8 Algebra

Požadavky

- Grupa, okruh, těleso – definice a příklady
- Podgrupa, normální podgrupa, faktorgrupa, ideál
- Homomorfismy grup
- Dělitelnost a ireducibilní rozklady polynomů
- Rozklady polynomů na kořenové činitele pro polynom s reálnými, racionálními, komplexními koeficienty.
- Násobnost kořenů a jejich souvislost s derivacemi mnohočlenu

8.1 Grupa, okruh, těleso – definice a příklady

Definice *(algebra)*
Pro množinu A je zobrazení $\alpha : A^n \to A$, kde $n \in \{0, 1, ...\}$ *n-ární operace* (n je *arita*). Jsou-li $\alpha_i, i \in I$ operace arity Ω_i na A, pak $(A, \alpha_i | i \in I)$ je *algebra.*

Definice *(grupoid)*
Algebra s 1 binární operací je *grupoid.* V něm je $e \in G : e \cdot g = g \cdot e = g \ \forall g \in G$ *neutrální prvek.* Algebra s jednou asociativní binární operací a neutrálním prvkem vzhledem k ní je *monoid.* Nechť je dán monoid s neutrálním prvkem $(M, \cdot, e)$ a nějakým prvek $m \in M$. Potom řekneme, že prvek $m^{-1} \in M$ je *inverzní* k prvku m, pokud $m \cdot m^{-1} = m^{-1} \cdot m = e$. Prvek je *invertibilní*, pokud má nějaký inverzní prvek.

Poznámka
Každý grupoid obsahuje nejvýš 1 neutrální prvek. V libovolném monoidu platí, že pokud $(a \cdot b = e)$ & $(b \cdot c = e)$, pak $a = c$ (tj. inverzní prvek zleva a zprava musí být ten samý). Každý inverzní prvek je sám invertibilní.

Definice *(grupa)*
Algebra $(G, \cdot, ^{-1}, e)$ je *grupa*, pokud je $(G, \cdot, e)$ monoid a $^{-1}$ je operace inv. prvku (tedy unární operace, která každému prvku přiřadí prvek k němu inverzní). Grupa G je *komutativní (abelovská)*, pokud je operace $\cdot$ komutativní.

Příklady
Příklady grup:

- Množina $\mathbb{R}$ s operací sčítání, inverzním prvkem $-x$ a neutrálním prvkem 0
- Množina $\mathbb{R}_+$ (kladných reálných čísel, tedy bez nuly, protože k té bychom inverzní prvek nenašli) s operací násobení, inverzním prvkem x^{-1} a neutrálním prvkem 1
- Množina $\mathbb{Z}_n = \{0, \ldots, n-1\}$ pro n libovolné přirozené číslo; s operací sčítání modulo n, inverzním prvkem $(-x)$ modulo n a neutrálním prvkem 0
- Množina polynomů stupně $\leq n$ se sčítáním, opačným polynomem (s opačnými koeficienty) a neutrálním prvkem 0
- Množina všech permutací prvků $(1, \ldots, n)$ s operací skládání permutací, opačnou permutací (takovou, že její složení s původní dává identitu) a neutrálním prvkem **id** (na rozdíl od všech předchozích pro permutace délky větší než 3 není abelovská)
- Množina regulárních matic $n \times n$ s operací maticového násobení, inverzními maticemi a jednotkovou maticí (taktéž není obecně abelovská)

Definice *(okruh)*
Nechť $(R, +, \cdot, -, 0, 1)$ je algebra taková, že $(R, +, -, 0)$ tvoří komutativní grupu, $(R, \cdot, 1)$ je monoid a platí $a(b + c) = ab + ac$ a $(a + b)c = ac + bc \ \forall a, b, c \in R$ (tedy distributivita násobení vzhledem k sčítání[1]). Pak je $(R, +, \cdot, -, 0, 1)$ *okruh.*[2]

Příklady
Příklady okruhů:

- Množina $\mathbb{Z}$ s operacemi sčítání a násobení, inverzem vůči sčítání – unárním minus a neutrálními prvky 0 a 1.
- Množina všech lineárních zobrazení na $\mathbb{R}^n$ s operacemi sčítání a skládání, opačným zobrazením (kde $(-f)(x) = -(f(x))$), nulovým zobrazením a identitou (pro obecná zobrazení toto nefunguje, neplatí distributivita)

[1] Žemlička píše ve skriptech sčítání vůči násobení, ale v literatuře se to píše většinou obráceně (asi to ale bude to samé)
[2] "–" je v něm stále unární operace

Poznámka *(Vlastnosti okruhů)*
V okruhu $(R, +, \cdot, -, 0, 1)$ pro každé 2 prvky $a, b \in R$ platí:

1. $0 \cdot a = a \cdot 0 = 0$
2. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$
3. $(-a) \cdot (-b) = a \cdot b$
4. $|R| > 1 \;\Leftrightarrow\; 0 \neq 1$

Definice *(těleso)*
Těleso je okruh $(F, +, -, \cdot, 0, 1)$, pro který navíc platí, že pro každé $x \in F$ kromě nuly existuje $y \in F$ takové, že $x \cdot y = y \cdot x = 1$, tj. pro všechny prvky kromě nuly existuje inverzní prvek vůči operaci $\cdot$ – x^{-1}. Navíc v F musí platit, že $0 \neq 1$ (vyloučení triviálních okruhů).

Komutativní těleso je takové těleso, ve kterém je operace $\cdot$ komutativní.

Příklady
Příklady těles:

- Tělesa $\mathbb{C}$ a $\mathbb{R}$, oproti tomu $\mathbb{Z}$ nebo $\mathbb{N}$ nejsou tělesa - nemají inverzní prvek k násobení
- Racionální čísla $\mathbb{Q} = \{\frac{a}{b} \; | a, b \in \mathbb{Z}, b \neq 0\}$
- $\mathbb{Z}_{p^n} = \{0, \ldots, p^n - 1\}$, kde p je prvočíslo a n přirozené číslo – tzv. *Gallois field*, pro dané p a n existuje vždy až na isomorfismus (přejmenování prvků) jen jedno. - *každé kon. těleso má p^n prvků (KAM TO PATRI???)*
- $(\mathbb{Z}_p, +, -, \cdot, 0, 1)$ je komutativní těleso charakteristiky p, ted obor integrity

Všechna uvedená tělesa jsou komutativní.

Ukázka tělesa $GF(4) = GF(2^2)$

Pro čtyřprvkovou množinu $T = \{0, 1, a, b\}$ definujeme operace sčítání a násobení takto:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Pro takto definované operace $+$ a $\cdot$ platí všechny axiomy tělesa.

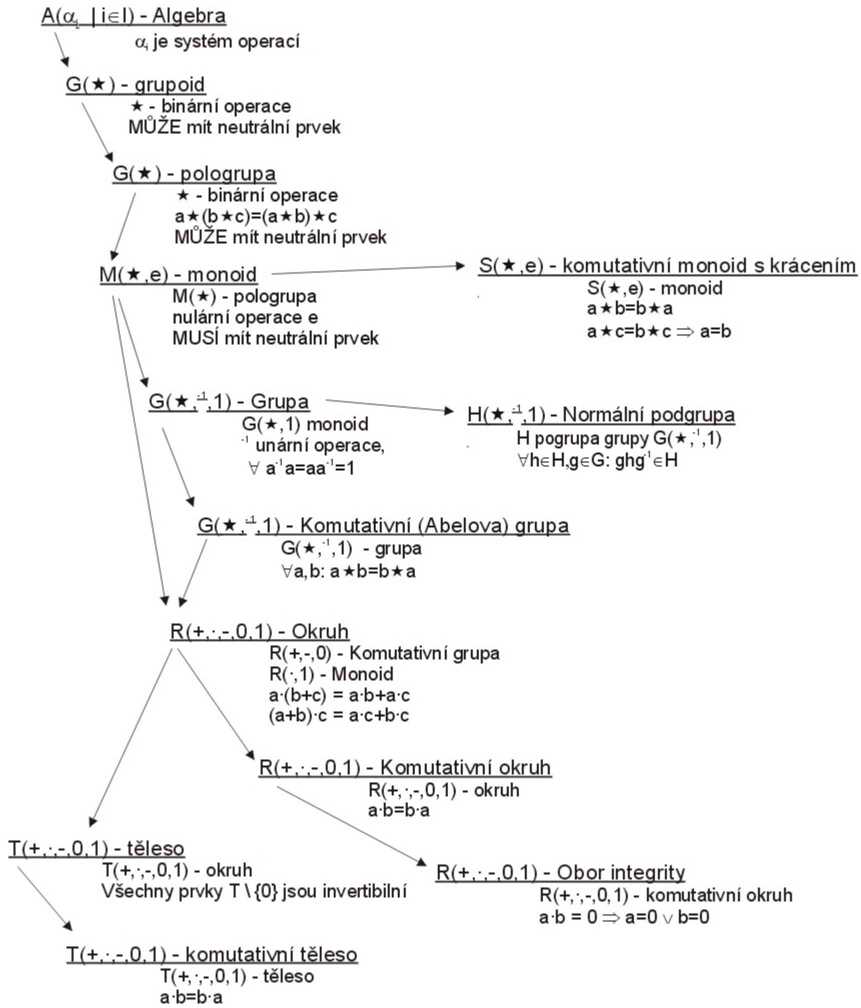
Jiný pohled na totéž těleso: vezmeme za prvky T polynomy maximálního stupně 1 s koeficienty v $\mathbb{Z}_2$, např. $a = x$, $b = x + 1$. Násobení pak provádíme modulo polynom $x^2 + x + 1$.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

★ **Věta** *(Wedderburnova věta)*
Všechna konečná tělesa jsou komutativní.

Report *(IOI 10.2.2011)*
Napište definici tělesa. Rozhodnete, zda existuje konene těleso řádu k pro hodnoty k z množiny $\{2, 3, 4, 6, 7, 8\}$. *Připomeňme, že řád tělesa je počet jeho prvků. Zvolte si nyní libovolné komutativni těleso T řádu 5,*
a) Popište pomocí tabulky, jak jsou v tomto tělese definovány operace sčítání a násobení
b)Vysvětlete, co znamená, že těleso T je komutativni.
c) Udejte příklad nekomutativního tělesa řádu 9 nebo zdůvodněte, proč takové těleso neexistuje



prostě dědičnost jako z C++

8.2 Podgrupa, normální podgrupa, faktorgrupa, ideál

Definice *(podalgebra)*
Množina B je *uzavřená* na operaci α, když $\forall b_1, \dots b_n \in B$ platí $\alpha(b_1, ...b_n) \in B$. Pro algebru $(A, \alpha_i | i \in I)$ je množina $B \subseteq A$ spolu s operacemi α_i *podalgebra* A, je-li množina B uzavřená na operaci α_i $\forall i \in I$.

Definice *(podgrupa)*
Podalgebra grupy je *podgrupa* (tj. jde o podmnožinu pův. množiny prvků, uzavřenou na $\cdot$ a $^{-1}$, spolu s původními operacemi). Podgrupa H grupy G je *normální*, pokud pro každé $g \in G$ (z původní množiny!) a pro každé $h \in H$ platí, že $g^{-1} \cdot h \cdot g \in H$ (někdy se píše zkráceně $G^{-1}HG \subseteq H$).

Poznámka *(Vlastnosti podgrup)*
Průnik podgrup $G \cap H$ je opět podgrupa. To určitě neplatí o sjednocení $G \cup H$ (to je podgrupou jen pokud je $G \subset H$ nebo $H \subset G$). Každá podmnožina grupy má nějakou nejmenší podgrupu, která ji obsahuje – to je *podgrupa generovaná* touto *množinou*. Podgrupa (i grupa) generovaná jedním prvkem se nazývá *cyklická*. Každá podgrupa cyklické grupy je také cyklická.

Podgrupy každé grupy společně s průnikem jako infimem a podgrupou generovanou sjednocením jako supremem tvoří úplný svaz (algebru se dvěma operacemi se speciálními vlastnostmi, supremem a infimem, definovanými pro všechny její podmnožiny). Úplný svaz se stejnými operacemi tvoří také normální podgrupy (jde o podsvaz prvního).

Poznámka *(Vlastnosti cyklických podgrup)*
Každá cyklická grupa G je komutativní (Abelova).

Důkaz. Protože x,y$\in G$ pak x,y=a$^m . a^n = a^{m+n} = a^{n+m} = y.x$

Příklady
Příklady podgrup:

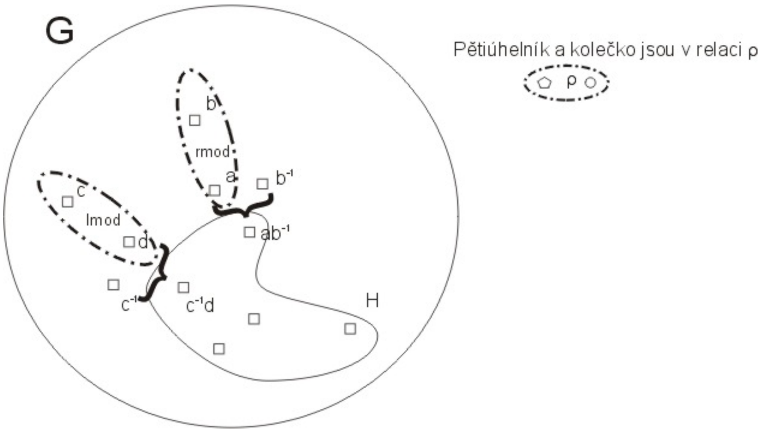
- grupa reálných čísel uzavřená na sčítání není cyklická
- G a $\{e\}$ jsou vždy normální podgrupy grupy $(G, \cdot, ^{-1}, e)$.
- Množina $Z(G) = \{z \in G | gz = zg \ \forall g \in G\}$ je normální podgrupou G (*centrum grupy*).
- $\mathbb{Z}_8$ má dvě netriviální podgrupy – $\{0, 4\}$ a $\{0, 2, 4, 6\}$ (je sama cyklická, takže obě jsou cyklické), plus samozřejmě triviální $\mathbb{Z}_8$ a $\{0\}$.
- grupa $(\mathbb{Z}_8^*, \cdot, 1)$ není cyklická, skládá se z 4 prvků: $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ a $3^2 = 5^2 = 7^2 = 1$ [3]

[3] je $\mathbb{Z}_8$ obsahující invertibilní prvky ($[0]_8$ ne)

Definice

Pro grupu G a její podgrupu H se relace rmod_H definuje předpisem $a, b \in G : (a, b) \in \mathrm{rmod}_H \equiv ab^{-1} \in H$. Symetricky se definuje relace lmod_H $((a, b) \in \mathrm{lmod}_H \equiv a^{-1}b \in H)$. Tyto relace jsou ekvivalence. *Index podgrupy v grupě* je $[G : H] = |G/\mathrm{rmod}_H| = |G/\mathrm{lmod}_H|$ (počet tříd ekvivalence podle rmod_H nebo lmod_H).

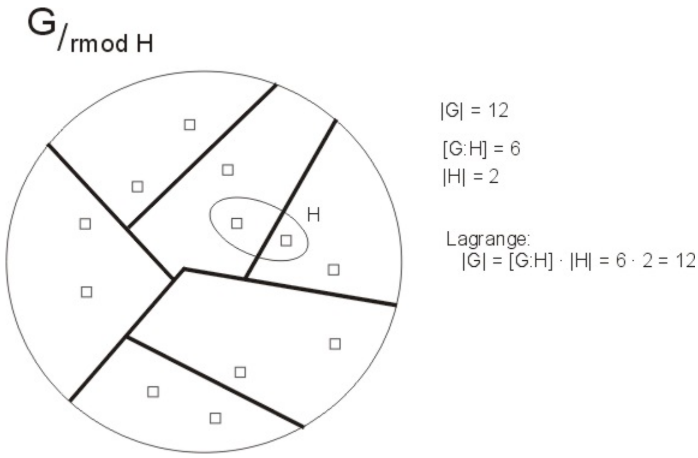
Řád G (počet jeho prvků) se značí $|G|$.



lmod, rmod. Mám grupu G a její podgrupu H. Potom $(a, b) \in \mathrm{rmod}H \leftrightarrow ab^{-1} \in H.(a, b) \in \mathrm{lmod}H \leftrightarrow a^{-1}b \in H$.

Věta *(Lagrangeova)*

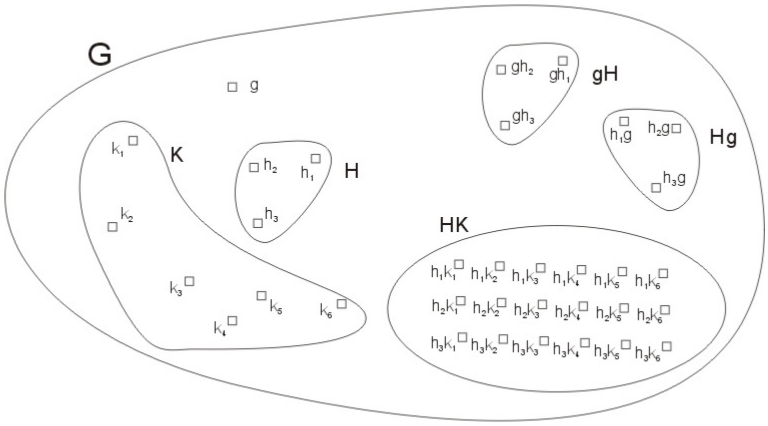
Pro grupu G a její podgrupu H platí: $|G| = [G : H] \cdot |H|$. Z toho plyne, že velikost podgrupy dělí velikost konečné grupy.



Index podgrupy H v grupě G ($[G : H]$) je prostě počet tříd ekvivalence relace rmod$H$. Dále řád grupy $|G|$ a ukázka Lagrangeovy věty v praxi.

Definice

$H, K \subseteq G(\cdot,^{-1}, 1),\ g \in G:\ HK = \{h.k|\ h \in H\, k \in K\},\ gH = \{g\}H,\ Hg = H\{g\}$



Definice *(faktorgrupa)*

Pro grupu $(G, \cdot,^{-1}, e)$ a nějakou její normální podgrupu N je *faktorgrupa* $G/N = \{gN|g \in G\}$ kde $gN = \{g.n|n \in N\}$ (gN se nazývá levá *rozkladová třída*).

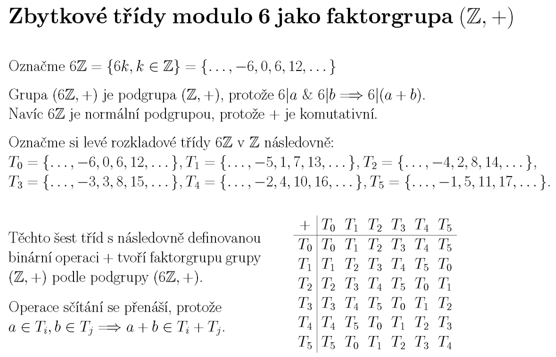
Tedy faktorgrupa je množina všech levých rozkladových tříd podle nějaké normální podgrupy. Faktorgrupa cyklické nebo abelovské grupy je také cyklická, resp. abelovská.

Příklady

Příklady faktorgrup:

- Pro grupu celých čísel $\mathbb{Z}$ a její normální podgrupu sudých celých čísel $2\mathbb{Z}$ je $\mathbb{Z}/2\mathbb{Z}$ faktorgrupou, isomorfní s grupou $\{0, 1\}$. Podobně to platí pro libovolné $n\mathbb{Z}$, kde n je přirozené.
- $\mathbb{R}/\mathbb{Z}$ je faktorgrupa grupy $\mathbb{R}$ (rozkladové třídy jsou tvaru $a + \mathbb{Z}$, kde a je reálné číslo v intervalu $\langle 0, 1)$.
- Faktorová grupa $\mathbb{Z}_4/\{0, 2\}$ je isomorfní se $\mathbb{Z}_2$.

- grupa $G = \{0, 1, 2, 3, 4, 5\}$ s operací $+$ s mod 6 a její normální podgrupu $N = \{0, 3\}$ pak faktorgrupa je definována jako
  $G/N = \{gN | g \in G\} = \{g\{0, 3\} | g \in \{0, 1, 2, 3, 4, 5\}\} =$
  $\{0\{0, 3\}, 1\{0, 3\}, 2\{0, 3\}, 3\{0, 3\}, 4\{0, 3\}, 5\{0, 3\}\} =$
  $\{\{(0 + 0) \mod 6, (0 + 3) \mod 6\}, \{(1 + 0) \mod 6, (1 + 3) \mod 6\},$
  $\{(2 + 0) \mod 6, (2 + 3) \mod 6\}, \{(3 + 0) \mod 6, (3 + 3) \mod 6\},$
  $\{(4 + 0) \mod 6, (4 + 3) \mod 6\}, \{(5 + 0) \mod 6, (5 + 3) \mod 6\}\} =$
  $\{\{0, 3\}, \{1, 4\}, \{2, 5\}, \{3, 0\}, \{4, 1\}, \{5, 2\}\} =$
  $\{\{0, 3\}, \{1, 4\}, \{2, 5\}, \{0, 3\}, \{1, 4\}, \{2, 5\}\} =$
  $\{\{0, 3\}, \{1, 4\}, \{2, 5\}\}$



Zbytkové třídy modulo 6 jako faktorgrupa $(\mathbb{Z}, +)$

Označme $6\mathbb{Z} = \{6k, k \in \mathbb{Z}\} = \{\dots, -6, 0, 6, 12, \dots\}$

Grupa $(6\mathbb{Z}, +)$ je podgrupa $(\mathbb{Z}, +)$, protože $6|a \;\&\; 6|b \Longrightarrow 6|(a + b)$.
Navíc $6\mathbb{Z}$ je normální podgrupou, protože $+$ je komutativní.

Označme si levé rozkladové třídy $6\mathbb{Z}$ v $\mathbb{Z}$ následovně:
$T_0 = \{\dots, -6, 0, 6, 12, \dots\}, T_1 = \{\dots, -5, 1, 7, 13, \dots\}, T_2 = \{\dots, -4, 2, 8, 14, \dots\},$
$T_3 = \{\dots, -3, 3, 8, 15, \dots\}, T_4 = \{\dots, -2, 4, 10, 16, \dots\}, T_5 = \{\dots, -1, 5, 11, 17, \dots\}.$

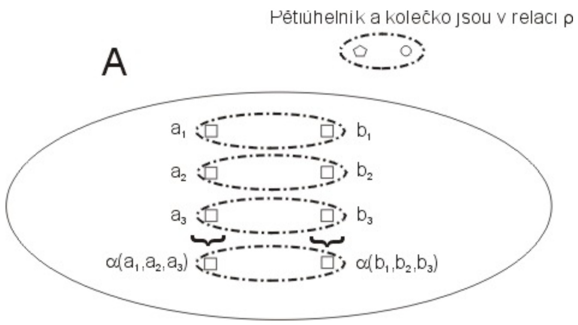
Těchto šest tříd s následovně definovanou binární operaci $+$ tvoří faktorgrupu grupy $(\mathbb{Z}, +)$ podle podgrupy $(6\mathbb{Z}, +)$.

Operace sčítání se přenáší, protože $a \in T_i, b \in T_j \Longrightarrow a + b \in T_i + T_j$.

$+$	T_0	T_1	T_2	T_3	T_4	T_5
T_0	T_0	T_1	T_2	T_3	T_4	T_5
T_1	T_1	T_2	T_3	T_4	T_5	T_0
T_2	T_2	T_3	T_4	T_5	T_0	T_1
T_3	T_3	T_4	T_5	T_0	T_1	T_2
T_4	T_4	T_5	T_0	T_1	T_2	T_3
T_5	T_5	T_0	T_1	T_2	T_3	T_4

Definice *(kongruence)*

Obecně v algebrách je *relace ρ slučitelná s operací α* arity n, pokud $a_1, \dots a_n, b_1, \dots b_n : (a_i, b_i) \in \rho \; \forall i$ implikuje $(\alpha(a_1, \dots a_n), \alpha(b_1, .$
ρ. *Kongruence* je každá ekvivalence slučitelná se všemi operacemi algebry.



Relace ρ slučitelná s operací α, česky řečeno, mám-li n-ární operaci, tak pro každé dvě n-tice pro které platí, že odpovídající si složky n-tice jsou v relaci, tak výsledky operace musí být také v relaci.

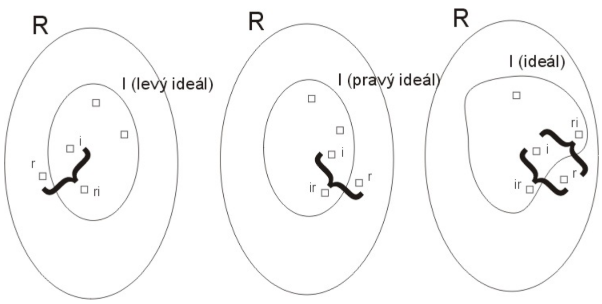
Poznámka

Faktorgrupa je vlastně grupa, v níž jsou jednotlivé prvky třídy ekvivalence na původní grupě podle nějaké kongruence (levé rozkladové třídy tvoří kongruence).

Definice *(ideál)*

Nechť $(R, +, \cdot, -, 0, 1)$ je okruh a $I \subseteq R$. Pak I je *pravý(levý) ideál*, pokud I podgrupa $(R, +, -, 0)$ (je i normální, protože R je z def. okruhu komutativní) a $\forall i \in I, r \in R$ platí $i.r \in I$ (levý $r.i \in I$) (důsledek: uzavřenost I na násobení).

I je *ideál*, pokud je pravý a zároveň levý ideál. Ideál je *netriviální (vlastní)*, pokud $I \neq R$ a $I \neq \{0\}$.



Příklady

Příklady ideálů:

- $\{0\}$ a R jsou (nevlastní, triviální) ideály v každém okruhu R
- Sudá celá čísla tvoří ideál v okruhu $\mathbb{Z}$, podobně to platí pro $n\mathbb{Z}$, kde n je přirozené.
- Množina polynomů dělitelných $x^2 + 1$ je ideálem v okruhu všech polynomů s 1 proměnnou a reálnými koeficienty
- Množina matic $n \times n$ s nulovým posledním sloupcem vpravo je levý ideál v okruhu všech matic $n \times n$, není to ale pravý ideál (podobně s řádky a opačnými ideály)

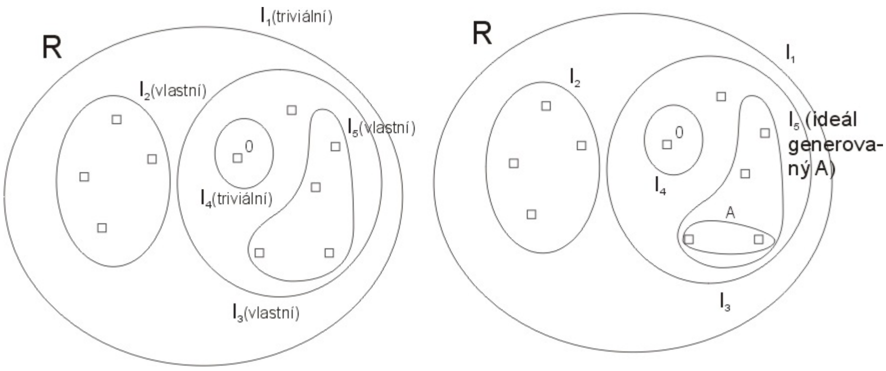
Poznámka *(Vlastnosti ideálů)*

Průnik (levých, pravých) ideálů tvoří opět (levý, pravý) ideál. *Ideál generovaný podmnožinou* A okruhu R je průnik všech ideálů v R, které A obsahují. Všechny ideály nad nějakým okruhem s průniky a ideály generovanými sjednocením tvoří úplný svaz.

I je *maximální ideál*, pokud je netriviální a žádný jiný netriviální ideál není jeho nevlastní nadmnožinou. *Prvoideál* P v okruhu R je takový ideál, že pro každé $a, b \in R$, pokud je $ab \in P$, potom musí být $a \in P$ nebo $b \in P$. Prvoideály mají v některých ohledech podobné vlastnosti jako prvočísla. Každý max.ideál je prvoideál.(fakt??)

Je-li ideál vlastní, pak neobsahuje 1. Každý ideál je neprázdný, protože jako podgrupa $(R, +, -, 0)$ musí obsahovat 0.

Ideál n$\mathbb{Z}$ je prvoideál $\Leftrightarrow$ n je prvočíslo.



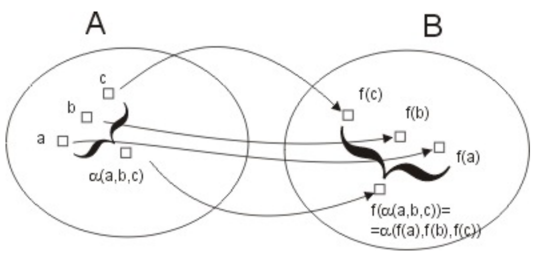
8.3 Homomorfismy grup

Obecná tvrzení o homomorfismech algeber (platí i pro grupy)

Definice *(homomorfismus)*

O zobrazení $f : A \to B$ řekneme, že je *slučitelné* s operací α, pokud pro každé $a_1, \ldots a_n \in A$ platí $f(\alpha_{(A)}(a_1, \ldots a_n)) = \alpha_{(B)}(f(a_1), \ldots f(a_n))$. Pro algebry stejného typu (se stejným počtem operací stejné arity) je zobrazení $f : A \to B$ *homomorfismus*, pokud je slučitelné se všemi jejich operacemi.

Bijektivní homomorfismus se nazývá *isomorfismus*, algebry stejného typu jsou *isomorfní*, existuje-li mezi nimi aspoň 1 isomorfismus.



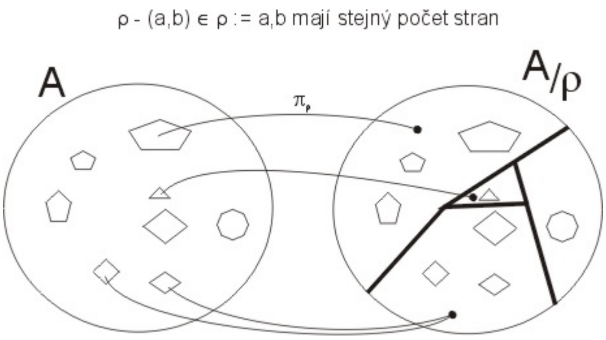
Slučitelnost s operací - pokud to nejprve zobrazím a pak aplikuji operaci, musí mi vyjít to samé jako kdybych nejprve použil operaci a zobrazil až výsledek.

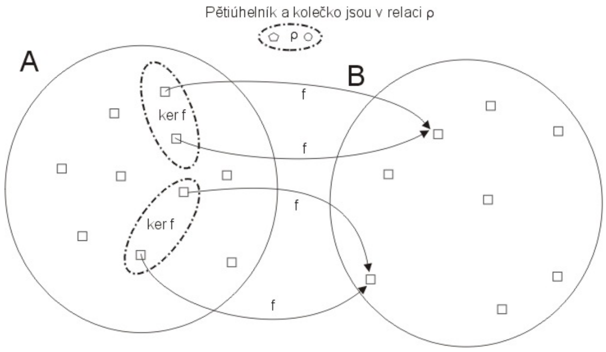
Poznámka *(Vlastnosti homomorfismů)*

Složení homomorfismů je homomorfismus. Je-li f bijekce a homomorfismus, je f^{-1} taky homomorfismus.

Definice *(přirozená projekce, jádro zobrazení)*

Přirozená projekce množiny A podle kongruence ρ je $\pi_\rho : A \to A/\rho$, kde $\pi_\rho(a) = [a]_\rho$. Pro zobrazení $f : A \to B$ se *jádro zobrazení* definuje jako relace ker$f$ předpisem $(a_1, a_2) \in \ker f \equiv^{def} f(a_1) = f(a_2)$.





Přirozená projekce prostě zobrazí prvek na jeho třídu ekvivalence.

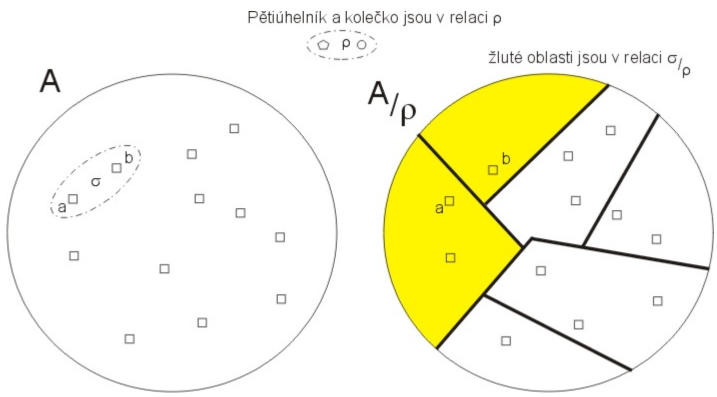
Poznámka *(homomorfismy a kongruence)*
Pro každou kongruenci ρ na libovolné algebře A je přirozená projekce $\pi_\rho : A \to A/\rho$ homomorfismus.

Věta *(O homomorfismu)*
Nechť $f : A \to B$ je homomorfismus algeber stejného typu a ρ kongruence na A. Potom:

1. existuje homomorfismus $g : A/\rho \to B$ takový, že $f = g\pi_\rho$ právě když $\rho \subseteq \ker f$,[4]
2. g je navíc isomorfismus, právě když f je na (surjekce) a $\rho = \ker f$.[5]

Definice *(faktor-ekvivalence)*
$\rho \subseteq \sigma$ 2 ekvivalence na A. Pak σ/ρ - *faktor-ekvivalence* je relace definovaná: $([a]_\rho, [b]_\rho) \in \sigma/\rho \overset{\text{def}}{\equiv} (a, b) \in \sigma$.

Relace ρ slučitelná s α, pak α na A/ρ def.: $\alpha([a_1]_\rho, ...[a_n]_\rho) = [\alpha(a_1, ...a_n)]_\rho$. Kongruence ρ na A, pak stejným způsobem def. na A/ρ strukturu algebry.



Česky řečeno, snažím se dát do relace chlívky, takže se neprve mrknu jestli jsou v relaci jejich reprezentanti.

Věta *(Věty o isomorfismu)*

1. Nechť $f : A \to B$ je homomorfismus algeber stejného typu, pak $f(A)$ je podalgebra B a ${}^{A}/_{\ker f}$ je isomorfní algebře $f(A)$.
2. Nechť $\rho \subseteq \eta$ jsou dvě kongruence na algebře A. Pak algebra ${}^{(A/\rho)}/_{(\eta/\rho)}$ je isomorfní algebře ${}^{A}/_{\eta}$.

Homomorfismy grup

Věta *(O homomorfismu grup)*
Je-li zobrazení $f : G \to H$, kde G, H jsou grupy, slučitelné s bin. operací, pak je homomorfismus. (Důkaz: nejdřív dokázat slučitelnost s e a pak $^{-1}$, oboje přímo z definice grupy.)

Definice *(mocnina prvku)*
V grupě lze definovat g^n (kde $n \in \mathbb{Z}$) jako:

- $g^0 = 1$,
- $g^{n+1} = g \cdot g^n \quad (n > 0)$,
- $g^n = (g^{-1})^{-n} \quad (n < 0)$.

Mocninná podgrupa grupy G je potom cyklická podgrupa – pro nějaký prvek $g \in G$ jde o množinu $\{\ldots, g^{-1}, g^0, g, g^2, \ldots\}$.

[4] přirozená projekce je taky homomorfismus
[5] surjekce je rozbrazení na celou cílovou množinu

Poznámka *(O mocnině prvku)*
Je-li zobrazení $\varphi : \mathbb{Z} \to G$ definováno předpisem $\varphi_g(n) = g^n$ (tj. jde o mocniny prvku g), kde $g \in (G, \cdot, ^{-1}, 1)$, pak je φ grupový homomorfismus $(\mathbb{Z}, +, -, 0)$ a $(G, \cdot, ^{-1}, 1)$.

Poznámka *(Vlastnosti cyklických grup)*
Nechť grupa $(G, \cdot, ^{-1}, 1)$ je cyklická. Potom platí:

1. Je-li G nekonečná, pak $G \simeq (\mathbb{Z}, +, -, 0)$ (je isomorfní s celými čísly).
2. Je-li $n = |G|$ konečné, pak $(G, \cdot, ^{-1}, 1) \simeq (\mathbb{Z}_n, +, -, 0)$ (je isomorfní s grupou zbytkových tříd odpovídající velikosti).

8.4 Dělitelnost a ireducibilní rozklady polynomů

Zdroje následujících sekcí: texty J. Žemličky k přednášce Algebra II
`http://www.karlin.mff.cuni.cz/~zemlicka/cvic6-7/algi.htm`
a skripta R. El Bashira k přednášce Algebra I a II pro matematiky
`http://www.karlin.mff.cuni.cz/~bashir/`

Největší společný dělitel

Definice *(Komutativní monoid s krácením)*
Monoid $(S, \cdot, 1)$ je *komutativní monoid s krácením*, pokud operace $\cdot$ je komutativní a navíc splňuje

$$\forall a, b, c \in S : a \cdot c = b \cdot c \;\Rightarrow\; a = b$$

Definice *(Dělení, asociovanost)*
O prvcích a, b nějakého komutativního monoidu s krácením S řekneme, že a *dělí* b ($a|b$, b je dělitelné a), pokud existuje takové $c \in S$, že $b = a \cdot c$. Řekneme, že a *je asociován s* b ($a||b$), jestliže $a|b$ a zároveň $b|a$.

Definice *(Obor integrity)*
Obor integrity je takový komutativní okruh $(R, +, \cdot, -, 0, 1)$, ve kterém platí, že $a \cdot b = 0$ implikuje $a = 0$ nebo $b = 0$.

Příklady

1. $(\mathbb{Z}, +, \cdot, -, 0, 1)$ je obor integrity.
2. Pro každý obor integrity $(R, +, \cdot, -, 0, 1)$ je $(R \setminus \{0\}, \cdot, 1)$ komutativní monoid s krácením (multiplikativní monoid).

Poznámka *(Vlastnosti $||$)*
V komutativním monoidu s krácením $(S, \cdot, 1)$ platí pro $a, b \in S$, že $a||b$, právě když existuje invertibilní prvek u z S takový, že $a = b \cdot u$. Relace $||$ tvoří kongruenci na S a faktoralgebra $(S/||, \cdot, [1]_{||})$ podle této kongruence je také komutativní monoid s krácením (relace $|$ na něm tvoří uspořádání).

Definice *(Největší společný dělitel)*
Mějme komutativní monoid s krácením $(S, \cdot, 1)$ a v něm prvky $a_1, \ldots, a_n$. Prvek c nazveme největším společným dělitelem prvků $a_1, \ldots, a_n$, pokud $c|a_i$ pro všechna $i \in \{1, \ldots, n\}$ a zároveň libovolný prvek $d \in S$, který dělí všechna a_i dělí i c. Píšeme $\mathbf{NSD}(a_1, \ldots, a_n) = c$.

Stejně se definuje největší společný dělitel pro obory integrity (bereme obor integrity $(R, +, \cdot, -, 1, 0)$ jako komutativní monoid s krácením $(R \setminus \{0\}, \cdot, 1)$).

Definice *(Ireducibilní prvek, prvočinitelé)*
Prvek c komutativního monoidu s krácením $(S, \cdot, 1)$ nazveme *ireducibilním*, pokud c není invertibilní a zároveň $c = a \cdot b$ pro nějaké $a, b \in S$ vždy implikuje $c||a$ nebo $c||b$. Prvek c nazveme *prvočinitelem*, pokud není invertibilní a zároveň $c|a \cdot b$ pro $a, b \in S$ vždy implikuje $c|a$ nebo $c|b$.

Na oborech integrity se prvočinitelé a ireducibilní prvky definují stejně.

Věta *(Vlastnosti* **NSD***)*
V komutativním monoidu s krácením $(S, \cdot, 1)$ pro prvky a, b, c, d, e platí:

1. $d = \mathbf{NSD}(a, b)$ & $e = \mathbf{NSD}(a \cdot c, b \cdot c) \;\Rightarrow\; (d \cdot c)||e$.
2. $1 = \mathbf{NSD}(a, b)$ & $a|(b \cdot c)$ & $\mathbf{NSD}(a \cdot c, b \cdot c)$ existuje $\;\Rightarrow\; a|c$.

Věta *(Vlastnosti prvočinitelů)*
V komutativním monoidu s krácením je každý prvočinitel ireducibilní. Pokud navíc pro každé dva jeho prvky existuje největší společný dělitel, je každý ireducibilní prvek prvočinitelem.

Polynomy

Definice *(Okruh polynomů)*
Nad okruhem $(R, +, \cdot, -, 0, 1)$ a monoidem $(M, \cdot, e)$ definujme okruh $(R[M], +, \cdot, -, 0, 1)$, kde:

- $R[M] = \{p : M \to R | \{m | p(m) \neq 0\}$ je konečné $\}$
- prvek $p \in R[M]$ se dá zapsat jako $p = \sum_{m \in M}(p(m).m)$
- operace $+$ je definována jako: $p + q = \sum_{m \in M}((p(m) + q(m)).m)$
- $\cdot$ je definováno následovně: $p \cdot q = \sum_{m \in M}((\sum_{r \cdot s = m} p(r) \cdot q(s)).m)$
- další operace:

- $-p = \sum_{m \in M} (-p(m)) \cdot m$,
- $0 = \sum_{m \in M} 0.m$,
- $1 = (1 \cdot e) + \sum_{m \in M \setminus \{e\}} 0.m$.

Pro okruh $(R, +, \cdot, -, 0, 1)$ a monoid $(\mathbb{N}_0, +, 0)$ nezáporných celých čísel se sčítáním nazveme $R[\mathbb{N}_0]$ (označme $R[x]$) *okruh polynomů jedné neznámé*. Jeho prvky potom nazveme *polynomy* a budeme je zapisovat ve tvaru $p = \sum_{n \in \mathbb{N}_0} p(n).x^n$.

Poznámka
$R[x]$ nad okruhem R je obor integrity, právě když R je obor integrity.

Definice *(Stupeň polynomu)*
Pro polynom p v okruhu $R[x]$ nad $(R, +, \cdot, -, 0, 1)$ definujeme *stupeň polynomu* (deg p, st p) následovně:

$$\deg p = \begin{cases} \text{největší } n \in \mathbb{N}_0 : p(n) \neq 0, \text{ je-li } p \neq 0 \\ -1, \text{ je-li } p = 0 \end{cases}$$

Poznámka *(Vlastnosti* deg p*)*
V okruhu $R[x]$ nad $(R, +, \cdot, -, 0, 1)$ platí pro $p, r \in R[x]$:

- $\deg\ -p = \deg p$
- $\deg\ (p+q) = \max(\deg p, \deg q)$
- Je-li $p \neq 0, q \neq 0$, pak $\deg\ (p \cdot q) \leq \deg p + \deg q$ (na oborech integrity platí rovnost)

Věta *(Dělení polynomů se zbytkem)*
Nechť jsou na oboru integrity $(R[x], +, \cdot, -, 0, 1)$ (nad oborem integrity R) dány prvky $a, b \in R[x]$. Nechť navíc $m = \deg b \geq 0$ a b_m je invertibilní v R. Potom existují jednoznačně určené polynomy $q, r \in R[x]$ takové, že $a = b \cdot q + r$ a $\deg r < \deg b$.

Poznámka
Polynom q je *podíl* polynomů a a b, polynom r je *zbytek* při dělení.

Největší společný dělitel

Definice *(Eukleidovský obor integrity)*
Obor integrity $(R, +, \cdot, -, 0, 1)$ je *eukleidovský*, jestliže existuje zobrazení $\nu : R \to \mathbb{N}_0 \cup \{-1\}$ (*eukleidovská funkce*), které pro každé $a, b \in R$ splňuje:

1. Jestliže $a|b$ a $b \neq 0$, pak $\nu(a) \leq \nu(b)$
2. Pokud $b \neq 0$, existují $q, r \in R$ taková, že $a = b \cdot q + r$ a $\nu(r) < \nu(b)$

Poznámka
Je-li $(T, +, \cdot, -, 0, 1)$ nějaké komutativní těleso, pak $T[x]$ je eukleidovským oborem integrity s eukleidovskou funkcí danou stupněm polynomů. Příkladem eukleidovského oboru integrity jsou např. i celá čísla (se sčítáním, násobením, unárním minus, jedničkou a nulou), kde eukleidovská funkce je funkce absolutní hodnoty prvku.

Algoritmus *(Eukleidův algoritmus)*
Na eukleidovském okruhu R s eukleidovskou funkcí ν pro dva prvky $a_0, a_1 \in R \setminus \{0\}$ najdeme největší společný dělitel následujícím postupem:

- Je-li $i \geq 1$ a $a_i \not| a_{i-1}$, vezmeme $a_{i+1} \in R$ takové, že $a_{i-1} = a_i \cdot q_i + a_{i+1}$ pro nějaké q_i a $\nu(a_{i+1}) < \nu(a_i)$. i zvýšíme o 1 a pokračujeme další iterací.
- Je-li $i \geq 1$ a $a_i | a_{i-1}$, potom $a_i = \mathbf{NSD}(a_0, a_1)$ a výpočet končí.

Dá se dokázat, že se výpočet zastaví a kroky jsou dobře definované (lze nalézt a_{i+1} a q_i), tedy libovolné dva polynomy mají největšího společného dělitele.

Poznámka
Největší společný dělitel je v polynomech $R[x]$ určen až na asociovanost ($||$) jednoznačně. Pro asociované polynomy p, q vždy platí, že $\deg p = \deg q$ a $p = r \cdot q$ pro nějaké $r \in R$.

8.5 Rozklady polynomů na kořenové činitele

Rozklady polynomů

Poznámka *(Ireducibilní polynomy)*
Polynom je ireducibilní, pokud není součinem dvou polynomů nižších stupňů a jeho stupeň je větší nebo roven jedné. Všechny polynomy stupně 1 jsou ireducibilní. Jedinými děliteli ireducibilního polynomu jsou asociované polynomy a nenulové skaláry (tj. polynomy stupně 0).

Věta *(Rozklad polynomu)*
Každý polynom stupně alespoň 1 má až na asociovanost jednoznačný rozklad na součin ireducibilních polynomů.
Důkaz existence: indukcí podle $\deg p$ – najdeme vždy dělitel p nejmenšího možného kladného stupně, vydělíme a pokračujeme, dokud nedostaneme polynom, který nemá dělitel kladného stupně menšího než je jeho vlastní.

Definice *(Dosazování do polynomů)*
Nechť $(S, +, \cdot, -, 0, 1)$ je okruh, R jeho podokruh ($R \subset S$) a nechť $\alpha \in S$. Potom zobrazení $j_\alpha : R[x] \to S$, dané předpisem $j_\alpha(\sum_{n\in\mathbb{N}_0} a_n.x^n) = \sum_{n\in\mathbb{N}_0} a_n \cdot \alpha^n$ je okruhový homomorfismus. Nazývá se *dosazovací homomorfismus.*

Poznámka *(Dosazovaní a $\deg p$)*
Pro obor integrity $R[x]$ nad oborem integrity $(R, +, \cdot, -, 0, 1)$ je polynom $p[x]$ invertibilní, právě když $\deg p = 0$ a $j_0(p) = p(0)$ je invertibilní na R.

Definice *(Kořen polynomu)*
Pro okruh $(S, +, \cdot, -, 0, 1)$ a jeho podokruh R je *kořen polynomu* $p \in R[x]$ takové $\alpha \in S$, že $j_\alpha(p) = p(\alpha) = 0$ (při dosazení α se polynom p zobrazí na 0).

Definice *(Kořenový činitel, rozklad)*
Je-li $a = c \cdot p_1^{k_1} \cdot \ldots p_n^{k_n}$ rozklad polynomu $p \in R[x]$ na ireducibilní polynomy, potom *kořenovým činitelem* polynomu p nazveme takové p_i, které je ve tvaru $x - \alpha$ (tedy stupně 1 s koeficienty 1 a α). Řekneme, že polynom $p \in R[x]$ se *rozkládá na kořenové činitele* v $R[x]$, jestliže existuje takový jeho rozklad na ireducibilní polynomy, že všechny p_i jsou kořenové činitele. Potom nazveme k_i *násobnostmi kořenů.*

Věta *(kořen a kořenový činitel)*
Na oboru integrity $R[x]$ nad oborem integrity R je $\alpha \in R$ kořenem polynomu $p \in R[x], p \neq 0$, právě když $(x - \alpha)|p$.

Komplexní, reálné a racionální polynomy

Definice *(Algebraicky uzavřené těleso)*
Nechť T je těleso a S jeho nadtěleso. Prvek $a \in S$ je *algebraický* nad T, pokud existuje nějaký nenulový polynom z $T[x]$, jehož je a kořenem. Pokud žádný takový polynom neexistuje, nazývá se prvek *transcendentní.* Těleso T je *algebraicky uzavřené*, pokud všechny nad ním algebraické prvky jsou i jeho prvky (jsou v něm obsaženy).

Poznámka
Každý polynom v okruhu polynomů o jedné neznámé nad algebraicky uzavřeným tělesem se rozkládá na kořenové činitele.

Věta *(Základní věta algebry)*
Těleso $\mathbb{C}$ komplexních čísel je algebraicky uzavřené.

Důsledek
Proto má každý polynom $p(x) \in \mathbb{C}[x]$ stupně alespoň 1 v $\mathbb{C}[x]$ rozklad tvaru $p(x) = a(x-\beta_1)^{k_1} \cdot \cdots \cdot (x-\beta_s)^{k_s}$, kde $\sum_{i=1}^{s} k_i = n$ a β_i jsou navzájem různá.

Věta *(Komplexně sdružené kořeny v $\mathbb{C}$)*
Má-li polynom p nad $\mathbb{C}[x]$ s reálnými koeficienty ($a_i \in \mathbb{R}$) kořen $\alpha \in \mathbb{C}$, pak je jeho kořenem i $\overline{\alpha}$, tedy číslo komplexně sdružené s α.

Důsledek
Polynom $p(x) \in \mathbb{R}[x]$ stupně alespoň 1 má v $\mathbb{R}[x]$ rozklad tvaru

$$p(x) = a(x - \alpha_1)^{k_1} \cdot \ldots (x - \alpha_r)^{k_r} \cdot (x^2 - a_1 x + b_1)^{l_1} \cdot \ldots (x^2 - a_s x + b_s)^{l_s}$$

a polynomy $x^2 + a_j x + b_j$, kde $j \in \{1, \ldots s\}$ mají za kořeny dvojice komplexně sdružených čísel (která nejsou čistě reálná). Navíc $\deg p = k_1 + \cdots + k_r + 2(l_1 + \cdots + l_s)$.

Důsledek
Každý polynom v $\mathbb{R}[x]$ lichého stupně má alespoň jeden reálný kořen.

Věta *(Ireducibilní polynomy v $\mathbb{Q}$)*
V $\mathbb{Q}[x]$ existují ireducibilní polynomy libovolného stupně většího nebo rovného jedné (tj. ne vždy existuje rozklad na kořenové činitele, ani rozklad na polynomy stupně max. 2 jako v reálných číslech).

8.6 Násobnost kořenů a jejich souvislost s derivacemi mnohočlenu

Věta *(o počtu kořenů)*
Každý nenulový polynom $p \in R[x]$, kde $R[x]$ je okruh polynomů nad oborem integrity $(R, +, \cdot, -, 0, 1)$, má nejvýše deg p kořenů (plyne z vlastností deg p).

Definice *(vícenásobný kořen)*
Pro komutativní okruh $(R, +, \cdot, -, 0, 1)$ a polynom $p \in R[x]$ je $\alpha \in R$ *vícenásobný kořen*, pokud polynom $(x - \alpha)(x - \alpha)$ dělí p.

Definice *(Derivace polynomu)*
Pro polynom $p = \sum_{i \geq 0} a_i x^i$ z okruhu polynomů $R[x]$ nad komutativním okruhem $(R, +, \cdot, -, 0, 1)$ definujeme *derivaci* (p', $p' \in R[x]$) předpisem

$$p' = \sum_{i \geq 0} (i + 1) a_{i+1} x^i$$

Poznámka *(Vlastnosti derivace)*
Pro okruh $(R, +, \cdot, -, 0, 1)$, prvek $\alpha \in R$ a polynomy $p, q \in R[x]$ platí:

- $(p + q)' = p' + q'$
- $(\alpha p)' = \alpha p'$
- $(p \cdot q)' = p' \cdot q + p \cdot q'$

Věta *(derivace a vícenásobný kořen)*
Nad oborem integrity $(R, +, \cdot, -, 0, 1)$ buď $p \in R[x]$ polynom. Je-li $\alpha \in R$ jeho kořen, pak α je vícenásobný kořen, právě když je α kořenem p'.

Definice *(Charakteristika oboru integrity)*
Pro obor integrity $(R, +, \cdot, -, 0, 1)$ definujeme *charakteristiku oboru integrity* jako

- 0 (nebo někdy ∞), pokud cyklická podgrupa grupy $(R, +, 0)$ generovaná prvkem 1 je nekonečná.
- p, pokud cyklická pogrupa grupy $(R, +, 0)$ generovaná jedničkou má konečný řád p.

Věta *(derivace snižuje stupeň polynomu)*
Nad oborem integrity charakteristiky 0 $(R, +, \cdot, -, 0, 1)$ buď p polynom ($p \in R[x]$) stupně $n > 0$. Potom p' je polynom stupně $n - 1$.

Věta *(derivace a násobný kořen)*
Nad tělesem charakteristiky 0 $(T, +, \cdot, -, 0, 1)$ buď p polynom ($p \in T[x]$) stupně alespoň 1. Potom prvek $\alpha \in U$, kde U je nějaké nadtěleso T, je k-násobným kořenem p, právě když platí obě následující podmínky:

- $p(\alpha) = j_\alpha(p) = 0,\ p'(\alpha) = 0,\ \ldots\ p^{(k-1)}(\alpha) = 0$
- $p^{(k)}(\alpha) \neq 0$

Věta *(derivace a největší společný dělitel)*
Mějme těleso $(T, +, \cdot, -, 0, 1)$ charakteristiky 0 a nad ním polynom $p \in T[x]$ stupně alespoň 1. Potom platí:

- Pokud $\mathbf{NSD}(p, p') = 1$, pak p nemá žádný vícenásobný kořen.
- Každý k-násobný kořen p je $(k - n)$-násobným kořenem n-té derivace p.
- Polynom $q \in R[T]$ takový, že $q \cdot \mathbf{NSD}(p, p') = p$ má stejné kořeny jako p, ale jednoduché.

Věta
Nechť $(R, +, \cdot, -, 0, 1)$ je obor integrity a jeho charakteristika nedělí přir. číslo n. Potom polynomy $x^n - 1$ a $x^{n+1} - x$ v $R[x]$ nemají vícenásobný kořen.