I. Cayleyova věta pro grupy

Izomorfní zobrazení:

Buď G_1, G_2 grupy, $f : G_1 \to G_2$. Řekneme, že f je izomorfní zobrazení, jestliže:

1. f je bijekce (injekce, surjekce)
2. $f(a) \cdot f(b) = f(a \cdot b)$, pro $\forall a, b \in G$ (homomorfismus)

Caleyova věta

Libovolná grupa G je izomorfní s jistou podgrupou grupy $S(A)$ všech permutací množiny A, pro vhodné A. Za A lze vzít i G.

Důkaz:

Nechť $(G, \cdot)$ je lib. grupa. Pro pevné $a \in G$ označme ρ_a: $G \to G$ zobrazení definované vztahem: $\rho_a(\mathrm{x}) = a.x$, $\forall x \in G$

Zobrazení ρ_a je :

1. injektivní: $\rho_a(x) = \rho_a(y) \Rightarrow ax = ay \Rightarrow x = y$
2. surjektivní: $y \in G$, hledáme $x \in G$, $\rho_a(x) = y \Rightarrow y = a.x \Rightarrow x = a^{-1}.y \Rightarrow x \in G$

Zkonstruhujeme *injektivní homomorfismus* z G do $S(G)$.
Definujeme: $f : G \to S(G)$ předpisem $f(a) = \rho_a$ pro $\forall a \in G$
Zobrazení f je:

1. injektivní: neboť $a, b \in G$, $f(a) = f(b) \Rightarrow \rho_a = \rho_b$ pro libovolné $x \in G$ je pak $\rho_a(x) = \rho_b(x)$, neboli $a.x = b.x \Rightarrow a = b$
2. homomorfismus: neboť pro $a, b \in G$, $x \in G$:
   $(f(a) \cdot f(b))(x) = (\rho_a \circ \rho_b)(x) = \rho_a(\rho_b(x)) = \rho_a(b.x) = a.b.x$
   $\iff f(a.b)(x) = \rho_{a \circ b}(x) = a.b.x$

Pak dostáváme, že f je vnoření G do $S(G)$, a tedy G je izomorfní s podgrupou $f(G)$ grupy $S(G)$.

Důsledek: Každá konečná grupa řádu n je izomorfní s jistou podgrupou grupy permutací S_n.

II. Klasifikace cyklických grup

Řád prvku:

Nechť $(G,\cdot)$ je grupa, $a \in G$. *Řád* prvku a definujeme jako nejmenší číslo n takové, že $a^n = 1$. Pokud takové číslo neexistuje, řekneme, že řád prvku je 0.

$< M >$, generátory grupy:

Buď M podmnožina grupy G. Symbolem $< M >$ označíme *průnik všech podgrup* grupy G obsahujících množinu M. $< M >$ se nazývá *podgrupa generovaná množinou* M. Množinu M nazýváme *množinou generátorů grupy* $< M >$.
Pokud $M = \{a_1, \ldots, a_n\}$, pak hovoříme o podgrupě generované prvky $a_1, \ldots, a_n$ a označujeme ji $< a_1, \ldots, a_n >$.

Věta:

Buď $M \neq \emptyset$ podmnožina grupy G.
Pak $< M >= \{a_1^{\varepsilon_1} \cdot \ldots \cdot a_n^{\varepsilon_n} \mid n \in N_0,\ a_i, \ldots, a_n \in M,\ \varepsilon_1, \ldots, \varepsilon_n \in \{1, -1\}\ \}$.

Důkaz:

1. $(Y,.)$ podgrupa grupy $(G,.)$.
   (a) $a^0 = 1 \Rightarrow 1 \in Y$
   (b) $a, b \in Y \Rightarrow a.b \in Y$
   (c) $a \in Y \Rightarrow a^{-1} \in Y$, protože $(a_1^{\varepsilon_1} \cdot \ldots \cdot a_n^{\varepsilon_n})^{-1} = a_n^{-\varepsilon_n} \cdot \ldots \cdot a_1^{-\varepsilon_1}$
2. $M \subseteq Y$:
   $a \in M$, $n = 1$, $a_1 = a$, $\varepsilon_1 = 1$
3. $M \subseteq Z$, Z je podgrupa $(G,.) \Rightarrow Y \subseteq Z$.

$a_1^{\varepsilon_1} \cdot \ldots \cdot a_n^{\varepsilon_n} \in Y$
$a_1, \ldots, a_n \in M \subseteq Z$ je podgrupa
$a_1^{\varepsilon_1}, \ldots, a_n^{\varepsilon_n} \in Z$ je podgrupa
$a_1^{\varepsilon_1} \cdot \ldots \cdot a_n^{\varepsilon_n} \in Z$

Cyklická grupa:

Grupa $(G,\cdot)$ se nazývá *cyklická*, existuje-li $a \in G$ takové, že $< a >= G$.

Věta:

1. Libovolná nekonečná cyklická grupa je isomorfní s $(Z,+)$.
2. Libovolná n-prvková cyklická grupa $(n \in N)$ je isomorfní se $(Z_n,+)$.

Důkaz:
Nechť $(G,.)$ cyklická grupa, a je její generátor, tj. $\{a^k \mid k \in Z\} = G$

1. $|G| \geq \aleph_0$, pak řád a je 0
   $\alpha : G \to Z$
   $a^k \mapsto k$ je korektní $(a^k = a^l \Leftrightarrow k = l)$
   (a) α je homomorfismus :
   $\alpha(a^k \cdot a^l) = \alpha(a^{k+l}) = k + l, \quad \alpha(a^k) + \alpha(a^l) = k + l$
   (b) α je prosté : $k = l \Rightarrow a^k = a^l$

(c) α je surjektivní : vzorem ke k je a^k

2. $|G| = n$, $n \in N$, pak a je řádu n
   $\alpha : G \to Z_n$, $a^k \mapsto [k]_n$ je korektní ($a^k = a^l \Leftrightarrow [k]_n = [l]_n$)

   (a) α je homomorfismus :
   $\alpha(a^k \cdot a^l) = \alpha(a^{k+l}) = [k+l]_n, \quad \alpha(a^k) + \alpha(a^l) = [k]_n + [l]_n = [k+l]_n$

   (b) α je prosté : $[k]_n = [l]_n \Rightarrow a^k = a^l$

   (c) α je surjektivní : $[k]_n$ má vzor a^k

III. Faktorové grupy

Levé třídy:

Buď G grupa, H její podgrupa, $a \in G$. Množinu $aH = \{a \cdot h \mid h \in H\}$ nazýváme *levá třída* grupy G podle podgrupy H (určená prvkem a).

levý rozklad: $G/H = \{aH \mid a \in G\}$

pravý rozklad: $H\backslash G = \{Ha \mid a \in G\}$

Lemma I.

Buď G je grupa, H je její podgrupa. $a, b \in G$ pak platí:
$a.H = b.H \iff a \in b.H \iff b^{-1}.a \in H$

Normální podgrupa:

Nechť G je grupa. Podgrupa H se nazývá *normální*, jestliže pro $\forall h \in H$, $\forall g \in G$ platí $g^{-1} \cdot h \cdot g \in H$.

Lemma II.

Podgrupa H grupy G je normální, právě když pro libovolné prvky $a \in G$, $h \in H$ existuje prvek $\bar{h} \in H$, takový že $h.a = a.\bar{h}$.

Důkaz:
$h.a = a.\bar{h} \Rightarrow a^{-1}.h.a = a^{-1}.a.\bar{h}$.

Věta o Faktorové grupě $(G/H, .)$

Buď G grupa, H její normální podgrupa. Definujeme součin dvou levých tříd $a \cdot H$, $b \cdot H$ grupy G podle H vztahem:

$$(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$$

Pak $\cdot$ je operace na množině G/H a $(G/H, \cdot)$ je grupa.
Důkaz:

1. Korektnost operace $\cdot$ na množině G/H.

   $a.H = a'.H$, $b.H = b'.H \stackrel{?}{\Longrightarrow} (a.b).H = (a'.b').H$

   Nechť $a, a', b, b' \in G$, $a.H = a'.H$, $b.H = b'.H$. Z Lemmatu I. plyne existence prvků $h_1, h_2 \in H$ taková, že $a = a'.h_1$, $b = b'.h_2$.
   Z Lemmatu II. plyne: $h \in H$, $h_1.b' = b'.\bar{h}$

   Platí $a.b = a'.h_1.b'.h_2 = a'.b'.\bar{h}.h_2 \in (a'.b').H \Longrightarrow (a.b).H = (a'.b').H$.

2. (G/H) je grupa.

   (a) Asociativita:
   Nechť $a, b, c \in G$. Pak $[(a.H).(b.H)] \cdot (c.H) = ((a.b).H).(c.H) = ((a.b).c).H = (a.(b.c)).H = (aH).[(b.H).(c.H)]$. Tedy (G/H) je pologrupa.

   (b) Jednotkový prvek:
   Levá třída $H = 1 \cdot H$ je jednotkový prvek ,neboť pro libovolné $.a \in G$ platí $(1 \cdot H) \cdot (a \cdot H) = (1 \cdot a) \cdot H = a \cdot H = (a \cdot H) \cdot (1 \cdot H)$.

   (c) Inverzní prvek:
   inverzním prvkem k levé třídě $a \cdot H$ je levá třída $a^{-1} \cdot H$, neboť $(a \cdot H) \cdot (a^{-1} \cdot H) = (a \cdot a^{-1}) \cdot H = 1 \cdot H = (a^{-1} \cdot H) \cdot (a \cdot H)$.

Věta:

Jestliže $(G,\cdot)$ je grupa, H je její normální podgrupa. Pak $(G/H,\cdot)$ je opět grupa a zobrazení $natH : G \to G/H$, $natH : a \mapsto aH$ je surjektivní homomorfismus.

Důkaz:

$(G/H,\cdot)$ je grupa - viz.předchozí věta. $natH(a \cdot b) = abH$; $natH(a) \cdot natH(b) = aH \cdot bH = abH$ -homomorfismus;
surjektivním vzorem aH je a - surjektivita;

Věta DĚLO:

Nechť $(G,\cdot),(K,\cdot)$ jsou grupy, $\alpha : (G,\cdot) \to (K,\cdot)$ je surjektivní homomorfismus. Pak:

1. $J(\alpha) = \{a \in G \mid \alpha(a) = 1\}$ je normální podgrupou v $(G,\cdot)$
2. $\beta : G/J(\alpha) \to K$, $\beta : aJ(\alpha) \mapsto \alpha(a)$ je isomorfismus.
3. $\beta \circ natJ(\alpha) = \alpha$

Důkaz:

1. $J(\alpha)$ je normální podgrupa:
   - $\alpha(1) = 1$
   - Nechť $a,b \in J(\alpha)$, $\alpha(a) = \alpha(b) = 1$, pak $\alpha(ab) = \alpha(a) \cdot \alpha(b) = 1 \cdot 1 = 1 \Longrightarrow a.b \in J(\alpha)$
   - $\alpha(a^{-1}) = (\alpha(a^1))^{-1} = 1^{-1} = 1 \in J(\alpha)$
   - normálnost: $g \in G$, $\alpha(g^{-1} \cdot a \cdot g) = (\alpha(g))^{-1} \cdot 1 \cdot \alpha(g) = 1 \in J(\alpha)$
2. Zobrazení β je :
   - korektně definováno:
     $aJ(\alpha) = bJ(\alpha) \Longrightarrow^{?} \alpha(a) = \alpha(b)$
     $aJ(\alpha) = bJ(\alpha) \Longleftrightarrow ab^{-1} \in J(\alpha) \Longleftrightarrow 1 = \alpha(ab^{-1}) = \alpha(a) \cdot \alpha(b)^{-1} \Rightarrow \alpha(a) = \alpha(b)$
   - homomorfismus:
     $\beta(aJ(\alpha) \cdot bJ(\alpha)) = \beta(abJ(\alpha)) = \alpha(ab) = \alpha(a).\alpha(b)$
     $\beta(aJ(\alpha)) \cdot \beta(bJ(\alpha)) = \alpha(a) \cdot \alpha(b) = \alpha(ab)$
   - surjektivní:
     $b \in K$, exist.$a \in G$ tak, že $\alpha(a) = b$, $\beta(aJ(\alpha)) = \alpha(a) = b$
   - prosté:
     $a,b \in G$, $\beta(aJ(\alpha)) = \beta(bJ(\alpha))$, pak $\alpha(a) = \alpha(b)$,
     $\alpha(a)((\alpha(b))^{-1} = 1$, $\alpha(ab^{-1}) = 1$, $ab^{-1} \in J(\alpha)$, $aJ(\alpha) = bJ(\alpha)$
3. Konečně:
   $a \in G, (\beta nat\, J(\alpha))(a) = \beta(nat\, J(\alpha)(a)) = \beta(aJ(\alpha)) = \alpha(a)$

IV. Okruhy Z_n

Kongruentnost:

Buď $n \in N$, $a, b \in Z$. a, b se nazývají kongruentní modle modulu n, jestliže platí $n|a-b$. Píšeme $a \equiv b(mod\ n)$.

Zbytkové třídy:

Buď $n \in N, a \in Z$. Množina $[a]_n = \{k.n + a \setminus k \in Z\}$ se nazývá *zbytková třída podle modulu n.*

Množina všech zbytkových tříd:

$Z_n = \{[a]_n \setminus a \in Z\}$

Lemma:

$[a]_n = [b]_n \leftrightarrow a \equiv b(mod\ n) \leftrightarrow n|a-b$

Operace $\cdot$ a $+$ na množině Z_n

- $[a]_n + [b]_n = [a+b]_n$

  Důkaz korektnosti:
  $[a]_n = [a']_n, [b]_n = [b']_n \Longrightarrow^? [a+b]_n = [a'+b']_n$

  $n|(a-a'), n|(b-b') \Longrightarrow^? n|((a+b)-(a'+b'))$
  $[a]_n = [a']_n \Longrightarrow a - a' = \alpha.n, \quad [b]_n = [b']_n \Longrightarrow b - b' = \beta.n$
  $(a+b)-(a'+b') = (\alpha+\beta)n \Longrightarrow n|((a+b)-(a'+b'))$

- $[a]_n \cdot [b]_n = [a \cdot b]_n$

  Důkaz korektnosti:
  $[a]_n = [a']_n, [b]_n = [b']_n \Longrightarrow^? [a \cdot b]_n = [a' \cdot b']_n$

  $n|(a-a'), n|(b-b') \Longrightarrow^? n|((a \cdot b)-(a' \cdot b'))$
  $[a]_n = [a']_n \Longrightarrow a - a' = \alpha.n, \quad [b]_n = [b']_n \Longrightarrow b - b' = \beta.n$
  $a \cdot b - a' \cdot b' = (a' + \alpha.n)(b' + \beta.n) - a'.b' =$
  $a'.b' + a'.\beta.n + \alpha.n.b' + \alpha.n.\beta.n - a'.b' = n(a'.\beta + b'.\alpha + \alpha.\beta.n)$
  $\Longrightarrow n|((a.b)-(a'.b'))$

Grupa $(Z_n, +)$

$(Z_n, +)$ je komutativní grupa pro libovolné $n \in N$.
Důkaz:

1. Z_n je uzavřená vzhledem k $+$.
2. $[0]_n$ je jednotkový prvek; $[0]_n + [a]_n = [a]_n = [a]_n + [0]_n$
3. inverzní prvek k $[a]_n$ je $[-a]_n$: $[a]_n + [-a]_n = [a + (-a)]_n = [0]_n = [-a]_n + [a]_n$
4. asociativita: $([a]_n + [b]_n) + [c]_n = [a+b]_n + [c]_n = [a+b+c]_n = [a]_n + [b+c]_n = [a]_n + ([b]_n + [c]_n)$
5. komutativita: $[a]_n + [b]_n = [a+b]_n = [b+a]_n = [b]_n + [a]_n$

Monoid $(Z_n, .)$

$(Z_n, .)$ je komutativní monoid pro libovolné $n \in N$.

Důkaz:

1. Z_n je uzavřená vzhledem k operaci $\cdot$.
2. $[1]_n$ je jednotkový prvek: $[1]_n.[a]_n = [a]_n = [a]_n \cdot [1]_n$
3. asociativita: $([a]_n \cdot [b]_n) \cdot [c]_n = [a.b]_n \cdot [c]_n = [a.b.c]_n = [a]_n \cdot [b.c]_n = [a]_n \cdot ([b]_n \cdot [c]_n)$
4. komutativita: $[a]_n \cdot [b]_n = [a.b]_n = [b.a]_n = [b]_n \cdot [a]_n$

Grupa $(Z_n^*, .)$

Buď n prvočíslo, $Z_n^* = [1]_n, \ldots, [n-1]_n$ všech nenulových zbytkových tříd podle modulu n. Pak $(Z_n^*, .)$ je grupa.

Důkaz:

Nechť $[a]_n, [b]_n \in Z_n^*$.

• $n \not| a, n \not| b \Longrightarrow n \not| a.b$ Tedy $[a.b]_n \in Z_n^*$. $(a, n) = 1$ pro libovolné $a \in Z^*$.

$(Z_n^*, .)$ je grupa pokud libovolné $[a]_n \in (Z_n^*, .)$ má inverzní prvek. Předpokládejme existenci takového inverzního prvku $[b]_n$. Platí $[a]_n \cdot [b]_n = [1]_n \Longrightarrow a.b = q.n + 1 \Longrightarrow a.b + n.(-q) = 1$.

Existence čísel b, q plyne z Bezoutovy věty: { a.u + b.v = 1 ⇔ (a,b)=1 } neboť $(a, n) = 1$.

Okruh $(Z_n, +, .)$

Buď $n \in N$ pak $(Z_n, +, .)$ je okruh.

Důkaz:

1. $(Z_n, +)$ je komutativní grupa.
2. $(Z_n, .)$ je monoid.
3. Distributivita: $[a], [b], [c] \in Z_n$
   $[a] \cdot ([b] + [c]) = [a] \cdot [b + c] = [a \cdot (b + c)] = [a.b + a.c] = [a] \cdot [b] + [a] \cdot [c]$
   $([b] + [c]) \cdot a = [b + c] \cdot [a] = [(b + c) \cdot a] = [b.a + c.a] = [b] \cdot [a] + [c] \cdot [a]$

Lemma o tělese:

Netriviální komutativní okruh $(R, +, .)$ je těleso, právě když $(R^*, .)$ je grupa.

Obor integrity $(Z_n, +, .)$

$(Z_n, +, .)$ je *obor integrity*, právě když n je prvočíslo. V tomto případě je Z_n dokonce *těleso*.

Důkaz:

Je-li n prvočíslo, pak $(Z_n, +, .)$ je těleso, neboť $(Z_n^*, .)$ je grupa, dále z lemmatu o tělese.

Pokud n není prvočíslo, pak $n = k.m$, kde $1 \leq k, m \leq n$. Ze vztahu $[k].[m] = [k.m] = [0]$ plyne, že $[k], [m]$ jsou dělitelé nuly v $(Z_n, .)$. Tedy $(Z_n, +, \cdot)$ není obor integrity.

V. Podílové těleso

Definice R^*:

Definujme $R^* = R - \{0\}$.

Lemma:

Nechť $\mathcal{R} = (R, +, \cdot)$ je obor integrity. na množině $R \times R^*$ definujeme relaci $\sim$ takto: $(a, b) \sim (c, d) \Leftrightarrow a \cdot d = b \cdot c$.

Pro libovolné $a, c \in R$, $b, d \in R^*$ je $\sim$ relace ekvivalence.

Důkaz:

1. reflexivita $(a, b) \sim (a, b) \Leftrightarrow ab = ba$
2. symetrie z definice
3. tranzitivita $(a, b) \sim (c, d) \wedge (c, d) \sim (e, f) \stackrel{?}{\Longrightarrow} (a, b) \sim (e, f)$
   Máme $ad = bc$, $cf = de$ a chceme $(a, b) \sim (e, f) \Leftrightarrow af = be$. ale $acf = bce$, $adf = bcf = bde \Longrightarrow d(af - be) = 0$, $(d \neq 0) \Longrightarrow af - be = 0 \Longrightarrow af = be$

Píšeme:

$$[(a, b)]_\sim = \frac{a}{b}, \quad Q(\mathcal{R}) = \{\frac{a}{b} \mid a \in R, b \in R^*\} = (R \times R^*/\sim, +, \cdot)$$

Na $R \times R^*/\sim$ definujeme operace $+, \cdot$ takto:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Lemma:

Uvedené formulky korektně definují operace na $Q(R)$.

Důkaz:
Nechť $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'}$.
Chceme: $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$, $\frac{ac}{bd} = \frac{a'c'}{b'd'}$,
$ab' = ba'$, $cd' = dc'$, $ab'cd' = a'bc'd$,
(chceme: $(ad + bc)b'd' = bd(a'd' + b'c')$, $a'c'bd = b'd'ac)$, ale $(ad + bc)b'd' = ab'dd' + bb'cd' = a'bdd' + bb'c'd = bd(a'd' + b'c')$ $\quad ab'cd' = a'bc'd$

Věta:

Je-li $(R, +, .)$ obor integrity, pak $Q(R) = (R \times R^*)/\sim, +, \cdot)$ je těleso.

Důkaz: $(R \times R^*, +)$ komutativní grupa:

- asociativita: $(\frac{a}{b} + \frac{c}{d}) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{adf+bcf+ebd}{bdf}$;
  $\frac{a}{b} + (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} + \frac{cf+cd}{df} = \frac{adf+bcf+cbf}{bdf}$
- komutativita: $\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$
- neutrální prvek: $\frac{0}{1} + \frac{a}{b} = \frac{0b+1a}{1b} = \frac{a}{b}$
- Inverzní prvek: $\frac{-a}{b} + \frac{a}{b} = \frac{-ab+ab}{bb} = \frac{0}{bb} = 0$

Důkaz: $(R \times R^*, .)$ grupa:

- asociativita: $(\frac{a}{b} . \frac{c}{d}) . \frac{e}{f} = \frac{a.c}{b.d} . \frac{e}{f} = \frac{a.c.e}{b.d.f}$;
  $\frac{a}{b} . (\frac{c}{d} . \frac{e}{f}) = \frac{a}{b} . (\frac{c.e}{d.f}) = \frac{a.c.e}{b.d.f}$
- komutativita: zřejmá

- neutrální prvek: $\frac{1}{1}$
- inverzní prvek: $(\frac{a}{b})^{-1} = \frac{b}{a}$

Distributivita:

- $\frac{a}{b}.(\frac{c}{d} + \frac{e}{f}) = \frac{a}{b}.\frac{c.f+d.e}{d.f} = \frac{a.c.f+a.d.e}{b.d.f}$,
- $\frac{a}{b}.\frac{c}{d} + \frac{a}{b}.\frac{e}{f} = \frac{a.c}{b.d} + \frac{a.e}{b.f} = \frac{a.c.b.f+b.d.a.e}{b.d.b.f} = \frac{a.c.f+a.d.e}{b.d.f}$

Věta:

Nechť $\mathcal{R} = (R, +, \cdot)$ je obor integrity a $\iota : R \to (R \times R^*/\sim)$ je definována předpisem $a \mapsto \frac{a}{1}$.Pak:

1. ι je prostý homomorfismus.
2. Pro libovolné těleso $\mathcal{S}(S, +, .)$ a prostý homomorfismus $\alpha : \mathcal{R} \to \mathcal{S}$ existuje homomorfismus $\beta : Q(\mathcal{R}) \to \mathcal{S}$ tak, že $\beta \circ \iota = \alpha$

Důkaz:
$(Q, +, .) := Q(Z, +, .)$

1. Zobrazení ι je:
   (a) prosté: $\frac{a}{1} = \frac{b}{1} \Rightarrow a = b$
   (b) homomorfismus:
      i. $\iota(1) = \frac{1}{1}$
      ii. $\iota(a + b) = \frac{a+b}{1}, \quad \iota(a) + \iota(b) = \frac{a}{1} + \frac{b}{1} = \frac{a+b}{1}$
      iii. $\iota(a.b) = \frac{a.b}{1}, \quad \iota(a).\iota(b) = \frac{a}{1}.\frac{b}{1} = \frac{a.b}{1}$
2. Zobrazení $\beta : Q(R) \to S$ splňující $\beta \circ \iota = \alpha$ musí být dáno tímto předpisem: $\beta(\frac{a}{b}) := \alpha(a).(\alpha(b))^{-1}$
   - Ukážeme že: $\beta \circ \iota = \alpha \Rightarrow \beta(\frac{a}{b}) = \alpha(a).(\alpha(b))^{-1}$
   - $\beta \circ \iota(a) = \beta(\frac{a}{1}) = \alpha(a) \Rightarrow \beta(\frac{a}{1}) = \alpha(a)$
   - $\beta \circ (b^{-1}) = \beta(\frac{1}{b}) = \alpha(b^{-1}) \Rightarrow \beta(\frac{1}{b}) = \alpha(b^{-1}) = \alpha(b)^{-1}$
   - $\beta \circ \iota(a.b^{-1}) = \beta \circ \iota(a).\beta \circ \iota(b^{-1}) = \alpha(a).(\alpha(b))^{-1}$
3. Zobrazení β je homomorfismus:
   (a) $\beta(\frac{1}{1}) = \alpha(1) \cdot (\alpha(1))^{-1} = 1$
   (b) $\beta(\frac{a}{b} + \frac{c}{d}) = \beta(\frac{ad+bc}{bd}) = \alpha(ad + bc) \cdot \alpha(bd)^{-1}$
   $\beta(\frac{a}{b}) + \beta(\frac{c}{d}) = \alpha(a) \cdot \alpha(b)^{-1} + \alpha(c) \cdot \alpha(d)^{-1} = (\alpha(ad) + \alpha(bc)) \cdot (\alpha(bd)^{-1}) = \alpha(ad + bc).\alpha(bd)^{-1}$
   (c) $\beta(\frac{a}{b}.\frac{c}{d}) = \beta(\frac{a}{b}.\frac{c}{d})$
   (d) $(\beta\iota)(a) = \beta(\iota(a)) = \beta(\frac{c}{1}) = \alpha(a).(\alpha(1))^{-1} = \alpha(a)$

Podílové těleso

$(Q(R), +, \cdot)$ nazýváme *podílové těleso.*

VI. Euklidův algoritmus

Dělitelnost:

Buď R komutativní okruh, $a, b \in R$. Řekneme že prvek b *dělí* prvek a, jestliže existuje prvek $q \in R$ takový, že $a = q.b$. Píšeme $b|a$.

Společný dělitel:

Buď R komutativní okruh, $a, b \in R$. Prvek $c \in R$ se nazývá *společný dělitel* prvků a, b, pokud $c|a$ a $c|b$.

Největší společný dělitel:

Buď R komutativní okruh, $a, b \in R$. Prvek $c \in R$ se nazývá jejich *největším společným dělitelem*, zkráceně $\mathsf{nsd}(a, b)$, jestliže je jejich společným dělitelem a pro libovolný společný dělitel $x \in R$ prvků a, b platí, že $x|c$.

Věta o dělitelnosti:

Buď R obor integrity, $f, g \in R[x]$ a nechť vedoucí koeficient polynomu g je jednotka okruhu R. Pak existuje právě jedna dvojice polynomů $q, r \in R[x]$ taková, že $st(r) < st(g)$ a $f = g.q + r$.

Euklidův algoritmus:

Buď R těleso. Pak v $R[x]$ libovolné dva nenulové polynomy mají největší společný dělitel k jehož nalezení slouží Euklidův algoritmus.

Buďte f, g nenulové polynomy z $R[x]$. Z věty o dělitelnosti plyne, že existuje nezáporné celé číslo n a polynomy $q_1, ...q_{n+1}, r_1, ..., r_n \in R[x]$ takové, že $st(g) > st(r_1) > ... > st(r_n) \geq 0$ a platí:

$$\begin{aligned}
f &= g.q_1 + r_1 \\
g &= r_1.q_2 + r_2 \\
r_1 &= r_2.q_3 + r_3 \\
&\vdots \\
r_{n-3} &= r_{n-2}.q_{n-1} + r_{n-1} \\
r_{n-2} &= r_{n-1}.q_n + r_n \\
r_{n-1} &= r_n.q_{n+1}
\end{aligned}$$

Důkaz:

1. Dokážeme, že r_n je společný dělitel polynomů f, g.
   $r_n \mid r_{n-1}$ z posledního řádku
   $r_n \mid r_{n-2}$ z předposledního řádku
   $\vdots$
   $r_n \mid g$
   $r_n \mid f$

2. Dokážeme, že r_n je $\mathsf{nsd}(f, g)$. $((a \mid f) \wedge (a \mid g) \Rightarrow a \mid r_n)$
   $a \mid f \wedge a \mid g \Rightarrow a \mid r_1$ z 1. rovnice
   $a \mid g \wedge a \mid r_1 \Rightarrow a \mid r_2$ z 2. rovnice
   $\vdots$
   $a \mid r_{n-2} \wedge a \mid r_{n-1} \Rightarrow a \mid r_n$ z (n+2). rovnice

VII. Násobnost kořene, použití derivace

Lemma pro R komutativní okruh

1. $(f+g)(c) = f(c) + g(c)$
2. $(f.g)(c) = f(c) \cdot g(c)$

Kořen polynomu:

Nechť R je okruh, $c \in R$, $f \in R[x], f = a_n x^n + \ldots + a_1 x + a_0$. Pokud platí $f(c) = a_n c^n + \ldots + a_1 c + a_0 = 0$, pak c je *kořenem* polynomu.

Věta o kořenu polynomu:

Buď R komutativní okruh. Pak $c \in R$ je kořen polynomu $f \in R[x]$, právě když $(x-c)|f$.

Důkaz:

$\Longleftarrow$ $q \in R[x]$. $(x-c).q = f$, $0 = (c-c).q(c) = f(c)$, c je kořen f.

$\Longrightarrow$ Nechť c je kořen pak podle: f=g.q + r existují $q, r \in R[x]$, takové, že r je konstantní a $f = (x-c).q + r \Rightarrow r = f - (x-c).q \Rightarrow r = r(c) = f(c) - (c-c).q(c) = 0$. Tedy $(x-c)|f$.

Násobnost kořene polynomu:

Buď R komutativní okruh, $f \in R[x]$, c je kořen f. Číslo $k \in N$ se nazývá *násobnost kořene* c, jestliže $(x-c)^k | f$ a $(x-c)^{k+1} \not| f$.

Derivace:

Nechť R je okruh, $f = a_n x^n + \ldots + a_1 x + a_0 \in R[x]$. Polynom $f' = n a_n x^{n-1} + \ldots + 2a_2 x + a_1 \in R[x]$ se nazývá *derivace polynomu* f.

Věta o počtu kořenů:

Buď R obor integrity. Pak nenulový polynom $f \in R[x]$ má nejvýše $n = st(f)$ kořenů, počítáme-li každý kořen tolikrát, kolikrát je násobný.

Důkaz:

Nechť f má kořeny $c_1, \ldots, c_l$, (po dvou různé) násobností $k_1, \ldots, k_l$.
Pak $(x-c_1)^{k_1}, \ldots, (x-c_l)^{k_l}$ dělí f.

Chceme ukázat že:
$f = (x-c_1)^{k_1} \cdot \ldots \cdot (x-c_l)^{k_l} \cdot q$, kde $q \in R[x]$,
pak $st(f) = k_1 + \ldots + k_l + st(q)$, $k_1, \ldots, k_l \leq st(f)$, tedy $k_1 + \ldots + k_l + st(q) \leq st(f)$.

1. $(x-c_1)^{k_1} | f$
2. $(x-c_2)^{k_2} | f$, $f = (x-c_1)^{k_1} h_1$
   $\{(x-c)^l, (x-d)^k$; $c \neq d$, jsou nesoudělné $\Rightarrow$ jednoznačnost rozkladů $\}$
   $\Rightarrow (x-c_2)^{k_2} | h_1 \Rightarrow \ldots (x-c_l)^{k_l} | f = (x-c_1)^{k_1} \cdot \ldots \cdot (x-c_{l-1})^{k_l - 1} | h_{l-1} \Rightarrow$
   $(x-c_l)^{k_l} | h_{l-2} \Rightarrow f = (x-c_1)^{k_1} \cdot \ldots \cdot (x-c_l)^{k_l} \cdot q$

Lemma:

Buď R okruh, $f, g \in R[x]$. Pak platí:

1. $(f+g)' = f' + g'$
2. $(f.g)' = f'.g + f.g'$

Věta I.

Je-li prvek c *komutativního okruhu* R k-násobným kořenem polynomu $f \in R[x]$, pak c je i kořenem polynomů $f', f'', \ldots, f^{'(k-1)}$

Důkaz: Pokud a je k-násobným kořenem pak $f = (x-c)^k.q$, $q \in R[x]$. Dále $(q.(x-c)^k)' = k(x-c)^{k-1}.q + (x-c)^k.q' = (x-c)^{k-1}(k.q + (x-c).q')$ Odsud plyne tvrzení věty.

Důsledek věty o počtu kořenů, použití derivace.

Buď $(R, +, \cdot)$ těleso charakteristiky 0, $f \in R[x]$, $f \neq 0$, $a \in R$ kořen f, pak pro libovolné $k \geq 2$ platí:
a je k násobný kořen $f \iff a$ je $(k-1)$ násobný kořen (f, f')

Důkaz:

$\Longrightarrow$ Je-li a k násobný kořen, pak a je podle věty I. $(k-1)$ násobný kořen f', takže $(x-a)^k | f$, $(x-a)^{k-1} | f' \Longrightarrow (x-a)^{k-1} | (f, f')$
$(x-a)^k \not| f'$ takže určitě $(x-a)^{k-1} \not| (f', f)$, tedy a je $(k-1)$ násobný kořen (f, f').

$\Longleftarrow$ Je-li $(k-1)$ násobný kořen (f, f') pak zejména a je kořen f s násobností l. Podle předpokladu předchozí části důkazu je a $(l-1)$násobný kořen (f, f') odtud lze $(k-1) = (l-1) \Longrightarrow k = l$

Věta II.

Buď R těleso charakteristiky 0, $f \in R[x]$, $a \in R$ a $k \geq 2 \in N$. Pak platí:
Je-li a k-násobný kořen f pak a je (k-1) násobný kořen f', dále je-li a jednoduchý kořen f pak a není kořenem f'.

Důkaz:
Buď a k-násobný kořen f. Pak $(x-a)^k | f$, $(x-a)^{k+1} \not| f$, dále $f = (x-a)^k.g$, $g \in R[x]$
Pak $f' = ((x-a)^k)'.g + (x-a)^k.g' = k(x-a)^{k-1}.g + (x-a)^k.g' = (x-a)^{k-1}[kg + (x-a)g']$ tedy $(x-a)^{k-1} | f'$.

Kdyby $(x-a)^k | f'$ potom vzhledem k jednoznačnosti rozkladu v $R[x]$ $(x-a) | [kg + (x-a)g']$ odtud $(x-a) | kg$. Poněvadž $k \neq 0$ ($(R, +, .)$ je charakteristiky 0) potom $(x-a) | q$ platilo by $(x-a)^{k+1} | f$ ...SPOR.

Tedy $(x-a)^k \not| f'$ čili a je $(k-1)$ násobný kořen f'.

VIII. Racionální kořeny polynomů nad Q

Primitivní polynom:

Nenulový polynom $g \in Z[x]$ se nazývá *primitivní*, je-li největší společný dělitel všech koeficientů roven 1.

Irreducibilní polynom:

Polynom $f \in R[x]$ se nazývá irreducibilní, jestliže je nekonstantní a nelze jej zapsat ve tvaru součinu dvou nekonstantních polynomů.

Věta o kořenu polynomu

Buď R komutativní okruh. Pak $c \in R$ je kořen polynomu $f \in R[x] \iff (x-c)|f$.

Důkaz:

$\Longleftarrow$ Jakmile $x - c|f$, zřejmě $f(c) = 0$. ($f = (x-c).q \Rightarrow 0 = (c-c).q(c) = f(c)$)

$\Longrightarrow$ Nechť c je kořen pak: $\mathsf{f = g.q + r}$ existují $q \in R[x]$, $r \in R$ takové, že $f = (x-c).q + r \Rightarrow r = f - (x-c).q \Rightarrow r = f(c) - (c-c).q(c) = 0$. Tedy $x - c|f$.

Asociované polynomy:

Buď R těleso. Polynomy $f, g \in R[x]$ nazývejme *asociované* právě když existuje $0 \neq c \in R$, tak že platí $f = c.g$

Lemma:

Každý polynom $f \in Q[x]$ je asociovaný s nějakým polynomem $g \in Z[x]$.

Důkaz:

Nechť $(\frac{a_n}{b_n})x^n + \ldots + (\frac{a_1}{b_1})x + (\frac{a_0}{b_0})$, $f \in f[x]$. $c = b_1 \cdot \ldots \cdot b_n$. Potom jistě $g = c.f$, $g \in Z[x]$.

Důsledek:

Při vyšetřování kořenů polynomů z $Q[x]$ se stačí omezit na $Z[x]$.

Věta o racionálních kořenech polynomu:

Nechť $f = a_n x^n + \ldots + a_1 x + a_0 a \in Z[x]$ a $\frac{r}{s}$ je racionální kořen polynomu f takový, že $(r, s) = 1$.

1. Pak $s|a_n$ a $r|a_0$.
2. Pro libovolné $c \in Z$ je $(r - cs)|f(c)$

Důkaz:

1. Polynom $a_n x^n + \ldots + a_1 x + a_0 = 0$. Za x dosadíme kořen $(\frac{r}{s})$.
   $a_n(\frac{r}{s})^n + a_{n-1}(\frac{r}{s})^{n-1} + \ldots + a_1(\frac{r}{s}) + a_0 = 0 \mid \times s^n$
   $a_n.r^n + a_{n-1}r^{n-1}.s + \ldots + a_1.r.s^{n-1} + a_0.s^n = 0$
   $\sum_{j=0}^{n} a_{n-j}.r^{n-j}.s^j = \sum_{j=0}^{n} a_j.r^j.s^{n-j}$

   Pak protože kořen je tvaru $(\frac{r}{s})$, $\begin{array}{l} r|a_0.s^n \Rightarrow r|a_0, \text{neboť} (r,s) = 1. \\ s|a_0.r^n \Rightarrow s|a_n, \text{neboť} (r,s) = 1. \end{array}$
2. Dělením polynomu f polynomem $(x - c)$ nad Z se zbytkem dostaneme: $f = (x-c)h + f(c)$, $h \in Z[x]$, odtud $f(c) = f - (x-c)h$. Dosazením $(\frac{r}{s})$ za x máme $f(c) = f(\frac{r}{s}) - (\frac{r}{s} - c).h(\frac{r}{s}) = -(\frac{r}{s} - c)h(\frac{r}{s})$ neboť $\frac{r}{s}$ je kořen f. Vynásobením s^n dostaneme $f(c)s^n = -(r - cs).(s^{n-1}.h(\frac{r}{s}))$ takže $(r - cs)|f(c)s^n$, ale poněvadž $(r, s) = 1$ také $(r - cs, s) = 1$, odtud $(r - cs)|f(c)$.

Důsledek:

Tato věta nám umožňuje najít racinální kořeny polynomu, neboť pokud $(\frac{r}{s})$ je kořenem f pak $s.x - r|f$ podle věty o kořenu polynomu.

Einsensteinovo kritérium:

Buď $a_n x^n + \ldots + a_1 x + a_0 a \in Z[x]$, p prvočíslo, $p|a_0, \ldots, p|a_{n-1}, p \not| a_n, p^2 \not| a_0$. Pak f je irreducibilní nad $Q[x]$.

Věta:

Polynom $f \in Z[x]$ je irreducibilní $\Leftrightarrow$ je irreducibilní nad Q.

K vytvoření tohoto textu nás poháněla nouze, ale nakonec se nám oběma "strašáka albřáka" podařilo udolat. Aby se Vám podařilo totéž Vám přejí:

Petr Handlar
Jiří Wotke