-1} = \mathrm{NSD}(a, b)$. Platí

$$\begin{array}{r} r_{k-2} = r_{k-1} q_k + 0 \Rightarrow r_{k-1} | r_{k-2}, \\ r_{k-3} = r_{k-2} q_{k-1} + r_{k-1} \Rightarrow r_{k-1} | r_{k-3}, \\ r_{k-4} = r_{k-3} q_{k-2} + r_{k-2} \Rightarrow r_{k-1} | r_{k-4}, \\ \vdots \\ r_1 = r_2 q_3 + r_3 \Rightarrow r_{k-1} | r_1, \\ a = r_1 q_2 + r_2 \Rightarrow r_{k-1} | a, \\ b = a q_1 + r_1 \Rightarrow r_{k-1} | b, \end{array}$$

tedy platí $r_{k-1} | a \wedge r_{k-1} | b$. Pokud naopak platí $t | a \wedge t | b$, plyne z toho analogicky, že $t | r_1$, $t | r_2$, $t | r_3$, $\ldots$, $t | r_{k-1}$.

Pro okruhy hlavních ideálů jsme dokázali, že $\mathrm{NSD}(a, b) = ax + by$, kde $x, y \in I$. V Eukleidových okruzích můžeme x, y vypočítat následovně:

$$\begin{array}{r} \mathrm{NSD}(a, b) = r_{k-1} = r_{k-3} + r_{k-2}(-q_{k-1}) = r_{k-3} + (r_{k-4} - r_{k-3} q_{k-2})(-q_{k-1}) = \\ = r_{k-4} \underbrace{(-q_{k-1})}_{\in I} + r_{k-3} \underbrace{(1 + q_{k-2} q_{k-1})}_{\in I} = \ldots = ax + by. \end{array}$$

Příklad(y) 5.31. Pomocí Euklidova algoritmu nalezneme $\mathrm{NSD}(84, 245)$ v $\mathbb{Z}$ (místo $b = aq + r$ píšeme $b : a = q(r)$):

1) $245 : 84 = 2(77)$;

2) $84 : 77 = 1(7)$;

3) $77 : 7 = 11(0)$.

Tedy $\mathrm{NSD}(84, 245) = 7$.

Kapitola 6

Teorie polí

6.1 Minimální pole

Definice 6.1. Pole $(K, +, 0, -, \cdot, 1)$ se nazývá *minimální* , pokud nemá žádná jiná podpole než sebe sama.

Věta 6.2. *Každé pole má vždy jediné podpole, které je minimální.*

Důkaz. Buď L libovolné pole a $K := \bigcap\{M \subseteq L \mid M \text{ je podpole pole } L\}$, tj. K je nejmenší podpole pole L. Zřejmě je K minimální. Jsou-li $K_1, K_2 \subseteq L$ dvě minimální pole, potom je $K_1 \cap K_2$ podpolem pole K_1 a pole K_2, takže $K_1 = K_1 \cap K_2 = K_2$. □

Buď $(R, +, 0, -, \cdot, 1)$ okruh s jednotkovým prvkem a pro libovolné $n \in \mathbb{Z}$ položme

$$n \cdot 1 := \begin{cases} \overbrace{1 + 1 + \cdots + 1}^{n\text{–krát}}, & \text{pokud } n > 0, \\ 0, & \text{pokud } n = 0, \\ \underbrace{(-1) + (-1) + \cdots + (-1)}_{|n|\text{–krát}}, & \text{pokud } n < 0. \end{cases}$$

Potom $\{n \cdot 1 \mid n \in \mathbb{Z}\}$ je (cyklická) podgrupa grupy $(R, +, 0, -)$ generovaná prvkem 1 (neboť pro libovolné $m, n \in \mathbb{Z}$ máme $n \cdot 1 + m \cdot 1 = (n + m) \cdot 1$ - srovnej s výpočtem mocnin v grupách, odstavec 1.3). Platí dokonce:

Lemma 6.3. *Buď $(R, +, 0, -, \cdot, 1)$ okruh s jednotkovým prvkem. Pak $\{n \cdot 1 \mid n \in \mathbb{Z}\}$ je komutativní podokruh okruhu R s tímtéž jednotkovým prvkem 1, totiž podokruh generovaný prvkem 1.*

Důkaz. Pro libovolné $n, m \in \mathbb{Z}$, $n, m > 0$, je $(n \cdot 1)(m \cdot 1) = (\underbrace{1 + \cdots + 1}_{n\text{–krát}})(\underbrace{1 + \cdots + 1}_{m\text{–krát}}) = \underbrace{1 \cdot 1 + \cdots + 1 \cdot 1}_{nm\text{–krát}} = \underbrace{1 + \cdots + 1}_{nm\text{–krát}} = (nm) \cdot 1$; všechny ostatní případy se dokáží analogicky. Samozřejmě platí $1 \in \{n \cdot 1 \mid n \in \mathbb{Z}\}$ a také je zřejmé, že operace $\cdot$ je na $\{n \cdot 1 \mid n \in \mathbb{Z}\}$ komutativní. □

Definice 6.4. Buď $(R, +, 0, -, \cdot)$ okruh. Pak symbolem $\operatorname{char} R$ označíme *charakteristiku okruhu* R, tj. nejmenší číslo $n \in \mathbb{N}$ takové, že pro každé $a \in R$ platí $n \cdot a = 0$ (kde $n \cdot a := \underbrace{a + a + \cdots + a}_{n\text{–krát}}$). Pokud takové číslo neexistuje, pak klademe $\operatorname{char} R = 0$.

Je-li $(R, +, 0, -, \cdot, 1)$ okruh s jednotkovým prvkem a $n \in \mathbb{N}$, pak pro každé $a \in R$ platí $n \cdot a = 0$, právě když platí $n \cdot 1 = 0$ (platí-li $n \cdot 1 = 0$ a je-li $a \in R$ libovolný prvek, pak

máme $n \cdot a = \underbrace{a + a + \cdots + a}_{n-\text{krát}} = (\underbrace{1 + 1 + \cdots + 1}_{n-\text{krát}}) \cdot a = (n \cdot 1) \cdot a = 0 \cdot a = 0$; opačná implikace je zřejmá.) Je-li tedy R okruh s jednotkovým prvkem 1, pak $\operatorname{char} R$ je nejmenší číslo $n \in \mathbb{N}$, pro něž platí $n \cdot 1 = 0$, případně $\operatorname{char} R = 0$, pokud takové číslo neexistuje. Odtud ihned plyne, že platí

$$\operatorname{char} R = \begin{cases} \mathrm{o}(1), & \text{pokud } \mathrm{o}(1) \in \mathbb{N}, \\ 0, & \text{pokud } \mathrm{o}(1) = \infty. \end{cases}$$

Připomeňme, že $\mathrm{o}(1)$ značí řád prvku 1 v abelovské grupě $(R, +)$ (viz odstavec 1.3), tedy $\mathrm{o}(1) = |\{n \cdot 1 \mid n \in \mathbb{Z}\}|$ pokud je tato kardinalita konečná, jinak $\mathrm{o}(1) = \infty$. Dostáváme tedy následující tvrzení:

Důsledek 6.5. *Buď $(R, +, 0, -, \cdot, 1)$ okruh s jednotkovým prvkem. Potom platí*

$$\operatorname{char} R = \begin{cases} |\{n \cdot 1 \mid n \in \mathbb{Z}\}|, & \textit{pokud se jedná o konečnou kardinalitu,} \\ 0 & \textit{jinak.} \end{cases}$$

Příklad(y) 6.6. 1) Pro okruh zbytkových tříd $(\mathbb{Z}_n, +, 0, -, \cdot, 1)$ platí $\operatorname{char} \mathbb{Z}_n = n$ $(n \in \mathbb{N}_0)$.

2) $\operatorname{char} \mathbb{Z} = \operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$.

Následující dvě lemmata uvádíme bez důkazů:

Lemma 6.7. *Buď $(R, +, 0, -, \cdot, 1)$ okruh s jednotkovým prvkem a nechť $m = \operatorname{char} R$. Potom $\{n \cdot 1 \mid n \in \mathbb{Z}\} \cong \mathbb{Z}_m$.*

Lemma 6.8. *1) Je-li R obor integrity a $m = \operatorname{char} R$, potom také $\{n \cdot 1 \mid n \in \mathbb{Z}\}$, a tedy i $\mathbb{Z}_m$, je obor integrity, takže platí $m = 0$ nebo $m \in \mathbb{P}$ ($\mathbb{P}$ značí mmnožinu všech prvočísel).*

2) Je-li R obor integrity a $\operatorname{char} R \in \mathbb{P}$, potom $\{n \cdot 1 \mid n \in \mathbb{Z}\}$ je pole.

Věta 6.9. *Buď $(K, +, 0, -, \cdot, 1)$ pole takové, že $\operatorname{char} K \in \mathbb{P}$. Potom $\{n \cdot 1 \mid n \in \mathbb{Z}\}$ je minimální podpole pole K. V tomto případě tedy platí: minimální podpole pole K je izomorfní se $\mathbb{Z}_m$, kde $m = \operatorname{char} K$.*

Důkaz. Plyne bezprostředně z posledního lemmatu. □

Věta 6.10. *Buď $(K, +, 0, -, \cdot, 1)$ pole, kde $\operatorname{char} K = 0$. Potom je $\{\frac{n \cdot 1}{m \cdot 1} \mid n \in \mathbb{Z},\ m \in \mathbb{Z} \setminus \{0\}\}$ nejmenším podpolem a tudíž minimálním podpolem pole K. Toto minimální podpole je izomorfní s $\mathbb{Q}$. Přitom jsme položili $\frac{n \cdot 1}{m \cdot 1} := (n \cdot 1)(m \cdot 1)^{-1}$.*

Důkaz. Buď L podpole pole K. Potom platí: $1 \in L \Rightarrow \forall n \in \mathbb{Z} : n \cdot 1 \in L \Rightarrow \forall n, m \in \mathbb{Z},\ m \neq 0 : \frac{n \cdot 1}{m \cdot 1} \in L \Rightarrow P := \{\frac{n \cdot 1}{m \cdot 1} \mid n \in \mathbb{Z},\ m \in \mathbb{Z} \setminus \{0\}\} \subseteq L$.
Ukážeme nyní, že zobrazení $\varphi : \mathbb{Q} \to P$, $\frac{n}{m} \mapsto \frac{n \cdot 1}{m \cdot 1}$, je korektně definováno a je izomorfizmus.
φ je korektně definováno a je bijektivní: $\frac{n \cdot 1}{m \cdot 1} = \frac{p \cdot 1}{q \cdot 1} \Leftrightarrow (n \cdot 1)(m \cdot 1)^{-1} = (p \cdot 1)(q \cdot 1)^{-1} \Leftrightarrow (n \cdot 1)(q \cdot 1) = (m \cdot 1)(p \cdot 1) \Leftrightarrow (nq) \cdot 1 = (mp) \cdot 1 \Leftrightarrow nq = mp \Leftrightarrow \frac{n}{m} = \frac{p}{q}$.
φ je homomorfizmus: $\varphi(\frac{n}{m} \cdot \frac{p}{q}) = \varphi(\frac{np}{mq}) = \frac{(np) \cdot 1}{(mq) \cdot 1} = \frac{(n \cdot 1)(p \cdot 1)}{(m \cdot 1)(q \cdot 1)} = \frac{(n \cdot 1)}{(m \cdot 1)} \cdot \frac{(p \cdot 1)}{(q \cdot 1)} = \varphi(\frac{n}{m})\varphi(\frac{p}{q})$; analogicky se dokáže, že platí: $\varphi(\frac{n}{m} + \frac{p}{q}) = \varphi(\frac{n}{m}) + \varphi(\frac{p}{q})$. □

Důsledek 6.11. *Každé minimální pole je izomorfní se $\mathbb{Z}_p$ ($p \in \mathbb{P}$) nebo $\mathbb{Q}$.*

6.2 Rozšíření pole

Definice 6.12. Buďte K, L pole a K podpole pole L. Potom se L nazývá *nadpole* nebo *rozšíření* pole K.

Je-li L nadpole pole K, potom je L také vektorovým prostorem nad K s operacemi

$$\begin{aligned} a+b &\ldots \text{součet v } L \ (a,b \in L), \\ \lambda a &\ldots \text{součin v } L \ (a \in L, \lambda \in K). \end{aligned}$$

Existuje proto báze vektorového prostoru L nad K. Vztahem $\dim_K L =: [L:K]$ definujeme tzv. *stupeň rozšíření L pole K* . Je-li $[L:K] < \infty$, pak se L nazývá *konečné rozšíření* pole K.

Poznámka 6.13. 1) $[L:K] = 1 \Leftrightarrow L = K$.

2) Je-li $p(x) \in K[x]$ ireducibilní polynom stupně k, pak existuje rozšíření L pole K a prvek $\alpha \in L$ tak, že $p(\alpha) = 0$ a $\{1, \alpha, \ldots, \alpha^{k-1}\}$ je báze L nad K. Tedy platí $[L:K] = k$.

Definice 6.14. Buď L nadpole pole K a $\alpha \in L$. α se nazývá *algebraický* prvek nad K $:\Leftrightarrow \exists f(x) \in K[x] \setminus \{0\} : f(\alpha) = 0$. α se nazývá *transcendentní* prvek nad $K :\Leftrightarrow \nexists f(x) \in K[x] \setminus \{0\} : f(\alpha) = 0$.

Příklad(y) 6.15. 1) $\sqrt{2}$ je algebraický prvek nad $\mathbb{Q}$ ($f(x) = x^2 - 2$, $L = \mathbb{R}$).

2) $\sqrt[3]{3}$ je algebraický prvek nad $\mathbb{Q}$ ($f(x) = x^3 - 3$, $L = \mathbb{R}$).

3) i je algebraický prvek nad $\mathbb{R}$ ($f(x) = x^2 + 1$, $L = \mathbb{C}$).

4) e, π jsou transcendentní prvky nad $\mathbb{Q}$ (bez důkazu).

Definice 6.16. Je-li L nadpole pole K a $S \subseteq L$, pak definujeme rozšíření $K(S)$ pole K takto:

$$K(S) := \bigcap \{E \subseteq L \mid E \text{ je podpole pole } L, \text{ které obsahuje } K \cup S\}.$$

Je-li $S = \{u_1, \ldots, u_r\}$ konečné, pak píšeme $K(S) =: K(u_1, \ldots, u_r)$. Je-li speciálně $S = \{\alpha\}$ jednoprvkové, pak píšeme $K(S) =: K(\alpha)$ („jednoduché rozšíření“ pole K) .

Jednoduchá rozšíření $K(\alpha)$, $\alpha \in L \supseteq K$.

1. případ: Je-li α transcendentní prvek nad K, pak $K(\alpha) \cong K(x)$, kde $K(x)$ je tzv. *pole racionálních funkcí nad K*, tj. pole

$$K(x) = \{\frac{p(x)}{q(x)} \mid p(x), q(x) \in K[x], \ q(x) \neq 0\}$$

s obvyklými operacemi sčítání a násobení zlomků. Izomorfizmus je dán vztahem $\frac{p(\alpha)}{q(\alpha)} \leftrightarrow \frac{p(x)}{q(x)}$. Protože mocniny α^n jsou lineárně nezávislé, platí $[K(\alpha) : K] = \infty$.

2. případ: Je-li α algebraický prvek nad K, pak $K(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1} \mid a_i \in K\}$, kde k je stupeň tzv. *minimálního polynomu* kořene α vzhledem ke K, tedy polynomu $f(x)$ nejmenšího stupně nad K, který má kořen α. Přitom se obecně předpokládá, že $f(x)$ je normovaný (a pak je jednoznačně určen).

Příklad(y) 6.17. 1) Pro $\alpha \in K$ je $x - \alpha$ minimální polynom kořene α vzhledem ke K.

2) $x^2 - 2$ je minimální polynom kořene $\sqrt{2}$ vzhledem ke $\mathbb{Q}$.

3) $x^3 - 3$ je minimální polynom kořene $\sqrt[3]{3}$ vzhledem ke $\mathbb{Q}$.

4) $x^2 + 1$ je minimální polynom kořene i vzhledem ke $\mathbb{R}$.

Platí: $[K(\alpha) : K] = \operatorname{grad} f(x)$, přičemž $f(x)$ je minimální polynom kořene α vzhledem ke K. Báze vektorového prostoru $K(\alpha)$ je potom množina $\{1, \alpha, \ldots, \alpha^{k-1}\}$, kde $k = \operatorname{grad} f(x)$.

6.3 Konečná pole (Galoisova pole)

Buď K konečné pole. Potom platí $\operatorname{char} K = p \in \mathbb{P}$ a minimální podpole P pole K je izomorfní se $\mathbb{Z}_p$. Protože K je vektorový prostor nad podpolem P, existuje báze $\{a_1, \ldots, a_n\}$ vektorového prostoru K nad P ($[K : P] = n \in \mathbb{N}$). Proto platí $K = \{\lambda_1 a_1 + \cdots + \lambda_n a_n \mid \lambda_i \in P\}$ a $|K| = p^n$, neboť každý koeficient λ_i lze zvolit $|P| = p$ způsoby.

Otázka: Existuje při daném $p \in \mathbb{P}$ a $n \in \mathbb{N}$ pole K takové, že $|K| = p^n$?

Odpověď na tuto otázku dává následující věta, kterou uvádíme bez důkazu.

Věta 6.18. *Řád každého konečného pole je mocnina prvočísla p^n ($p \in \mathbb{P}$, $n \in \mathbb{N}$). Obráceně, ke každé mocnině prvočísla p^n existuje až na izomorfizmus jediné pole K takové, že $|K| = p^n$.*

Způsob zápisu pro K, kde $|K| = p^n$: $K = \mathrm{GF}(p^n)$ (*Galoisovo pole*) .

Věta 6.19. *Je-li K konečné pole, pak je grupa $(K \setminus \{0\}, \cdot)$ cyklická.*

Důkaz. Buď $a \in K \setminus \{0\}$ prvek maximálního řádu r. Musíme dokázat, že $r = p^n - 1$ (přičemž $|K| = p^n$). Buď $b \in K \setminus \{0\}$ libovolné, $\mathrm{o}(b) = s$. Uvažujme rozklady na prvočíselné činitele r a s: $r = p_1^{e_1} \cdots p_k^{e_k}$, $s = p_1^{f_1} \cdots p_k^{f_k}$. Máme

$$\mathrm{NSN}(r, s) \quad = \quad \prod_{i=1}^{k} p_i^{\max(e_i, f_i)} \quad = \quad \underbrace{p_1^{e_1} \cdots p_j^{e_j}}_{=: \tilde{r}} \underbrace{p_{j+1}^{f_{j+1}} \cdots p_k^{f_k}}_{=: \tilde{s}}, \qquad 1 \le j \le k.$$

Přitom platí $\mathrm{NSD}(\tilde{r}, \tilde{s}) = 1$ a $\mathrm{NSN}(\tilde{r}, \tilde{s}) = \tilde{r}\tilde{s} = \mathrm{NSN}(r, s)$. Buď $\tilde{a} := a^{r/\tilde{r}}$ a $\tilde{b} := b^{s/\tilde{s}}$. Potom $\mathrm{o}(\tilde{a}) = \tilde{r}$ (neboť $\tilde{a}^{\tilde{r}} = a^r = 1$ a $\mathrm{o}(a) = r$) a $\mathrm{o}(\tilde{b}) = \tilde{s}$ (analogicky).

Ukážeme nyní, že $\mathrm{o}(\tilde{a}\tilde{b}) = \tilde{r}\tilde{s} = \mathrm{o}(\tilde{a})\mathrm{o}(\tilde{b})$. Vzhledem k tomu, že $(\tilde{a}\tilde{b})^{\tilde{r}\tilde{s}} = (\tilde{a}^{\tilde{r}})^{\tilde{s}}(\tilde{b}^{\tilde{s}})^{\tilde{r}} = 1 \cdot 1 = 1$ platí $\mathrm{o}(\tilde{a}\tilde{b}) | \tilde{r}\tilde{s}$. Dále platí: $(\tilde{a}\tilde{b})^m = 1$ pro $m \in \mathbb{N} \Rightarrow \tilde{a}^m = \tilde{b}^{-m} \Rightarrow 1 = \tilde{a}^{m\tilde{r}} = \tilde{b}^{-m\tilde{r}} \Rightarrow \mathrm{o}(\tilde{b}) = \tilde{s} | -m\tilde{r} \Rightarrow \tilde{s} | m$. Analogicky: $\tilde{r} | m$. Z $\mathrm{NSD}(\tilde{r}, \tilde{s}) = 1$ tedy plyne $\tilde{r}\tilde{s} | m$.

Platí tedy $\mathrm{o}(\tilde{a}\tilde{b}) = \tilde{r}\tilde{s} = \mathrm{NSN}(r, s) = \frac{rs}{\mathrm{NSD}(r,s)} \le r$, protože r je maximální. Odtud obdržíme $s \le \mathrm{NSD}(r, s) \Rightarrow s = \mathrm{NSD}(r, s) \Rightarrow s | r$. Protože b bylo libovolné, platí $b^r = 1$ pro všechna $b \in K \setminus \{0\}$. Proto polynom $f(x) = x^r - 1 \in K[x]$ má $p^n - 1$ kořenů, takže platí $p^n - 1 \le r$. Zřejmě platí $r | p^n - 1$, tedy $r \le p^n - 1$. Odtud plyne $r = p^n - 1$. □

Nyní se budeme zabývat problémem zkonstruování konečného pole K, kde $|K| = p^n$ pro daná čísla $p \in \mathbb{P}$ a $n \in \mathbb{N}$, tedy Galoisova pole K=GF(p^n).

Každý generátor grupy $(K \setminus \{0\}, \cdot)$ se nazývá *primitivní prvek* K. Je-li α primitivní prvek K, pak $K = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{|K|-2}\}$. Buď $\mathbb{Z}_q$, $q \in \mathbb{P}$, minimální podpole pole K. Pak pro libovolný primitivní prvek α z K platí $K \cong \mathbb{Z}_q(\alpha)$ a α je algebraický prvek nad $\mathbb{Z}_q$ (neboť je kořenem polynomu $x^{|K|-1} - 1 \in \mathbb{Z}_q[x]$). Buď $f(x)$ minimální polynom kořene α vyhledem k $\mathbb{Z}_q$. Potom je $f(x)$ ireducibilní a platí

$$\mathbb{Z}_q(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{m-1} \mid a_i \in \mathbb{Z}_q\},$$

kde $m = \operatorname{grad} f(x)$. Odtud stáváme $|\mathbb{Z}_q(\alpha)| = q^m$ a z podmínky $|\mathbb{Z}_q(\alpha)| = |K| = p^n$ nyní vyplývá $q = p$ a $m = n$.

Při určování konečného pole K=GF(p^n), tj. při sestavování tabulek jeho operací, lze proto postupovat následujícím způsobem:

1) Za minimální podpole pole K se vezme $\mathbb{Z}_p$.

2) Zvolíme normovaný ireducibilní polynom $q(x) \in \mathbb{Z}_p[x]$ stupně n. Nechť např. $q(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_1x - a_0$, kde $a_i \in \mathbb{Z}_p$.

3) Položíme $q(\alpha) = 0$ a uvažujeme bázi $\{1, \alpha, \ldots, \alpha^{n-1}\}$ vektorového prostoru GF(p^n) nad $\mathbb{Z}_p$ (víme, že $[\mathrm{GF}(p^n) : \mathbb{Z}_p] = n$). Spočítáme použitím $q(\alpha) = 0$ (tj. $\alpha^n = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$) mocniny α. Platí-li $\alpha^{p^n-1} = 1$ a $\alpha^j \neq 1$ pro $1 \leq j < p^n - 1$, je α primitivní prvek GF(p^n). Jinak učiníme další pokus s novým polynomem $q(x)$.

Příklad(y) 6.20. Určení GF(9) = GF(3^2): Vezmeme $\mathbb{Z}_3 = \{0, 1, 2\}$ za minimální pole. Polynom $x^2 - x - 1 \in \mathbb{Z}_3[x]$ je ireducibilní, protože nemá v $\mathbb{Z}_3$ žádný kořen. Položíme $\alpha^2 - \alpha - 1 = 0$, tedy máme $\alpha^2 = \alpha + 1$, a uvažujeme bázi $\{1, \alpha\}$ vektorového prostoru GF(3^2). Spočítáme nyní prvky GF(9) i s jejich souřadnicemi v bázi $\{1, \alpha\}$:

Prvky	Vyjádření v souřadnicích
0	$(0, 0)$
$\alpha^0 = 1$	$(1, 0)$
$\alpha^1 = \alpha$	$(0, 1)$
$\alpha^2 = 1 + \alpha$	$(1, 1)$
$\alpha^3 = 1 + 2\alpha$	$(1, 2)$
$\alpha^4 = 2$	$(2, 0)$
$\alpha^5 = 2\alpha$	$(0, 2)$
$\alpha^6 = 2 + 2\alpha$	$(2, 2)$
$\alpha^7 = 2 + \alpha$	$(2, 1)$
$\alpha^8 = 1$	$(1, 0)$

Mocniny α^j, $0 \leq j < 8$, jsou navzájem různé, tedy je α primitivní prvek GF(9). Můžeme proto sestavit tabulku operací pole GF(9).
Násobení: $0 \cdot \alpha^i = 0$, $\alpha^i\alpha^j = \alpha^{(i+j) \bmod 8}$ ($(\mathrm{GF}(9) \setminus \{0\}, \cdot)$ je cyklická grupa).
Sčítání: např.

$$\begin{array}{ccccc} \alpha^2 & + & \alpha^4 & = & \alpha \\ \downarrow & & \downarrow & & \uparrow \\ (1,1) & + & (2,0) & = & (0,1) \end{array}$$

Cvičení

1. Buď $(A, \circ)$ algebra typu (2) taková, že platí:

   a) $\circ$ je asociativní,

   b) existuje levý jednotkový prvek e,

   c) ke každému $x \in A$ existuje $y \in A$ takové, že $y \circ x = e$.

   Dokažte, že potom je e jednotkovým prvkem a každé $x \in A$ je invertibilní.

2. Buď M libovolná množina, $\circ$ binární operace skládání funkcí definovaná na M^M a $f \in M^M$. Dokažte:

   a) $\circ$ je asociativní.

   b) id_M je jednotkový prvek vzhledem k $\circ$.

   c) f je injektivní $\Leftrightarrow$ f má levý inverzní prvek.

   d) f je surjektivní $\Leftrightarrow$ f má pravý inverzní prvek.

   e) f je bijektivní $\Leftrightarrow$ f je invertibilní.

3. Určete všechny dvojice (a, b) reálných čísel, pro která je operace daná vztahem

$$x \circ y = ax + by \quad (x, y \in \mathbb{R})$$

   asociativní na $\mathbb{R}$.

4. Buď A množina všech čtvercových matic řádu 2 tvaru

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}, \quad \text{kde } a, b \in \mathbb{Z}.$$

   Dokažte, že A tvoří vzhledem k násobení matic pologrupu, ve které existuje nekonečně mnoho levých jednotkových prvků, ale ani jeden pravý jednotkový prvek.

5. Uveďte všechny binární operace na $A = \{a, b\}$ a zjistěte, zda jsou komutativní, asociativní, invertibilní a zda pro ně existuje pravý (levý) jednotkový prvek.

6. Uveďte všechny binární operace $\circ$ na $A = \{a, b, c\}$ takové, že $\circ$ je komutativní a a je jednotkový prvek, a prozkoumejte, zda jsou asociativní a regulární.

7. Je možno následující tabulku operací doplnit tak, že $\circ$ se stane asociativní binární operací na $A = \{a, b, c, d\}$?

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	d	c	d
d				

8. Dokažte, že symetrická diference $A \triangle B := (A \cup B) \setminus (A \cap B)$ považovaná za binární operaci na potenční množině $\mathcal{P}(M)$ je asociativní, komutativní a invertibilní.

9. Buď A množina se dvěma binárními operacemi $+$ a $\cdot$. Buď přitom $\cdot$ distributivní nad $+$ a nechť existuje jednotkový prvek pro $\cdot$. Nechť je $+$ asociativní a regulární. Dokažte, že z toho plyne komutativita operace $+$.

10. Sestavte pro množinu D_3 všech pokrývajících zobrazení rovnostranného trojúhelníka, která se skládá ze tří otočení o $0°$, $120°$ resp. $240°$ a tří symetrií podle os trojúhelníka, tabulku pro operaci $\circ$ skládání zobrazení. Existuje jednotkový prvek vzhledem k $\circ$? Pokud ano, které prvky jsou invertibilní?

11. Dokažte: Je-li $(H, \cdot)$ pologrupa, potom platí pro $a_1, \ldots, a_n \in H$, $n \geq 3$, a $r, s \in \mathbb{N}_0$, $0 \leq r < s \leq n$:
$$a_1 \cdots a_n = a_1 \cdots a_r (a_{r+1} \cdots a_s) a_{s+1} \cdots a_n.$$

12. Dokažte sestavením tabulky operace, že všechny grupy s nejvýše čtyřmi prvky jsou komutativní.

13. Buď $(H, \circ)$ konečný grupoid. Dokažte: $\circ$ je s krácením $\Leftrightarrow$ $\circ$ je invertibilní.

14. Dokažte, že $(\mathbb{Q} \setminus \{-1\}, \circ)$, kde
$$a \circ b := a + b + ab,$$
tvoří abelovskou grupu.

15. Buď M množina a $S_M := \{f \in M^M \mid f \text{ bijektivní}\}$. Dokažte, že $(S_M, \circ)$ tvoří grupu, a vytvořte pro $M = \{1, 2, 3\}$ tabulku operace S_M.

16. Definujme na $\{e, a, b, c, d, f\}$ grupovou operaci $\cdot$ tak, že e se stane jednotkovým prvkem a platí vztahy $a^2 = b^3 = e$ a $ab = b^2a$. Kterou známou grupu tak dostaneme (až na označení prvků)?

17. Buď $A := \{r + s\sqrt{p} \mid r, s \in \mathbb{Q},\ r^2 + s^2 \neq 0\}$ pro pevné prvočíslo p. Dokažte, že A spolu s obyčejným násobením tvoří grupu.

18. Buď $(H, \cdot, e)$ monoid a $G := \{x \in H \mid x \text{ invertibilní}\}$. Dokažte, že zúžení $\cdot$ na $G \times G$ je binární operace na G a $(G, \cdot)$ je grupa.

19. Buď m pevné přirozené číslo a $\mathbb{Z}_m := \{0, 1, \ldots, m-1\}$. V $\mathbb{Z}_m$ buď definována binární operace $\oplus$:
$$a \oplus b := \begin{cases} a + b & \text{pro } a + b < m, \\ a + b - m & \text{pro } a + b \geq m. \end{cases}$$
Dokažte: $(\mathbb{Z}_m, \oplus)$ je abelovská grupa.

20. Dokažte: Grupa G s operací $\circ$ a jednotkovým prvkem e je abelovská, je-li splněna jedna z následujících podmínek:

    a) $a \circ a = e$ pro všechna $a \in G$.

    b) $(a \circ b)^2 = a^2 \circ b^2$ pro všechna $a, b \in G$.

    c) $b^{-1} \circ a^{-1} \circ b \circ a = e$ pro všechna $a, b \in G$.

    Platí také obrácená tvrzení?

21. Dokažte, že pro prvočíslo p tvoří množina $\{a+b\sqrt{p} \mid a,b \in \mathbb{Z}\}$ s obvyklými operacemi sčítání a násobení reálných čísel obor integrity.

22. Buď $n \in \mathbb{N}$ a $T_n := \{k \in \mathbb{N} \mid k \text{ dělí } n\}$. Dokažte, že T_ns operacemi

$$a \cap b := \mathrm{NSD}(a,b), \qquad a \cup b := \mathrm{NSN}(a,b) \qquad (a,b \in T_n),$$

tvoří distributivní svaz s nulou a jedničkou. Pro která n je tento svaz Booleovský svaz?

23. Určete řád všech prvků symetrické grupy S_4.

24. Dokažte: Okruh $(R,+,\cdot)$, ve kterém je každý prvek idempotentní , tj. ve kterém pro všechna $a \in R$ platí $a^2 = a$, je nutně komutativní.

25. Buď $(R,+,\cdot)$ okruh s právě jedním pravým neutrálním prvkem e vzhledem k násobení. Dokažte, že e je pak jednotkovým prvkem tohoto okruhu.

26. Dokažte: Komutativní okruh $(R,+,\cdot)$, kde $|R| > 1$, je pole, právě když pro každé $a \in R \setminus \{0\}$ má rovnice $axa = a$ v R právě jedno řešení.

27. Dokažte: $S := \{a + b\sqrt[3]{3} + c\sqrt[3]{9} \mid a,b,c \in \mathbb{Q}\}$ je podpole pole $(\mathbb{R},+,\cdot)$ (s obvyklými operacemi + a $\cdot$).

28. Nechť $(B,\cap,\cup,0,1,')$ je Booleova algebra a $+$, $-$, $\cdot$ nechť jsou definovány vztahy

$$x+y := (x \cap y') \cup (x' \cap y), \qquad -x := x, \qquad x \cdot y := x \cap y \qquad (x,y \in B).$$

Dokažte, že potom $(B,+,0,-,\cdot,1)$ je komutativní okruh s jednotkovým prvkem, ve kterém platí $x^2 = x$ pro všechna $x \in B$ (takovýto okruh se nazývá *Booleův okruh*).

29. Buď $(B,+,0,-,\cdot,1)$ komutativní okruh s jednotkovým prvkem, ve kterém platí $x^2 = x$ pro všechna $x \in B$, a nechť jsou na B definovány operace $\cap$, $\cup$, $'$ pomocí vztahů

$$x \cap y := x \cdot y, \qquad x \cup y := x + y + x \cdot y, \qquad x' := x + 1 \qquad (x,y \in B).$$

Dokažte, že potom $(B,\cap,\cup,0,1,')$ je Booleova algebra.

30. Dokažte, že přiřazení mezi Booleovými algebrami a Boleovými okruhy (tj. komutativními okruhy s jednotkovým prvkem a vlastností $x^2 = x$ pro každý prvek x) z příkladů 28 a 29 definují navzájem inverzní zobrazení.

31. Určete všechny podgrupy symetrické grupy S_3.

32. Dokažte: Je-li $(G,\cdot)$ grupa, potom je každá konečná neprázdná podpologrupa grupy $(G,\cdot)$ podgrupa.

33. Dokažte: $\{(12),(13),\ldots,(1n)\}$ je systém generátorů symetrické grupy S_n, $n \geq 2$. Návod: použijte fakt, že množina všech transpozic je systémem generátorů grupy S_n.

34. Dokažte, že
a) $\{(12),(23),\ldots,(n-1\,n)\}$ a
b) $\{(12),(12\ldots n)\}$
jsou systémy generátorů grupy S_n, $n \geq 2$.
Návod pro a): Využijte příklad 33.

35. Buď $(G, \cdot)$ grupa a $a \in G$. Dokažte, že $N(a) := \{x \in G \mid xa = ax\}$ je podgrupa grupy G. (Tato podgrupa se nazývá *normalizátor* prvku a.)

36. Dokažte: Je-li H podgrupa grupy G a $a \in G$, potom je také $a^{-1}Ha := \{a^{-1}xa \mid x \in H\}$ podgrupa grupy G.

37. Dokažte: $\mathbb{Q}$ je nejmenší podpole pole $\mathbb{R}$.

38. Dokažte: Je-li π relace ekvivalence na množině M a pro $a \in M$

$$[a]_\pi := \{b \in M \mid b\pi a\},$$

pak je $M/\pi := \{[a]_\pi \mid a \in M\}$ rozklad množiny M na třídy ekvivalence.

39. Dokažte: a) Je-li $\mathcal{P}$ rozklad množiny M na třídy ekvivalence a je-li relace π na M definovaná vztahem $a\pi b :\Leftrightarrow \exists C \in \mathcal{P} : a, b \in C$, potom je π relace ekvivalence a $M/\pi = \mathcal{P}$.
b) $\pi \mapsto M/\pi$ definuje bijektivní zobrazení množiny všech relací ekvivalence na M na množinu všech rozkladů množiny M na třídy ekvivalence.

40. Dokažte: Nechť M, N jsou množiny, $f : M \to N$ zobrazení a relace π_f nechť je definována následujícím způsobem:

$$x\pi_f y :\Leftrightarrow f(x) = f(y), \quad x, y \in M.$$

Potom platí: a) π_f je relace ekvivalence na M.
b) $[x]_{\pi_f} \mapsto f(x)$ definuje bijektivní zobrazení množiny M/π_f na $f(M)$.

V příkladech 41–44 značí G cyklickou grupu $G = \langle x \rangle$.

41. Dokažte: a) Je-li $\mathrm{o}(x) = m \in \mathbb{N}$, pak je G izomorfní s $(\mathbb{Z}_m, \oplus)$ (srovnej s př. 19).
b) Je-li $\mathrm{o}(x) = \infty$, pak je G izomorfní s $(\mathbb{Z}, +)$.

42. Dokažte: Každá podgrupa H grupy G je rovněž cyklická.

43. Dokažte: Je-li $\mathrm{o}(x) = m \in \mathbb{N}$, pak platí pro všechna $k \in \mathbb{Z}$: $\mathrm{o}(x^k) = m/\mathrm{NSD}(k, m)$.

44. Dokažte: Pro $\mathrm{o}(x) = m \in \mathbb{N}$ existuje ke každému děliteli t prvku m právě jedna podgrupa H grupy G taková, že $|H| = t$.

45. Určete všechny podgrupy symetrické grupy S_4. Návod: Je jich 30.

46. Buďte $\mathcal{A}, \mathcal{A}^*, \mathcal{A}^{**}$ algebry stejného typu. Dokažte:
a) Je-li f homomorfizmus $\mathcal{A}$ do $\mathcal{A}^*$ a g homomorfizmus $\mathcal{A}^*$ do $\mathcal{A}^{**}$, pak je $g \circ f$ homomorfizmus $\mathcal{A}$ do $\mathcal{A}^{**}$. Jsou-li f, g izomorfizmy, pak je také $g \circ f$ izomorfizmus.
b) Je-li f izomorfizmus $\mathcal{A}$ do $\mathcal{A}^*$, pak je f^{-1} izomorfizmus $\mathcal{A}^*$ do $\mathcal{A}$.

47. Dokažte: a) Endomorfizmy algebry $\mathcal{A}$ tvoří vzhledem k operaci skládání $\circ$ pologrupu.
b) Automorfizmy $\mathcal{A}$ tvoří vzhledem k operaci $\circ$ grupu. Tuto grupu určete pro $\mathcal{A} = S_3$.

48. Nechť $\mathcal{A}, \mathcal{A}^*$ jsou algebry stejného typu a f nechť je homomorfizmus $\mathcal{A}$ do $\mathcal{A}^*$. Dokažte:
a) Je-li U podalgebra algebry $\mathcal{A}$, potom je $f(U)$ podalgebra algebry $\mathcal{A}^*$.
b) Je-li U^* podalgebra algebry $\mathcal{A}^*$, potom je $f^{-1}(U^*)$ podalgebra algebry $\mathcal{A}$.

49. Buď $(G, \cdot)$ grupa. Dokažte, že vztah

$$h \sim g :\Leftrightarrow \exists x \in G : h = xgx^{-1}$$

definuje relaci ekvivalence na G a určete pro $G = S_3$ příslušný rozklad na třídy ekvivalence. Jaký výsledek je možno z tohoto faktu pro $G = S_4$ (obecně pro $G = S_n$) odvodit?

50. Nechť $(G, \cdot)$ je grupa a pro $x \in G$ nechť je $\varphi_x : G \to G$ definováno vztahem $\varphi_x(g) := xgx^{-1}$, $g \in G$. Dokažte: φ_x je automorfizmus grupy G (tzv. *vnitřní automorfizmus*) , a $\{\varphi_x \mid x \in G\}$ je podgrupa grupy automorfizmů grupy G.

51. Určete všechny normální podgrupy grupy S_4. Návod: Použijte př. 49.

52. Dokažte: Abelovská grupa G taková, že $|G| > 1$, je právě tehdy prostá, když má prvočíselný řád.

53. Dokažte: Okruh matic $M_n(K)$ nad polem K je vždy prostý.

54. Nechť G, H jsou grupy s jednotkovými prvky e, e^* a $f : G \to H$ nechť je homomorfizmus. Dokažte:
a) $\operatorname{Ker} f := \{a \in G \mid f(a) = e^*\}$ je normální dělitel grupy G.
b) f je monomorfizmus $\Leftrightarrow \operatorname{Ker} f = \{e\}$.

55. Pro grupu G definujeme *centrum* grupy G takto: $Z(G) := \{x \in G \mid \forall g \in G : xg = gx\}$.
a) Dokažte, že $Z(G)$ je normální podgrupa grupy G.
b) Určete centrum grupy S_n.

56. Určete až na izomorfizmus všechny čtyřprvkové okruhy s cyklickou aditivní grupou.

57. Buď G grupa a pro $a, b \in G$ definujme „komutátor“ $K(a, b)$ grupy G takto: $K(a, b) := aba^{-1}b^{-1}$. Dále nechť $K := \langle\{K(a, b) \mid a, b \in G\}\rangle$ je podgrupa grupy G generovaná množinou všech komutátorů. Dokažte:
a) K je normální podgrupa grupy G.
b) Je-li N normální podgrupa grupy G, potom platí: G/N je abelovská grupa $\Leftrightarrow$ $N \supseteq K$.

58. Dokažte: Jsou-li A, B ideály okruhu R, pak také $A + B$ a $A \cap B$ jsou ideály R.

59. Dokažte s využitím A_4, že nemusí ke každému kladnému děliteli řádu grupy existovat podgrupa tohoto řádu.

60. Buď G konečná grupa, N normální podgrupa grupy G a $m := [G : N]$. Dokažte, že $a^m \in N$ pro všechna $a \in G$.

61. Buď $(R, +, \cdot)$ komutativní okruh. Prvek $a \in R$ se nazývá *nilpotentní* , jestliže existuje $n \in \mathbb{N}$ takové, že $a^n = 0$. Dokažte, že množina I všech nilpotentních prvků okruhu R je ideál okruhu R a faktorový okruh R/I kromě nulového prvku neobsahuje žádné jiné nilpotentní prvky.

62. Dokažte, že v každém svazu platí:

$$a \leq b \wedge c \leq d \Rightarrow a \cap c \leq b \cap d \wedge a \cup c \leq b \cup d$$

(monotónnost svazových operací $\cap$ a $\cup$) .

63. Dokažte, že v každém svazu $(V, \cap, \cup)$ platí takzvané „distributivní nerovnosti“

$$x \cap (y \cup z) \geq (x \cap y) \cup (x \cap z), \qquad x \cup (y \cap z) \leq (x \cup y) \cap (x \cup z).$$

64. Sestavte Hasseovy diagramy všech svazů s nejvýše 6 prvky.

65. Buď $(M, \leq)$ uspořádaná množina taková, že existuje $\inf A$ pro všechna $A \subseteq M$. Dokažte, že potom pro všechna $A \subseteq M$ existuje také $\sup A$.

66. Dokažte, že množina všech podalgeber algebry $(A, (\omega_i)_{i \in I})$ tvoří vzhledem k množinové inkluzi svazově uspořádanou množinu, přičemž $\inf\{U_1, U_2\} = U_1 \cap U_2$, $\sup\{U_1, U_2\} = \langle U_1 \cup U_2 \rangle$.

67. Dokažte, že množina všech normálních podgrup nějaké grupy $(G, \cdot)$ s množinovou inkluzí tvoří svazově uspořádanou množinu, přičemž $\inf\{N_1, N_2\} = N_1 \cap N_2$, $\sup\{N_1, N_2\} = N_1 \cdot N_2$ (součin množin).

68. Dokažte, že množina všech ideálů nějakého okruhu s operacemi $\cap$ a $+$ (srovnej s př. 58) tvoří svaz.

69. Buď A algebra a $\mathrm{Con}(A)$ množina všech relací kongruence algebry A. Dokažte, že potom $(\mathrm{Con}(A), \subseteq)$ je svazově uspořádaná množina.

70. Určete Hasseův diagram svazu podgrup grupy symetrií D_4 čtverce.

71. Buď $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$, $f(x) \neq 0$ polynom a p/q racionální kořen $f(x)$ takový, že $p, q \in \mathbb{Z}$, $\mathrm{NSD}(p, q) = 1$.
a) Dokažte: $p | a_0$ a $q | a_n$.
b) Najděte všechny kořeny polynomu $12x^4 - 31x^3 + 27x^2 - 9x + 1$.

72. a) Určete kořeny polynomu $x^n - 1$ v $\mathbb{C}$ (n-té odmocniny z jednotky) .
b) Dokažte, že n-té odmocniny z jednotky tvoří v $\mathbb{C}$ vzhledem k násobení cyklickou grupu řádu n.

73. Je-li R komutativní okruh s jednotkovým prvkem a $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$, potom nechť $f'(x) := a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$ (*derivace* f). Dokažte, že pro všechna $f, g \in R[x]$, $a \in R$ platí:

$$(f + g)' = f' + g', \qquad (f \cdot g)' = f'g + g'f, \qquad (af)' = af'.$$

74. Dokažte: Je-li $f(x) \in \mathbb{R}[x]$, $z \in \mathbb{C}$ a $f(z) = 0$, pak je také $f(\bar{z}) = 0$.

75. Dokažte: a) Je-li $a \in I$ k-násobný kořen ($k > 1$) polynomu $p(x) \in I[x]$, pak je a aspoň $(k-1)$-násobný kořen polynomu $p'(x)$ (I obor integrity).
b) Jsou-li $p(x)$ a $p'(x)$ nesoudělné, pak má $p(x)$ pouze prosté kořeny. Platí také obrácené tvrzení?

76. Nechť $f : \mathbb{R} \to \mathbb{R}$ je funkce a nechť $f(1) = 2$, $f(-1) = 0$, $f(2) = 2$, $f(5) = -40$. Určete k zadaným hodnotám
a) Lagrangeův interpolační polynom,
b) Newtonův interpolační polynom.

77. Buď $I = \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$. Dokažte, že I s obvyklými operacemi součtu a součinu v $\mathbb{C}$ tvoří obor integrity, ve kterém je prvek 3 sice ireducibilní, ale není prvoičinitelem. Je I Gaussův okruh?

78. Určete v $\mathbb{Z}_2[x]$ všechny ireducibilní polynomy až do řádu 3.

79. Buď $D \neq 1$ celé číslo bez kvadratických dělitelů.
a) Určete pro $D < 0$ jednotky v $\mathbb{Z}[\sqrt{D}] := \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$. Návod: Uvažujte „normu“ $N(a + b\sqrt{D}) := a^2 - b^2 D$.
b) Dokažte, že pro $D = 2$ existuje v $\mathbb{Z}[\sqrt{D}] \subseteq \mathbb{R}$ nekonečně mnoho jednotek.

80. Buď I obor integrity a $a, b, c \in I$, přičemž $c \neq 0$. Dokažte: existuje-li $\mathrm{NSD}(ac, bc)$, pak také existuje $\mathrm{NSD}(a, b)$, a platí $c \cdot \mathrm{NSD}(a, b) \sim \mathrm{NSD}(ac, bc)$.

81. Dokažte: Jestliže K je pole a grupa $(K \setminus \{0\}, \cdot)$ je cyklická, pak je K konečné.

82. Dokažte, že $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$ s obvyklými operacemi v $\mathbb{C}$ je Eukleidův okruh (nazývaný *okruh celých Gaussových čísel*). Návod: Položte $H(z) := |z|^2$.

83. Určete v $\mathbb{Z}[i]$ NSD prvků $a = 3 - i$ a $b = 1 + 3i$ a vyjádřete jej ve tvaru $ax + by$, kde $x, y \in \mathbb{Z}[i]$.

84. Najděte v $\mathbb{Z}[i]$ faktorizace prvků $27 + 6i$ a $-3 + 4i$.

85. a) Určete v $\mathbb{Z}$ NSD čísel 6188 a 4709 a vyjádřete jej jako celočíselnou lineární kombinaci čísel 6188 a 4709.
b) Analogicky pro čísla 525 a 231.

86. a) Určete v $\mathbb{Q}[x]$ všechny NSD polynomů $4x^4 - 2x^3 - 16x^2 + 5x + 9$ a $2x^3 - 5x + 4$ a vyjádřete normovaný NSD jako lineární kombinaci obou polynomů.
b) Analogicky pro $2x^6 + 3x^5 - 4x^4 - 5x^3 - 2x - 2$ a $x^5 - 2x^3 - 1$.

87. Dokažte, že faktorový okruh $\mathbb{Z}_2[x]/(x^3 + x + 1)$ je pole, a demonstrujte na příkladu výpočet multiplikativního inverzního prvku (Eukleidovým algoritmem).

Dále buď K pole.

88. Nechť L je rozšíření pole K a E rozšíření pole L takové, že $[E : K] < \infty$. Dokažte, že platí $[E : K] = [E : L] \cdot [L : K]$ (věta o stupni).

89. Dokažte: Je-li α transcendentní nad K, pak je $K(\alpha) \cong K(x)$.

90. Dokažte: Je-li $\mathrm{char}\, K = 0$, pak má každý iredicibilní polynom $f(x) \in K[x]$ v každém rozšíření pole K pouze prosté kořeny.

91. Nechť $\mathrm{char}\, K = 0$ a nechť $u_1, \ldots, u_r \in L$ jsou algebraické prvky nad K, přičemž L je rozšíření pole K. Dokažte: Existuje $\alpha \in L$ takové, že $K(u_1, \ldots, u_r) = K(\alpha)$.

92. Najděte minimální polynom pro
a) $\sqrt{2}+\sqrt{3}$,
b) $\sqrt{3}+i$
nad $\mathbb{Q}$.

93. Buď $\alpha \in \mathbb{C}$ takové, že $\alpha^5 = 1$, ale $\alpha \neq 1$. Najděte minimální polynom pro α nad $\mathbb{Q}$.

94. Určete $\alpha \in \mathbb{C}$ tak, aby $\mathbb{Q}(i, \sqrt{3}) = \mathbb{Q}(\alpha)$.

95. Určete stupeň $\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15})$ nad $\mathbb{Q}$.

96. Pro $\alpha, \beta, \gamma \in \mathbb{C}$ kořeny polynomu $x^3 - 2$ určete stupeň $\mathbb{Q}(\alpha, \beta, \gamma)$ nad $\mathbb{Q}$.

97. Zkonstruujte tabulky operací konečného pole s 8 prvky.

98. Dokažte: Je-li K konečné pole charakteristiky p, potom $a \mapsto a^p$ $(a \in K)$ definuje automorfizmus na K.

99. Určete počet normovaných ireducibilních polynomů stupně 2 nad $\mathrm{GF}(q)$.

100. Dokažte: Je-li φ automorfizmus pole K a P minimální podpole pole K, pak platí $\varphi(a) = a$ pro všechna $a \in P$.

101. Buď K pole charakteristiky $p > 0$. Dokažte: $x^p + a \in K[x]$ je buďto ireducibilní, nebo p-tá mocnina lineárního polynomu.

102. Dokažte, že v $\mathbb{Z}_p[x]$ platí: $x^{p^k} - x | x^{p^n} = x \Leftrightarrow k|n$.

103. Dokažte: V $\mathrm{GF}(p^n)$ existuje ke každému kladnému děliteli k čísla n právě jedno podpole $\mathrm{GF}(p^k)$.

Seznam literatury

H. Bürger — D. Dorninger — W. Nöbauer: *Boolesche Algebra und Anwendungen*, Österr. Bundesverlag, Wien 1974.

D. Dorninger — W. B. Müller: *Allgemeine Algebra und Anwendungen*, B. G. Teubner, Stuttgart 1984.

G. Eigenthaler: *Begleitmaterial zur Vorlesung ALGEBRA*, Institut für Mathematik und Geometrie, Technische Universität Wien, 2004.

G. Fischer — R. Sacher: *Einführung in die Algebra*, B. G. Teubner, Stuttgart 1978.

J. B. Fraleigh: *A first course in abstract algebra*, Addison-Wesley, Reading (Massachusetts) 1976.

E. Fried: *Abstrakte Algebra — eine elementare Einführung*, Akadémiai Kiadó, Budapest 1983.

G. Grätzer: *Universal Algebra*, Second Edition, Springer-Verlag, New York 1979.

Th. W. Hungerford: *Algebra*, Springer-Verlag, 3. Auflage, New York 1984.

Th. Ihringer: *Allgemeine Algebra*, B. G. Teubner, Stuttgart 1993.

H. Kaiser: *Skriptum zur Vorlesung Algebra*, Institut für Algebra und Computermathematik, Technische Universität Wien 1999.

H. Kaiser — R. Lidl — J. Wiesenbauer: *Aufgabensammlung zur Algebra*, Akademische Verlagsgesellschaft, Wiesbaden 1975.

H. Kaiser — R. Mlitz — G. Zeilinger: *Algebra für Informatiker*, Springer-Verlag, Wien 1985.

O. Körner: *Algebra*, Akademische Verlagsgesellschaft, Frankfurt/Main 1974.

G. Kowol — H. Mitsch: *Algebra I, II*, Prugg-Verlag, Eisenstadt 1982/84.

R. Kochendörffer: *Einführung in die Algebra*, Wissenschaftsverlag, Berlin 1962.

E. Kunz: *Algebra*, Vieweg, Braunschweig 1991.

A. G. Kuroš: *Vorlesungen über allgemeine Algebra*, B. G. Teubner, Leipzig 1964.

S. Lang: *Undergraduate Algebra*, Springer-Verlag, New York 1987.

S. Lang: *Algebra*, Addison-Wesley, 3. Auflage, Reading (Massachusetts) 1993.

H. Lausch — W. Nöbauer: *Algebra of Polynomials*, North Holland, Amsterdam 1973.

R. Lidl — H. Niederreiter: *Introduction to finite fields and their applications*, Cambridge University Press, Cambridge 1986.

R. Lidl — G. Pilz: *Angewandte abstrakte Algebra I, II*, BI-Wissenschaftsverlag, Mannheim 1982.

R. Lidl — J. Wiesenbauer: *Ringtheorie und Anwendungen*, Akademische Verlagsgesellschaft, Wiesbaden 1980.

S. MacLane — G. Birkhoff: *Algebra*, Chelsea Publishing Company, New York 1988.

K. Meyberg: *Algebra 1, 2*, Carl Hanser Verlag, München 1975/76.

K. Meyberg — P. Vachenauer: *Aufgaben und Lösungen zur Algebra*, Carl Hanser Verlag, München 1978.

L. Rédei: *Algebra*, Pergamon Press, Oxford 1967.

E. Scholz (Hrsg.): *Geschichte der Algebra*, BI-Wissenschaftsverlag, Mannheim 1990.

G. Szász: *Einführung in die Verbandtheorie*, Akadémiai Kiadó, Budapest 1962.

B. L. van der Waerden: *Algebra I, II*, Springer-Verlag, Berlin 1966/67.