Fermatova a Eulerova věta, Podílová tělesa oborů integrity

Algebra 2

Mgr. Markéta Trnečková, Ph.D.

Palacký University, Olomouc

Fermatova věta

Aditivní grupy $\mathbb{Z}_n$ a $\mathbb{Z}/n\mathbb{Z}$ jsou přirozeně isomorfní.
Třídy $a + n\mathbb{Z}$ pro každé $a \in \mathbb{Z}_n$.
Sčítání tříd v $\mathbb{Z}/n\mathbb{Z}$ jsme definovali sčítáním reprezentantů tříd
Ze $\mathbb{Z}/n\mathbb{Z}$ uděláme okruh tak, že budeme třídy analogickým způsobem násobit.
Musíme jen ukázat, že takto definovaný součin je dobře definovaný.
Asociativita a distributivní zákony plynou z vlastností reprezentantů v $\mathbb{Z}$.
Vybereme reprezentanty tříd $a + rn \in a + n\mathbb{Z}$ a $b + sn \in b + n\mathbb{Z}$
$(a + rn)(b + sn) = ab + (as + rb + rsn)n$, což je prvek $ab + n\mathbb{Z}$.

Tvrzení

Pro libovolné těleso, nenulové prvky s násobením tvoří grupu.

Fermatova věta

Věta 46 (Malá Fermatova věta)

Pokud $a \in \mathbb{Z}$ *a* p *je prvočíslo, které nedělí* a*, pak* p *dělí* $a^{p-1} - 1$*, tj.* $a^{p-1} \equiv 1 \pmod{p}$ *pro* $a \not\equiv 0 \pmod{p}$.

Důkaz

Uvažujme $\mathbb{Z}_p$*. Nenulové prvky* $1, 2, \ldots p-1$*. Z předchozího tvrzení vidíme, že tvoří grupu řádu* $p-1$ *s násobením modulo* p.

Protože řád libovolného prvku v grupě dělí řád té grupy, vidíme, že pro $b \in \mathbb{Z}$*,* $b \neq 0$ *platí, že* $b^{p-1} = 1$.

Použitím toho, že $\mathbb{Z}_p$ *je isomorfní s okruhem tříd rozkladu ve tvaru* $a + p\mathbb{Z}$ *vidíme, že pro libovolné* $a \in \mathbb{Z}$*,* $a \notin 0 + p\mathbb{Z}$ *musí platit*

$a^{p-1} \equiv 1 \pmod{p}$.

Fermatova věta

Důsledek 12

Pokud $a \in \mathbb{Z}$, *pak* $a^p \equiv a \pmod{p}$ *pro libovolné prvočíslo* p.

Důkaz

Pro $a \not\equiv 0 \pmod{p}$ *to plyne z předchozí věty.*
Pro $a \equiv 0 \pmod{p}$ *se obě strany redukují na* $0 \pmod{p}$.

Příklad 93

Spočítejte zbytek 8^{103} *po dělení* 13.
Využijte Malou Fermatovu větu.

Fermatova věta

Příklad

Spočítejte zbytek 8^{103} *po dělení* 13.

- 8 nedělí 13
- $8^{103} = (8^{12})^8(8^7)$
- $(8^{12}) = (8^{13-1})$, $(8^{13-1}) \equiv 1 \pmod{13}$
- $(8^{12})^8(8^7) \equiv (1^8)(8^7) \equiv 8^7 \pmod{13}$
- $8^7 = (-5)^7$
- $(-5)(-5)^6 = (-5)(25)^3 = (-5)(-1)^3 = (-8)$
- $8^{103} \equiv 5 \pmod{13}$

Příklad 94

Ukažte, že $2^{11213} - 1$ *není dělitelné* 11.

Fermatova věta

Příklad

Ukažte, že $2^{11213} - 1$ *není dělitelné* 11.

- Dle Fermatovy věty $2^{10} \equiv 1 \pmod{11}$
- $2^{11213} - 1 \equiv [(2^{10})^{1121} \cdot 2^3] - 1 \equiv [1^{1121} \cdot 2^3] - 1 \equiv 2^3 - 1 \equiv 8 - 1 \equiv 7 \pmod{11}$
- Zbytek po dělení čísla $2^{11213} - 1$ číslem 11 je 7 (ne 0)

Příklad 95

Ukažte, že pro všechny $n \in \mathbb{Z}$ *platí, že* $n^{33} - n$ *je dělitelné* 15.

Fermatova věta

Příklad

Ukažte, že pro všechny $n \in \mathbb{Z}$ *platí, že* $n^{33} - n$ *je dělitelné* 15.

- $15 = 3 \cdot 5$
- Pomocí Fermatovy věty ukážeme, že všechna $n^{33} - n$ jsou dělitelná 3 i 5
- Pokud 3 dělí n, pak určitě dělí $n(n^{32} - 1)$
- Pokud 3 nedělí n, dle Fermatovy věty $n^2 \equiv 1 \pmod 3$, takže
  $n^{32} - 1 \equiv (n^2)^{16} - 1 \equiv 1^{16} - 1 \equiv 0 \pmod 3$
  3 dělí $n^{32} - 1$ tedy i $n(n^{32} - 1)$
- Pokud 5 dělí n, pak určitě dělí $n(n^{32} - 1)$
- Pokud 5 nedělí n, dle Fermatovy věty $n^4 \equiv 1 \pmod 5$, takže
  $n^{32} - 1 \equiv (n^4)^8 - 1 \equiv 1^8 - 1 \equiv 0 \pmod 5$
  5 dělí $n^{32} - 1$ tedy i $n(n^{32} - 1)$

Fermatova věta

Tvrzení

Z malé Fermatovy věty plyne $a^{-1} \equiv a^{p-2} \pmod{p}$.

Příklad

Určete a^{-1} *v* $\mathbb{Z}_7$ *pro* $a = 2$.

Fermatova věta

Příklad

Určete a^{-1} *v* $\mathbb{Z}_7$ *pro* $a = 2$.

- $a^{-1} \equiv a^{p-2} \pmod p$
- $2^{-1} \equiv 2^{7-2} \pmod 7$
- $2^{-1} \equiv 2^5 \pmod 7$
- $2^5 \pmod 7 = 4$

Eulerovo zobecnění Fermatovy věty

Věta 47

Nechť G_n je množina nenulových čísel z $\mathbb{Z}_n$, které nejsou dělitelé nuly. Pak G_n s násobením modulo n tvoří grupu.

Důkaz

Musíme ukázat, že $\underline{G_n \text{ je uzavřená na násobení modulo } n}$
$a, b \in G_n$. *Pokud $ab \notin G_n$, pak by v $\mathbb{Z}_n$ existovalo $c \neq 0$ takové, že $(ab)c = 0$.*
Z asociativity plyne $(ab)c = a(bc) = 0$.
Protože $b \in G_n$ a $c \neq 0$, máme, že $bc \neq 0$ (dle definice G_n).
To by ale pak znamenalo, že $a \notin G_n$, protože $a(bc) = 0$.
Což je spor.

Ukázali jsme, že pro každý okruh je množina nenulových prvků, které nejsou dělitelé nuly, uzavřená na násobení.

Eulerovo zobecnění Fermatovy věty

Důkaz (Pokračování)

Musíme ukázat, že G_n je grupa
Násobení modulo n je asociativní.
$1 \in G_n$
Zbývá ukázat existenci inverzních prvků. Nechť $1, a_1, \ldots, a_r$ jsou prvky G_n.
Pro $a \in G_n$ jsou prvky $a1, aa_1, \ldots, aa_r$ všechny různé. To proto, že $aa_i = aa_j$ by znamenalo $a(a_i - a_j) = 0$ a a není dělitel 0, pak musí $(a_i - a_j) = 0$ $(a_i = a_j)$.
Musí platit $a1 = 1$ nebo nějaké $aa_i = 1$ a tedy a má inverzi.

Eulerovo zobecnění Fermatovy věty

Definice

Mějme $n \in \mathbb{N}$*. Funkce* $\varphi : \mathbb{N} \to \mathbb{N}$ *je funkce, která* n *přiřadí počet čísel v* $\mathbb{N}$ *menších nebo rovno* n*, které jsou nesoudělné s* n*. Této funkci říkáme* **Eulerova funkce***.*

Příklad 96

Vypočítejte $\varphi(n)$ *pro* $n = 12$*.*

Eulerovo zobecnění Fermatovy věty

Příklad

Vypočítejte $\varphi(n)$ *pro* $n = 12$.

- Čísla nesoudělná s 12:
  $1, 5, 7, 11$
- $\varphi(12) = 4$

Eulerovo zobecnění Fermatovy věty

Z věty 41 víme, že v okruhu $\mathbb{Z}_n$ jsou dělitelé nuly právě ty prvky, které nejsou nesoudělné s n.

Tvrzení

$\varphi(n)$ *je počet nenulových prvků* $\mathbb{Z}_n$, *které nejsou dělitelé nuly.*

Eulerovo zobecnění Fermatovy věty

Věta 48 (Eulerova věta)

Pokud a je celé číslo nesoudělné s n, pak $a^{\varphi(n)} - 1$ je dělitelné n. Tedy
$a^{\varphi(n)} \equiv 1 \pmod n$

Důkaz

Pokud je a nesoudělné s n, pak třída $a + n\mathbb{Z}$ dle podgrupy $n\mathbb{Z}$ obsahující a obsahuje číslo $b < n$, které je nesoudělné s n.
Použitím faktu, že součin tříd lze vyjádřit součinem jejich reprezentantů (součin modulo n) a platí
$a^{\varphi(n)} \equiv b^{\varphi(n)} \pmod n$
b je prvek multiplikativní grupy G_n řádu $\varphi(n)$ obsahující $\varphi(n)$ prvků $\mathbb{Z}_n$ nesoudělných s n.
Takže $b^{\varphi(n)} \equiv 1 \pmod n$.

Příklad 97

Vyzkoušejte platnost věty pro $n = 12$.

Eulerovo zobecnění Fermatovy věty

Příklad

Vyzkoušejte platnost věty 48 pro $n = 12$.

- $\varphi(12) = 4$.
- a nesoudělné s 12: $a^4 \equiv 1 \pmod{12}$
- 5:
  $5^4 = (25)^2 = 625 = 12(52) + 1$
  $5^4 \equiv 1 \pmod{12}$
- 7:
  $7^4 = (49)^2 = 2401 = 12(200) + 1$
  $7^4 \equiv 1 \pmod{12}$

Řešení rovnic

Věta 49

Nechť $m \in \mathbb{N}$ *a* $a \in \mathbb{Z}$ *je nesoudělné s* m*.*
Pro každé $b \in \mathbb{Z}_m$*, rovnice* $ax = b$ *má unikátní řešení v* $\mathbb{Z}_m$*.*

Důkaz

Dle věty 47 víme, že a *má multiplikativní inverzi (je jednotka) v* $\mathbb{Z}_m$*.* $s = a^{-1}b$ *je jistě řešením rovnice. Násobením* a^{-1} *obě strany rovnice* $ax = b$ *dostaneme, že je to jediné řešení.*

Předchozí věta v řeči kongruencí.

Důsledek 13

Pokud a *a* m *jsou nesoudělné, tak pro libovolná celá čísla* b *má kongruence*

$$ax \equiv b \pmod{m}$$

jako řešení všechna čísla v právě jedné zbytkové třídě modulo m*.*

Řešení rovnic

Věta 50

Nechť $m \in \mathbb{N}$ a $a, b \in \mathbb{Z}$, $d = gcd(a, m)$.
Rovnice $ax = b$ *má řešení v* $\mathbb{Z}_m$ *právě, když* d *dělí* b.
Když d *dělí* b, *má tato rovnice právě* d *řešení v* $\mathbb{Z}_m$.

Důkaz

Prvně ukažme, že neexistuje řešení $ax = b$ *v* $\mathbb{Z}_m$ *pokud* d *nedělí* b.
Předpokládejme, že $s \in \mathbb{Z}_m$ *je řešení. Pak* $as - b = qm$ *v* $\mathbb{Z}$. *Takže* $b = as - qm$. *Protože* d *dělí* a *i* m, *vidíme, že* d *dělí pravou stranu a tedy musí dělit i* b. *Řešení existuje jen, když* d *dělí* b.

Počet řešení. Předpokládejme, že d *dělí* b.
Nechť $a = a_1 d$, $b = b_1 d$ *a* $m = m_1 d$
Pak rovnice $as - b = qm$ *v* $\mathbb{Z}$ *může být přepsána jako* $d(a_1 s - b_1) = dqm_1$. *Vidíme, že* $as - b$ *je násobek* m *právě, když* $a_1 s - b_1$ *je násobek* m_1. *Takže řešení rovnice* $ax = b$ *v* $\mathbb{Z}_m$ *jsou právě ty prvky, které modulo* m_1 *dají řešení rovnice* $a_1 x = b_1$ *v* $\mathbb{Z}_{m_1}$.

Řešení rovnic

Důkaz (Pokračování)

Nechť $s \in \mathbb{Z}_{m_1}$ *je unikátní řešení* $a_1x = b_1$ *(dané větou 49). Čísla v* $\mathbb{Z}_m$*, které se zredukují na* s *modulo* m_1*, jsou přesně ty, které mohou být vypočítány v* $\mathbb{Z}_m$ *jako*
$s,\ s + m_1,\ s + 2m_1,\ \dots,\ s + (d-1)m_1$
Takže existuje právě d *řešení rovnice v* $\mathbb{Z}_m$*.*

Důsledek 14

Nechť $d = gcd(a, m)$*. Kongruence* $ax \equiv b \pmod{m}$ *má řešení právě když* d *dělí* b*, Pokud to platí, řešení jsou v právě* d *různých zbytkových třídách modulo* m*.*

- Z důkazu věty plyne i to, že když je libovolné řešení s nalezeno, tak řešení jsou právě všechny prvky zbytkových tříd $(s + km_1) + m\mathbb{Z}$, kde $m_1 = m/d$ a $k = 0, \dots, d-1$.
- Také můžeme najít takové s nalezením $a_1 = a/d$ a $b_1 = b/d$ a řešením $a_1x \equiv b_1 \pmod{m_1}$.
- Při řešení kongruence můžeme uvažovat nahrazení a_1 a b_1 jejich zbytky modulo m_1 a řešit $a_1x = b_1$ v $\mathbb{Z}_{m_1}$.

Řešení rovnic

Příklad 98

Najděte všechna řešení kongruence $12x \equiv 27 \pmod{18}$.

Využijte předchozí důsledek.

Řešení rovnic

Příklad

Najděte všechna řešení kongruence $12x \equiv 27 \pmod{18}$.

- $gcd(12, 18) = 6$
- 6 není dělitel 27, takže řešení neexistuje.

Příklad 99

Najděte všechna řešení kongruence $15x \equiv 27 \pmod{18}$.

Řešení rovnic

Příklad

Najděte všechna řešení kongruence $15x \equiv 27 \pmod{18}$.

- $gcd(15, 18) = 3$ a 3 je dělitel 27
- Vše vydělíme 3 a uvažujeme kongruenci $5x \equiv 9 \pmod 6$
- Řešíme rovnici $5x = 3$ v $\mathbb{Z}_6$
- Jednotky v $\mathbb{Z}_6$ jsou 1 a 5
  5 je zjevně svoje vlastní inverze
- Řešení je $x = (5^{-1})(3) = (5)(3) = 3$
- Řešení $15x \equiv 27 \pmod{18}$ jsou čísla v následujících zbytkových třídách
  $3 + 18\mathbb{Z} = \{\dots, -33, -15, 3, 21, 39, \dots\}$
  $9 + 18\mathbb{Z} = \{\dots, -27, -9, 9, 27, 45, \dots\}$
  $15 + 18\mathbb{Z} = \{\dots, -21, -3, 15, 33, 51, \dots\}$
  Všechna tato čísla padnou do zbytkové třídy $3 + 6\mathbb{Z}$ modulo 6, protože vzešly z řešení $x = 3$ rovnice $5x = 3$ v $\mathbb{Z}_6$

Řešení rovnic – shrnutí

$ax \equiv 0 \pmod{n}$:

- Vždy existuje řešení $x = 0$
- **Existují i jiná?**
- Pokud $gcd(a, n) = 1$, pouze jedno řešení $[0]$
- Pokud $gcd(a, n) \neq 1$ více řešení

Příklad

$3x = 0$ v $\mathbb{Z}_{19}$, $gcd(3, 19) = 1$ *jen jedno řešení* $[0]$.

$3x = 0$ v $\mathbb{Z}_{15}$, $gcd(3, 15) = 3$ *jen jedno řešení* $[0]$.
Vykrátíme 3
$x \equiv 0 \pmod{5}$
Řešení: $\{0, 5, 10\}$
$x + 0 = 0$
$x + 5 = 0$
$x + 10 = 0$

Řešení rovnic – shrnutí

$ax \equiv b \pmod{n}$:

- b není násobkem $gcd(a,n)$ – nemá řešení
- b je násobkem $gcd(a,n)$
  - $gcd(a,n) = 1$ jedno řešení
  - $gcd(a,n) \neq 1$ více řešení (**Kolik?**)

Příklad

$3x = 5$ v $\mathbb{Z}_{15}$, $gcd(3,15) = 3$, 5 *není násobkem* 3 *– nemá řešení*

$3x = 5$ v $\mathbb{Z}_{11}$, $gcd(3,11) = 1$, 5 *je dělitelné* 1 *– jedno řešení*
$4 \cdot 3x \equiv 4 \cdot 5 \pmod{11}$ *Vlevo chceme x, hledáme inverzní prvek k 3 a tím vynásobíme*
$12x \equiv 20 \pmod{11}$
$x \equiv 9 \pmod{11}$

$3x = 9$ v $\mathbb{Z}_{15}$, $gcd(3,11) = 3$, 9 *je dělitelné* 3 *– více řešení*
$3x \equiv 9 \pmod{15}$ *Vykrátíme 3*
$x \equiv 3 \pmod{5}$
$x = 3,\ x = 3 + 5 = 8,\ x = 3 + 5 + 5 = 13$

Podílová tělesa oborů integrity

- Pokud má každý nenulový prvek oboru integrity multiplikativní inverzi, jedná se o komutativní těleso.
- Mnoho oborů integrity ale těleso netvoří. Například $\mathbb{Z}$.
- Ukážeme si ale, že každý obor integrity může být obsažen (můžeme ho rozšířit na) v nějakém komutativním tělese, které nazýváme **podílové těleso oboru integrity**.
- Toto těleso bude minimální těleso obsahující ten obor integrity
  Například pro $\mathbb{Z}$ jím je $\mathbb{Q}$. (Prvky $\mathbb{Q}$ můžeme vyjádřit jako podíly prvků $\mathbb{Z}$)

Podílová tělesa oborů integrity

Postup konstrukce

- Nechť D je obor integrity, který chceme rozšířit na podílové těleso F.
- Hrubá kostra:
  1. Definujeme, co budou prvky F
  2. Definujeme binární operaci sčítání a násobení v F
  3. Zkontrolujeme, zda v F platí všechny axiomy komutativního tělesa
  4. Ukážeme, že F můžeme vnímat tak, že obsahuje D jako podobor integrity

Podílová tělesa oborů integrity

Krok 1 – definice prvků F

- Nechť D je obor integrity
  $D \times D = \{(a,b) | a,b \in D\}$
- Dvojici (a,b) budeme chápat jako reprezentaci formálního podílu a/b
  Např. pro $D = \mathbb{Z}$ dvojice $(2,3)$ představuje $\frac{2}{3}$.
- Nebudeme však uvažovat všechny prvky kartézského součinu, jen
  $S = \{(a,b) | a,b \in D, b \neq 0\}$
  Např. pro $D = \mathbb{Z}$ dvojice $(2,0)$ nereprezentuje žádné číslo.
- Stále nemáme výsledné pole, protože různé dvojice mohou reprezentovat stejné číslo.
  Např. pro $D = \mathbb{Z}$ to mohou být dvojice $(2,6)$ a $(1,3)$.
- Proto definujeme následující ekvivalenci na S

Podílová tělesa oborů integrity

Definice

Dva prvky (a, b) *a* (c, d) *v* S *jsou* **ekvivalentní** *právě, když* $ad = bc$.
Značíme $(a, b) \sim (c, d)$.

- Definice je rozumná, protože je kritérium definováno pouze na prvcích D a na jeho operaci násobení.
  Např. pro $D = \mathbb{Z}$.Dvojice $(2, 6)$ a $(1, 3)$ je ekvivalentní, protože $(2)(3) = (6)(1)$, což odpovídá našemu chápání rovnosti zlomků $\frac{2}{6} = \frac{1}{3}$.

Věta 51

Relace $\sim$ *mezi prvky* S *je ekvivalence.*

Důkaz

Reflexivita:
Pokud $(a, b) \sim (a, b)$, *pak* $ab = ba$. *To platí, protože násobení v* D *je komutativní.*

Podílová tělesa oborů integrity

Důkaz (Pokračování)

Symetrie:
Pokud $(a,b) \sim (c,d)$*, pak* $ad = bc$*. Protože násobení v* D *je komutativní, platí* $cb = da$ *a následně* $(c,d) \sim (a,b)$*.*

tranzitivita:
Pokud $(a,b) \sim (c,d)$ *a* $(c,d) \sim (e,f)$*, pak* $ad = bc$ *a* $cf = de$*. Spolu s využitím komutativity násobení dostaneme*
$afd = fad = fbc = bcf = bde = bed$
Protože $d \neq 0$ *a* D *je obor integrity, platí zákon o krácení a tedy z* $afd = bed$ *dostaneme* $af = be$*, takže* $(a,b) \sim (e,f)$*.*

- $\sim$ určuje rozklad S
  třídu obsahující (a,b) označíme $[(a,b)]$
- Množinou F rozumíme třídy rozkladu S podle $\sim$
  Množinu všech tříd $[(a,b)]$

Podílová tělesa oborů integrity

Krok 2 – definice operací

Lemma 2

Pro $[(a,b)]$ *a* $[(c,d)]$ *v* F*, rovnice*
$[(a,b)] + [(c,d)] = [(ad+bc, bd)]$
$[(a,b)][(c,d)] = [(ac, bd)]$
jsou dobře definované operace sčítání a násobení v F*.*

Pokud bychom brali $D = \mathbb{Z}$, $[(a,b)]$ je $\frac{a}{b}$ a výše definované operace jsou operace v $\mathbb{Q}$.

Důkaz

Výsledky jsou v F

Pokud jsou $[(a,b)]$ *a* $[(c,d)]$ *v* F*, pak* (a,b)*,* (c,d) *jsou v* S*, takže* $b \neq 0$ *a* $d \neq 0$*.*
Protože D *je obor integrity,* $bd \neq 0$ *a tedy* $(ad+bc, bd)$ *a* (ac, bd) *jsou v* S*. To znamená, že* $[(ad+bc, bd)]$ *a* $[(ac, bd)]$ *jsou v* F*.*

Podílová tělesa oborů integrity

Důkaz (Pokračování)

<u>Operace jsou dobře definované</u>: (byly definované pomocí reprezentantů, když vybereme jiné, zda dostaneme stejné výsledky)
Předpokládejme, že $(a_1, b_1) \in [(a,b)]$ *a* $(c_1, d_1) \in [(c,d)]$
<u>Sčítání</u>: Musíme ukázat, že $(a_1 d_1 + b_1 c_1, b_1 d_1) \in [(ad + bc, bd)]$.
$(a_1, b_1) \in [(a,b)]$ *znamená* $(a_1, b_1) \sim (a,b)$ *tj.* $a_1 b = a b_1$. *Obdobně* $(c_1, d_1) \in [(c,d)]$ *implikuje* $c_1 d = c d_1$.
Obě strany rovnice $a_1 b = a b_1$ *vynásobíme* $d_1 d$ *a* $c_1 d = c d_1$ *vynásobíme* $b_1 b$. *Sečtením rovnic dostaneme*
$a_1 b d_1 d + c_1 d b_1 b = b_1 a d_1 d + d_1 c b_1 b$.
Díky tomu, že je D *obor integrity můžeme rovnici upravit:*
$(a_1 d_1 + b_1 c_1) bd = b_1 d_1 (ad + bc)$ *a odtud dostaneme*
$(a_1 d_1 + b_1 c_1, b_1 d_1) \sim (ad + bc, bd)$
a tedy $(a_1 d_1 + b_1 c_1, b_1 d_1) \in [(ad + bc, bd)]$.

Podílová tělesa oborů integrity

Důkaz (Pokračování)

Násobení: Musíme ukázat, že $(a_1c_1, b_1d_1) \in [(ac, bd)]$.
$(a_1, b_1) \in [(a, b)]$ *znamená* $(a_1, b_1) \sim (a, b)$ *tj.* $a_1b = ab_1$. *Obdobně* $(c_1, d_1) \in [(c, d)]$ *implikuje* $c_1d = cd_1$.
Vynásobením rovnic $a_1b = ab_1$ *a* $c_1d = cd_1$ *dostaneme*
$a_1bc_1d = b_1ad_1c$.
Díky tomu, že je D *obor integrity můžeme rovnici upravit:*
$a_1c_1bd = b_1d_1ac$ *a odtud dostaneme*
$(a_1c_1, b_1d_1) \sim (ac, bd)$
a tedy $(a_1c_1, b_1d_1) \in [(ac, bd)]$.

Podílová tělesa oborů integrity

Krok 3 – ověření platnosti axiomů

1. Sčítání je v F komutativní
2. Sčítání je v F asociativní
3. $[(0,1)]$ je neutrální prvek sčítání v F
4. $[(-a,b)]$ je inverzní prvek sčítání pro $[(a,b)]$ v F
5. Násobení je F asociativní
6. Násobení je v F komutativní
7. V F platí distributivní zákony
8. $[(1,1)]$ je neutrální prvek násobení v F
9. Pokud $[(a,b)] \in F$ není neutrální prvek sčítání, pak $a \neq 0$ v D a $[(b,a)]$ je inverze vzhledem k násobení k prvku $[(a,b)]$

Podílová tělesa oborů integrity

Důkaz (1)

Sčítání je v F komutativní.
Dle definice
$[(a,b)] + [(c,d)] = [(ad + bc, bd)]$.
$[(c,d)] + [(a,b)] = [(cb + da, db)]$.
Potřebujeme ukázat, že $(ad + bc, bd) \sim (cb + da, db)$
Jelikož je D obor integrity platí, že
$ad + bc = cb + da$ a $bd = db$

Podílová tělesa oborů integrity

Důkaz (9)

Nechť $[(a, b)] \in F$. *pokud* $a = 0$, *tak*
$a1 = b0 = 0$, *takže* $(a, b) \sim (0, 1)$ *a tedy* $[(a, b)] = [(0, 1)]$.
$[(0, 1)]$ *je aditivní neutrální prvek. Pokud tedy* $[(a, b)]$ *není neutrální aditivní prvek v* F,
pak $a \neq 0$
$[(a, b)][(b, a)] = [(ab, ba)]$. *V* D *platí* $ab = ba$ *takže* $(ab)1 = (ba)1$ *a* $(ab, ba) \sim (1, 1)$
Takže $[(a, b)][(b, a)] = [(1, 1)]$ *a* $[(1, 1)]$ *je multiplikativní neutrální prvek.*

Podílová tělesa oborů integrity

Krok 4 – D je podobor integrity F

- Najdeme isomorfismus i oboru integrity D na podobor F
- Pak přejmenujeme obraz D skrze i, použitím jmen z D

Lemma 3

Zobrazení $i : D \to F$ dané předpisem $i(a) = [(a, 1)]$ je isomorfismus D na podokruh tělesa F.

Důkaz

Pro $a, b \in D$ platí $i(a + b) = [(a + b, 1)]$. Také
$i(a) + i(b) = [(a, 1)] + [(b, 1)] = [(a1 + 1b, 1)] = [(a + b, 1)]$
Takže $i(a + b) = i(a) + i(b)$ (homomorfismus)
Injektivita:
pokud $i(a) = i(b)$, tak $[(a, 1)] = [(b, 1)]$, takže $(a, 1) \sim (b, 1)$, což nám dá $a1 = 1b$ neboli $a = b$.
Takže i je isomorfismus D s $i[D]$ a samozřejmě $i[D]$ je podokruh F.

Podílová tělesa oborů integrity

Věta 52

Obor integrity D může být rozšířen na komutativní těleso F (nebo vnořen do F) tak, že každý prvek F může být vyjádřen jako podíl dvou prvků z D. F se nazývá **podílové těleso oboru integrity** *D.*

Na začátku jsme řekli, že F můžeme v jakémsi smyslu uvažovat jako minimální komutativní těleso obsahující D.
Je evidentní, že každé komutativní těleso musí obsahovat prvky a/b pro každé $a, b \in D$, kde $b \neq 0$.

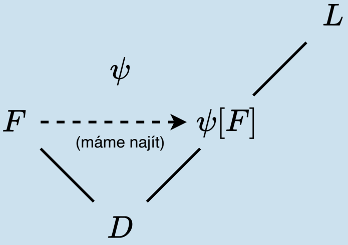
Podílová tělesa oborů integrity

Věta 53

Nechť F je podílové těleso oboru integrity D a L pole obsahující D. Pak existuje zobrazení $\psi : F \to L$, které je isomorfismus F na podtěleso L takový, že $\psi(a) = a$ pro $a \in D$.

Důkaz

Prvek z F je ve tvaru $a/_F b$, kde $/_F$ označuje podíl prvku $a \in D$ a $b \in D$, jako prvků F.
Samozřejmě chceme zobrazit $a/_F b$ na $a/_L b$, kde $/_L$ označuje podíl prvků v L. Hlavní úkol je ukázat, že je toto zobrazení dobře definované.
Musíme definovat $\psi : F \to L$. $\psi(a) = a$ pro $a \in D$.
Každé $x \in F$ je podíl $a/_F b$ pro dva prvky $a, b \neq 0$ v D.
Definujeme $\psi(a/_F b) = \psi(a)/_L \psi(b)$.



Podílová tělesa oborů integrity

Důkaz (Pokračování)

Definujeme $\psi(a/_F b) = \psi(a)/_L \psi(b)$.
Protože ψ *je identita na* D, *pro* $b \neq 0$ *platí* $\psi(b) \neq 0$, *takže definice* $\psi(a/_F b) = \psi(a)/_L \psi(b)$ *má smysl.*
Pokud $a/_F b = c/_F d$ *v* F, *pak* $ad = bc$ *v* D, *takže* $\psi(ad) = \psi(bc)$, *ale protože je* ψ *identita na* D
$\psi(ad) = \psi(a)\psi(d)$ *a* $\psi(bc) = \psi(b)\psi(c)$
Takže $\psi(a)/_L \psi(b) = \psi(c)/_L \psi(d)$ *v* L *a tak je* ψ *dobře definované.*

Rovnice $\psi(xy) = \psi(x)\psi(y)$ *a* $\psi(x+y) = \psi(x) + \psi(y)$ *vycházejí přímo z definice* ψ *na* F *a z toho, že* ψ *je identita na* D.
Pokud $\psi(a/_F b) = \psi(c/_F d)$, *platí*
$\psi(a)/_L \psi(b) = \psi(c)/_L \psi(d)$
Takže $\psi(a)\psi(d) = \psi(b)\psi(c)$.
Protože ψ *je identita na* D, *dostáváme, že* $ad = bc$, *takže* $a/_F b = c/_F d$.
Takže ψ *je injektivní.*

Podílová tělesa oborů integrity

Důsledek 15

Každé komutativní těleso L obsahující obor integrity D obsahuje podílové těleso oboru integrity D.

Důkaz

V důkazu předchozí věty je každý prvek podtělesa $\psi[F]$ tělesa L podíl v L prvků z D.

Důsledek 16

Libovolná dvě podílová tělesa oboru integrity D jsou isomorfní.

Důkaz

Předpokládejme, že v předchozí větě je L podílové těleso oboru integrity D, takže každý prvek $x \in L$ může být vyjádřen ve tvaru $a/_L b$ pro $a, b \in D$.
Pak L je těleso $\psi[F]$ důkazu předchozí věty a je tedy isomorfní s F.