Nadpole, Vektorové prostory

Algebra 2

Mgr. Markéta Trnečková, Ph.D.

Palacký University, Olomouc

Připomenutí

Definice

Aditivní podgrupa N okruhu R splňující
$aN \subseteq N$ a $Nb \subseteq N$ pro všechna $a, b \in R$
se nazývá **ideál**.

Definice

Maximální ideál okruhu R *je ideál $M \neq R$ takový, že neexistuje žádný vlastní ideál N, takový, že $M \subset N$.*

Věta (Věta 70)

Nechť R je komutativní okruh s jedničkou.
Pak M je maximální ideál R, právě když R/M je pole.

Věta (Věta 75)

Ideál $\langle p(x) \rangle \neq \{0\}$ okruhu $F[x]$ je maximální, právě když $p(x)$ je nedělitelný nad F.

Nadpole

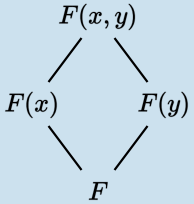
Definice

Pole E je **nadpole** *(též* **rozšíření***) pole F, pokud $F \leq E$. (Zapisujeme také $E \geq F$)*

Příklad 128

- $\mathbb{R}$ *je nadpole* $\mathbb{Q}$, $\mathbb{C}$ *je nadpole* $\mathbb{R}$ *i* $\mathbb{Q}$

- $F(x)$ *označuje podílové těleso okruhu* $F[x]$



Nadpole

Věta 76 (Kroneckerova věta)

Nechť F je pole a $f(x)$ je nekonstantní polynom v $F[x]$. Pak existuje $E \geq F$ a $\alpha \in E$ takové, že $f(\alpha) = 0$.

Důkaz

Dle věty 62, $f(x)$ má faktorizaci v $F[x]$ na polynomy, které jsou nedělitelné nad F.
Nechť $p(x)$ je nedělitelný polynom v takové faktorizaci.
Zjevně stačí najít takové nadpole E pole F, které obsahuje α takové, že $p(\alpha) = 0$.
Dle věty 75 je $\langle p(x) \rangle$ maximální ideál v $F[x]$, takže $F[x]/\langle p(x) \rangle$ je pole.
Tvrdíme, že F může být identifikováno s podpolem pole $F[x]/\langle p(x) \rangle$ přirozeným způsobem, použitím zobrazení $\psi : F \to F[x]/\langle p(x) \rangle$ dané
$\psi(a) = a + \langle p(x) \rangle$, pro $a \in F$.

Důkaz (Pokračování)

$\psi(a) = a + \langle p(x)\rangle$, *pro* $a \in F$
Toto zobrazení je injektivní, protože pokud $\psi(a) = \psi(b)$, *pak* $a + \langle p(x)\rangle = b + \langle p(x)\rangle$ *pro nějaké* $a, b \in F$, *tak* $(a - b) \in \langle p(x)\rangle$, *takže* $a - b$ *musí být násobek polynomu* $p(x)$ *stupně* ≥ 1.
$a, b \in F$ *implikuje* $a - b \in F$, *takže musíme mít* $a - b = 0$, *neboli* $a = b$.
Sčítání a násobení v $F[x]/\langle p(x)\rangle$ *jsme definovali přes reprezentanty, takže můžeme vybrat* $a \in (a + \langle p(x)\rangle)$. *A tedy* ψ *je homomorfismus, který bijektivně zobrazuje* F *na nějaké podpole* $F[x]/\langle p(x)\rangle$.
Identifikujeme F *s* $\{a + \langle p(x)\rangle | a \in F\}$ *skrze zobrazení* ψ.
Na $E = F[x]/\langle p(x)\rangle$ *se budeme dívat jako na nadpole pole* F.
Vytvořili jsme tedy hledané nadpole E *pole* F.

Nadpole

Důkaz (Pokračování)

Zbývá ukázat, že E obsahuje kořen $p(x)$.
Postavme $\alpha = x + \overline{\langle p(x) \rangle}$, takže $\alpha \in E$.
Uvažujme homomorfismus vyhodnocení $\phi_\alpha : F[x] \to E$ (dle věty 55).
Pro $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, kde $a_i \in F$, platí
$\phi(p(x)) = a_0 + a_1(x + \langle p(x) \rangle) + \cdots + a_n(x + \langle p(x) \rangle)^n$
v $E = F[x]/\langle p(x) \rangle$.
Ale v $F[x]/\langle p(x) \rangle$ můžeme počítat výběrem reprezentantů a x je reprezentant třídy $\alpha = x + \langle p(x) \rangle$. Takže
$p(\alpha) = (a_0 + a_1 x + \cdots + a_n x^n) + \langle p(x) \rangle = p(x) + \langle p(x) \rangle = \langle p(x) \rangle = 0$
v $F[x]/\langle p(x) \rangle$.
Našli jsme tedy prvek α v $E = F[x]/\langle p(x) \rangle$ takový, že $p(\alpha) = 0$ a tedy $f(\alpha) = 0$.

Nadpole

Příklad 129

Nechť $F = \mathbb{R}$, $f(x) = x^2 + 1$ *(víme, že nemá kořeny v* $\mathbb{R}$*, je nedělitelný v* $\mathbb{R}$*).*
Pak $\langle x^2 + 1 \rangle$ *je maximální ideál v* $\mathbb{R}[x]$*, takže* $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ *je pole.*
Identifikujeme $r \in \mathbb{R}$ *s* $r + \langle x^2 + 1 \rangle$ *v* $\mathbb{R}[x]/\langle x^2 + 1 \rangle$*.*
Pak se na $\mathbb{R}$ *můžeme dívat jako na nadpole* $E = \mathbb{R}[x]/\langle x^2 + 1 \rangle$*.*
Pak $\alpha = x + \langle x^2 + 1 \rangle$*.*
Počítáním v $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ *dostaneme*
$\alpha^2 + 1 = (x + \langle x^2 + 1 \rangle)^2 + (1 + \langle x^2 + 1 \rangle) = (x^2 + 1) + \langle x^2 + 1 \rangle = 0.$
Takže α *je kořen* $x^2 + 1$*.*
Později si ukážeme, že $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ *je* $\mathbb{C}$*.*

Nadpole

Příklad 130

Nechť $F = \mathbb{Q}$, $f(x) = x^4 - 5x^2 + 6$.
$f(x)$ *se dá rozložit a* $(x^2 - 2)(x^2 - 3)$, *kde oba ty faktory jsou nedělitelné nad* $\mathbb{Q}$.
Začneme s $x^2 - 2$ *(nebo s* $x^2 - 3$*) a zkonstruujeme nadpole* E *pole* $\mathbb{Q}$ *obsahující* α *takové, že* $\alpha^2 - 2 = 0$ *(obsahující* β *takové, že* $\beta^2 - 3 = 0$*) stejným způsobem jako v předchozím příkladě.*

Nadpole

Definice

Prvek α nadpole E pole F je **algebraický nad** F*, když $f(\alpha) = 0$ pro nějaký nenulový $f(x) \in F[x]$.*
Pokud α není algebraický nad F, tak je **transcendentální nad** F*.*

Příklad 131

Rozhodněte, zda jsou následující prvky algebraické nad $\mathbb{Q}$.

1. $\sqrt{2}$
2. i

Nadpole

Příklad

Rozhodněte, zda jsou následující prvky algebraické nad $\mathbb{Q}$.

1. $\sqrt{2}$
2. i

- $\mathbb{C}$ je nadpole $\mathbb{Q}$, $\sqrt{2}, i \in \mathbb{C}$
- $\sqrt{2}$ je kořen polynomu $x^2 - 2$, vidíme, že $\sqrt{2}$ je algebraický prvek nad $\mathbb{Q}$
- i je kořen polynomu $x^2 + 1$, vidíme, že i je algebraický prvek nad $\mathbb{Q}$

Nadpole

Příklad 132

Je známo (ale je těžké dokázat), že reálná čísla π a Eulerova konstanta e jsou transcendentální nad $\mathbb{Q}$.

Příklad 133

Je π algebraický nebo transcendentální prvek nad $\mathbb{R}$?

Nadpole

Příklad

Je π algebraický nebo transcendentální prvek nad $\mathbb{R}$?

- Algebraický. Je to kořen polynomu $(x - \pi) \in \mathbb{R}[x]$

Příklad 134

Je $\alpha = \sqrt{1 + \sqrt{3}} \in \mathbb{R}$ algebraické nad $\mathbb{Q}$?

Nadpole

Příklad

Je $\alpha = \sqrt{1+\sqrt{3}} \in \mathbb{R}$ *algebraické nad* $\mathbb{Q}$*?*

- Ano, je algebraické
- $\alpha^2 = 1 + \sqrt{3}$
- $\alpha^2 - 1 = \sqrt{3}$
- $(\alpha^2 - 1)^2 = 3$
- $\alpha^4 - 2\alpha + 1 = 3$
- $\alpha^4 - 2\alpha - 2 = 0$
- α je kořen $x^4 - 2x - 2$, což je polynom v $\mathbb{Q}[x]$

Nadpole

Věta 77

Nechť E je nadpole pole F a $\alpha \in E$. Nechť $\phi_\alpha : F[x] \to E$ je homomorfismus vyhodnocení takový, že $\phi_\alpha(a) = a$ pro $a \in F$ a $\phi_\alpha(x) = \alpha$. Pak α je transcendentální nad F, právě když ϕ_α dává isomorfismus $F[x]$ s podoborem pole E, tedy právě když ϕ_α je injektivní.

Důkaz

Prvek α je transcendentální nad F, právě když $f(\alpha) \neq 0$ pro všechny nenulové $f(x) \in F[x]$, což platí dle definice právě když $\phi_\alpha(f(x)) \neq 0$ pro všechny nenulové $f(x) \in F[x]$, což platí, právě když $Ker(\phi_\alpha) = \{0\}$ tedy právě když ϕ_α je injektivní.

Nedělitelné polynomy pro α

Věta 78

Nechť $E \geq F$ a $\alpha \in E$, kde α je algebraický prvek nad F. Pak existuje polynom $p(x) \in F[x]$ nedělitelný nad F takový, že $p(\alpha) = 0$. Tento polynom je unikátně určen až na konstantní faktor v F, jeho stupeň je ≥ 1.
Pokud $f(\alpha) = 0$ pro $f(x) \in F[x]$, $f(x) \neq 0$, pak $p(x)$ dělí $f(x)$.

Důkaz

Nechť ϕ_α je homomorfismus vyhodnocení $F[x] \to E$. $Ker(\phi_\alpha)$ je ideál (dle věty 74 hlavní ideál) generovaný nějakým $p(x) \in F[x]$. $\langle p(x) \rangle$ se skládá z prvků $F[x]$, které mají kořen α
Takže pokud $f(\alpha) = 0$ pro $f(x) \neq 0$, pak $f(x) \in \langle p(x) \rangle$. A tedy $p(x)$ dělí $f(x)$.
Takže $p(x)$ je polynom minimálního stupně ≥ 1, který má kořen α, a každý jiný polynom stejného stupně s kořenem α musí být ve tvaru $(a)(p(x))$ pro nějaké $a \in F$.
Zbývá naám ukázat, že $p(x)$ je nedělitelný. Pokud by $p(x) = r(x)s(x)$, byla by faktorizace na polynomy nižších stupňů, pak $p(\alpha) = 0$ by znamenalo $r(\alpha) = 0$ nebo $s(\alpha) = 0$, protože E je pole. To by ale bylo v rozporu s faktem, že $p(x)$ je minimálního stupně ≥ 1, takový, že $p(\alpha) = 0$. Takže $p(x)$ je nedělitelný.

Nedělitelné polynomy pro α

Definice

Pokud má polynom vedoucí koeficient (koeficient u nejvyšší mocniny) roven 1*, nazýváme ho* **monický**.

Zřejmě můžeme vynásobením polynomu vhodnou konstantou převést na monický.

Definice

Nechť $E \geq F$ *a* $\alpha \in E$ *je algebraický prvek nad* F.
Unikátní monický polynom $p(x)$ *s vlastností z předchozí věty je* **nedělitelný polynom pro** α **nad** F*, značíme* $irr(\alpha, F)$.
Stupeň polynomu $irr(\alpha, F)$ *je* **stupeň** α **nad** F*, značen* $deg(\alpha, F)$.

Nedělitelné polynomy pro α

Příklad 135

Určete stupeň prvku $\sqrt{2}$ nad $\mathbb{Q}$ a nad $\mathbb{R}$.

Nedělitelné polynomy pro α

Příklad

Určete stupeň prvku $\sqrt{2}$ nad $\mathbb{Q}$ a nad $\mathbb{R}$.

- $\sqrt{2} \in \mathbb{R}$ je stupně 2 nad $\mathbb{Q}$
  $irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2$
- $\sqrt{2} \in \mathbb{R}$ je stupně 1 nad $\mathbb{R}$
  $irr(\sqrt{2}, \mathbb{Q}) = x - \sqrt{2}$

Nedělitelné polynomy pro α

Příklad 136

Určete stupeň prvku $\alpha = \sqrt{1+\sqrt{3}} \in \mathbb{R}$ *nad* $\mathbb{Q}$.

Nedělitelné polynomy pro α

Příklad

Určete stupeň prvku $\alpha = \sqrt{1+\sqrt{3}} \in \mathbb{R}$ *nad* $\mathbb{Q}$.

- Víme, že je kořen polynomu $x^4 - 2x - 2 \in \mathbb{Q}$.
- Tento polynom je nedělitelný nad $\mathbb{Q}$ (dle Eisensteinova kritéria pro $p = 2$)
  $irr(\sqrt{1+\sqrt{3}}, \mathbb{Q}) = x^4 - 2x - 2$
- A tedy $\sqrt{1+\sqrt{3}}$ je algebraický prvek stupně 4 nad $\mathbb{Q}$

Jednoduché rozšíření pole

Nechť $E \geq F$, $\alpha \in E$. Nechť $\phi_\alpha : F[x] \to E$ je homomorfismus vyhodnocení daný $\phi_\alpha(a) = a$ pro $a \in F$ a $\phi_\alpha(x) = \alpha$.

α je algebraický prvek nad F:

- Pak $Ker(\phi_\alpha) = \langle irr(\alpha, F) \rangle$ (Viz věta 78)
- $\langle irr(\alpha, F) \rangle$ je maximální ideál $F[x]$ (Viz věta 75)
- $F[x]/\langle irr(\alpha, F) \rangle$ je pole a je isomorfní obrazu $\psi_\alpha(F[x])$ v E
- Toto podpole $\psi_\alpha(F[x]) \leq E$ je nejmenší podpole E obsahující F a α.
- Označme ho $F(\alpha)$.

α je transcendentální prvek nad F:

- ψ_α dá isomorfismus s nějakým podoborem pole E (Viz věta 77)
- $\psi_\alpha(F[x])$ není pole, je to obor integrity. Označme ho $F[\alpha]$
- E obsahuje podílové těleso tohoto oboru $F[\alpha]$, které je pak nejmenší podpole E obsahující F a α (Viz důsledek 15)
- Označme ho $F(\alpha)$.

Jednoduché rozšíření pole

Příklad 137

Protože π je transcendentální nad $\mathbb{Q}$, je pole $\mathbb{Q}(\pi)$ racionálních funkcí nad $\mathbb{Q}$ s neurčitou x.

Z pohledu struktury se prvek, který je transcendentální nad F, chová jako by to byla neurčitá nad F.

Jednoduché rozšíření pole

Definice

Nadpole $E \geq F$ je **jednoduché rozšíření** F*, pokud $E = F(\alpha)$ pro nějaké $\alpha \in E$.*

Jednoduché rozšíření pole

Věta 79

Nechť E je jednoduché rozšíření pole F, α je algebraický prvek nad F a $irr(\alpha, F) = n \geq 1$. Pak každý prvek β z $E = F(\alpha)$ může být unikátně vyjádřen ve tvaru $\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$, kde $b_i \in F$.

Důkaz

Pro obvyklý homomorfismus vyhodnocení ψ_α je každý prvek $F(\alpha) = \psi_\alpha(F[x])$ tvaru $\psi_\alpha(f(x)) = f(\alpha)$ polynom s neurčitou α s koeficienty v F.
Nechť $irr(\alpha, F) = p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$.
Pak $p(\alpha) = 0$, takže
$\alpha^n = -a_{n-1}\alpha^{n-1} - \ldots - a_0$.
Tato rovnice v $F(\alpha)$ může být použita k vyjádření jakéhokoliv polynomu α^m pro $m \geq n$ pomocí mocnin α, které jsou menší než n.
Např. $\alpha^{n+1} = \alpha\alpha^n = -a_{n-1}\alpha^n - a_{n-2}\alpha^{n-1} - \ldots - a_0\alpha$
Takže každé $\beta \in F(\alpha)$ může být vyjádřeno ve tvaru
$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$

Jednoduché rozšíření pole

Důkaz (Pokračování)

Unikátnost *Když*
$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = b'_0 + b'_1\alpha + \cdots + b'_{n-1}\alpha^{n-1}$
Pak $(b_0 - b'_0) + (b_1 - b'_1)x + \cdots + (b_{n-1} - b'_{n-1})x^{n-1} = g(x)$
je v $F[x]$ *a* $g(\alpha) = 0$, *stupeň* $g(x)$ *je menší než stupeň* $irr(\alpha, F)$.
Protože $irr(\alpha, F)$ *je nenulový polynom minimálního stupně v* $F[x]$ *mající kořen* α, *musí platit* $g(x) = 0$.
Takže $(b_i - b'_i) = 0$, *takže* $b_i = b'_i$ *a tím je dokázána unikátnost.*

Jednoduché rozšíření pole

Příklad 138

Polynom $p(x) = x^2 + x + 1$ *v* $\mathbb{Z}_2$. *Je nedělitelný nad* $\mathbb{Z}_2$ (**Jakto?**).
Protože 0 *ani* 1 *není kořen* $p(x)$.
Dle předchozí věty má $\mathbb{Z}_2(\alpha)$ *prvky* $0 + 0\alpha$, $0 + 1\alpha$, $1 + 0\alpha$, $1 + 1\alpha$ *tedy* 0, 1, α *a* $1 + \alpha$.
To nám dává nové konečné pole o 4 *prvcích.*
Jak budou vypadat operace sčítání a násobení?

Jednoduché rozšíření pole

Příklad

Polynom $p(x) = x^2 + x + 1$ *v* $\mathbb{Z}_2$.
$\mathbb{Z}_2(\alpha)$ *má prvky* 0, 1, α *a* $1 + \alpha$.
To nám dává nové konečné pole o 4 *prvcích.*
Jak budou vypadat operace sčítání a násobení?

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Např. $(1+\alpha)(1+\alpha)$ v $\mathbb{Z}_2(\alpha)$, $p(\alpha) = \alpha^2 + \alpha + 1 = 0$, pak
$\alpha^2 = -\alpha - 1 = \alpha + 1$
Takže, $(1+\alpha)(1+\alpha) = 1 + \alpha + \alpha + \alpha^2 = 1 + \alpha^2 = 1 + \alpha + 1 = \alpha$

Jednoduché rozšíření pole

Příklad 139

Pomocí předchozí věty nyní můžeme dokázat, že $\mathbb{R}[x]/\langle x^2+1\rangle$ je isomorfní s $\mathbb{C}$.

- $\mathbb{R}[x]/\langle x^2+1\rangle$ je nadpole pole $\mathbb{R}$
- Nechť $\alpha = x + \langle x^2+1\rangle$
- Pak $\mathbb{R}(\alpha) = \mathbb{R}[x]/\langle x^2+1\rangle$ a sestává se ze všech prvků ve tvaru $a + b\alpha$ pro $a, b \in \mathbb{R}$
- Protože $\alpha^2 + 1 = 0$, vidíme, že α hraje roli $i \in \mathbb{C}$ a $a + b\alpha$ roli $(a + bi) \in \mathbb{C}$
- Takže $\mathbb{R}(\alpha) \simeq \mathbb{C}$
- Toto je algebraický způsob, jak zkonstruovat $\mathbb{C}$ z $\mathbb{R}$

Vektorové prostory

Definice

Nechť F je pole. **Vektorový prostor nad F** *(F-vektorový prostor) sestává z abelovské (aditivní) grupy V s operací skalárního součinu (Ve skutečnosti to není binární operace, ale zobrazení $F \times V \to V$.) každého prvku V s každým prvkem z F zleva takový, že pro všechna $a, b \in F$ a $\alpha, \beta \in V$ platí:*

- $a\alpha \in V$
- $a(b\alpha) = (ab)\alpha$
- $(a + b)\alpha = (a\alpha) + (b\alpha)$
- $a(\alpha + \beta) = (a\alpha) + (a\beta)$
- $1\alpha = \alpha$

Prvky V se nazývají **vektory** *a prvky F se nazývají* **skaláry**.

Pokud je F zjevné z kontextu, vynecháváme ho z pojmenování – vektorový prostor.

Příklad 140

Uvažujme abelovskou grupu $\langle \mathbb{R}^n, + \rangle = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$, *kde je sčítání definováno po komponentách. Definujme skalární součin následujícím způsobem:*
$r\alpha = (ra_1, ra_2, \ldots, ra_n)$ *pro* $r \in \mathbb{R}$, $\alpha = (a_1, \ldots, a_n)$.
Ověřte, že se jedná o vektorový prostor.

Příklad 141

Pro libovolné pole F mlžeme $F[x]$ vnímat jako vektorový prostor nad F, kde sčítání vektorů je běžné sčítání polynomů v $F[x]$ a skalární součin $a\alpha$ je běžné násobení polynomu skalárem.
Ověřte.

Přímo vyplývá z toho, že $F[x]$ je okruh s jedničkou.

Příklad 142

Nechť $E \geq F$. Pak E může být vnímáno jako vektorový prostor nad F, kde sčítání i skalární součin jsou běžné sčítání a násobení v E.
Ověřte.

Přímo vyplývá z toho, že E je pole.

Věta 80

Pro vektorový prostor V nad F platí:
$0\alpha = 0$, $a0 = 0$, $(-a)\alpha = a(-\alpha) = -(a\alpha)$
pro všechna $a \in F$ a $\alpha \in V$.

Důkaz

Znáte z AL1.

Lineární kombinace

Definice

Nechť V *je vektorový prostor nad* F*. Vektory v podmnožině*
$S = \{\alpha_i | i \in I\} \subseteq V$
generují V*, pokud pro každé* $\beta \in V$ *platí*
$\beta = a_1\alpha_{i_1} + a_2\alpha_{i_2} + \cdots + a_n\alpha_{i_n}$ *pro nějaká* $a_i \in F$ *a* $\alpha_{i_j} \in S$, $j = 1, \ldots, n$.
Vektor $\sum_{j=1}^{n} a_j\alpha_{i_j}$ *je* **lineární kombinace** *vektorů* α_{i_j}.

Lineární kombinace

Příklad 143

Generují následující vektory ve vektorovém prostoru $\mathbb{R}^n$ z příkladu 140 tento vektorový prostor?
$(1,0,\ldots,0)$, $(0,1,\ldots,0)$, $\ldots$, $(0,0,\ldots,1)$

Ano

Lineární kombinace

Příklad 144

Generují monomy x^m pro $m \geq 0$ vektorový prostor $F[x]$ nad F? (Vektorový prostor z příkladu 141)

Ano

Lineární kombinace

Příklad 145

Nechť $E \geq F$, $\alpha \in E$ je algebraický prvek nad F. Pak $F(\alpha)$ je vektorový prostor nad F a je generovaný vektory $\{1, \alpha, \ldots, \alpha^{n-1}\}$, kde $n = deg(\alpha, F)$.

Ukážeme si ve větě, kterou představíme později.

Dimenze

Definice

Vektorový prostor V nad polem F je **konečné dimenze**, *pokud existuje konečná podmnožina V, jejíž vektory generují V.*

Příklad 146

Jsou vektorové prostory představené v příkladech 140 - 142 konečné dimenze?
$\mathbb{R}^n$
$F[x]$
$F(\alpha)$ *($E \geq F$, α algebraický prvek nad F)*

Dimenze

Příklad

Jsou vektorové prostory představené v příkladech 140 - 142 konečné dimenze?

- $\mathbb{R}^n$: Ano
- $F[x]$: Ne
  Polynomy libovolného stupně nemohou být lineárními kombinacemi žádné konečné množiny polynomů
- $F(\alpha)$: Ano

Lineární nezávislost

Definice

Vektory v podmnožině $S = \{\alpha_i | i \in I\} \subseteq V$ vektorového prostoru V nad polem F jsou **lineárně nezávislé** *nad F, pokud pro libovolné různé vektory $\alpha_{i_j} \in S$, skaláry $a_j \in F$ a $n \in \mathbb{N}$ platí $\sum_{j=1}^{n} a_j \alpha_{i_j} = 0$ ve V jen tehdy, když $a_j = 0$ pro $j = 1, \ldots, n$.*
Pokud vektory nejsou lineárně nezávislé nad F, tak jsou **lineárně závislé** *nad F.*

Příklad 147

Rozhodněte, zda jsou následující vektory lineárně závislé.

- *Vektory generující prostor $\mathbb{R}^n$ z příkladu 143.*
- *Monomy $\{x^m | m \geq 0\}$ z příkladu 144.*
- *Vektory $(1, -1)$, $(2, 1)$ a $(-3, 2)$ v $\mathbb{R}^2$.*

Lineární nezávislost

Příklad

Rozhodněte, zda jsou následující vektory lineárně závislé.

- *Vektory generující prostor $\mathbb{R}^n$ z příkladu 143.*
- *Monomy $\{x^m | m \geq 0\}$ z příkladu 144.*
- *Vektory $(1, -1)$, $(2, 1)$ a $(-3, 2)$ v $\mathbb{R}^2$.*

- Vektory generující prostor $\mathbb{R}^n$ z příkladu 143.
  Jsou lineárně nezávislé.
- Monomy $\{x^m | m \geq 0\}$ z příkladu 144.
  Jsou lineárně nezávislé.
- Vektory $(1, -1)$, $(2, 1)$ a $(-3, 2)$ v $\mathbb{R}^2$.
  Jsou lineárně závislé.
  $7(1, -1) + (2, 1) + 3(-3, 2) = (0, 0)$

Lineární nezávislost

Příklad 148

Nechť $E \geq F$, $\alpha \in E$ je algebraický prvek nad F. Pokud $deg(\alpha, F) = n$, pak každý prvek $F(\alpha)$ je unikátně vyjádřen ve tvaru
$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$
pro $b_i \in F$. Zvláště $0 + 0\alpha + \cdots + 0\alpha^{n-1}$ musí být unikátní vyjádření pro nulový vektor.
Takže prvky $1, \alpha, \ldots, \alpha^{n-1}$ jsou lineárně nezávislé vektory v $F(\alpha)$ nad F.
Také generují $F(\alpha)$.

Báze

Definice

Pokud V je vektorový prostor nad F, vektory v podmnožině $B = \{\beta_i | i \in I\} \subseteq V$ tvoří **bázi prostoru V nad F**, *pokud generují V a jsou lineárně nezávislé.*

Báze

Lemma 4

Nechť V je vektorový prostor nad F a $\alpha \in V$. Pokud je α lineární kombinace vektorů β_i ve V pro $i = 1, \ldots, m$ a každé β_i je lineární kombinace vektorů γ_j ve V pro $j = 1, \ldots, n$, pak α je lineární kombinace γ_j.

Důkaz

Nechť $\alpha = \sum_{i=1}^{m} a_i \beta_i$ *a* $\beta_i = \sum_{j=1}^{n} b_{ij} \gamma_j$, *kde* $a_i, b_{ij} \in F$. *Pak*
$\alpha = \sum_{i=1}^{m} a_i (\sum_{j=1}^{n} b_{ij} \gamma_j) = \sum_{j=1}^{n} (\sum_{i=1}^{m} a_i b_{ij}) \gamma_j$
a $\sum_{i=1}^{m} a_i b_{ij} \in F$

Báze

Věta 81

Ve vektorovém prostoru konečné dimenze každá konečná množina vektorů, která generuje ten prostor, obsahuje podmnožinu, která je báze tohoto prostoru.

Důkaz

Nechť V je vektorový prostor konečné dimenze nad F a vektory $\alpha_1, \ldots, \alpha_n$ z V generují V. Projdeme ty vektory α_i postupně zleva (začneme $i = 1$) a odstraníme první α_j, které je lineární kombinací předchozích α_i, $i < j$.
Pokračujeme stejně s dalšími α (α_{j+1}). Po konečném počtu kroků dojdeme k α_n.
Dle předchozího lemmatu tato zredukovaná množina α_i stále generuje V.

Pro tuto zredukovanou množinu α_i uvažujme
$a_1\alpha_{i_1} + \cdots + a_r\alpha_{i_r} = 0$. *Pro $i_1 < i_2 < \cdots < i_r$ a že nějaké $a_j \neq 0$. Můžeme předpokládat $a_r \neq 0$. Dostaneme*
$\alpha_{i_r} = (-\frac{a_1}{a_r})\alpha_{i_1}) + \cdots + (-\frac{a_{r-1}}{a_r})\alpha_{i_{r_1}})$,
což ukazuje, že α_{i_r} je lineární kombinace předchůdců, což je v rozporu s konstrukcí.
Takže vektory α_i v redukované sadě jsou nezávislé, generují V a tak tvoří bázi V nad F.

Báze

Důsledek 29

Vektorový prostor konečné dimenze má konečnou bázi.

Důkaz

Dle definice má vektorový prostor konečné dimenze konečnou podmnožinu, která ho generuje. Takže přímo vyplývá z předchozí věty.

Báze

Věta 82

Nechť $S = \{\alpha_1, \ldots, \alpha_r\}$ je konečná množina lineárně nezávislých vektorů vektorového prostoru V konečné dimenze nad F.
Pak S může být rozšířena na bázi prostoru V nad F.
Dále, pokud $B = \{\beta_1, \ldots, \beta_n\}$ je libovolná báze prostoru V nad F pak $r \leq n$.

Důkaz

Dle předchozího důsledku existuje báze $B = \{\beta_1, \ldots, \beta_n\}$ prostoru V nad F. Uvažujme konečnou posloupnost vektorů
$\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_n$
Tyto vektory generují V, protože B je báze. Pomocí techniky z důkazu věty 81 odstraníme postupně ty vektory, které jsou lineárními kombinacemi předchozích.
Všimněme si, že žádné α_i nebude odstraněno, protože jsou lineárně nezávislé. Takže S může být rozšířeno na bázi V nad F.

Důkaz (Pokračování)

Pro druhou část věty, uvažujme posloupnost
$\alpha_1, \beta_1, \ldots, \beta_n$
Tyto vektory nejsou lineárně nezávislé nad F, *protože* α_1 *je lineární kombinací* β_i *(ty tvoří bázi). Takže*
$\alpha_1 = b_1\beta_1 + \cdots + b_n\beta_n$. *Takže*
$\alpha_1 + (-b_1)\beta_1 + \cdots + (-b_n)\beta_n = 0$.
Vektory v té posloupnosti generují V *a pokud vytvoříme bázi technikou z důkazu věty 81, musíme vyřadit alespoň jedno* β_i *a dostaneme bázi*
$\{\alpha_1, \beta_1^{(1)}, \ldots, , \beta_m^{(1)}\}$, *kde* $m \leq n - 1$.
Aplikací stejné techniky dostaneme bázi
$\{\alpha_1, \alpha_2, \beta_1^{(2)}, \ldots, , \beta_s^{(2)}\}$, *kde* $s \leq n - 2$
...
$\{\alpha_1, \alpha_2, \ldots, \alpha_r, \beta_1^{(r)}, \ldots, , \beta_t^{(r)}\}$, *kde*
$0 \leq t \leq n - r$, *tedy* $r \leq n$

Báze

Důsledek 30

Libovolné dvě báze vektorového prostoru V konečné dimenze nad F mají stejný počet prvků.

Důkaz

Nechť $B = \{\beta_1, \ldots, \beta_n\}$, $B' = \{\beta'_1, \ldots, \beta'_n\}$ jsou dvě báze. Dle předchozí věty, kdybychom B uvažovali jako množinu nezávislých vektorů a B' jako bázi dostaneme, že $n \leq m$. Když ale budeme uvažovat B' jako množinu nezávislých vektorů a B jako bázi, dostaneme $m \leq n$. Tudíž $m = n$.

Báze

Definice

Pokud V je vektorový prostor konečné dimenze nad polem F, tak počet prvků v bázi je **dimenze V nad F.**

Příklad 149

Jaké dimenze je vektorový prostor z příkladu 145?
$E \geq F$, $\alpha \in E$ je algebraický prvek nad F. Pak $F(\alpha)$ je vektorový prostor nad F.

Báze

Příklad

Jaké dimenze je vektorový prostor z příkladu 145?
$E \geq F$, $\alpha \in E$ je algebraický prvek nad F. Pak $F(\alpha)$ je vektorový prostor nad F.

- je generovaný vektory $\{1, \alpha, \ldots, \alpha^{n-1}\}$, kde $n = deg(\alpha, F)$
- n je dimenze

Aplikace na teorii polí

Věta 83

Nechť $E \geq F$ a $\alpha \in E$ je algebraický prvek nad F. Pokud $deg(\alpha, F) = n$ pak $F(\alpha)$ je vektorový prostor nad F dimenze n s bází $\{1, \alpha, \ldots, \alpha^{n-1}\}$.
Každý prvek $\beta \in F(\alpha)$ je algebraický nad F a $deg(\beta, F) \leq deg(\alpha, F)$.

Důkaz

Vše až na poslední větu věty už máme dokázáno.
Nechť $\beta \in F(\alpha)$, kde $\alpha \in E$ je algebraický prvek nad F. Dimenze $F(\alpha)$ je n.
Uvažujme prvky $1, \beta, \beta^2, \ldots, \beta^n$.
Toto nemůže být $n+1$ různých prvků $F(\alpha)$, které jsou lineárně nezávislé nad F, protože dle věty 82 libovolná báze $F(\alpha)$ nad F by musela obsahovat alespoň tolik prvků, kolik jich je v libovolné množině lineárně nezávislých vektorů nad F. Ale báze $\{1, \alpha, \ldots, \alpha^{n-1}\}$ má právě n prvků.
Pokud $\beta^i = \beta^j$, pak $\beta^i - \beta^j = 0$, takže $b_0 + b_1\beta + b_2\beta^2 + \cdots + b_n\beta^n = 0$, kde alespoň jedno $b_i \neq 0$.
Pak $f(x) = b_n x^n + \cdots + b_1 x + b_0$ je nenulový prvek $F[x]$ takový, že $f(\beta) = 0$. Takže β je algebraický prvek nad F a $deg(\beta, F)$ je nejvýše n.