Lineární algebra a geometrie

LADISLAV BICAN

ACADEMIA

Obsah

PŘEDMLUVA

Tento učební text je určen hlavně posluchačům 1. ročníku odborného studia matematiky a přiměřeným způsobem jej lze použít pro posluchače 1. ročníku učitelství. Některé podrobnosti týkající se této možnosti jsou uvedeny níže. Nezbytnost sepsání tohoto textu vychází ze skutečnosti, že převážná většina učebnic a učebních textů z lineární algebry vyšla již poměrně dávno, a jsou tudíž posluchačům dosti těžko dostupná.

Nyní několik slov k obsahu skript. Text začíná kapitolou 0, kde jsou shrnuty některé základní pojmy a bez důkazů jejich nejdůležitější vlastnosti, které jsou pro studium dalších kapitol zcela nezbytné a používají se automaticky. Jedná se o konstrukci tělesa komplexních čísel, kořeny polynomů s koeficienty v libovolném tělese, pojem algebraického uzávěru, jeho existenci a jednoznačnost. Zvláštní část je věnována této problematice pro tělesa komplexních, reálných a racionálních čísel včetně metody hledání racionálních kořenů polynomů s racionálními koeficienty. V závěru jsou některé z těchto poznatků použity k popisu jedné z metod konstrukce konečných těles. Zvláštní poznámku zasluhuje pojem charakteristiky oboru integrity, a tudíž i (komutativního) tělesa. Žádné speciální vlastnosti těles se nikde v textu nepoužívají. Proto si čtenář téměř ve všech případech může pod tělesem T představovat buď těleso reálných, nebo racionálních, nebo komplexních čísel. Na několika málo místech se požaduje, aby dané těleso bylo algebraicky uzavřené. V tomto případě nelze za T brát ani těleso racionálních, ani reálných čísel, ale pouze těleso čísel komplexních. Pro platnost některých tvrzení je zase nezbytný předpoklad, aby těleso T mělo charakteristiku různou od 2. Pro všechna výše zmíněná číselná tělesa je tento předpoklad samozřejmě splněn. Poznamenejme ještě, že některé základní poznatky z teorie polynomů nad komutativními tělesy jsou i s důkazy probrány v kapitole 16. Obsah a metody této kapitoly jsou nezávislé na ostatním textu, a lze ji tudíž studovat v podstatě kdykoliv.

Teorie soustav lineárních rovnic a jejich řešení je jedním z hlavních nástrojů lineární algebry. Proto je tato teorie zařazena do textu co nejdříve (i když lze předpokládat, že čtenář tuto problematiku zná alespoň intuitivně z dřívějška), a to hned za základy teorie vektorových prostorů, zejména konečné dimenze a nezbytné poznatky z maticového počtu.

V další části jsou probrány vlastnosti permutací a determinanty čtvercových matic. Následující tři kapitoly pojednávají speciálně o regulárních maticích a souvislostech mezi maticemi a homomorfismy vektorových prostorů. Lineární, bilineární a kvadratické formy na vektorových prostorech tvoří obsah dalších tří kapitol, přičemž další vlastnosti kvadratických forem, potřebné ke studiu kvadrik v projektivních prostorech, jsou uvedeny v kapitole 22. Kapitola 14 je věnována prostorům se skalárním součinem, vlastní hodnoty a Jordanův normální tvar matice tvoří obsah kapitol 15 - 19. Kapitoly 19 - 21 pojednávají o základních vlastnostech afinního, euklidovského a projektivního prostoru a kapitoly 23 - 25 se zabývají kvadrikami v projektivních prostorech a jejich afinní a metrickou klasifikací. Závěrečné dvě kapitoly jsou věnovány jednak principu duality, jednak komplexnímu rozšíření vektorových (a dalších) prostorů nad tělesem reálných čísel.

Na závěr slíbený komentář k obsahu předmětu Lineární algebra pro učitelské studium. Zde kapitoly 0 - 7 plně pokrývají teorii vektorových prostorů, soustav lineárních rovnic a determinantů. Vybrané odstavce z kapitol 8 - 10 tvoří potřebný základ pro studium homomorfismů vektorových prostorů a jejich matic včetně hodnosti. Podobná situace je, i pokud se týče lineárních, bilineárních a kvadratických forem v kapitolách 11, 12 a 13. Prostory se skalárním součinem jsou dostatečně probrány v kapitole 14, vlastní hodnoty a vlastní vektory matic jsou pak obsahem kapitoly 15, čímž je osnova tohoto předmětu prakticky pokryta.

Praha, září 2000 *Autor*

Vzhledem k tomu, že ke studiu lineární algebry jsou zapotřebí některé základní poznatky z jiných algebraických disciplín, shrneme si v této úvodní kapitole nezbytné pojmy a tvrzení týkající se komplexních čísel, kořenů algebraických rovnic, dělitelnosti polynomů a teorie komutativních těles. Přitom se budeme zabývat pouze věcmi nezbytnými ke studiu dalších kapitol a veškerá tvrzení budeme uvádět bez důkazů.

0.1. Komplexní čísla.

Komplexním číslem rozumíme prvek množiny K všech uspořádaných dvojic (a, b) reálných čísel, v níž jsou definovány rovnost a operace sčítání a násobení takto:

$$(a,b) = (c,d)\,, \quad \text{právě když} \quad a = c \quad \text{a} \quad b = d,$$
$$(a,b) + (c,d) = (a+c, b+d),$$
$$(a,b) * (c,d) = (ac - bd, ad + bc).$$

Množinu všech reálných čísel značíme zpravidla písmenem R. Zobrazení $f : R \to K$ množiny všech reálných čísel do množiny všech komplexních čísel definované předpisem $f(r) = (r, 0)$ je zřejmě prosté zobrazení (tj. $f(r) \neq f(s)$, kdykoliv $r \neq s$) splňující podmínky $f(r+s) = f(r) + f(s)$ a $f(rs) = f(r)f(s)$. Z tohoto důvodu můžeme tedy místo dvojice $(r, 0)$ psát prostě jenom r. Označíme-li ještě dvojici $(0, 1)$ písmenem i, můžeme každé komplexní číslo (a, b) napsat ve tvaru $a + bi$, neboť $(a, b) = (a, 0) + (0, b) = a + b(0, 1) = a + bi$.

Buď $\alpha = a + bi$ komplexní číslo. Komplexní číslo $\bar{\alpha} = a - bi$ nazýváme číslem *komplexně sdruženým* k číslu α. Je ihned patrné, že rovnost $\alpha = \bar{\alpha}$ platí právě tehdy, když číslo α je reálné. Dále, nezáporné reálné číslo $\sqrt{\alpha\bar{\alpha}} = \sqrt{a^2 + b^2}$ nazýváme *absolutní hodnotou* nebo *normou* komplexního čísla α a značíme $||\alpha||$. Přitom zřejmě $||\alpha|| = 0$, právě když $\alpha = 0$. Dále je patrné, že pro každé nenulové komplexní číslo α platí $\alpha \cdot \frac{\bar{\alpha}}{||\alpha||^2} = 1$, takže ke každému nenulovému komplexnímu číslu existuje číslo *inverzní*, které se značí buď α^{-1}, nebo $\frac{1}{\alpha}$.

0.2. Odmocniny z komplexních čísel.

Odmocninou z komplexního čísla α rozumíme každé komplexní číslo β, pro které platí rovnost $\beta^2 = \alpha$. Jestliže $\alpha = a + bi$ a $\beta = x + yi$, pak nutně $x^2 - y^2 = a$ a $2xy = b$. Odtud $||\alpha|| = \sqrt{a^2 + b^2} = \sqrt{(x^2 - y^2)^2 + (2xy)^2} = x^2 + y^2$, a tedy $x = \pm\sqrt{\frac{||\alpha||+a}{2}}$, $y = \pm\sqrt{\frac{||\alpha||-a}{2}}$. Ať vezmeme u obou těchto čísel jakákoliv znaménka, je vždy $x^2 - y^2 = a$. Na druhé straně snadno spočteme, že $2xy = |b|$. Vezmeme-li tedy u čísla x jedno ze znamének plus a minus, je znaménko u čísla y již jednoznačně určeno podmínkou $2xy = b$. Celkově tedy vidíme, že ke každému komplexnímu číslu α existují právě dvě komplexní čísla β, lišící se pouze znaménkem, která jsou obě odmocninou z čísla α.

0.3. Obory integrity, tělesa.

Některé pojmy, které si zavedeme v tomto odstavci, lze nalézt v kapitole 16, kde jsou rozebrány s větší podrobností pro účely kapitol následujících.

Neprázdná množina R spolu se dvěma binárními operacemi sčítání $+$ a násobení $\cdot$ definovanými na R se nazývá *okruh*, jestliže pro každé tři prvky $a, b, c \in R$ jsou splněny následující podmínky:

1 $a + b \in A, \quad a \cdot b \in A$

2 $(a + b) + c = a + (b + c)$, 3 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(asociativní zákony)*,

4 $a + b = b + a$ *(komutativní zákon)*

5 existuje prvek $0 \in R$ takový, že $0 + a = a$ *(existence nulového prvku)*,

6 ke každému $a \in R$ existuje prvek $-a \in R$ takový, že $a + (-a) = 0$ *(existence opačného prvku)*,

7 existuje prvek $1 \in R$ tak, že $1 \cdot a = a \cdot 1 = a$ *(existence jednotkového prvku)*,

8 $a \cdot (b + c) = a \cdot b + a \cdot c$, 9 $(b + c) \cdot a = b \cdot a + c \cdot a$ *(distributivní zákony)*.

Prvek 0 se nazývá *nulový prvek*, prvek 1 se nazývá *jednotkový prvek* a prvek $-a$ se nazývá *prvek opačný* k prvku a. V dalším textu budeme zpravidla pro jednoduchost psát ab místo $a \cdot b$ a $a - b$ místo $a + (-b)$. Jestliže platí rovnost $ab = ba$ pro libovolné dva prvky $a, b \in R$, pak říkáme, že okruh R je *komutativní*. Komutativní okruh R, v němž z rovnosti $ab = 0$ plyne buď $a = 0$, nebo $b = 0$, se nazývá *obor integrity*. Typickým příkladem oboru integrity je množina Z všech celých čísel spolu s obvyklými operacemi sčítání a násobení. Okruh s alespoň dvěma prvky, v němž ke každému nenulovému prvku a existuje prvek inverzní a^{-1} takový, že $aa^{-1} = a^{-1}a = 1$, se nazývá *těleso*. Místo a^{-1} se často používá zápisu $\frac{1}{a}$. Jako příklady těles uveďme například množiny všech racionálních, reálných a komplexních čísel spolu s obvyklými operacemi sčítání a násobení. Je-li v tělese T splněn navíc komutativní zákon pro násobení, tj. platí-li rovnost $ab = ba$ pro každé dva prvky $a, b \in T$, pak hovoříme o *komutativním tělese*. Protože v tomto textu budeme pracovat výhradně s komutativními tělesy, budeme pro stručnost místo názvu komutativní těleso používat pouze slovo těleso. Je-li T těleso, $a, b \in T$, $ab = 0$ a $a \neq 0$, pak $b = a^{-1}ab = 0$, takže každé těleso je obor integrity.

0.4. Charakteristika oboru integrity.

Buď R obor integrity a n buď celé číslo. *Celistvým násobkem* $n \times a$ prvku a rozumíme prvek 0 pro $n = 0$, součet n sčítanců $a + a + \cdots + a$ pro $n > 0$ a součet $-n$ sčítanců $-a - a - \cdots - a$ pro $n < 0$. Protože $a \cdot 1 = a$ pro každý prvek $a \in R$, *plyne z distributivního zákona snadno rovnost $n \times a = (n \times 1) \cdot a$. Speciálně tedy pro $a \neq 0$ je $n \times a = 0$ právě když $n \times 1 = 0$.* Podívejme se nyní na *tzv. přirozené násobky* jednotkového prvku, tj. na prvky $n \times 1$, kde n je přirozené číslo.

Mohou nastat dva případy. Jsou-li všechny přirozené násobky navzájem různé, pak říkáme, že R je *obor integrity charakteristiky* 0. V opačném případě existují přirozené násobky takové, že $m \times 1 = n \times 1$, přičemž můžeme bez újmy na obecnosti předpokládat, že $m > n$. Pak ovšem $(m - n) \times 1 = 0$, takže *existují přirozená čísla k s vlastností $k \times 1 = 0$. Nejmenší takové přirozené číslo p se nazývá charakteristika oboru integrity R.* Charakteristika oboru integrity R se obvykle značí symbolem char R. Ukažme si ještě, že charakteristika oboru integrity je vždy buď 0, nebo prvočíslo p. Nechť tedy $p \neq 0$ a předpokládejme, že $p = mn$, $m < p$, $n < p$, je složené číslo. Pak $p \times 1 = (m \times 1) \cdot (n \times 1) = 0$, takže buď $m \times 1 = 0$, nebo $n \times 1 = 0$ vzhledem k tomu, že R je obor integrity. To je však spor s volbou čísla p vzhledem k tomu, že $m < p$ a $n < p$.

0.5. Kořeny polynomů.

Buď $f(x) = f = \sum_{i=0}^{n} a_i x^i$ polynom stupně n (tj. $a_n \neq 0$) s koeficienty v tělese T, $a_0, a_1, \ldots, a_n \in T$. Prvek $\alpha \in T$ se nazývá *kořen polynomu* f, jestliže $f(\alpha) = 0$. Je-li α kořen polynomu f, pak existuje polynom g stupně $n-1$ takový, že $f = (x - \alpha)g$. Polynom g přitom zřejmě získáme dělením polynomu f lineárním polynomem $x - \alpha$.

Buďte $T \subseteq T'$ dvě tělesa. Jestliže součet $a + b$ i součin ab libovolných prvků $a, b \in T$ je v tělese T stejný jako v tělese T', pak říkáme, že T je *podtěleso* v tělese T' nebo že T' je *nadtěleso* tělesa T nebo také že T' je *rozšířením* tělesa T. Tak například těleso K všech komplexních čísel je rozšířením tělesa R všech reálných čísel a těleso R je rozšířením tělesa Q všech racionálních čísel. Říkáme, že prvek $\alpha \in T'$ je *algebraický prvek* nad T, jestliže existuje nenulový polynom $f = \sum_{i=0}^{n} a_i x^i$ (tj. alespoň jedno a_i je různé od nuly) s koeficienty v T, jehož kořenem je prvek α. Jestliže každý prvek tělesa T' je algebraický nad T, pak říkáme, že T' je *algebraické rozšíření* tělesa T. Těleso T takové, že každý polynom kladného stupně má v T alespoň jeden kořen, se nazývá *algebraicky uzavřené*. Buď f polynom kladného stupně n s koeficienty v algebraicky uzavřeném tělese T. Pak polynom f má v tělese T kořen α_1 a podle začátku tohoto odstavce existuje polynom f_1 stupně $n - 1$ s koeficienty v tělese T tak, že $f = (x - \alpha_1)f_1$. Je-li $n > 1$, má polynom f_1 opět kořen α_2 v tělese T a jest $f = (x - \alpha_1)(x - \alpha_2)f_2$ pro nějaký polynom f_2 s koeficienty v tělese T. Pokračujeme-li stejným způsobem dále, dostaneme nakonec rozklad polynomu f v tzv. *kořenové činitele*, $f = a_n(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$. Jsou-li $\alpha_1, \alpha_2, \ldots, \alpha_k$, $k \leq n$, právě všechny navzájem různé kořeny polynomu f, můžeme rozklad polynomu f na kořenové činitele přepsat ve tvaru $f = a_n(x - \alpha_1)^{n_1}(x - \alpha_2)^{n_2}\ldots(x - \alpha_k)^{n_k}$, kde $n_i \geq 1$ jsou přirozená čísla a $\sum_{i=1}^{k} n_i = n$. Číslo n_i se nazývá *násobnost* kořene α_i polynomu f. V některých případech je s ohledem na jednodušší vyjadřování výhodné nazvat libovolný prvek $\alpha \in T$, který není kořenem polynomu f, *0-násobným kořenem* tohoto polynomu. Nadtěleso T' tělesa T, které je algebraicky uzavřené a zároveň je algebraickým rozšířením tělesa T, se nazývá *algebraický uzávěr* tělesa T.

0.6. Věta. *Ke každému tělesu T existuje algebraický uzávěr.* ■

0.7. Věta. *Nechť tělesa T' a T'' jsou dva algebraické uzávěry tělesa T. Pak existuje izomorfismus $f : T' \to T''$ takový, že $f(a) = a$ pro každé $a \in T$.* ■

Připomeňme, že izomorfismem rozumíme každé prosté zobrazení množiny T' na množinu T'' takové, že pro libovolné dva prvky $a, b \in T'$ platí $f(a+b) = f(a)+f(b)$, $f(ab) = f(a)f(b)$ a $f(1) = 1$.

Je-li a prvek algebraicky uzavřeného tělesa T, má polynom $x^2 - a$ podle předchozího výkladu právě dva kořeny. Je patrné, že tyto kořeny se liší pouze znaménkem a každý z nich se nazývá (druhá) *odmocnina z prvku a*.

0.8. Věta. (Základní věta algebry.) *Každý polynom s komplexními koeficienty stupně alespoň 1 má alespoň jeden komplexní kořen.* ■

Je-li $\alpha \in K$ libovolné komplexní číslo, je α kořenem polynomu $(x - \alpha)(x - \bar{\alpha}) = x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha}$ s reálnými koeficienty, takže K je algebraické nad R. Těleso komplexních čísel je tedy algebraickým uzávěrem tělesa reálných čísel.

Na druhé straně těleso R všech reálných čísel není algebraicky uzavřené, neboť např. polynom $x^2 + 1$ nemá žádný reálný kořen.

Buď $f = \sum_{i=0}^{n} a_i x^i$ polynom kladného stupně s reálnými koeficienty. Je-li komplexní číslo α kořenem tohoto polynomu, pak $f(\bar{\alpha}) = \sum_{i=0}^{n} a_i \bar{\alpha}^i = \sum_{i=0}^{n} \overline{a_i \alpha^i} = \overline{\sum_{i=0}^{n} a_i \alpha^i} = \overline{f(\alpha)} = 0$, takže $\bar{\alpha}$ je rovněž kořenem polynomu f. Odtud ihned plyne následující tvrzení.

0.9. Věta. *Každý polynom lichého stupně s reálnými koeficienty má alespoň jeden reálný kořen.* ■

Buď $f = \sum_{i=0}^{n} a_i x^i$ polynom s koeficienty z tělesa racionálních čísel a buď m nejmenší společný násobek jmenovatelů všech racionálních čísel $a_0, a_1, \ldots, a_n$. Pak polynom mf má zřejmě celočíselné koeficienty a stejné kořeny jako polynom. Pro racionální kořeny polynomů s celočíselnými koeficienty platí následující věta.

0.10. Věta. *Buď $f = \sum_{i=0}^{n} a_i x^i$ polynom s celočíselnými koeficienty. Je-li $\frac{r}{s}$ racionální kořen polynomu f, pak r dělí a_0 a s dělí a_n.* ■

Tato věta nám umožňuje nalézt buď některé, nebo všechny kořeny daného polynomu s celými koeficienty.

0.11. Příklad. Nalezněme kořeny polynomu $f(x) = x^7 - 7x^6 + 14x^5 + 5x^4 - 55x^3 + 86x^2 - 68x + 24$.

Ř e š e n í : Podle věty 0.10 připadají v úvahu racionální kořeny $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24$. Dosazením čísla 1 zjistíme, že 1 je kořenem polynomu f. Vydělením $f(x)$ polynomem $x-1$ dostaneme polynom $x^6 - 6x^5 + 8x^4 + 13x^3 - 42x^2 + 44x - 24$. Dosazením zjistíme, že číslo 2 je kořenem tohoto polynomu, a po vydělení $x - 2$ dostaneme $x^5 - 4x^4 + 13x^3 - 16x + 12$. Číslo 2 je opět kořenem a po vydělení $x - 2$ máme $x^4 - 2x^3 - 4x^2 + 5x - 6$. Z možných kořenů $\pm 1, \pm 2, \pm 3, \pm 6$ tohoto polynomu vyhovuje např. číslo -2. Vydělením $x + 2$ dostaneme polynom $x^3 - 4x^2 + 4x - 3$, který má kořen 3. Po vydělení $x - 3$ zbývá kvadratický polynom $x^2 - x + 1$ s kořeny $(1 + i\sqrt{3})/2$ a $(1 - i\sqrt{3})/2$. Polynom f má tedy kořeny $1, 2, -2, 3, (1 + i\sqrt{3})/2, (1 - i\sqrt{3})/2$, přičemž kořen 2 je dvojnásobný.

Konečné těleso je těleso mající konečný počet prvků. Je zřejmé, že každé konečné těleso má nutně nenulovou charakteristiku p.

0.12. Věta. *Buď T konečné těleso charakteristiky p. Pak existuje přirozené číslo n takové, že T má právě p^n prvků. Obráceně, ke každému prvočíslu p a každému přirozenému číslu n existuje konečné těleso mající právě p^n prvků.* ■

0.13. Věta. *Dvě konečná tělesa T a T' jsou izomorfní, právě když mají týž počet prvků.* ■

Vidíme tedy, že pro každé prvočíslo p a každé přirozené číslo n existuje až na izomorfismus jediné těleso o p^n prvcích. Toto těleso se obvykle značí symbolem $GF(p^n)$ (písmena GF jsou zkratkou anglického názvu „Galois field" - Galoisovo těleso).

0.14. Konstrukce konečných těles. Buď p libovolné prvočíslo. Na množině $Z_p = \{0, 1, \ldots, p-1\}$ definujme operace sčítání a násobení tak, že položíme $a + b = r$, $ab = s$, kde r je nejmenší nezáporný zbytek při dělení součtu celých čísel a a b

prvočíslem p a s je nejmenší nezáporný zbytek při dělení součinu celých čísel a a b prvočíslem p. To znamená, že označíme-li součet celých čísel a, b písmenem c a jejich součin písmenem d, existují celá čísla u, r, v, s taková, že $c = pu + r$, $d = pv + s$, kde $0 \le r, s < p$. Je známo, že vzhledem k temto operacím je množina Z_p tělesem $GF(p)$.

Buď nyní f ireducibilní polynom stupně n s koeficienty z tělesa T a označme symbolem $T[x]/\langle f \rangle$ množinu skládající se ze všech polynomů s koeficienty v T, jejichž stupeň je menší než n a z polynomu nulového. Jsou-li g, h dva prvky z $T[x]/\langle f \rangle$, pak zřejmě $g + h \in T[x]/\langle f \rangle$ a existují polynomy q a r s koeficienty z T takové, že $gh = fq + r$, kde buď $r = 0$, nebo $r \in T[x]/\langle f \rangle$ (tj. st $r < n$) (viz věta 16.7). Položíme-li nyní $g \cdot h = r$, je množina $T[x]/\langle f \rangle$ spolu s těmito operacemi tělesem.

Právě popsané metody nám umožňují konstruovat některá nová tělesa, zejména pak konečná, což si ukážeme v následujícím odstavci na konkrétních příkladech.

0.15. Příklady. 1. Pro prvočíslo 5 dostáváme podle první části předchozího odstavce těleso $GF(5)$ s prvky $0, 1, 2, 3, 4$, kde sčítání a násobení je dáno následujícím tabulkami, kde součet (součin) prvků a, b leží v průsečíku řádku, kde je prvek a, a sloupce, kde je prvek b.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

2. Vezměme ireducibilní polynom $f = x^2 + 1$ nad tělesem reálných čísel. Protože nad tělesem reálných čísel je $(a + bx)(c + dx) = ac + bdx^2 + (ad + bc)x = bd(x^2 + 1) + ac - bd + (ad + bc)x$, je v $R[x]/\langle f \rangle (a + bx) \cdot (c + dx) = ac - bd + (ad + bc)x$. Napíšeme-li místo x symbol i, vidíme, že $R[x]/\langle x^2 + 1 \rangle$ je těleso komplexních čísel nebo přesněji řečeno zobrazení f dané předpisem $f(a + bx) = a + bi$ je izomorfismus tělesa $R[x]/\langle x^2 + 1 \rangle$ na těleso komplexních čísel.

3. Snadno se ověří, že polynom $f = x^3 + x^2 + 1$ je ireducibilní nad dvouprvkovým tělesem $GF(2)$. Označíme-li prvky $x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$ z $GF(2)[x]/\langle f \rangle$ po řadě písmeny a, b, c, d, e, f, dostaneme tyto tabulky pro sčítání a násobení v tělese $GF(2^3) = GF(2)[x]/\langle x \rangle$:

+	0	1	a	b	c	d	e	f
0	0	1	a	b	c	d	e	f
1	1	0	b	a	d	c	f	e
a	a	b	0	1	e	f	c	d
b	b	a	1	0	f	e	d	c
c	c	d	e	f	0	1	a	b
d	d	c	f	e	1	0	b	a
e	e	f	c	d	a	b	0	1
f	f	e	d	c	b	a	1	0

$\cdot$	0	1	a	b	c	d	e	f
0	0	0	0	0	0	0	0	0
1	0	1	a	b	c	d	e	f
a	0	a	c	e	d	f	1	b
b	0	b	e	d	1	a	f	c
c	0	c	d	1	f	b	a	e
d	0	d	f	a	b	e	c	1
e	0	e	1	f	a	c	b	d
f	0	f	b	c	e	1	d	a

Na závěr se domluvme, že v celém následujícím textu bude písmeno T značit libovolné těleso, Q těleso racionálních čísel, K těleso komplexních čísel, a pokud nebude řečeno jinak, R těleso reálných čísel. Ve všech případech, kde se výslovně nejedná o tělesa nenulové charakteristiky, si čtenář může představovat pod tělesem T buď těleso racionálních, nebo reálných, nebo komplexních čísel a pod algebraicky uzavřeným tělesem si může vždy představovat těleso čísel komplexních.

Připomeňme si ještě některé běžné základní pojmy. Identické zobrazení množiny M na sebe se značí symbolem 1_M, tj. $1_M : M \to M$ je zobrazení, které každému prvku $x \in M$ přiřazuje opět prvek $x \in M$. Je-li $f : M \to N$ zobrazení množiny M do množiny N, pak f se nazývá *injektivní*, je-li prosté, tj. jestliže pro každé dva prvky $x, y \in M$, $x \neq y$, platí $f(x) \neq f(y)$. Zobrazení f se nazývá *surjektivní*, jestliže zobrazuje množinu M na celou množinu N, tj. jestliže ke každému prvku $y \in N$ existuje alespoň jeden prvek $x \in M$ takový, že $f(x) = y$. *Bijektivní* zobrazení, nebo krátce *bijekce*, je každé zobrazení $f : M \to N$, které je zároveň injektivní i surjektivní, tj. které je vzájemně jednoznačné. Je-li $f : M \to N$ zobrazení a $K \subseteq M$ je libovolná podmnožina, pak *restrikcí* f na podmnožinu K rozumíme zobrazení $g = f|K : K \to N$ takové, že $g(x) = f(x)$ pro každé $x \in K$.

1.1. Definice. Buď T libovolné těleso. *Vektorovým prostorem nad tělesem T* rozumíme neprázdnou množinu V, na níž je definováno sčítání dvojic prvků (tj. každé dvojici prvků $\boldsymbol{u}$, $\boldsymbol{v} \in V$ je jednoznačně přiřazen prvek $\boldsymbol{u}+\boldsymbol{v} \in V$) a násobení prvků z V prvky z tělesa T (tj. každému $\boldsymbol{u} \in V$ a každému $r \in T$ je jednoznačně přiřazen prvek $r\boldsymbol{u} \in V$). Přitom pro všechna $\boldsymbol{u}$, $\boldsymbol{v}$, $\boldsymbol{w} \in V$ a všechna $r, s \in T$ musí být splněny tyto podmínky:

1. $\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{v}+\boldsymbol{u}$,
2. $(\boldsymbol{u}+\boldsymbol{v})+\boldsymbol{w}=\boldsymbol{u}+(\boldsymbol{v}+\boldsymbol{w})$,
3. existuje prvek $\boldsymbol{o} \in V$ takový, že $0 \cdot \boldsymbol{u}= \boldsymbol{o}$ pro každé $\boldsymbol{u} \in V$,
4. $r(\boldsymbol{u}+\boldsymbol{v})=r\boldsymbol{u}+r\boldsymbol{v}$,
5. $(r+s)\boldsymbol{u}=r\boldsymbol{u}+s\boldsymbol{u}$
6. $r(s\boldsymbol{u})=(rs)\boldsymbol{u}$,
7. $1 \cdot \boldsymbol{u}=\boldsymbol{u}$.

Prvky vektorového prostoru se nazývají *vektory*, vektor $\boldsymbol{o}$ se nazývá *nulový vektor*. Prvkům z tělesa T se též někdy říká *skaláry*.

1.2. Poznámka. Vzhledem k tomu, že z kontextu je vždy zcela jasné, kdy se jedná o nulový vektor $\boldsymbol{o}$ a kdy o nulový prvek $0 \in T$, je zbytečné tyto prvky symbolicky od sebe odlišovat. Proto budeme pro jednoduchost jak prvek $0 \in T$, tak i nulový vektor $\boldsymbol{o}$ značit týmž symbolem, totiž 0. Nejjednodušším příkladem vektorového prostoru je tzv. *triviální* nebo *nulový vektorový prostor* 0, skládající se pouze z nulového vektoru. Vzhledem k tomu, že ani v tomto případě nemůže dojít k nedorozumění, budeme triviální vektorový prostor značit rovněž symbolem 0.

V literatuře bývá často vektorový prostor definován tak, že místo axiomu 3 se požaduje platnost těchto dvou axiomů:

3'. existuje prvek $0 \in V$ takový, že $0+\boldsymbol{u}=\boldsymbol{u}$ pro každé $\boldsymbol{u} \in V$,

3". ke každému $\boldsymbol{u} \in V$ existuje vektor $(-\boldsymbol{u}) \in V$ tak, že $\boldsymbol{u}+(-\boldsymbol{u})=0$.

Dříve než si ozřejmíme, že obě definice jsou ekvivalentní poznamenejme, že uvedené dvě podmínky spolu s ostatními axiomy vektorového prostoru neříkají nic jiného, než že V je vzhledem k operaci sčítání komutativní grupa. Jsou-li splněny podmínky 3' a 3", pak $0=(0\boldsymbol{u})+(-0\boldsymbol{u})=(0+0)\boldsymbol{u}+(-0)\boldsymbol{u}=0\boldsymbol{u}+0\boldsymbol{u}+(-0\boldsymbol{u})= 0\boldsymbol{u}+0=0\boldsymbol{u}$ a V je vektorový prostor. Obráceně, je-li V vektorový prostor, pak $0+\boldsymbol{u}=0\boldsymbol{u}+1\boldsymbol{u}=(0+1)\boldsymbol{u}=1\boldsymbol{u}=\boldsymbol{u}$ a pro $(-\boldsymbol{u})=(-1)\boldsymbol{u}$ je $\boldsymbol{u}+(-\boldsymbol{u})= 1\boldsymbol{u}+(-1)\boldsymbol{u}=(1-1)\boldsymbol{u}=0\boldsymbol{u}=0$ a podmínky 3' a 3" jsou splněny.

Viděli jsme, že pro $-\boldsymbol{u}=(-1)\boldsymbol{u}$ platí $\boldsymbol{u}+(-\boldsymbol{u})=0$. Vektor $-\boldsymbol{u}$ se nazývá *vektor opačný* k vektoru $\boldsymbol{u}$. Místo $\boldsymbol{u}+(-\boldsymbol{v})$ budeme v dalším jednoduše psát $\boldsymbol{u}-\boldsymbol{v}$.

1.3. Příklady vektorových prostorů. 1. Těleso T spolu s operacemi sčítání a násobení definovanými na T je zřejmě vektorový prostor nad T.

2. Speciálně těleso reálných čísel R je vektorový prostor nad R. Vektorový prostor nad R budeme nazývat *reálným vektorovým prostorem.*

3. Těleso komplexních čísel K je vzhledem k obvyklým operacím sčítání a násobení jak reálný, tak *komplexní vektorový prostor* (tj. vektorový prostor nad K).

4. Množina P všech kladných reálných čísel spolu s operacemi $\oplus$ a $\odot$, kde $\boldsymbol{u}\oplus\boldsymbol{v}= \boldsymbol{u}\boldsymbol{v}$, $r \odot \boldsymbol{u}=\boldsymbol{u}^r$, $\boldsymbol{u}, \boldsymbol{v} \in P, r \in R$, je reálný vektorový prostor.

5. Buď S neprázdná množina a označme T^S množinu všech zobrazení definovaných na S s hodnotami v T. Definujeme-li pro $f, g \in T^S$, $r \in T$ operace $(f+g)(x) = f(x) + g(x)$ a $(rf)(x) = rf(x)$ pro každé $x \in S$, je množina T^S spolu s těmito operacemi zřejmě vektorovým prostorem nad T.

6. Množina $C\langle a, b\rangle$ všech spojitých reálných funkcí definovaných na uzavřeném intervalu $\langle a, b\rangle$ je vzhledem k operacím z příkladu 5 reálný vektorový prostor.

7. Podobně je reálný vektorový prostor množina $C^n\langle a, b\rangle$ všech reálných funkcí definovaných na uzavřeném intervalu $\langle a, b\rangle$ a majících na tomto intervalu spojité derivace až do řádu n včetně.

8. Množina $P(T)$ všech polynomů s koeficienty v T je spolu s obvyklými operacemi sčítání polynomů a násobení prvkem z T vektorový prostor nad T.

1.4. Definice. Buď n přirozené číslo. Na množině T^n všech uspořádaných n-tic prvků z množiny T definujme binární operaci sčítání prvků předpisem

$$(u_1, u_2, \ldots, u_n) + (v_1, v_2, \ldots, v_n) = (u_1 + v_1, u_2 + v_2, \ldots, u_n + v_n)$$

a operaci násobení prvku z T^n prvkem z tělesa T předpisem

$$r(u_1, u_2, \ldots, u_n) = (ru_1, ru_2, \ldots, ru_n).$$

Množina T^n spolu s těmito operacemi se nazývá *aritmetický vektorový prostor dimenze n nad tělesem T* nebo též *n-rozměrný aritmetický vektorový prostor nad tělesem T*.

1.5. Poznámka. Všimněme si, že aritmetický vektorový prostor T^n je speciálním případem vektorového prostoru T^S z příkladu 5. Stačí totiž vzít za S množinu $\{1, 2, \ldots, n\}$ a každé zobrazení $f \in T^S$ ztotožnit s uspořádanou n-ticí prvků $(f(1), f(2), \ldots, f(n))$.

1.6. Definice. Neprázdná podmnožina W vektorového prostoru V se nazývá *podprostorem* ve V, jestliže je uzavřená vzhledem k operacím sčítání vektorů a násobení vektoru prvkem z tělesa T, tj. jestliže platí:

(i) jsou-li $\boldsymbol{u}, \boldsymbol{v} \in W$ dva libovolné vektory, pak $\boldsymbol{u} + \boldsymbol{v} \in W$;

(ii) je-li $\boldsymbol{u} \in W$ libovolný vektor a $r \in T$ libovolný prvek, pak $r\boldsymbol{u} \in W$.

Skutečnost, že W je podprostorem ve V budeme značit symbolem $W \leq V$. Množina $\{0\}$ a celý prostor V jsou zřejmě podprostory prostoru V. Tyto podprostory se nazývají *nevlastní* (nebo *triviální*), všechny ostatní podprostory se pak nazývají *vlastní* (*netriviální*). Ve smyslu poznámky 1.2 budeme nulový prostor $\{0\}$ rovněž značit jednoduše symbolem 0, neboť ani v tomto případě nemůže dojít k nedorozumění.

1.7. Příklady. 1. Množina prvků

$$M = \{(x+y, y+1, 2x+y) \mid x, y \in R\} \subseteq R^3$$

není podprostorem v R^3. Tato množina totiž nesplňuje dokonce ani jednu z podmínek uvedených v předchozí definici. Pro $x = y = 1$ máme $\boldsymbol{u} = (2, 2, 3) \in M$ a pro $x = 1, y = 2$ pak $\boldsymbol{v} = (3, 3, 4) \in M$. Součet vektorů $\boldsymbol{u} + \boldsymbol{v} = (5, 5, 7)$ však nepatří do M, neboť v opačném případě bychom z první a třetí složky dostali $x + y = 5$, $2x + y = 7$, odkud $x = 2, y = 3$. Dosazením do druhé složky však máme

$y + 1 = 4 \neq 5$. Podobně máme $2\boldsymbol{u} = (4, 4, 6) \notin M$, neboť v opačném případě by muselo platit $x + y = 4$, $2x + y = 6$, tedy $x = 2, y = 2$ a opět $y + 1 = 3 \neq 4$.

2. Množina prvků

$$W = \{(x + y, y, 2x + y) \mid x, y \in R\} \subseteq R^3$$

je podprostorem v R^3. Skutečně, jsou-li $\boldsymbol{u} = (x_1 + y_1, y_1, 2x_1 + y_1)$ a $\boldsymbol{v} = (x_2 + y_2, y_2, 2x_2 + y_2)$ dva vektory z W, pak pro $x = x_1 + x_2$ a $y = y_1 + y_2$ máme $\boldsymbol{u} + \boldsymbol{v} = (x_1 + y_1 + x_2 + y_2, y_1 + y_2, 2x_1 + y_1 + 2x_2 + y_2) = (x + y, y, 2x + y) \in W$ a pro libovolné $r \in R$, $x = rx_1, y = ry_1$ jest $r\boldsymbol{u} = r(x_1 + y_1, y_1, 2x_1 + y_1) = (x + y, y, 2x + y) \in W$.

3. Množina prvků

$$M = \{(x + 2y, x^2 + y, x - y) \mid x, y \in R\} \subseteq R^3$$

není podprostorem v R^3. Podobně jako v prvním příkladě totiž máme pro $x = y = 1$ a $x = 2, y = 1$ vektory $\boldsymbol{u} = (3, 2, 0) \in M$ a $\boldsymbol{v} = (4, 5, 1) \in M$. Pro $\boldsymbol{u} + \boldsymbol{v} = (7, 7, 1) \in M$ pak musí platit $x + 2y = 7, x - y = 1$, tedy $x = 3, y = 2$ a z druhé složky potom dostáváme $x^2 + y = 11 \neq 7$. Podobně pro $2\boldsymbol{u} = (6, 4, 0)$ je $x + 2y = 6, x - y = 0$, tedy $x = y = 2$, avšak $x^2 + y = 6 \neq 4$.

4. Množina $P_n(T)$ všech polynomů stupně nejvýše n s koeficienty v T je podprostorem vektorového prostoru $P(T)$ z příkladu 8 z odstavce 1.3, neboť součet dvou polynomů stupně nejvýše n je opět polynom stupně nejvýše n, stejně tak jako r-násobek takového polynomu.

5. Množina $\widetilde{P}_n(T)$ všech polynomů z $P(T)$ stupně *právě* n *není* podprostorem v $P(T)$, protože součet dvou takových polynomů může být stupně menšího, např. $(x^2 + 2x - 1) + (-x^2 + 1) = 2x$.

1.8. Věta. *Průnik libovolného neprázdného systému podprostorů vektorového prostoru V je opět podprostorem ve V.*

Důkaz. Buďte W_α, $\alpha \in A$, $A \neq \emptyset$, podprostory ve V. Protože nulový vektor je zřejmě prvkem každého W_α, je průnik $W = \bigcap_{\alpha \in A} W_\alpha$ neprázdný. Jsou-li nyní $\boldsymbol{u}, \boldsymbol{v} \in W$ a $r \in T$ libovolné prvky, je $\boldsymbol{u}, \boldsymbol{v} \in W_\alpha$ pro každé $\alpha \in A$, takže $\boldsymbol{u} + \boldsymbol{v}, r\boldsymbol{u} \in W_\alpha$ pro každé $\alpha \in A$. Tedy $\boldsymbol{u} + \boldsymbol{v}, r\boldsymbol{u} \in W$ a W je podprostor ve V. ∎

1.9. Definice. Buď M podmnožina vektorového prostoru V. Průnik všech podprostorů prostoru V obsahujících množinu M nazýváme *lineárním obalem* množiny M a značíme $\langle M \rangle$. Je-li množina M konečná, $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$, pak místo $\langle \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\} \rangle$ budeme krátce psát $\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n \rangle$.

Vzhledem k větě 1.8 je $\langle M \rangle$ nejmenším podprostorem prostoru V obsahujícím množinu M, avšak sama definice nedává žádnou představu o tom, jak tento podprostor vypadá, tj. ze kterých vektorů z V sestává. Odpověď na tuto otázku dávají následující dva odstavce.

1.10. Definice. Buďte $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n$ vektory z vektorového prostoru V. *Lineární kombinací* vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n$ rozumíme každý vektor

$$\boldsymbol{u} = r_1\boldsymbol{u}_1 + r_2\boldsymbol{u}_2 + \dots + r_n\boldsymbol{u}_n = \sum_{i=1}^{n} r_i\boldsymbol{u}_i ,$$

kde $r_1, r_2, \dots, r_n \in T$. Prvky $r_1, r_2, \dots, r_n$ se nazývají *koeficienty lineární kombinace*. Lineární kombinace se nazývá *triviální*, jsou-li všechny její koeficienty rovny nule, a *netriviální* v opačném případě, tj. je-li alespoň jeden z jejích koeficientů od nuly různý.

1.11. Věta. *Buď M podmnožina vektorového prostoru V. Pak platí:*
(i) je-li $M = \emptyset$, je $\langle M \rangle = 0$;
(ii) je-li $M \neq \emptyset$, pak

$$\langle M \rangle = \{ \sum_{i=1}^{n} r_i \boldsymbol{u}_i \mid \boldsymbol{u}_i \in M, r_i \in T, i = 1, 2, \dots, n \}$$

je množina právě všech lineárních kombinací vektorů z množiny M.

Důkaz. První tvrzení je zcela zřejmé, neboť $\emptyset$ je obsažena v každém podprostoru a 0 je nejmenší podprostor ve V.

Označme tedy symbolem W množinu všech lineárních kombinací vektorů z množiny M. Protože součet dvou lineárních kombinací vektorů z M a násobek takové lineární kombinace prvkem z tělesa T je opět prvkem z W, je W podprostorem ve V. Přitom pro $\boldsymbol{u} \in M$ je $\boldsymbol{u} = 1\boldsymbol{u} \in W$, tedy $M \subseteq W$, W je podprostorem ve V obsahující M a $\langle M \rangle \subseteq W$ podle definice 1.9. Na druhé straně, je-li $W' \subseteq V$ libovolný podprostor obsahující množinu M, plyne snadno z definice 1.6 že W' obsahuje všechny lineární kombinace vektorů z množiny M, tj. $W \subseteq W'$. Podle definice lineárního obalu 1.9 je tedy i $W \subseteq \langle M \rangle$, takže $\langle M \rangle = W$ a jsme hotovi. ■

1.12. Definice. Buďte W a W' dva podprostory vektorového prostoru V. *Spojením podprostorů* W a W' rozumíme nejmenší podprostor obsahující jak W tak W', tj. lineární obal sjednocení $W \cup W'$. Spojení podprostorů budeme označovat symbolem $W \vee W'$. Tedy $W \vee W' = \langle W \cup W' \rangle$.

1.13. Věta. *Buďte W a W' dva podprostory vektorového prostoru V. Pak $W \vee W'$ je množina právě všech vektorů z V tvaru $\boldsymbol{w} + \boldsymbol{w}'$, kde $\boldsymbol{w} \in W$ a $\boldsymbol{w}' \in W'$.*

Důkaz. Podle věty 1.11 je $W \vee W'$ množinou všech lineárních kombinací $\boldsymbol{u} = \sum_{i=1}^{n} r_i \boldsymbol{v}_i$, kde $\boldsymbol{v}_i \in W \cup W'$ pro každé $i = 1, 2, \dots n$. Bez újmy na obecnosti můžeme předpokládat, že vektory $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k$ leží ve W a vektory $\boldsymbol{v}_{k+1}, \dots, \boldsymbol{v}_n$ leží ve W'. Položíme-li $\boldsymbol{w} = \sum_{i=1}^{k} r_i \boldsymbol{v}_i$ a $\boldsymbol{w}' = \sum_{i=k+1}^{n} r_i \boldsymbol{v}_i$, je $\boldsymbol{w} \in W$, $\boldsymbol{w}' \in W'$ a $\boldsymbol{u} = \boldsymbol{w} + \boldsymbol{w}'$, odkud již tvrzení snadno plyne. ■

1.14. Poznámka. Nechť $W_1, W_2, \dots, W_n$ jsou podprostory vektorového V. Podobně jako v definici 1.12 můžeme definovat spojení $W_1 \vee W_2 \vee \cdots \vee W_n = \vee_{i=1}^{n} W_i$ jako lineární obal sjednocení $\cup_{i=1}^{n} W_i$. Podobně jako v předchozí větě pak dostaneme, že $\vee_{i=1}^{n} W_i$ je právě množina všech vektorů tvaru $w = w_1 + w_2 + \cdots + w_n$, kde $w_i \in W_i$, $i = 1, 2, \dots, n$. Skutečně, pro $n = 2$ toto tvrzení platí podle věty 1.13. Je-li $n > 2$ a předpokládáme-li, že pro $n-1$ již tvrzení platí, pak $W = \vee_{i=1}^{n} W_i = (W_1 \vee W_2 \vee \cdots \vee W_{n-1}) \vee W_n$, takže každý prvek $w \in W$ lze podle předchozí věty psát ve tvaru $w' + w_n$, kde $w' \in W_1 \vee W_2 \vee \cdots \vee W_{n-1}$ a $w_n \in W_n$. Podle předpokladu je $w' = w_1 + w_2 + \cdots + w_{n-1}$, $w_i \in W_i$, $i = 1, 2, \dots, n-1$, tedy $w = \sum_{i=1}^{n} w_i$, a tvrzení je úplnou indukcí dokázáno.

2.1. Definice. Buď V vektorový prostor nad tělesem T. Podmnožina $M \subseteq V$ se nazývá *množina generátorů* prostoru V, jestliže $\langle M \rangle = V$. V tomto případě též říkáme, že *M generuje V*.

2.2. Věta. *Buď V vektorový prostor nad T. Podmnožina $M \subseteq V$ generuje V, právě když každý vektor z V je lineární kombinací vektorů z množiny M.*

Důkaz. Plyne ihned z věty 1.11. ∎

2.3. Věta. *Buďte $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n, \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m, \boldsymbol{u}$ prvky vektorového prostoru V. Jestliže každý z vektorů $\boldsymbol{v}_j$, $j = 1, 2, \ldots, m$, je lineární kombinací vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ a je-li $\boldsymbol{u}$ lineární kombinací vektorů $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$, je $\boldsymbol{u}$ lineární kombinací vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$.*

Důkaz. Podle předpokladu je $\boldsymbol{v}_j = \sum_{i=1}^{n} s_{ji}\boldsymbol{u}_i$ pro každé $j = 1, 2, \ldots, m$ a $\boldsymbol{u} = \sum_{j=1}^{m} r_j \boldsymbol{v}_j$. Pak $\boldsymbol{u} = \sum_{j=1}^{m} r_j \sum_{i=1}^{n} s_{ji}\boldsymbol{u}_i = \sum_{i=1}^{n}\sum_{j=1}^{m}(r_j s_{ji})\boldsymbol{u}_i$ a jsme hotovi. ∎

2.4. Důsledek. *Je-li $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m\}$ množina generátorů vektorového prostoru V a je-li každý z vektorů $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$ lineární kombinací vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$, pak $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ je rovněž množina generátorů prostoru V.*

Důkaz. Každý vektor $\boldsymbol{u} \in V$ je podle věty 2.2 lineární kombinací vektorů $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$. Podle předchozí věty je vektor $\boldsymbol{u}$ lineární kombinací vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ a stačí opět použít větu 2.2. ∎

2.5. Definice. Říkáme, že vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$, $n \geq 1$, z vektorového prostoru V jsou *lineárně nezávislé*, jestliže pouze triviální lineární kombinace těchto vektorů je rovna nulovému vektoru. V opačném případě říkáme, že vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ jsou *lineárně závislé*.

2.6. Poznámka. Vzhledem k zásadnímu významu právě zavedených pojmů lineární závislosti a lineární nezávislosti vektorů si tuto definici probereme poněkud podrobněji. Tak tedy lineární nezávislost vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ říká, že pokud pro nějakou lineární kombinaci těchto vektorů platí $\sum_{i=1}^{n} r_i\boldsymbol{u}_i = 0$, pak je tato kombinace *nutně* triviální, tj. $r_1 = r_2 = \cdots = r_n = 0$. Naopak tedy jsou vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ lineárně závislé, pokud existuje jejich lineární kombinace $\sum_{i=1}^{n} r_i\boldsymbol{u}_i = 0$ taková, že *alespoň jeden* z koeficientů $r_1, r_2, \ldots, r_n$ není roven nule. Speciálně, je-li jeden z vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$, např. $\boldsymbol{u}_1$, roven nulovému vektoru, jsou vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ lineárně závislé, neboť platí $1\boldsymbol{u}_1 + 0\boldsymbol{u}_2 + \cdots + 0\boldsymbol{u}_n = 0$. Podobně, pokud jsou mezi vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ dva stejné, např $\boldsymbol{u}_1 = \boldsymbol{u}_2$, jsou vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ opět lineárně závislé, protože jest $1\boldsymbol{u}_1 + (-1)\boldsymbol{u}_2 + 0\boldsymbol{u}_3 + \cdots + 0\boldsymbol{u}_n = 0$. Vidíme tedy, že lineárně nezávislé vektory jsou po dvou různé, takže můžeme mluvit o (neprázdné) lineárně nezávislé množině $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ vektorů z vektorového prostoru V. Na druhé straně si uvědomme, že máme-li jediný vektor $\boldsymbol{u} \in V$, pak vektor $\boldsymbol{u}$ je lineárně nezávislý, právě když $\boldsymbol{u} \neq 0$. Je-li totiž $\boldsymbol{u} \neq 0$, pak z $r\boldsymbol{u} = 0$ pro $r \neq 0$ dostáváme $\boldsymbol{u} = 1\boldsymbol{u} = r^{-1}r\boldsymbol{u} = r^{-1}0 = 0$, což je spor.

2.7. Věta. *Neprázdná podmnožina lineárně nezávislé množiny $\{u_1, u_2, \dots, u_n\} \subseteq V$ vektorů z vektorového prostoru V je opět lineárně nezávislá.*

Důkaz. Buď $\{v_1, v_2, \dots, v_k\}$ neprázdná podmnožina množiny $\{u_1, u_2, \dots, u_n\}$ a buď $\sum_{j=1}^{k} s_j v_j$ libovolná lineární kombinace vektorů $\{v_1, v_2, \dots, v_k\}$ rovná nulovému vektoru. Utvoříme-li lineární kombinaci $\sum_{i=1}^{n} r_i u_i$ tak, že pro $u_i = v_j$ položíme $r_i = s_j$ a pro $u_i \notin \{v_1, v_2, \dots, v_k\}$ položíme $r_i = 0$, pak zřejmě $\sum_{i=1}^{n} r_i u_i = 0$, takže vzhledem k lineární nezávislosti množiny $\{u_1, u_2, \dots, u_n\}$ je $r_i = 0$ pro všechna $i = 1, 2, \dots, n$. Speciálně je tedy $s_1 = s_2 = \dots = s_k = 0$, takže vektory $\{v_1, v_2, \dots, v_k\}$ jsou lineárně nezávislé podle definice 2.5. ■

2.8. Příklady. 1. Ukažme, že vektory $u = (1, 2, 3)$ a $v = (3, 1, 2)$ z R^3 jsou lineárně nezávislé. Uvažujme tedy lineární kombinaci $ru + sv$ a položme ji rovnou nulovému vektoru. Naším cílem je ukázat, že v tomto případě nutně platí $r = s = 0$. Máme tedy $ru + sv = (r + 3s, 2r + s, 3r + 2s) = (0, 0, 0)$, takže $r + 3s = 0$, $2r + s = 0$, $3r + 2s = 0$. Odečteme-li dvojnásobek první rovnice od rovnice druhé, dostaneme $-5s = 0$, tedy nutně $s = 0$ a první (kterákoliv) rovnice dává $r = 0$. Vektory u a v jsou tedy skutečně lineárně nezávislé.

2. Ukažme, že vektory $u = (2, 1, 3)$, $v = (1, 3, 2)$ a $w = (4, 7, 7)$ z R^3 jsou lineárně závislé. Opět utvoříme lineární kombinaci $ru+sv+tw$, položíme ji rovnou nulovému vektoru a budeme chtít tentokrát ukázat, že tuto rovnost je možno získat pomocí ne vesměs nulových koeficientů r, s, t. Máme tedy $ru + sv + tw = (2r + s + 4t, r + 3s+7t, 3r+2s+7t) = (0, 0, 0)$, tudíž $2r+s+4t = 0$, $r+3s+7t = 0$, $3r+2s+7t = 0$. Odečteme-li dvojnásobek druhé rovnice od první a její trojnásobek od rovnice třetí, dostaneme $-5s - 10t = 0$ a $-7s - 14t = 0$. Tyto rovnice lze splnit například volbou $s = 2, t = -1$. Z druhé rovnice pak vychází $r = -3s - 7t = 1$. Dostáváme tedy celkem např. $u + 2v - w = 0$ a vektory u, v, w jsou lineárně závislé.

2.9. Definice. Říkáme, že podmnožina $\{u_1, u_2, \dots, u_n\}$ vektorového prostoru V nebo že vektory $u_1, u_2, \dots, u_n$ tvoří *bázi* tohoto prostoru, jsou-li tyto vektory lineárně nezávislé a zároveň generují V.

2.10. Věta. *Nechť $M = \{u_1, u_2, \dots, u_n\}$ je báze vektorového prostoru V. Pak každý vektor $u \in V$ lze jediným způsobem napsat ve tvaru $u = \sum_{i=1}^{n} r_i u_i$.*

Důkaz. Protože $V = \langle u_1, u_2, \dots, u_n \rangle$, lze každý vektor $u \in V$ vyjádřit jako lineární kombinaci vektorů $u_1, u_2, \dots, u_n$ podle věty 2.2. K důkazu jednoznačnosti uvažme dvě vyjádření vektoru u ve tvaru lineární kombinace vektorů $u_1, u_2, \dots, u_n$, $u = \sum_{i=1}^{n} r_i u_i = \sum_{i=1}^{n} s_i u_i$. Pak ale $\sum_{i=1}^{n} (r_i - s_i) u_i = 0$, takže $r_i - s_i = 0$ a $r_i = s_i$ pro každé $i = 1, 2, \dots, n$ vzhledem k lineární nezávislosti vektorů $u_1, u_2, \dots, u_n$. ■

2.11. Definice. Říkáme, že vektorový prostor V nad T je *konečně generovaný*, nebo že má *konečnou dimenzi*, jestliže ve V existuje konečná množina generátorů.

2.12. Věta. *Z každé množiny generátorů vektorového prostoru $V \neq 0$ konečné dimenze lze vybrat konečnou bázi.*

Důkaz. Podle předpokladu existuje v prostoru V konečná množina generátorů $N = \{v_1, v_2, \dots, v_k\}$. Je-li nyní M libovolná množina generátorů prostoru V, je podle věty 2.2 každý z vektorů $v_1, v_2, \dots, v_k$ lineární kombinací konečného počtu vektorů z množiny M. Odtud je ihned patrné, že existuje konečná podmnožina $M' =$

$\{u_1, u_2, \dots, u_n\}$ množiny M taková, že každý vektor z množiny N je lineární kombinací vektorů z množiny M'. Protože N generuje V, vidíme podle důsledku 2.4, že také M' generuje V. Ukázali jsme zatím, že z každé množiny generátorů prostoru V lze vybrat konečnou podmnožinu, která rovněž generuje V. Zbývá tedy ukázat, že z každé konečné množiny generátorů $M = \{u_1, u_2, \dots, u_n\}$ prostoru V lze vybrat (konečnou) bázi. Mezi všemi podmnožinami množiny M, které generují V, vyberme nějakou podmnožinu K o nejmenším možném počtu prvků, řekněme $K = \{w_1, w_2, \dots, w_l\}$, a ukažme, že K je lineárně nezávislá, tj. že K je báze prostoru V. Předpokládejme tedy naopak existenci netriviální lineární kombinace $\sum_{i=1}^{l} r_i w_i$ rovné nulovému vektoru. Bez újmy na obecnosti (přečíslování vektorů) můžeme předpokládat, že např. $r_l \neq 0$. Pak ale $w_l = -r_l^{-1}(r_1 w_1 + r_2 w_2 + \dots r_{l-1} w_{l-1})$, takže $\{w_1, w_2, \dots, w_{l-1}\}$ generuje V vzhledem k tomu, že K generuje V podle předpokladu. To je však spor s volbou množiny K, speciálně s minimálností počtu jejích prvků. Podmnožina K množiny M je tedy bází prostoru V a jsme hotovi. ■

2.13. Věta (Steinitz). *Buď $\{u_1, u_2, \dots, u_n\}$ množina generátorů vektorového prostoru $V \neq 0$ a buďte vektory $v_1, v_2, \dots, v_k \in V$ lineárně nezávislé. Pak $k \leq n$ a při vhodném očíslování vektorů $u_1, u_2, \dots, u_n$ je množina $\{v_1, v_2, \dots, v_k, u_{k+1}, \dots, u_n\}$ množinou generátorů prostoru V.*

Důkaz. Budeme postupovat úplnou indukcí podle počtu k lineárně nezávislých vektorů. Buď tedy nejprve $k = 1$. Protože $\{u_1, u_2, \dots, u_n\}$ je množina generátorů prostoru V, je vektor v_1 lineární kombinací vektorů $u_1, u_2, \dots, u_n$, $v_1 = \sum_{i=1}^{n} r_i u_i$. Protože vektor v_1 je lineárně nezávislý, je nenulový podle poznámky 2.6, takže alespoň jeden z koeficientů $r_1, r_2, \dots, r_n$ je nenulový. Vhodným očíslováním vektorů $u_1, u_2, \dots, u_n$ lze jistě dosáhnout toho, že $r_1 \neq 0$. Pak však z rovnosti $v_1 = \sum_{i=1}^{n} r_i u_i$ ihned plyne rovnost $u_1 = \frac{1}{r_1} v_1 - \sum_{i=2}^{n} \frac{r_i}{r_1} u_i$. Podle důsledku 2.4 je tedy $\{v_1, u_2, \dots, u_n\}$ množinou generátorů prostoru V a z $r_1 \neq 0$ plyne $1 \leq n$.

Předpokládejme tedy, že $k > 1$ a že pro $k-1$ lineárně nezávislých vektorů tvrzení platí. Z lineární nezávislosti vektorů $v_1, v_2, \dots, v_k$ plyne podle věty 2.7 lineární nezávislost vektorů $v_1, v_2, \dots, v_{k-1}$, takže podle indukčního předpokladu je $k-1 \leq n$ a při vhodném očíslování vektorů $u_1, u_2, \dots, u_n$ je množina $\{v_1, v_2, \dots, v_{k-1}, u_k, \dots, u_n\}$ množinou generátorů prostoru V. Podle věty 2.2 tedy existují prvky $r_1, r_2, \dots, r_{k-1}, s_k, \dots, s_n$ z tělesa T takové, že $v_k = \sum_{i=1}^{k-1} r_i v_i + \sum_{j=k}^{n} s_j u_j$. Uvědomme si nejprve, že alespoň jeden z koeficientů $s_k, \dots, s_n$ je nenulový. V opačném případě bychom totiž měli $v_k - \sum_{i=1}^{k-1} r_i v_i = 0$, což by byl spor s lineární nezávislostí vektorů $v_1, v_2, \dots, v_k$. Vhodným očíslováním vektorů $u_k, u_{k+1}, \dots, u_n$ můžeme dosáhnout toho, že $s_k \neq 0$. Odtud a z rovnosti $v_k = \sum_{i=1}^{k-1} r_i v_i + \sum_{j=k}^{n} s_j u_j$ plyne jednak požadovaná nerovnost $k \leq n$, jedna rovnost $u_k = -\sum_{i=1}^{k-1} \frac{r_i}{s_k} v_i + \frac{1}{s_k} v_k - \sum_{j=k+1}^{n} \frac{s_j}{s_k} u_j$, takže množina $\{v_1, v_2, \dots, v_k, u_{k+1}, \dots, u_n\}$ generuje V podle důsledku 2.4. ■

2.14. Věta. *Každé dvě báze konečně generovaného vektorového prostoru $V \neq 0$ mají týž počet prvků.*

Důkaz. Buďte $M = \{u_1, u_2, \dots, u_n\}$ a $N = \{v_1, v_2, \dots, v_m\}$ dvě báze vektorového prostoru V. Protože množina M je lineárně nezávislá a N generuje V, je $n \leq m$ podle Steinitzovy věty. Z téže věty zároveň plyne, že také naopak je $m \leq n$ vzhledem k tomu, že množina N je lineárně nezávislá a M generuje V. ■

2.15. Definice. Buď $V \neq 0$ vektorový prostor konečné dimenze. *Dimenzí* prostoru V rozumíme počet prvků libovolné jeho báze. Triviálnímu vektorovému prostoru $V = 0$, který nemá žádnou bázi, přiřadíme dimenzi 0. Vektorový prostor dimenze n budeme značit buď V_n, nebo budeme psát $\dim V = n$. Říkáme také, že V_n je *n-rozměrný vektorový prostor.*

2.16. Věta. *Je-li $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ množina generátorů vektorového prostoru V, pak $\dim V \leq n$.*

Důkaz. Z množiny generátorů $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ lze podle věty 2.12 vybrat konečnou bázi prostoru V. ■

2.17. Věta. *Buď $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ množina generátorů vektorového prostoru $V \neq 0$ a buďte $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$ vektory z V. Je-li $k > n$, jsou vektory $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$ lineárně závislé.*

Důkaz. Kdyby vektory $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$ byly lineárně nezávislé, bylo by $k \leq n$ podle Steinitzovy věty. ■

2.18. Poznámka. Podle věty 2.7 je každá neprázdná podmnožina lineárně nezávislé množiny opět lineárně nezávislá. Na druhé straně lineárně nezávislá množina nemůže mít podle předchozí věty více než $\dim V$ prvků. Jinými slovy, lineárně nezávislé množiny jsou co do počtu prvků „malé", zatímco množiny generátorů jsou „velké" vzhledem k tomu, že každá podmnožina ve V obsahující množinu generátorů je zřejmě sama množinou generátorů. V následujícím tvrzení ukážeme, že maximální (co do počtu prvků) lineárně nezávislé množiny ve vektorových prostorech konečné dimenze jsou zároveň množinami generátorů a duálně minimální množiny generátorů jsou lineárně nezávislé.

2.19. Věta. *Buďte $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ vektory z vektorového prostoru $V_n \neq 0$. Pak následující podmínky jsou ekvivalentní:*

(i) vektory $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ jsou lineárně nezávislé;
(ii) vektory $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ generují V_n;
(iii) množina $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n\}$ je bází prostoru V_n.

Důkaz. Stačí ukázat, že z (i) plyne (iii) a z (ii) plyne (iii). Je-li $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ libovolná báze prostoru V_n, pak z (i) plyne (iii), neboť podle Steinitzovy věty 2.13 je $V_n = \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n \rangle = \langle \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n \rangle$ při vhodném očíslování vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$. Jestliže vektory $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ generují V_n, lze z těchto vektorů vybrat podle věty 2.12 bázi. Tato báze musí mít podle věty 2.14 n prvků, takže z (ii) plyne (iii). ■

2.20. Poznámka. Dalším velmi důležitým důsledkem Steinitzovy věty je následující věta, v jejímž důkazu je obsažen fakt, že každou lineárně nezávislou množinu vektorů ve vektorovém prostoru V_n lze doplnit na bázi tohoto prostoru, a to dokonce tak, že za přidané prvky lze vzít vhodné prvky z předem zadané báze.

2.21. Věta. *Buďte $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$ lineárně nezávislé vektory z vektorového prostoru $V_n \neq 0$. Je-li $k = n$, pak množina $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k\}$ je bází vektorového prostoru V_n. Je-li $k < n$, pak ve V_n existuje $n - k$ vektorů, jejichž připojením k množině $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k\}$ vznikne báze prostoru V_n.*

Důkaz. Je-li $k = n$, je množina $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k\}$ bází prostoru V_n podle věty 2.19. Je-li $k < n$ a je-li $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ libovolná báze prostoru V_n, je při vhodném očíslování vektorů $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ množina $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k, \boldsymbol{u}_{k+1}, \dots, \boldsymbol{u}_n\}$ množinou generátorů prostoru V_n podle Steinitzovy věty a opět stačí použít větu 2.19. ∎

2.22. Věta. *Buď W podprostor vektorového prostoru V_n. Pak* $\dim W \le n$, *přičemž rovnost nastane, právě když $W = V_n$.*

Důkaz. Uvědomme si, že z definice lineární nezávislosti 2.5 bezprostředně plyne, že vůbec nezáleží na tom, ve kterém prostoru dané vektory vyšetřujeme, jinými slovy vektory z podprostoru W jsou lineárně nezávislé ve W, právě když jsou lineárně nezávislé ve V_n. To tedy podle věty 2.17 znamená, že každá lineárně nezávislá množina vektorů ve W sestává nejvýše z n prvků. Buď tedy $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k\}$ lineárně nezávislá množina vektorů z W s největším možným počtem prvků k. Je-li nyní $\boldsymbol{v} \in W$ libovolný vektor, jsou vektory $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k, \boldsymbol{v}$ lineárně závislé, takže existuje netriviální lineární kombinace $\sum_{i=1}^{k} r_i \boldsymbol{v}_i + r\boldsymbol{v} = 0$. Pak ale nutně $r \ne 0$, neboť v opačném případě je $\sum_{i=1}^{k} r_i \boldsymbol{v}_i = 0$ a daná lineární kombinace je triviální vzhledem k lineární nezávislosti vektorů $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k$. Pak ale $\boldsymbol{v} = -\sum_{i=1}^{k} \frac{r_i}{r} \boldsymbol{v}_i$, vektor $\boldsymbol{v}$ leží v lineárním obalu množiny $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k\}$, takže $\langle \boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k \rangle = W$ a $\dim W = k \le n$. Je-li $\dim W = k = n$, je $W = V_n$ podle věty 2.21. ∎

2.23. Věta. (O dimenzi spojení a průniku.) *Buďte W a W' dva podprostory vektorového prostoru V_n. Pak platí:*

$$\dim (W \vee W') + \dim (W \cap W') = \dim W + \dim W' .$$

Důkaz. Podprostory W, W', $W \cap W'$ a $W \vee W'$ mají podle předchozí věty konečnou dimenzi. Je-li $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k\}$ báze průniku $W \cap W'$, existují podle věty 2.21 vektory $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_l$ a $\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_m$ takové, že množina $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k, \boldsymbol{v}_1, \dots, \boldsymbol{v}_l\}$ je báze prostoru W a množina $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k, \boldsymbol{w}_1, \dots, \boldsymbol{w}_m\}$ je báze prostoru W'. K dokončení důkazu nyní stačí ověřit, že množina $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k, \boldsymbol{v}_1, \dots, \boldsymbol{v}_l, \boldsymbol{w}_1, \dots, \boldsymbol{w}_m\}$ je báze spojení $W \vee W'$, neboť v tomto případě máme $\dim (W \vee W') = k+l+m$, $\dim (W \cap W') = k$, $\dim W = k+l$ a $\dim W' = k+m$. Vzhledem k tomu, že z vět 1.13 a 2.2 ihned plyne, že množina $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k, \boldsymbol{v}_1, \dots, \boldsymbol{v}_l, \boldsymbol{w}_1, \dots, \boldsymbol{w}_m\}$ generuje podprostor $W \vee W'$, stačí ověřit, že tato množina je lineárně nezávislá. Nechť tedy $\sum_{i=1}^{k} r_i \boldsymbol{u}_i + \sum_{j=1}^{l} s_j \boldsymbol{v}_j + \sum_{r=1}^{m} t_r \boldsymbol{w}_r = 0$. Pak ale z $\sum_{i=1}^{k} r_i \boldsymbol{u}_i + \sum_{j=1}^{l} s_j \boldsymbol{v}_j = -\sum_{r=1}^{m} t_r \boldsymbol{w}_r \in W \cap W'$ plyne $\sum_{r=1}^{m} t_r \boldsymbol{w}_r = \sum_{i=1}^{k} \alpha_i \boldsymbol{u}_i$, a tedy $t_1 = t_2 = \dots = t_m = 0$ vzhledem k lineární nezávislosti vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k, \boldsymbol{w}_1, \dots, \boldsymbol{w}_m$. Pak ale z lineární nezávislosti vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k, \boldsymbol{v}_1, \dots, \boldsymbol{v}_l$ a z rovnosti $\sum_{i=1}^{k} r_i \boldsymbol{u}_i + \sum_{j=1}^{l} s_j \boldsymbol{v}_j = 0$ dostáváme $r_1 = r_2 = \dots = r_k = s_1 = s_2 = \dots = s_l = 0$ a jsme hotovi. ∎

2.24. Poznámka. Buď n přirozené číslo. Pro každé $i \in \{1, 2, \dots, n\}$ označme $\boldsymbol{e}_i \in T^n$ aritmetický vektor mající na i-tém místě prvek 1 a na všech ostatních místech prvek 0. Je zřejmé, že libovolný vektor $\boldsymbol{u} = (r_1, r_2, \dots, r_n)$ je lineární kombinací vektorů $\boldsymbol{e}_1, \boldsymbol{e}_2, \dots, \boldsymbol{e}_n$, $\boldsymbol{u} = \sum_{i=1}^{n} r_i \boldsymbol{e}_i$. Na druhé straně, je-li $\sum_{i=1}^{n} r_i \boldsymbol{e}_i = (r_1, r_2, \dots, r_n) = 0$, je $r_1 = r_2 = \dots, r_n = 0$. Vidíme tedy, že množina $K =$

$\{e_1, e_2, \ldots, e_n\}$ je bází aritmetického vektorového prostoru T^n. Tato báze se obvykle nazývá *kanonická báze* prostoru T^n.

Je-li V vektorový prostor nad tělesem T, pak množina V^n všech uspořádaných n-tic vektorů z V je vektorovým prostorem vzhledem k přirozeným operacím sčítání vektorů a násobení prvky z tělesa T po složkách. Pro $M = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$, $M' = (\boldsymbol{v}'_1, \boldsymbol{v}'_2, \ldots, \boldsymbol{v}'_n)$ z V^n a $r \in T$ stačí totiž definovat $M + M' = (\boldsymbol{v}_1 + \boldsymbol{v}'_1, \boldsymbol{v}_2 + \boldsymbol{v}'_2, \ldots, \boldsymbol{v}_n + \boldsymbol{v}'_n)$ a $rM = (r\boldsymbol{v}_1, r\boldsymbol{v}_2, \ldots, r\boldsymbol{v}_n)$. Bez obav z nedorozumění můžeme symbolem $\langle M \rangle$ označit lineární obal množiny tvořené vektory $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$.

V odstavci 1.10 jsme definovali lineární kombinaci $\boldsymbol{v}$ vektorů $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n \in V$ s koeficienty $r_1, r_2, \ldots, r_n \in T$ předpisem $\boldsymbol{v} = \sum_{i=1}^n r_i \boldsymbol{v}_i$. Až doposud jsme při zkoumání vlastností vektorových prostorů vycházeli z pevně dané n-tice vektorů $M \in V^n$, zatímco n-tice koeficientů $\boldsymbol{u} = (r_1, r_2, \ldots, r_n) \in T^n$ byly v podstatě libovolné. Podíváme se nyní na tento pojem podrobněji a z poněkud jiného hlediska. Lineární kombinace je vlastně vektor $\boldsymbol{v} \in V$ přiřazený dvojici $(\boldsymbol{u}, M)$, kde $\boldsymbol{u} = (r_1, r_2, \ldots, r_n) \in T^n$ a $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n) \in V^n$, takže se vlastně jedná o zobrazení, které každému vektoru z T^n a každému vektoru $M \in V^n$ (uspořádané n-tici prvků z V) přiřazuje vektor z prostoru V, totiž lineární kombinaci s koeficienty $\boldsymbol{u}$. Máme tedy $\boldsymbol{v} = \sum_{i=1}^n r_i \boldsymbol{v}_i = (r_1, r_2, \ldots, r_n) * (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n) = \boldsymbol{u} * M$, kde $*$ představuje zobrazení $* : T^n \times V^n \to V$. Tomuto zobrazení budeme pro zjednodušení říkat *smíšený součin*. I když je tento termín poněkud nepřesný, neboť nebere v úvahu číslo n, nebudeme jej dále komplikovat, protože z kontextu bude vždy jednoznačně patrné, o které n se jedná. Pro libovolnou podmnožinu $N \subseteq T^n$ definujme ještě smíšený součin $N * M = \{\boldsymbol{u} * M \mid \boldsymbol{u} \in N\}$ a podívejme se nyní na některé základní a jednoduché vlastnosti smíšeného součinu, které však pro nás budou mít zásadní důležitost, jak uvidíme v následujících odstavcích.

2.25. Věta. *Buďte $r \in T$, $\boldsymbol{u}, \boldsymbol{u}' \in T^n$, $N \subseteq T^n$ a $M = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n), M' = (\boldsymbol{v}'_1, \boldsymbol{v}'_2, \ldots, \boldsymbol{v}'_n) \in V^n$. Pak platí*

(i) $(\boldsymbol{u} + \boldsymbol{u}') * M = \boldsymbol{u} * M + \boldsymbol{u}' * M$;

(ii) $\boldsymbol{u} * (M + M') = \boldsymbol{u} * M + \boldsymbol{u} * M'$;

(iii) $r\boldsymbol{u} * M = \boldsymbol{u} * rM = r(\boldsymbol{u} * M)$;

(iv) $\langle N \rangle * M = \langle N * M \rangle =\subseteq \langle M \rangle$;

(v) $T^n * M = \{\boldsymbol{u} * M \mid \boldsymbol{u} \in T^n\} = \langle \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n \rangle$;

(vi) jsou-li vektory $\boldsymbol{u}_1 * M, \boldsymbol{u}_2 * M, \ldots, \boldsymbol{u}_k * M \in V$ lineárně nezávislé, jsou lineárně nezávislé i vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \in T^n$. Jsou-li navíc lineárně nezávislé vektory $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n \in V$, pak z lineární nezávislosti vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \in T^n$ plyne lineární nezávislost vektorů $\boldsymbol{u}_1 * M, \boldsymbol{u}_2 * M, \ldots, \boldsymbol{u}_k * M$.

(vii) označíme-li $\mathrm{Ker}(M) = \{\boldsymbol{u} \in T^n \mid \boldsymbol{u} * M = 0\}$, *pak* $\mathrm{Ker}(M) \leq T^n$ *a* $\dim \mathrm{Ker}(M) + \dim\langle M \rangle = n$.

Důkaz. Tvrzení (i)–(iii) a (v) se ověří velmi snadno, a lze je tudíž přenechat čtenáři jako cvičení.

(iv) Je-li $\boldsymbol{u} \in \langle N \rangle$, pak $\boldsymbol{u} = \sum_{i=1}^k r_i \boldsymbol{u}_i$, $\boldsymbol{u}_i \in N, r_i \in T$, $i = 1, 2, \ldots, k$, takže podle (i) a (iii) je $\boldsymbol{u} * M = (\sum_{i=1}^k r_i \boldsymbol{u}_i) * M = \sum_{i=1}^k r_i(\boldsymbol{u}_i * M) \in \langle N * M \rangle$. Naopak, je-li $\sum_{i=1}^k r_i(\boldsymbol{u}_i * M) \in \langle N * M \rangle$ libovolný prvek, pak $\sum_{i=1}^k r_i(\boldsymbol{u}_i * M) = (\sum_{i=1}^k r_i \boldsymbol{u}_i) * M \in \langle N \rangle * M$, odkud požadovaná rovnost ihned plyne. Zbytek tvrzení je zřejmý.

(vi) Jsou-li $\boldsymbol{u}_1 * M, \boldsymbol{u}_2 * M, \dots, \boldsymbol{u}_k * M$ lineárně nezávislé, pak z $\sum_{i=1}^k r_i \boldsymbol{u}_i = 0$ dostáváme $\sum_{i=1}^k r_i(\boldsymbol{u}_i * M) = (\sum_{i=1}^k r_i \boldsymbol{u}_i) * M = 0$, tedy $r_1 = r_2 = \dots = r_k = 0$ a vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k$ jsou lineárně nezávislé. Předpokládejme naopak, že vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k$ jsou lineárně nezávislé, a nechť $\sum_{i=1}^k r_i(\boldsymbol{u}_i * M) = 0$. Označíme-li $\boldsymbol{u} = \sum_{i=1}^k r_i \boldsymbol{u}_i$, pak podle (i) a (iii) máme $\sum_{i=1}^k r_i(\boldsymbol{u}_i * M) = (\sum_{i=1}^k r_i \boldsymbol{u}_i) * M = \boldsymbol{u} * M = 0$, takže $\boldsymbol{u} = 0$ vzhledem k lineární nezávislosti vektorů $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n$. Z lineární nezávislosti vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k$ pak dostáváme $r_i = 0$ pro každé $i = 1, 2, \dots, k$ a vektory $\boldsymbol{u}_1 * M, \boldsymbol{u}_2 * M, \dots, \boldsymbol{u}_k * M$ jsou lineárně nezávislé.

(vii) Označíme-li $k = \dim\langle M \rangle$, můžeme bez újmy na obecnosti předpokládat, že vektory $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k$ tvoří bázi $\langle M \rangle$. Pak $\boldsymbol{v}_j = \sum_{i=1}^k r_{ji} \boldsymbol{v}_i$ pro vhodné prvky $r_{ji} \in T$, $i = 1, 2, \dots, k$, $j = k+1, \dots, n$. Jestliže pro každé $j = k+1, \dots, n$ položíme $\boldsymbol{u}_j = (r_{j1}, r_{j2}, \dots, r_{jk}, 0, \dots, 0, -1, 0 \dots, 0)$ s prvkem -1 na j-tém místě, jsou vektory $\boldsymbol{u}_{k+1}, \dots, \boldsymbol{u}_n$ zřejmě lineárně nezávislé a leží v $\mathrm{Ker}(M)$. K dokončení důkazu tedy stačí ověřit, že vektory $\boldsymbol{u}_{k+1}, \dots, \boldsymbol{u}_n$ generují $\mathrm{Ker}(M)$. Je-li $\boldsymbol{u} = (r_1, r_2, \dots, r_n) \in \mathrm{Ker}(M)$ libovolný prvek, je $0 = \sum_{i=1}^n r_i \boldsymbol{v}_i = \sum_{i=1}^k r_i \boldsymbol{v}_i + \sum_{j=k+1}^n r_j \boldsymbol{v}_j = \sum_{i=1}^k r_i \boldsymbol{v}_i + \sum_{j=k+1}^n r_j \sum_{i=1}^k r_{ji} \boldsymbol{v}_i = \sum_{i=1}^k (r_i + \sum_{j=k+1}^n r_j r_{ji}) \boldsymbol{v}_i$, takže $r_i + \sum_{j=k+1}^n r_j r_{ji} = 0$ pro každé $i = 1, 2, \dots, k$, vzhledem k lineární nezávislosti vektorů $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k$. Pak ale $\sum_{j=k+1}^n (-r_j) \boldsymbol{u}_j = \sum_{j=k+1}^n (-r_j r_{j1}, -r_j r_{j2}, \dots, -r_j r_{jk}, 0 \dots, 0, r_j, 0, \dots, 0) = (r_1, r_2, \dots, r_k, r_{k+1}, \dots, r_n) = \boldsymbol{u}$ a jsme hotovi. ■

2.26. Důsledek. *Buď $M = (\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n)$ uspořádaná n-tice vektorů aritmetického vektorového prostoru T^n taková, že vektory $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n$ jsou lineárně nezávislé. Pak existují lineárně nezávislé vektory $\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n \in T^n$ takové, že $\boldsymbol{b}_i * M = \boldsymbol{e}_i$, $i = 1, 2, \dots, n$.*

Důkaz. Existence plyne z tvrzení (v) a věty 2.19, lineární nezávislost z tvrzení (vi). ■

2.27. Definice. Nechť $W_1, W_2, \dots, W_n$ jsou podprostory vektorového prostoru V. Řekneme, že V je *direktním součtem* podprostorů $W_1, W_2, \dots, W_n$, $W = W_1 \oplus W_2 \oplus \dots \oplus W_n = \oplus_{i=1}^n W_i$, jestliže $V = \vee_{i=1}^n W_i$ a $W_i \cap (\vee_{j \neq i} W_j) = 0$ pro každé $i = 1, 2, \dots, n$.

2.28. Věta. *Vektorový prostor V je direktním součtem svých podprostorů $W_1, W_2, \dots, W_n$, právě když každý vektor $\boldsymbol{v} \in V$ lze jediným způsobem zapsat ve tvaru $\boldsymbol{v} = \boldsymbol{w}_1 + \boldsymbol{w}_2 + \dots + \boldsymbol{w}_n$, $\boldsymbol{w}_i \in W_i$, $i = 1, 2, \dots, n$.*

Důkaz. Jestliže $V = \oplus_{i=1}^n W_i$, lze každý vektor $\boldsymbol{v} \in V$ zapsat ve tvaru $\boldsymbol{v} = \sum_{i=1}^n \boldsymbol{w}_i$, $\boldsymbol{w}_i \in W_i$, $i = 1, 2, \dots, n$, alespoň jedním způsobem podle poznámky 1.14. Je-li $\boldsymbol{v} = \sum_{i=1} \boldsymbol{w}'_i$, $\boldsymbol{w}'_i \in W_i$, jiné vyjádření prvku $\boldsymbol{v}$ v požadovaném tvaru, pak porovnáním obou součtů dostaneme pro každé $i \in \{1, 2, \dots, n\}$ rovnost $\boldsymbol{w}_i - \boldsymbol{w}'_i = (\boldsymbol{w}'_1 - \boldsymbol{w}_1) + \dots + (\boldsymbol{w}'_{i-1} - \boldsymbol{w}_{i-1}) + (\boldsymbol{w}'_{i+1} - \boldsymbol{w}_{i+1}) + \dots + (\boldsymbol{w}'_n - \boldsymbol{w}_n) \in W_i \cap (\vee_{j \neq i} W_j) = 0$, odkud plyne, že $\boldsymbol{w}_i = \boldsymbol{w}'_i$, $i = 1, 2, \dots, n$, a jednoznačnost je dokázána.

Naopak, je-li podmínka věty splněna, je $V = \vee_{i=1}^n W_i$ podle poznámky 1.14. Je-li dále $\boldsymbol{v} \in W_i \cap (\vee_{j \neq i} W_j)$, $i \in \{1, 2, \dots, n\}$, libovolný vektor, můžeme s přihlédnutím k poznámce 1.14 vektor $\boldsymbol{v}$ zapsat ve tvaru $\boldsymbol{v} = \boldsymbol{w}_1 + \dots + \boldsymbol{w}_{i-1} + \boldsymbol{w}_{i+1} + \dots + \boldsymbol{w}_n$, kde $\boldsymbol{w}_j \in W_j$, $j \in \{1, \dots, i-1, i+1, \dots n\}$. Pak ale $\boldsymbol{w}_1 + \dots + \boldsymbol{w}_{i-1} - \boldsymbol{v} + \boldsymbol{w}_{i+1} + \dots + \boldsymbol{w}_n = 0$, odkud vzhledem k předpokladu jednoznačnosti zápisu plyne $\boldsymbol{w}_1 = \dots = \boldsymbol{w}_{i-1} = \boldsymbol{v} = \boldsymbol{w}_{i+1} = \dots = \boldsymbol{w}_n = 0$ a jsme hotovi. ■

2.29. Věta. *Nechť vektorový prostor V_m je direktním součtem svých podprostorů $W_1, W_2, \ldots, W_n$, $V_m = \oplus_{i=1}^n W_i$. Je-li M_i báze podprostoru W_i, $i = 1, 2, \ldots, n$, pak množina $M = \cup_{i=1}^n M_i$ je báze prostoru V_m.*

Důkaz. Podle předchozí věty lze každý vektor $\boldsymbol{v} \in V_m$ zapsat ve tvaru $\boldsymbol{v} = \boldsymbol{w}_1 + \boldsymbol{w}_2 + \cdots + \boldsymbol{w}_n$, $\boldsymbol{w}_i \in W_i, i = 1, 2, \ldots, n$. Protože množina M_i generuje podle předpokladu podprostor W_i, je každé $\boldsymbol{w}_i$ lineární kombinací vektorů z M_i, odkud je patrné, že každý vektor $\boldsymbol{v} \in V_m$ je lineární kombinací vektorů z množiny $M = \cup_{i=1}^n M_i$, a množina M tedy generuje prostor V_m. K dokončení důkazu zbývá ukázat lineární nezávislost množiny M. Nechť tedy $M_i = \{\boldsymbol{u}_{ij} \,|\, j \in J_i\}$ pro vhodnou konečnou množinu J_i a každé $i = 1, 2, \ldots, n$. Je-li nyní $\sum_{i=1}^n \sum_{j \in J_i} r_{ij} \boldsymbol{u}_{ij} = 0$, pak pro libovolné $i \in \{1, 2, \ldots, n\}$ je $\sum_{j \in J_i} r_{ij} \boldsymbol{u}_{ij} = -\sum_{k \neq i} \sum_{j \in J_k} r_{kj} \boldsymbol{u}_{kj}$ a tento vektor zřejmě leží v průniku $W_i \cap (\vee_{k \neq i} W_k) = 0$. Tedy $\sum_{j \in J_i} r_{ij} \boldsymbol{u}_{ij} = 0$, takže $r_{ij} = 0$ pro každé $j \in J_i$ vzhledem k tomu, že M_i je báze podprostoru W_i. Protože toto platí pro každé $i = 1, 2, \ldots, n$, je množina M lineárně nezávislá a věta je dokázána. ∎

3. Elementární transformace

Množiny, zejména množiny konečné, bývají často zadány výčtem svých prvků. Přitom se automaticky předpokládá, že každý prvek je zapsán pouze jednou. Vzhledem k tomu, že v dalším textu budeme pracovat často s výčtem vektorů, z nichž některé se mohou opakovat, zavedeme si pojem skupiny vektorů. Skupina vektorů $[\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n]$ bude tedy znamenat prostě vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n$, z nichž se některé mohou, ale nemusí rovnat. Máme-li třeba množinu vektorů $\{\boldsymbol{u}, \boldsymbol{v}\} \subseteq V$, můžeme z této množiny utvořit např. skupiny $[\boldsymbol{u}, \boldsymbol{v}]$, $[\boldsymbol{u}, \boldsymbol{u}, \boldsymbol{v}]$, $[\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{v}, \boldsymbol{v}, \boldsymbol{u}]$, $[\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{u}, \boldsymbol{v}, \boldsymbol{v}, \boldsymbol{u}]$ apod.

3.1. Definice. Buďte $M = [\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n]$ a $M' = [\boldsymbol{u}'_1, \boldsymbol{u}'_2, \dots, \boldsymbol{u}'_n]$ dvě skupiny vektorů vektorového prostoru V. Řekneme, že skupina M' vznikla ze skupiny M *elementární transformací*, jestliže existuje index $i \in \{1, 2, \dots, n\}$ tak, že

$$\boldsymbol{u}'_j = \boldsymbol{u}_j \qquad \text{pro všechna } j \neq i, \quad j = 1, 2, \dots, n,$$

a buďto

$$\boldsymbol{u}'_i = \boldsymbol{u}_i + \sum_{\substack{i=1 \\ i \neq j}}^{n} r_j \boldsymbol{u}_j, \qquad r_j \in T,$$

nebo

$$\boldsymbol{u}'_i = r\boldsymbol{u}_i, \qquad 0 \neq r \in T.$$

Řekneme dále, že skupina M' vznikla z M *konečným počtem elementárních transformací*, jestliže existují skupiny

$$M = M_0, M_1, \dots, M_k = M'$$

takové, že skupina M_{j+1} vznikla z M_j elementární trasformací pro každé $j = 0, 1, \dots, k-1$.

3.2. Věta. *Buďte M a M' dvě skupiny vektorů vektorového prostoru V. Jestliže M' vznikne z M konečným počtem elementárních transformací, pak také M vznikne z M' konečným počtem elementárních transformací.*

Důkaz. Je zřejmé, že se stačí omezit na případ, kdy M' vznikne z M jedinou elementární transformací. Buď tedy $M = [\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n]$, $M' = [\boldsymbol{u}'_1, \boldsymbol{u}'_2, \dots, \boldsymbol{u}'_n]$ a nechť existuje index $i = 1, 2, \dots, n$ takový, že $\boldsymbol{u}'_j = \boldsymbol{u}_j$ pro všechna $j \neq i$. Jestliže $\boldsymbol{u}'_i = \boldsymbol{u}_i + \sum_{\substack{i=1 \\ i \neq j}}^{n} r_j \boldsymbol{u}_j$, pak $\boldsymbol{u}_i = \boldsymbol{u}'_i - \sum_{\substack{i=1 \\ i \neq j}}^{n} r_j \boldsymbol{u}'_j$, a jestliže $\boldsymbol{u}'_i = r\boldsymbol{u}_i$, $r \neq 0$, pak $\boldsymbol{u}_i = \frac{1}{r}\boldsymbol{u}'_i$. ■

3.3. Věta. *Nechť $M = [\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n]$ je skupina vektorů vektorového prostoru V. Vyměníme-li navzájem vektory $\boldsymbol{u}_i$ a $\boldsymbol{u}_j$, dostaneme skupinu vektorů, která vznikne z M konečným počtem elementárních transformací.*

Důkaz. Bez újmy na obecnosti můžeme předpokládat, že $i < j$. Pak v následujících skupinách vznikne vždy každá skupina z předchozí skupiny elementární transformací: M, $[\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i+\boldsymbol{u}_j, \boldsymbol{u}_{i+1}, \ldots, \boldsymbol{u}_j, \ldots, \boldsymbol{u}_n]$, $[\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i+\boldsymbol{u}_j, \boldsymbol{u}_{i+1}, \ldots, -\boldsymbol{u}_i, \ldots, \boldsymbol{u}_n]$, $[\boldsymbol{u}_1, \ldots, \boldsymbol{u}_j, \boldsymbol{u}_{i+1}, \ldots, -\boldsymbol{u}_i, \ldots, \boldsymbol{u}_n]$, $[\boldsymbol{u}_1, \ldots, \boldsymbol{u}_j, \ldots, \boldsymbol{u}_{i+1}, \ldots, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_n]$. ■

3.4. Věta. *Buďte M a M' dvě skupiny vektorů vektorového prostoru V. Jestliže M' vznikne z M konečným počtem elementárních transformací pak $\langle M \rangle = \langle M' \rangle$.*

Důkaz. Z definice 3.1 je zřejmé, že se stačí omezit na případ, kdy M' vznikne z M jednou elementární transformací. Nechť tedy $M = [\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n]$, $M' = [\boldsymbol{u}'_1, \boldsymbol{u}'_2, \ldots, \boldsymbol{u}'_n]$ a nechť existuje index $i = 1, 2, \ldots, n$ takový, že $\boldsymbol{u}'_j = \boldsymbol{u}_j$ pro všechna $j \neq i$. Jestliže $\boldsymbol{u}'_i = \boldsymbol{u}_i + \sum\limits_{\substack{i=1\\ i\neq j}}^{n} r_j \boldsymbol{u}_j$, pak $\boldsymbol{u}_i = \boldsymbol{u}'_i - \sum\limits_{\substack{i=1\\ i\neq j}}^{n} r_j \boldsymbol{u}'_j$, takže $\langle M \rangle = \langle M' \rangle$ podle věty 2.3. Jestliže $\boldsymbol{u}'_i = r\boldsymbol{u}_i$, $r \neq 0$, pak $\boldsymbol{u}_i = \frac{1}{r}\boldsymbol{u}'_i$ a opět $\langle M \rangle = \langle M' \rangle$. ■

3.5. Věta. *Buďte $M = [\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n]$ a $M' = [\boldsymbol{u}'_1, \boldsymbol{u}'_2, \ldots, \boldsymbol{u}'_n]$ dvě skupiny vektorů vektorového prostoru V a nechť M' vznikne z M konečným počtem elementárních transformací. Pak vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ jsou lineárně nezávislé, právě když vektory $\boldsymbol{u}'_1, \boldsymbol{u}'_2, \ldots, \boldsymbol{u}'_n$ jsou lineárně nezávislé.*

Důkaz. Jsou-li vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ lineárně nezávislé, je $\dim \langle M \rangle = n$, takže podle předchozí věty je $\dim \langle M' \rangle = n$ a vektory $\boldsymbol{u}'_1, \boldsymbol{u}'_2, \ldots, \boldsymbol{u}'_n$ jsou lineárně nezávislé podle věty 2.19. K důkazu obráceného tvrzení stačí použít větu 3.2 a to, co bylo právě dokázáno. ■

3.6. Věta. *Buďte $k_1 < k_2 < \cdots < k_m \leq n$ přirozená čísla a buďte $\boldsymbol{u}_i = (a_{i1}, a_{i2}, \ldots, a_{in})$, $i = 1, 2, \ldots, m$, vektory z T^n takové, že $a_{ij} = 0$ pro $j < k_i$, $a_{ik_i} \neq 0$, $i = 1, 2, \ldots, m$. Pak vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m$ jsou lineárně nezávislé.*

Důkaz. Nechť $\sum_{i=1}^m r_i \boldsymbol{u}_i = (a_1, a_2, \ldots, a_n)$. Podle předpokladu je $a_{k_1} = r_1 a_{1k_1}$, $a_{k_2} = r_1 a_{1k_2} + r_2 a_{2k_2}, \ldots, a_{k_m} = r_1 a_{1k_m} + r_2 a_{2k_m} + \cdots + r_m a_{mk_m}$. Jestliže $\sum_{i=1}^m r_i \boldsymbol{u}_i = 0$, pak z $a_{1k_1} \neq 0$ plyne $r_1 = 0$, takže z $a_{k_2} \neq 0$ plyne $r_2 = 0$ atd., až konečně z $a_{k_m} \neq 0$ plyne $r_m = 0$. ■

3.7. Důsledek. *Buďte $\boldsymbol{u}_i = (a_{i1}, a_{i2}, \ldots a_{in})$, $i = 1, 2, \ldots, m$, $m \leq n$, vektory z T^n takové, že $a_{ij} = 0$ pro $j < i$ a $a_{jj} \neq 0$, $j = 1, 2, \ldots, m$. Pak vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m$ jsou lineárně nezávislé.*

Důkaz. V předchozí větě stačí položit $k_i = i$, $i = 1, 2, \ldots, m$. ■

3.8. Příklady. 1. Určeme dimenzi podprostoru $V = \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4, \boldsymbol{u}_5 \rangle$ aritmetického vektorového prostoru R^5, jestliže $\boldsymbol{u}_1 = (1, 1, 1, 1, 0)$, $\boldsymbol{u}_2 = (1, -1, -1, 0, 0)$, $\boldsymbol{u}_3 = (1, 1, -1, -1, -1)$, $\boldsymbol{u}_4 = (2, 2, 0, 0, -1)$, $\boldsymbol{u}_5 = (1, 1, 5, 5, 2)$.

Ř e š e n í: Jednotlivé vektory napíšeme (obecně v libovolném pořadí) do tzv. matice (viz následující kapitola), provedení jedné či více elementárních transformací označíme vlnovkou mezi maticemi. Jest

$$\begin{pmatrix} 1, & 1, & 1, & 1, & 0 \\ 1, & -1, & -1, & 0, & 0 \\ 1, & 1, & -1, & -1, & -1 \\ 2, & 2, & 0, & 0, & -1 \\ 1, & 1, & 5, & 5, & 2 \end{pmatrix} \sim \begin{pmatrix} 1, & 1, & 1, & 1, & 0 \\ 0, & -2, & -2, & -1, & 0 \\ 1, & 1, & -1, & -1, & -1 \\ 2, & 2, & 0, & 0, & -1 \\ 1, & 1, & 5, & 5, & 2 \end{pmatrix} \sim \begin{pmatrix} 1, & 1, & 1, & 1, & 0 \\ 0, & -2, & -2, & -1, & 0 \\ 0, & 0, & -2, & -2, & -1 \\ 2, & 2, & 0, & 0, & -1 \\ 1, & 1, & 5, & 5, & 2 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1, & 1, & 1, & 1, & 0 \\ 0, & -2, & -2, & -1, & 0 \\ 0, & 0, & -2, & -2, & -1 \\ 0, & 0, & -2, & -2, & -1 \\ 1, & 1, & 5, & 5, & 2 \end{pmatrix} \sim \begin{pmatrix} 1, & 1, & 1, & 1, & 0 \\ 0, & -2, & -2, & -1, & 0 \\ 0, & 0, & -2, & -2, & -1 \\ 0, & 0, & -2, & -2, & -1 \\ 0, & 0, & 4, & 4, & 2 \end{pmatrix} \sim \begin{pmatrix} 1, & 1, & 1, & 1, & 0 \\ 0, & -2, & -2, & -1, & 0 \\ 0, & 0, & -2, & -2, & -1 \\ 0, & 0, & 0, & 0, & 0 \\ 0, & 0, & 0, & 0, & 0 \end{pmatrix},$$

takže $\dim V = 3$ podle předchozího důsledku. Je patrné, že první čtyři elementární transformace jsme mohli udělat najednou a zkrátit tak celý postup. V dalším textu budeme proto provádět v každém kroku zpravidla několik elementárních transformací najednou.

2. Zjistěme dimenzi průniku $W \cap W' \subseteq R^4$, jestliže $W = \langle (3,1,5,4),(2,2,3,3) \rangle$ a $W' = \langle (1,-1,2,1),(4,3,7,7),(3,4,5,6) \rangle$.

Ř e š e n í: Předně máme

$$\begin{pmatrix} 3, & 1, & 5, & 4 \\ 2, & 2, & 3, & 3 \end{pmatrix} \sim \begin{pmatrix} 1, & -1, & 2, & 1 \\ 2, & 2, & 3, & 3 \end{pmatrix} \sim \begin{pmatrix} 1, & -1, & 2, & 1 \\ 0, & 4, & -1, & 1 \end{pmatrix}$$

a

$$\begin{pmatrix} 1, & -1, & 2, & 1 \\ 4, & 3, & 7, & 7 \\ 3, & 4, & 5, & 6 \end{pmatrix} \sim \begin{pmatrix} 1, & -1, & 2, & 1 \\ 0, & 7, & -1, & 3 \\ 0, & 7, & -1, & 3 \end{pmatrix} \sim \begin{pmatrix} 1, & -1, & 2, & 1 \\ 0, & 7, & -1, & 3 \\ 0, & 0, & 0, & 0 \end{pmatrix},$$

takže $\dim W = \dim W' = 2$. Dále podle vět 3.4 a 1.13 vektory $(1,-1,2,1)$, $(0,4,-1,1)$, $(1,-1,2,1)$, $(0,7,-1,3)$ generují $W \vee W'$. Přitom

$$\begin{pmatrix} 1, & -1, & 2, & 1 \\ 0, & 4, & -1, & 1 \\ 1, & -1, & 2, & 1 \\ 0, & 7, & -1, & 3 \end{pmatrix} \sim \begin{pmatrix} 1, & -1, & 2, & 1 \\ 0, & 4, & -1, & 1 \\ 0, & 0, & 0, & 0 \\ 0, & 7, & -1, & 3 \end{pmatrix} \sim \begin{pmatrix} 1, & -1, & 2, & 1 \\ 0, & 4, & -1, & 1 \\ 0, & 0, & 3, & 5 \\ 0, & 0, & 0, & 0 \end{pmatrix},$$

takže $\dim(W \vee W') = 3$. Podle věty o dimenzi spojení a průniku 2.23 je $\dim(W \cap W') = 1$.

V tomto odstavci zavedeme pojem matice nad tělesem, budeme definovat základní algebraické operace s maticemi a budeme zkoumat jejich nejdůležitější vlastnosti.

4.1. Definice. Soubor

$$A = (a_{ij}) = \begin{pmatrix} a_{11}, & a_{12}, & \dots, & a_{1n} \\ a_{21}, & a_{22}, & \dots, & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1}, & a_{m2}, & \dots, & a_{mn} \end{pmatrix}$$

prvků z tělesa T nazýváme *maticí typu* (m, n) (nad tělesem T). Aritmetický vektor $(a_{i1}, a_{i2}, \dots, a_{in})$ z T^n nazýváme *i-tým řádkem* matice A a aritmetický vektor $(a_{1j}, a_{2j}, \dots, a_{mj})$ z T^m nazýváme *j-tým sloupcem* matice A.

Součtem dvou matic

$$A = \begin{pmatrix} a_{11}, & a_{12}, & \dots, & a_{1n} \\ a_{21}, & a_{22}, & \dots, & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1}, & a_{m2}, & \dots, & a_{mn} \end{pmatrix} \quad \text{a} \quad B = \begin{pmatrix} b_{11}, & b_{12}, & \dots, & b_{1n} \\ b_{21}, & b_{22}, & \dots, & b_{2n} \\ \dots & \dots & \dots & \dots \\ b_{m1}, & b_{m2}, & \dots, & b_{mn} \end{pmatrix}$$

téhož typu (m, n) rozumíme matici

$$A + B = \begin{pmatrix} a_{11} + b_{11}, & a_{12} + b_{12}, & \dots, & a_{1n} + b_{1n} \\ a_{21} + b_{21}, & a_{22} + b_{22}, & \dots, & a_{2n} + b_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} + b_{m1}, & a_{m2} + b_{m2}, & \dots, & a_{mn} + b_{mn} \end{pmatrix}.$$

Je-li $r \in T$ libovolný prvek, pak *r-násobkem matice* A rozumíme matici

$$rA = \begin{pmatrix} ra_{11}, & ra_{12}, & \dots, & ra_{1n} \\ ra_{21}, & ra_{22}, & \dots, & ra_{2n} \\ \dots & \dots & \dots & \dots \\ ra_{m1}, & ra_{m2}, & \dots, & ra_{mn} \end{pmatrix}.$$

Matice A se rovná matici B, právě když $a_{ij} = b_{ij}$ pro všechna $i = 1, 2, \dots, m$, $j = 1, 2, \dots, n$. O prvcích $a_{11}, a_{22}, \dots, a_{kk}$ matice A typu (m, n), kde $k = \min\{m, n\}$, říkáme, že leží v (hlavní) *diagonále* nebo že tvoří diagonálu matice A. Matice A sestávající ze samých nul, tj. taková, že $a_{ij} = 0$ pro všechna $i = 1, 2, \dots, m$ a $j = 1, 2, \dots, n$ se nazývá *nulová matice*. Matice A typu (n, n) se nazývá *čtvercová matice* stupně n. Čtvercová matice stupně n, která má mimo hlavní diagonálu samé 0, tj. $a_{ij} = 0$ pro $i \neq j$, $i, j = 1, 2, \dots, n$, se nazývá *diagonální*. Diagonální matice $E = (e_{ij})$ stupně n taková, že $e_{ii} = 1$ pro každé $i = 1, 2, \dots, n$ se nazývá *jednotková matice stupně n*.

4.2. Definice. Nenulová matice $\boldsymbol{A}$ typu (m,n) ad tělesem T se nazývá *Gaussova*, jestliže existují indexy $1 \leq i_1 < i_2 < \cdots < i_k \leq n$ tak, že $a_{1i_1} \neq 0$, $a_{2i_2} \neq 0$, $\ldots, a_{ki_k} \neq 0$ a $a_{ji} = 0$, jestliže buď $k < j \leq m$, nebo $j \leq k$ a zároveň $i < i_j$. Matice $\boldsymbol{A}$ se nazývá *Jordanova*, je-li Gaussova a prvek $a_{ji_j} = 1$ je jediným nenulovým prvkem i_j-tého sloupce matice $\boldsymbol{A}$, $j = 1, 2, \ldots, k$. Speciálně budeme v tomto případě hovořit o Gaussově či Jordanově matici s indexy $(i_1, i_2, \ldots, i_k)$.

4.3. Věta. *Každou nenulovou matici $\boldsymbol{A}$ typu (m,n) lze konečným počtem elementárních transformací na řádky matice převést na Gaussovu matici.*

Důkaz. Budeme postupovat úplnou indukcí podle počtu m řádků matice $\boldsymbol{A}$. Pro $m = 1$ je matice tvořena jediným nenulovým řádkem a i_1 je číslo sloupce, ve kterém je první nenulový prvek matice. Buď tedy $m > 1$ a předpokládejme, že pro každou nenulovou matici s méně než m řádky tvrzení platí. Buď nyní i_1 číslo prvního nenulového sloupce matice $\boldsymbol{A}$. Bez újmy na obecnosti můžeme předpokládat, že $a_{1i_1} \neq 0$, a to vzhledem k tomu, že vzájemnou výměnu řádků matice lze uskutečnit konečným počtem elementárních transformací podle věty 3.3. Je-li první řádek matice $\boldsymbol{A}$ jejím jediným nenulovým řádkem, jsme hotovi. V opačném případě přičtením vhodných násobků prvního řádku k řádkům ostatním snadno dosáhneme toho, že a_{1i_1} je jediným nenulovým prvkem i_1-tého sloupce. Je-li nyní $\boldsymbol{B}$ dílčí matice matice $\boldsymbol{A}$, která vznikne vynecháním prvního řádku a prvních $i_1 - 1$ sloupců, lze podle indukčního předpokladu tuto matici převést konečným počtem elementárních transformací na řádky na Gaussovu matici. Vzhledem k tomu, že prvních $i_1 - 1$ sloupců je nulových, je okamžitě patrné, že použití stejných elementárních transformací na řádky matice $\boldsymbol{A}$ vede ke Gaussově matici. ∎

4.4. Věta. *Každou nenulovou matici $\boldsymbol{A}$ typu (m,n) lze konečným počtem elementárních transformací na řádky matice převést na Jordanovu matici.*

Důkaz. Vzhledem k předchozí větě můžeme předpokládat, že matice $\boldsymbol{A}$ je Gaussova. Když vynásobíme j-tý řádek matice $\boldsymbol{A}$ prvkem $a_{ji_j}^{-1}$, $j = 1, 2, \ldots, k$, dostaneme Gaussovu matici $\boldsymbol{B}$ takovou, že $b_{ji_j} = 1$ pro každé $j = 1, 2, \ldots, k$. K dokončení důkazu nyní zřejmě stačí pro každé $j = 1, 2, \ldots, k$ přičíst vhodné násobky j-tého řádku k řádkům předcházejícím. ∎

4.5. Definice. Buď $\boldsymbol{A} = (a_{ij})$ matice typu (m,n) a $\boldsymbol{B} = (b_{ij})$ typu (n,p) nad tělesem T. *Součinem* $\boldsymbol{AB}$ těchto matic (v tomto pořadí!) rozumíme matici $\boldsymbol{C} = (c_{ij})$ typu (m,p), kde $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$.

4.6. Poznámka. Pojem součinu matic je, jak uvidíme později, pojmem velmi důležitým, a proto se nad ním zamyslíme poněkud podrobněji. Předně si uvědomme, že je-li $\boldsymbol{A}$ matice typu (m,n) a $\boldsymbol{B}$ matice typu (k,p), pak součin $\boldsymbol{AB}$ je definován pouze v případě, kdy $n = k$, a v tomto případě je matice $\boldsymbol{AB}$ typu (m,p). Speciálně tedy součin $\boldsymbol{AB}$ může být definován, zatímco součin $\boldsymbol{BA}$ nikoliv. Je zřejmé, že oba součiny $\boldsymbol{AB}$ a $\boldsymbol{BA}$ jsou definovány, právě když matice $\boldsymbol{A}$ je typu (m,n) a matice $\boldsymbol{B}$ je typu (n,m). Součin $\boldsymbol{AB}$ je pak čtvercová matice stupně m, zatímco $\boldsymbol{BA}$ je čtvercová matice stupně n. Jsou-li speciálně $\boldsymbol{A}$ i $\boldsymbol{B}$ čtvercové matice stupně n, jsou oba součiny $\boldsymbol{AB}$ i $\boldsymbol{BA}$ definovány, avšak obecně neplatí rovnost $\boldsymbol{AB} = \boldsymbol{BA}$. Vezmeme-li např.

$$A = \begin{pmatrix} 1, & 3 \\ 2, & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 3, & 1 \\ 1, & 2 \end{pmatrix},$$

je

$$AB = \begin{pmatrix} 6, & 7 \\ 7, & 4 \end{pmatrix}, \qquad BA = \begin{pmatrix} 5, & 10 \\ 5, & 5 \end{pmatrix}.$$

4.7. Věta. *Buď $\boldsymbol{A}$ matice typu (m,n), $\boldsymbol{B}$, $\boldsymbol{C}$ buďte matice typu (n,p), $\boldsymbol{D}$ buď matice typu (p,q), $\boldsymbol{E}_n$ a $\boldsymbol{E}_m$ buďte jednotkové matice stupňů n a m a $r \in T$ buď libovolný prvek. Pak platí*

(i) $\boldsymbol{A}(\boldsymbol{B}+\boldsymbol{C}) = \boldsymbol{AB}+\boldsymbol{AC}$, $(\boldsymbol{B}+\boldsymbol{C})\boldsymbol{D} = \boldsymbol{BD}+\boldsymbol{CD}$;

(ii) $(\boldsymbol{AB})\boldsymbol{D} = \boldsymbol{A}(\boldsymbol{BD})$;

(iii) $(r\boldsymbol{A})\boldsymbol{B} = \boldsymbol{A}(r\boldsymbol{B}) = r(\boldsymbol{AB})$;

(iv) $\boldsymbol{E}_m\boldsymbol{A} = \boldsymbol{AE}_n = \boldsymbol{A}$.

Důkaz. (i) Označíme-li $\boldsymbol{K} = (k_{ij}) = \boldsymbol{A}(\boldsymbol{B}+\boldsymbol{C})$ a $\boldsymbol{L} = (l_{ij}) = \boldsymbol{AB}+\boldsymbol{AC}$, pak platí $k_{ij} = \sum_{r=1}^{n} a_{ir}(b_{rj}+c_{rj}) = \sum_{r=1}^{n} a_{ir}b_{rj} + \sum_{i=1}^{n} a_{ir}c_{rj} = l_{ij}$ pro všechna $i = 1,2,\ldots.m$, $j = 1,2,\ldots,p$. Druhá z rovností se dokáže analogicky.

(ii) Označme $\boldsymbol{K} = (k_{ij}) = \boldsymbol{AB}$, $\boldsymbol{L} = \boldsymbol{KD} = (\boldsymbol{AB})\boldsymbol{D}$, $\boldsymbol{M} = \boldsymbol{BD}, \boldsymbol{N} = \boldsymbol{AM} = \boldsymbol{A}(\boldsymbol{BD})$. Pak $l_{ij} = \sum_{r=1}^{p} k_{ir}d_{rj} = \sum_{r=1}^{p}\sum_{s=1}^{n} a_{is}b_{sr}d_{rj} = \sum_{s=1}^{n} a_{is}\sum_{r=1}^{p} b_{sr}d_{rj} = \sum_{s=1}^{n} a_{is}m_{sj} = n_{ij}$ pro všechna $i = 1,2,\ldots,m$, $j = 1,2,\ldots,q$.

(iii) Označíme-li $\boldsymbol{K} = r(\boldsymbol{AB})$, $\boldsymbol{L} = (r\boldsymbol{A})\boldsymbol{B}$, $\boldsymbol{M} = \boldsymbol{A}(r\boldsymbol{B})$, je $k_{ij} = r\sum_{s=1}^{n} a_{is}b_{sj} = \sum_{s=1}^{n} ra_{is}b_{sj} = l_{ij} = \sum_{s=1}^{n} a_{is}rb_{sj} = m_{ij}$ pro všechna $i = 1,2,\ldots,m$, $j = 1,2,\ldots,p$.

(iv) Zřejmé. ∎

4.8. Definice. Buď $\boldsymbol{A}$ matice typu (m,n) nad tělesem T. *Hodností $h(\boldsymbol{A})$ matice* $\boldsymbol{A}$ rozumíme dimenzi podprostoru prostoru T^n generovaného řádkovými vektory matice $\boldsymbol{A}$.

4.9. Věta. *Buď $\boldsymbol{A}$ matice typu (m,n) nad tělesem T. Je-li $\boldsymbol{B}$ Gaussova matice, která vznikla z matice $\boldsymbol{A}$ konečným počtem elementárních transformací na řádky, pak $h(\boldsymbol{A})$ je rovna počtu nenulových řádků matice $\boldsymbol{B}$.*

Důkaz. Řádkové vektory matice $\boldsymbol{A}$ a řádkové vektory matice $\boldsymbol{B}$ generují týž podprostor prostoru T^n podle věty 3.4. Vzhledem k větě 3.6 tvoří nenulové řádky matice $\boldsymbol{B}$ bázi tohoto podprostoru. ∎

4.10. Věta. *Buď $\boldsymbol{A} = (a_{ij})$ matice (m,n) a $\boldsymbol{B} = (b_{ij})$ matice matice typu (n,p). Označme $\boldsymbol{a}_i = (a_{1i}, a_{2i}, \ldots, a_{mi}) \in T^m$, $i = 1,2,\ldots,n$, sloupcové vektory matice $\boldsymbol{A}$ a $\boldsymbol{b}_j = (b_{j1}, b_{j2}, \ldots, b_{jp}) \in T^p$, $j = 1,2,\ldots,n$, řádkové vektory matice $\boldsymbol{B}$. Označíme-li dále $\boldsymbol{c}_i = (c_{i1}, c_{i2}, \ldots, c_{ip}) \in T^p$, $i = 1,2,\ldots,n$, řádkové vektory matice $\boldsymbol{C} = \boldsymbol{AB}$ a označíme-li $\boldsymbol{d}_j = (c_{1j}, c_{2j}, \ldots, c_{mj}) \in T^m$, $j = 1,2,\ldots,p$, sloupcové vektory matice $\boldsymbol{C}$, platí*

(i) $\boldsymbol{c}_i = \sum_{j=1}^{n} a_{ij}\boldsymbol{b}_j$, $i = 1,2,\ldots,m$;

(ii) $\boldsymbol{d}_j = \sum_{i=1}^{n} b_{ij}\boldsymbol{a}_i$, $j = 1,2,\ldots,p$.

Důkaz. (i) Jest $\sum_{j=1}^{n} a_{ij}\boldsymbol{b}_j = \sum_{j=1}^{n} a_{ij}(b_{j1}, b_{j2}, \ldots, b_{jp}) = \sum_{j=1}^{n}(a_{ij}b_{j1}, a_{ij}b_{j2}, \ldots, a_{ij}b_{jp}) = (\sum_{j=1}^{n} a_{ij}b_{j1}, \sum_{j=1}^{n} a_{ij}b_{j2}, \ldots, \sum_{j=1}^{n} a_{ij}b_{jp}) = (c_{i1}, c_{i2}, \ldots, c_{ip}) = \boldsymbol{c}_i$.

(ii) Podobně jest $\sum_{i=1}^n b_{ij}\boldsymbol{a}_i = \sum_{i=1}^n b_{ij}(a_{1i}, a_{2i}, \dots, a_{mi}) = \sum_{i=1}^n (b_{ij}a_{1i}, b_{ij}a_{2i}, \dots, b_{ij}a_{mi}) = (\sum_{i=1}^n a_{1i}b_{ij}, \sum_{i=1}^n a_{2i}b_{ij}, \dots, \sum_{i=1}^n a_{mi}b_{ij}) = (c_{1j}, c_{2j}, \dots, c_{mj}) = \boldsymbol{d}_j$. ■

4.11. Poznámka. Právě dokázaná věta neříká nic jiného, než že násobit matici $\boldsymbol{B}$ zleva maticí $\boldsymbol{A}$ znamená provést jisté lineární kombinace na řádky matice $\boldsymbol{B}$. Přitom koeficienty lineární kombinace týkající se i-tého řádku jsou obsaženy v i-tém řádku matice $\boldsymbol{A}$. Podobně násobení matice $\boldsymbol{A}$ maticí $\boldsymbol{B}$ zprava lze interpretovat jako provádění jistých lineárních kombinací na sloupce matice $\boldsymbol{A}$, přičemž koeficienty lineární kombinace týkající se j-tého sloupce jsou obsaženy v j-tém sloupci matice $\boldsymbol{B}$.

4.12. Věta. *Buď $\boldsymbol{A}$ matice typu (m,n) a $\boldsymbol{B}$ matice typu (n,p) nad tělesem $\boldsymbol{T}$. Pak $h(\boldsymbol{AB}) \le min\,(h(\boldsymbol{A}), h(\boldsymbol{B}))$.*

Důkaz. Označíme-li $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_m$ řádkové vektory matice $\boldsymbol{A}$, $\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n$ řádkové vektory matice $\boldsymbol{B}$ a $M = (\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n)$, pak $\boldsymbol{a}_1 * M, \boldsymbol{a}_2 * M, \dots, \boldsymbol{a}_m * M$ jsou řádkové vektory matice $\boldsymbol{AB}$ podle věty 4.10. Podle věty 2.25 je $\langle \boldsymbol{a}_1 * M, \boldsymbol{a}_2 * M, \dots, \boldsymbol{a}_m * M\rangle \subseteq \langle M\rangle$, takže $h(\boldsymbol{AB}) \le h(\boldsymbol{B})$. Bez újmy na obecnosti můžeme předpokládat, že $\boldsymbol{a}_1 * M, \boldsymbol{a}_2 * M, \dots, \boldsymbol{a}_k * M$ je báze $\langle \boldsymbol{a}_1 * M, \boldsymbol{a}_2 * M, \dots, \boldsymbol{a}_m * M\rangle$. Podle věty 2.25 jsou vektory $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_k$ lineárně nezávislé, takže $h(\boldsymbol{AB}) = k \le \dim\langle \boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_m\rangle = h(\boldsymbol{A})$ a věta je dokázána. ■

4.13. Definice. Buď

$$\boldsymbol{A} = \begin{pmatrix} a_{11}, & a_{12}, & \dots, & a_{1n} \\ a_{21}, & a_{22}, & \dots, & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1}, & a_{m2}, & \dots, & a_{mn} \end{pmatrix}$$

matice stupně typu (m,n) nad tělesem $\boldsymbol{T}$. Matici

$$\boldsymbol{A}^T = \begin{pmatrix} a_{11}, & a_{21}, & \dots, & a_{m1} \\ a_{12}, & a_{22}, & \dots, & a_{m2} \\ \dots & \dots & \dots & \dots \\ a_{1n}, & a_{2n}, & \dots, & a_{mn} \end{pmatrix}$$

typu (n,m), kterou dostaneme z matice $\boldsymbol{A}$ vzájemnou výměnou řádků za sloupce a naopak, nazýváme *maticí transponovanou* k matici $\boldsymbol{A}$. Čtvercová matice $\boldsymbol{A}$ stupně n se nazývá *symetrická*, jestliže $\boldsymbol{A} = \boldsymbol{A}^T$, tj. $a_{ij} = a_{ji}$, $i,j = 1,2,\dots,n$, a *antisymetrická*, jestliže $\boldsymbol{A} = -\boldsymbol{A}^T$, tj. $a_{ij} = -a_{ji}$, $i,j = 1,2,\dots,n$.

4.14. Věta. *Buď $\boldsymbol{A}$ matice typu (m,n) a $\boldsymbol{B}$ matice typu (n,p) nad tělesem $\boldsymbol{T}$. Pak platí:*

(i) $(\boldsymbol{A}^T)^T = \boldsymbol{A}$;
(ii) $(\boldsymbol{AB})^T = \boldsymbol{B}^T\boldsymbol{A}^T$.

Důkaz. (i) Z definice vyplývá, že označíme-li $\boldsymbol{A}^T = (a_{ij}^T)$, pak $a_{ij}^T = a_{ji}$. Tedy $(\boldsymbol{A}^T)^T = ((a_{ij}^T)^T) = (a_{ji}^T) = (a_{ij}) = \boldsymbol{A}$.

(ii) Označme $\boldsymbol{C} = (c_{ij}) = \boldsymbol{AB}$ součin matic $\boldsymbol{A}$ a $\boldsymbol{B}$, který je typu (m,p) a $\boldsymbol{D} = (d_{ij}) = \boldsymbol{B}^T\boldsymbol{A}^T$ typu (p,m). Pak $c_{ij}^T = c_{ji} = \sum_{k=1}^n a_{jk}b_{ki} = \sum_{k=1}^n b_{ik}^T a_{kj}^T = d_{ij}$, takže $\boldsymbol{C}^T = \boldsymbol{D} = \boldsymbol{B}^T\boldsymbol{A}^T$. ■

5.1. Definice. *Soustavou m lineárních rovnic o n neznámých* nad tělesem T rozumíme soustavu tvaru

$$(*)\qquad \begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \dots & + & a_{1n}x_n & = & b_1\,, \\ a_{21}x_1 & + & a_{22}x_2 & + & \dots & + & a_{2n}x_n & = & b_2\,, \\ \multicolumn{9}{c}{\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots} \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \dots & + & a_{mn}x_n & = & b_m\,, \end{array}$$

kde $a_{ij}, b_i, i = 1, \dots, m, j = 1, \dots, n$ jsou nějaké prvky z tělesa T. Matice $\boldsymbol{A} = (a_{ij})$ typu (m, n) se nazývá *matice soustavy*, matice

$$\left(\begin{array}{cccc|c} a_{11}, & a_{12} & \dots, & a_{1n} & b_1 \\ a_{21}, & a_{22} & \dots, & a_{2n} & b_2 \\ \multicolumn{4}{c|}{\dots\dots\dots\dots\dots\dots} & \dots \\ a_{m1}, & a_{m2} & \dots, & a_{mn} & b_m \end{array}\right)$$

typu $(m, n+1)$ se nazývá *rozšířená matice* soustavy $(*)$. Vektor $\boldsymbol{u} = (x_1, x_2, \dots, x_n) \in T^n$ takový, že jeho dosazením do soustavy $(*)$ je splněno všech m rovností, se nazývá *řešením soustavy* $(*)$. Vektor $\boldsymbol{b} = (b_1, b_2, \dots, b_m) \in T^m$ se nazývá *sloupec pravých stran*, v případě $\boldsymbol{b} = 0$ hovoříme o *homogenní soustavě* lineárních rovnic, v opačném případě se jedná o *nehomogenní soustavu* lineárních rovnic. Rozšířenou matici soustavy budeme stručně označovat symbolem $(\boldsymbol{A}, \boldsymbol{b})$ složeným z matice soustavy a sloupce pravých stran. Homogenní soustavu lineárních rovnic s maticí $\boldsymbol{A}$ budeme nazývat *homogenní soustavou příslušnou soustavě* $(*)$.

5.2. Poznámka. Zatímco homogenní soustava lineárních rovnic je vždycky řešitelná, neboť nulový vektor $\boldsymbol{u} = 0$ je jejím řešením, u nehomogenních soustav je situace poněkud odlišná, jak je patrno z následujícího triviálního příkladu

$$\begin{array}{ccccc} x & + & y & = & 1, \\ x & + & y & = & 2. \end{array}$$

Budeme se tedy nejprve zabývat otázkou řešitelnosti soustavy $(*)$.

5.3. Věta. *Nehomogenní soustava lineárních rovnic $(*)$ je řešitelná, právě když sloupec $\boldsymbol{b}$ pravých stran je lineární kombinací sloupcových vektorů matice $\boldsymbol{A}$.*

Důkaz. Jestliže označíme $\boldsymbol{c}_1 = (a_{11}, a_{21}, \dots, a_{m1})$, $\boldsymbol{c}_2 = (a_{12}, a_{22}, \dots, a_{m2}), \dots$, $\boldsymbol{c}_n = (a_{1n}, a_{2n}, \dots, a_{mn})$ sloupcové vektory matice $\boldsymbol{A}$ a $M = (\boldsymbol{c}_1, \boldsymbol{c}_2, \dots, \boldsymbol{c}_n) \in (T^m)^n$, vidíme, že vektor $\boldsymbol{u} = (x_1, x_2, \dots, x_n)$ je řešením soustavy $(*)$, právě když $\sum_{i=1}^{n} \boldsymbol{c}_i x_i = \boldsymbol{u} * M = \boldsymbol{b}$. ∎

5.4. Poznámka. Provedeme-li na řádky rozšířené matice konečný počet elementárních transformací (viz 3.1), dostaneme novou soustavu rovnic, přičemž zřejmě každé řešení soustavy $(*)$ je řešením soustavy nové a naopak. Podle vět 4.3 nebo 4.4 můžeme rozšířenou matici $(\boldsymbol{A}, \boldsymbol{b})$ převést konečným počtem elementárních transformací na Gaussův či Jordanův tvar, přičemž soustava rovnic příslušná této nové matici má stejnou množinu řešení jako soustava původní $(*)$. Přitom je-li speciálně $(\boldsymbol{E}, \boldsymbol{c})$ Jordanův tvar matice $(\boldsymbol{A}, \boldsymbol{b})$ je zřejmě vektor $\boldsymbol{c}$ (jediným) řešením soustavy soustavy $(*)$.

5.5. Věta. *Je-li $\boldsymbol{A} = (a_{ij})$ matice typu (m, n) nad tělesem T, pak $h(\boldsymbol{A}) = h(\boldsymbol{A}^T)$.* *Jinými slovy: Dimenze podprostoru prostoru T^n generovaného řádkovými vektory matice $\boldsymbol{A}$ je rovna dimenzi podprostoru prostoru T^m generovaného sloupcovými vektory matice $\boldsymbol{A}$.*

Důkaz. Nechť Jordanův tvar $\boldsymbol{C}$ matice $\boldsymbol{A}$ má indexy $(i_1, i_2, \ldots, i_k)$. Pro $k = n$ je zřejmě matice $\boldsymbol{C}$ jednotková, takže $h(\boldsymbol{A}) = h(\boldsymbol{E}) = n \leq h(\boldsymbol{A}^T) \leq n$, vzhledem k tomu, že transponovaná matice $\boldsymbol{A}^T$ má n řádků. Je-li nyní $k < n$ a $i \in \{1, 2, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_k\}$ libovolný prvek, můžeme utvořit matici $\boldsymbol{B}$ typu $(m, k+1)$ sestávající postupně ze sloupců matice $\boldsymbol{A}$ s čísly $i_1, i_2, \ldots, i_k$ a i. Je patrné, že provedeme-li na řádky matice $\boldsymbol{B}$ stejné elementární transformace, pomocí kterých jsme matici $\boldsymbol{A}$ převedli na matici $\boldsymbol{C}$, dostaneme matici tvaru $(\boldsymbol{E}, \boldsymbol{c})$, kde $\boldsymbol{E}$ je jednotková matice stupně k. Pohlížíme-li nyní na matici $\boldsymbol{B}$ jako na rozšířenou matici nehomogenní soustavy lineárních rovnic, vidíme z předchozí poznámky, že vektor $\boldsymbol{c}$ je řešením této soustavy, takže z věty 5.3 dostáváme, že i-tý sloupcový vektor matice $\boldsymbol{A}$ je lineární kombinací sloupcových vektorů s čísly $i_1, i_2, \ldots, i_k$. Z důsledku 2.4 tedy ihned plyne, že sloupcové vektory matice $\boldsymbol{A}$ s čísly $i_1, i_2, \ldots, i_k$ generují podprostor prostoru T^n generovaný (všemi) sloupcovými vektory matice $\boldsymbol{A}$. Odtud dostáváme nerovnost $h(\boldsymbol{A}^T) \leq k = h(\boldsymbol{A})$. Provedeme-li stejnou úvahu s transponovanou maticí $\boldsymbol{A}^T$, dostaneme $h(\boldsymbol{A}) = h((\boldsymbol{A}^T)^T) \leq h(\boldsymbol{A}^T)$ a jsme hotovi. ∎

5.6. Věta. (Frobenius) *Nehomogenní soustava lineárních rovnic $(*)$ je řešitelná, právě když hodnost matice soustavy $h(\boldsymbol{A})$ je rovna hodnosti matice rozšířené $h((\boldsymbol{A}, \boldsymbol{b}))$.*

Důkaz. Označíme-li $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n$ sloupce matice $\boldsymbol{A}$, pak soustava $(*)$ je podle věty 5.3 řešitelná, právě když $\boldsymbol{b} \in \langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n \rangle$, tj. právě když $\langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n \rangle = \langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n, \boldsymbol{b} \rangle$. To ale znamená, že $h(\boldsymbol{A}^T) = h((\boldsymbol{A}, \boldsymbol{b})^T)$, takže podle předchozí věty je $h(\boldsymbol{A}) = h(\boldsymbol{A}^T) = h((\boldsymbol{A}, \boldsymbol{b})^T) = h((\boldsymbol{A}, \boldsymbol{b}))$. ∎

Nyní zredukujeme otázku nalezení všech řešení nehomogenní soustavy $(*)$ na nalezení jednoho (partikulárního) řešení a na nalezení všech řešení příslušné soustavy homogenní. Poté se budeme věnovat řešení homogenních soustav lineárních rovnic. V dalším budeme používat pro jednoduchost následující úmluvu. Je-li $(*)$ nehomogenní soustava lineárních rovnic s maticí $\boldsymbol{A}$, pak symbolem $\widetilde{W}_{\boldsymbol{A}}$ označíme množinu všech řešení soustavy $(*)$ a symbolem $W_{\boldsymbol{A}}$ množinu všech řešení příslušné homogenní soustavy. Speciálně tedy v případě homogenní soustavy lineárních rovnic s maticí $\boldsymbol{A}$ je $\widetilde{W}_{\boldsymbol{A}} = W_{\boldsymbol{A}}$.

5.7. Věta. *Buď $\boldsymbol{u} = (x_1, x_2, \ldots, x_n) \in T^n$ řešení nehomogenní soustavy lineárních rovnic $(*)$ a buď $W_{\boldsymbol{A}}$ množina všech řešení příslušné homogenní soustavy lineárních rovnic. Pak $\boldsymbol{u} + W_{\boldsymbol{A}} = \{\boldsymbol{u} + \boldsymbol{v} \mid \boldsymbol{v} \in W_{\boldsymbol{A}}\}$ je právě množina všech řešení nehomogenní soustavy lineárních rovnic $(*)$. Tedy $\widetilde{W}_{\boldsymbol{A}} = \boldsymbol{u} + W_{\boldsymbol{A}}$.*

Důkaz. Označíme-li, stejně jako v důkazu věty 5.3, $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n$ sloupcové vektory matice $\boldsymbol{A}$ a $M = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n) \in (T^m)^n$, pak vektor $\boldsymbol{v} \in T^n$ leží ve $W_{\boldsymbol{A}}$, právě když $\boldsymbol{v} * M = 0$, a leží ve $\widetilde{W}_{\boldsymbol{A}}$, právě když $\boldsymbol{v} * M = \boldsymbol{b}$. Pro $\boldsymbol{v} \in W_{\boldsymbol{A}}$ tedy podle věty [illegible]áme $(\boldsymbol{u} + \boldsymbol{v}) * M = (\boldsymbol{u} * M) + (\boldsymbol{v} * M) = \boldsymbol{b}$, takže $\boldsymbol{u} + W_{\boldsymbol{A}} \subseteq \widetilde{W}_{\boldsymbol{A}}$. Na druhé straně, je-li $\boldsymbol{w} \in \widetilde{W}_{\boldsymbol{A}}$ libovolný prvek, pak $\boldsymbol{w} = \boldsymbol{u} + (\boldsymbol{w} - \boldsymbol{u}) \in \boldsymbol{u} + W_{\boldsymbol{A}}$, a tedy

$\widetilde{W_A} \subseteq \boldsymbol{u} + W_A$ vzhledem k tomu, že $(\boldsymbol{w} - \boldsymbol{u}) * M = (\boldsymbol{w} * M) - (\boldsymbol{u} * M) = 0$. Tedy $\boldsymbol{u} + W_A$ je množina všech řešení nehomogenní soustavy lineárních rovnic $(*)$. ∎

5.8. Věta. *Množina W_A všech řešení homogenní soustavy lineárních rovnic s maticí $\boldsymbol{A}$ typu (m, n) tvoří podprostor aritmetického vektorového prostoru T^n, jehož dimenze je rovna $n - h(\boldsymbol{A})$.*

Důkaz. Nechť $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n$ jsou sloupcové vektory matice $\boldsymbol{A}$. Jsou-li $\boldsymbol{u} = (x_1, x_2, \ldots, x_n)$ a $\boldsymbol{v} = (y_1, y_2, \ldots, y_n)$ dva vektory z W_A a $r \in T$ je libovolný prvek, pak $(\boldsymbol{u} + \boldsymbol{v}) * M = (\boldsymbol{u} * M) + (\boldsymbol{v} * M) = 0$, $r\boldsymbol{u} * M = r(\boldsymbol{u} * M) = 0$, $\boldsymbol{u} + \boldsymbol{v}$ a $r\boldsymbol{u}$ tedy leží ve W_A a W_A je podprostor v T^n podle definice 1.6.

Použijeme-li označení z věty 2.25, vidíme, ihned, že $\mathrm{Ker}(M) = W_A$ a $\dim W_A = n - \dim\langle M \rangle = n - h(\boldsymbol{A}^T) = n - h(\boldsymbol{A})$ podle vět 2.25 a 5.5. ∎

5.9. Důsledek. *Buď $\boldsymbol{A}$ čtvercová matice stupně n. Následující podmínky jsou ekvivalentní:*

(i) homogenní soustava lineárních rovnic s maticí $\boldsymbol{A}$ má pouze triviální řešení;
(ii) nehomogenní soustava lineárních rovnic s rozšířenou maticí $(\boldsymbol{A}, \boldsymbol{b})$ má jediné řešení pro libovolný sloupec $\boldsymbol{b} \in T^n$ pravých stran;
(iii) $h(\boldsymbol{A}) = n$.

Důkaz. Ekvivalence podmínek (i) a (iii) plyne ihned z předchozí věty. Platí-li (ii), je podle věty 5.7 $W_A = 0$ a k platnosti (iii) stačí opět použít větu 5.8. Předpokládáme-li naopak (iii) a převedeme-li matici $(\boldsymbol{A}, \boldsymbol{b})$ pomocí elementárních transformací na řádky na Jordanovu matici $(\boldsymbol{B}, \boldsymbol{c})$, je $h(\boldsymbol{B}) = h(\boldsymbol{A}) = n$ podle věty 3.4, takže $\boldsymbol{B} = \boldsymbol{E}$ je jednotková matice stupně n a $\boldsymbol{c}$ je jediné řešení uvažované soustavy. ∎

5.10. Poznámka. Uvědomme si, že důkaz věty 5.8 spolu s důkazem tvrzení 2.25 (vi) dává vlastně konkrétní návod na řešení homogenní soustavy lineárních rovnic. Tento postup, často nazývaný *Gaussova eliminační metoda*, spočívá v převedení matice soustavy na Gaussův (Jordanův) tvar s indexy $(i_1, i_2, \ldots, i_k)$ a výpočtu vektorů $\boldsymbol{u}_j, j \in J = \{1, 2, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_k\}$. Pro $j \in J$ položíme $u_{jj} = 1$, $u_{ji} = 0$ pro každé $i \in J \setminus \{i\}$ a postupně z jednotlivých rovnic dopočteme $u_{ji_k}, u_{ji_{k-1}}, \ldots, u_{ji_1}$. Ukažme si tento postup na několika konkrétních příkladech.

5.11. Příklady. Domluvme se, že pokud dostaneme při provádění elementárních transformací na řádky matice nulový řádek, budeme tento řádek pro jednoduchost prostě vynechávat.

1. Nalezněme všechna řešení homogenní soustavy lineárních rovnic s maticí

$$\boldsymbol{A} = \begin{pmatrix} 1, -1, & 2, & 3 \\ 2, -2, & 3, & 4 \\ 3, -3, & 5, & 7 \\ 4, -4, & 7, & 10 \end{pmatrix}.$$

Ř e š e n í : Prováděním elementárních transformací na řádky postupně dostaneme

$$\begin{pmatrix} 1, -1, & 2, & 3 \\ 2, -2, & 3, & 4 \\ 3, -3, & 5, & 7 \\ 4, -4, & 7, & 10 \end{pmatrix} \sim \begin{pmatrix} 1, -1, & 2, & 3 \\ 0, & 0, -1, & -2 \\ 0, & 0, -1, & -2 \\ 0, & 0, -1, & -2 \end{pmatrix} \sim \begin{pmatrix} 1, -1, & 2, & 3 \\ 0, & 0, & 1, & 2 \end{pmatrix}.$$

Vidíme tedy, že v tomto případě je příslušná Gaussova matice s indexy $(1,3)$ a můžeme tedy spočítat vektory $\boldsymbol{u}_2 = (1,1,0,0)$, $\boldsymbol{u}_4 = (1,0,-2,1)$, takže $W_{\boldsymbol{A}} = \langle \boldsymbol{u}_2, \boldsymbol{u}_4 \rangle$.

2. Nalezněme všechna řešení homogenní soustavy lineárních rovnic s maticí

$$\boldsymbol{A} = \begin{pmatrix} 1,-1,-1, & 3, & 2, & 2 \\ 2,-1,-2, & 7, & 4, & 5 \\ 3,-2,-3, & 9, & 6, & 5 \\ 5,-3,-5, & 16, & 10, & 10 \\ 7,-4,-7, & 23, & 14, & 15 \\ 8,-5,-8, & 23, & 16, & 11 \end{pmatrix}.$$

Řešení: Podobně jako v předchozím příkladu postupně máme

$$\begin{pmatrix} 1,-1,-1, & 3, & 2, & 2 \\ 2,-1,-2, & 7, & 4, & 5 \\ 3,-2,-3, & 9, & 6, & 5 \\ 5,-3,-5, & 16, & 10, & 10 \\ 7,-4,-7, & 23, & 14, & 15 \\ 8,-5,-8, & 23, & 16, & 11 \end{pmatrix} \sim \begin{pmatrix} 1,-1,-1, & 3, & 2, & 2 \\ 0, \ 1, \ 0, & 1, & 0, & 1 \\ 0, \ 1, \ 0, & 0, & 0, & -1 \\ 0, \ 2, \ 0, & 1, & 0, & 0 \\ 0, \ 3, \ 0, & 2, & 0, & 1 \\ 0, \ 3, \ 0, & -1, & 0, & -5 \end{pmatrix} \sim$$

$$\begin{pmatrix} 1,-1,-1, & 3, & 2, & 2 \\ 0, \ 1, \ 0, & 1, & 0, & 1 \\ 0, \ 0, \ 0, & -1, & 0, & -2 \\ 0, \ 0, \ 0, & -1, & 0, & -2 \\ 0, \ 0, \ 0, & -1, & 0, & -2 \\ 0, \ 0, \ 0, & -4, & 0, & -8 \end{pmatrix} \sim \begin{pmatrix} 1,-1,-1, & 3, & 2, & 2 \\ 0, \ 1, \ 0, & 1, & 0, & 1 \\ 0, \ 0, \ 0, & 1, & 0, & 2 \end{pmatrix}.$$

Jedná se tedy o Gaussovu matici s indexy $(1,2,4)$ a dostáváme tedy $W_{\boldsymbol{A}} = \langle \boldsymbol{u}_3, \boldsymbol{u}_5, \boldsymbol{u}_6 \rangle$, kde $\boldsymbol{u}_3 = (1,0,1,0,0,0)$, $\boldsymbol{u}_5 = (-2,0,0,0,1,0)$ a $\boldsymbol{u}_6 = (5,1,0,-2,0,1)$.

3. Nalezněme všechna řešení nehomogenní soustavy lineárních rovnic s rozšířenou maticí

$$(\boldsymbol{A}, \boldsymbol{b}) = \left(\begin{array}{ccc|c} 2, & 3, & 1 & 7 \\ 3, & 1, & 2 & 3 \\ 1, & 3, & 2 & 5 \end{array}\right).$$

Řešení: Stejně jako u předcházejících úloh prováděním elementárních transformací na řádky rozšířené matice postupně dostaneme

$$\left(\begin{array}{ccc|c} 2, & 3, & 1 & 7 \\ 3, & 1, & 2 & 3 \\ 1, & 3, & 2 & 5 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1, & 3, & 2 & 5 \\ 0, & -3, & -3 & -3 \\ 0, & -8, & -4 & -12 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1, & 3, & 2 & 5 \\ 0, & 1, & 1 & 1 \\ 0, & 0, & 1 & -1 \end{array}\right).$$

Odtud tedy ihned vidíme, že řešením soustavy je vektor $(1,2,-1)$. Poznamenejme v této souvislosti, že hodnost matice soustavy je rovna 3, takže soustava má skutečně jediné řešení podle důsledku 5.9.

4. Nalezněme všechna řešení nehomogenní soustavy lineárních rovnic s rozšířenou maticí

$$(\boldsymbol{A},\boldsymbol{b})=\left(\begin{array}{cccc|c}1, & 2, & 4, & 3 & 10\\ 2, & -1, & 1, & -2 & 0\\ 3, & 2, & -1, & 1 & 5\\ 6, & 3, & 4, & 2 & 14\end{array}\right).$$

Ř e š e n í : Jest

$$\left(\begin{array}{cccc|c}1, & 2, & 4, & 3 & 10\\ 2, & -1, & 1, & -2 & 0\\ 3, & 2, & -1, & 1 & 5\\ 6, & 3, & 4, & 2 & 14\end{array}\right)\sim\left(\begin{array}{cccc|c}1, & 2, & 4, & 3 & 10\\ 0, & -5, & -7, & -8 & -20\\ 0, & -4, & -13, & -8 & -25\\ 0, & -9, & -20, & -16 & -46\end{array}\right)\sim$$

$$\left(\begin{array}{cccc|c}1, & 2, & 4, & 3 & 10\\ 0, & 5, & 7, & 8 & 20\\ 0, & 0, & -37, & -8 & -45\\ 0, & 0, & 37, & 8 & 50\end{array}\right)\sim\left(\begin{array}{cccc|c}1, & 2, & 4, & 3 & 10\\ 0, & 5, & 7, & 8 & 20\\ 0, & 0, & 37, & 8 & 45\\ 0, & 0, & 0, & 0 & 5\end{array}\right).$$

Vidíme, že $h(\boldsymbol{A})=3<4=h((\boldsymbol{A},\boldsymbol{b}))$, a soustava tudíž není podle Frobeniovy věty 5.6 řešitelná.

5. Nalezněme všechna řešení nehomogenní soustavy lineárních rovnic s rozšířenou maticí

$$(\boldsymbol{A},\boldsymbol{b})=\left(\begin{array}{ccccc|c}1, & 3, & 2, & 5, & 4 & 15\\ 2, & 1, & 3, & -1, & 2 & 7\\ 3, & 1, & -1, & 2, & -1 & 4\\ 3, & 4, & 5, & 4, & 6 & 22\\ 5, & 2, & 2, & 1, & 1 & 11\\ 6, & 5, & 4, & 6, & 5 & 26\end{array}\right).$$

Ř e š e n í : Máme

$$\left(\begin{array}{ccccc|c}1, & 3, & 2, & 5, & 4 & 15\\ 2, & 1, & 3, & -1, & 2 & 7\\ 3, & 1, & -1, & 2, & -1 & 4\\ 3, & 4, & 5, & 4, & 6 & 22\\ 5, & 2, & 2, & 1, & 1 & 11\\ 6, & 5, & 4, & 6, & 5 & 26\end{array}\right)\sim\left(\begin{array}{ccccc|c}1, & 3, & 2, & 5, & 4 & 15\\ 0, & -5, & -1, & -11, & -6 & -23\\ 0, & -8, & -7, & -13, & -13 & -41\\ 0, & -5, & -1, & -11, & -6 & -23\\ 0, & -13, & -8, & -24, & -19 & -64\\ 0, & -13, & -8, & -24, & -19 & -64\end{array}\right)\sim\left(\begin{array}{ccccc|c}1, & 3, & 2, & 5, & 4 & 15\\ 0, & 5, & 1, & 11, & 6 & 23\\ 0, & 0, & 27, & -23, & 17 & 21\end{array}\right).$$

Snadno se nahlédne, že partikulární řešení soustavy je např. vektor $(1,1,1,1,1)$. Řešení příslušné homogenní soustavy $W_{\boldsymbol{A}}$ má dimenzi 2 a je generováno vektory $\boldsymbol{u}_4,\boldsymbol{u}_5$, kde $\boldsymbol{u}_4=(11,-64,23,27,0)$, $\boldsymbol{u}_5=(-13,29,17,0,-27)$. Celkem tedy máme $\widetilde{W}_{\boldsymbol{A}}=(1,1,1,1,1)+W_{\boldsymbol{A}}$.

Permutací na množině M se rozumí každé prosté zobrazení množiny M na sebe samu. V případě, že množina M je konečná, je snadno patrné, že každé zobrazení množiny M na sebe je již prosté a každé prosté zobrazení množiny M do sebe je již surjektivní. Této skutečnosti budeme v dalším mlčky využívat.

6.1. Definice. *Permutací Π na množině $M = \{1, 2, \ldots, n\}$* rozumíme každé prosté zobrazení množiny M na ni samu. Permutaci Π budeme zpravidla zapisovat v tzv. *základním tvaru*, tj. ve tvaru tabulky

$$\Pi = \begin{pmatrix} 1, 2, \ldots, n \\ r_1, r_2, \ldots, r_n \end{pmatrix},$$

kde $\Pi(i) = r_i$ pro každé $i = 1, 2, \ldots, n$. Je-li $s_1, s_2, \ldots, s_n$ libovolné pořadí prvků $1, 2 \ldots, n$ a $\Pi(s_i) = t_i$, $i = 1, 2, \ldots, n$, můžeme tutéž permutaci zapsat v tzv. *obecném tvaru*

$$\Pi = \begin{pmatrix} s_1, s_2, \ldots, s_n \\ t_1, t_2, \ldots, t_n \end{pmatrix}.$$

Prvek $r \in M$ nazýváme *samodružným prvkem* permutace Π, jestliže $\Pi(r) = r$. V opačném případě nazýváme prvek r *nesamodružným*.

Například na množině $M = \{1, 2, 3, 4\}$ máme

$$\begin{pmatrix} 2, & 4, & 1, & 3 \\ 4, & 1, & 3, & 2 \end{pmatrix} = \begin{pmatrix} 3, & 1, & 2, & 4 \\ 2, & 3, & 4, & 1 \end{pmatrix} = \begin{pmatrix} 4, & 2, & 1, & 3 \\ 1, & 4, & 3, & 2 \end{pmatrix} = \begin{pmatrix} 1, & 2, & 3, & 4 \\ 3, & 4, & 2, & 1 \end{pmatrix}$$

různé tvary permutace Π, přičemž poslední z nich je tvarem základním.

6.2. Věta. *Množina $M = \{1, 2, \ldots, n\}$ má právě $n!$ navzájem různých permutací.*

Důkaz. Pro $n = 1$ existuje zřejmě právě jedna permutace, totiž $\Pi(1) = 1$. Předpokládejme tedy $n > 1$ a postupujme úplnou indukcí podle n. Ze základního tvaru permutace je patrné, že počet permutací je roven počtu všechy možných pořadí prvků z množiny M. Protože na prvním místě může být kterýkoliv z prvků $1, 2, \ldots, n$ a ke každému z nich existuje podle indukčního předpokladu právě $(n-1)!$ navzájem různých pořadí zbývajících $n - 1$ prvků, vidíme ihned, že všech permutací na množině M je $n \cdot (n-1)! = n!$ a jsme hotovi. ∎

6.3. Definice. Permutaci I množiny $M = \{1, 2, \ldots, n\}$ nazýváme *identickou* nebo *jednotkovou*, je-li každý prvek množiny M samodružným prvkem permutace I. Permutaci

$$\Pi^{-1} = \begin{pmatrix} s_1, s_2, \ldots, s_n \\ r_1, r_2, \ldots, r_n \end{pmatrix}$$

nazýváme *inverzní permutací* k permutaci

$$\Pi = \begin{pmatrix} r_1, r_2, \ldots, r_n \\ s_1, s_2, \ldots, s_n \end{pmatrix}.$$

Jsou-li

$$\Pi_1 = \begin{pmatrix} r_1, r_2, \dots, r_n \\ s_1, s_2, \dots, s_n \end{pmatrix} \quad \text{a} \quad \Pi_2 = \begin{pmatrix} s_1, s_2, \dots, s_n \\ t_1, t_2, \dots, t_n \end{pmatrix}$$

dvě permutace množiny M, pak permutaci

$$\Pi = \begin{pmatrix} r_1, r_2, \dots, r_n \\ t_1, t_2, \dots, t_n \end{pmatrix}$$

nazýváme *součinem permutací* Π_1, Π_2 a značíme $\Pi = \Pi_2 \Pi_1$.

6.4. Věta. *Buďte Π, Π_1, Π_2, Π_3 permutace množiny $M = \{1, 2, \dots, n\}$. Pak platí:*

(i) $\Pi_1(\Pi_2\Pi_3) = (\Pi_1\Pi_2)\Pi_3$;
(ii) $\Pi I = I\Pi = \Pi$;
(iii) $\Pi^{-1}\Pi = \Pi\Pi^{-1} = I$.

Důkaz. Lze přenechat čtenáři jako jednoduché cvičení. ∎

6.5. Definice. Množina všech permutací na množině $M = \{1, 2, \dots, n\}$ je vzhledem k operaci násobení permutací grupa řádu $n!$. Tato grupa se nazývá *symetrická grupa permutací stupně* n a značí se S_n.

6.6. Definice. Buď $\{r_1, r_2, \dots, r_k\}$ podmožina množiny $M = \{1, 2, \dots, n\}$, $k \geq 2$. Permutaci $\Pi \in S_n$ takovou, že $\Pi(r_1) = r_2$, $\Pi(r_2) = r_3, \dots, \Pi(r_{k-1}) = r_k$, $\Pi(r_k) = r_1$, $\Pi(s) = s$ pro každé $s \in M \setminus \{r_1, r_2, \dots, r_k\}$ nazýváme *cyklem délky* k a značíme $(r_1, r_2, \dots, r_k)$. Cykl délky 2 se nazývá *transpozice*. Dva cykly $(r_1, r_2, \dots, r_k)$, $(s_1, s_2, \dots, s_l)$ se nazývají *nezávislé*, jestliže $\{r_1, r_2, \dots, r_k\} \cap \{s_1, s_2, \dots, s_l\} = \emptyset$. Cykly $\Pi_1, \Pi_2, \dots, \Pi_m$ jsou *nezávislé*, jsou-li nezávislé každé dva cykly Π_i, Π_j, $i \neq j$, $i, j = 1, 2, \dots, m$.

6.7. Poznámka. Z definice cyklu je ihned patrné, že pro každé $i = 1, 2, \dots, n$ platí $(r_1, r_2, \dots, r_k) = (r_i, r_{i+1}, \dots, r_k, r_1, \dots, r_{i-1})$ a že $(r_1, r_2, \dots, r_k)^{-1} = (r_k, r_{k-1}, \dots, r_2, r_1)$. Kromě toho je ihned vidět, že každé dva nezávislé cykly Π_1, $\Pi_2 \in S_n$ spolu komutují, tj. platí $\Pi_1\Pi_2 = \Pi_2\Pi_1$. Přitom násobení permutací obecně komutativní není, jak je patrno z následujícího jednoduchého příkladu:
Pro permutace

$$\Pi_1 = \begin{pmatrix} 1, & 2, & 3 \\ 2, & 3, & 1 \end{pmatrix} \text{ a } \Pi_2 = \begin{pmatrix} 1, & 2, & 3 \\ 2, & 1, & 3 \end{pmatrix}$$

máme

$$\Pi_1\Pi_2 = \begin{pmatrix} 1, & 2, & 3 \\ 3, & 2, & 1 \end{pmatrix} \text{ a } \Pi_2\Pi_1 = \begin{pmatrix} 1, & 2, & 3 \\ 1, & 3, & 2 \end{pmatrix}.$$

6.8. Věta. *Každou permutaci $\Pi \in S_n$ lze rozložit v součin nezávislých cyklů. Tento rozklad je až na pořadí činitelů jednoznačný.*

Důkaz. Začneme důkazem existence, budeme postupovat úplnou indukcí podle počtu l nesamodružných prvků permutace Π. Pro $l = 0$ je $\Pi = I$ identická permutace, která je prázdným součinem nezávislých cyklů (součin s nulovým počtem činitelů). Buď tedy $l > 0$ a předpokládejme, že každou permutaci s méně než l nesamodružnými prvky lze rozložit v součin nezávislých cyklů. Je-li nyní $\Pi \in S_n$ permutace s právě l nesamodružnými prvky, definujme posloupnost $r_1, r_2, \ldots$ prvků množiny M indukcí takto: Za r_1 vezmeme libovolný nesamodružný prvek permutace Π, a jsou-li $r_1, r_2, \ldots, r_m$ již definovány, položíme $r_{m+1} = \Pi(r_m)$. Protože množina M je konečná, nemohou být všechny prvky této posloupnosti navzájem různé, takže můžeme nalézt první index $j+1$ takový, že prvek r_{j+1} se už v posloupnosti $r_1, r_2, \ldots, r_j$ vyskytl, tedy $r_{j+1} = r_i$ pro nějaké $i = 1, 2, \ldots, j$. Předně vidíme, že $j > 1$, neboť v opačném případě bychom dostali spor $r_2 = r_1$ s nesamodružností prvku r_1. Snadno též ukážeme, že $i = 1$. Pro $i > 1$ bychom totiž dostali spor s volbou čísla $j+1$, neboť by platilo $r_j = \Pi^{-1}(r_{j+1}) = \Pi^{-1}(r_i) = r_{i-1}$. Ukázali jsme tedy, že restrikce Π_1 permutace Π na množinu $\{r_1, r_2, \ldots, r_j\}$ je cykl. Každý samodružný bod permutace Π je zřejmě samodružným bodem cyklu Π_1 a tedy i součinu $\Pi_1^{-1}\Pi$. Kromě toho je $\Pi_1^{-1}\Pi(r_1) = \Pi_1^{-1}(r_2) = r_1$, takže permutace $\Pi_1^{-1}\Pi$ má více samodružných, a tedy méně nesamodružných, bodů než permutace Π, takže podle indukčního předpokladu je permutace $\Pi_1^{-1}\Pi$ součinem nezávislých cyklů, $\Pi_1^{-1}\Pi = \Pi_2 \ldots \Pi_m$. Odtud $\Pi = \Pi_1\Pi_2 \ldots \Pi_m$ a zbývá ověřit, že cykly $\Pi_1, \Pi_2, \ldots, \Pi_m$ jsou nezávislé. Cykly $\Pi_2, \ldots, \Pi_m$ jsou nezávislé podle indukčního předpokladu a protože každé $r_i, i = 1, 2, \ldots, j$, je zřejmě samodružným bodem permutace $\Pi_1^{-1}\Pi = \Pi_2 \ldots \Pi_m$, je cykl Π_1 nezávislý s každým z cyklů $\Pi_2, \ldots, \Pi_m$.

Přejděme tedy k důkazu jednoznačnosti a postupujme indukcí podle počtu m činitelů v nějakém rozkladu permutace Π v součin nezávislých cyklů. Pro $m = 0$ je permutace Π identická a prázdný součin je zřejmě jediný možný rozklad permutace Π v součin nezávislých cyklů. Buď tedy $m > 0$ a buďte $\Pi = \Pi_1\Pi_2 \ldots \Pi_m = \Pi'_1\Pi'_2 \ldots \Pi'_{m'}$ dva rozklady permutace Π v součin nezávislých cyklů. Jestliže $\Pi_1 = (r_1, r_2, \ldots, r_k)$, pak r_1 se vzhledem k nezávislosti cyklů $\Pi'_1, \Pi'_2, \ldots, \Pi'_m$ vyskytuje právě v jednom z nich, přičemž vzhledem k tomu, že nezávislé cykly podle poznámky 6.7 spolu komutují, můžeme bez újmy na obecnosti předpokládat, že prvek r_1 se vyskytuje právě v cyklu Π'_1. Podle poznámky 6.7 můžeme navíc psát $\Pi'_1 = (s_1, s_2, \ldots, s_{k'})$, kde $s_1 = r_1$. Pak ale indukcí snadno dostáváme $s_2 = \Pi'_1(s_1) = \Pi(s_1) = \Pi(r_1) = r_2, \ldots, s_k = \Pi'_1(s_{k-1}) = \Pi(s_{k-1}) = \Pi(r_{k-1}) = r_k$, $\Pi'_1(s_k) = \Pi(s_k) = \Pi(r_k) = r_k$, takže $\Pi'_1 = \Pi_1$. Permutace $\Pi_1^{-1}\Pi = \Pi_2 \ldots \Pi_m = \Pi'_2 \ldots \Pi'_{m'}$ má rozklad na součin $m-1$ nezávislých cyklů, takže podle indukčního předpokladu je $m = m'$ a při vhodném očíslování cyklů $\Pi'_2, \ldots, \Pi'_m$ je $\Pi'_i = \Pi_i$, $i = 2, \ldots, m$. ∎

6.9. Věta. *Každou permutaci $\Pi \in S_n$ lze rozložit v součin transpozic. Je-li speciálně $\Pi = (r_1, r_2, \ldots, r_k)$ cykl, je $\Pi = (r_1, r_k), (r_1, r_{k-1}), \ldots, (r_1, r_2)$.*

Důkaz. Vzhledem k tom, že druhá část tvrzení je zřejmá, stačí k důkazu prvního použít předchozí větu. ∎

6.10. Poznámka. O nezávislosti transpozic v předchozí větě nemá smysl hovořit, protože každý součin nezávislých transpozic má sudý počet nesamodružných prvků, zatímco např. permutace $\Pi = \begin{pmatrix} 1,2,3 \\ 2,3,1 \end{pmatrix}$ má 3 nesamodružné prvky. Stejná situace je i s jednoznačností, pro výše uvedenou permutaci např. máme $\Pi = (1,3)(1,2) = (1,2)(2,3)$. Přesto však rozklady permutací na součin transpozic v sobě mají jistý prvek jednoznačnosti, jak ukazuje tato velmi důležitá věta umožňující v dalším definovat tzv. znaménko permutace.

6.11. Věta. *Buď $\Pi \in S_n$ permutace a buďte $\Pi = T_1T_2 \dots T_m = S_1S_2 \dots S_l$ dva rozklady permutace Π v součin transpozic. Pak čísla m a l jsou buď obě sudá, nebo obě lichá.*

Důkaz. Předně si uvědomme, že je-li $S = (r, s)$ transpozice, je $S^2 = S \cdot S = I$ identická permutace, takže $S^{-1} = S$. Pak z rovnosti $T_1T_2 \dots T_m = S_1S_2 \dots S_l$ dostáváme $T_1T_2 \dots T_mS_lS_{l-1} \dots S_2S_1 = I$, tedy rozklad identické permutace v součin $m + l$ transpozic. Protože součet $m + l$ je sudý, právě když jsou čísla m a l buď obě sudá, nebo obě lichá, vidíme, že k dokončení důkazu věty stačí ukázat, že každý rozklad identické permutace v součin transpozic má sudý počet činitelů. Buď tedy $I = T_1T_2 \dots T_l$ a postupujme indukcí podle l. Pro $l = 0$ se jedná o prázdný součin, který má sudý počet činitelů. Buď tedy $l > 0$ a předpokládejme, že každý rozklad identické permutace v součin méně než l činitelů má sudý počet činitelů. Snadno se ověří, že pro každé tři prvky $r, u, t \in M$ platí rovnost

$$(u, t)(r, t)(u, t) = (r, u).$$

Nechť nyní $T_1 = (r, s)$. Pak jistě existuje index $1 < i \le l$ takový, že transpozice T_i obsahuje prvek r. V opačném případě je totiž r samodružným bodem všech transpozic $T_2, \dots, T_l$, takže $r = I(r) = T_1T_2 \dots T_l(r) = T_1(r) = s$, což není možné. Je-li $i > 1$ nejmenší index takový, že $T_i = (r, t)$, pak pro $i > 2$ jsou buď transpozice T_{i-1}, T_i nezávislé, a tedy $T_{i-1}T_i = T_iT_{i-1}$ podle poznámky 6.7, nebo $T_{i-1} = (u, t)$ a z výše uvedené rovnosti dostáváme $T_{i-1}T_i = (u, t)(r, t) = (r, u)(u, t) = T'_{i-1}T'_i$. Vidíme tedy, že rozklad identické permutace, který obsahuje prvek r v transpozici na i-tém místě, můžeme nahradit stejně dlouhým rozkladem obsahujícím transpozici s prvkem r na $(i - 1)$-ním místě. Odtud snadno plyne, že opakováním tohoto postupu dojdeme nakonec k rozkladu $I = (r, s_1)(r, s_2) \dots (r, s_k)T'_{k+1} \dots T'_l$, kde transpozice $T'_{k+1}, \dots, T'_l$ již neobsahují prvek r (případ $k = l$ ovšem není vyloučen). Ukažme, že existuje index $i = 1, 2, \dots, k - 1$ takový, že $s_k = s_i$. V opačném případě bychom totiž vzhledem k tomu, že transpozice $T'_{k+1}, \dots, T'_l$ neobsahují prvek r měli $r = I(r) = (r, s_1)(r, s_2) \dots (r, s_k)T'_{k+1}, \dots, T'_l(r) = (r, s_1)(r, s_2) \dots (r, s_k)(r) = (r, s_1)(r, s_2) \dots (r, r_{k-1})(s_k) = s_k$, což není možné. Buď tedy $i = 1, 2, \dots, k - 1$ největší prvek takový, že $S_i = S_k$. Předpokládejme nejprve, že $i < k - 1$. Položíme-li nyní ve výše uvedené rovnosti $t = r, u = s_i, r = s_{i+1}$, dostaneme $(r, s_i)(r, s_{i+1}) = (s_i, s_{i+1})(r, s_i)$. Nahradíme-li tedy v našem součinu příslušnou část touto rovností, dostaneme opět rozklad identické permutace na součin l transpozic, avšak prvek $s_k = s_i$ se bude vyskytovat v transpozici na $(i + 1)$-místě. Opakováním tohoto postupu zřejmě nakonec dostaneme rozklad $I = (r, s_1)(r, s_2) \dots (r, s_{i-1})T''_i \dots T''_{k-2}$ $(r, s_i)(r, s_k)T'_{k+1} \dots T'_l$. Protože $s_i = s_k$, je $(r, s_i)(r, s_k) = I$, takže $I = (r, s_1)(r, s_2)$ $\dots (r, s_{i-1})T''_i \dots T''_{k-2}T'_{k+1} \dots T'_l$ je rozklad identické permutace v součin $l-2$ transpozic. Podle indukčního předpokladu je číslo $l - 2$ sudé, tedy i l je sudé a věta je dokázána. ∎

6.12. Definice. Řekneme, že permutace $\Pi \in S_n$ je *sudá*, jestliže ji lze rozložit na součin sudého počtu transpozic, a řekneme, že permutace Π je *lichá*, jestliže ji lze rozložit na součin lichého počtu transpozic. *Znaménko permutace* $\operatorname{zn} \Pi$ definujeme tak, že sudé permutaci přiřadíme $\operatorname{zn} \Pi = 1$ a liché permutaci $\operatorname{zn} \Pi = -1$.

6.13. Věta. *Buďte Π a Π' dvě permutace na množině $M = \{1, 2, \ldots, n\}$. Pak platí:*

(i) $\operatorname{zn}(\Pi\Pi') = \operatorname{zn}\Pi \operatorname{zn}\Pi'$;

(ii) $\operatorname{zn}\Pi^{-1} = \operatorname{zn}\Pi$.

Důkaz. (i) Jsou-li $\Pi = T_1T_2 \ldots T_m$ a $\Pi' = S_1S_2 \ldots S_l$ rozklady permutací Π a Π' v součin transpozic, pak $\Pi\Pi' = T_1T_2 \ldots T_mS_1S_2 \ldots S_l$ a tvrzení plyne ihned z definice.

(ii) Protože $\Pi\Pi^{-1} = I$, je $1 = \operatorname{zn} I = \operatorname{zn}\Pi \cdot \operatorname{zn}\Pi^{-1}$ podle (i) a permutace Π a Π^{-1} mají nutně stejná znaménka. ∎

6.14. Poznámka. Množina $\{1, -1\}$ je zřejmě multiplikativní grupa vzhledem k přirozenému násobení prvků, tj. 1 je jednotkový prvek a $(-1)(-1) = 1$. Předcházející věta tedy vlastně říká, že znaménko permutace je vlastně homomorfismus $\operatorname{zn} : S_n \to \{1, -1\}$ grupy S_n na multiplikativní grupu $\{1, -1\}$. Označíme-li A_n jádro tohoto homomorfismu, je A_n normální podgrupa grupy S_n. Z věty o homomorfismu dostáváme $S_n/A_n \cong \{1, -1\}$, takže A_n je indexu 2 v S_n. Protože A_n sestává právě ze všech sudých permutací, znamená to, že na množině $M = \{1, 2, \ldots, n\}$ existuje právě $\frac{n!}{2}$ sudých a $\frac{n!}{2}$ lichých permutací. Grupa A_n se nazývá *alternující grupa permutací* stupně n. Na závěr této poznámky si uvědomme ještě jednu snadnou, leč důležitou skutečnost. Je-li $\Pi = T_1T_2 \ldots T_m$ rozklad permutace Π na součin transpozic, pak $\operatorname{zn}\Pi = (-1)^m$.

6.15. Věta. *Nechť permutace $\Pi \in S_n$ je součinem nezávislých cyklů $\Pi = \Pi_1\Pi_2 \ldots \Pi_m$, kde každý z cyklů Π_i, $i = 1, 2, \ldots, m$, má délku $k_i + 1$. Pak $\operatorname{zn}\Pi = \prod_{i=1}^{m}(-1)^{k_i} = (-1)^{\sum_{i=1}^{m} k_i}$.*

Důkaz. Podle věty 6.13 je $\operatorname{zn}\Pi = \operatorname{zn}\Pi_1 \operatorname{zn}\Pi_2 \ldots \operatorname{zn}\Pi_m$, takže zbývá ukázat, že je-li $\Pi = (r_1, r_2, \ldots, r_{k+1})$ cykl délky $k+1$, pak $\operatorname{zn}\Pi = (-1)^k$. Podle věty 6.9 je však $\Pi = (r_1, r_{k+1})(r_1, r_k) \ldots (r_1, r_2)$, takže $\operatorname{zn}\Pi = (-1)^k$ podle předchozí poznámky. ∎

6.16. Příklady. Právě dokázaná věta dává jednu z metod pro výpočet znaménka permutace. Stačí rozložit danou permutaci na součin nezávislých cyklů a použít předchozí vzorec. Přitom rozklad permutace na součin nezávislých cyklů můžeme podle důkazu věty 6.8 nalézt takto: Vezmeme první nesamodružný prvek permutace Π a utvoříme cykl Π_1. Vezmeme první nesamodružný prvek permutace Π, který není obsažen v Π_1, a stejným způsobem pokračujeme dále až do vyčerpání všech nesamodružných prvků permutace Π. Spočtěme znaménko permutace

$$\Pi = \begin{pmatrix} 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, & 10, & 11, & 12, & 13, & 14, & 15, & 16, & 17 \\ 7, & 17, & 3, & 13, & 4, & 15, & 6, & 11, & 14, & 1, & 5, & 12, & 16, & 2, & 10, & 8, & 9 \end{pmatrix}.$$

Řešení: První nesamodružný prvek permutace Π je 1, takže $\Pi_1 = (1, 7, 6, 15, 10)$. Dále máme $\Pi_2 = (2, 17, 9, 14)$. Prvek 3 je samodružný a první nesamodružný prvek neležící ani v Π_1, ani v Π_2 tedy je 4. Takže $\Pi_3 = (4, 13, 16, 8, 11, 5)$ a můžeme tudíž psát $\Pi = \Pi_1\Pi_2\Pi_3 = (1, 7, 6, 15, 10)(2, 17, 9, 14)(4, 13, 16, 8, 11, 5)$ a předchozí věta dává $\operatorname{zn}\Pi = (-1)^4(-1)^3(-1)^5 = 1$. Daná permutace je tedy sudá.

Na závěr tohoto paragrafu si ukážeme ještě jednu metodu pro výpočet znaménka permutace. Poznamenejme, že tvrzení následující věty bývá v některých učebnicích uváděno jako definice znaménka permutace.

6.17. Věta. *Buď* $\Pi = \begin{pmatrix} 1, & 2, & \dots, & n \\ r_1, & r_2, & \dots, & r_n \end{pmatrix}$ *permutace na množině* $M = \{1, 2, \dots, n\}$. *Pak*

$$\operatorname{zn} \Pi = \prod_{i>j} \frac{r_i - r_j}{i - j}.$$

Důkaz. Označme výraz na pravé straně dokazované rovnosti symbolem $\operatorname{sgn} \Pi$, tj. $\operatorname{sgn} \Pi = \prod_{i>j} \frac{r_i - r_j}{i-j}$, a ukažme, že $\operatorname{sgn} \Pi = \operatorname{zn} \Pi$ pro každé $\Pi \in S_n$. K tomu zřejmě stačí ukázat dvě věci. Jednak, že $\operatorname{sgn} S = -1$ pro každou transpozici S, jednak, že $\operatorname{sgn}(\Pi\Pi') = \operatorname{sgn}\Pi \operatorname{sgn}\Pi'$. V tomto případě totiž je $\operatorname{zn} S = \operatorname{sgn} S = -1$ pro každou transpozici S, a protože $\operatorname{zn}(\Pi\Pi') = \operatorname{zn}\Pi \operatorname{zn}\Pi'$ podle věty 6.13 pro každé dva prvky $\Pi, \Pi' \in S_n$, je $\operatorname{zn}\Pi = \operatorname{sgn}\Pi$ pro každé $\Pi \in S_n$ vzhledem k tomu, že každou permutaci lze podle věty 6.9 rozložit na součin transpozic.

Uvědomme si nejprve, že čitatel výrazu pro $\operatorname{sgn}\Pi$ obsahuje až na znaménka tytéž činitele jako jmenovatel, takže $\operatorname{sgn}\Pi = \pm 1$. Kromě toho je patrné, že $\operatorname{sgn}\Pi$ nezávisí na tvaru zápisu permutace Π, tj. zapíšeme-li Π v obecném tvaru $\Pi = \begin{pmatrix} r_1, & r_2, & \dots, & r_n \\ s_1, & s_2, & \dots, & s_n \end{pmatrix}$ je $\operatorname{sgn}\Pi = \prod_{i>j} \frac{s_i - s_j}{r_i - r_j}$. Odtud však ihned dostáváme pro $\Pi_1 = \begin{pmatrix} 1, & 2, & \dots, & n \\ r_1, & r_2, & \dots, & r_n \end{pmatrix}$ a $\Pi_2 = \begin{pmatrix} r_1, & r_2, & \dots, & r_n \\ s_1, & s_2, & \dots, & s_n \end{pmatrix}$ rovnost $\operatorname{sgn}(\Pi_2\Pi_1) = \prod_{i>j} \frac{s_i - s_j}{i-j} = \prod_{i>j} \frac{s_i - s_j}{r_i - r_j} \cdot \frac{r_i - r_j}{i - j} = \prod_{i>j} \frac{s_i - s_j}{r_i - r_j} \cdot \prod_{i>j} \frac{r_i - r_j}{i-j} = \operatorname{sgn}\Pi_2 \operatorname{sgn}\Pi_1$. Nakonec buď $S = (k, l) = \begin{pmatrix} 1, & 2, & \dots, & k, \dots, & l, \dots, & n \\ 1, & 2, & \dots, & l, \dots, & k, \dots, & n \end{pmatrix}$ transpozice. Protože z předchozího plyne, že $\operatorname{sgn} S$ záleží výhradně na počtu záporných činitelů v čitateli výrazu pro $\operatorname{sgn} S$, podívejme se, o které činitele se jedná. Jsou to jednak činitelé $k - l, k - (k+1), \dots, k - (l-1)$, jednak činitelé $(k+1) - l, (k+2) - l, \dots, (l-1) - l$, v celkovém počtu $1 + (l-1) - k + (l-1) - k = 2(l-k) - 1$. Vidíme tedy, že počet záporných činitelů je liché číslo, takže $\operatorname{sgn} S = -1$ a věta je dokázána. ■

6.18. Poznámka. Jak jsme viděli v právě dokončeném důkazu, znaménko permutace je dáno počtem záporných činitelů v čitateli výrazu pro $\operatorname{sgn}\Pi$. Ty odpovídají těm činitelům, pro něž je $i > j$ a zároveň $r_i < r_j$. Řekneme proto, že dvojice (i, j) tvoří *inverzi*, jestliže $i > j$ a $r_i < r_j$. Je-li nyní p počet všech inverzí permutace Π, je $\operatorname{zn}\Pi = (-1)^p$. Prakticky to znamená, že máme-li permutaci Π v základním tvaru $\Pi_1 = \begin{pmatrix} 1, & 2, & \dots, & n \\ r_1, & r_2, & \dots, & r_n \end{pmatrix}$, počítáme, kolik prvků ve druhém řádku za r_1 je menších než r_1, kolik prvků za r_2 je menších než r_2, atd. Celkový počet takto získaný dává exponent p.

6.19. Příklad. Vraťme se k příkladu z odstavce 6.16 a spočtěme $\operatorname{zn}\Pi$ právě popsanou metodou. Máme

$$\Pi = \begin{pmatrix} 1, & 2, 3, & 4, 5, & 6, 7, & 8, & 9, 10, 11, 12, 13, 14, 15, 16, 17 \\ 7, & 17, 3, & 13, 4, & 15, 6, & 11, & 14, \ 1, \ 5, 12, 16, \ 2, 10, \ 8, \ 9 \end{pmatrix},$$

vpravo od 7 je 6 menších čísel, totiž 3,4,6,1,5,2. Podobně v pravo od 17 je 15 menších čísel, totiž všechna kromě 7, vpravo od 3 jsou 2, totiž 1 a 2, atd. Celkem tedy máme $p = 6 + 15 + 2 + 10 + 2 + 10 + 3 + 6 + 7 + 0 + 1 + 4 + 4 + 0 + 2 + 0 = 72$, takže $\operatorname{zn} \Pi = (-1)^{72} = 1$ a permutace Π je sudá. V praxi nás ovšem součet p samotný nezajímá, zajímá nás pouze to, zda číslo p je sudé nebo liché. Ve výše napsaném součtu tedy můžeme sudé sčítance vynechávat, liché sčítance vynechávat po dvou a záleží pak na tom, co zbude. Pokud zbude jeden lichý sčítanec, je permutace lichá, v opačném případě, když nezbude nic, se jedná o permutaci sudou.

7.1. Definice. Buď

$$A = \begin{pmatrix} a_{11}, & a_{12}, & \dots, & a_{1n} \\ a_{21}, & a_{22}, & \dots, & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1}, & a_{n2}, & \dots, & a_{nn} \end{pmatrix}$$

čtvercová matice stupně n nad tělesem T. *Determinantem matice* $\boldsymbol{A}$ rozumíme prvek

$$\det \boldsymbol{A} = \sum_{\Pi \in S_n} \operatorname{zn} \Pi a_{1r_1} a_{2r_2} \dots a_{nr_n}$$

tělesa T, kde sčítáme přes všechny permutace

$$\Pi = \begin{pmatrix} 1, 2, \dots, n \\ r_1, r_2, \dots, r_n \end{pmatrix}$$

množiny $M = \{1, 2, \dots, n\}$. Determinant matice $\boldsymbol{A}$ budeme též značit symbolem $|\boldsymbol{A}|$ nebo

$$\begin{vmatrix} a_{11}, & a_{12}, & \dots, & a_{1n} \\ a_{21}, & a_{22}, & \dots, & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1}, & a_{n2}, & \dots, & a_{nn} \end{vmatrix}.$$

7.2. Poznámka. Je dobře si explicitně uvědomit, co přesně definice determinantu vlastně říká. Jednotlivé sčítance dostaneme tak, že v každém řádku a sloupci vezmeme jeden prvek a tuto n-tici spolu vynásobíme a opatříme znaménkem příslušné permutace, která vlastně „řídí" výběr prvků z řádků a sloupců. Z těchto úvah je patrné, že definici determinantu můžeme vyslovit i s použitím permutací v obecném tvaru, nikoliv pouze v základním. Tedy $\det \boldsymbol{A} = \sum_{\Pi \in S_n} \operatorname{zn} \Pi a_{r_1 s_1} a_{r_2 s_2} \dots a_{r_n s_n}$, kde se sčítá přes všechny možné permutace $\Pi \in S_n$ tvaru $\Pi = \begin{pmatrix} r_1, r_2, \dots, r_n \\ s_1, s_2, \dots, s_n \end{pmatrix}$. Této jednoduché skutečnosti využijeme v důkazu věty 7.3.

7.3. Věta. *Pro libovolnou čtvercovou matici* $\boldsymbol{A} = (a_{ij})$ *stupně* n *nad tělesem* T *platí* $\det \boldsymbol{A} = \det \boldsymbol{A}^T$, *kde* $\boldsymbol{A}^T$ *je matice transponovaná k matici* $\boldsymbol{A}$.

Důkaz. Podle definice determinantu máme $\det \boldsymbol{A}^T = \sum_{\Pi' \in S_n} \operatorname{zn} \Pi' a^T_{1r_1} a^T_{2r_2} \dots a^T_{nr_n}$ $= \sum_{\Pi' \in S_n} \operatorname{zn} \Pi' a_{r_1 1} a_{r_2 2} \dots a_{r_n n}$, kde sčítáme přes všechny možné permutace $\Pi' = \begin{pmatrix} 1, 2, \dots, n \\ r_1, r_2, \dots, r_n \end{pmatrix}$ množiny $\{1, 2, \dots, n\}$. Na druhé straně podle předchozí poznámky, $\det \boldsymbol{A} = \sum_{\Pi \in S_n} \operatorname{zn} \Pi a_{r_1 1} a_{r_2 2} \dots a_{r_n n}$, kde sčítáme přes všechny permutace $\Pi = \begin{pmatrix} r_1, r_2, \dots, r_n \\ 1, 2, \dots, n \end{pmatrix}$ množiny $\{1, 2, \dots, n\}$. Protože Π' je inverzní permutace k Π, je $\operatorname{zn} \Pi' = \operatorname{zn} \Pi$ podle věty 6.13, takže $\det \boldsymbol{A} = \det \boldsymbol{A}^T$, neboť oba tyto prvky jsou součtem týchž sčítanců. ∎

7.4. Poznámka. Jak víme, každá matice sestává z řádkových a ze sloupcových vektorů. V další části uvidíme, že vlastnosti determinantů zavisejí na řádkových či sloupcových vektorech. Právě dokázaná věta o rovnosti determinantů dané čtvercové matice $\boldsymbol{A}$ a matice $\boldsymbol{A}^T$ k ní transponované nám říká, že nahradíme-li v platné větě o determinantech slovo řádek slovem sloupec a naopak, dostaneme opět platnou větu o determinantech. K důkazu takové věty totiž stačí přejít k matici transponované $\boldsymbol{A}^T$ a opakováním důkazu pro matici $\boldsymbol{A}$ získáme důkaz místo pro řádky matice $\boldsymbol{A}$ pro její sloupce. Z tohoto důvodu budeme v dalším textu formulovat věty pouze pro řádky, při počítání konkrétních příkladů však budeme pochopitelně používat obou typů vět podle toho, co bude pro nás momentálně výhodnější.

7.5. Příklad. Podíváme-li se na definici determinantu, zjistíme, že je sice poměrně jednoduchá, ale pro praktické počítání zcela nevyhovující. Sčítá se v ní totiž přes všechny permutace $\Pi \in S_n$, kterých je podle věty 6.2 právě $n!$, takže již např. pro $n = 6$ se jedná o 720 sčítanců. Ukážeme si nyní jak vypadají determinanty stupňů 2 a 3 a v dalším textu se pak zaměříme na metody výpočtu determinantů vyšších stupňů.

Pro $n = 2$ máme dvě permutace, jednotkovou I a transpozici $S = (1,2)$. Těm odpovídají členy $a_{11}a_{22}$ a $a_{12}a_{21}$, z nichž druhý bude se znaménkem -1. Tedy

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21},$$

čili vynásobíme prvky v hlavní diagonále a od součinu odečteme součin prvků ve vedlejší diagonále.

Pro $n = 3$ máme těchto $3! = 6$ permutací

$$\Pi_1 = I = \begin{pmatrix} 1, & 2, & 3 \\ 1, & 2, & 3 \end{pmatrix}, \quad \Pi_2 = \begin{pmatrix} 1, & 2, & 3 \\ 2, & 3, & 1 \end{pmatrix}, \quad \Pi_3 = \begin{pmatrix} 1, & 2, & 3 \\ 3, & 1, & 2 \end{pmatrix},$$

$$\Pi_4 = \begin{pmatrix} 1, & 2, & 3 \\ 3, & 2, & 1 \end{pmatrix}, \quad \Pi_5 = \begin{pmatrix} 1, & 2, & 3 \\ 1, & 3, & 2 \end{pmatrix}, \quad \Pi_6 = \begin{pmatrix} 1, & 2, & 3 \\ 2, & 1, & 3 \end{pmatrix}.$$

Vidíme, že permutace Π_2 a Π_3 jsou cykly délky 3, takže jejich znaménko je 1, zatímco Π_4, Π_5, Π_6 jsou transpozice se znaménkem -1. Máme tedy

$$\det \boldsymbol{A} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}.$$

Součiny s kladným znaménkem jsou tedy: Součin prvků v hlavní diagonále, součin prvků v naddiagonále s levým dolním rohem a součin pravého horního rohu s poddiagonálou. Podobně součiny se znaménkem -1 jsou: součin prvků ve vedlejší diagonále, součin prvků ve vedlejší poddiagonále s levým horním rohem a součin prvků ve vedlejší naddiagonále s levým dolním rohem. V praxi to znamená toto: Připišme k matici $\boldsymbol{A}$ zprava 1. a 2. sloupec,

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{pmatrix}.$$

Kladné členy pak jsou součiny v hlavní diagonále, naddiagonále a druhé naddiagonále, záporné členy pak jsou součiny ve vedlejší diagonále, poddiagonále a druhé poddiagonále. Této metodě výpočtu determinantu čtvercové matice třetího stupně se říká *Sarrusovo pravidlo.*

7.6. Věta. *Buď* $\boldsymbol{B}$ *čtvercová matice, která vznikne z matice* $\boldsymbol{A}$ *vzájemnou výměnou* i*-tého a* j*-tého řádku,* $i \neq j$*. Pak* $\det \boldsymbol{B} = -\det \boldsymbol{A}$.

Důkaz. Bez újmy na obecnosti můžeme předpokládat, že $i < j$. Podle definice máme $\det \boldsymbol{B} = \sum_{\Pi \in S_n} \operatorname{zn}\Pi b_{1r_1} b_{2r_2} \dots b_{nr_n}$, kde sčítáme přes všechny permutace $\Pi \in S_n$ tvaru $\Pi = \begin{pmatrix} 1, & 2, & \dots, & n \\ r_1, & r_2, & \dots, & r_n \end{pmatrix}$. Označíme-li nyní $S = (i,j)$ transpozici a $\Pi' = \Pi\, S = \begin{pmatrix} 1, & 2, & \dots, i, & \dots, & j, & \dots, & n \\ r_1, & r_2, & \dots, r_j, & \dots, & r_i, & \dots, & r_n \end{pmatrix}$, pak jestliže Π probíhá všechny permutace z S_n, Π' probíhá rovněž celé S_n, neboť každou permutaci σ můžeme napsat ve tvaru $(\sigma\, S)\, S$. Ve smyslu poznámky 7.2 tedy jest $\det \boldsymbol{A} = \sum_{\Pi' \in S_n} \operatorname{zn} \Pi' a_{1r_1} a_{2r_2} \dots a_{ir_j} \dots a_{jr_i} \dots a_{nr_n}$. Vzhledem k větě 6.13 o znaménku součinu dvou permutací tedy máme $\det \boldsymbol{B} = \sum_{\Pi \in S_n} \operatorname{zn} \Pi b_{1r_1} b_{2r_2} \dots b_{ir_i} \dots b_{jr_j} \dots b_{nr_n} = -\sum_{\Pi' \in S_n} \operatorname{zn}(\Pi\, S) a_{1r_1} a_{2r_2} \dots a_{jr_i} \dots a_{ir_j} \dots a_{nr_n} = -\det \boldsymbol{A}$. ∎

7.7. Důsledek. *Buď* $\Pi \in S_n$ *libovolná permutace a* $\boldsymbol{A}$ *čtvercová matice stupně* n *nad tělesem* T*. Jestliže matice* $\boldsymbol{B}$ *vznikne z* $\boldsymbol{A}$ *tak, že na řádky matice* $\boldsymbol{A}$ *provedeme permutaci* Π*, pak* $\det \boldsymbol{B} = \operatorname{zn} \Pi \det \boldsymbol{A}$.

Důkaz. Podle věty 6.9 lze permutaci Π rozložit v součin transpozic, takže tvrzení plyne úplnou indukcí z předchozí věty. ∎

7.8. Věta. *Má-li čtvercová matice* $\boldsymbol{A}$ *stupně* n *nad tělesem* T *dva řádky stejné, je* $\det \boldsymbol{A} = 0$.

Důkaz. Nechť i-tý řádek matice $\boldsymbol{A}$ je roven j-tému. Je-li charakteristika tělesa T různá od 2, pak vzájemnou výměnou i-tého a j-tého řádku matice $\boldsymbol{A}$ dostaneme podle věty 7.6 $\det \boldsymbol{A} = -\det \boldsymbol{A}$ a tedy $\det \boldsymbol{A} = 0$. Je-li $\operatorname{char} T = 2$, můžeme bez újmy na obecnosti předpokládat, že $i < j$ a determinant matice můžeme vzhledem ke skutečnosti, že $-1 = 1$ napsat ve tvaru $\det \boldsymbol{A} = \sum_{\Pi \in S_n} (a_{1r_1} a_{2r_2} \dots a_{ir_i} \dots a_{jr_j} \dots a_{nr_n} + a_{1r_1} a_{2r_2} \dots a_{ir_j} \dots a_{jr_i} \dots a_{nr_n})$, kde se sčítá přes všechny permutace tvaru $\Pi = \begin{pmatrix} 1, & 2, & \dots, & i, & \dots, & j, & \dots, & n \\ r_1, & r_2, & \dots, & r_i, & \dots, & r_j, & \dots, & r_n \end{pmatrix}$, takové, že $r_i < r_j$. Protože $a_{ir_i} = a_{jr_i}$ a $a_{jr_j} = a_{ir_j}$, jsou oba sčítance v závorce stejné, jejich součet je tudíž 0 a $\det \boldsymbol{A} = 0$. ∎

7.9. Úmluva. Buď $\boldsymbol{A} = (a_{ij})$ čtvercová matice stupně n nad tělesem T a buďte $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n$ její řádkové vektory a $\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n$ její sloupcové vektory. Jak jsme se zmínili již výše, řada výsledků o determinantech plyne z vlastností řádků, či sloupců, matice $\boldsymbol{A}$. Pro zjednodušení vyjadřování a zejména zápisu proto zavedeme následující označení pro determinant matice $\boldsymbol{A}$: $\det \boldsymbol{A} = [\![\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n]\!] = [\![\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n]\!]$.

7.10. Definice. Buď $\boldsymbol{A} = (a_{ij})$ matice typu (m, n) nad tělesem T. *Dílčí maticí matice* $\boldsymbol{A}$ rozumíme každou matici $\boldsymbol{B}$, která vznikne z $\boldsymbol{A}$ vynecháním některých (libovolných) řádků a některých sloupců. Determinant každé čtvercové dílčí matice nazýváme *subdeterminantem matice* $\boldsymbol{A}$. Je-li navíc $\boldsymbol{A}$ čtvercová matice stupně n, pak vynecháním libovolných k řádků, $k < n$, a libovolných k sloupců z matice $\boldsymbol{A}$ dostaneme dílčí čtvercovou matici stupně $n - k$. Determinant každé takové dílčí matice nazýváme *subdeterminantem matice $\boldsymbol{A}$ stupně $n - k$*. Speciálně pro $k = 1$ označíme subdeterminant matice vzniklý vynecháním i-tého řádku a j-tého sloupce symbolem M_{ij}. Opatříme-li tento subdeterminant znaménkem, pak prvek $A_{ij} = (-1)^{i+j} M_{ij}$ se nazývá *algebraický doplněk* prvku a_{ij} v matici $\boldsymbol{A}$. *Kroneckerovo delta* δ_{ij} je symbol definovaný vztahy $\delta_{ij} = 0$ pro $i \neq j$, $\delta_{ii} = 1$, $i, j = 1, 2, \ldots, n$.

7.11. Věta. (Rozvoj determinantu podle řádku.) *Buď $\boldsymbol{A} = (a_{ij})$ čtvercová matice stupně n nad tělesem T. Pak*

$$\sum_{k=1}^{n} a_{ik} A_{jk} = \delta_{ij} \det \boldsymbol{A}$$

pro všechna $i, j = 1, 2, \ldots, n$.

Důkaz. Připomeňme, že podle definice 7.1 je $\det \boldsymbol{A} = \sum_{\Pi \in S_n} a_{1r_1} a_{2r_2} \ldots a_{nr_n}$, kde se sčítá přes všechny permutace $\Pi = \begin{pmatrix} 1, & 2, & \ldots, & n \\ r_1, & r_2, & \ldots, & r_n \end{pmatrix} \in S_n$. Z poznámky 7.2 víme, že každý sčítanec obsahuje z každého řádku a každého sloupce právě jeden prvek. Zvolme nyní $j = 1, 2, \ldots, n$ libovolně, ale pevně. Každý sčítanec tedy obsahuje právě jeden prvek z j-tého řádku, takže můžeme dát k sobě sčítance obsahující a_{j1}, dále a_{j2}, atd., až a_{jn}. Vytkneme-li nyní z příslušných sčítanců prvky $a_{j1}, a_{j2}, \ldots, a_{jn}$, můžeme determinant matice $\boldsymbol{A}$ zapsat ve tvaru $[\![\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n]\!] = \sum_{k=1}^{n} a_{jk} B_{jk}$. Uvědomíme-li si nyní, že prvky B_{jk} jsou utvořeny z prvků v řádcích $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_{j-1}, \boldsymbol{a}_{j+1}, \ldots, \boldsymbol{a}_n$, tj. nezávisí vůbec na j-tém řádku, pak nahrazením j-tého řádku matice $\boldsymbol{A}$ řádkem i-tým, $i \neq j$, dostaneme podle věty 7.8 $0 = [\![\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_n]\!] = \sum_{k=1}^{n} a_{ik} B_{jk} = \delta_{ij} \det \boldsymbol{A}$. Vidíme tedy, že k dokončení důkazu zbývá ověřit, že prvky B_{ik} jsou rovny algebraickým doplňkům A_{ik} pro všechny dvojice indexů $i, k = 1, 2, \ldots, n$.

Nejprve probereme speciální případ $i = k = 1$. Součet všech členů determinantu matice $\boldsymbol{A}$ obsahujících prvek a_{11} zřejmě je $\sum_{\Pi} \operatorname{zn} \Pi a_{11} a_{2r_2} \ldots a_{nr_n}$, kde se sčítá přes všechny permutace $\Pi \in S_n$ tvaru $\Pi = \begin{pmatrix} 1, & 2, & \ldots, & n \\ 1, & r_2, & \ldots, & r_n \end{pmatrix}$. Jinými slovy $B_{11} = \sum_{\Pi'} \operatorname{zn} \Pi' a_{2r_2} \ldots a_{nr_n}$, kde sčítáme přes všechny permutace $\Pi' = \begin{pmatrix} 2, & \ldots, & n \\ r_2, & \ldots, & r_n \end{pmatrix}$ množiny $\{2, \ldots, n\}$. Protože zřejmě $\operatorname{zn} \Pi' = \operatorname{zn} \Pi$, je jistě $B_{11} = M_{11} = A_{11}$.

Přejděme tedy k obecnému případu B_{ik} a pokusme se jej převést na případ právě rozřešený. Provedeme-li na řádky matice $\boldsymbol{A}$ cykl $\Pi_1 = (1, 2, \ldots, i)$ a na její sloupce cykl $\Pi_2 = (1, 2, \ldots, k)$, dostaneme matici

$$\boldsymbol{C} = \begin{pmatrix} a_{ik}, & a_{i2}, & \ldots, & a_{i,k-1}, & a_{i,k+1}, & \ldots, & a_{in} \\ a_{1k}, & a_{11}, & \ldots, & a_{1,k-1}, & a_{1,k+1}, & \ldots, & a_{1n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{i-1,k}, & a_{i-1,2}, & \ldots, & a_{i-1,k-1}, & a_{i-1,k+1}, & \ldots, & a_{i-1,n} \\ a_{i+1,k}, & a_{i+1,2}, & \ldots, & a_{i+1,k-1}, & a_{i+1,k+1}, & \ldots, & a_{i+1,n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{nk}, & a_{n1}, & \ldots, & a_{n,k-1}, & a_{n,k+1}, & \ldots, & a_{nn} \end{pmatrix}.$$

Podle věty 6.15 je zn $\Pi_1 = (-1)^{i-1}$, zn $\Pi_2 = (-1)^{k-1}$, takže podle důsledku 7.7 a poznámky 7.4 je $\det \boldsymbol{C} = (-1)^{i-1}(-1)^{k-1}\det \boldsymbol{A} = (-1)^{i+k}\det \boldsymbol{A}$, a tedy zřejmě $\det \boldsymbol{A} = (-1)^{i+k}\det \boldsymbol{C}$. Podle předchozí části je $C_{11} = M_{ik}$, kde C_{11} značí algebraický doplněk prvku $c_{11} = a_{ik}$ v matici $\boldsymbol{C}$. Stejným způsobem, jako jsme na začátku důkazu rozepsali determinant matice $\boldsymbol{A}$ na součet n sčítanců pomocí j-tého řádku, můžeme determinant matice $\boldsymbol{C} = (c_{ij})$ rozepsat podle prvního řádku takto: $\det \boldsymbol{C} = c_{11}D_{11} + c_{12}D_{12} + \cdots + c_{1n}D_{1n}$, kde $C_{11} = D_{11}$ podle předchozí části důkazu. Celkem tedy máme $\det \boldsymbol{A} = a_{i1}B_{i1} + a_{i2}B_{i2} + \ldots a_{ik}B_{ik} + \cdots + a_{in}B_{in} = (-1)^{i+k}\det \boldsymbol{C} = (-1)^{i+k}(c_{11}D_{11} + c_{12}D_{12} + \cdots + c_{1n}D_{1n}) = (-1)^{i+k}(a_{ik}M_{ik} + a_{i2}D_{12} + \cdots + a_{in}D_{1n})$.

Vzhledem k tomu, že součinitelé u prvků a_{ik} vznikají vytknutím tohoto prvku ze všech sčítanců, které jej obsahují, a to jak v matici $\boldsymbol{A}$, tak v matici $\boldsymbol{C}$, je tento součinitel jednoznačně určen, takže $B_{ik} = (-1)^{i+k}M_{ik} = A_{ik}$ a věta je dokázána. ■

Věta o rozvoji determinantu podle i-tého řádku, $\det \boldsymbol{A} = \sum_{k=1}^{n} a_{ik}A_{ik}$ má praktický význam pro numerický výpočet determinantu matice $\boldsymbol{A}$ zejména v případě, kdy se v i-tém řádku vyskytuje „hodně" nulových prvků, neboť v tomto případě řada sčítanců vypadne. Speciálně, je-li $a_{ij} \neq 0$ a $a_{ik} = 0$ pro všechna $k \neq j$, $k = 1, 2, \ldots, n$, pak $\det \boldsymbol{A} = a_{ij}A_{ij}$ a výpočet se redukuje na výpočet determinantu matice stupně o jedničku nižšího. Naším dalším cílem bude ukázat, že každou čtvercovou matici lze převést na takovýto tvar, aniž se determinant změní.

7.12. Věta. *Buď $\boldsymbol{A}$ čtvercová matice stupně n nad tělesem T. Jestliže matice $\boldsymbol{B}$ vznikne z matice $\boldsymbol{A}$ vynásobením i-tého řádku prvkem $c \in T$ pak $\det \boldsymbol{B} = c \det \boldsymbol{A}$ čili $[\![\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, c\boldsymbol{a}_i, \ldots, \boldsymbol{a}_n]\!] = c[\![\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_n]\!]$.*

Důkaz. Podle věty o rozvoji determinantu podle i-tého řádku máme $[\![\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, c\boldsymbol{a}_i, \ldots, \boldsymbol{a}_n]\!] = \sum_{k=1}^{n} ca_{ik}A_{ik} = c\sum_{k=1}^{n} a_{ik}A_{ik} = c[\![\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_n]\!]$. ■

7.13. Věta. *Buď $\boldsymbol{A}$ čtvercová matice stupně n nad tělesem T. Jestliže i-tý řádek $\boldsymbol{a}_i$ matice $\boldsymbol{A}$ je součtem dvou vektorů, $\boldsymbol{a}_i = \boldsymbol{b}_i + \boldsymbol{c}_i$, kde $\boldsymbol{b}_i = (b_{i1}, b_{i2}, \ldots, b_{in})$, $\boldsymbol{c}_i = (c_{i1}, c_{i2}, \ldots, c_{in})$, pak $[\![\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_n]\!] = [\![\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{b}_i, \ldots, \boldsymbol{a}_n]\!] + [\![\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{c}_i, \ldots, \boldsymbol{a}_n]\!]$.*

Důkaz. Podle věty o rozvoji determinantu podle řádku máme $[\![\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_n]\!] = \sum_{k=1}^{n} a_{ik}A_{ik} = \sum_{k=1}^{n}(b_{ik} + c_{ik})A_{ik} = \sum_{k=1}^{n} b_{ik}A_{ik} + \sum_{k=1}^{n} c_{ik}A_{ik} = [\![\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{b}_i, \ldots, \boldsymbol{a}_n]\!] + [\![\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{c}_i, \ldots, \boldsymbol{a}_n]\!]$. ■

7.14. Věta. *Buď $\boldsymbol{A}$ čtvercová matice stupně n nad tělesem T. Přičteme-li k libovolnému řádku matice $\boldsymbol{A}$ libovolnou lineární kombinaci řádků ostatních, determinant se nezmění.*

Důkaz. Vzhledem k tomu, že při vzájemné výměně dvou řádků změní determinant podle věty 7.6 pouze znaménko, můžeme bez újmy na obecnosti předpokládat, že k vektoru $\boldsymbol{a}_1$ přičteme vektor $\boldsymbol{b} = \sum_{i=2}^{n} r_i\boldsymbol{a}_i$. Podle vět 7.12, 7.13 a 7.8 pak platí $[\![\boldsymbol{a}_1 + \boldsymbol{b}, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n]\!] = [\![\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n]\!] + \sum_{i=2}^{n} r_i[\![\boldsymbol{a}_i, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n]\!] = [\![\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n]\!]$. ■

7.15. Příklad. Právě dokázaná věta je spolu s větou 7.11 o rozvoji determinantu podle řádku (sloupce) důležitým nástrojem pro numerický výpočet determinantu.

Pomocí elementárních transformací na řádky (sloupce) determinantu se snažíme nejprve dosáhnout toho, aby v některém řádku či sloupci byly samé nuly, až na nejvýše jeden prvek. Rozvojem podle příslušného řádku či sloupce pak dosáhneme snížení stupně determinantu o jedničku a stejným způsobem pokračujeme dále, až dostaneme determinant stupně 2 nebo 3, který vypočteme podle odstavce 7.5. Spočtěme determinant

$$\begin{vmatrix} 1, & 2, & 1, & 3, & 1, & -1 \\ 2, & 1, & 1, & 3, & -1, & 2 \\ 3, & -1, & 2, & -1, & 1, & 2 \\ -1, & 2, & -1, & 3, & -2, & -3 \\ -3, & -1, & -2, & 1, & 2, & -1 \\ -2, & 1, & 1, & -2, & 1, & -2 \end{vmatrix}.$$

Řešení: Jest

$$\begin{vmatrix} 1, & 2, & 1, & 3, & 1, & -1 \\ 2, & 1, & 1, & 3, & -1, & 2 \\ 3, & -1, & 2, & -1, & 1, & 2 \\ -1, & 2, & -1, & 3, & -2, & -3 \\ -3, & -1, & -2, & 1, & 2, & -1 \\ -2, & 1, & 1, & -2, & 1, & -2 \end{vmatrix} = \begin{vmatrix} 1, & 2, & 1, & 3, & 1, & -1 \\ 0, & -3, & -1, & -3, & -3, & 4 \\ 0, & -7, & -1, & -10, & -2, & 5 \\ 0, & 4, & 0, & 6, & -1, & -4 \\ 0, & 5, & 1, & 10, & 5, & -4 \\ 0, & 5, & 3, & 4, & 3, & -4 \end{vmatrix} = \begin{vmatrix} -3, & -1, & -3, & -3, & 4 \\ -7, & -1, & -10, & -2, & 5 \\ 4, & 0, & 6, & -1, & -4 \\ 5, & 1, & 10, & 5, & -4 \\ 5, & 3, & 4, & 3, & -4 \end{vmatrix} =$$

$$\begin{vmatrix} 2, & 0, & 7, & 2, & 0 \\ -2, & 0, & 0, & 3, & 1 \\ 4, & 0, & 6, & -1, & -4 \\ 5, & 1, & 10, & 5, & -4 \\ -10, & 0, & -26, & -12, & 8 \end{vmatrix} = \begin{vmatrix} 2, & 7, & 2, & 0 \\ -2, & 0, & 3, & 1 \\ 4, & 6, & -1, & -4 \\ -10, & -26, & -12, & 8 \end{vmatrix} = \begin{vmatrix} 2, & 7, & 2, & 0 \\ 0, & 0, & 0, & 1 \\ -4, & 6, & 11, & -4 \\ 6, & -26, & -36, & 8 \end{vmatrix} =$$

$$\begin{vmatrix} 2, & 7, & 2 \\ -4, & 6, & 11 \\ 6, & -26, & -36 \end{vmatrix} = \begin{vmatrix} 2, & 7, & 2 \\ 0, & 20, & 15 \\ 0, & -47, & -42 \end{vmatrix} = -2 \cdot 5 \begin{vmatrix} 4, & 3 \\ 47, & 42 \end{vmatrix} = -10(168 - 141) = -270.$$

7.16. Věta. *Buď $\boldsymbol{A} = (a_{ij})$ matice typu (m, n) nad tělesem T a nechť pro některé $h = 1, 2, \ldots, \min\{m, n\}$ je subdeterminant*

$$A_h = \begin{vmatrix} a_{11}, & a_{12}, & \ldots, & a_{1h} \\ a_{21}, & a_{22}, & \ldots, & a_{2h} \\ \ldots & \ldots & \ldots & \ldots \\ a_{h1}, & a_{h2}, & \ldots, & a_{hh} \end{vmatrix} \neq 0,$$

přičemž každý subdeterminant matice $\boldsymbol{A}$ stupně $h' > h$ je roven nule. Jsou-li $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m$ řádkové vektory matice $\boldsymbol{A}$, pak $\langle \boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m \rangle = \langle \boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_h \rangle$.

Důkaz. Protože zřejmě $\langle \boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_h \rangle \subseteq \langle \boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m \rangle$, stačí podle definice lineárního obalu 1.9 ukázat, že $\boldsymbol{a}_{h+1}, \ldots, \boldsymbol{a}_m \in \langle \boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m \rangle$, tj. vzhledem k větě 1.11, že vektory $\boldsymbol{a}_{h+1}, \ldots, \boldsymbol{a}_m$ jsou lineárními kombinacemi vektorů $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_h$. Pro každé $i = h + 1, \ldots, m$ a každé $j = 1, 2, \ldots, n$ je

$$\begin{vmatrix} a_{11}, & a_{12}, & \dots, & a_{1h} & a_{1j} \\ a_{21}, & a_{22}, & \dots, & a_{2h} & a_{2j} \\ \dots & \dots & \dots & \dots & \\ a_{h1}, & a_{h2}, & \dots, & a_{hh} & a_{hj} \\ a_{i1}, & a_{i2}, & \dots, & a_{ih} & a_{ij} \end{vmatrix} = 0,$$

neboť pro $j = 1, 2, \dots, h$ má determinant dva sloupce stejné, a je tudíž nulový podle vět 7.3 a 7.7, zatímco pro $j = h+1, \dots, n$ se jedná o subdeterminant matice $\boldsymbol{A}$ stupně $h+1$ který je nulový podle předpokladu. Rozvojem tohoto determinantu podle posledního sloupce dostaneme $a_{1j}B_1 + a_{2j}B_2 + \dots a_{hj}B_h + a_{ij}A_h = 0$, přičemž tato rovnost platí pro všechna $j = 1, 2, \dots, n$. Kromě toho, prvky $B_1, B_2, \dots, B_h, A_h \in T$ nezávisí na indexu j, jsou utvořeny pouze z prvních h sloupců vyšetřovaného determinantu. Přepíšeme-li nyní poslední rovnost ve vektorovém tvaru, dostaneme $B_1\boldsymbol{a}_1 + B_2\boldsymbol{a}_2 + \dots + B_h\boldsymbol{a}_h + A_h\boldsymbol{a}_i = 0$, odkud $\boldsymbol{a}_i = -\frac{B_1}{A_h}\boldsymbol{a}_1 - \frac{B_2}{A_h}\boldsymbol{a}_2 - \dots - \frac{B_h}{A_h}\boldsymbol{a}_h$ vzhledem k tomu, že $A_h \neq 0$ podle předpokladu. ∎

7.17. Poznámka. Buďte $\boldsymbol{a}_i = (a_{i1}, a_{i2}, \dots, a_{in})$, $i = 1, 2, \dots, m$, vektory z aritmetického vektorového prostoru T^n. Vzhledem k tomu, že operace s aritmetickými vektory se provádějí po složkách, nezávisí lineární závislost či nezávislost těchto vektorů na pořadí složek, pokud bychom pořadí složek měnili ve všech vektorech stejně. Přesněji řečeno, jedná se o následující skutečnost. Buď $\boldsymbol{A} = (a_{ij})$ matice typu (m, n), jejíž řádkové vektory jsou právě $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_m$. Provedeme-li na sloupce matice $\boldsymbol{A}$ libovolnou permutaci $\Pi \in S_n$, dostaneme matici $\boldsymbol{B}$ s řádkovými vektory $\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_m$. Pak vektory $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_m$ jsou zřejmě lineárně nezávislé (závislé) právě tehdy, jsou-li lineárně nezávislé (závislé) vektory $\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_m$. Kromě toho vektor $\boldsymbol{a}_m$ je lineární kombinací vektorů $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_{m-1}$, $\boldsymbol{a}_m = \sum_{i=1}^{m-1} r_i\boldsymbol{a}_i$, právě když vektor $\boldsymbol{b}_m$ je lineární kombinací vektorů $\boldsymbol{b}_1, , \dots, \boldsymbol{b}_{m-1}$, a to se stejnými koeficienty, $\boldsymbol{b}_m = \sum_{i=1}^{m-1} r_i\boldsymbol{b}_i$. Uvědomme si ještě jeden důsledek operací po složkách. Jestliže matice $\boldsymbol{C}$ vznikne z matice $\boldsymbol{A}$ vynecháním některých sloupců a řádky matice $\boldsymbol{C}$ jsou lineárně nezávislé, pak jsou lineárně nezávislé i řádky $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_m$ matice $\boldsymbol{A}$. Idea důkazu je velmi jednoduchá, „vybrané" složky vektorů $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_m$ stačí k tomu, aby lineární kombinace těchto vektorů rovná nulovému vektoru byla triviální. Připomeňme ještě, že poslední tvrzení můžeme formulovat také takto: Jsou-li řádkové vektory matice $\boldsymbol{A}$ lineárně závislé, pak jsou lineárně závislé i řádkové vektory matice $\boldsymbol{C}$.

7.18. Věta. *Buď $\boldsymbol{A} = (a_{ij})$ čtvercová matice stupně n nad tělesem T. Pak $\det \boldsymbol{A} = 0$, právě když řádkové vektory matice $\boldsymbol{A}$ jsou lineárně závislé.*

Důkaz. Předpokládejme nejprve, že řádky $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n$ matice $\boldsymbol{A}$ jsou lineárně závislé, tj. že existuje netriviální lineární kombinace $\sum_{i=1}^{n} r_i\boldsymbol{a}_i$ těchto vektorů rovná nulovému vektoru. Vzhledem k tomu, že při provedení nějaké permutace na řádky matice $\boldsymbol{A}$ její determinant podle důsledku 7.7 nejvýše změní znaménko, můžeme bez újmy na obecnosti předpokládat, že $r_1 \neq 0$. Pak podle vět 7.12 a 7.14 máme $|\boldsymbol{A}| = [\![\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n]\!] = \frac{1}{r_1}[\![r_1\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n]\!] = \frac{1}{r_1}[\![\sum_{i=1}^{n} r_i\boldsymbol{a}_i, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n]\!] = \frac{1}{r_1}[\![0, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n]\!] = \frac{1}{r_1}[\![0 \cdot a_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n]\!] = \frac{1}{r_1} \cdot 0[\![\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n]\!] = 0$.

Předpokládejme tedy naopak, že $\det \boldsymbol{A} = 0$, a ukažme, že řádky $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n$ matice $\boldsymbol{A}$ jsou lineárně závislé. Jsou-li všechny subdeterminanty (všech stupňů) matice $\boldsymbol{A}$ nulové, jsou speciálně všechny subdeterminanty matice $\boldsymbol{A}$ stupně 1 rovny nule, takže $\boldsymbol{A}$ je nulová matice a tvrzení je zřejmé. V opačném případě zřejmě existuje číslo $1 \neq h < n$ takové, že některý subdeterminant matice $\boldsymbol{A}$ stupně h je nenulový a všechny subdeterminanty stupně h' většího než h jsou rovny nule. Vzhledem k poznámce 7.17 a důsledku 7.7 můžeme jistě předpokládat, že

$$A_h = \begin{vmatrix} a_{11}, & a_{12}, & \dots, & a_{1h} \\ a_{21}, & a_{22}, & \dots, & a_{2h} \\ \dots & \dots & \dots & \dots \\ a_{h1}, & a_{h2}, & \dots, & a_{hh} \end{vmatrix} \neq 0.$$

Podle věty 7.16 je $\langle \boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n \rangle = \langle \boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_h \rangle$, takže $\dim\langle \boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n \rangle \leq h < n$ podle věty 2.12 a vektory $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n$ jsou lineárně závislé podle věty 2.17. ■

7.19. Věta. *Buď $\boldsymbol{A} = (a_{ij})$ matice typu (m, n) nad tělesem T. Pak $h(\boldsymbol{A}) = h$, právě když existuje nenulový subdeterminant matice $\boldsymbol{A}$ stupně h a každý subdeterminant matice $\boldsymbol{A}$ stupně většího než h je roven nule.*

Důkaz. Předpokládejme nejprve, že $h(\boldsymbol{A}) = h$, tj. $\dim\langle \boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_m \rangle$, kde $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_m$ jsou řádky matice $\boldsymbol{A}$, je rovna h. Buď $h < h' \leq \min(m, n)$ a buď

$$A_{h'} = \begin{vmatrix} a_{i_1 j_1}, & a_{i_1 j_2}, & \dots, & a_{i_1 j_{h'}} \\ a_{i_2 j_1}, & a_{i_2 j_2}, & \dots, & a_{i_2 j_{h'}} \\ \dots & \dots & \dots & \dots \\ a_{i_{h'} j_1}, & a_{i_{h'} j_2}, & \dots, & a_{i_{h'} j_{h'}} \end{vmatrix}$$

libovolný subdeterminant matice $\boldsymbol{A}$ stupně h'. Podle věty 2.17 jsou řádky $\boldsymbol{a}_{i_1}, \boldsymbol{a}_{i_2}, \dots, \boldsymbol{a}_{i_{h'}}$ lineárně závislé, takže ve smyslu poznámky 7.17 jsou lineárně závislé i řádky determinantu $A_{h'}$ a $A_{h'} = 0$ podle předchozí věty 7.18. Alespoň jeden subdeterminant matice $\boldsymbol{A}$ stupně h je nenulový, neboť v opačném případě by z věty 7.16 plynulo, že $h(\boldsymbol{A}) = \dim\langle \boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_m \rangle < h$.

Buď tedy naopak splněna podmínka věty a buď

$$A_h = \begin{vmatrix} a_{i_1 j_1}, & a_{i_1 j_2}, & \dots, & a_{i_1 j_h} \\ a_{i_2 j_1}, & a_{i_2 j_2}, & \dots, & a_{i_2 j_h} \\ \dots & \dots & \dots & \dots \\ a_{i_h j_1}, & a_{i_h j_2}, & \dots, & a_{i_h j_h} \end{vmatrix} \neq 0.$$

Podle věty 7.16 je $\langle \boldsymbol{a}_{i_1}, \boldsymbol{a}_{i_2}, \dots, \boldsymbol{a}_{i_h} \rangle = \langle \boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_m \rangle$. Mimoto podle věty 7.18 jsou řádky determinantu A_h lineárně nezávislé, takže podle poznámky 7.17 jsou lineárně nezávislé i vektory $\boldsymbol{a}_{i_1}, \boldsymbol{a}_{i_2}, \dots, \boldsymbol{a}_{i_h}$ To ale znamená, že $h(\boldsymbol{A}) = \dim\langle \boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_m \rangle = \dim\langle \boldsymbol{a}_{i_1}, \boldsymbol{a}_{i_2}, \dots, \boldsymbol{a}_{i_h} \rangle = h$ a jsme hotovi. ■

7.20. Poznámka. Předchozí věta charakterizuje hodnost matice $\boldsymbol{A}$ typu (m, n) pomocí maximálního nenulového subdeterminantu této matice. Uvědomíme-li si, že podle věty 7.3 je $\det \boldsymbol{B} = \det \boldsymbol{B}^T$, pro každou čtvercovou matici $\boldsymbol{B}$, vidíme, že matice $\boldsymbol{A}$ má nenulové subdeterminanty stejných stupňů jako matice transponovaná $\boldsymbol{A}^T$. Jinými slovy to znamená, že $h(\boldsymbol{A}) = h(\boldsymbol{A}^T)$, a dostáváme tak jiný důkaz věty 5.5.

7.21. Věta. (O násobení determinantů.) *Jsou-li* $\boldsymbol{A} = (a_{ij})$ *a* $\boldsymbol{B} = (b_{ij})$ *dvě čtvercové matice stupně* n *nad tělesem* T, *pak* $\det(\boldsymbol{AB}) = \det \boldsymbol{A} \cdot \det \boldsymbol{B}$.

Důkaz. Označme $\boldsymbol{AB} = \boldsymbol{C} = (c_{ij})$ součin matic $\boldsymbol{A}$ a $\boldsymbol{B}$. Označíme-li $\boldsymbol{c}_1, \boldsymbol{c}_2, \dots, \boldsymbol{c}_n$ řádkové vektory matice $\boldsymbol{C}$ a $\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n$ řádkové vektory matice $\boldsymbol{B}$, pak podle věty 4.10 a poznámky 4.11 máme $\boldsymbol{c}_i = \sum_{k=1}^n a_{ik}\boldsymbol{b}_k$ pro každé $i = 1, 2, \dots, n$. Několikanásobným použitím vět 7.12 a 7.13 dostáváme $|\boldsymbol{AB}| = [\![\boldsymbol{c}_1, \boldsymbol{c}_2, \dots, \boldsymbol{c}_n]\!] = [\![\sum_{k_1=1}^n a_{1k_1}\boldsymbol{b}_{k_1}, \sum_{k_2=1}^n a_{2k_2}\boldsymbol{b}_{k_2}, \dots, \sum_{k_n=1}^n a_{nk_n}\boldsymbol{b}_{k_n}]\!] = \sum_{(k_1,k_2,\dots,k_n)} a_{1k_1}a_{2k_2}\dots a_{nk_n}[\![\boldsymbol{b}_{k_1}, \boldsymbol{b}_{k_2}, \dots, \boldsymbol{b}_{k_n}]\!]$, kde sčítáme přes všechny možné n-tice (s opakováním) $(k_1, k_2, \dots, k_n)$ utvořené z čísel $1, 2, \dots, n$. Pokud jsou některé dva prvky z $k_1, k_2, \dots, k_n$ stejné, je determinant $[\![\boldsymbol{b}_{k_1}, \boldsymbol{b}_{k_2}, \dots, \boldsymbol{b}_{k_n}]\!]$ roven nule podle věty 7.8. To ale znamená, že ve výše daném součtu se můžeme omezit jen na ty sčítance, kde prvky $k_1, k_2, \dots, k_n$ jsou navzájem různé, a tedy kdy n-tice $(k_1, k_2, \dots, k_n)$ je nějaké pořadí čísel $1, 2, \dots, n$. Podle důsledku 7.7 je pak $[\![\boldsymbol{b}_{k_1}, \boldsymbol{b}_{k_2}, \dots, \boldsymbol{b}_{k_n}]\!] = \operatorname{zn}\Pi[\![\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n]\!]$ $= \operatorname{zn}\Pi \det \boldsymbol{B}$, kde $\Pi = \begin{pmatrix} 1, & 2, & \dots, & n \\ k_1, & k_2, & \dots, & k_n \end{pmatrix}$. Odtud dále dostáváme $\det(\boldsymbol{AB}) = \sum_{\Pi\in S_n} a_{1k_1}a_{2k_2}\dots a_{nk_n}[\![\boldsymbol{b}_{k_1}, \boldsymbol{b}_{k_2}, \dots, \boldsymbol{b}_{k_n}]\!] = \sum_{\Pi\in S_n} a_{1k_1}a_{2k_2}\dots a_{nk_n}\operatorname{zn}\Pi\det\boldsymbol{B} = \det\boldsymbol{B}\sum_{\Pi\in S_n}\operatorname{zn}\Pi a_{1k_1}a_{2k_2}\dots a_{nk_n}$ kde se sčítá přes všechny permutace tvaru $\Pi = \begin{pmatrix} 1, & 2, & \dots, & n \\ k_1, & k_2, & \dots, & k_n \end{pmatrix} \in S_n$. Použijeme-li nyní definici determinantu 7.1, pak nakonec dostaneme $\det(\boldsymbol{AB}) = \det\boldsymbol{A}\cdot\det\boldsymbol{B}$. ∎

7.22. Příklady. 1. V závislosti na parametru n spočtěme determinant stupně n

$$|\boldsymbol{C}| = \begin{vmatrix} a_1 + b_1, & a_1 + b_2, & \dots, & a_1 + b_n \\ a_2 + b_1, & a_2 + b_2, & \dots, & a_2 + b_n \\ \dots & \dots & \dots & \dots \\ a_n + b_1, & a_n + b_2, & \dots, & a_n + b_n \end{vmatrix},$$

kde a_i, b_i, $i = 1, 2, \dots, n$ jsou libovolné prvky tělesa T.

Ř e š e n í : Snadno ověříme, že daná matice je součinem dvou matic, totiž

$$\boldsymbol{A}\cdot\boldsymbol{B} = \begin{pmatrix} a_1, & 1, & ,0, & \dots, & 0 \\ a_2, & 1, & ,0, & \dots, & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_n, & 1, & ,0, & \dots, & 0 \end{pmatrix} \begin{pmatrix} 1, & 1, & \dots, & 1 \\ b_1, & b_2, & \dots, & b_n \\ \dots & \dots & \dots & \dots \\ 0, & 0, & \dots, & 0 \end{pmatrix}.$$

Podle věty o násobení determinantů je tedy $|\boldsymbol{C}| = |\boldsymbol{A}||\boldsymbol{B}|$, takže $|\boldsymbol{C}| = 0$ pro všechna $n \geq 3$ vzhledem k tomu, že matice $\boldsymbol{A}$ (matice $\boldsymbol{B}$) má v tomto případě alespoň jeden nulový sloupec (řádek). Ve zbývajících dvou případech pak je $|\boldsymbol{C}| = a_1 + b_1$ pro $n = 1$ a $|\boldsymbol{C}| = (a_1 - a_2)(b_2 - b_1)$ pro $n = 2$.

2. Pro libovolná reálná čísla x, y spočtěme determinant

$$|\boldsymbol{A}| = \begin{vmatrix} \cos x, & \sin x\cos y, & \sin x\sin y \\ -\sin x, & \cos x\cos y, & \cos x\sin y \\ 0, & -\sin y, & \cos y \end{vmatrix}.$$

Ř e š e n í : a) Nejprve spočteme $\det \boldsymbol{A}$ pomocí Sarrusova pravidla (viz 7.5). Jest $|\boldsymbol{A}| = \cos^2 x\cos^2 y + \sin^2 x\sin^2 y + \cos^2 x\sin^2 y + \sin^2 x\cos^2 y = \cos^2 x(\cos^2 y + \sin^2 y) + \sin^2 x(\sin^2 y + \cos^2 y) = 1$.

b) Spočteme součin $\boldsymbol{B} = \boldsymbol{A} \cdot \boldsymbol{A}^T$.

$$\begin{pmatrix} \cos x, & \sin x \cos y, & \sin x \sin y \\ -\sin x, & \cos x \cos y, & \cos x \sin y \\ 0, & -\sin y, & \cos y \end{pmatrix} \begin{pmatrix} \cos x, & -\sin x, & 0 \\ \sin x \cos y, & \cos x \cos y, & -\sin y \\ \sin x \sin y, & \cos x \sin y, & \cos y \end{pmatrix} = \begin{pmatrix} 1, & 0, & 0, \\ 0, & 1, & 0 \\ 0, & 0, & 1 \end{pmatrix}.$$

Podle věty o násobení determinantů 7.21 a věty 7.3 je $1 = \det \boldsymbol{B} = \det(\boldsymbol{A}\boldsymbol{A}^T) = \det \boldsymbol{A} \cdot \det \boldsymbol{A}^T = (\det \boldsymbol{A})^2$, takže $\det \boldsymbol{A} = \pm 1$ a zbývá rozhodnout o znaménku $\det \boldsymbol{A}$. Protože však determinant nezávisí na proměnných x a y, určíme znaménko dosazením třeba $x = y = 0$. V tomto případě je zřejmě $\boldsymbol{A} = \boldsymbol{E}$, a tedy $\det \boldsymbol{A} = 1$.

8.1. Lemma. *Buďte $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$ čtvercové matice stupně n takové, že $\boldsymbol{BA} = \boldsymbol{E} = \boldsymbol{AC}$. Pak $\boldsymbol{B} = \boldsymbol{C}$.*

Důkaz. Podle věty 4.7 (iv) a (ii) jest $\boldsymbol{B} = \boldsymbol{BE} = \boldsymbol{B}(\boldsymbol{AC}) = (\boldsymbol{BA})\boldsymbol{C} = \boldsymbol{EC} = \boldsymbol{C}$. ■

8.2. Definice. Buďte $\boldsymbol{A}$, $\boldsymbol{B}$ čtvercové matice stupně n. Řekneme, že $\boldsymbol{B}$ je *inverzní matice* k matici $\boldsymbol{A}$ nebo že $\boldsymbol{A}$ je inverzní matice k matice $\boldsymbol{B}$, jestliže $\boldsymbol{BA} = \boldsymbol{AB} = \boldsymbol{E}$. Inverzní matice k matici $\boldsymbol{A}$, pokud existuje, je podle předchozího lemmatu určena jednoznačně a značí se $\boldsymbol{A}^{-1}$. Matice $\boldsymbol{A}$, k níž existuje inverzní matice, se nazývá *regulární*, v opačném případě se $\boldsymbol{A}$ nazývá *singulární*.

8.3. Příklady. 1. Jednotková matice $\boldsymbol{E}$ stupně n je podle věty 4.7 (iv) regulární, neboť $\boldsymbol{EE} = \boldsymbol{E}$, a tedy $\boldsymbol{E}^{-1} = \boldsymbol{E}$. Na druhé straně pro nulovou matici $\mathbf{0}$ a libovolnou matici $\boldsymbol{A}$ stupně n máme $\mathbf{0}\boldsymbol{A} = \boldsymbol{A}\mathbf{0} = \mathbf{0}$, takže nulová matice je singulární.

2. Matice

$$\boldsymbol{A} = \begin{pmatrix} 1, & 2, & 3 \\ 2, & 3, & 1 \\ 3, & 1, & -17 \end{pmatrix}$$

je regulární. Položme

$$\boldsymbol{B} = \begin{pmatrix} a, & b, & c \\ d, & e, & f \\ g, & h, & i \end{pmatrix}$$

a hledejme matici $\boldsymbol{B}$ tak, aby $\boldsymbol{BA} = \boldsymbol{E}$. Vynásobením dostaneme celkem tři nehomogenní soustavy lineárních rovnic

$$\begin{aligned} a + 2b + 3c &= 1, & d + 2e + 3f &= 0, & g + 2h + 3i &= 0, \\ 2a + 3b + c &= 0, & 2d + 3e + f &= 1, & 2g + 3h + i &= 0, \\ 3a + b - 17c &= 0, & 3d + e - 17f &= 0, & 3g + h - 17i &= 1, \end{aligned}$$

které můžeme řešit Jordanovou eliminační metodou současně tak, že místo jednoho sloupce pravých stran napíšeme všechny tři. To můžeme učinit vzhledem k tomu, že výrazy na levých stranách jsou ve všech třech případech stejné. Máme tedy

$$\left(\begin{array}{ccc|ccc} 1, & 2, & 3 & 1, & 0, & 0 \\ 2, & 3, & 1 & 0, & 1, & 0 \\ 3, & 1, & -17 & 0, & 0, & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1, & 2, & 3 & 1, & 0, & 0 \\ 0, & -1, & -5 & -2, & 1, & 0 \\ 0, & -5, & -26 & -3, & 0, & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1, & 2, & 3 & 1, & 0, & 0 \\ 0, & 1, & 5 & 2, & -1, & 0 \\ 0, & 0, & -1 & 7, & -5, & 1 \end{array}\right) \sim$$

$$\left(\begin{array}{ccc|ccc} 1, & 2, & 0 & 22, & -15, & 3 \\ 0, & 1, & 0 & 37, & -26, & 5 \\ 0, & 0, & 1 & -7, & 5, & -1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1, & 0, & 0 & -52, & 37, & -7 \\ 0, & 1, & 0 & 37, & -26, & 5 \\ 0, & 0, & 1 & -7, & 5, & -1 \end{array}\right).$$

Vidíme tedy, že

$$B = \begin{pmatrix} -52, & 37, & -7 \\ 37, & -26, & 5 \\ -7, & 5, & -1 \end{pmatrix}$$

je inverzní matice k matici $\boldsymbol{A}$, neboť, jak se snadno ověří, je $\boldsymbol{AB} = \boldsymbol{BA} = \boldsymbol{E}$.

3. Ukažme, že matice

$$A = \begin{pmatrix} 1, & 3, & 2 \\ 2, & 3, & 1 \\ 3, & 1, & -2 \end{pmatrix}$$

je singulární. Podobně jako v předchozím příkladu máme

$$\left(\begin{array}{ccc|ccc} 1, & 3, & 2 & 1, & 0, & 0 \\ 2, & 3, & 1 & 0, & 1, & 0 \\ 3, & 1, & -2 & 0, & 0, & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1, & 3, & 2 & 1, & 0, & 0 \\ 0, & -3, & -3 & -2, & 1, & 0 \\ 0, & -8, & -8 & -3, & 0, & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1, & 3, & 2 & 1, & 0, & 0 \\ 0, & -3, & -3 & -2, & 1, & 0 \\ 0, & 0, & 0 & 7, & -8, & 3 \end{array}\right),$$

odkud je již vidět, že matice (každé) soustavy má hodnost 2, zatímco hodnost rozšířené matice každé ze tří soustav je rovna 3, takže ani jedna ze tří soustav není podle Frobeniovy věty 5.6 řešitelná.

Později uvidíme, že právě použitá metoda je jednou z metod pro hledání inverzních matic. Zároveň jsem viděli, že regulárnost čtvercových matic souvisí s jejich hodností. Naším nejbližším cílem bude ukázat, že čtvercová matice stupně n je regulární, právě když její hodnost je rovna n.

8.4. Věta. *Buď $\boldsymbol{A}$ čtvercová matice stupně n nad tělesem T. Následující podmínky jsou ekvivalentní:*

(i) $\boldsymbol{A}$ je regulární;
(ii) $h(\boldsymbol{A}) = n$;
(iii) řádkové vektory matice $\boldsymbol{A}$ generují T^n;
(iv) sloupcové vektory matice $\boldsymbol{A}$ generují T^n;
(v) řádkové vektory matice $\boldsymbol{A}$ jsou lineárně nezávislé;
(vi) sloupcové vektory matice $\boldsymbol{A}$ jsou lineárně nezávislé;
(vii) $\det \boldsymbol{A} \neq 0$.

Důkaz. Podmínky (ii), (iii) (v) jsou ekvivalentní podle věty 2.19 a podle věty 5.5 jsou s nimi ekvivalentní i podmínky (iv) a (vi).

Z (i) plyne (ii). Je-li $\boldsymbol{A}$ regulární, existuje čtvercová matice $\boldsymbol{B}$ stupně n taková, že $\boldsymbol{BA} = \boldsymbol{E}$. Označíme-li $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n$ řádky matice $\boldsymbol{A}$ a $\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n$ řádky matice $\boldsymbol{B}$, pak pro $M = (\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n) \in (T^n)^n$ je $\boldsymbol{b}_i * M = \boldsymbol{e}_i$ pro každé $i = 1, 2, \dots, n$. Protože zřejmě $T^n = \langle \boldsymbol{b}_1 * M, \boldsymbol{b}_2 * M, \dots, \boldsymbol{b}_n * M \rangle \subseteq \langle \boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n \rangle$, vektory $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n$ generují T^n, a jsou tudíž lineárně nezávislé podle věty 2.19, takže $h(\boldsymbol{A}) = n$.

Z (ii) plyne (i). Podle důsledku 2.26 existují lineárně nezávislé vektory $\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n \in T^n$ takové, že $\boldsymbol{b}_i * M = \boldsymbol{e}_i$ pro každé $i = 1, 2, \dots, n$. Označíme-li $\boldsymbol{B}$ čtvercovou matici stupně n s řádky $\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n$, je $\boldsymbol{BA} = \boldsymbol{E}$ podle věty 4.10. Provedeme-li nyní stejnou úvahu s maticí $\boldsymbol{B}$, dostaneme existenci čtvercové matice $\boldsymbol{C}$ stupně n

takové, že $CB = E$. Podle lemmatu 8.1 je $C = A$, takže $B = A^{-1}$ a matice A je regulární.

Z (i) plyne (vii). Podle věty o násobení determinantů 7.21 jest $\det A \cdot \det A^{-1} = \det E = 1$, a tedy $\det A \neq 0$.

Z (vii) plyne (v). Jestliže $\det A \neq 0$, jsou řádky matice A lineárně nezávislé podle věty 7.18 a důkaz věty je dokončen. ■

8.5. Důsledek. *Buď A čtvercová matice stupně n nad tělesem T. Pak A je regulární, právě když existuje čtvercová matice B (C) téhož stupně n taková, že $BA = E$ ($AC = E$). V tomto případě je B (C) inverzní maticí k matici A.*

Důkaz. Z věty o násobení determinantů plyne, že $\det B \neq 0$, takže B je regulární, a tedy $CB = E$ pro nějakou čtvercovou matici C. Podle lemmatu 8.1 je $C = A$ a tedy $B = A^{-1}$. Zbytek je zřejmý. ■

8.6. Věta. *Buďte A, B regulární čtvercové matice stupně n. Pak platí:*

(i) součin AB je regulární matice a platí $(AB)^{-1} = B^{-1}A^{-1}$;

(ii) matice A^{-1} je regulární a platí $(A^{-1})^{-1} = A$;

(iii) $(A^T)^{-1} = (A^{-1})^T$.

Důkaz. (i) Podle věty 4.7 máme $(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}B = E$, takže $(AB)^{-1} = B^{-1}A^{-1}$ podle předchozího důsledku.

(ii) Z rovností $AA^{-1} = A^{-1}A = E$ plyne, že A je matice inverzní k matici A^{-1}.

(iii) Podle věty 4.14 (ii) máme $A^T \cdot (A^{-1})^T = (A^{-1}A)^T = E^T = E$, takže $(A^T)^{-1} = (A^{-1})^T$ podle důsledku 8.5. ■

8.7. Definice. Buďte $M = [u_1, u_2, \dots, u_n]$ a $M' = [u'_1, u'_2, \dots, u'_n]$ dvě skupiny vektorů vektorového prostoru V a nechť M' vznikne z M elementární transformací.

(i) Jestliže $u'_j = u_j$, $j \neq i$, $j = 1, 2, \dots, n$, $u'_i = u_i + \sum\limits_{\substack{j=1\\ j\neq i}}^{n} a_{ij}u_j$, pak čtvercovou matici

$$\begin{pmatrix} 1, & 0, & \dots, & 0, & \dots, & 0 \\ 0, & 1, & \dots, & 0, & \dots, & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{i1}, & a_{i2}, & \dots, & 1, & \dots, & a_{in} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0, & 0, & \dots, & 0, & \dots, & 1 \end{pmatrix}$$

stupně n nazveme *maticí* této *elementární transformace.*

(ii) Jestliže $u'_j = u_j$, $j \neq i$, $j = 1, 2, \dots, n$, $u'_i = ru_i$, $0 \neq r \in T$, pak čtvercovou matici

$$\begin{pmatrix} 1, & 0, & \dots, & 0, & \dots, & 0 \\ 0, & 1, & \dots, & 0, & \dots, & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0, & 0, & \dots, & r, & \dots, & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0, & 0, & \dots, & 0, & \dots, & 1 \end{pmatrix}$$

stupně n nazveme *maticí* této *elementární transformace.*

8.8. Věta. *Buď $\boldsymbol{A}$ matice typu (m,n) s řádkovými vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_m$ a $\boldsymbol{A}'$ matice téhož typu (m,n), jejíž řádkové vektory $\boldsymbol{u}'_1, \boldsymbol{u}'_2, \dots, \boldsymbol{u}'_m$ vzniknou z $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_m$ elementární transformací, jejíž matice je $\boldsymbol{B}$. Pak $\boldsymbol{A}' = \boldsymbol{B}\boldsymbol{A}$.*

Důkaz. Plyne přímo z věty 4.10. ■

8.9. Poznámka. Buď $\boldsymbol{A}$ regulární čtvercová matice stupně n. Snadno se nahlédne, že matici $\boldsymbol{A}$ můžeme dostat z jednotkové matice pomocí konečného počtu elementárních transformací, takže podle věty 3.2 můžeme jednotkovou matici dostat z matice $\boldsymbol{A}$ pomocí konečného počtu elementárních transformací. Existují tedy podle předchozí věty elementární transformace s maticemi $\boldsymbol{B}_1, \boldsymbol{B}_2, \dots, \boldsymbol{B}_k$ tak, že $\boldsymbol{B}_k \boldsymbol{B}_{k-1} \dots \boldsymbol{B}_1 \boldsymbol{A} = \boldsymbol{E}$. Budeme-li tedy na řádky matice $\boldsymbol{A}$ provádět elementární transformace s maticemi $\boldsymbol{B}_1, \boldsymbol{B}_2, \dots, \boldsymbol{B}_k$ tak, abychom dostali jednotkovou matici, pak při současném provádění těchto elementárních transformací na jednotkovou matici $\boldsymbol{E}$ dostaneme matici $\boldsymbol{A}^{-1}$. V tom záleží již dříve ohlášená metoda pro hledání inverzní matice. Prakticky se tedy inverzní matice k dané regulární matici $\boldsymbol{A}$ hledá takto: Utvoříme matici $(\boldsymbol{A}|\boldsymbol{E})$ typu $(n, 2n)$, kde v prvních n sloupcích jsou sloupce matice $\boldsymbol{A}$ a ve zbývajících n sloupcích jsou sloupce jednotkové matice $\boldsymbol{E}$. Pak tuto matici konečným počtem elementárních transformací převedeme na matici tvaru $(\boldsymbol{E}|\boldsymbol{B})$ téhož typu $(n, 2n)$. Podle toho, co bylo řečeno dříve je, $\boldsymbol{B} = \boldsymbol{A}^{-1}$.

8.10. Příklad. Nalezněme inverzní matici k matici

$$\boldsymbol{A} = \begin{pmatrix} 1,-3,-2,\ 4 \\ -3,10,\ 3,-2 \\ -1,\ 4,\ 0,-5 \\ -3,11,\ 1,-2 \end{pmatrix}.$$

Ř e š e n í : Podle předchozí poznámky postupně dostaneme

$$\left(\begin{array}{rrrr|rrrr} 1,&-3,&-2,&4 & 1,&0,&0,&0 \\ -3,&10,&3,&-2 & 0,&1,&0,&0 \\ -1,&4,&0,&-5 & 0,&0,&1,&0 \\ -3,&11,&1,&-2 & 0,&0,&0,&1 \end{array}\right) \sim \left(\begin{array}{rrrr|rrrr} 1,&-3,&-2,&4 & 1,&0,&0,&0 \\ 0,&1,&-3,&10 & 3,&1,&0,&0 \\ 0,&1,&-2,&-1 & 1,&0,&1,&0 \\ 0,&2,&-5,&10 & 3,&0,&0,&1 \end{array}\right) \sim$$

$$\left(\begin{array}{rrrr|rrrr} 1,&-3,&-2,&4 & 1,&0,&0,&0 \\ 0,&1,&-3,&10 & 3,&1,&0,&0 \\ 0,&0,&1,&-11 & -2,&-1,&1,&0 \\ 0,&0,&1,&-10 & -3,&-2,&0,&1 \end{array}\right) \sim \left(\begin{array}{rrrr|rrrr} 1,&-3,&-2,&4 & 1,&0,&0,&0 \\ 0,&1,&-3,&10 & 3,&1,&0,&0 \\ 0,&0,&1,&-11 & -2,&-1,&1,&0 \\ 0,&0,&0,&1 & -1,&-1,&-1,&1 \end{array}\right) \sim$$

$$\left(\begin{array}{rrrr|rrrr} 1,&-3,&-2,&0 & 5,&4,&4,&-4 \\ 0,&1,&-3,&0 & 13,&11,&10,&-10 \\ 0,&0,&1,&0 & -13,&-12,&-10,&11 \\ 0,&0,&0,&1 & -1,&-1,&-1,&1 \end{array}\right) \sim \left(\begin{array}{rrrr|rrrr} 1,&-3,&0,&0 & -21,&-20,&-16,&18 \\ 0,&1,&0,&0 & -26,&-25,&-20,&23 \\ 0,&0,&1,&0 & -13,&-12,&-10,&11 \\ 0,&0,&0,&1 & -1,&-1,&-1,&1 \end{array}\right) \sim$$

$$\left(\begin{array}{rrrr|rrrr} 1,&0,&0,&0 & -99,&-95,&-76,&87 \\ 0,&1&0,&0 & -26,&-25,&-20,&23 \\ 0,&0,&1,&0 & -13,&-12,&-10,&11 \\ 0,&0,&0,&1 & -1,&-1,&-1,&1 \end{array}\right),$$

takže

$$A^{-1} = \begin{pmatrix} -99, -95, -76, & 87 \\ -26, -25, -20, & 23 \\ -13, -12, -10, & 11 \\ -1, \ -1, \ -1, & 1 \end{pmatrix}.$$

Na závěr tohoto odstavce si ukážeme ještě jednu metodu pro výpočet inverzní matice, která je v podstatě založena na větě 7.11 o rozvoji determinantu podle řádku.

8.11. Definice. Buď $\boldsymbol{A} = (a_{ij})$ čtvercová matice stupně n nad tělesem T. Matice $\bar{\boldsymbol{A}} = (\bar{a}_{ij})$, kde $\bar{a}_{ij} = A_{ji}$ je algebraický doplněk prvku a_{ji} v matici $\boldsymbol{A}$, se nazývá *matice adjungovaná* k matici $\boldsymbol{A}$.

8.12. Věta. *Buď $\boldsymbol{A} = (a_{ij})$ čtvercová matice stupně n nad tělesem T.*
(i) Je-li $\bar{\boldsymbol{A}} = (\bar{a}_{ij})$ matice adjungovaná k matici $\boldsymbol{A}$, pak $\boldsymbol{A}\bar{\boldsymbol{A}} = \det\boldsymbol{A} \cdot \boldsymbol{E}$;
(ii) je-li matice $\boldsymbol{A}$ regulární, pak $\boldsymbol{A}^{-1} = \frac{\bar{\boldsymbol{A}}}{|\boldsymbol{A}|}$, tj. $\boldsymbol{A}^{-1} = (b_{ij})$, kde $b_{ij} = \frac{A_{ji}}{|\boldsymbol{A}|}$.

Důkaz. (i) Označíme-li $\boldsymbol{C} = (c_{ij}) = \boldsymbol{A}\bar{\boldsymbol{A}}$ je $c_{ij} = \sum_{k=1}^{n} a_{ik}\bar{a}_{kj} = \sum_{k=1}^{n} a_{ik}A_{jk} = \delta_{ij}|\boldsymbol{A}|$ podle věty o rozvoji determinantu podle řádku 7.11.
(ii) Tvrzení plyne ihned z (i). ■

8.13. Věta. (Cramerovo pravidlo.) *Buď $\boldsymbol{A} = (a_{ij})$ regulární čtvercová matice stupně n a $\boldsymbol{b} = (b_1, b_2, \ldots, b_n) \in T^n$ buď libovolný vektor. Označme $\boldsymbol{A}_j$ matici, která vznikne z matice $\boldsymbol{A}$ nahrazením j-tého sloupce vektorem $\boldsymbol{b}$ a buď $x_j = \frac{\det \boldsymbol{A}_j}{\det \boldsymbol{A}}$, $j = 1, 2, \ldots, n$. Pak vektor $\boldsymbol{u} = (x_1, x_2, \ldots, x_n)$ je (jediným) řešením nehomogenní soustavy lineárních rovnic s rozšířenou maticí $(\boldsymbol{A}, \boldsymbol{b})$.*

Důkaz. Protože matice $\boldsymbol{A}$ je regulární, je $h(\boldsymbol{A}) = n$ podle věty 8.4 a soustava má podle důsledku 5.9 jediné řešení. Zároveň je $\det \boldsymbol{A} \neq 0$, takže výrazy pro x_j mají smysl. Vynásobme nyní i-tou rovnici soustavy $\sum_{k-1}^{n} a_{ik}x_k = b_i$ algebraickým doplňkem A_{ij} prvku a_{ij} v matici $\boldsymbol{A}$ a všechny takto získané výrazy sečtěme. Dostaneme $\sum_{i=1}^{n} A_{ij} \sum_{k=1}^{n} a_{ik}x_k = \sum_{i=1}^{n} b_i A_{ij}$. Na pravé straně rovnosti je podle věty 7.11 a poznámky 7.4 rozvoj determinantu matice $\boldsymbol{A}_j$ podle j-tého sloupce, takže na pravé straně je $\det \boldsymbol{A}_j$. Na levé straně z téhož důvodu máme $\sum_{k=1}^{n} x_k \sum_{i=1}^{n} a_{ik}A_{ij} = \sum_{k=1}^{n} x_k\delta_{kj}\det \boldsymbol{A} = x_j\det \boldsymbol{A}$, odkud tvrzení ihned plyne. ■

8.14. Poznámka. Cramerovo pravidlo není pro soustavy s větším počtem neznámých příliš výhodné, neboť vyžaduje výpočet $n + 1$ determinantů stupně n. V některých úlohách však potřebujeme znát jen jednu, případně několik málo složek řešení a v tomto případě můžeme použít Cramerova pravidla.

Buď opět $\boldsymbol{A} = (a_{ij})$ regulární čtvercová matice stupně n, $\boldsymbol{b} = (b_1, b_2, \ldots, b_n) \in T^n$, $\boldsymbol{u} = (x_1, x_2, \ldots, x_n) \in T^n$. Nehomogenní soustavu lineárních rovnic s rozšířenou maticí $(\boldsymbol{A}, \boldsymbol{b})$ můžeme zapsat v maticovém tvaru (vektor je vlastně matice typu $(1, n)$) $\boldsymbol{A}\boldsymbol{u}^T = \boldsymbol{b}^T$. Vynásobíme-li tuto (maticovou) rovnost inverzní maticí $\boldsymbol{A}^{-1}$ zleva, dostaneme pomocí věty 4.7 řešení soustavy takto: $\boldsymbol{A}^{-1}(\boldsymbol{A}\boldsymbol{u}^T) = (\boldsymbol{A}^{-1}\boldsymbol{A})\boldsymbol{u}^T = \boldsymbol{u}^T = \boldsymbol{A}^{-1}\boldsymbol{b}^T$.

Cramerovo pravidlo můžeme též použít v případě libovolné řešitelné nehomogenní soustavy lineárních rovnic s maticí $\boldsymbol{A} = (a_{ij})$ typu (m, n) a se sloupcem

$\boldsymbol{b} = (b_1, b_2, \ldots, b_m) \in T^m$ pravých stran. Je-li h hodnost matice $\boldsymbol{A}$, pak podle věty 7.19 existuje nenulový subdeterminant matice $\boldsymbol{A}$ stupně h a každý subdeterminant matice $\boldsymbol{A}$ stupně většího než h je roven nule. Jelikož neznámé můžeme libovolně přečíslovat a rovnice v soustavě libovolným způsobem přerovnat, můžeme bez újmy na obecnosti předpokládat, že

$$A_h = \begin{vmatrix} a_{11}, & a_{12}, & \ldots, & a_{1h} \\ a_{21}, & a_{22}, & \ldots, & a_{2h} \\ \ldots & \ldots & \ldots & \ldots \\ a_{h1}, & a_{h2}, & \ldots, & a_{hh} \end{vmatrix} \neq 0.$$

Danou soustavu rovnic pak můžeme přepsat ve tvaru

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1h}x_h &= b_1 - a_{1,h+1}x_{h+1} - \ldots - a_{1n}x_n, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2h}x_h &= b_2 - a_{2,h+1}x_{h+1} - \ldots - a_{2n}x_n, \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots \\ a_{h1}x_1 + a_{h2}x_2 + \ldots + a_{hh}x_h &= b_h - a_{h,h+1}x_{h+1} - \ldots - a_{hn}x_n. \end{aligned}$$

Vzhledem k tomu, že podle Frobeniovy věty 5.6 hodnost rozšířené matice je rovna h, prvních h řádků matice $(\boldsymbol{A}, \boldsymbol{b})$ generuje podprostor generovaný řádky této matice a ve smyslu poznámky 5.4 každé řešení této soustavy je řešením původní soustavy a naopak. Na tuto soustavu můžeme použít Cramerovo pravidlo, přičemž neznámé $x_{h+1}, \ldots, x_n$ můžeme volit zcela libovolně. Podívejme se nyní na pár ilustrativních příkladů.

8.15. Příklady. 1. Nad tělesem reálných čísel řešme nehomogenní soustavu lineárních rovnic s rozšířenou maticí

$$(\boldsymbol{A}, \boldsymbol{b}) = \left(\begin{array}{rrr|r} 1, & 2, & 1 & 8 \\ 2, & 3, & -1 & 5 \\ -1, & 1, & 6 & 19 \end{array}\right).$$

Ř e š e n í : a) Gaussovou eliminační metodou:

$$(\boldsymbol{A}, \boldsymbol{b}) = \left(\begin{array}{rrr|r} 1, & 2, & 1 & 8 \\ 2, & 3, & -1 & 5 \\ -1, & 1, & 6 & 19 \end{array}\right) \sim \left(\begin{array}{rrr|r} 1, & 2, & 1 & 8 \\ 0, & -1, & -3 & -11 \\ 0, & 3, & 7 & 27 \end{array}\right) \sim \left(\begin{array}{rrr|r} 1, & 2, & 1 & 8 \\ 0, & 1, & 3 & 11 \\ 0, & 0, & -2 & -6 \end{array}\right),$$

odkud postupně dostáváme $x_3 = 3, x_2 = 2, x_1 = 1$.

b) Metodou inverzní matice: Jest

$$\left(\begin{array}{rrr|rrr} 1, & 2, & 1 & 1, & 0, & 0 \\ 2, & 3, & -1 & 0, & 1, & 0 \\ -1, & 1, & 6 & 0, & 0, & 1 \end{array}\right) \sim \left(\begin{array}{rrr|rrr} 1, & 2, & 1 & 1, & 0, & 0 \\ 0, & -1, & -3 & -2, & 1, & 0 \\ 0, & 3, & 7 & 1, & 0, & 1 \end{array}\right) \sim \left(\begin{array}{rrr|rrr} 1, & 2, & 1 & 1, & 0, & 0 \\ 0, & 1, & 3 & 2, & -1, & 0 \\ 0, & 0, & -2 & -5, & 3, & 1 \end{array}\right) \sim$$

$$\left(\begin{array}{rrr|rrr} 1, & 2, & 0 & -\frac{3}{2}, & \frac{3}{2}, & \frac{1}{2} \\ 0, & 1, & 0 & -\frac{11}{2}, & \frac{7}{2}, & \frac{3}{2} \\ 0, & 0, & 1 & \frac{5}{2}, & -\frac{3}{2}, & -\frac{1}{2} \end{array}\right) \sim \left(\begin{array}{rrr|rrr} 1, & 0, & 0 & \frac{19}{2}, & -\frac{11}{2}, & -\frac{5}{2} \\ 0, & 1, & 0 & -\frac{11}{2}, & \frac{7}{2}, & \frac{3}{2} \\ 0, & 0, & 1 & \frac{5}{2}, & -\frac{3}{2}, & -\frac{1}{2} \end{array}\right),$$

takže

$$A^{-1} = \frac{1}{2}\begin{pmatrix} 19,-11,-5 \\ -11, \ 7, \ 3 \\ 5, -3,-1 \end{pmatrix}.$$

Pak

$$A^{-1}b^T = \frac{1}{2}\begin{pmatrix} 19,-11,-5 \\ -11, \ 7, \ 3 \\ 5, -3,-1 \end{pmatrix}\begin{pmatrix} 8 \\ 5 \\ 19 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 \\ 4 \\ 6 \end{pmatrix} = u^T.$$

c) Cramerovým pravidlem: Máme

$$|A| = \begin{vmatrix} 1, & 2, & 1 \\ 2, & 3, & -1 \\ -1, & 1, & 6 \end{vmatrix} = \begin{vmatrix} 1, & 2, & 1 \\ 0, & -1, & -3 \\ 0, & 3, & 7 \end{vmatrix} = 2, \quad |A_1| = \begin{vmatrix} 8, & 2, & 1 \\ 5, & 3, & -1 \\ 19, & 1, & 6 \end{vmatrix} = \begin{vmatrix} 13, & 5, & 1 \\ 0, & 0, & -1 \\ 49, & 19, & 6 \end{vmatrix} = 2,$$

$$|A_2| = \begin{vmatrix} 1, & 8, & 1 \\ 2, & 5, & -1 \\ -1, & 19, & 6 \end{vmatrix} = \begin{vmatrix} 1, & 8, & 1 \\ 0, & -11, & -3 \\ 0, & 27, & 7 \end{vmatrix} = 4, \quad |A_3| = \begin{vmatrix} 1, & 2, & 8 \\ 2, & 3, & 5 \\ -1, & 1, & 19 \end{vmatrix} \begin{vmatrix} 1, & 2, & 8 \\ 0, & -1, & -11 \\ 0, & 3, & 27 \end{vmatrix} = 6$$

a opět $u = (1, 2, 3)$.

2. Nad tělesem reálných čísel řešme nehomogenní soustavu lineárních rovnic s rozšířenou maticí

$$\left(\begin{array}{cccccc|c} 1, & 3, & 2, & 5, & 3, & 4 & 6 \\ 2, & 5, & 3, & 7, & 4, & 7 & 10 \\ 2, & 3, & 1, & 2, & 1, & 5 & 6 \\ 3, & 8, & 5, & 12, & 7, & 11 & 16 \\ 4, & 8, & 4, & 9, & 5, & 12 & 16 \end{array}\right).$$

Řešení: a) Gaussova eliminační metoda dává

$$\left(\begin{array}{cccccc|c} 1, & 3, & 2, & 5, & 3, & 4 & 6 \\ 2, & 5, & 3, & 7, & 4, & 7 & 10 \\ 2, & 3, & 1, & 2, & 1, & 5 & 6 \\ 3, & 8, & 5, & 12, & 7, & 11 & 16 \\ 4, & 8, & 4, & 9, & 5, & 12 & 16 \end{array}\right) \sim \left(\begin{array}{cccccc|c} 1, & 3, & 2, & 5, & 3, & 4 & 6 \\ 0, & -1, & -1, & -3, & -2, & -1 & -2 \\ 0, & -3, & -3, & -8, & -5, & -3 & -6 \\ 0, & -1, & -1, & -3, & -2, & -1 & -2 \\ 0, & -4, & -4, & -11, & -7, & -4 & -8 \end{array}\right) \sim$$

$$\left(\begin{array}{cccccc|c} 1, & 3, & 2, & 5, & 3, & 4 & 6 \\ 0, & 1, & 1, & 3, & 2, & 1 & 2 \\ 0, & 0, & 0, & 1, & 1, & 0 & 0 \\ 0, & 0, & 0, & 0, & 0, & 0 & 0 \\ 0, & 0, & 0, & 1, & 1, & 0 & 0 \end{array}\right) \sim \left(\begin{array}{cccccc|c} 1, & 3, & 2, & 5, & 3, & 4 & 6 \\ 0, & 1, & 1, & 3, & 2, & 1 & 2 \\ 0, & 0, & 0, & 1, & 1, & 0 & 0 \end{array}\right).$$

Dostali jsme Gaussovu matici s indexy 1, 2, 4, takže snadno spočteme tři lineárně nezávislá řešení příslušné homogenní soustavy $u_3 = (1, -1, 1, 0, 0, 0)$, $u_5 =$

$(-1, 1, 0, -1, 1, 0)$, $\boldsymbol{u}_6 = (-1, -1, 0, 0, 0, 1)$ a partikulární řešení $\boldsymbol{u} = (0, 2, 0, 0, 0, 0)$. Všechna řešení dané soustavy tedy podle věty 5.4 jsou $\boldsymbol{u} + \langle \boldsymbol{u}_3, \boldsymbol{u}_5, \boldsymbol{u}_6 \rangle$.

b) Pomocí Cramerova pravidla z předchozí poznámky. Jak jsme viděli v předchozí části, je $h(\boldsymbol{A}) = 3$ a můžeme vzít třeba dílčí matici z prvních třech řádků a 1. 2. a 4. sloupce, která je, jak uvidíme, regulární. Soustavu můžeme tedy přepsat ve tvaru

$$\begin{aligned} x_1 + 3x_2 + 5x_4 &= 6 - 2x_3 - 3x_5 - 4x_6, \\ 2x_1 + 5x_2 + 7x_4 &= 10 - 3x_3 - 4x_5 - 7x_6, \\ 2x_1 + 3x_2 + 2x_4 &= 6 - x_3 - x_5 - 5x_6. \end{aligned}$$

Podle Cramerova pravidla máme

$$|\boldsymbol{A}| = \begin{vmatrix} 1, & 3, & 5 \\ 2, & 5, & 7 \\ 2, & 3, & 2 \end{vmatrix} = \begin{vmatrix} 1, & 3, & 5 \\ 0, & -1, & -3 \\ 0, & -3, & -8 \end{vmatrix} = -1,$$

$$|\boldsymbol{A}_1| = \begin{vmatrix} 6 - 2x_3 - 3x_5 - 4x_6, & 3, & 5 \\ 10 - 3x_3 - 4x_5 - 7x_6, & 5, & 7 \\ 6 - x_3 - x_5 - 5x_6, & 3, & 2 \end{vmatrix} = -x_3 + x_5 + x_6,$$

neboť rozvojem podle prvního sloupce dostáváme $|\boldsymbol{A}_1| = -11(6 - 2x_3 - 3x_5 - 4x_6) + 9(10 - 3x_3 - 4x_5 - 7x_6) - 4(6 - x_3 - x_5 - 5x_6) = -x_3 + x_5 + x_6$. Podobně

$$|\boldsymbol{A}_2| = \begin{vmatrix} 1, & 6 - 2x_3 - 3x_5 - 4x_6, & 5 \\ 2, & 10 - 3x_3 - 4x_5 - 7x_6, & 7 \\ 2, & 6 - x_3 - x_5 - 5x_6, & 2 \end{vmatrix} = 2 + x_3 - x_5 + x_6,$$

$$|\boldsymbol{A}_4| = \begin{vmatrix} 1, & 3, & 6 - 2x_3 - 3x_5 - 4x_6 \\ 2, & 5, & 10 - 3x_3 - 4x_5 - 7x_6 \\ 2, & 3, & 6 - x_3 - x_5 - 5x_6 \end{vmatrix} = x_5.$$

Pomocí x_3, x_5, x_6 nyní snadno spočteme Cramerovým pravidlem x_1, x_2, x_4, takže všechna řešení soustavy jsou tvaru $(x_3 - x_5 - x_6, 2 - x_3 + x_5 - x_6, x_3, -x_5, x_5, x_6) = (0, 2, 0, 0, 0, 0) + x_3(1, -1, 1, 0, 0, 0) + x_5(-1, 1, 0, -1, 1, 0) + x_6(-1, -1, 0, 0, 0, 1) = \boldsymbol{u} + \langle \boldsymbol{u}_3, \boldsymbol{u}_5, \boldsymbol{u}_6 \rangle$, tedy stejná jako při postupu z bodu a). Poznamenejme, že obecně nemusí vyjít řešení ve stejném tvaru, neboť řešení je nekonečně mnoho a my můžeme vybrat libovolné partikulární řešení a libovolnou bázi podprostoru $W_{\boldsymbol{A}}$. Řešení dané soustavy může být např. zapsáno ve tvaru $\boldsymbol{v} + \langle \boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3 \rangle$, kde $\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{u}_3 + \boldsymbol{u}_5 + \boldsymbol{u}_6 = (-1, 1, 1, -1, 1, 1)$, $\boldsymbol{v}_1 = \boldsymbol{u}_3 + \boldsymbol{u}_5 = (0, 0, 1, -1, 1, 0)$, $\boldsymbol{v}_2 = \boldsymbol{u}_3 + \boldsymbol{u}_6 = (0, -2, 1, 0, 0, 1)$ a $\boldsymbol{v}_3 = \boldsymbol{u}_5 + \boldsymbol{u}_6 = (-2, 0, 0, -1, 1, 1)$.

8.16. Věta. *Buď $\boldsymbol{B}$ regulární čtvercová matice stupně n, $\boldsymbol{C}$ regulární čtvercová matice stupně m a $\boldsymbol{A}$ matice typu (n, m) nad tělesem T. Pak $h(\boldsymbol{A}) = h(\boldsymbol{BAC})$.*

Důkaz. Označíme-li $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n \in T^m$ řádkové vektory matice $\boldsymbol{A}$, $\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n \in T^n$ řádkové vektory matice $\boldsymbol{B}$ a $M = (\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n)$, jsou $\boldsymbol{b}_1 * M, \boldsymbol{b}_2 * M, \dots, \boldsymbol{b}_n * M$ řádkové vektory matice $\boldsymbol{BA}$. Podle vět 2.25 a 8.4 je $\langle M \rangle = T^n * M = \langle \boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n \rangle * M = \langle \boldsymbol{b}_1 * M, \boldsymbol{b}_2 * M, \dots, \boldsymbol{b}_n * M \rangle$, takže $h(\boldsymbol{A}) = \dim\langle M \rangle = \dim\langle \boldsymbol{b}_1 * M, \boldsymbol{b}_2 * M, \dots, \boldsymbol{b}_n * M \rangle = h(\boldsymbol{BA})$. Z vět 5.5, 4.13 a z toho, co bylo právě dokázáno, dostáváme $h(\boldsymbol{AC}) = h((\boldsymbol{AC})^T) = h(\boldsymbol{C}^T \boldsymbol{A}^T) = h(\boldsymbol{A}^T) = h(\boldsymbol{A})$, a tedy konečně $h(\boldsymbol{BAC}) = h(\boldsymbol{AC}) = h(\boldsymbol{A})$. ∎

8.17. Důsledek. *Jsou-li $\boldsymbol{A}$, $\boldsymbol{B}$ čtvercové matice stupně n nad tělesem T, $\boldsymbol{B}$ regulární, pak $h(\boldsymbol{A}) = h(\boldsymbol{B}\boldsymbol{A}\boldsymbol{B}^{-1})$.*

Důkaz. Plyne bezprostředně z předchozí věty. ∎

9. Homomorfismy vektorových prostorů

9.1. Definice. Buďte V a V' vektorové prostory nad tělesem T. Zobrazení f množiny V do množiny V' se nazývá *homomorfismus* (*lineární zobrazení*), jestliže pro všechna $\boldsymbol{u}, \boldsymbol{v} \in V, r \in T$ platí

$$f(\boldsymbol{u}+\boldsymbol{v}) = f(\boldsymbol{u}) + f(\boldsymbol{v}),$$

$$f(r\boldsymbol{u}) = rf(\boldsymbol{u}).$$

Prostý (injektivní) homomorfismus se nazývá *monomorfismus*, surjektivní homomorfismus (zobrazení V na V') se nazývá *epimorfismus*. *Izomorfismus* je homomorfismus, který je současně monomorfismem i epimorfismem (prostý homomorfismus V na V'). Řekneme, že vektorové prostory V a V' jsou *izomorfní*, $V \cong V'$, jestliže existuje izomorfismus prostoru V na prostor V'. Homomorfismus f vektorového prostoru V do vektorového prostoru V' budeme značit symbolem $f : V \to V'$.

9.2. Poznámka. Z definice homomorfismu bezprostředně plyne několik jednoduchých skutečností. Předně z rovností $f(0) = f(0+0) = f(0) + f(0)$ plyne přičtením opačného prvku k $f(0)$ k oběma stranám rovnost $f(0) = 0$. Odtud dále je $0 = f(0) = f(\boldsymbol{u}-\boldsymbol{u}) = f(\boldsymbol{u}+(-\boldsymbol{u})) = f(\boldsymbol{u}) + f(-\boldsymbol{u})$, takže $f(-\boldsymbol{u}) = -f(\boldsymbol{u})$ a tedy také $f(\boldsymbol{u}-\boldsymbol{v}) = f(\boldsymbol{u}+(-\boldsymbol{v})) = f(\boldsymbol{u})+f(-\boldsymbol{v}) = f(\boldsymbol{u}) - f(\boldsymbol{v})$. Nakonec, je-li V vektorový prostor nad tělesem T, pak identické zobrazení $1_V : V \to V$ definované vztahem $1_V(\boldsymbol{u}) = \boldsymbol{u}$ pro každé $\boldsymbol{u} \in V$ je zřejmě izomorfismus V na V.

9.3. Definice. Buď $f : V \to V'$ homomorfismus vektorového prostoru V do vektorového prostoru V'. Podmnožinu $\operatorname{Ker} f = \{\boldsymbol{u} \in V \mid f(\boldsymbol{u}) = 0\}$ prostoru V nazýváme *jádrem homomorfismu* f a podmnožinu $\operatorname{Im} f = \{f(\boldsymbol{u}) \mid \boldsymbol{u} \in V\} = f(V)$ prostoru V' nazýváme *obrazem homomorfismu* f.

9.4. Věta. *Buď $f : V \to V'$ homomorfismus vektorového prostoru V do vektorového prostoru V'. Pak:*

(i) $\operatorname{Ker} f \le V$, $\operatorname{Im} f \le V'$;
(ii) f je monomorfismus, právě když $\operatorname{Ker} f = 0$;
(iii) f je epimorfismus, právě když $\operatorname{Im} f = V'$;
(iv) je izomofismus, právě když $\operatorname{Ker} f = 0$ *a* $\operatorname{Im} f = V'$.

Důkaz. (i) Pro $\boldsymbol{u}, \boldsymbol{v} \in \operatorname{Ker} f$, $r \in T$ libovolné máme $f(\boldsymbol{u}+\boldsymbol{v}) = f(\boldsymbol{u}) + f(\boldsymbol{v}) = 0$, $f(r\boldsymbol{u}) = rf(\boldsymbol{u}) = 0$, takže $\boldsymbol{u}+\boldsymbol{v}, r\boldsymbol{u} \in \operatorname{Ker} f$ a $\operatorname{Ker} f \le V$ podle definice 1.6. Dále, jsou-li $\boldsymbol{u}', \boldsymbol{v}' \in \operatorname{Im} f$, $r \in T$, libovolné prvky, existují prvky $\boldsymbol{u}, \boldsymbol{v} \in V$ takové, že $f(\boldsymbol{u}) = \boldsymbol{u}'$ a $f(\boldsymbol{v}) = \boldsymbol{v}'$. Pak ale $\boldsymbol{u}' + \boldsymbol{v}' = f(\boldsymbol{u}) + f(\boldsymbol{v}) = f(\boldsymbol{u}+\boldsymbol{v}) \in \operatorname{Im} f$, $r\boldsymbol{u}' = rf(\boldsymbol{u}) = f(r\boldsymbol{u}) \in \operatorname{Im} f$ a $\operatorname{Im} f \le V'$.

(ii) Buď nejprve f monomorfismus. Protože $f(0) = 0$ podle poznámky 9.2, je $f(\boldsymbol{u}) \neq 0$ pro každé $0 \neq \boldsymbol{u} \in V$, takže $\operatorname{Ker} f = 0$. Nechť tedy naopak $\operatorname{Ker} f = 0$. Jsou-li $\boldsymbol{u}, \boldsymbol{v} \in V$ dva vektory takové, že $f(\boldsymbol{u}) = f(\boldsymbol{v})$, pak $f(\boldsymbol{u}-\boldsymbol{v}) = f(\boldsymbol{u}) - f(\boldsymbol{v}) = 0$, takže $\boldsymbol{u}-\boldsymbol{v} \in \operatorname{Ker} f$, tedy $\boldsymbol{u}-\boldsymbol{v} = 0$, $\boldsymbol{u} = \boldsymbol{v}$ a f je prosté zobrazení.

Tvrzení (iii) je zřejmé a (iv) plyne bezprostředně z (ii) a (iii). ∎

9.5. Věta. *Nechť $f, h : V \to V'$ a $g : V' \to V''$ jsou homomorfismy vektorových prostorů a $r \in T$ buď libovolný prvek. Pak platí:*

(i) zobrazení $gf : V \to V''$ definované pro každé $\boldsymbol{u} \in V$ předpisem $(gf)(\boldsymbol{u}) = g(f(\boldsymbol{u}))$ je homomorfismus;

(ii) zobrazení $f+h : V \to V'$ definované pro každé $\boldsymbol{u} \in V$ předpisem $(f+h)(\boldsymbol{u}) = f(\boldsymbol{u}) + h(\boldsymbol{v})$ je homomorfismus;

(iii) zobrazení $rf : V \to V'$ definované pro každé $\boldsymbol{u} \in V$ předpisem $(rf)(\boldsymbol{u}) = rf(\boldsymbol{u})$ je homomorfismus.

Důkaz. Musíme ověřit, že všechna tři zobrazení splňují podmínky z definice 9.1.

(i) Pro libovolné dva prvky $\boldsymbol{u}, \boldsymbol{v} \in V$ a libovolný prvek $r \in T$ máme $(gf)(\boldsymbol{u} + \boldsymbol{v}) = g(f(\boldsymbol{u} + \boldsymbol{v})) = g(f(\boldsymbol{u}) + f(\boldsymbol{v})) = g(f(\boldsymbol{u})) + g(f(\boldsymbol{u})) = (gf)(\boldsymbol{u}) + (gf)(\boldsymbol{v})$ a $(gf)(r\boldsymbol{u}) = g(f(r\boldsymbol{u})) = g(rf(\boldsymbol{u})) = rg(f(\boldsymbol{u})) = r(gf)(\boldsymbol{u})$.

(ii) Podobně pro všechna $\boldsymbol{u}, \boldsymbol{v} \in V$ a $r \in T$ je $(f+h)(\boldsymbol{u}+\boldsymbol{v}) = f(\boldsymbol{u}+\boldsymbol{v})+h(\boldsymbol{u}+\boldsymbol{v}) = f(\boldsymbol{u})+f(\boldsymbol{v})+h(\boldsymbol{u})+h(\boldsymbol{v}) = (f+h)(\boldsymbol{u})+(f+h)(\boldsymbol{v})$ a $(f+h)(r\boldsymbol{u}) = f(r\boldsymbol{u})+h(r\boldsymbol{u}) = rf(\boldsymbol{u}) + rh(\boldsymbol{u}) = r(f(\boldsymbol{u}) + h(\boldsymbol{u})) = r(f + h)(\boldsymbol{u})$.

(iii) Pro všechna $\boldsymbol{u}, \boldsymbol{v} \in V$ a $s \in T$ platí $(rf)(\boldsymbol{u} + \boldsymbol{v}) = rf(\boldsymbol{u} + \boldsymbol{v}) = r(f(\boldsymbol{u}) + f(\boldsymbol{v})) = rf(\boldsymbol{u}) + rf(\boldsymbol{v}) = (rf)(\boldsymbol{u}) + (rf)(\boldsymbol{v})$ a $(rf)(s\boldsymbol{u}) = rf(s\boldsymbol{u}) = rsf(\boldsymbol{u}) = srf(\boldsymbol{u}) = s(rf)(\boldsymbol{u})$. ■

9.6. Definice. Buďte $f, h : V \to V'$ a $g : V' \to V''$ homomorfismy vektorových prostorů. Homomorfismus $gf : V \to V''$ definovaný v předchozí větě se nazývá *součinem (složením)* homomorfismů f a g. *Součtem homomorfismů* f a h a *násobkem homomorfismu* f prvkem $r \in T$ rozumíme homomorfismy $f + h$, a rf z předchozí věty.

9.7. Věta. *Nechť $f : V \to V'$ a $g : V' \to V''$ jsou homomorfismy vektorových prostorů. Pak platí:*

(i) jsou-li f a g monomorfismy, je i gf momomorfismus;

(ii) jsou-li f a g epimorfismy, je i gf epimorfismus;

(iii) jsou-li f a g izomorfismy, je i gf izomorfismus;

(iv) je-li gf monomorfismus, je i f monomorfismus;

(v) je-li gf epimorfismus, je i g epimorfismus.

Důkaz. (i) Je-li $(gf)(\boldsymbol{u}) = 0$, je $g(f(\boldsymbol{u})) = 0$, takže $f(\boldsymbol{u}) = 0$ vzhledem k tomu, že g je monomorfismus. Z prostoty zobrazení f plyne $\boldsymbol{u} = 0$, tedy $\operatorname{Ker} gf = 0$ a gf je monomorfismus podle věty 9.4.

(ii) Potřebujeme ukázat, že každý vektor $\boldsymbol{u}'' \in V''$ je obrazem nějakého vektoru $\boldsymbol{u} \in V$. Protože g je epimorfismus, existuje vektor $\boldsymbol{u}' \in V'$ takový, že $g(\boldsymbol{u}') = \boldsymbol{u}''$. Podobně existuje vektor $\boldsymbol{u} \in V$ tak, že $f(\boldsymbol{u}) = \boldsymbol{u}'$. Celkem tedy máme $(gf)(\boldsymbol{u}) = g(f(\boldsymbol{u})) = g(\boldsymbol{u}') = \boldsymbol{u}'$ a gf epimorfismus.

(iii) Tvrzení ihned plyne z (i) a (ii).

(iv) Vzhledem k větě 9.4 potřebujeme ukázat, že $\operatorname{Ker} f = 0$. Pro $\boldsymbol{u} \in \operatorname{Ker} f$ však je $f(\boldsymbol{u}) = 0$, tedy $(gf)(\boldsymbol{u}) = g(f(\boldsymbol{u})) = 0$ podle poznámky 9.2, takže $\boldsymbol{u} = 0$ podle předpokladu.

(v) Buď $\boldsymbol{u}'' \in V''$ libovolný prvek. Podle předpokladu existuje vektor $\boldsymbol{u} \in V$ takový, že $(gf)(\boldsymbol{u}) = \boldsymbol{u}''$. Označíme-li $\boldsymbol{u}' = f(\boldsymbol{u})$, je $g(\boldsymbol{u}') = g(f(\boldsymbol{u})) = (gf)(\boldsymbol{u}) = \boldsymbol{u}''$ a g je epimorfismus. ■

9.8. Věta. *Buď $f : V \to V'$ homomorfismus vektorových prostorů. Pak f je izomorfismus, právě když existuje homomorfismus $g : V' \to V$ takový, že $gf = 1_V$ a $fg = 1_{V'}$. Přitom homomorfismus g je izomorfismus a je izomorfismem f určen jednoznačně.*

Důkaz. Předpokládejme nejprve, že existuje homomorfismus $g : V' \to V$ takový, že $gf = 1_V$ a $fg = 1_{V'}$. Podle věty 9.7 jsou obě zobrazení f i g jak monomorfismy, tak epimorfismy, takže jsou izomorfismy.

Nechť tedy naopak zobrazení f je izomorfismus. Protože f je speciálně epimorfismus, existuje ke každému $\boldsymbol{u}' \in V'$ vektor $\boldsymbol{u} \in V$ takový, že $f(\boldsymbol{u}) = \boldsymbol{u}'$. Vektor $\boldsymbol{u}$ je přitom určen jednoznačně vzhledem k tomu, že f je monomorfismus, takže můžeme definovat zobrazení $g : V' \to V$ předpisem $g(\boldsymbol{u}') = \boldsymbol{u}$, právě když $f(\boldsymbol{u}) = \boldsymbol{u}'$, a potřebujeme ověřit, že g je homomorfismus. Buďte $\boldsymbol{u}', \boldsymbol{v}' \in V'$ a $r \in T$ libovolné prvky. Pak existují $\boldsymbol{u}, \boldsymbol{v} \in V$ tak, že $f(\boldsymbol{u}) = \boldsymbol{u}'$ a $f(\boldsymbol{v}) = \boldsymbol{v}'$ a platí $g(\boldsymbol{u}' + \boldsymbol{v}') = g(f(\boldsymbol{u}) + f(\boldsymbol{v})) = g(f(\boldsymbol{u} + \boldsymbol{v})) = \boldsymbol{u} + \boldsymbol{v} = g(\boldsymbol{u}') + g(\boldsymbol{v}')$, $g(r\boldsymbol{u}') = g(rf(\boldsymbol{u})) = g(f(r\boldsymbol{u})) = r\boldsymbol{u} = rg(\boldsymbol{u}')$. Vzhledem k definici zobrazení g je evidentní, že $gf = 1_V$ a $fg = 1_{V'}$, takže zbývá dokázat jednoznačnost izomorfismu g. Buď tedy $g' : V' \to V$ homomorfismus takový, že $g'f = 1_V$ a $fg' = 1_{V'}$. Pak máme $g = g1_{V'} = g(fg') = (gf)g' = 1_V g' = g'$ a jsme hotovi. ∎

9.9. Definice. Buď $f : V \to V'$ izomorfismus. Izomorfismus $g : V' \to V$ z předchozí věty se nazývá *izomorfismus inverzní k f* a značí se f^{-1}.

9.10. Poznámka. Izomorfismus mezi vektorovými prostory je ekvivalence na třídě všech vektorových prostorů, tj. je to reflexivní, symetrická a tranzitivní relace na této třídě. Skutečně, je-li V vektorový prostor, je $V \cong V$ prostřednictvím identického zobrazení 1_V podle poznámky 9.2 a relace $\cong$ je reflexivní. Dále, je-li $f : V \to V'$ izomorfismus, je $f^{-1} : V' \to V$ izomorfismus podle věty 9.8, takže relace $\cong$ je symetrická. Konečně je relace $\cong$ tranzitivní, neboť jsou-li $f : V \to V'$ a $g : V' \to V''$ izomorfismy, je jejich složení $gf : V \to V''$ izomorfismus podle věty 9.7.

Podívejme se nyní na vzájemné vztahy mezi homomorfismy a dvěma základními pojmy z teorie vektorových prostorů, totiž lineárními obaly a lineární nezávislostí.

9.11. Věta. *Buď $f : V \to V'$ homomorfismus vektorových prostorů a $M \subseteq V$ buď libovolná podmnožina. Pak $f(\langle M \rangle) = \langle f(M) \rangle$.*

Důkaz. Je-li $M = \emptyset$, je $\langle M \rangle = 0$ podle věty 1.11, takže $f(\langle M \rangle) = f(0) = 0 = \langle f(\emptyset) \rangle$ a můžeme se omezit na případ $M \neq \emptyset$. Je-li $\boldsymbol{u} \in \langle M \rangle$ libovolný vektor, je $\boldsymbol{u} = \sum_{i=1}^{n} r_i \boldsymbol{u}_i$, $\boldsymbol{u}_i \in M$, $r_i \in T$, podle věty 1.11 a $f(\boldsymbol{u}) = f(\sum_{i=1}^{n} r_i \boldsymbol{u}_i) = \sum_{i=1}^{n} r_i f(\boldsymbol{u}_i) \in \langle f(M) \rangle$. Na druhé straně, je-li $\boldsymbol{u}' \in \langle f(M) \rangle$, je $\boldsymbol{u}' = \sum_{i=1}^{n} r_i f(\boldsymbol{u}_i)$ pro nějaké vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n \in M$, takže $\boldsymbol{u}' = f(\sum_{i=1}^{n} r_i \boldsymbol{u}_i) \in f(\langle M \rangle)$. ∎

9.12. Důsledek. *Buď $f : V \to V'$ epimorfismus vektorového prostoru V na vektorový prostor V'. Je-li $M \subseteq V$ množina generátorů prostoru V, je $f(M)$ množina generátorů prostoru V'.*

Důkaz. Podle předchozí věty je $\langle f(M) \rangle = f(\langle M \rangle) = f(V) = V'$ vzhledem k tomu, že f je podle předpokladu epimorfismus. ∎

9.13. Poznámka. V odstavci 2.5 jsme definovali lineárně nezávislé vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ tak, že pouze triviální lineární kombinace těchto vektorů dává nulový vektor. V poznámce 2.6 jsme konstatovali, že lineárně nezávislé vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$

jsou navzájem různé, a tvoří tudíž množinu $\{u_1, u_2, \dots, u_n\}$. Přitom např. vektor u_n neleží v lineárním obalu vektorů $u_1, u_2, \dots, u_{n-1}$, neboť v opačném případě bychom podle věty 1.11 měli $u_n = \sum_{i=1}^{n-1} r_i u_i$, tedy $\sum_{i=1}^{n-1} r_i u_i - u_n = 0$, což jest spor s lineární nezávislostí vektorů $u_1, u_2, \dots, u_n$. Jinými slovy jsme ukázali, že je-li N neprázdná podmnožina lineárně nezávislé množiny $M = \{u_1, u_2, \dots, u_n\}$, pak $\langle N \rangle \subset \langle M \rangle$. Můžeme proto pojem lineární nezávislosti zobecnit na libovolné nekonečné množiny, což učiníme v následující definici.

9.14. Definice. Neprázdná podmnožina M vektorového prostoru V nad tělesem T se nazývá *lineárně nezávislá*, jestliže pro každou vlastní podmnožinu $N \subset M$ je $\langle N \rangle \subset \langle M \rangle$. V opačném případě, tj. když existuje vlastní podmnožina $N \subset M$ taková, že $\langle N \rangle = \langle M \rangle$, se množina M nazývá *lineárně závislá.*

9.15. Věta. *Každá neprázdná podmnožina N lineárně nezávislé množiny M vektorů vektorového prostoru V je opět lineárně nezávislá.*

Důkaz. Předpokládejme naopak, že existuje neprázdná podmnožina N množiny M, která je lineárně závislá. Existuje tedy vlastní podmnožina $K \subset N$ taková, že $\langle K \rangle = \langle N \rangle$. Pak ale $K \cup (M \setminus N)$ je jistě vlastní podmnožina množiny M a zbývá ukázat, že $\langle K \cup (M \setminus N) \rangle = \langle M \rangle$. Je-li $u \in \langle M \rangle$ libovolný vektor, existují podle věty 1.11 vektory $u_1, u_2, \dots, u_n \in N$ a vektory $v_1, v_2, \dots, v_m \in M \setminus N$ takové, že vektor u je jejich lineární kombinací. Protože každý vektor z $\langle N \rangle$ je lineární kombinací vektorů z K, je vektor u lineární kombinací vektorů z $K \cup (M \setminus N)$ podle věty 2.3, takže $\langle M \rangle \subseteq \langle K \cup (M \setminus N) \rangle$. Obrácená inkluze je zřejmá. ∎

9.16. Věta. *Neprázdná podmnožina M vektorového prostoru V je lineárně nezávislá, právě když každá její neprázdná konečná podmnožina je lineárně nezávislá.*

Důkaz. Podmínka je nutná podle předchozí věty. K důkazu postačitelnosti předpokládejme, že M je lineárně závislá, a ukažme, že pak existuje neprázdná konečná podmnožina K množiny M, která je rovněž lineárně závislá. Podle předpokladu existuje vlastní podmnožina N množiny M taková, že $\langle N \rangle = \langle M \rangle$. Je-li nyní $u \in M \setminus N$ libovolný vektor, existují podle věty 1.11 vektory $u_1, u_2, \dots, u_n \in N$ takové, že $u = \sum_{i=1}^{n} r_i u_i$. Můžeme samozřejmě předpokládat, že vektory $u_1, u_2, \dots, u_n$ jsou navzájem různé, a vzhledem k tomu, že $u \notin N$, je $K = \{u, u_1, u_2, \dots, u_n\}$ konečná podmnožina množiny M. Jelikož $u - \sum_{i=1}^{n} r_i u_i = 0$, je množina K lineárně závislá. ∎

9.17. Poznámka. Právě dokázaná věta má zásadní důležitost. Ukazuje totiž, že lineární nezávislost či závislost je vlastností konečných podmnožin dané množiny, a redukuje tudíž celou problematiku na studium konečných množin. Jak víme z příkladu 1.3, je množina $P(T)$ všech polynomů s koeficienty v tělese T spolu s obvyklými operacemi sčítání polynomů a násobení polynomu prvkem z T, vektorový prostor nad T. Protože $f(x) = \sum_{i=0}^{n} r_i x^i = 0$, právě když $r_i = 0$ pro všechna $i = 0, 1, \dots, n$, jsou vektory $1, x, x^2, \dots, x^n$ lineárně nezávislé. Protože každá konečná podmnožina K množiny $\{1, x, x^2, \dots\}$ je obsažena v $\{1, x, x^2, \dots, x^n\}$ pro nějaké $n = 0, 1, \dots$, je množina K lineárně nezávislá podle věty 2.7. Podle předchozí věty je tedy množina $\{1, x, x^2, \dots\}$ lineárně nezávislá. Jelikož každý polynom $f(x)$ je lineární kombinací konečného počtu mocnin prvky x, $f(x) = \sum_{i=0}^{n} r_i x^i$, je množina $\{1, x, x^2, \dots\}$ bází vektorového prostoru $P(T)$ ve smyslu následující definice.

9.18. Definice. Neprázdná podmnožina M vektorového prostoru V se nazývá *báze*, je-li M lineárně nezávislá množina generátorů prostoru V.

9.19 Věta. *Je-li M báze vektorového prostoru V, pak lze každý nenulový vektor $\boldsymbol{u} \in V$ zapsat jednoznačně ve tvaru lineární kombinace $\boldsymbol{u} = \sum_{i=1}^{n} r_i \boldsymbol{u}_i$, kde $\boldsymbol{u}_i$ jsou po dvou různé vektory z báze M a r_i, $i = 1, 2, \ldots, n$, jsou nenulové koeficienty z tělesa T.*

Důkaz. Protože množina M generuje prostor V, lze každý vektor $\boldsymbol{u} \in V$ vyjádřit jako lineární kombinaci vektorů z množiny M podle věty 2.2, a tedy každý nenulový vektor z V má alespoň jedno vyjádření popsané ve větě.

K důkazu jednoznačnosti předpokládejme, že $0 \neq \boldsymbol{u} = \sum_{i=1}^{n} r_i \boldsymbol{u}_i = \sum_{j=1}^{m} s_j \boldsymbol{v}_j$, kde vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n \in M$ a vektory $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m \in M$ jsou po dvou různé a koeficienty $r_1, r_2, \ldots, r_n, s_1, s_2, \ldots, s_m$ jsou vesměs nenulové. Nejprve ukážeme, že $n = m$ a $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\} = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots \boldsymbol{v}_n\}$. Předpokládáme-li naopak, že některý z vektorů $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$ neleží v množině $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$, můžeme bez újmy na obecnosti předpokládat, že $\boldsymbol{v}_m \notin \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$. Protože některé z vektorů $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{m-1}$ mohou ležet v množině $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$, označme $K = \{\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_r\}$ množinu vektorů sestávajících z vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots \boldsymbol{u}_n, \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{m-1}$. Potom $\boldsymbol{v}_m \notin K$ a množina $K \cup \{\boldsymbol{v}_m\} \subseteq M$ je podle věty 9.16 lineárně nezávislá. Pak ale z rovnosti $\sum_{i=1}^{n} r_i \boldsymbol{u}_i - \sum_{j=1}^{m} s_j \boldsymbol{v}_j = 0$ dostáváme $\sum_{k=1}^{r} t_k \boldsymbol{w}_k - s_m \boldsymbol{v}_m = 0$, odkud $s_m = 0$ vzhledem k lineární nezávislosti množiny $K \cup \{\boldsymbol{v}_m\}$, což jest spor s předpokladem $s_m \neq 0$. Ukázali jsme tedy, že $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m\} \subseteq \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$, a tudíž z důvodů symetrie je $m = n$ a $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots \boldsymbol{u}_n\} = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n\}$. Při vhodném očíslování vektorů $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ můžeme tedy předpokládat, že $\boldsymbol{u}_i = \boldsymbol{v}_i$ pro každé $i = 1, 2, \ldots, n$, takže z rovnosti $\sum_{i=1}^{n} r_i \boldsymbol{u}_i = \sum_{i=1}^{n} s_i \boldsymbol{u}_i$ dostáváme $\sum_{i=1}^{n} (r_i - s_i) \boldsymbol{u}_i = 0$, a tedy $r_i = s_i$ vzhledem k lineární nezávislosti podmnožiny $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ množiny M (věta 9.16). Tím je důkaz věty dokončen. ■

9.20. Věta. *Buď $f : V \to V'$ homomorfismus a M buď podmnožina vektorového prostoru V. Je-li restrikce $f|M$ prosté zobrazení a množina $f(M) \subseteq V'$ je lineárně nezávislá, pak i množina M je lineárně nezávislá. Je-li speciálně f monomorfismus, pak podmnožina $M \subseteq V$ je lineárně nezávislá, právě když je lineárně nezávislá podmnožina $f(M)$ prostoru V'.*

Důkaz. Vzhledem k větě 9.16 stačí ukázat, že libovolná konečná podmnožina $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ množiny M je lineárně nezávislá. Je-li nyní $\sum_{i=1}^{n} r_i \boldsymbol{u}_i = 0$, pak $0 = f(\sum_{i=1}^{n} r_i \boldsymbol{u}_i) = \sum_{i=1}^{n} r_i f(\boldsymbol{u}_i)$. Protože restrikce $f|M$ je prosté zobrazení, jsou vektory $f(\boldsymbol{u}_1), f(\boldsymbol{u}_2), \ldots, f(\boldsymbol{u}_n)$ navzájem různé, množina $\{f(\boldsymbol{u}_1), f(\boldsymbol{u}_2), \ldots, f(\boldsymbol{u}_n)\}$ je tedy lineárně nezávislá podle předpokladu, takže $r_1 = r_2 = \cdots = r_n = 0$.

Je-li speciálně f monomorfismus, je předpoklad první části splněn a z lineární nezávislosti množiny $f(M)$ plyne lineární nezávislost množiny M. Nechť tedy naopak je lineárně nezávislá množina M a buď $\{\boldsymbol{u}'_1, \boldsymbol{u}'_2, \ldots, \boldsymbol{u}'_n\} \subseteq f(M)$ libovolná podmnožina. Existují tedy prvky $\boldsymbol{u}_i \in M$ takové, že $f(\boldsymbol{u}_i) = \boldsymbol{u}'_i$ pro každé $i = 1, 2, \ldots, n$ a množina $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\} \subseteq M$ je lineárně nezávislá podle předpokladu. Je-li nyní $\sum_{i=1}^{n} r_i \boldsymbol{u}'_i = 0$, je $0 = \sum_{i=1}^{n} r_i f(\boldsymbol{u}_i) = f(\sum_{i=1}^{n} r_i \boldsymbol{u}_i)$, a tedy $\sum_{i=1}^{n} r_i \boldsymbol{u}_i = 0$ vzhledem k tomu, že f je monomorfismus. Protože vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ jsou lineárně nezávislé, je $r_1 = r_2 = \cdots = r_n = 0$ a důkaz je hotov. ■

9.21. Věta. *Buď M báze vektorového prostoru V a buď $f : V \to V'$ izomorfismus. Pak $f(M)$ je báze vektorového prostoru V'.*

Důkaz. Protože f je monomorfismus, je množina $f(M)$ lineárně nezávislá podle předchozí věty. Jelikož f je zároveň epimorfismus, je $f(M)$ množina generátorů prostoru V' podle důsledku 9.12. ∎

Následující tvrzení ukazuje, že homomorfismus $f : V \to V'$ vektorového prostoru V do vektorového prostoru V' je jednoznačně určen hodnotami na nějaké bázi prostoru V. Názorně řečeno to znamená, že „předepíšeme-li" si libovolné „hodnoty" na nějaké (libovolné) bázi prostoru V, dostaneme jednoznačně určený homomorfismus. Kromě toho lze z vlastností množiny obrazů dané báze rozhodnout, zda jde speciálně o monomorfismus, či epimorfismus.

9.22. Věta. *Buď M báze vektorového prostoru V a buď $F : M \to M'$ bijekce množiny M na skupinu M' vektorů vektorového prostoru V'. Pak platí*

(i) existuje právě jeden homomorfismus $f : V \to V'$ takový, že $f(\boldsymbol{u}) = F(\boldsymbol{u})$ pro každý vektor $\boldsymbol{u} \in M$;

(ii) je-li M' lineárně nezávislá podmnožina vektorového prostoru V', je f monomorfismus;

(iii) jestliže M' generuje prostor V', pak f je epimorfismus prostoru V na prostor V';

(iv) je-li M' báze prostoru V', pak f je izomorfismus.

Důkaz. (i) Podle věty 9.19 můžeme každý nenulový vektor $\boldsymbol{v} \in V$ napsat jednoznačně ve tvaru $\boldsymbol{v} = \sum_{i=1}^{n} r_i \boldsymbol{u}_i$, kde vektory $\boldsymbol{u}_i \in M$ jsou po dvou různé a koeficienty $r_i \in T$, $i = 1, 2, \ldots, n$, jsou nenulové. Definujeme-li nyní zobrazení $f : V \to V'$ předpisem $f(0) = 0$ a $f(\boldsymbol{v}) = \sum_{i=1}^{n} r_i F(\boldsymbol{u}_i)$ pro $0 \neq \boldsymbol{v} \in V$, je zřejmě f homomorfismus takový, že $f(\boldsymbol{u}) = F(\boldsymbol{u})$ pro každé $\boldsymbol{u} \in M$, a zbývá tedy dokázat jednoznačnost. Buď tedy $g : V \to V'$ libovolný homomorfismus takový, že $g(\boldsymbol{u}) = F(\boldsymbol{u})$ pro každý vektor $\boldsymbol{u} \in M$. Pak pro každé $0 \neq \boldsymbol{v} \in V$ je $\boldsymbol{v} = \sum_{i=1}^{n} r_i \boldsymbol{u}_i$, $\boldsymbol{u} \in M$, $r_i \in T$, takže $g(\boldsymbol{v}) = g(\sum_{i=1}^{n} r_i \boldsymbol{u}) = \sum_{i=1}^{n} r_i g(\boldsymbol{u}_i) = \sum_{i=1}^{n} r_i F(\boldsymbol{u}_i) = f(\boldsymbol{v})$ a tedy $g = f$ vzhledem ke zřejmé rovnosti $g(0) = 0 = f(0)$.

(ii) S přihlédnutím k větě 9.4 stačí ukázat, že $\operatorname{Ker} f = 0$. Buď tedy $\boldsymbol{v} \in \operatorname{Ker} f$ libovolný prvek. Je-li $\boldsymbol{v} \neq 0$, můžeme vektor $\boldsymbol{v}$ napsat podle věty 9.19 jednoznačně ve tvaru lineární kombinace $\boldsymbol{v} = \sum_{i=1}^{n} r_i \boldsymbol{u}_i$, kde $\boldsymbol{u}_i \in M$ jsou navzájem různé vektory a $r_i, i = 1, 2, \ldots, n$, jsou nenulové prvky z tělesa T. Pak máme $f(\boldsymbol{v}) = \sum_{i=1}^{n} r_i F(\boldsymbol{u}_i) = 0$, takže $r_1 = r_2 = \cdots = r_n = 0$ vzhledem k předpokladu lineární nezávislosti množiny M' a větě 9.16. Dostali jsme tedy spor s nenulovostí koeficientů $r_1, r_2, \ldots, r_n$, takže nutně $\boldsymbol{v} = 0$ a f je monomorfismus.

(iii) Jestliže skupina vektorů M' generuje prostor V', je $\operatorname{Im} f = f(V) = f(\langle M \rangle) = \langle f(M) \rangle = \langle M' \rangle = V'$ podle věty 9.11, a f je tudíž epimorfismus.

(iv) Tvrzení plyne okamžitě z (ii) a (iii). ∎

9.23. Definice. Buď W podprostor vektorového prostoru V. Říkáme, že podprostor W' je *doplňkem* W v prostoru V, jestliže $W \cap W' = 0$ a $W \vee W' = V$. Vzhledem k symetrii je zřejmé, že v tomto případě je také W doplňkem W' ve V.

9.24. Věta. *Ke každému podprostoru W vektorového prostoru V_n konečné dimenze n existuje doplněk W'. Přitom platí, že* $\dim W + \dim W' = n$.

Důkaz. Podle věty 2.22 má podprostor W konečnou dimenzi, $\dim W = r \leq n$. Můžeme předpokládat, že $r < n$, neboť v opačném případě stačí vzít $W' = 0$. Je-li $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_r\}$ libovolná báze prostoru W, existují podle věty 2.21 vektory $\boldsymbol{w}_1, \boldsymbol{w}_2, \dots \boldsymbol{w}_{n-r}$ takové, že množina $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_r, \boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_{n-r}\}$ je bází prostoru V_n. Jestliže položíme $W' = \langle \boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_{n-r}\rangle$, dostáváme z věty 1.13 ihned, že $W \vee W' = V_n$. Z věty o dimenzi spojení a průniku 2.23 máme $\dim (W \cap W') = \dim W + \dim W' - \dim (W \vee W') = r + n - r - n = 0$, takže $W \cap W' = 0$ a W' je doplňkem podprostoru W ve V_n. Kromě toho je zřejmé $\dim W + \dim W' = r + n - r = n$ a jsme hotovi. ■

9.25. Věta. *Buď W' doplněk podprostoru W ve vektorovém prostoru V. Pak platí*

(i) každý vektor $\boldsymbol{u} \in V$ lze napsat jednoznačně ve tvaru $\boldsymbol{u} = \boldsymbol{w} + \boldsymbol{w}'$, kde $\boldsymbol{w} \in W$ a $\boldsymbol{w}' \in W'$;

(ii) je-li M báze W a M' báze W', je $M \cup M'$ báze V.

Důkaz. Podle definice 2.27 je V direktním součtem svých podprostorů W a W', $V = W \oplus W'$, takže tvrzení (i) plyne z věty 2.28. K důkazu tvrzení (ii) si nejprve uvědomme, že z věty 1.13 snadno plyne, že množina $M \cup M'$ generuje prostor V. Vzhledem k větě 9.16 tedy stačí ukázat, že každá neprázdná konečná podmnožina K množiny $M \cup M'$ je lineárně nezávislá. Nechť tedy $K = N \cup N'$, $N \subseteq M$, $N' \subseteq M'$ je konečná podmnožina v $M \cup M'$. Je-li buď $N = \emptyset$, nebo $N' = \emptyset$, je K lineárně nezávislá podle předpokladu a věty 9.15. V opačném případě je $\langle N\rangle \cap \langle N'\rangle \subseteq W \cap W' = 0$, takže $\langle K\rangle = \langle N\rangle \oplus \langle N'\rangle$, a protože N je zřejmě báze $\langle N\rangle$ a N' báze $\langle N'\rangle$, je K báze $\langle K\rangle$ podle věty 2.29. Speciálně je tedy množina K lineárně nezávislá, což jsme chtěli dokázat. ■

9.26. Věta. *Buď $f : V \to V'$ homomorfismus a buď W doplněk Ker f ve V. Pak platí*

(i) restrikce $f|W$ je monomorfismus vektorového prostoru W do prostoru V';

(ii) $\mathrm{Im} f = f(W)$.

Důkaz. (i) Je-li $\boldsymbol{u} \in \mathrm{Ker}\,(f|W)$ libovolný vektor, je $\boldsymbol{u} \in \mathrm{Ker}\, f \cap W = 0$, takže $f|W$ je monomorfismus podle věty 9.4 (ii).

(ii) Podle věty 9.25 lze každý vektor $\boldsymbol{u} \in V$ psát jednoznačně ve tvaru $\boldsymbol{u} = \boldsymbol{v} + \boldsymbol{w}$, kde $\boldsymbol{v} \in \mathrm{Ker}\, f$ a $\boldsymbol{w} \in W$. Je-li nyní $\boldsymbol{u}' \in \mathrm{Im} f$ libovolný vektor, existuje vektor $\boldsymbol{u} \in V$ takový, že $\boldsymbol{u}' = f(\boldsymbol{u}) = f(\boldsymbol{v} + \boldsymbol{w}) = f(\boldsymbol{w}) \in f(W)$, takže $\mathrm{Im} f \leq f(W)$ a tedy $\mathrm{Im} f = f(W)$ vzhledem k tomu, že obrácená inkluze je zřejmá. ■

9.27. Věta. *Buď $f : V_n \to V_m$ homomorfismus vektorového prostoru V_n do vektorového prostoru V_m. Pak* $\dim \mathrm{Ker}\, f + \dim \mathrm{Im}\, f = n$.

Důkaz. Podle věty 9.24 existuje k podprostoru Ker f doplněk W ve V_n a platí $\dim \mathrm{Ker}\, f + \dim W = n$. K dokončení důkazu tedy zbývá ukázat, že $\dim W = \dim \mathrm{Im}\, f$. Podle věty 9.26 je restrikce $f|W$ izomorfismus podprostoru $W \leq V_n$ na podprostor $\mathrm{Im}\, f \leq V_m$. Použitím věty 9.21 však dostáváme, že obrazem nějaké báze prostoru W je báze prostoru Im f, takže $\dim W = \dim \mathrm{Im}\, f$ podle definice dimenze 2.15. ■

10.1. Definice. Buď $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ báze vektorového prostoru V_n. Podle věty 2.10 lze každý vektor $\boldsymbol{u} \in V_n$ napsat jednoznačně ve tvaru lineární kombinace $\boldsymbol{u} = \sum_{i=1}^{n} x_i \boldsymbol{u}_i$. Aritmetický vektor $(x_1, x_2, \dots, x_n) \in T^n$ nazýváme *souřadnicemi vektoru* $\boldsymbol{u}$ *vzhledem k bázi* M a značíme $\{\boldsymbol{u}\}_M = (x_1, x_2, \dots, x_n)$.

10.2. Věta. *Buď* $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ *báze vektorového prostoru* V_n. *Pak platí:*
(i) $\{\boldsymbol{u} + \boldsymbol{v}\}_M = \{\boldsymbol{u}\}_M + \{\boldsymbol{v}\}_M$, $\{r\boldsymbol{u}\} = r\{\boldsymbol{u}\}_M$ *pro každé dva vektory* $\boldsymbol{u}, \boldsymbol{v} \in V_n$ *a každé* $r \in T$;
(ii) zobrazení $f : V_n \to T^n$ *definované pro každé* $\boldsymbol{u} \in V_n$ *předpisem* $f(\boldsymbol{u}) = \{\boldsymbol{u}\}_M$ *je izomorfismus prostoru* V_n *na aritmetický vektorový prostor* T^n;
(iii) vektory $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k \in V_n$ *jsou lineárně nezávislé, právě když jsou lineárně nezávislé vektory* $\{\boldsymbol{v}_1\}_M, \{\boldsymbol{v}_2\}_M, \dots, \{\boldsymbol{v}_k\}_M$ *v prostoru* T^n;
(iv) jsou-li $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k \in V_n$ *libovolné vektory, pak platí* $\dim \langle \boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k \rangle = \dim \langle \{\boldsymbol{v}_1\}_M, \{\boldsymbol{v}_2\}_M, \dots, \{\boldsymbol{v}_k\}_M \rangle$.

Důkaz. (i) Nechť $\{\boldsymbol{u}\}_M = (x_1, x_2, \dots, x_n)$, $\{\boldsymbol{v}\}_M = (y_1, y_2, \dots, y_n)$. Pak $\boldsymbol{u} = \sum_{i=1}^{n} x_i \boldsymbol{u}_i$, $\boldsymbol{v} = \sum_{i=1}^{n} y_i \boldsymbol{u}_i$, takže $\boldsymbol{u} + \boldsymbol{v} = \sum_{i=1}^{n} (x_i + y_i)\boldsymbol{u}_i$, a tedy $\{\boldsymbol{u} + \boldsymbol{v}\}_M = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n) = (x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) = \{\boldsymbol{u}\}_M + \{\boldsymbol{v}\}_M$. Podobně je $r\boldsymbol{u} = r \sum_{i=1}^{n} x_i \boldsymbol{u}_i = \sum_{i=1}^{n} r x_i \boldsymbol{u}_i$, takže $\{r\boldsymbol{u}\}_M = (rx_1, rx_2, \dots, rx_n) = r(x_1, x_2, \dots, x_n) = r\{\boldsymbol{u}\}_M$.

(ii) Podle předchozího tvrzení je zobrazení f homomorfismus. Přitom pro $f(\boldsymbol{u}) = 0$ je $\{\boldsymbol{u}\}_M = (0, 0, \dots, 0)$, takže $\boldsymbol{u} = \sum_{i=0}^{n} 0 \cdot \boldsymbol{u}_i = 0$ a f je monomorfismus podle věty 9.4 (ii). Pro libovolný vektor $(x_1, x_2, \dots, x_n) \in T^n$ je zřejmě $f(\sum_{i=1}^{n} x_i \boldsymbol{u}_i) = (x_1, x_2, \dots, x_n)$, takže zobrazení f je rovněž epimorfismus.

(iii) Plyne ihned z (ii) a věty 9.20.

(iv) Je-li $\dim\langle \boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k \rangle = r$, můžeme z množiny $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k\}$ vybrat podle věty 2.12 r-prvkovou bázi. Při vhodném očíslování daných vektorů můžeme bez újmy na obecnosti předpokládat, že $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_r\}$ je báze lineárního obalu $\langle \boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k \rangle$. Nyní si stačí uvědomit, že podle věty 9.21 je množina $\{\{\boldsymbol{v}_1\}_M, \{\boldsymbol{v}_2\}_M, \dots, \{\boldsymbol{v}_r\}_M\}$ bází prostoru $f(\langle \boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k \rangle$. Podle věty 9.11 je však $f(\langle \boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k \rangle) = \langle f(\boldsymbol{v}_1), f(\boldsymbol{v}_2), \dots, f(\boldsymbol{v}_k) \rangle = \langle \{\{\boldsymbol{v}_1\}_M, \{\boldsymbol{v}_2\}_M, \dots, \{\boldsymbol{v}_k\}_M \rangle$, čímž je důkaz větu dokončen. ■

10.3. Věta. *Dva vektorové prostory* V *a* V' *konečné dimenze jsou izomorfní, právě když mají stejnou dimenzi.*

Důkaz. Je-li $f : V \to V'$ izomorfismus a $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ je báze prostoru V, je podle věty 9.21 množina $\{f(\boldsymbol{u}_1), f(\boldsymbol{u}_2), \dots, f(\boldsymbol{u}_n)\}$ báze prostoru V', takže $\dim V = \dim V'$.

Předpokládejme naopak, že $\dim V = \dim V' = n$. Podle věty 10.2 existují izomorfismy $f : V \to T^n$ a $g : V' \to T^n$. Pak ale podle věty 9.7 (iii) je složení izomorfismu f a inverzního izomorfismu $g^{-1} : T^n \to V'$ opět izomorfismus $g^{-1}f : V \to V'$ a prostory V a V' jsou izomorfní. ■

10.4. Definice. Buď $f : V_n \to V_m$ homomorfismus, $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ báze prostoru V_n a $M' = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_m\}$ báze prostoru V_m. Označme $\{f(\boldsymbol{u}_i)\}_{M'} = (a_{1i}, a_{2i}, \dots, a_{mi})$ souřadnice vektoru $f(\boldsymbol{u}_i)$ vzhledem k bázi M' a utvořme matici

$\boldsymbol{A} = (a_{ij})$ typu (m, n). Matice $\boldsymbol{A}$ se nazývá *matice homomorfismu f vzhledem k bázím M a M'.*

10.5. Věta. *Buď $f : V_n \to V_m$ homomorfismus, $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ báze prostoru V_n, $M' = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_m\}$ báze prostoru V_m a $\boldsymbol{A} = (a_{ij})$ matice homomorfismu f vzhledem k bázím M a M'. Pak pro každý vektor $\boldsymbol{u} \in V_n$ je*

$$\{f(\boldsymbol{u})\}_{M'} = \{\boldsymbol{u}\}_M \cdot \boldsymbol{A}^T.$$

Důkaz. Označíme-li $\{\boldsymbol{u}\}_M = (x_1, x_2, \dots, x_n)$ souřadnice vektoru $\boldsymbol{u}$ vzhledem k bázi M, pak máme $\boldsymbol{u} = \sum_{i=1}^n x_i \boldsymbol{u}_i$. Protože podle předpokladu máme $f(\boldsymbol{u}_i) = \sum_{j=1}^m a_{ji}\boldsymbol{v}_j$, je $f(\boldsymbol{u}) = f(\sum_{i=1}^n x_i \boldsymbol{u}_i) = \sum_{i=1}^n x_i f(\boldsymbol{u}_i) = \sum_{i=1}^n x_i \sum_{j=1}^m a_{ji}\boldsymbol{v}_j = \sum_{j=1}^m (\sum_{i=1}^n x_i a_{ji})\boldsymbol{v}_j$, odkud je ihned patrné, že $\{f(\boldsymbol{u})\}_{M'} = \{\boldsymbol{u}\}_M \cdot \boldsymbol{A}^T$. ■

10.6. Věta. *Buďte $f : V_n \to V_m$ a $g : V_m \to V_k$ dva homomorfismy vektorových prostorů, buď M báze prostoru V_n, M' báze prostoru V_m a M'' báze prostoru V_k. Je-li $\boldsymbol{A}$ matice homomorfismu f vzhledem k bázím M a M' a $\boldsymbol{B}$ matice homomorfismu g vzhledem k bázím M' a M'', pak součin $\boldsymbol{BA}$ je maticí složeného homomorfismu $gf : V_n \to V_k$ vzhledem k bázím M a M''.*

Důkaz. Označíme-li $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$, $M' = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_m\}$ a $M'' = \{\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_k\}$, pak podle předpokladu je $f(\boldsymbol{u}_j) = \sum_{l=1}^m a_{lj}\boldsymbol{v}_l$, $j = 1, 2, \dots, n$, a $g(\boldsymbol{v}_l) = \sum_{i=1}^k b_{il}\boldsymbol{w}_i$, $l = 1, 2, \dots, m$. Odtud dostáváme $(gf)(\boldsymbol{u}_j) = g(f(\boldsymbol{u}_j)) = g(\sum_{l=1}^m a_{lj}\boldsymbol{v}_l) = \sum_{l=1}^m a_{lj} g(\boldsymbol{v}_l) = \sum_{l=1}^m a_{lj} \sum_{i=1}^k b_{il}\boldsymbol{w}_i = \sum_{i=1}^k (\sum_{l=1}^m b_{il}a_{lj})\boldsymbol{w}_i = \sum_{i=1}^k c_{ij}\boldsymbol{w}_i$, kde $c_{ij} = \sum_{l=1}^m b_{il}a_{lj}$. Vidíme tedy, že $\boldsymbol{C} = (c_{ij}) = \boldsymbol{BA}$ a věta je dokázána. ■

10.7. Věta. *Buď M báze vektorového prostoru V_n, M' báze vektorového prostoru V_m a buď $\boldsymbol{A} = (a_{ij})$ matice typu (m, n) nad tělesem T. Pak existuje právě jeden homomorfismus $f : V_n \to V_m$, jehož matice vzhledem k bázím M a M' je rovna $\boldsymbol{A}$.*

Důkaz. Nechť $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ a $M' = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_m\}$. Jestliže položíme $\boldsymbol{v}'_i = \sum_{j=1}^m a_{ji}\boldsymbol{v}_j$, existuje podle věty 9.22 právě jeden homomorfismus $f : V_n \to V_m$ takový, že $f(\boldsymbol{u}_i) = \boldsymbol{v}'_i$ pro všechna $i = 1, 2, \dots, n$. Matice homomorfismu f vzhledem k bázím M a M' je přitom zřejmě rovna $\boldsymbol{A}$. ■

10.8. Věta. *Buď $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ báze vektorového prostoru V a $M' = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n\}$ báze vektorového prostoru V' téže dimenze n. Pak homomorfismus $f : V \to V'$ prostoru V do prostoru V' je izomorfismus, právě když matice $\boldsymbol{A}$ homomorfismu f vzhledem k bázím M a M' je regulární. V tomto případě je matice $\boldsymbol{A}^{-1}$ matice homomorfismu $f^{-1} : V' \to V$ vzhledem k bázím M' a M.*

Důkaz. Buď nejprve f izomorfismus. Podle věty 9.8 existuje izomorfismus $g : V \to V'$ takový, že $gf = 1_V$. Označíme-li $\boldsymbol{B}$ matici homomorfismu g vzhledem k bázím M' a M, je podle věty 10.6 $\boldsymbol{BA}$ maticí homomorfismu gf vzhledem k bázím M a M. Protože $gf = 1_V$, je zřejmě $\boldsymbol{BA} = \boldsymbol{E}$ a $\boldsymbol{B} = \boldsymbol{A}^{-1}$ podle důsledku 8.5.

Je-li naopak matice $\boldsymbol{A}$ regulární, označme $\boldsymbol{B} = (b_{ij}) = \boldsymbol{A}^{-1}$ matici k ní inverzní. Podle věty 10.7 existuje homomorfismus $g : V' \to V$, jehož matice vzhledem k bázím M' a M je rovna $\boldsymbol{B}$. Podle věty 10.6 je $\boldsymbol{BA} = \boldsymbol{E}$ matice homomorfismu gf vzhledem k bázím M a M, $\boldsymbol{AB} = \boldsymbol{E}$ matice homomorfismu fg vzhledem k bázím M' a M'. To ale zřejmě znamená, že $gf = 1_V$, $fg = 1_{V'}$ a f je izomorfismus podle věty 9.8. Z právě provedené části důkazu bezprostředně plyne, že $\boldsymbol{B} = \boldsymbol{A}^{-1}$ je maticí izomorfismu f^{-1} vzhledem k bázím M' a M. ∎

10.9. Definice. Homomorfismus $f : V \to V$ vektorového prostoru V do V se nazývá *endomorfismus prostoru* V. V případě, že f je dokonce izomorfismus, hovoříme o *automorfismu prostoru* V. Je-li V prostor konečné dimenze a je-li M jeho báze, pak matice homomorfismu f vzhledem k bázím M a M se stručně nazývá *matice f vzhledem k bázi M*.

10.10. Věta. *Buď f endomorfismus vektorového prostoru V_n a buď M báze tohoto prostoru. Pak následující podmínky jsou ekvivalentní:*

(i) f je automorfismus;

(ii) f je monomorfismus;

(iii) f je epimorfismus;

(iv) matice $\boldsymbol{A}$ endomorfismu f vzhledem k bázi M je regulární.

Důkaz. Z (i) plyne zřejmě (ii). Je-li f monomorfismus, je podle věty 9.27 $\dim \operatorname{Im} f = n - \dim \operatorname{Ker} f = n$, takže $\operatorname{Im} f = V_n$ podle věty 2.22 a platí tedy (iii). Podobně, je-li splněna podmínka (iii), je $\dim \operatorname{Ker} f = n - \dim \operatorname{Im} f = 0$ podle věty 9.27, a f je tudíž monomorfismus podle věty 9.4 (ii). Podmínky (i) a (iv) jsou ekvivalentní podle věty 10.8. ∎

10.11. Definice. Buďte M a M' dvě báze vektorového prostoru V_n. *Maticí přechodu od báze M k bázi M'* rozumíme matici identického homomorfismu 1_V prostoru V vzhledem k bázím M' a M (opačné pořadí!).

10.12. Poznámka. Podívejme se na předchozí definici s ohledem na její význam poněkud podrobněji. Nechť $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ a $M' = \{\boldsymbol{u}'_1, \boldsymbol{u}'_2, \ldots, \boldsymbol{u}'_n\}$. Jestliže $\{1_V(\boldsymbol{u}'_i)\}_M = \{\boldsymbol{u}'_i\}_M = (a_{1i}, a_{2i}, \ldots, a_{ni})$ jsou souřadnice vektoru $\boldsymbol{u}'_i$ vzhledem k bázi M, pak čtvercová matice $\boldsymbol{A} = (a_{ij})$ je matice přechodu od báze M k bázi M'.

10.13. Věta. *Buďte M, M' báze vektorového prostoru V_n a N, N' báze vektorového prostoru V_m. Buď dále $\boldsymbol{A}$ matice přechodu od báze M k bázi M', $\boldsymbol{B}$ matice přechodu od báze N' k bázi N (opačné pořadí!) a $\boldsymbol{C}$ matice homomorfismu f vzhledem k bázím M a N. Pak $\boldsymbol{BCA}$ je matice homomorfismu f vzhledem k bázím M' a N'.*

Důkaz. Podle definice 10.11 je $\boldsymbol{A}$ matice identického homomorfismu 1_V vzhledem k bázím M' a M a $\boldsymbol{B}$ je matice $1_{V'}$ vzhledem k bázím N a N'. Z věty 10.6 tedy dostáváme, že $\boldsymbol{BCA}$ je matice homomorfismu $f = 1_{V'} f 1_V$ vzhledem k bázím M' a N'. ∎

10.14. Věta. *Buďte M a M' dvě báze vektorového prostoru V_n a buď $\boldsymbol{A}$ matice přechodu od báze M k bázi M'. Pak*

(i) $\{\boldsymbol{u}\}_M = \{\boldsymbol{u}\}_{M'} \cdot \boldsymbol{A}^T$ pro každý vektor $\boldsymbol{u} \in V_n$;

(ii) matice $\boldsymbol{A}$ je regulární a $\boldsymbol{A}^{-1}$ je maticí přechodu od báze M' k bázi M.

Důkaz. (i) Podle definice je $\boldsymbol{A}$ matice identického homomorfismu 1_V vzhledem k bázím M' a M. Věta 10.5 pak dává $\{\boldsymbol{u}\}_M = \{1_V(\boldsymbol{u})\}_M = \{\boldsymbol{u}\}_{M'} \cdot \boldsymbol{A}^T$.

(ii) Vzhledem k tom, že identický homomorfismus 1_V je sám k sobě inverzní, plyne tvrzení ihned z věty 10.8. ∎

10.15. Věta. *Buďte M, M', M'' báze vektorového prostoru V_n, buď $\boldsymbol{A}$ matice přechodu od báze M k bázi M' a $\boldsymbol{B}$ matice přechodu od báze M' k bázi M''. Pak $\boldsymbol{AB}$ je matice přechodu od báze M k bázi M''.*

Důkaz. Podle definice 10.11 je $\boldsymbol{A}$ matice automorfismu 1_V vzhledem k bázím M' a M a $\boldsymbol{B}$ je matice téhož automorfismu vzhledem k bázím M'' a M'. Pak ale podle věty 10.6 je $\boldsymbol{AB}$ matice automorfismu 1_V vzhledem k bázím M'' a M, tj. matice přechodu od báze M k bázi M''. ■

10.16. Věta. *Buď $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ báze vektorového prostoru V_n a buď $\boldsymbol{A} = (a_{ij})$ regulární čtvercová matice stupně n nad tělesem T. Pak množina $M' = \{\boldsymbol{u}'_1, \boldsymbol{u}'_2, \dots, \boldsymbol{u}'_n\}$, kde $\boldsymbol{u}'_i = \sum_{j=1}^n a_{ji}\boldsymbol{u}_j$, $i = 1, 2 \dots, n$, je bází prostoru V_n a $\boldsymbol{A}$ je matice přechodu od báze M k bázi M'.*

Důkaz. Zřejmě stačí ukázat, že množina M' je báze prostoru V_n. K tomu podle věty 2.19 stačí ukázat, že vektory $\boldsymbol{u}'_1, \boldsymbol{u}'_2, \dots, \boldsymbol{u}'_n$ jsou lineárně nezávislé. Nechť tedy $\sum_{i=1}^n r_i\boldsymbol{u}'_i = 0$. Po dosazení dostaneme $\sum_{i=1}^n r_i \sum_{j=1}^n a_{ji}\boldsymbol{u}_j = \sum_{j=1}^n (\sum_{i=1}^n r_i a_{ji})\boldsymbol{u}_j = 0$, takže vzhledem k lineární nezávislosti vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n$ je $\sum_{i=1}^n r_i a_{ji} = 0$ pro každé $j = 1, 2, \dots, n$. Buď $\boldsymbol{B} = (b_{ij}) = \boldsymbol{A}^{-1}$ matice inverzní k matici $\boldsymbol{A}$ a buď $k \in \{1, 2, \dots, n\}$ libovolný index. Vynásobme každou z rovností $\sum_{i=1}^n r_i a_{ji} = 0$ prvkem b_{kj} a všechny takto získané rovnosti sečtěme podle j. Uvědomíme-li si, že z rovnosti $\boldsymbol{BA} = \boldsymbol{E}$ dostáváme pro každou dvojici indexů $k, i \in \{1, 2, \dots, n\}$ rovnost $\sum_{j=1}^n b_{kj}a_{ji} = e_{ki} = \delta_{ki}$, máme $0 = \sum_{j=1}^n b_{kj} \sum_{i=1}^n r_i a_{ji} = \sum_{i=1}^n r_i \sum_{j=1}^n b_{kj}a_{ji} = \sum_{i=1}^n r_i\delta_{ki} = r_k$. Vidíme tedy, že $r_1 = r_2 = \dots = r_n = 0$, vektory $\boldsymbol{u}'_1, \boldsymbol{u}'_2, \dots, \boldsymbol{u}'_n$ jsou lineárně nezávislé a věta je dokázána. ■

10.17. Věta. *Buďte M , M' báze vektorového prostoru V_n, buď $\boldsymbol{A}$ matice přechodu od báze M k bázi M' a buď $\boldsymbol{B}$ matice endomorfismu $f : V_n \to V_n$ vektorového prostoru V_n vzhledem k bázi M. Pak $\boldsymbol{A}^{-1}\boldsymbol{BA}$ je matice endomorfismu f vzhledem k bázi M'.*

Důkaz. Podle věty 10.14 (ii) je $\boldsymbol{A}^{-1}$ matice přechodu od báze M' k bázi M, takže tvrzení je bezprostředním důsledkem věty 10.13. ■

10.18. Definice. *Hodností $h(f)$ homomorfismu $f : V_n \to V_m$* rozumíme dimenzi obrazu $\operatorname{Im} f$.

10.19. Věta. *Buď M báze vektorového prostoru V_n, M' báze vektorového prostoru V_m a buď $\boldsymbol{A}$ matice homomorfismu $f : V_n \to V_m$ vzhledem k bázím M a M'. Pak $h(f) = h(\boldsymbol{A})$.*

Důkaz. Nechť $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$. Protože podle věty 5.5 je $h(\boldsymbol{A}) = h(\boldsymbol{A}^T)$, plynou z vět 9.11 a 10.2 (iv) rovnosti $h(f) = \dim \operatorname{Im} f = \dim f(V_n) = \dim f(\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n \rangle) = \dim \langle f(\boldsymbol{u}_1), f(\boldsymbol{u}_2), \dots, f(\boldsymbol{u}_n)\rangle = \dim \langle \{f(\boldsymbol{u}_1)\}_{M'}, \{f(\boldsymbol{u}_2)\}_{M'}, \dots, \{f(\boldsymbol{u}_n)\}_{M'}\rangle = h(\boldsymbol{A}^T) = h(\boldsymbol{A})$ vzhledem k tom, že vektory $\{f(\boldsymbol{u}_1)\}_{M'}$, $\{f(\boldsymbol{u}_2)\}_{M'}$, $\dots, \{f(\boldsymbol{u}_n)\}_{M'}$ jsou sloupcové vektory matice $\boldsymbol{A}$. ■

10.20. Poznámka. Buď $\boldsymbol{B}$ regulární čtvercová matice stupně n, $\boldsymbol{C}$ regulární čtvercová matice stupně m a buď $\boldsymbol{A}$ matice typu (n, m) nad tělesem T. Je-li M báze vektorového prostoru V_m a N báze vektorového prostoru V_n, pak podle věty 10.7 existuje právě jeden homomorfismus $f : V_m \to V_n$, jehož matice vzhledem k bázím

M a N je rovna $\boldsymbol{A}$. Dále podle věty 10.16 existuje báze M' prostoru V_m taková, že $\boldsymbol{C}$ je matice přechodu od báze M k bázi M'. Podobně existuje báze N' prostoru V_n taková, že $\boldsymbol{B}^{-1}$ je matice přechodu od báze N k bázi N'. Podle věty 10.14 (ii) je $\boldsymbol{B}$ matice přechodu od báze N' k bázi N, takže podle věty 10.13 je $\boldsymbol{BAC}$ matice homomorfismu f vzhledem k bázím M' a N'. Použitím předchozí věty tak dostáváme $h(\boldsymbol{A}) = h(f) = h(\boldsymbol{BAC})$, a tedy jiný důkaz věty 8.16.

10.21. Poznámka. Nechť V a V' jsou dva vektorové prostory nad tělesem T. Množina všech homomorfismů prostoru V do prostoru V' se obvykle značí symbolem $\mathrm{Hom}\,(V, V')$ a není obtížné ověřit, že tato množina je vzhledem k operacím sčítání homomorfismů a násobení homomorfismu prvkem z tělesa T z definice 9.6 vektorovým prostorem nad tělesem T. Stejně snadno se ověří, že množina $T_{m,n}$ všech matic typu (m, n) nad tělesem T je vzhledem k operacím sčítání matic a násobení matice prvkem z T z definice 4.1 rovněž vektorovým prostorem nad tělesem T. Buď M báze vektorového prostoru V_n a M' buď báze vektorového prostoru V_m. Podle definice 10.4 je pak každému homomorfismu $f : V_n \to V_m$ jednoznačně přiřazena matice typu (m, n) nad tělesem T, totiž matice tohoto homomorfismu vzhledem k bázím M a M' příslušných prostorů. Označíme-li nyní matici homomorfismu f vzhledem k bázím M a M' symbolem $\varphi(f)$, dostaneme zobrazení $\varphi : \mathrm{Hom}\,(V_n, V_m) \to T_{m,n}$.

10.22. Věta. *Zobrazení $\varphi : \mathrm{Hom}\,(V_n, V_m) \to T_{m,n}$ z předchozí poznámky je izomorfismus vektorového prostoru* $\mathrm{Hom}\,(V_n, V_m)$ *všech homomorfismů vektorového prostoru V_n do vektorového prostoru V_m na vektorový prostor $T_{m,n}$ všech matic typu (m, n) nad tělesem T. Přitom* $\dim T_{m,n} = \dim \mathrm{Hom}\,(V_n, V_m) = mn$.

Důkaz. Buď $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ a nechť $f, g : V_n \to V_m$ jsou dva homomorfismy. Pak podle definice 9.6 a věty 10.2 je $\{(f + g)(\boldsymbol{u}_i)\}_{M'} = \{f(\boldsymbol{u}_i) + g(\boldsymbol{u}_i)\}_{M'} = \{f(\boldsymbol{u}_i)\}_{M'} + \{g(\boldsymbol{u}_i)\}_{M'}$ a $\{(rf)(\boldsymbol{u}_i)\}_{M'} = \{rf(\boldsymbol{u}_i)\}_{M'} = r\{f(\boldsymbol{u}_i)\}_{M'}$ pro každé $r \in T$, odkud vzhledem k definici 4.1 ihned plyne, že je-li $\boldsymbol{A}$ matice homomorfismu f a $\boldsymbol{B}$ matice homomorfismu g vzhledem k bázím M a M', pak $\boldsymbol{A} + \boldsymbol{B}$ je matice homomorfismu $f + g$ a $r\boldsymbol{A}$ je matice homomorfismu rf vzhledem k bázím M a M'. Vidíme tedy, že $\varphi(f+g) = \varphi(f) + \varphi(g)$, $\varphi(rf) = r\varphi(f)$ a φ je homomorfismus. Z věty 10.7 je ihned patrné, že φ je epimorfismus. Dále, je-li $\varphi(f) = 0$, je $\{f(\boldsymbol{u}_i)\}_{M'} = 0$ takže $f(\boldsymbol{u}_i) = 0$ pro každé $i = 1, 2, \ldots, n$ podle věty 10.2(ii). Pak ale $f = 0$ je nulový homomorfismus, $\mathrm{Ker}\,\varphi = 0$ a φ je izomorfismus podle věty 9.4. Zbývá tedy dokázat tvrzení o dimenzích, přičemž vzhledem k větě 10.3 stačí ověřit, že $\dim T_{m,n} = m \cdot n$. Pro každé $i = 1, 2, \ldots, m$ a každé $j = 1, 2, \ldots, n$ označme $\boldsymbol{E}^{(i,j)} = (r_{kl})$ matici typu (m, n) nad tělesem T takovou, že $r_{ij} = 1$ a $r_{kl} = 0$, kdykoliv $k \neq i$ nebo $l \neq j$. Je-li nyní $\boldsymbol{A} = (a_{ij})$ libovolná matice z $T_{m,n}$, je zřejmě $\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} \boldsymbol{E}^{(i,j)} = \boldsymbol{A}$, takže $\{\boldsymbol{E}^{(i,j)} \mid i = 1, 2, \ldots, m, j = 1, 2, \ldots, n\}$ je množina generátorů prostoru $T_{m,n}$. Na druhé straně, vezmeme-li lineární kombinaci $\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} \boldsymbol{E}^{(i,j)}$ a položíme ji rovnou nulové matici, vidíme ihned, že $a_{ij} = 0$ pro všechna $i = 1, 2, \ldots, m$ a $j = 1, 2, \ldots, n$, a množina $\{\boldsymbol{E}^{(i,j)} \mid i = 1, 2, \ldots, m, j = 1, 2, \ldots, n\}$ je báze prostoru $T_{m,n}$ a jsme hotovi. ■

10.23. Důsledek. *(i) Množina $\{\boldsymbol{E}^{(i,j)} \mid i = 1, 2, \ldots, m, j = 1, 2, \ldots, n\}$ matic $\boldsymbol{E}^{(i,j)} = (r_{kl})$, kde $r_{ij} = 1$ a $r_{kl} = 0$, kdykoliv buď $k \neq i$, nebo $l \neq j$ tvoří bázi vektorového prostoru $T_{m,n}$ všech matic typu (m, n) nad tělesem T;*

(ii) buď $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ báze vektorového prostoru V_n a $M' = \{\boldsymbol{u}'_1, \boldsymbol{u}'_2, \ldots, \boldsymbol{u}'_m\}$ báze vektorového prostoru V_m nad tělesem T. Pak množina $\{f_{ij} \mid i = 1, 2, \ldots, n,\ j = 1, 2, \ldots, m\}$ homomorfismů prostoru V_n do prostoru V_m takových, že $f_{ij}(\boldsymbol{u}_i) = \boldsymbol{u}'_j$ a $f_{ij}(\boldsymbol{u}_k) = 0$, kdykoliv $k \neq i$, tvoří bázi vektorového prostoru $\mathrm{Hom}\,(V_n, V_m)$.

Důkaz. (i) Toto tvrzení bylo dokázáno v důkazu předchozí věty.

(ii) Matice homomorfismu f_{ij} vzhledem k bázím M a M' je zřejmě matice $\boldsymbol{E}^{(j,i)}$, takže $\varphi(f_{ij}) = \boldsymbol{E}^{(j,i)}$ neboli $\varphi^{-1}(\boldsymbol{E}^{(j,i)}) = f_{ij}$, kde φ^{-1} je izomorfismus inverzní k izomorfismu φ. Nyní stačí použít větu 9.21. ∎

11.1. Definice. Homomorfismus $f : V \to T$ vektorového prostoru V nad tělesem T do tělesa T nazýváme *lineární formou* na vektorovém prostoru V. Je-li $f = 0$, tj. $f(\boldsymbol{u}) = 0$ pro každé $\boldsymbol{u} \in V$, nazývá se forma *triviální* nebo *nulová*. V opačném případě se forma f nazývá *netriviální*.

11.2. Definice. Nechť V je vektorový prostor nad tělesem T. Vektorový prostor $\mathrm{Hom}\,(V, T)$ všech lineárních forem na V se nazývá *duální prostor* k prostoru V a značí se $\widetilde{V}$.

11.3. Věta. *Je-li V_n vektorový prostor dimenze n, pak $\widetilde{V}_n$ má rovněž dimenzi n.*

Důkaz. Protože $\dim T = 1$ je $\dim \widetilde{V}_n = \dim \mathrm{Hom}\,(V_n, T) = n$ podle věty 10.22. ∎

11.4. Definice. Buď $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ báze vektorového prostoru V_n. Pak množina $\widetilde{M} = \{f_1, f_2, \dots, f_n\}$ lineárních forem na V_n takových, že $f_i(\boldsymbol{u}_j) = \delta_{ij}$ pro všechna $i, j = 1, 2, \dots, n$, je podle důsledku 10.23 (zde je $M' = \{1\}$) bází duálního prostoru $\widetilde{V}_n$ a nazývá se *duální bází* k bázi M.

11.5. Definice. Buď $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ báze vektorového prostoru V_n a buď f lineární forma na V_n. Prvky $r_i = f(\boldsymbol{u}_i) \in T$, $i = 1, 2, \dots, n$, se nazývají *koeficienty lineární formy f vzhledem k bázi M*. Vektor $\{f\}_M = (r_1, r_2, \dots, r_n) \in T^n$ nazýváme *souřadnicemi formy f* vzhledem k bázi M. Jestliže $\{\boldsymbol{u}\}_M = (x_1, x_2, \dots, x_n)$, pak výraz $f(\boldsymbol{u}) = \sum_{i=1}^n r_i x_i$ nazýváme *analytickým vyjádřením formy f* vzhledem k bázi M.

11.6. Poznámka. Ve smyslu definice 10.4 a poznámky 10.21 je každé lineární formě f na vektorovém prostoru V_n přiřazena matice typu $(1, n)$ nad tělesem T tak, že pokud $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ je báze prostoru V_n a vezmeme-li $M' = \{1\}$ za bázi prostoru T, je $\{f\}_M$ právě matice formy f vzhledem k bázím M a M'. V předchozí definici jsme uspořádanou n-tici koeficientů $(r_1, r_2, \dots, r_n)$ formy f vzhledem k bázi M nazvali souřadnicemi $\{f\}_M$ formy f vzhledem k bázi M. V následující větě ukážeme oprávněnost tohoto pojmu tím, že dokážeme, že $\{f\}_M$ jsou vlastně souřadnice lineární formy f jakožto vektoru z duálního prostoru $\widetilde{V}_n$ vzhledem k bázi $\widetilde{M}$ duální k bázi M.

11.7. Věta. *Buď $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ báze vektorového prostoru V_n a $\widetilde{M} = \{f_1, f_2, \dots, f_n\}$ buď báze duálního prostoru $\widetilde{V}_n$ duální k bázi M. Pak pro každé $f \in \widetilde{V}_n$ je $\{f\}_M = \{f\}_{\widetilde{M}}$. Duálně pro každý vektor $\boldsymbol{u} \in V_n$ je $\{\boldsymbol{u}\}_M = (f_1(\boldsymbol{u}), f_2(\boldsymbol{u}), \dots, f_n(\boldsymbol{u}))$.*

Důkaz. Označíme-li $\{f\}_M = (r_1, r_2, \dots, r_n)$ a $\{f\}_{\widetilde{M}} = (x_1, x_2, \dots, x_n)$, pak máme $r_i = f(\boldsymbol{u}_i)$ pro každé $i = 1, 2, \dots, n$ a $f = \sum_{j=1}^n x_j f_j$. Potom ale je $r_i = f(\boldsymbol{u}_i) = (\sum_{j=1}^n x_j f_j)(\boldsymbol{u}_i) = \sum_{j=1}^n x_j f_j(\boldsymbol{u}_i) = \sum_{j=1}^n x_j \delta_{ij} = x_i$. Duálně, pro $\{\boldsymbol{u}\}_M = (x_1, x_2, \dots, x_n)$, tj. $\boldsymbol{u} = \sum_{j=1}^n x_j \boldsymbol{u}_j$ máme $f_i(\boldsymbol{u}) = f_i(\sum_{j=1}^n x_j \boldsymbol{u}_j) = \sum_{j=1}^n x_j f_i(\boldsymbol{u}_j) = \sum_{j=1}^n x_j \delta_{ij} = x_i$, což jsme chtěli dokázat. ∎

11.8. Věta. *Buďte M a M' dvě báze vektorového prostoru V_n. Je-li $\boldsymbol{A}$ matice přechodu od báze M k bázi M', pak $(\boldsymbol{A}^{-1})^T$ je matice přechodu od báze $\widetilde{M}$ k bázi $\widetilde{M}'$.*

Důkaz. Vzhledem k větě 8.6 (iii) stačí podle věty 10.14 (ii) ukázat, že $\boldsymbol{A}^T$ je matice přechodu od báze $\widetilde{M}'$ k bázi $\widetilde{M}$. Nechť tedy $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$, $M' = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n\}$, $\widetilde{M} = \{g_1, g_2, \dots, g_n\}$ a $\widetilde{M}' = \{f_1, f_2, \dots, f_n\}$. Označíme-li $\boldsymbol{B} = (b_{ij})$ matici přechodu od báze $\widetilde{M}'$ k bázi $\widetilde{M}$, pak máme $g_i = \sum_{j=1}^n b_{ji} f_j$, takže podle věty 11.7 je $b_{ji} = g_i(\boldsymbol{v}_j)$. Protože $\boldsymbol{v}_j = \sum_{k=1}^n a_{kj}\boldsymbol{u}_k$, je $b_{ji} = g_i(\sum_{k=1}^n a_{kj}\boldsymbol{u}_k) = \sum_{k=1}^n a_{kj} g_i(\boldsymbol{u}_k) = \sum_{k=1}^n a_{kj}\delta_{ik} = a_{ij}$ a $\boldsymbol{B} = \boldsymbol{A}^T$. ■

11.9. Věta. *Buďte M a M' dvě báze vektorového prostoru V_n a buď $\boldsymbol{A}$ matice přechodu od báze M k bázi M'. Je-li f lineární forma na prostoru V_n, pak $\{f\}_{M'} = \{f\}_M \cdot \boldsymbol{A}$.*

Důkaz. Podle předchozí věty je $(\boldsymbol{A}^{-1})^T$ matice přechodu od báze $\widetilde{M}$ k bázi $\widetilde{M}'$. Protože $(\boldsymbol{A}^{-1})^T = (\boldsymbol{A}^T)^{-1}$ podle věty 8.6 (iii), je $\boldsymbol{A}^T$ matice přechodu od báze $\widetilde{M}'$ k bázi $\widetilde{M}$. Použitím vět 11.7 a 10.14 (i) pak máme $\{f\}_{M'} = \{f\}_{\widetilde{M}'} = \{f\}_{\widetilde{M}} \cdot (\boldsymbol{A}^T)^T = \{f\}_M \cdot \boldsymbol{A}$. ■

11.10. Definice. Každý podprostor dimenze $n-1$ vektorového prostoru V_n se nazývá *nadrovina*. Je-li f lineární forma na vektorovém prostoru V, pak jádro $\operatorname{Ker} f$ se nazývá *nulová množina* lineární formy f.

11.11. Věta. *Podprostor W vektorového prostoru V_n je nadrovina, právě když pro libovolný vektor $\boldsymbol{u} \in V_n \setminus W$ je $W \vee \langle \boldsymbol{u} \rangle = V_n$.*

Důkaz. Je-li W nadrovina ve V_n, pak pro libovolný vektor $\boldsymbol{u} \in V_n \setminus W$ je $\dim W < \dim(W \vee \langle \boldsymbol{u} \rangle)$, takže nutně $\dim(W \vee \langle \boldsymbol{u} \rangle) = n$ a $W \vee \langle \boldsymbol{u} \rangle = V_n$ podle věty 2.22.

Nechť tedy naopak $W \vee \langle \boldsymbol{u} \rangle = V_n$ pro nějaký vektor $\boldsymbol{u} \in V_n \setminus W$. Pak $W \cap \langle \boldsymbol{u} \rangle = 0$, neboť pro $0 \neq r\boldsymbol{u} \in W$ je $r \neq 0$, a tedy $\boldsymbol{u} = r^{-1}(r\boldsymbol{u}) \in W$, což není možné. Podle věty o dimenzi spojení a průniku 2.23 pak máme $\dim W = \dim(W \vee \langle \boldsymbol{u} \rangle) + \dim(W \cap \langle \boldsymbol{u} \rangle) - \dim \langle \boldsymbol{u} \rangle = n-1$ a W je nadrovina ve V_n. ■

11.12. Poznámka. Předchozí věta nám umožňuje zavést pojem nadroviny v libovolném vektorovém prostoru jako každý podprostor, ze kterého přidáním jediného vektoru dostaneme celý prostor. Je-li tedy W nadrovina ve V a $\boldsymbol{u} \in V \setminus W$ libovolný vektor, je předně $W \cap \langle \boldsymbol{u} \rangle = 0$, neboť pro $0 \neq \boldsymbol{u} \in W$ je $r \neq 0$, a tedy $\boldsymbol{u} = r^{-1} r\boldsymbol{u} \in W$, což je spor s volbou vektoru $\boldsymbol{u}$. Je-li nyní $v \in V$ libovolný vektor, můžeme tento vektor zapsat ve tvaru $\boldsymbol{v} = r\boldsymbol{u} + \boldsymbol{w}$, $w \in W$, a to jediným způsobem. Skutečně, je-li $r\boldsymbol{u} + \boldsymbol{w} = s\boldsymbol{u} + \widetilde{\boldsymbol{w}}$, je $(r-s)\boldsymbol{u} = \widetilde{\boldsymbol{w}} - \boldsymbol{w} \in W \cap \langle \boldsymbol{u} \rangle = 0$, takže $r = s$ a $\boldsymbol{w} = \widetilde{\boldsymbol{w}}$.

11.13. Definice. Podprostor W vektorového prostoru V se nazývá *nadrovina*, jestliže existuje vektor $\boldsymbol{u} \in V$ takový, že $W \vee \langle \boldsymbol{u} \rangle = V$. Poznamenejme, že pak $V = W \vee \langle \boldsymbol{u} \rangle$ pro libovolný vektor $\boldsymbol{u} \in V \setminus W$.

11.14. Věta. *Buď V vektorový prostor nad tělesem T.*

(i) Je-li f netriviální lineární forma na V, pak $\operatorname{Ker} f$ *je nadrovina ve V;*
(ii) je-li W nadrovina ve V, pak existuje netriviální lineární forma f na V taková, že $\operatorname{Ker} f = W$*;*

(iii) jsou-li f, g lineární formy na V, pak $\operatorname{Ker} f = \operatorname{Ker} g$, *právě když* $g = rf$ *pro nějaký nenulový prvek* $r \in T$.

Důkaz. (i) Protože f je netriviální, existuje vektor $\boldsymbol{u} \in V$ takový, že $f(\boldsymbol{u}) = r \neq 0$. Označme $W = \operatorname{Ker} f$ a buď $\boldsymbol{v} \in V$ libovolný vektor. Označíme-li $f(\boldsymbol{v}) = s$, máme $f(\boldsymbol{v}) = s = \frac{s}{r} \cdot f(\boldsymbol{u}) = f(\frac{s}{r}\boldsymbol{u})$, takže $f(\boldsymbol{v} - \frac{s}{r}\boldsymbol{u}) = 0$. Vidíme tedy, že $\boldsymbol{v} - \frac{s}{r}\boldsymbol{u} = \boldsymbol{w} \in W$, odkud $\boldsymbol{v} = \boldsymbol{w} + \frac{s}{r}\boldsymbol{u} \in W \vee \langle \boldsymbol{u} \rangle$ a W je nadrovina ve V.

(ii) Podle předpokladu existuje vektor $\boldsymbol{u} \in V$ takový, že $W \vee \langle \boldsymbol{u} \rangle = V$ a podle poznámky 11.12 má každý vektor $\boldsymbol{v} \in V$ jednoznačné vyjádření ve tvaru $\boldsymbol{v} = \boldsymbol{w} + r\boldsymbol{u}$, $r \in T$, $\boldsymbol{w} \in W$. Definujeme-li nyní zobrazení $f : V \to T$ předpisem $f(\boldsymbol{w} + r\boldsymbol{u}) = r$, je f zřejmě lineární forma na V a $\operatorname{Ker} f = W$.

(iii) Jestliže $g = rf$ pro nějaké $0 \neq r \in T$, je $f(\boldsymbol{v}) = 0$, právě když $g(\boldsymbol{v}) = rf(\boldsymbol{v}) = 0$, a tedy $\operatorname{Ker} f = \operatorname{Ker} g$. Nechť tedy naopak $\operatorname{Ker} f = \operatorname{Ker} g = W$. Je-li $W = V$, jsou formy f a g triviální, a tedy $g = 1 \cdot f = 0$. V opačném případě je W nadrovina ve V, $V = W \vee \langle \boldsymbol{u} \rangle$ pro nějaký vektor $\boldsymbol{u} \in V$. Protože $\boldsymbol{u} \notin W$, je $f(\boldsymbol{u}) \neq 0 \neq g(\boldsymbol{u})$, takže $g(\boldsymbol{u}) = rf(\boldsymbol{u})$ pro nějaký nenulový prvek $r \in T$. Pak ale libovolný vektor $\boldsymbol{v} \in V$ můžeme zapsat ve tvaru $\boldsymbol{v} = \boldsymbol{w} + s\boldsymbol{u}$, $\boldsymbol{w} \in W$, a $g(\boldsymbol{v}) = g(\boldsymbol{w} + s\boldsymbol{u}) = g(s\boldsymbol{u}) = sg(\boldsymbol{u}) = srf(\boldsymbol{u}) = rf(s\boldsymbol{u}) = rf(\boldsymbol{w} + s\boldsymbol{u}) = rf(\boldsymbol{v})$, takže $g = rf$ a jsme hotovi. ∎

11.15. Věta. *Buďte $f_1, f_2, \ldots, f_k$ lineární formy na vektorovém prostoru V_n.*

(i) Lineární forma f je lineární kombinací vektorů $f_1, f_2, \ldots, f_k \in \widetilde{V}_n$, právě když $\bigcap_{i=1}^{k} \operatorname{Ker} f_i \subseteq \operatorname{Ker} f$;

(ii) vektory $f_1, f_2, \ldots f_k \in \widetilde{V}_n$ jsou lineárně nezávislé, právě když $\dim \bigcap_{i=1}^{k} \operatorname{Ker} f_i = n - k$.

Důkaz. (i) Je-li $f = \sum_{i=1}^{k} r_i f_i$, je zřejmě $\bigcap_{i=1}^{k} \operatorname{Ker} f_i \subseteq \operatorname{Ker} f$. Předpokládejme tedy naopak, že $\bigcap_{i=1}^{k} \operatorname{Ker} f_i \subseteq \operatorname{Ker} f$, a postupujme indukcí podle k. Pro $k = 1$ je $\operatorname{Ker} f_1 \subseteq \operatorname{Ker} f$, takže pro $\operatorname{Ker} f = V_n$ je $f = 0 = 0 \cdot f_1$, zatímco pro $\operatorname{Ker} f_1 = \operatorname{Ker} f$ stačí použít větu 11.14 (iii). Nechť tedy $k > 1$ a předpokládejme, že pro $k-1$ tvrzení platí. Označme $W = \bigcap_{i=1}^{k} \operatorname{Ker} f_i$ a $W' = \bigcap_{i=1}^{k-1} \operatorname{Ker} f_i$. Pro $W' \subseteq \operatorname{Ker} f$ je podle indukčního předpokladu $f = \sum_{i=1}^{k-1} r_i f_i = \sum_{i=1}^{k-1} r_i f_i + 0 \cdot f_k$. V opačném případě je $W = W' \cap \operatorname{Ker} f_k$, přičemž $\operatorname{Ker} f_k$ je nadrovina ve V_n (jinak totiž $\operatorname{Ker} f_k = V_n$ a $W = W' \subseteq \operatorname{Ker} f$). Podle věty o dimenzi spojení a průniku máme 2.23 $\dim W + \dim(W' \vee \operatorname{Ker} f_k) = \dim W' + n - 1$, a tedy $\dim W' = \dim W + 1$. Vidíme tedy, že W je nadrovina ve W', takže podle poznámky 11.12 je $W' = W \vee \langle \boldsymbol{u} \rangle$ pro nějaký vektor $\boldsymbol{u} \in W' \setminus W$ a každý vektor $\boldsymbol{w}' \in W'$ lze jednoznačně zapsat ve tvaru $\boldsymbol{w}' = r\boldsymbol{u} + \boldsymbol{w}$, $r \in T$, $\boldsymbol{w} \in W$. Protože $\boldsymbol{u} \notin W$, je $f_k(\boldsymbol{u}) \neq 0$, takže $f(\boldsymbol{u}) = r_k f_k(\boldsymbol{u})$ pro nějaký prvek $r_k \in T$. Pak ale $(f - r_k f_r)(\boldsymbol{u}) = 0$, a tedy $W' \subseteq \operatorname{Ker}(f - r_k f_k)$ vzhledem k tomu, že $(f - r_k f_k)(\boldsymbol{w}') = (f - r_k f_k)(r\boldsymbol{u} + \boldsymbol{w}) = (f - r_k f_k)(r\boldsymbol{u}) + (f - r_k f_k)(\boldsymbol{w}) = r(f - r_k f_k)(\boldsymbol{u}) + f(\boldsymbol{w}) - r_k f_k(\boldsymbol{w}) = 0$, neboť $W \subseteq \operatorname{Ker} f_k$ a $W \subseteq \operatorname{Ker} f$ podle předpokladu. Použitím indukčního předpokladu tedy je $f - r_k f_k = \sum_{i=1}^{k-1} r_i f_i$, a tedy $f = \sum_{i=1}^{k} r_i f_i$.

(ii) Předpokládejme nejprve, že formy $f_1, f_2, \ldots, f_k$ jsou lineárně nezávislé, a postupujme úplnou indukcí podle k. Pro $k = 1$ je $f_1 \neq 0$ podle poznámky 2.6 a stačí použít větu 11.14 (i). Pro $k > 1$ jsou vektory $f_1, f_2, \ldots, f_{k-1}$ lineárně nezávislé podle věty 2.7, takže podle indukčního předpokladu je $\dim \bigcap_{i=1}^{k-1} \operatorname{Ker} f_i = n - (k-1) = n - k + 1$. Nyní podprostor $W' = \bigcap_{i=1}^{k-1} \operatorname{Ker} f_i$ není obsažen v $\operatorname{Ker} f_k$, neboť v opačném případě by vektor f_k byl podle prvního tvrzení lineární kombinací vektorů $f_1, f_2, \dots, f_{k-1}$, což vzhledem k lineární nezávislosti forem $f_1, f_2, \dots, f_k$ není možné. Protože $\operatorname{Ker} f_k$ je nadrovina ve V_n, je $W' \vee \operatorname{Ker} f_k = V_n$ a podle věty o dimenzi spojení a průniku 2.23 máme $\dim \cap_{i=1}^{k} \operatorname{Ker} f_i = \dim(W' \cap \operatorname{Ker} f_k) = \dim W' + \dim \operatorname{Ker} f_k - \dim (W' \vee \operatorname{Ker} f_k) = n - k + 1 + n - 1 - n = n - k$.

Předpokládejme tedy naopak, že $\dim \cap_{i=1}^{k} \operatorname{Ker} f_i = n - k$ ukažme, že formy $f_1, f_2, \dots, f_k$ jsou lineárně nezávislé. Budeme postupovat nepřímo. Jsou-li vektory $f_1, f_2, \dots, f_k$ lineárně závislé, můžeme podle věty 2.12 předpokládat, že při vhodném očíslování vektorů $f_1, f_2, \dots, f_k$ je množina $\{f_1, f_2, \dots, f_l\}$ bází lineárního obalu $\langle f_1, f_2, \dots, f_k \rangle$, přičemž zřejmě $l < k$. Podle (i) je $\cap_{i=1}^{l} \operatorname{Ker} f_i \subseteq \operatorname{Ker} f_j$ pro každé $j \in \{l+1, \dots, k\}$, takže $\cap_{i=1}^{l} \operatorname{Ker} f_i = \cap_{i=1}^{k} \operatorname{Ker} f_i$. Podle první části důkazu pak máme $\dim \cap_{i=1}^{k} \operatorname{Ker} f_i = \dim \cap_{i=1}^{l} \operatorname{Ker} f_i = n - l > n - k$, což jest spor s předpokladem a důkaz je hotov. ∎

11.16. Poznámka. V definici 11.4 jsme zavedli pojem duální báze $\widetilde{M}$ vektorového prostoru $\widetilde{V}_n$ k bázi M vektorového prostoru V_n, jejíž existence plyne bezprostředně z důsledku 10.23. V tomto okamžiku máme již dostatek teoretických poznatků k tomu, abychom ukázali, že mezi bázemi prostoru V_n a bázemi k nim duálními je vzájemně jednoznačná korespondence v tom smyslu, že ke každé bázi N prostoru $\widetilde{V}_n$ existuje právě jedna báze M prostoru V_n taková, že $\widetilde{M} = N$. Můžeme tedy říkat, že báze M a $\widetilde{M}$ jsou *vzájemně duální.*

11.17. Věta. *Buď $N = \{f_1, f_2, \dots, f_n\}$ báze vektorového prostoru $\widetilde{V}_n$. Pak existuje právě jedna báze $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ vektorového prostoru V_n taková, že $\widetilde{M} = N$.*

Důkaz. Začneme s důkazem existence. Pro každé $i = 1, 2, \dots, n$ je podle věty 11.15 (ii) $\dim \bigcap_{\substack{j=1 \\ j \neq i}}^{n} \operatorname{Ker} f_j = 1$, takže $\bigcap_{\substack{j=1 \\ j \neq i}}^{n} \operatorname{Ker} f_j = \langle \boldsymbol{v}_i \rangle$ pro nějaký vektor $\boldsymbol{v}_i \in V_n$. Přitom $f_i(\boldsymbol{v}_i) = c_i \neq 0$ vzhledem k tomu, že podle téže věty je $\cap_{j=1}^{n} \operatorname{Ker} f_j = 0$. Položíme-li $\boldsymbol{u}_i = \frac{1}{c_i} \boldsymbol{v}_i$ pro každé $i = 1, 2, \dots, n$ je zřejmě $f_j(\boldsymbol{u}_i) = \delta_{ji}$, $i, j = 1, 2, \dots, n$, takže zbývá ukázat, že vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n$ tvoří bázi prostoru V_n. K tomu stačí podle věty 2.19 ověřit lineární nezávislost těchto vektorů. Jestliže $\sum_{i=1}^{n} x_i \boldsymbol{u}_i = 0$, pak pro každé $j = 1, 2, \dots, n$ je $0 = f_j(0) = f_j(\sum_{i=1}^{n} x_i \boldsymbol{u}_i) = \sum_{i=1}^{n} x_i \delta_{ij} = x_j$ a důkaz existence je hotov.

Ukažme nyní jednoznačnost. Je-li $M' = \{\boldsymbol{u}_1', \boldsymbol{u}_2', \dots, \boldsymbol{u}_n'\}$ báze vektorového prostoru V_n taková, že $f_j(\boldsymbol{u}_i') = \delta_{ji}$ pro všechna $i, j = 1, 2, \dots, n$, pak $\boldsymbol{u}_i' \in \bigcap_{\substack{j=1 \\ j \neq i}}^{n} \operatorname{Ker} f_j = \langle \boldsymbol{u}_i \rangle$, takže $\boldsymbol{u}_i' = r_i \boldsymbol{u}_i$ pro nějaké $r_i \in T$, $i = 1, 2, \dots, n$. Přitom $1 = f_i(\boldsymbol{u}_i') = f_i(r_i \boldsymbol{u}_i) = r_i$, $i = 1, 2, \dots, n$, a tedy $M' = M$. ∎

11.18. Poznámka. V předchozí větě jsme viděli, že báze prostoru V_n a báze prostoru $\widetilde{V}_n$ k ní duální si vzájemně jednoznačně odpovídají. Ve zbývající části tohoto odstavce si ukážeme, že podobná situace je i mezi endomorfismy prostorů V_n a $\widetilde{V}_n$ a v jistém smyslu i mezi podprostory těchto prostorů.

11.19. Věta. *Buď φ endomorfismus vektorového prostoru V. Pak zobrazení $\widetilde{\varphi}$ definované předpisem $(\widetilde{\varphi}(f))(\boldsymbol{u}) = f(\varphi(\boldsymbol{u}))$, $f \in \widetilde{V}$, $\boldsymbol{u} \in V$, je endomorfismus prostoru $\widetilde{V}$.*

Důkaz. Potřebujeme ověřit dvě věci. Jednak že pro každou lineární formu f na V je $\widetilde{\varphi}(f)$ opět lineární forma na V, jednak že $\widetilde{\varphi}$ je endomorfismus duálního prostoru $\widetilde{V}$. Nechť tedy $\boldsymbol{u}, \boldsymbol{v} \in V$ a $r \in T$ jsou libovolné prvky. Máme $\widetilde{\varphi}(f)(\boldsymbol{u}+\boldsymbol{v}) = f(\varphi(\boldsymbol{u}+\boldsymbol{v})) = f(\varphi(\boldsymbol{u}) + \varphi(\boldsymbol{v}) = f(\varphi(\boldsymbol{u})) + f(\varphi(\boldsymbol{v})) = (\widetilde{\varphi}(f)(\boldsymbol{u}) + \widetilde{\varphi}(f))(\boldsymbol{v})$, $(\widetilde{\varphi}(f))(r\boldsymbol{u}) = f(\varphi(r\boldsymbol{u})) = f(r\varphi(\boldsymbol{u})) = rf(\varphi(\boldsymbol{u})) = r(\widetilde{\varphi}(f))(\boldsymbol{u})$, a $\widetilde{\varphi}$ je tedy lineární forma na prostoru V. Dále nechť $f, g \in \widetilde{V}$, $r \in T$, jsou libovolné prvky. Pro libovolný vektor $\boldsymbol{u} \in V$ je podle definice 9.6 $(\widetilde{\varphi}(f+g))(\boldsymbol{u}) = (f+g)(\varphi(\boldsymbol{u})) = f(\varphi(\boldsymbol{u})) + g(\varphi(\boldsymbol{u})) = (\widetilde{\varphi}(f))(\boldsymbol{u}) + (\widetilde{\varphi}(g))(\boldsymbol{u}) = (\widetilde{\varphi}(f) + \widetilde{\varphi}(g))(\boldsymbol{u})$, takže $\widetilde{\varphi}(f+g) = \widetilde{\varphi}(f) + \widetilde{\varphi}(g)$. Podobně máme $(\widetilde{\varphi}(rf))(\boldsymbol{u}) = (rf)(\varphi(\boldsymbol{u})) = rf(\varphi(\boldsymbol{u})) = r(\widetilde{\varphi}(f))(\boldsymbol{u})$, tedy $\widetilde{\varphi}(rf) = r\widetilde{\varphi}(f)$ a $\widetilde{\varphi}$ je endomorfismus vektorového prostoru $\widetilde{V}$. ∎

11.20. Definice. Buď φ endomorfismus vektorového prostoru V. Endomorfismus $\widetilde{\varphi}$ duálního vektorového prostoru $\widetilde{V}$ zavedený v předchozí větě se nazývá *duální endomorfismus* k endomorfismu φ.

11.21. Věta. *Buď $\boldsymbol{A}$ matice endomorfismu φ vektorového prostoru V_n vzhledem k bázi M a buď $\widetilde{M}$ báze duální k bázi M. Pak $\boldsymbol{A}^T$ je matice duálního endomorfismu $\widetilde{\varphi}$ vzhledem k duální bázi $\widetilde{M}$.*

Důkaz. Nechť $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$, $\widetilde{M} = \{f_1, f_2, \ldots, f_n\}$ a označme $\boldsymbol{B} = (b_{ij})$ matici endomorfismu $\widetilde{\varphi}$ vzhledem k bázi $\widetilde{M}$. Podle definice 10.4 tedy máme $\varphi(\boldsymbol{u}_j) = \sum_{k=1}^{n} a_{kj}\boldsymbol{u}_k$, $j = 1, 2, \ldots, n$, a $\{\widetilde{\varphi}(f_i)\}_{\widetilde{M}} = (b_{1i}, b_{2i}, \ldots, b_{ni})$, $i = 1, 2, \ldots, n$. Přitom podle věty 11.7 je $\{\widetilde{\varphi}(f_i)\}_{\widetilde{M}} = \{\widetilde{\varphi}(f_i)\}_M$, $i = 1, 2, \ldots, n$, takže $b_{ji} = (\widetilde{\varphi}(f_i))(\boldsymbol{u}_j) = f_i(\varphi(\boldsymbol{u}_j)) = f_i(\sum_{k=1}^{n} a_{kj}\boldsymbol{u}_k) = \sum_{k=1}^{n} a_{kj}\delta_{ik} = a_{ij}$ podle definice duální báze a tedy $\boldsymbol{B} = \boldsymbol{A}^T$. ∎

11.22. Věta. *Buď V_n vektorový prostor nad tělesem T.*

(i) Je-li Φ endomorfismus vektorového prostoru $\widetilde{V}_n$, pak existuje právě jeden endomorfismus φ prostoru V_n takový, že $\widetilde{\varphi} = \Phi$;

(ii) Endomorfismus φ vektorového prostoru V_n je automorfismus, právě když duální endomorfismus $\widetilde{\varphi}$ je automorfismem duálního prostoru $\widetilde{V}_n$;

(iii) zobrazení $\Psi : \operatorname{End} V_n \to \operatorname{End} \widetilde{V}_n$ vektorového prostoru $\operatorname{End} V_n = \operatorname{Hom}(V_n, V_n)$ všech endomorfismů vektorového prostoru V_n do vektorového prostoru $\operatorname{End} \widetilde{V}_n$ definované vztahem $\Psi(\varphi) = \widetilde{\varphi}$, $\varphi \in \operatorname{End} V_n$, je izomorfismus. Při tomto izomorfismu si vzájemně jednoznačně odpovídají automorfismy prostoru V_n a automorfismy duálního prostoru $\widetilde{V}_n$.

Důkaz. (i) Buď M báze vektorového prostoru V_n, $\widetilde{M}$ báze k ní duální a buď $\boldsymbol{A}$ matice endomorfismu Φ vzhledem k bázi $\widetilde{M}$. Podle věty 10.7 existuje právě jeden endomorfismus φ prostoru V_n, jehož matice vzhledem k bázi M je $\boldsymbol{A}^T$. Podle předchozí věty je $(\boldsymbol{A}^T)^T = \boldsymbol{A}$ matice endomorfismu $\widetilde{\varphi}$ vzhledem k bázi $\widetilde{M}$. Endomorfismy $\widetilde{\varphi}$ a Φ mají tedy stejné matice vzhledem k bázi $\widetilde{M}$, takže $\widetilde{\varphi} = \Phi$ podle věty 10.7.

(ii) Podle věty 10.10 je φ automorfismus, právě když jeho matice vzhledem k libovolné bázi je regulární. Tato podmínka je podle věty 8.4 ekvivalentní s tím, že determinant $\det \boldsymbol{A}$ je nenulový. Podle věty 7.3 je $\det \boldsymbol{A}^T \neq 0$, $\widetilde{\varphi}$ je tudíž automorfismus prostoru $\widetilde{V}_n$ opět podle věty 8.4 a důkaz je hotov.

(iii) Podle věty 11.19 je Ψ zobrazení množiny $\operatorname{End} V_n$ do množiny $\operatorname{End} \widetilde{V}_n$, které je podle (i) surjektivní a při němž si podle (ii) vzájemně odpovídají automorfismy. Protože podle věty 11.3 a 10.22 je $\dim \operatorname{End} V_n = \dim \operatorname{End} \widetilde{V}_n = n^2$, stačí ověřit, že Ψ je homomorfismus, neboť podle věty 9.27 potom máme $\dim \operatorname{Ker} \Psi = n^2 - \dim \operatorname{Im} \Psi = 0$, Ψ je monomorfismus, a tedy automorfismus. Buďte tedy $\varphi_1, \varphi_2 \in \operatorname{End} V_n$ a $r \in T$ libovolné prvky. Pak pro každé $f \in \widetilde{V}_n$ a každé $\boldsymbol{u} \in V_n$ je $((\Psi(\varphi_1 + \varphi_2))(f))(\boldsymbol{u}) = ((\widetilde{\varphi_1 + \varphi_2})(f))(\boldsymbol{u}) = (f(\varphi_1 + \varphi_2))(\boldsymbol{u}) = (f(\varphi_1) + f(\varphi_2))(\boldsymbol{u}) = (\widetilde{\varphi}_1(f))(\boldsymbol{u}) + (\widetilde{\varphi}_2(f))(\boldsymbol{u}) = (\widetilde{\varphi}_1(f) + \widetilde{\varphi}_2(f))(\boldsymbol{u}) = ((\Psi(\varphi_1))(f) + (\Psi(\varphi_2))(f))(\boldsymbol{u}) = ((\Psi(\varphi_1) + \Psi(\varphi_2))(f))(\boldsymbol{u})$, takže $(\Psi(\varphi_1 + \varphi_2))(f) = (\Psi(\varphi_1) + \Psi(\varphi_2))(f)$ pro každé $f \in \widetilde{V}_n$ a tedy $\Psi(\varphi_1 + \varphi_2) = \Psi(\varphi_2) + \Psi(\varphi_2)$. Podobně máme $((\Psi(r\varphi))(f))(\boldsymbol{u}) = ((\widetilde{r\varphi}(f))(\boldsymbol{u}) = f((r\varphi)(\boldsymbol{u})) = f((r\varphi(\boldsymbol{u})) = rf(\varphi(\boldsymbol{u})) = r(\widetilde{\varphi}(f))(\boldsymbol{u}) = ((r\Psi(\varphi))(f))(\boldsymbol{u})$ pro každé $\boldsymbol{u} \in V_n$, takže $\Psi(r\varphi))(f) = (r\Psi(\varphi))(f)$ pro každé $f \in \widetilde{V}_n$ a tedy $\Psi(r\varphi) = r\Psi(\varphi)$, což jsme chtěli dokázat. ∎

11.23. Definice. Buď V vektorový prostor. Pro každou podmnožinu $M \subseteq V$ označíme $\Phi(M) = \{f \in \widetilde{V} \mid M \subseteq \operatorname{Ker} f\}$ a pro každou podmnožinu $N \subseteq \widetilde{V}$ označíme $\Psi(N) = \cap_{f \in N} \operatorname{Ker} f$.

11.24. Věta. *Buď V vektorový prostor. Pak platí:*

(i) $\Phi(M_2) \subseteq \Phi(M_1)$, kdykoliv $M_1 \subseteq M_2 \subseteq V$;

(ii) $\Psi(N_2) \subseteq \Psi(N_1)$, kdykoliv $N_1 \subseteq N_2 \subseteq \widetilde{V}$;

(iii) pro každou podmnožinu $M \subseteq V$ je $\Phi(M) = \Phi(\langle M \rangle) \leq \widetilde{V}$;

(iv) pro každou podmnožinu $N \subseteq \widetilde{V}$ je $\Psi(N) = \Psi(\langle N \rangle) \leq V$.

Důkaz. (i) Podle definice máme $\Phi(M_2) = \{f \in \widetilde{V} \mid M_2 \subseteq \operatorname{Ker} f\} \subseteq \{f \in \widetilde{V} \mid M_1 \subseteq \operatorname{Ker} f\} = \Phi(M_1)$.

(ii) Podobně máme $\Psi(N_2) = \cap_{f \in N_2} \operatorname{Ker} f \subseteq \cap_{f \in N_1} \operatorname{Ker} f = \Psi(N_1)$.

(iii) Protože $M \subseteq \langle M \rangle$, je podle (i) $\Phi(\langle M \rangle) \subseteq \Phi(M)$. Na druhé straně, je-li $f \in \Phi(M)$ libovolný prvek, je $M \subseteq \operatorname{Ker} f$, takže $\langle M \rangle \subseteq \operatorname{Ker} f$ podle definice lineárního obalu 1.9, a tedy $f \in \Phi(\langle M \rangle)$, odkud již rovnost $\Phi(M) = \Phi(\langle M \rangle)$ bezprostředně plyne. Zbývá ukázat, že $\Phi(M)$ je podprostorem ve $\widetilde{V}$. Pro libovolné prvky $f, g \in \Phi(M)$ a $r \in T$ máme $M \subseteq \operatorname{Ker} f$, $M \subseteq \operatorname{Ker} g$, takže i $M \subseteq \operatorname{Ker}(f+g)$, $M \subseteq \operatorname{Ker}(rf)$, a tedy $f+g, rf \in \Phi(M)$ a $\Phi(M) \leq \widetilde{V}$.

(iv) Podobně jako v předchozím případě z $N \subseteq \langle N \rangle$ plyne $\Psi(\langle N \rangle) \subseteq \Psi(N)$ podle (ii). Je-li naopak $f \in \langle N \rangle$ libovolný prvek, lze f vyjádřit podle věty 1.11 ve tvaru lineární kombinace $f = \sum_{i=1}^{k} r_i f_i$, $f_i \in N$, $r_i \in T$, $i = 1, 2, \ldots, k$. Podle věty 11.15 (i) je $\cap_{i=1}^{k} \operatorname{Ker} f_i \subseteq \operatorname{Ker} f$ a tedy $\Psi(N) = \cap_{g \in N} \operatorname{Ker} g \subseteq \cap_{i=1}^{k} \operatorname{Ker} f_i \subseteq \operatorname{Ker} f$, odkud ihned plyne inkluze $\Psi(N) \subseteq \Psi(\langle N \rangle)$. Přitom je $\Psi(N)$ podprostorem ve V podle vět 11.14 a 1.8. ∎

11.25. Věta. *Buď V_n vektorový prostor konečné dimenze n. Pak platí:*

(i) pro každou podmnožinu $M \subseteq V_n$ je $\Psi\Phi(M) = \langle M \rangle$;

(ii) pro každou podmnožinu $N \subseteq \widetilde{V}_n$ je $\Phi\Psi(N) = \langle N \rangle$;

(iii) zobrazení Φ je prosté zobrazení množiny všech podprostorů prostoru V_n na množinu všech podprostorů prostoru $\widetilde{V}_n$ a zobrazení Ψ je inverzní k zobrazení Φ;

(iv) pro každou podmnožinu $N \subseteq \widetilde{V}_n$ je $\dim \Psi(N) = n - \dim \langle N \rangle$;

(v) pro každou podmnožinu $\subseteq V_n$ je $\dim \Phi(M) = n - \dim \langle M \rangle$.

Důkaz. (i) Pro každé $f \in \Phi(M)$ je $M \subseteq \operatorname{Ker} f$, takže $M \subseteq \cap_{f\in\Phi(M)}\operatorname{Ker} f = \Psi\Phi(M)$, a tedy i $\langle M\rangle \subseteq \Psi\Phi(M)$ podle definice lineárního obalu 1.9. Buď tedy $\boldsymbol{u} \notin \langle M\rangle$ libovolný vektor a buď $\{\boldsymbol{u}_2,\dots,\boldsymbol{u}_k\}$ báze lineárního obalu $\langle M\rangle$. Pak vektory $\boldsymbol{u},\boldsymbol{u}_2,\dots,\boldsymbol{u}_k$ jsou zřejmě lineárně nezávislé, takže podle věty 2.21 existuje báze $\{\boldsymbol{u},\boldsymbol{u}_2,\dots,\boldsymbol{u}_k,\boldsymbol{u}_{k+1},\dots,\boldsymbol{u}_n\}$ prostoru V_n. Podle věty 9.22 existuje lineární forma $f \in \widetilde{V}_n$ taková, že $f(\boldsymbol{u}) = 1$, $f(\boldsymbol{u}_i) = 0$, $i = 2,\dots,n$. Speciálně tedy je $\langle M\rangle \subseteq \operatorname{Ker} f$, takže $f \in \Phi(M)$. Kromě toho vidíme, že $\boldsymbol{u} \notin \operatorname{Ker} f$, a tedy $\boldsymbol{u} \notin \Psi\Phi(M)$. Ukázali jsme, že pro každé $\boldsymbol{u} \notin \langle M\rangle$ je $\boldsymbol{u} \notin \Psi\Phi(M)$, odkud požadovaná rovnost ihned plyne.

(ii) Buď $\{f_1, f_2,\dots,f_k\}$ báze lineárního obalu $\langle N\rangle$. Podle věty 11.15 je $f \in \langle N\rangle$, právě když $\Psi(N) = \cap_{i=1}^{k}\operatorname{Ker} f_i \subseteq \operatorname{Ker} f$, což je zřejmě ekvivalentní s $f \in \Phi\Psi(N) = \Phi\Psi(\langle N\rangle)$, odkud požadovaná rovnost ihned plyne.

(iii) Tvrzení plyne bezprostředně z (i) a (ii).

(iv) Buď $\{f_1, f_2,\dots,f_k\}$ báze lineárního obalu $\langle N\rangle$. Pak podle věty 11.15 jest $\cap_{i=1}^{k}\operatorname{Ker} f_i \subseteq \operatorname{Ker} f$ pro každé $f \in \langle N\rangle$, takže $\Psi(\langle N\rangle) = \Psi(N) = \cap_{i=1}^{k}\operatorname{Ker} f_i$. Potom však podle věty 11.15 (ii) je $\dim\Psi(N) = n - k = n - \dim\langle N\rangle$.

(v) Nechť $\{\boldsymbol{u}_1,\boldsymbol{u}_2,\dots,\boldsymbol{u}_k\}$ je báze linerního obalu $\langle M\rangle$. Podle věty 2.21 lze tuto lineárně nezávislou množinu doplnit na bázi $M = \{\boldsymbol{u}_1,\boldsymbol{u}_2,\dots,\boldsymbol{u}_n\}$ prostoru V_n. Je-li nyní $\widetilde{M} = \{f_1, f_2,\dots,f_n\}$ báze duální k bázi M, je zřejmě $f_{k+1},\dots,f_n \in \Phi(M)$, takže $\dim\Phi(M) \geq n - k = n - \dim\langle M\rangle$ a tedy $\dim\langle M\rangle \geq n - \dim\Phi(M)$. Odtud podle (i) a (iv) dostáváme $\dim\langle M\rangle = \dim\Psi\Phi(M) = n - \dim\Phi(M) \leq \dim\langle M\rangle$, odkud tvrzení ihned plyne. ■

11.26. Poznámka. V právě dokázané větě jsme viděli, že si vzájemně jednoznačně odpovídají jisté podprostory vektorového prostoru V_n s podprostory prostoru duálního $\widetilde{V}_n$. Přitom podprostoru dimenze k ve V_n odpovídá podprostor „komplementární" dimenze $n - k$ ve $\widetilde{V}_n$. S podobnými korespondencemi se v algebře setkáváme poměrně často, a mají proto svůj název – *dualita.* Poznamenejme ještě, že první tři tvrzení předchozí věty platí v každém vektorovém prostoru, nikoliv pouze v prostorech konečné dimenze, kde jsme tato tvrzení dokazovali. K tomu, abychom mohli uvedená tvrzení dokázat v plné obecnosti, potřebovali bychom znát některá další tvrzení o lineárně nezávislých množinách a bázích v obecných vektorových prostorech, což však přesahuje rámec tohoto textu. Pro ilustraci poznamenejme, že např. je-li M podmnožina ve V a $\boldsymbol{u} \notin \langle M\rangle$ libovolný vektor, pak existuje lineární forma $f \in \widetilde{V}$ taková, že $f(\boldsymbol{u}) = 1$ a $\langle M\rangle \subseteq \operatorname{Ker} f$. Čtenář nyní snadno sám ověří, že tato skutečnost již stačí k důkazu planosti tvrzení (i) v obecném případě.

12.1. Definice. Buď V vektorový prostor nad tělesem T. Zobrazení $f : V \times V \to T$ množiny všech uspořádaných dvojic vektorů z prostoru V do tělesa T se nazývá *bilineární forma* na prostoru V, jestliže pro libovolné vektory $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in V$ a libovolný prvek $r \in T$ platí

$$f(\boldsymbol{u}, \boldsymbol{v} + \boldsymbol{w}) = f(\boldsymbol{u}, \boldsymbol{v}) + f(\boldsymbol{u}, \boldsymbol{w}),$$

$$f(\boldsymbol{u} + \boldsymbol{w}, \boldsymbol{v}) = f(\boldsymbol{u}, \boldsymbol{v}) + f(\boldsymbol{w}, \boldsymbol{v}),$$

$$f(r\boldsymbol{u}, \boldsymbol{v}) = rf(\boldsymbol{u}, \boldsymbol{v}) = f(\boldsymbol{u}, r\boldsymbol{v}).$$

Zobrazení $f : V \times V \to T$ takové, že $f(\boldsymbol{u}, \boldsymbol{v}) = 0$ pro libovolnou dvojici vektorů $\boldsymbol{u}, \boldsymbol{v} \in V$ je zřejmě bilineární forma na V, tato forma se nazývá *nulová*, nebo *triviální*, každá jiná bilineární forma je pak *nenulová*, nebo *netriviální*.

12.2. Definice. Buď $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ báze vektorového prostoru V_n a buď f bilineární forma na V_n. Matice $\boldsymbol{A} = (a_{ij}) \in T_n$, kde $a_{ij} = f(\boldsymbol{u}_i, \boldsymbol{u}_j)$, $i, j = 1, 2, \dots, n$ se nazývá *matice formy f vzhledem k bázi M*.

12.3. Věta. *Buď $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ báze vektorového prostoru V_n, buď f bilineární forma na V_n a buď $\boldsymbol{A} = (a_{ij})$ matice formy f vzhledem k bázi M. Pak pro libovolné dva vektory $\boldsymbol{u}, \boldsymbol{v} \in V_n$ o souřadnicích $\{\boldsymbol{u}\}_M = (x_1, x_2, \dots, x_n)$, $\{\boldsymbol{v}\}_M = (y_1, y_2, \dots, y_n)$ vzhledem k bázi M platí*

(a) $f(\boldsymbol{u}, \boldsymbol{v}) = \sum_{i,j=1}^{n} a_{ij} x_i y_j$;

(b) $f(\boldsymbol{u}, \boldsymbol{v}) = \{\boldsymbol{u}\}_M \boldsymbol{A} \{\boldsymbol{v}\}_M^T$.

Důkaz. (a) Podle definice 10.1 je $\boldsymbol{u} = \sum_{i=1}^{n} x_i \boldsymbol{u}_i$, $\boldsymbol{v} = \sum_{j=1}^{n} y_j \boldsymbol{v}_j$, odkud úplnou indukcí podle definice 12.1 dostáváme $f(\boldsymbol{u}, \boldsymbol{v}) = f(\sum_{i=1}^{n} x_i \boldsymbol{u}_i, \sum_{j=1}^{n} y_j \boldsymbol{v}_j) = \sum_{i=1}^{n} x_i f(\boldsymbol{u}_i, \sum_{j=1}^{n} y_j \boldsymbol{v}_j) = \sum_{i=1}^{n} \sum_{j=1}^{n} x_i y_j f(\boldsymbol{u}_i, \boldsymbol{v}_j) = \sum_{i,j=1}^{n} a_{ij} x_j y_j$.

(b) Podle definice součinu matic 4.5 je na pravé straně dokazované rovnosti matice typu $(1, 1)$, tj. prvek z tělesa T, a to prvek $\sum_{i,j=1}^{n} x_i a_{ij} y_j$, takže stačí použít tvrzení (a). ■

12.4. Definice. Je-li $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ báze vektorového prostoru V_n a $\boldsymbol{A} = (a_{ij})$ matice bilineární formy f na prostoru V_n vzhledem k bázi M, pak výraz $f(\boldsymbol{u}, \boldsymbol{v}) = \sum_{i,j=1}^{n} a_{ij} x_i y_j$ se nazývá *analytické vyjádření formy f vzhledem k bázi M*.

12.5. Věta. *Buď $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ báze vektorového prostoru V_n a buď $\boldsymbol{A} = (a_{ij})$ čtvercová matice stupně n nad tělesem T. Pak existuje právě jedna bilineární forma f na prostoru V_n, jejíž matice vzhledem k bázi M je právě matice $\boldsymbol{A}$.*

Důkaz. Jsou-li $\boldsymbol{u}, \boldsymbol{v} \in V_n$ libovolné vektory a $\{\boldsymbol{u}\}_M = (x_1, x_2, \dots, x_n)$, $\{\boldsymbol{v}\}_M = (y_1, y_2, \dots, y_n)$ jejich souřadnice vzhledem k bázi M, pak položíme-li $f(\boldsymbol{u}, \boldsymbol{v}) = \sum_{i,j=1}^{n} a_{ij} x_i y_j$, je f zřejmě bilineární forma na prostoru V_n. Přitom $\{\boldsymbol{u}_i\}_M = \boldsymbol{e}_i$, $\{\boldsymbol{u}_j\}_M = \boldsymbol{e}_j$, takže $f(\boldsymbol{u}_i, \boldsymbol{u}_j) = a_{ij}$ a $\boldsymbol{A}$ je matice formy f vzhledem k bázi M.

K důkazu jednoznačnosti poznamenejme, že je-li g bilineární forma na V_n s maticí $\boldsymbol{A}$ vzhledem k bázi M, je podle věty 12.3(i) $g(\boldsymbol{u}, \boldsymbol{v}) = \sum_{i,j=1}^{n} a_{ij} x_i y_j = f(\boldsymbol{u}, \boldsymbol{v})$. ■

12.6. Poznámka. Z právě dokázané věty bezprostředně plyne, že je-li dána báze M vektorového prostoru V_n, pak si vzájemně jednoznačně odpovídají bilineární formy a jejich matice vzhledem k dané bázi M. Je proto užitečné si uvědomit, jak se změní matice bilineární formy, jestliže se změní báze prostoru V_n.

12.7. Věta. *Buďte M a M' dvě báze vektorového prostoru V_n a buď f bilineární forma na V_n. Je-li $\boldsymbol{A}$ matice formy f vzhledem k bázi M a $\boldsymbol{B}$ matice přechodu od báze M k bázi M', pak $\boldsymbol{B}^T \boldsymbol{A} \boldsymbol{B}$ je matice formy f vzhledem k bázi M'.*

Důkaz. Nechť $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ a $M' = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n\}$. Označme $\boldsymbol{C} = (c_{ij})$ matici formy f vzhledem k bázi M', tj. $c_{ij} = f(\boldsymbol{v}_i, \boldsymbol{v}_j)$. Protože $\boldsymbol{B}$ je matice přechodu od báze M k bázi M', je $\boldsymbol{v}_i = \sum_{k=1}^{n} b_{ki} \boldsymbol{u}_k$, $\boldsymbol{v}_j = \sum_{l=1}^{n} b_{lj} \boldsymbol{u}_l$, takže $c_{ij} = f(\boldsymbol{v}_i, \boldsymbol{v}_j) = f(\sum_{k=1}^{n} b_{ki} \boldsymbol{u}_k, \sum_{l=1}^{n} b_{lj} \boldsymbol{u}_l) = \sum_{k=1}^{n} \sum_{l=1}^{n} b_{ki} b_{lj} f(\boldsymbol{u}_k, \boldsymbol{u}_l) = \sum_{k=1}^{n} \sum_{l=1}^{n} b_{ik}^T a_{kl} b_{lj}$, kde b_{ik}^T značí příslušný prvek matice $\boldsymbol{B}^T$ transponované k matici $\boldsymbol{B}$. Odtud je již patrná rovnost $\boldsymbol{C} = \boldsymbol{B}^T \boldsymbol{A} \boldsymbol{B}$. ■

12.8. Definice. Buď f bilineární forma na vektorovém prostoru V. Množina $V_l(f) = \{\boldsymbol{u} \in V \mid f(\boldsymbol{u}, \boldsymbol{v}) = 0$ pro každé $\boldsymbol{v} \in V\}$ se nazývá *levý vrchol formy f* a množina $V_p(f) = \{\boldsymbol{v} \in V \mid f(\boldsymbol{u}, \boldsymbol{v}) = 0$ pro každé $\boldsymbol{u} \in V\}$ se nazývá *pravý vrchol formy f*. Je-li speciálně $V_l(f) = V_p(f)$ pro nějakou bilineární formu f, pak množinu $V(f) = V_l(f) = V_p(f)$ nazýváme *vrcholem formy f*.

12.9. Poznámka. Pro triviální bilineární formu $f = 0$ jistě platí $V_l(f) = V_p(f) = V$. Stejnou vlastnost však má i daleko širší a důležitější třída bilineárních forem zvaných symetrické. Symetrické jsou takové bilineární formy f, pro které je $f(\boldsymbol{u}, \boldsymbol{v}) = f(\boldsymbol{v}, \boldsymbol{u})$ pro každou dvojici vektorů $\boldsymbol{u}, \boldsymbol{v} \in V$. Symetrickými bilineárními formami se budeme později zabývat podrobněji, na tomto místě si ukážeme jeden zajímavý příklad. V poznámce 9.17 jsme ukázali, že množina $M = \{1, x, x^2, \ldots\}$ tvoří bázi vektorového prostoru $P(T)$ všech polynomů nad tělesem T. Pro každé celé nezáporné číslo k položme $f(x^{2k+1}, x^k) = 1$, $f(x^{2k+1}, x^j) = 0$ pro každé $j = 0, 1, \ldots, j \neq k$, a $f(x^{2k}, x^j) = 0$ pro každé $j = 0, 1, \ldots$ Tímto způsobem máme tedy „předepsány" hodnoty zobrazení f na všech možných dvojicích prvků báze M. Použijeme-li nyní úvahy z důkazu věty 12.3, tj. položíme-li $f(\boldsymbol{u}, \boldsymbol{v}) = \sum_{i=0}^{n} \sum_{j=0}^{n} a_i b_j f(x^i, x^j)$ pro libovolné dva prvky $\boldsymbol{u} = \sum_{i=0}^{n} a_i x^i$ a $\boldsymbol{v} = \sum_{j=1}^{n} b_j x^j$ z prostoru $P(T)$, dostaneme zřejmě bilineární formu na tomto vektorovém prostoru. Protože $f(x^{2k}, x^j) = 0$ pro každé $j = 0, 1, \ldots$, je $\langle x^{2k} \mid k = 0, 1, \ldots \rangle \subseteq V_l(f)$ a není obtížné ověřit, že dokonce $\langle x^{2k} \mid k = 0, 1, \ldots \rangle = V_l(f)$. Na druhé straně pro $\boldsymbol{u} = \sum_{i=0}^{n} a_i x^i \in V_p(f)$ dostáváme $f(x^j, \boldsymbol{u}) = f(x^j, \sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} a_i f(x^j, x^i) = 0$ pro každé $j = 0, 1, \ldots$ Zvolíme-li nyní $j = 2k + 1$ pro některé pevné, ale jinak libovolné $k \in \{0, 1, \ldots, n\}$, dostaneme pro všechna $i = 0, 1, \ldots, n$ jediný nenulový člen $f(x^{2k+1}, x^k) = 1$, odkud ihned plyne $a_i = 0$, $i = 0, 1, \ldots, n$, a tedy $V_p(f) = 0$. Vidíme tedy, že v případě prostoru nekonečné dimenze může jeden z vrcholů být např. nulový a druhý může mít nekonečnou dimenzi apod. Nyní si ukážeme, že podobná situace nemůže nastat v případě prostorů konečné dimenze, kde oba dva vrcholy, i když mohou být různé, musí mít stejnou dimenzi.

12.10. Věta. *Buď M báze vektorového prostoru V_n a buď $\boldsymbol{A}$ matice bilineární formy f na prostoru V_n vzhledem k bázi M. Pak*

(i) levý vrchol $V_l(f)$ formy f je právě množina všech vektorů $\boldsymbol{u} \in V_n$, jejichž souřadnice vzhledem k bázi M tvoří množinu $W_{\boldsymbol{A}^T}$ všech řešení homogenní soustavy lineárních rovnic s maticí $\boldsymbol{A}^T$;

(ii) pravý vrchol $V_p(f)$ formy f je právě množina všech vektorů $\boldsymbol{u} \in V_n$, jejichž souřadnice vzhledem k bázi M tvoří množinu $W_{\boldsymbol{A}}$ všech řešení homogenní soustavy lineárních rovnic s maticí $\boldsymbol{A}$;

(iii) $\dim V_l(f) = \dim V_p(f) = n - h(\boldsymbol{A})$.

Důkaz. (i) Podle věty 12.3 je $f(\boldsymbol{u}, \boldsymbol{v}) = \sum_{i,j1}^{n} a_{ij} x_i y_j$, $\{\boldsymbol{u}\}_M = (x_1, x_2, \dots, x_n)$, $\{\boldsymbol{v}\}_M = (y_1, y_2, \dots, y_n)$, analytické vyjádření formy f vzhledem k bázi M. Pak $\boldsymbol{u} \in V_l(f)$, právě když $f(\boldsymbol{u}, \boldsymbol{v}) = 0$ pro každý vektor $\boldsymbol{v} \in V_n$, tj. právě když $\sum_{i,j=1}^{n} a_{ij} x_i y_j = \sum_{j=1}^{n} (\sum_{i=1}^{n} a_{ij} x_i) y_j = 0$ pro libovolný vektor $\{\boldsymbol{v}\}_M \in T^n$. Dosadíme-li postupně za $\{\boldsymbol{v}\}_M$ jednotkové vektory $\boldsymbol{e}_1, \boldsymbol{e}_2, \dots, \boldsymbol{e}_n$ z T^n, vidíme, že uvedená podmínka je ekvivalentní s tím, že $\sum_{i=1}^{n} a_{ij} x_i = 0$ pro každé $j = 1, 2, \dots, n$. To však znamená přesně totéž, jako že $\{\boldsymbol{u}\}_M$ je řešením homogenní soustavy lineárních rovnic s maticí $\boldsymbol{A}^T$.

(ii) Analogicky jako prve máme $\boldsymbol{v} \in V_p(f)$, právě když $\sum_{i=1}^{n} (\sum_{j=1}^{n} a_{ij} y_j) x_i = 0$ pro každý vektor $\{\boldsymbol{u}\}_M$, což je ekvivalentní s tím, že $\{\boldsymbol{v}\}_M \in W_{\boldsymbol{A}}$.

(iii) Podle (i) a věty 10.2 (iv) je $\dim V_l(f) = \dim W_{\boldsymbol{A}^T}$, takže podle věty 5.8 je $\dim V_l(f) = n - h(\boldsymbol{A}^T)$. Stejným způsobem dostaneme z (ii) rovnost $\dim V_p(f) = n - h(\boldsymbol{A})$ a stačí použít větu 5.5, podle které je $h(\boldsymbol{A}) = h(\boldsymbol{A}^T)$. ∎

12.11. Definice. Buď f bilineární forma na vektorovém prostoru V_n. *Nulitou formy* f rozumíme číslo $n(f) = \dim V_l(f) = \dim V_p(f)$. *Hodností $h(f)$ formy* f rozumíme číslo $h(f) = n - n(f)$. Forma f se nazývá *regulární*, je-li $n(f) = 0$ a *singulární* v opačném případě.

12.12. Poznámka. Na tomto místě je vhodné si uvědomit, že věta 12.10 vlastně říká, že je-li M libovolná báze prostoru V_n a $\boldsymbol{A}$ matice bilineární formy f vzhledem k bázi M, pak $h(f) = h(\boldsymbol{A})$. Speciálně je tedy forma f regulární, právě když její matice vzhledem k libovolné bázi je regulární.

12.13. Věta. *Buď f bilineární forma na vektorovém prostoru V. Definujeme-li $(\Phi_l^f(\boldsymbol{u}))(\boldsymbol{v}) = f(\boldsymbol{u}, \boldsymbol{v})$ a $(\Phi_p^f(\boldsymbol{u}))(\boldsymbol{v}) = f(\boldsymbol{v}, \boldsymbol{u})$ pro každou dvojici vektorů $\boldsymbol{u}, \boldsymbol{v} \in V$, pak Φ_l^f a Φ_p^f jsou homomorfismy z vektorového prostoru V do duálního vektorového prostoru $\widetilde{V}$.*

Důkaz. Důkaz provedeme např. pro Φ_l^f, neboť pro Φ_p^f je důkaz analogický a lze jej přenechat čenáři jako cvičení. Nejprve musíme ověřit, že pro každé $\boldsymbol{u} \in V$ je $\Phi_l^f(\boldsymbol{u}) \in \widetilde{V}$, tj. že se jedná o lineární formu. Pro každé dva prvky $\boldsymbol{v}, \boldsymbol{w} \in V$ a každý prvek $r \in T$ máme $(\Phi_l^f(\boldsymbol{u}))(\boldsymbol{v} + \boldsymbol{w}) = f(\boldsymbol{u}, \boldsymbol{v} + \boldsymbol{w}) = f(\boldsymbol{u}, \boldsymbol{v}) + f(\boldsymbol{u}, \boldsymbol{w}) = (\Phi_l^f)\boldsymbol{u}))(\boldsymbol{v}) + (\Phi_l^f(\boldsymbol{u}))(\boldsymbol{w})$ a $(\Phi_l^f(\boldsymbol{u}))(r\boldsymbol{v}) = f(\boldsymbol{u}, r\boldsymbol{v}) = rf(\boldsymbol{u}, \boldsymbol{v}) = r(\Phi_l^f(\boldsymbol{u}))(\boldsymbol{v})$. K dokončení důkazu zbývá nyní ověřit, že $\Phi_l^f : V \to \widetilde{V}$ je homomorfismus. Pro libovolné tři vektory $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in V$ předně máme $(\Phi_l^f(\boldsymbol{u} + \boldsymbol{v}))(\boldsymbol{w}) = f(\boldsymbol{u} + \boldsymbol{v}, \boldsymbol{w}) = f(\boldsymbol{u}, \boldsymbol{v}) + f(\boldsymbol{v}, \boldsymbol{w}) = (\Phi_l^f(\boldsymbol{u}))(\boldsymbol{w}) + (\Phi_l^f)\boldsymbol{v}))(\boldsymbol{w}) = (\Phi_l^f \boldsymbol{u}) + \Phi_l^f(\boldsymbol{v}))(\boldsymbol{w})$, takže $\Phi_l^f(\boldsymbol{u} +$

$v) = \Phi_l^f(u) + \Phi_l^f(v)$. Podobně pro každé $u, v \in V$ a každé $r \in T$ jest $(\Phi_l^f(ru))(v) = f(ru, v) = rf(u, v) = r(\Phi_l^f(u))(v) = (r\Phi_l^f(u))(v)$, a tedy $\Phi_l^f(ru) = r\Phi_l^f(u)$. ■

12.14. Definice. Homomorfismus Φ_l^f z předchozí věty se nazývá *levý homomorfismus z V do $\widetilde{V}$ zprostředkovaný bilineární formou f* a Φ_p^f se nazývá *pravý homomorfismus z V do $\widetilde{V}$ zprostředkovaný bilineární formou f*. V případě, že oba homomorfismy splývají (např. v případě symetrických bilineárních forem), používáme zjednodušené označení $\Phi^f = \Phi_l^f = \Phi_p^f$.

12.15. Věta. *Buď M báze vektorového prostoru V_n a buď f bilineární forma na V_n. Pak platí*

(i) $\operatorname{Ker}\Phi_l^f = V_l(f)$, $\operatorname{Ker}\Phi_p^f = V_p(f)$;

(ii) je-li A matice formy f vzhledem k bázi M, pak A^T je matice homomorfismu Φ_l^f vzhledem k bázím M a $\widetilde{M}$ a A je matice homomorfismu Φ_p^f vzhledem k bázím M a $\widetilde{M}$.

(iii) homomorfismy Φ_l^f a Φ_p^f jsou izomorfismy, právě když forma f je regulární.

Důkaz. (i) Vektor $u \in V_n$ leží v levém vrcholu formy f, právě když $f(u, v) = (\Phi_l^f(u)(v) = 0$ pro každý vektor $v \in V_n$, tj. právě když lineární forma $\Phi_l^f(u)$ je triviální, což znamená, že vektor u leží v Ker Φ_l^f. Druhá rovnost se dokáže analogicky.

(ii) Buď $M = \{u_1, u_2, \ldots, u_n\}$ báze prostoru V_n, $\widetilde{M} = \{g_1, g_2, \ldots, g_n\}$ báze k ní duální a buď $B = (b_{ij})$ matice homomorfismu Φ_l^f vzhledem k bázím M a $\widetilde{M}$. Podle definice tedy je $\{\Phi_l^f(u_j)\}_{\widetilde{M}} = (b_{1j}, b_{2j}, \ldots, b_{nj})$ pro každé $j = 1, 2, \ldots, n$. Protože podle věty 11.7 je $\{\Phi_l^f(u_j)\}_{\widetilde{M}} = \{\Phi_l^f(u_j)\}_M$, je $b_{ij} = (\Phi_l^f(u_j))(u_i) = f(u_j, u_i) = a_{ji}$ a $B = A^T$. Podobně, je-li $C = (c_{ij})$ matice homomorfismu Φ_p^f vzhledem k bázím M a $\widetilde{M}$, je $c_{ij} = (\Phi_p^f(u_j))(u_i) = f(u_i, u_j) = a_{ij}$, a tedy $C = A$.

(iii) Podle (i) a věty 9.27 jsou Φ_l^f a Φ_p^f izomorfismy, právě když $n(f) = 0$, tj. právě když je forma f regulární. ■

12.16. Věta. *Buď $\varphi : V_n \to \widetilde{V}_n$ homomorfismus vektorového prostoru V_n do duálního prostoru $\widetilde{V}_n$. Pak existuje právě jedna bilineární forma f a právě jedna bilineární forma g na V_n taková, že $\varphi = \Phi_l^f = \Phi_p^g$.*

Důkaz. Buď M báze vektorového prostoru V_n a $\widetilde{M}$ báze duálního prostoru $\widetilde{V}_n$ duální k bázi M. Je-li A matice homomorfismu φ vzhledem k bázím M a $\widetilde{M}$, existuje podle věty 12.5 právě jedna bilineární forma f na V_n, jejíž matice vzhledem k bázi M je A^T a právě jedna bilineární forma g na V_n, jejíž matice vzhledem k bázi M je A. Podle předchozí věty 12.15 (ii) je $A = (A^T)^T$ matice homomorfismů Φ_l^f a Φ_p^f vzhledem k bázím M a $\widetilde{M}$, takže $\varphi = \Phi_l^f = \Phi_p^g$ podle věty 10.7. ■

12.17. Příklady. 1. Určeme levý a pravý vrchol, hodnost a nulitu bilineární formy na aritmetickém vektorovém prostoru R^3, jejíž analytické vyjádření vzhledem ke kanonické bázi tohoto prostoru je $f(u, v) = x_1y_1 + 2x_1y_2 + 3x_1y_3 + 3x_2y_1 + x_2y_2 + 2x_2y_3 + 5x_3y_1 + 5x_3y_2 + 8x_3y_3$.

Ř e š e n í: Matice formy f vzhledem ke kanonické bázi K prostoru R^3 je

$$A = \begin{pmatrix} 1, & 2, & 3 \\ 3, & 1, & 2 \\ 5, & 5, & 8 \end{pmatrix},$$

takže podle věty 12.10 je transponovaná matice A^T maticí homogenní soustavy lineárních rovnic, jejíž řešení je právě levý vrchol formy f a A je maticí homogenní soustavy lineárních rovnic, jejíž řešení je právě pravý vrchol formy f. Máme tedy

$$\begin{pmatrix} 1, & 3, & 5 \\ 2, & 1, & 5 \\ 3, & 2, & 8 \end{pmatrix} \sim \begin{pmatrix} 1, & 3, & 5 \\ 0, & -5, & -5 \\ 0, & -7, & -7 \end{pmatrix} \sim \begin{pmatrix} 1, & 3, & 5 \\ 0, & 1, & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1, & 2, & 3 \\ 3, & 1, & 2 \\ 5, & 5, & 8 \end{pmatrix} \sim \begin{pmatrix} 1, & 2, & 3 \\ 0, & -5, & -7 \\ 0, & -5, & -7 \end{pmatrix} \sim \begin{pmatrix} 1, & 2, & 3 \\ 0, & 5, & 7 \end{pmatrix},$$

takže $V_l(f) = \langle(2,1,-1)\rangle$, $V_p(f) = \langle(1,7,-5)\rangle$, $n(f) = 1$ a $h(f) = 2$.

2. Určeme levý a pravý vrchol, hodnost a nulitu bilineární formy f na aritmetickém vektorovém prostoru R^4, jejíž analytické vjádření vzhledem ke kanonické bázi tohoto prostoru je $f(\boldsymbol{u},\boldsymbol{v}) = x_1y_1 + 2x_1y_2 + 3x_1y_3 + 4x_1y_4 + 4x_2y_1 + 3x_2y_2 + 2x_2y_3 + x_2y_4 + 6x_3y_1 + 7x_3y_2 + 8x_3y_3 + 9x_3y_4 + 9x_4y_1 + 8x_4y_2 + 7x_4y_3 + 6x_4y_4$.

Ř e š e n í: Podobně jako v předchozím příkladu jest

$$\begin{pmatrix} 1, & 4, & 6, & 9 \\ 2, & 3, & 7, & 8 \\ 3, & 2, & 8, & 7 \\ 4, & 1, & 9, & 6 \end{pmatrix} \sim \begin{pmatrix} 1, & 4, & 6, & 9 \\ 0, & -5, & -5, & -10 \\ 0, & -10, & -10, & -20 \\ 0, & -15, & -15, & -30 \end{pmatrix} \sim \begin{pmatrix} 1, & 4, & 6, & 9 \\ 0, & 1, & 1, & 2 \end{pmatrix},$$

$$\begin{pmatrix} 1, & 2, & 3, & 4 \\ 4, & 3, & 2, & 1 \\ 6, & 7, & 8, & 9 \\ 9, & 8, & 7, & 6 \end{pmatrix} \sim \begin{pmatrix} 1, & 2, & 3, & 4 \\ 0, & -5, & -10, & -15 \\ 0, & -5, & -10, & -15 \\ 0, & -10, & -20, & -30 \end{pmatrix} \sim \begin{pmatrix} 1, & 2, & 3, & 4 \\ 0, & 1, & 2, & 3 \end{pmatrix},$$

takže $V_l(f) = \langle(-1,-2,0,1),(-2,-1,1,0)\rangle$, $V_p(f) = \langle(2,-3,0,1),(1,-2,1,0)\rangle$, $n(f) = h(f) = 2$.

3. Pro bilineární formu f z příkladu 1 nalezněme $\Phi_l^f(\boldsymbol{u})$ a $\Phi_p^f(\boldsymbol{u})$ pro vektor $\boldsymbol{u} = (1,2,-1)$.

Ř e š e n í : Protože $(\Phi_l^f(\boldsymbol{u}))(\boldsymbol{v}) = f(\boldsymbol{u},\boldsymbol{v})$ podle definice 12.4, stačí do analytického vyjádření bilineární formy f dosadit $\boldsymbol{u} = (1,2,-1)$, $v = (x_1,x_2,x_3)$ a dostaneme analytické vyjádření $(\Phi_l^f(\boldsymbol{u}))(\boldsymbol{v}) = (x_1 + 2x_2 + 3x_3) + 2(3x_1 + x_2 + 2x_3) - (5x_1 + 5x_2 + 8x_3) = 2x_1 - x_2 - x_3$ lineární formy $\Phi_l^f(\boldsymbol{u})$ vzhledem ke kanonické bázi prostoru R^3. Podobně $(\Phi_p^f(\boldsymbol{u}))(\boldsymbol{v}) = f(\boldsymbol{v},\boldsymbol{u})$, takže dosazením $\boldsymbol{u} = (x_1,x_2,x_3)$ a $\boldsymbol{v} = (1,2,-1)$ dostaneme $(\Phi_p^f(\boldsymbol{u}))(\boldsymbol{v}) = (x_1 + 3x_2 + 5x_3) + 2(2x_1 + x_2 + 5x_3) - (3x_1 + 2x_2 + 8x_3) = 2x_1 + 3x_2 + 7x_3$.

12.18. Definice. Bilineární forma f na vektorovém prostoru V se nazývá *symetrická*, jestliže $f(\boldsymbol{u},\boldsymbol{v}) = f(\boldsymbol{v},\boldsymbol{u})$, a *antisymetrická*, jestliže $f(\boldsymbol{u},\boldsymbol{v}) = -f(\boldsymbol{v},\boldsymbol{u})$ pro každé dva vektory $\boldsymbol{u},\boldsymbol{v} \in V$.

12.19. Poznámka. Nechť f, g jsou bilineární formy na vektorovém prostoru V a $r \in T$ buď libovolný prvek. Zobrazení $f+g$ a rf z $V \times V$ do T definovaná pro každou dvojici vektorů $\boldsymbol{u},\boldsymbol{v} \in V$ předpisy $(f+g)(\boldsymbol{u},\boldsymbol{v}) = f(\boldsymbol{u},\boldsymbol{v}) + g(\boldsymbol{u},\boldsymbol{v})$ a $(rf)(\boldsymbol{u},\boldsymbol{v}) = rf(\boldsymbol{u},\boldsymbol{v})$ jsou, jak se snadno ověří, opět bilineární formy na prostoru V. Není obtížné dokázat, že množina $B(V)$ všech bilineárních forem na prostoru V tvoří vzhledem k těmto operacím vektorový prostor a že podmnožiny $BS(V)$ a $BA(V)$ všech symetrických, resp. antisymetrických bilineárních forem na V jsou podprostory prostoru $B(V)$.

12.20. Věta. *Buď V vektorový prostor nad tělesem T,* char $T \neq 2$. *Pak platí*

(i) Podprostor $BA(V)$ je doplňkem podprostoru $BS(V)$ v prostoru $B(V)$;

(ii) každou bilineární formu f na prostoru V lze jednoznačně zapsat ve tvaru $f = f_s + f_a$, kde f_s je symetrická a f_a antisymetrická bilineární forma na prostoru V;

(iii) je-li f bilineární forma na V a $f = f_s + f_a$ její rozklad z tvrzení (ii), pak $f_s(\boldsymbol{u},\boldsymbol{v}) = \frac{1}{2}(f(\boldsymbol{u},\boldsymbol{v}) + f(\boldsymbol{v},\boldsymbol{u}))$ a $f_a(\boldsymbol{u},\boldsymbol{v}) = \frac{1}{2}(f(\boldsymbol{u},\boldsymbol{v}) - f(\boldsymbol{v},\boldsymbol{u}))$ pro každou dvojici vektorů $\boldsymbol{u},\boldsymbol{v} \in V$.

Důkaz. Je-li bilineární forma f na prostoru V současně symetrická i antisymetrická, platí pro každou dvojici vektorů $\boldsymbol{u},\boldsymbol{v} \in V$ rovnosti $f(\boldsymbol{u},\boldsymbol{v}) = f(\boldsymbol{v},\boldsymbol{u}) = -f(\boldsymbol{u},\boldsymbol{v})$, takže $f(\boldsymbol{u},\boldsymbol{v}) = 0$ vzhledem k tomu, že char $T \neq 2$ podle předpokladu. Tedy $BS(V) \cap BA(V) = 0$. Forma f_s z tvrzení (iii) je zřejmě symetrická, $f = f_s + f_a$ a f_a je antisymetrická, neboť $f_a(\boldsymbol{v},\boldsymbol{u}) = \frac{1}{2}(f(\boldsymbol{v},\boldsymbol{u}) - f(\boldsymbol{u},\boldsymbol{v})) = -\frac{1}{2}(f(\boldsymbol{u},\boldsymbol{v}) - f(\boldsymbol{v},\boldsymbol{u})) = -f_a(\boldsymbol{u},\boldsymbol{v})$. To však znamená, že $BA(V)$ je doplňkem $BS(V)$ v prostoru $B(V)$. K dokončení důkazu zbývá poznamenat, že jednoznačnost vyjádření v tvrzení (ii) plyne ihned z věty 9.25. ∎

12.21. Věta. *Buď f symetrická bilineární forma na vektorovém prostoru V a buď W doplněk vrcholu $V(f)$ formy f na V. Pak restrikce $g = f|W^2$ formy f na podprostor W je regulární bilineární forma na prostoru W.*

Důkaz. Potřebujeme ukázat, že vrchol $V(g)$ formy g je nulový. Buď tedy $\boldsymbol{u} \in V(g) \subseteq W$ libovolný vektor. Podle věty 9.25 lze libovolný vektor z prostoru V zapsat ve tvaru součtu $\boldsymbol{v} + \boldsymbol{w}$, kde $\boldsymbol{v} \in V(f)$ a $\boldsymbol{w} \in W$. Pak $f(\boldsymbol{u},\boldsymbol{w}) = 0$, protože $\boldsymbol{u} \in V(g)$. Celkem tedy máme $f(\boldsymbol{u},\boldsymbol{v}+\boldsymbol{w}) = f(\boldsymbol{u},\boldsymbol{v}) + f(\boldsymbol{u},\boldsymbol{w}) = 0$, takže $\boldsymbol{u} \in V(f)$ vzhledem k tomu, že $\boldsymbol{v}+\boldsymbol{w}$ byl libovolný vektor z prostoru V. Vidíme tedy, že $\boldsymbol{u} \in V(f) \cap W = 0$, tedy $V(g) = 0$ a věta je dokázána. ∎

12.22. Věta. *Buď f regulární symetrická bilineární forma na vektorovém prostoru V, buď $\boldsymbol{u}$ nenulový vektor z V a buď W nulová množina lineární formy $\Phi^f(\boldsymbol{u})$. Pak*

(i) restrikce $g = f|W^2$ je regulární symetrická bilineární forma na W, právě když $f(\boldsymbol{u},\boldsymbol{u}) \neq 0$;

(ii) je-li $f(\boldsymbol{u},\boldsymbol{u}) = 0$, pak $\langle \boldsymbol{u} \rangle$ je vrchol bilineární formy g.

Důkaz. Předpokládejme nejprve, že $f(\boldsymbol{u},\boldsymbol{u}) \neq 0$. Pak $(\Phi^f(\boldsymbol{u}))(\boldsymbol{u}) = f(\boldsymbol{u},\boldsymbol{u}) \neq 0$, takže $\boldsymbol{u} \notin W$. Podle věty 11.14 (i) je W nadrovina na V a podle poznámky 11.12 je $V = W \vee \langle \boldsymbol{u} \rangle$. Buď nyní $\boldsymbol{v} \in V(g) \subseteq W$ libovolný vektor. Každý vektor $\boldsymbol{u}' \in V$

lze zapsat ve tvaru $u' = ru + w$ pro nějaké $r \in T$ a $w \in W$ a platí $f(v, u') = rf(v, u) + f(v, w) = 0$, neboť $f(v, w) = 0$, protože $v \in V(g)$ a $f(v, u) = 0$ vzhledem k tomu, že $v \in W = \operatorname{Ker} \Phi^f(u)$ a $f(v, u) = (\Phi^f(u))(v)$. Vidíme tedy, že $f(v, u') = 0$ pro každé $u' \in V$, takže $v \in V(f) = 0$, neboť forma f je podle předpokladu regulární. Ukázali jsme, že $V(g) = 0$, a forma g je tudíž regulární symetrická bilineární forma na W.

K dokončení celého důkazu nyní zřejmě stačí dokázat tvrzení (ii). Předně víme, že $(\Phi^f(u))(w) = f(u, w) = 0$, právě když $w \in W$, takže speciálně $u \in W$ podle předpokladu, a tedy $u \in V(g)$. Zbývá dokázat naopak, že každý vektor z $V(g)$ leží v $\langle u \rangle$. Buď tedy $w \in V(g)$ libovolný vektor. Protože forma f je regulární, existuje vektor $u' \in V$ takový, že $f(u, u') \neq 0$, takže $f(w, u') = rf(u, u')$ pro nějaký prvek $r \in T$. Přitom $u' \notin W$, takže $V = W \vee \langle u' \rangle$ podle poznámky 11.12 vzhledem k tomu, že W je nadrovina ve V. Buď $su' + v$, $s \in T$, $v \in W$, libovolný vektor z V. Protože $w \in V(g)$, je $f(w, v) = 0$ a $f(u, v) = 0$, neboť $u \in V(g)$ a $v \in W$. Pak ale $f(w - ru, su' + v) = sf(w, u') - rsf(u, u') = 0$, vektor $w - ru$ leží ve vrcholu $V(f) = 0$ formy f, takže $w = ru$ a $V(g) = \langle u \rangle$. ∎

12.23. Věta. *Buď f regulární symetrická bilineární forma na vektorovém prostoru V nad tělesem T,* char $T \neq 2$. *Pak existuje vektor $u \in V$ takový, že $f(u, u) \neq 0$.*

Důkaz. Protože forma f je regulární, existují vektory $u, v \in V$ takové, že $f(u, v) \neq 0$. Předpokládáme-li nyní, že pro každý vektor $w \in V$ je $f(w, w) = 0$, máme speciálně $0 = f(u + v, u + v) = f(u, u) + 2f(u, v) + f(v, v) = 2f(u, v)$. Na druhé straně z char $T \neq 2$ plyne $2f(u, v) \neq 0$ a věta je dokázána. ∎

12.24. Definice. Báze $M = \{u_1, u_2, \ldots, u_n\}$ vektorového prostoru V_n se nazývá *polární báze* symetrické bilineární formy f, jestliže pro všechna $i, j = 1, 2, \ldots, n$, $i \neq j$, je $f(u_i, u_j) = 0$, tj. jestliže matice formy f vzhledem k bázi M je diagonální.

12.25. Věta. *Ke každé symetrické bilineární formě f na vektorovém prostoru V_n nad tělesem T,* char $T \neq 2$, *existuje polární báze.*

Důkaz. Předpokládejme nejprve, že forma f je regulární a postupujme úplnou indukcí podle dimenze n. Pro $n = 1$ je zřejmě každá báze polární. Nechť tedy $n > 1$ a předpokládejme, že pro $n - 1$ již tvrzení platí. Podle věty 12.23 existuje vektor $u_1 \in V_n$ takový, že $f(u_1, u_1) \neq 0$, takže podle věty 12.22 (i) je $g = f|W^2$, kde $W = \operatorname{Ker} \Phi^f(u_1)$, regulární symetrická bilineární forma. Protože W je nadrovina na V_n podle věty 11.14, existuje podle indukčního předpokladu polární báze $\{u_2, \ldots, u_n\}$ formy g. Jelikož $u_1 \notin W$, je množina $\{u_1, u_2, \ldots, u_n\}$ bází prostoru V_n, a protože $f(u_1, u_i) = (\Phi^f(u_1))(u_i) = 0$ pro každé $i = 2, \ldots, n$, je tato báze polární bází formy f.

Nechť tedy nyní forma f je singulární a buď W doplněk vrcholu $V(f)$ ve V_n. Podle věty 12.21 je restrikce $g = f|W^2$ regulární symetrická bilineární forma na W. Je-li nyní $\{u_1, u_2, \ldots, u_k\}$ libovolná báze vrcholu $V(f)$ a $\{u_{k+1}, \ldots u_n\}$ polární báze formy g, jejíž existenci jsme dokázali v první části důkazu, pak podle věty 9.25 je $\{u_1, u_2, \ldots, u_n\}$ báze prostoru V_n a z konstrukce vyplývá, že se jedná o polární bázi formy f vzhledem k tomu, že $f(u, v) = 0$ pro každý vektor $u \in V(f)$ a každý vektor $v \in V_n$. ∎

12.26. Poznámka. Důkaz předchozí věty je zároveň návodem k hledání polární báze symetrické bilineární formy, což si ukážeme v následujícím odstavci na konkrétních příkladech. Nyní si vyložíme podstatu jiné metody pro hledání polárních bází. Předně si uvědomme, že podle věty 10.2 je přiřazení souřadnic vzhledem k bázi vektorů z V_n izomorfismus prostoru V_n na aritmetický vektorový prostor T^n, takže se v dalším můžeme omezit na aritmetické vektorové prostory. Protože matice formy vzhledem k polární bázi je diagonální, potřebujeme popsat algoritmus, pomocí něhož lze převést matici dané formy f vzhledem k dané bázi tak, abychom dostali diagonální matici, která je zároveň maticí formy f vzhledem k nějaké (tedy polární) bázi. Buď tedy $\boldsymbol{A} \in T_n$ matice symetrické bilineární formy f vzhledem k dané bázi M prostoru T^n. Z věty 8.8 víme, že provést elementární transformaci na řádkové vektory matice $\boldsymbol{A}$ znamená vynásobit matici $\boldsymbol{A}$ maticí $\boldsymbol{B}$ této elementární transformace zleva. Přitom matice transponovaná $\boldsymbol{B}^T$ je matice přechodu od báze M k bázi M' vzniklé z M elementární transformací. Pak ale součin $\boldsymbol{BAB}^T$ je podle věty 12.7 matice formy f vzhledem k bázi M'. Pohlížíme-li nyní na bázi M jako na matici, jejíž řádkové vektory jsou právě prvky této báze, je zřejmě $\boldsymbol{B}M = M'$. Teď již algoritmus snadno popíšeme. Utvořme matici $(\boldsymbol{A}|M)$ typu $(n, 2n)$ a provádějme na řádky této matice elementární transformace tak, abychom nakonec dostali pod diagonálou samé nuly. Po provedení každé elementární transformace provedeme stejnou transformaci na sloupce matice. Je zřejmé, že tyto sloupcové operace se týkají pouze prvních n sloupců a že po konečném počtu kroků dostaneme v levé části matice matici diagonální. Ze shora uvedeného výkladu pak ihned plyne, že v pravé části matice bude po řádcích psaná polární báze formy f.

12.27. Příklady. 1. Najděme polární bázi symetrické bilineární formy f, jejíž analytické vyjádření ke kanonické bázi K aritmetického vektorového prostoru R^4 je $f(\boldsymbol{u}, \boldsymbol{v}) = 2x_1y_1 + 3x_1y_2 + 3x_2y_1 + x_1y_3 + x_3y_1 - x_1y_4 - x_4y_1 + 4x_2y_2 + 2x_2y_3 + 2x_3y_2 + 2x_3y_3$.

Ř e š e n í : Matice formy f vzhledem k bázi K je

$$\boldsymbol{A} = \begin{pmatrix} 2, & 3, & 1, & -1 \\ 3, & 4, & 2, & 0 \\ 1, & 2, & 2, & 0 \\ -1, & 0, & 0, & 0 \end{pmatrix}.$$

Rozvojem podle posledního sloupce a pak posledního řádku snadno spočteme determinant matice $\boldsymbol{A}$

$$\det \boldsymbol{A} = \begin{vmatrix} 3, & 4, & 2 \\ -1, & 2, & 2 \\ -1, & 0, & 0 \end{vmatrix} = -\det \begin{vmatrix} 4, & 2 \\ 2, & 2 \end{vmatrix} = -4,$$

takže forma f je regulární podle poznámky 12.12 a věty 8.4. Zvolíme-li $\boldsymbol{u}_1 = \boldsymbol{e}_1 = (1, 0, 0, 0)$, je $f(\boldsymbol{u}_1, \boldsymbol{u}_1) = 2$ a $(\Phi^f(\boldsymbol{u}_1))(\boldsymbol{u}) = 2x_1 + 3x_2 + x_3 - x_4$. Druhý vektor hledáme tak, aby ležel v Ker $\Phi^f(\boldsymbol{u}_1)$, tj. aby splňoval rovnici $2x_1 + 3x_2 + x_3 - x_4 = 0$ a přitom aby bylo $f(\boldsymbol{u}_2, \boldsymbol{u}_2) \neq 0$. Např. pro $\boldsymbol{u}_2 = (0, 0, 1, 1)$ je $f(\boldsymbol{u}_2, \boldsymbol{u}_2) = 2$ a $(\Phi^f(\boldsymbol{u}_2))(\boldsymbol{u}) = 2x_2 + 2x_3$. Dále vektor $\boldsymbol{u}_3$ hledáme v průniku Ker $\Phi^f(\boldsymbol{u}_1) \cap$ Ker $\Phi^f(\boldsymbol{u}_2)$ tak, aby $f(\boldsymbol{u}_3, \boldsymbol{u}_3) \neq 0$. Vezmeme-li $\boldsymbol{u}_3 = (1, 0, 0, 2)$, je $f(\boldsymbol{u}_3, \boldsymbol{u}_3) = -2$ a $(\Phi^f(\boldsymbol{u}_3))(\boldsymbol{u}) = 3x_2 + x_3 - x_4$. Poslední vektor nalezneme tak, aby ležel v průniku Ker

$\Phi_f(\boldsymbol{u}_1)\cap$ Ker $\Phi^f(\boldsymbol{u}_2)\cap$ Ker $\Phi^f(\boldsymbol{u}_3)$. Zde leží např. vektor $\boldsymbol{u}_4 = (0,1,-1,2)$ a hledaná polární báze formy f je $M = \{(1,0,0,0), (0,0,1,1,), (1,0,0,2), (0,1,-1,2)\}$.

2. Najděme polární bázi symetrické bilineární formy f, jejíž analytické vyjádření vzhledem ke kanonické bázi K aritmetického vektorového prostoru R^4 je $f(\boldsymbol{u},\boldsymbol{v}) = x_1y_1 + x_2y_2 + x_3y_3 - x_4y_4 - x_1y_2 - x_2y_1$.

Řešení: Matice formy f vzhledem ke kanonické bázi K je

$$\boldsymbol{A} = \begin{pmatrix} 1, & -1, & 0, & 0 \\ -1, & 1, & 0, & 0 \\ 0, & 0, & 1, & 0 \\ 0, & 0, & 0, & -1 \end{pmatrix}.$$

Snadno se nahlédne, že det $\boldsymbol{A} = 0$, takže forma f je singulární. Podle věty 12.10 je vrchol formy f právě množina všech řešení homogenní soustavy lineárních rovnic s maticí $\boldsymbol{A}$, takže je okamžitě patrné, že $V(f) = \langle(1,1,0,0)\rangle$. Podle poznámky 2.20 můžeme vektor $\boldsymbol{u}_1 = (1,1,0,0)$ doplnit na bázi prostoru R^4 např. vektory $\boldsymbol{e}_2, \boldsymbol{e}_3, \boldsymbol{e}_4$ z kanonické báze, takže $W = \langle \boldsymbol{e}_2, \boldsymbol{e}_3, \boldsymbol{e}_4\rangle$ je doplněk $V(f)$ v R^4. Forma $g = f|W$ je podle věty 12.21 regulární a její analytické vyjádření k bázi $N = \{\boldsymbol{e}_2, \boldsymbol{e}_3, \boldsymbol{e}_4\}$ je $g(\boldsymbol{u},\boldsymbol{v}) = x_1y_1 + x_2y_2 - x_3y_3$, kde $\{\boldsymbol{u}\}_N = (x_1,x_2,x_3)$ a $\{\boldsymbol{v}\}_N = (y_1,y_2,y_3)$. Odtud je ihned patrné, že N je polární báze formy g, a tedy $M = \{(1,1,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1)\}$ je polární bází formy f.

3. Metodou z poznámky 12.26 nalezněme polární bázi symetrické bilineární formy z předchozího příkladu.

Řešení: Vzhledem k tomu, že vycházíme z kanonické báze, máme

$$\left(\begin{array}{cccc|cccc} 1, & -1, & 0, & 0 & 1, & 0, & 0, & 0 \\ -1, & 1, & 0, & 0 & 0, & 1, & 0, & 0 \\ 0, & 0, & 1, & 0 & 0, & 0, & 1, & 0 \\ 0, & 0, & 0, & -1 & 0, & 0, & 0, & 1 \end{array}\right) \sim \left(\begin{array}{cccc|cccc} 1, & -1, & 0, & 0 & 1, & 0, & 0, & 0 \\ 0, & 0, & 0, & 0 & 1, & 1, & 0, & 0 \\ 0, & 0, & 1, & 0 & 0, & 0, & 1, & 0 \\ 0, & 0, & 0, & -1 & 0, & 0, & 0, & 1 \end{array}\right) \sim$$

$$\left(\begin{array}{cccc|cccc} 1, & 0, & 0, & 0 & 1, & 0, & 0, & 0 \\ 0, & 0, & 0, & 0 & 1, & 1, & 0, & 0 \\ 0, & 0, & 1, & 0 & 0, & 0, & 1, & 0 \\ 0, & 0, & 0, & -1 & 0, & 0, & 0, & 1 \end{array}\right),$$

takže $M = \{(1,0,0,0), (1,1,0,0), (0,0,1,0), (0,0,0,1)\}$ je polární báze formy f, přičemž druhý vektor, odpovídající nulovému řádku v levé polovině matice, je generátor vrcholu formy f.

13.1. Definice. Buď f bilineární forma na vektorovém prostoru V. Zobrazení $f_2 : V \to T$ definovaná pro každé $\boldsymbol{u} \in V$ předpisem $f_2(\boldsymbol{u}) = f(\boldsymbol{u}, \boldsymbol{u})$ se nazývá *kvadratická forma* na prostoru V *vytvořená bilineární formou* f. Jestliže $f_2(\boldsymbol{u}) = 0$ pro každé $\boldsymbol{u} \in V$, nazývá se forma f *triviální* nebo *nulová*. V opačném případě říkáme, že forma f je *netriviální* nebo *nenulová*.

13.2. Věta. *Buďte f, g bilineární formy na vektorovém prostoru V nad tělesem T,* $\operatorname{char} T \neq 2$. *Pak platí*

(i) je-li f antisymetrická, je f_2 triviální;
(ii) $f_2 = (f_s)_2$;
(iii) $f_2 = g_2$, právě když $f_s = g_s$;
(iv) $f_s(\boldsymbol{u}, \boldsymbol{v}) = \frac{1}{2}(f_2(\boldsymbol{u}+\boldsymbol{v}) - f_2(\boldsymbol{u}) - f_2(\boldsymbol{v}))$.

Důkaz. (i) Pro libovolný vektor $\boldsymbol{u} \in V$ jest $f(\boldsymbol{u}, \boldsymbol{u}) = -f(\boldsymbol{u}, \boldsymbol{u})$, takže $f_2(\boldsymbol{u}) = f(\boldsymbol{u}, \boldsymbol{u}) = 0$ vzhledem k tomu, že $\operatorname{char} T \neq 2$.

(ii) Podle věty 12.20 (ii) je $f = f_s + f_a$, kde f_s je symetrická a f_a antisymetrická bilineární forma a stačí použít (i).

(iii) Je-li $f_s = g_s$, je $f_2 = g_2$ podle (ii). K důkazu obrácené implikace stačí dokázat tvrzení (iv).

(iv) Použitím (ii) dostáváme $f_2(\boldsymbol{u}+\boldsymbol{v}) = f_s(\boldsymbol{u}+\boldsymbol{v}, \boldsymbol{u}+\boldsymbol{v}) = f_2(\boldsymbol{u}) + 2f_s(\boldsymbol{u}, \boldsymbol{v}) + f_2(\boldsymbol{v})$, odkud dokazovaná rovnost ihned plyne. ∎

13.3. Poznámka. Právě dokázaná věta jinými slovy říká, že je-li V vektorový prostor nad tělesem T, $\operatorname{char} T \neq 2$, pak každá kvadratická forma na V jednoznačně určuje symetrickou bilineární formu, která ji vytváří. Kvadratické a symetrické bilineární formy si tedy v tomto smyslu vzájemně jednoznačně odpovídají.

13.4. Definice. Buď f_2 kvadratická forma na vektorovém prostoru V nad tělesem T, $\operatorname{char} T \neq 2$. Jednoznačně určená symetrická bilineární forma g vytvářející kvadratickou formu f_2 daná podle věty 13.2 předpisem $g(\boldsymbol{u}, \boldsymbol{v}) = \frac{1}{2}(f_2(\boldsymbol{u}+\boldsymbol{v}) - f_2(\boldsymbol{u}) - f_2(\boldsymbol{v}))$, $\boldsymbol{u}, \boldsymbol{v} \in V$, se nazývá *polární bilineární forma* kvadratické formy f_2.

13.5. Definice. Buď f_2 kvadratická forma na vektorovém prostoru V s polární bilineární formou f. *Vrcholem (nulitou, polární bází)* formy f_2 rozumíme vrchol (nulitu, polární bázi) polární bilineární formy f.

13.6. Definice. Buď $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ báze vektorového prostoru V_n. Je-li $\{\boldsymbol{u}\}_M = (x_1, x_2, \dots, x_n)$, pak výraz $f_2(\boldsymbol{u}) = \sum_{i,j=1}^{n} x_i x_j f(\boldsymbol{u}_i, \boldsymbol{u}_j)$, kde f je polární bilineární forma kvadratické formy f_2, nazýváme *analytickým vyjádřením* formy f_2 vzhledem k bázi M. Matice formy f vzhledem k bázi M se nazývá *matice formy* f_2 vzhledem k bázi M. Forma f_2 se nazývá *regulární (singulární)*, je-li její polární bilineární forma f regulární (singulární).

13.7. Příklad. Kvadratická forma f_2 na aritmetickém vektorovém prostoru R^3 je dána analytickým vyjádřením $f_2(\boldsymbol{u}) = x_1^2 + 2x_1x_2 + 6x_1x_3 + 2x_2^2 + 8x_2x_3 + 10x_3^2$ vzhledem ke kanonické bázi K tohoto prostoru. Nalezněme polární bilineární formu f formy f_2, matici vzhledem k bázi K, vrchol a (nějakou) polární bázi formy f_2.

Ř e š e n í: Polární bilineární formu f formy f_2 můžeme nalézt pomocí formule z věty 13.2 (iv). Tato metoda je však poměrně zdlouhavá, a proto zkusíme jinou cestu. Stačí si totiž uvědomit, jak jednotliví sčítanci analytického vyjádření formy f_2 z polární bilineární formy f vznikají. Člen x_i^2 vznikne pouze ze členu $x_i y_i$, zatímco člen $x_i x_j, i \neq j$, vznikne jednak z $x_i y_j$, jednak ze symetrického členu $x_j y_i$. Prakticky to tedy znamená, že místo x_i^2 píšeme $x_i y_i$ se stejným koeficientem a místo $x_i x_j$ píšeme $x_i y_j$ a $x_j y_i$, každý s polovičním koeficientem. V našem případě tedy máme $f(\boldsymbol{u}, \boldsymbol{v}) = x_1y_1 + x_1y_2 + x_2y_1 + 3x_1y_3 + 3x_3y_1 + 2x_2y_2 + 4x_2y_3 + 4x_3y_2 + 10x_3y_3$. Nyní již snadno napíšeme matici a spočteme vrchol $V(f_2)$. Jest

$$\begin{pmatrix} 1, & 1, & 3 \\ 1, & 2, & 4 \\ 3, & 4, & 10 \end{pmatrix} \sim \begin{pmatrix} 1, & 1, & 3 \\ 0, & 1, & 1 \\ 0, & 1, & 1 \end{pmatrix},$$

takže $V(f_2) = \langle(2, 1, -1)\rangle$ a forma je singulární, $n(f_2) = 1$, $h(f_2) = 2$. Je patrné, že např. $W = \langle \boldsymbol{e}_1, \boldsymbol{e}_2 \rangle$ je doplňkem vrcholu $V(f_2)$ v R^3. Přitom $N = \{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ je báze W a forma $g = f|W$ má vzhledem k bázi N analytické vyjádření $g(\boldsymbol{u}, \boldsymbol{v}) = x_1y_1 + x_1y_2 + x_2y_1 + 2x_2y_2$, $\{\boldsymbol{u}\}_N = (x_1, x_2)$, $\{\boldsymbol{v}\}_N = (y_1, y_2)$. Polární bázi formy g nyní snadno nalezneme. Jest $\{\boldsymbol{u}_1\}_N = (1, 0)$, $g_2(\boldsymbol{u}_1) = 1$, $g(\boldsymbol{u}_1, \boldsymbol{v}) = x_1 + x_2 = 0$, $\{\boldsymbol{u}_2\}_N = (1, -1)$. Ve smyslu poznámky 12.26 je tedy $M = \{(2, 1, -1), (1, 0, 0), (1, -1, 0)\}$ polární báze formy f_2.

13.8. Věta. *Buď $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ polární báze kvadratické formy f_2 na vektorovém prostoru V_n. Pak platí*

(i) $f_2(\boldsymbol{u}) = \sum_{i=1}^n x_i^2 f_2(\boldsymbol{u}_i)$ je analytické vyjádření formy f_2 vzhledem k bázi M.
(ii) $\boldsymbol{u}_i \in V(f_2)$, právě když $f_2(\boldsymbol{u}_i) = 0$;
(iii) $V(f_2) = \langle \boldsymbol{u}_i \mid f_2(\boldsymbol{u}_i) = 0, i \in \{1, 2, \dots, n\}\rangle$;

Důkaz. (i) Tvrzení je bezprostředním důsledkem definice polární báze 12.24.

(ii) Je-li $\boldsymbol{u} \in V_n$ libovolný vektor, $\{\boldsymbol{u}\}_M = \{x_1, x_2, \dots, x_n\}$, je $\boldsymbol{u} = \sum_{j=1}^n x_j \boldsymbol{u}_j$, a tedy $f(\boldsymbol{u}_i, \boldsymbol{u}) = f(\boldsymbol{u}_i, \sum_{j=1}^n x_j \boldsymbol{u}_j) = \sum_{j=1}^n x_j f(\boldsymbol{u}_i, \boldsymbol{u}_j) = x_i f_2(\boldsymbol{u}_i)$. Vidíme tedy, že $\boldsymbol{u}_i \in V(f_2)$, právě když $f(\boldsymbol{u}_i, \boldsymbol{u}) = 0$ pro každé $\boldsymbol{u} \in V_n$, což je podle předchozího ekvivalentní s tím, že $f_2(\boldsymbol{u}_i) = 0$.

(iii) Je zřejmé, že změníme-li pořadí vektorů v polární bázi, dostaneme opět polární bázi dané kvadratické formy. Můžeme tedy bez újmy na obecnosti předpokládat, že pro nějaké $k \in \{0, 1, \dots, n\}$ je $f_2(\boldsymbol{u}_1) = f_2(\boldsymbol{u}_2) = \cdots = f_2(\boldsymbol{u}_k) = 0$ a $f_2(\boldsymbol{u}_{k+1}) \neq 0, \dots, f_2(\boldsymbol{u}_n) \neq 0$. Označíme-li $W = \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k \rangle$, je $W \subseteq V(f_2)$ podle (ii). Buď tedy obráceně $\boldsymbol{u} \in V(f_2)$ libovolný vektor, $\boldsymbol{u} = \sum_{j=1}^n x_j \boldsymbol{u}_j$. Pro libovolný index $i \in \{k+1, \dots, n\}$ máme $f(\boldsymbol{u}, \boldsymbol{u}_i) = f(\sum_{j=1}^n x_j \boldsymbol{u}_j, \boldsymbol{u}_i) = \sum_{j=1}^n x_j f(\boldsymbol{u}_j, \boldsymbol{u}_i) = x_i f_2(\boldsymbol{u}_i) = 0$ vzhledem k tomu, že $\boldsymbol{u} \in V(f_2)$. Protože $f_2(\boldsymbol{u}_i) \neq 0$, je nutně $x_i = 0$, a tedy $\boldsymbol{u} = \sum_{j=1}^k x_j \boldsymbol{u}_j \in W$. ■

13.9. Definice. Buď W podprostor reálného vektorového podprostoru V a buď f_2 kvadratická forma na V. Řekneme, že forma f_2 je *pozitivně (negativně) definitní na W*, jestliže pro každé $0 \neq \boldsymbol{u} \in W$ je $f_2(\boldsymbol{u}) > 0$ $(f_2(\boldsymbol{u}) < 0)$.

13.10. Definice. Buď $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ polární báze kvadratické formy f_2 na reálném vektorovém prostoru V_n. Označme $p(f_2)$ počet těch vektorů $\boldsymbol{u}_i \in M$, pro něž $f_2(\boldsymbol{u}_i) > 0$ a $q(f_2)$ počet těch vektorů $\boldsymbol{u}_j \in M$, pro něž $f_2(\boldsymbol{u}_j) < 0$. Uspořádaná trojice $< n(f_2), p(f_2), q(f_2) >$ se nazývá *signatura kvadratické formy f_2*.

13.11. Poznámka. Právě definovaný pojem signatury kvadratické formy je vázán k *dané* polární bázi M. Přesněji bychom tedy měli hovořit o signatuře formy f_2 vzhledem k polární bázi M. Důvodem, proč tak nečiníme, je tzv. zákon setrvačnosti kvadratických forem (věta 13.14), který říká, že signatura formy f_2 nezávisí na volbě polární fáze této formy.

13.12. Věta. *Buď* $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k, \boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_l, \boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_m\}$ *polární báze kvadratické formy* f_2 *na reálném vektorovém prostoru* V_n *taková, že* $f_2(\boldsymbol{u}_i) = 0, i = 1, 2, \dots, k$, $f_2(\boldsymbol{v}_j) > 0, j = 1, 2, \dots, l$, *a* $f_2(\boldsymbol{w}_r) < 0, r = 1, 2, \dots, m$, *a buď* W *podprostor prostoru* V_n. *Pak*

(i) *je-li* f_2 *pozitivně definitní na* W, *je* $\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k, \boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_m\rangle \cap W = 0$;

(ii) *je-li* f_2 *negativně definitní na* W, *je* $\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k, \boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_l\rangle \cap W = 0$.

Důkaz. (i) Je-li $\boldsymbol{u} \in \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k, \boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_m\rangle \in W$ libovolný vektor, je $f_2(\boldsymbol{u}) \geq 0$ a $f_2(\boldsymbol{u}) = 0$, právě když $\boldsymbol{u} = 0$ vzhledem k tomu, že $\boldsymbol{u} \in W$. Na druhé straně je $\boldsymbol{u} = \sum_{i=1}^{k} r_i \boldsymbol{u}_i + \sum_{j=1}^{m} s_j \boldsymbol{w}_j$, takže $f_2(\boldsymbol{u}) = \sum_{j=1}^{m} s_j^2 f_2(\boldsymbol{w}_j) \leq 0$, odkud tvrzení ihned plyne. Druhé tvrzení se dokáže analogicky. ∎

13.13. Věta. *Buď* $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k, \boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_l, \boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_m\}$ *polární báze kvadratické formy* f_2 *na reálném vektorovém prostoru* V_n *taková, že* $f_2(\boldsymbol{u}_i) = 0, i = 1, 2, \dots, k$, $f_2(\boldsymbol{v}_j) > 0, j = 1, 2, \dots, l$ *a* $f_2(\boldsymbol{w}_r) < 0, r = 1, 2, \dots, m$. *Pak*

(i) $\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k\rangle = V(f_2)$;

(ii) f_2 *je pozitivně definitní na* $\langle \boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_l\rangle$;

(iii) f_2 *je negativně definitní na* $\langle \boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_m\rangle$.

Důkaz. (i) Viz věta 13.8 (iii).

(ii) Pro libovolný vektor $\boldsymbol{v} = \sum_{i=1}^{l} r_i \boldsymbol{v}_i \in \langle \boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_l\rangle$ je $f_2(\boldsymbol{v}) = \sum_{i=1}^{l} r_i^2 f_2(\boldsymbol{v}_i) \geq 0$, přičemž $f_2(\boldsymbol{v}) = 0$, právě když $r_1 = r_2 = \dots = r_l = 0$, tj. právě když $\boldsymbol{v} = 0$.

(iii) Analogicky jako (ii). ∎

13.14. Věta. (Zákon setrvačnosti kvadratických forem.) *Buď* f_2 *kvadratická forma na reálném vektorovém prostoru* V_n. *Pak signatura formy* f_2 *nezávisí na volbě polární báze a platí*

$$n(f_2) + p(f_2) + q(f_2) = n.$$

Důkaz. Podle věty 13.13 (i) je $n(f_2)$ rovno počtu vektorů $\boldsymbol{u}$ z polární báze takových, že $f_2(\boldsymbol{u}) = 0$. Rovnost $n(f_2) + p(f_2) + q(f_2) = n$ pak plyne přímo z definice signatury. Buďte nyní $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k, \boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_l, \boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_m\}$ a $M' = \{\boldsymbol{u}'_1, \boldsymbol{u}'_2, \dots, \boldsymbol{u}'_{k'}, \boldsymbol{v}'_1, \boldsymbol{v}'_2, \dots, \boldsymbol{v}'_{l'}, \boldsymbol{w}'_1, \boldsymbol{w}'_2, \dots, \boldsymbol{w}'_{m'}\}$ dvě polární báze formy f_2 takové, že $f_2(\boldsymbol{u}_i) = f_2(\boldsymbol{u}'_{i'}) = 0, i = 1, 2, \dots, k$, $i' = 1, 2, \dots, k'$, $f_2(\boldsymbol{v}_j) > 0, f_2(\boldsymbol{v}'_{j'}) > 0$, $j = 1, 2, \dots, l$, $j' = 1, 2, \dots, l'$, a $f_2(\boldsymbol{w}_r) < 0, f_2(\boldsymbol{w}'_{r'}) < 0, r = 1, 2, \dots, m, r' = 1, 2, \dots, m'$. Podle tvrzení (i) předchozí věty je $k = k'$. Podle tvrzení (ii) téže věty je forma f_2 pozitivně definitní na $W_1 = \langle \boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_l\rangle$, takže položíme-li $W'_2 = \langle \boldsymbol{u}'_1, \boldsymbol{u}'_2, \dots, \boldsymbol{u}'_k, \boldsymbol{w}'_1, \boldsymbol{w}'_2, \dots, \boldsymbol{w}'_{m'}\rangle$, je $W_1 \cap W'_2 = 0$ podle věty 13.12 (i). Pak ale pomocí věty o dimenzi spojení a průniku 2.23 dostáváme $\dim W_1 + \dim W'_2 = l + k + m' = \dim W_1 \vee W'_2 \leq n = l + k + m$, odkud plyne nerovnost $m' \leq m$. Podobným způsobem pro $W'_1 = \langle \boldsymbol{v}'_1, \boldsymbol{v}'_2, \dots, \boldsymbol{v}'_{l'}\rangle$ a $W_2 = \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k, \boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_m\rangle$ dostaneme nerovnost $l' + k + m \leq l' + k + m'$ tj. $m \leq m'$, a tedy $m = m'$. Pak ale $l' = n - k - m' = n - k - m = l$ a jsme hotovi. ∎

13.15. Definice. Buď f_2 netriviální kvadratická forma na reálném vektorovém prostoru V_n a buď $\langle n(f_2), p(f_2), q(f_2)\rangle$ její signatura. Říkáme, že forma f_2 je
- *pozitivně definitní*, jestliže $n(f_2) = q(f_2) = 0$;
- *pozitivně semidefinitní*, jestliže $q(f_2) = 0$ a $n(f_2) > 0$;
- *negativně definitní*, jestliže $n(f_2) = p(f_2) = 0$;
- *negativně semidefinitní*, jestliže $p(f_2) = 0$ a $n(f_2) > 0$;
- *indefinitní*, jestliže $p(f_2) > 0$ a $q(f_2) > 0$.

Je-li f_2 buď pozitivně, nebo negativně definitní (semidefinitní), pak říkáme, že f_2 je *definitní (semidefinitní)*. O symetrické bilineární formě f na V_n říkáme, že je *pozitivně definitní (negativně definitní atd.)*, je-li jí vytvořená kvadratická forma f_2 pozitivně definitní (negativně definitní atd.).

13.16. Věta. *Buď f_2 regulární kvadratická forma na reálném vektorovém prostoru V_n a buď $\boldsymbol{A}$ její matice vzhledem k bázi M prostoru V_n. Označme $D_i, i = 1, 2, \ldots, n$, determinant dílčí matice $\boldsymbol{A}$, která vznikne z matice $\boldsymbol{A}$ vynecháním posledních $n - i$ řádků a posledních $n-i$ sloupců. Je-li $D_1D_2 \ldots D_n \neq 0$, pak $p(f_2)$ je počet kladných členů posloupnosti D_1, D_1D_2, $D_2D_3, \ldots, D_{n-1}D_n$ a $q(f_2)$ je počet záporných členů této posloupnosti.*

Důkaz. Pro zjednodušení zápisu položme $D_0 = 1$. Označme $\boldsymbol{A}_i$ dílčí matici matice $\boldsymbol{A}$, která vznikne z $\boldsymbol{A}$ vynecháním posledních $n-i$ řádků a posledních $n-i$ sloupců. Pro každé $i = 1, 2, \ldots, n$ a $j = 1, 2, \ldots, i$ buď A_{ij} algebraický doplněk prvku a_{ij} v matici $\boldsymbol{A}_i$ a definujme vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ pomocí jejich souřadnic vzhledem k bázi M takto: $\{\boldsymbol{u}_1\}_M = (1, 0, \ldots, 0)$, $\{\boldsymbol{u}_2\}_M = (A_{21}, A_{22}, 0, \ldots, 0)$, ..., $\{\boldsymbol{u}_i\}_M = (A_{i1}, A_{i2}, \ldots, A_{ii}, 0, \ldots, 0)$, ..., $\{\boldsymbol{u}_n\}_M = (A_{n1}, A_{n2}, \ldots, A_{nn})$. Podle věty o rozvoji determinantu podle řádku 7.11 pro každé $i = 1, 2, \ldots, n$ je $\boldsymbol{A} \cdot \{\boldsymbol{u}_i\}_M^T = (0, 0, \ldots, 0, D_i, d_{i,i+1}, \ldots, d_{in})$, kde d_{ik}, $k = i + 1, \ldots, n$ jsou nějaká reálná čísla. Podle věty 12.3 je $f(\boldsymbol{u}_j, \boldsymbol{u}_i) = \{\boldsymbol{u}_j\}_M \boldsymbol{A} \{\boldsymbol{u}_i\}_M^T$, odkud je ihned vidět, že pro $j < i$ je $f(\boldsymbol{u}_j, \boldsymbol{u}_i) = 0$ a pro $j = i$ je $f_2(\boldsymbol{u}_i) = A_{ii}D_i = D_{i-1}D_i$. Ukázali jsme tedy, že množina $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ je polární bází formy f_2, $f_2(\boldsymbol{u}_i) = D_{i-1}D_i$ pro každé $i = 1, 2, \ldots, n$ a tvrzení plyne bezprostředně z definice signatury. ∎

13.17. Důsledek. *Buď f_2 kvadratická forma na reálném vektorovém prostoru V_n a nechť čísla $D_i, i = 1, 2, \ldots, n$, mají stejný význam jako v předešlé větě. Pak forma f_2 je pozitivně definitní, právě když $D_i > 0$ pro všechna $i = 1, 2, \ldots, n$.*

Důkaz. Podmínka je podle předešlé věty zřejmě postačující. Nechť tedy forma f_2 je pozitivně definitní a nechť $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ jsou vektory z důkazu předešlé věty. K důkazu nerovnosti $D_i > 0$, $i = 1, 2, \ldots, n$, použijeme úplnou indukci. Pro $i = 1$ máme $D_1 = f_2(\boldsymbol{u}_1) > 0$. Předpokládáme-li nyní, že $i > 1$ a $D_{i-1} > 0$, plyne z rovnosti $A_{ii} = D_{i-1} > 0$ nenulovost vektoru $\boldsymbol{u}_i$, takže $f_2(\boldsymbol{u}_i) = D_{i-1}D_i > 0$, a tedy i $D_i > 0$. Odtud již tvrzení ihned plyne. ∎

13.18. Poznámka. Je-li f_2 regulární kvadratická forma na reálném vektorovém prostoru V_n, nemusí ještě obecně platit, že $D_1D_2, \ldots, D_n \neq 0$ (například je-li $f_2(\boldsymbol{u}) = 2x_1x_2$ kvadratická forma na $\boldsymbol{R}^2$, je $D_1 = 0, D_2 = -1$). Není však zpravidla obtížné přechodem k jiné bázi dosáhnout toho, aby předpoklady věty 13.16 byly splněny. Podle věty 12.7 k tomu stačí provádět elementární transformace na řádky matice formy a současně s tím tytéž transformace na její sloupce. V následujícím odstavci si tento postup ukážeme na konkrétním příkladě.

13.19. Příklady. Určeme signatury následujících kvadratických forem na vektorových prostorech R^n, jsou-li formy dány analytickými vyjádřeními vzhledem ke kanonickým bázím příslušných prostorů:

a) $f_2(\boldsymbol{u}) = 2x_1x_3 - 4x_2x_3$ na R^3;

b) $f_2(\boldsymbol{u}) = x_1^2 + x_2^2 + 3x_3^2 + 4x_1x_2 + 2x_1x_3 + +2x_2x_3$ na R^3;

c) $f_2(\boldsymbol{u}) = 2x_1x_3 + 4x_1x_4 + 4x_2x_3 + 2x_2x_4 + 3x_3^2 + +2x_3x_4 + 2x_4^2$ na R^4.

Ř e š e n í: a) Matice formy f_2 vzhledem ke kanonické bázi zřejmě je

$$\boldsymbol{A} = \begin{pmatrix} 0, & 0, & 1 \\ 0, & 0, & -2 \\ 1, & -2, & 0 \end{pmatrix},$$

odkud je ihned vidět, že $h(\boldsymbol{A}) = 2$, a tedy $n(f_2) = 1$. Podle věty 12.10 je $V(f_2) = \langle(2,1,0)\rangle$. Ve smyslu poznámky 2.20 můžeme vzít např. $N = \{\boldsymbol{e}_2, \boldsymbol{e}_3\}$ za bázi doplňku W vrcholu $V(f_2)$, takže restrikce $g_2 = f_2|W$ bude mít vzhledem k bázi N analytické vyjádření $g(\boldsymbol{u}, \boldsymbol{v}) = -2x_1y_2 - 2x_2y_1$. Najděme polární bázi formy g_2. Jest $\{\boldsymbol{u}_1\}_N = (1,1)$, $g_2(\boldsymbol{u}_1) = -4$, $g(\boldsymbol{u}_1, \boldsymbol{u}) = -2x_1 - 2x_2 = 0$, $\{\boldsymbol{u}_2\}_N = (1,-1)$, $g_2(\boldsymbol{u}_2) = 4$. Nyní je již zcela zřejmé, že $\{(2,1,0),(0,1,1),(0,1,-1)\}$ je polární báze a že vzhledem k větě 13.8 je signatura formy f_2 rovna $\langle 1,1,1\rangle$.

b) Napišme matici formy f_2 vzhledem ke kanonické bázi prostoru R^3 a zjistěme její hodnost. Jest

$$\begin{pmatrix} 1, & 2, & 1 \\ 2, & 1, & 1 \\ 1, & 1, & 3 \end{pmatrix} \sim \begin{pmatrix} 1, & 2, & 1 \\ 0, & -3, & -1 \\ 0, & -1, & 2 \end{pmatrix} \sim \begin{pmatrix} 1, & 2, & 1, \\ 0, & -1, & 2 \\ 0, & 0, & -7 \end{pmatrix}$$

a forma je regulární. Najděme polární bázi formy f_2. Jest $\boldsymbol{u}_1 = (1,0,0)$, $f_2(\boldsymbol{u}_1) = 1$, $f(\boldsymbol{u}_1, \boldsymbol{u}) = x_1 + 2x_2 + x_3 = 0$, $\boldsymbol{u}_2 = (1,0,-1)$, $f_2(\boldsymbol{u}_2) = 2$ $f(\boldsymbol{u}_2, \boldsymbol{u}) = x_2 - 2x_3 = 0$, $\boldsymbol{u}_3 = (-5,2,1)$, $f_2(\boldsymbol{u}_3) = -14$, a signatura formy f_2 je $\langle 0,2,1\rangle$. Stejný výsledek dostaneme použitím věty 13.16. Zde máme $D_1 = 1, D_2 = -3$ a

$$D_3 = \begin{vmatrix} 1, & 2, & 1 \\ 2, & 1, & 1 \\ 1, & 1, & 3 \end{vmatrix} = \begin{vmatrix} 1, & 2, & 1 \\ 0, & -3, & -1 \\ 0, & -1, & 2 \end{vmatrix} = -7,$$

takže $D_1 = 1, D_1D_2 = -3, D_2D_3 = 21$.

c) Napišme matici $\boldsymbol{A}$ formy f_2,

$$\boldsymbol{A} = \begin{pmatrix} 0, & 0, & 1, & 2 \\ 0, & 0, & 2, & 1 \\ 1, & 2, & 3, & 1 \\ 2, & 1, & 1, & 2 \end{pmatrix},$$

a spočtěme její determinant. Máme (rozvoj nejprve podle druhého, pak podle prvního řádku)

$$|\boldsymbol{A}| = \begin{vmatrix} 0, & 0, & 1, & 2 \\ 0, & 0, & 0, & -3 \\ 1, & 2, & 3, & 1 \\ 0, & -3, & -5, & 0 \end{vmatrix} = -3 \begin{vmatrix} 0, & 0, & 1 \\ 1, & 2, & 3 \\ 0, & -3, & -5 \end{vmatrix} = -3 \begin{vmatrix} 1, & 2 \\ 0, & -3 \end{vmatrix} = 9.$$

Vidíme, že forma f_2 je regulární, přičemž $D_1 = 0, D_2 = 0$ a $D_3 = 0$ vzhledem k tomu, že první dva řádky matice $\boldsymbol{A}_3$ jsou lineárně závislé. Nemůžeme tedy použít větu 13.16 přímo, avšak zkusme přičíst 3. řádek k 1. a 4. řádek ke 2. a poté udělejme obě operace rovněž na sloupce. Postupně dostaneme

$$\begin{pmatrix} 1, & 2, & 4, & 3 \\ 2, & 1, & 3, & 3 \\ 1, & 2, & 3, & 1 \\ 2, & 1, & 1, & 2 \end{pmatrix} \quad \text{a} \quad \begin{pmatrix} 5, & 5, & 4, & 3 \\ 5, & 4, & 3, & 3 \\ 4, & 3, & 3, & 1 \\ 3, & 3, & 1, & 2 \end{pmatrix},$$

přičemž poslední matice je podle věty 12.7 maticí formy f_2 vzhledem k nějaké bázi. Pro tuto matici předně máme $D_4 = |\boldsymbol{A}| = 9$ vzhledem k větě 7.14. Dále je $D_1 = 5, D_2 = -5$ a (nejprve odečteme druhý řádek od prvního a třetí od druhého, pak odečteme třetí sloupec od druhého)

$$D_3 = \begin{vmatrix} 5, & 5, & 4 \\ 5, & 4, & 3 \\ 4, & 3, & 3 \end{vmatrix} = \begin{vmatrix} 0, & 1, & 1 \\ 1, & 1, & 0 \\ 4, & 3, & 3 \end{vmatrix} = \begin{vmatrix} 0, & 0, & 1 \\ 1, & 1, & 0 \\ 4, & 0, & 3 \end{vmatrix} = -4.$$

Celkem tedy máme $D_1 = 5$, $D_1D_2 = -25$, $D_2D_3 = 20$, $D_3D_4 = -36$ a $< 0, 2, 2 >$ je signatura formy f_2.

14. Prostory se skalárním součinem

V celém tomto odstavci bude T značit těleso reálných čísel.

14.1. Definice. *Unitárním prostorem* rozumíme dvojici (V, g), kde V je vektorový prostor a g je pozitivně definitní symetrická bilineární forma na V. Forma g se nazývá *skalární součin* a číslo $g(\boldsymbol{u}, \boldsymbol{v})$ se nazývá *skalární součin vektorů* $\boldsymbol{u}, \boldsymbol{v} \in V$. Jestliže $g(\boldsymbol{u}, \boldsymbol{v}) = 0$, pak říkáme, že vektory $\boldsymbol{u}, \boldsymbol{v}$ jsou navzájem *kolmé (ortogonální)*, a pro tuto skutečnost používáme zápis $\boldsymbol{u} \perp \boldsymbol{v}$. Je-li $\boldsymbol{u} \in V$ a $M \subseteq V$ podmnožina, pak říkáme, že vektor $\boldsymbol{u}$ je *kolmý k množině* M, $\boldsymbol{u} \perp M$, jestliže $\boldsymbol{u} \perp \boldsymbol{v}$ pro každý vektor $\boldsymbol{v} \in M$. Dvě podmnožiny M, N prostoru V jsou k sobě *kolmé*, je-li každý vektor z množiny M kolmý k množině N, tj. když $\boldsymbol{u} \perp \boldsymbol{v}$ pro každé $\boldsymbol{u} \in M$ a každé $\boldsymbol{v} \in N$. Nakonec, je-li $M \subseteq V$ libovolná podmnožina, pak *ortogonálním (kolmým) doplňkem* množiny M rozumíme množinu $M^\perp = \{\boldsymbol{u} \in V | \boldsymbol{u} \perp M\} = \{\boldsymbol{u} \in V \mid g(\boldsymbol{u}, \boldsymbol{v}) = 0 \text{ pro každé } \boldsymbol{v} \in M\}$.

14.2. Poznámka. Pro dva vektory $\boldsymbol{u} = (x_1, x_2, \dots, x_n)$ a $\boldsymbol{v} = (y_1, y_2, \dots, y_n)$ z R^n položme $\omega(\boldsymbol{u}, \boldsymbol{v}) = \sum_{i=1}^n x_i y_i$. Je-li $\boldsymbol{w} = (z_1, z_2, \dots, z_n)$ další prvek z R^n a $r \in R$ libovolné reálné číslo, pak $\omega(\boldsymbol{u}, \boldsymbol{v} + \boldsymbol{w}) = \sum_{i=1}^n x_i(y_i + z_i) = \sum_{i=1}^n x_i y_i + \sum_{i=1}^n x_i z_i = \omega(\boldsymbol{u}, \boldsymbol{v}) + \omega(\boldsymbol{u}, \boldsymbol{w})$, $\omega(\boldsymbol{u}, r\boldsymbol{v}) = \sum_{i=1}^n x_i(r y_i) = r \sum_{i=1}^n x_i y_i = r\omega(\boldsymbol{u}, \boldsymbol{v})$, odkud vzhledem ke zřejmé symetrii $\omega(\boldsymbol{v}, \boldsymbol{u}) = \omega(\boldsymbol{u}, \boldsymbol{v})$ plyne, že ω je symetrická bilineární forma na prostoru R^n. Kromě toho pro každý nenulový vektor $\boldsymbol{u} \in R^n$ je $\omega(\boldsymbol{u}, \boldsymbol{u}) = \sum_{i=1}^n x_i^2 > 0$, takže ω je skalární součin na R^n a (R^n, ω) je unitární prostor.

14.3. Věta. *Buď (V, g) unitární prostor a $M \subseteq V$ libovolná podmnožina. Pak*
(i) $M^\perp \leq V$;
(ii) pro $M \subseteq N \subseteq V$ je $N^\perp \leq M^\perp$;
(iii) $M^\perp = \langle M \rangle^\perp$.

Důkaz. (i) Buďte $\boldsymbol{u}_1, \boldsymbol{u}_2 \in M^\perp$ a $r \in R$ buď libovolné reálné číslo. Pak pro každý vektor $\boldsymbol{v} \in M$ platí $g(\boldsymbol{u}_1 + \boldsymbol{u}_2, \boldsymbol{v}) = g(\boldsymbol{u}_1, \boldsymbol{v}) + g(\boldsymbol{u}_2, \boldsymbol{v}) = 0$, $g(r\boldsymbol{u}_1, \boldsymbol{v}) = rg(\boldsymbol{u}_1, \boldsymbol{v}) = 0$, takže $\boldsymbol{u}_1 + \boldsymbol{u}_2, r\boldsymbol{u}_1 \in M^\perp$ a $M^\perp \leq V$.

(ii) Je-li $\boldsymbol{u} \in N^\perp$, je vektor $\boldsymbol{u}$ kolmý ke každému vektoru $\boldsymbol{v} \in N$. Speciálně je tedy $\boldsymbol{u} \perp M$ a $\boldsymbol{u} \in M^\perp$.

(iii) Ze zřejmé inkluze $M \subseteq \langle M \rangle$ plyne $\langle M \rangle^\perp \subseteq M^\perp$ podle (ii). Na druhé straně, jsou-li $\boldsymbol{u} \in M^\perp$ a $\boldsymbol{v} \in \langle M \rangle$ libovolné vektory, je $\boldsymbol{v} = \sum_{i=1}^n r_i \boldsymbol{v}_i, \boldsymbol{v}_i \in M$, podle věty 1.11, takže $g(\boldsymbol{u}, \boldsymbol{v}) = g(\boldsymbol{u}, \sum_{i=1}^n r_i \boldsymbol{v}_i) = \sum_{i=1}^n r_i g(\boldsymbol{u}, \boldsymbol{v}_i) = 0$, což znamená, že vektor $\boldsymbol{u}$ leží v $\langle M \rangle^\perp$ a věta je dokázána. ■

14.4. Definice. Báze $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ unitárního prostoru (V_n, g) se nazývá *ortogonální báze*, jestliže je polární bází bilineární formy g, tj. je-li $g(\boldsymbol{u}_i, \boldsymbol{u}_j) = 0$ pro všechna $i, j = 1, 2, \dots, n, i \neq j$. Ortogonální báze, pro kterou navíc platí $g_2(\boldsymbol{u}_i) = 1$, $i = 1, 2, \dots, n$, se nazývá *ortonormální báze* unitárního prostoru V_n.

14.5. Poznámka. Předchozí definice jinými slovy říká, že matice skalárního součinu g vzhledem k ortogonální bázi je diagonální a vzhledem k ortonormální bázi dokonce jednotková. Je-li $\boldsymbol{v} \in V_n$ libovolný nenulový vektor, pak položíme-li $\boldsymbol{u} = \frac{\boldsymbol{v}}{\sqrt{g_2(\boldsymbol{v})}}$, dostaneme $g_2(\boldsymbol{u}) = g(\frac{\boldsymbol{v}}{\sqrt{g_2(\boldsymbol{v})}}, \frac{\boldsymbol{v}}{\sqrt{g_2(\boldsymbol{v})}}) = \frac{1}{g_2(\boldsymbol{v})} \cdot g_2(\boldsymbol{v}) = 1$. Vidíme tedy, že pokud máme nějakou ortogonální bázi $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n\}$ unitárního prostoru (V_n, g), pak

„znormováním" jednotlivých prvků báze, tj. přechodem k vektorům $\boldsymbol{u}_i = \frac{\boldsymbol{v}_i}{\sqrt{g_2(\boldsymbol{v}_i)}}$, $i = 1, 2, \ldots, n$, dostaneme ortonormální bázi prostoru (V_n, g). Poznamenejme ještě, že je-li $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ ortonormální báze unitárního prostoru (V_n, g), pak pro $\{\boldsymbol{u}\}_M = (x_1, x_2, \ldots, x_n)$ a $\{\boldsymbol{v}\}_M = (y_1, y_2, \ldots, y_n)$ je $\boldsymbol{u} = \sum_{i=1}^n x_i \boldsymbol{u}_i$, $\boldsymbol{v} = \sum_{j=1}^n y_j \boldsymbol{u}_j$, a tedy $g(\boldsymbol{u}, \boldsymbol{v}) = g(\sum_{i=1}^n x_i \boldsymbol{u}_i, \sum_{j=1}^n y_j \boldsymbol{u}_j) = \sum_{i=1}^n \sum_{j=1}^n x_i y_j g(\boldsymbol{u}_i, \boldsymbol{u}_j)$ $= \sum_{i=1}^n x_i y_i$.

14.6. Věta. *V každém unitárním prostoru (V_n, g) existuje ortonormální báze.*

Důkaz. Podle věty 12.25 existuje ortogonální báze prostoru (V_n, g) a stačí použít předchozí poznámku. ■

14.7. Věta. *Buď (V_n, g) unitární prostor dimenze n. Pak platí*
(i) Je-li $W \leq V_n$ podprostor ve V_n, pak $W^\perp$ je doplněk k W ve V_n;
(ii) je-li $M \subseteq V_n$ podmnožina, pak $\dim M^\perp = n - \dim \langle M \rangle$;
(iii) je-li $M \subseteq V_n$ podmnožina, pak $(M^\perp)^\perp = \langle M \rangle$.

Důkaz. (i) Je-li $\boldsymbol{u} \in W \cap W^\perp$ libovolný vektor, je $g(\boldsymbol{u}, \boldsymbol{u}) = g_2(\boldsymbol{u}) = 0$, takže $W \cap W^\perp = 0$ vzhledem k pozitivní definitnosti skalárního součinu g. Zbývá tedy ukázat, že $W \vee W^\perp = V_n$. Předpokládejme tedy naopak, že existuje vektor $\boldsymbol{u} \in V_n \setminus (W \vee W^\perp)$, a buď $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k\}$ ortonormální báze podprostoru W unitárního prostoru (V_n, g). Položme $\boldsymbol{v} = \boldsymbol{u} - \sum_{i=1}^k r_i \boldsymbol{u}_i$, kde $r_i = g(\boldsymbol{u}, \boldsymbol{u}_i)$, $i = 1, 2, \ldots, k$. Protože $\boldsymbol{u} \notin W \vee W^\perp$, je zřejmé, že $\boldsymbol{v} \notin W \vee W^\perp$, a tedy i $\boldsymbol{v} \notin W^\perp$.

Na druhé straně pro libovolný vektor $\boldsymbol{w} = \sum_{j=1}^k s_j \boldsymbol{u}_j \in W$ je $g(\boldsymbol{v}, \boldsymbol{w}) = g(\boldsymbol{u} - \sum_{i=1}^k r_i \boldsymbol{u}_i, \sum_{j=1}^k s_j \boldsymbol{u}_j) = g(\boldsymbol{u}, \sum_{j=1}^k s_j \boldsymbol{u}_j) - g(\sum_{i=1}^k r_i \boldsymbol{u}_i, \sum_{j=1}^k s_j \boldsymbol{u}_j) = \sum_{j=1}^k s_j$ $g(\boldsymbol{u}, \boldsymbol{u}_j) - \sum_{i=1}^k \sum_{j=1}^k r_i s_j g(\boldsymbol{u}_i, \boldsymbol{u}_j) = \sum_{j=1}^k r_j s_j - \sum_{j=1}^k r_j s_j = 0$. Vidíme tedy, že $\boldsymbol{v} \in W^\perp$, což je spor dokazující tvrzení.

(ii) Plyne ihned z (i) a věty 9.24.

(iii) Protože $\langle M \rangle \perp \langle M \rangle^\perp$, je zřejmě $\langle M \rangle \subseteq \langle M^\perp \rangle^\perp$. Přitom podle (ii) je dim $\langle M^\perp \rangle^\perp = n -$ dim $M^\perp = n - (n - \dim \langle M \rangle) = \dim \langle M \rangle$ a $\langle M \rangle = \langle M^\perp \rangle^\perp$ podle věty 2.22. ■

14.8. Věta. *Buď $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k\}$ libovolná báze podprostoru W unitárního prostoru (V_n, g). Pak existuje ortonormální báze $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k\}$ prostoru W taková, že $\boldsymbol{v}_i \in \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_i \rangle$ pro každé $i = 1, 2, \ldots, k$.*

Důkaz. Budeme postupovat úplnou indukcí podle k. Přitom vzhledem k poznámce 14.5 nám stačí dokázat tvrzení pouze pro ortogonální bázi. Pro $k = 1$ vezmeme $\boldsymbol{v}_1 = \boldsymbol{u}_1$ a $\{\boldsymbol{v}_1\}$ je zřejmě ortogonální bází prostoru W. Buď tedy $k > 1$ a předpokládejme, že existuje ortogonální báze $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{k-1}\}$ podprostoru $\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{k-1} \rangle$ taková, že $\boldsymbol{v}_i \in \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_i \rangle$ pro každé $i = 1, 2, \ldots, k-1$. Položíme-li nyní $\boldsymbol{v}_k = \boldsymbol{u}_k - \sum_{j=1}^{k-1} \frac{g(\boldsymbol{u}_k, \boldsymbol{v}_j)}{g_2(\boldsymbol{v}_j)} \boldsymbol{v}_j$, pak pro každé $i = 1, 2, \ldots, k-1$ je $g(\boldsymbol{v}_k, \boldsymbol{v}_i) = g(\boldsymbol{u}_k - \sum_{j=1}^{k-1} \frac{g(\boldsymbol{u}_k, \boldsymbol{v}_j)}{g_2(\boldsymbol{v}_j)} \boldsymbol{v}_j, \boldsymbol{v}_i) = g(\boldsymbol{u}_k, \boldsymbol{v}_i) - \sum_{j=1}^{k-1} \frac{g(\boldsymbol{u}_k, \boldsymbol{v}_j)}{g_2(\boldsymbol{v}_j)} g(\boldsymbol{v}_j, \boldsymbol{v}_i) = g(\boldsymbol{u}_k, \boldsymbol{v}_i) - g(\boldsymbol{u}_k, \boldsymbol{v}_i) = 0$ a jsme hotovi. ■

14.9. Poznámka. Předchozí věta nám dává metodu pro hledání ortonormálních bází postupným rozšiřováním. Tato metoda je známa buď pod názvem Schmidtův, nebo Grammův–Schmidtův ortogonalizační proces. Připomeňme znovu, že ve smyslu poznámky 14.5 stačí nejprve nalézt ortogonální bázi a z té potom pomocí vhodných násobků vytvořit bázi ortonormální.

14.10. Příklad. V unitárním prostoru (R^4, ω) nalezneme ortonormální bázi podprostoru $W = \langle(1,2,2,-1),(1,1,-5,3),(3,2,8,-7)\rangle$.

Ř e š e n í: Nejprve zjistíme dimenzi podprostoru W. Jest

$$\begin{pmatrix} 1, & 2, & 2, & -1 \\ 1, & 1, & -5, & 3 \\ 3, & 2, & 8, & -7 \end{pmatrix} \sim \begin{pmatrix} 1, & 2, & 2, & -1 \\ 0, & -1, & -7, & 4 \\ 0, & -4, & 2, & -4 \end{pmatrix},$$

odkud je již patrné, že $\dim W = 3$.

Označme $\boldsymbol{u}_1 = (1,2,2,-1), \boldsymbol{u}_2 = (1,1,-5,3)$, $\boldsymbol{u}_3 = (3,2,8,-7)$, položme $\boldsymbol{v}_1 = \boldsymbol{u}_1$ a hledejme $\boldsymbol{v}_2$ ve tvaru $\boldsymbol{u}_2 + r\boldsymbol{v}_1$ tak, aby $\boldsymbol{v}_2 \perp \boldsymbol{v}_1$. Jest $(1+r, 1+2r, -5+2r, 3-r)(1,2,2,-1) = -10+10r = 0$, $r = 1$ a $\boldsymbol{v}_2 = (2,3,-3,2)$. Dále hledáme vektor $\boldsymbol{v}_3$ ve tvaru $\boldsymbol{u}_3 + r\boldsymbol{v}_1 + s\boldsymbol{v}_2$ kolmý jak k $\boldsymbol{v}_1$, tak k $\boldsymbol{v}_2$. Máme tedy $\boldsymbol{v}_3 = (3,2,8,-7) + r(1,2,2,-1) + s(2,3,-3,2)$, $\boldsymbol{v}_3\boldsymbol{v}_1 = 30+10r = 0$, $\boldsymbol{v}_3\boldsymbol{v}_2 = -26+26s = 0$, takže $r = -3$, $s = 1$, $\boldsymbol{v}_3 = (2,-1,-1,-2)$ a $\{(1,2,2,-1),(2,3,-3,2),(2,-1,-1,-2)\}$ je ortogonální báze prostoru W. Podle poznámky 14.5 je tedy $\{\frac{1}{\sqrt{10}}(1,2,2,-1)$, $\frac{1}{\sqrt{26}}(2,3,-3,2)$, $\frac{1}{\sqrt{10}}(2,-1,-1,-2)\}$ ortonormální báze tohoto prostoru.

14.11. Definice. Buďte (V,g) a (V',g') dva unitární prostory. Zobrazení $f : V \to V'$ se nazývá *unitární*, jestliže pro všechna $\boldsymbol{u}, \boldsymbol{v} \in V$ platí $g'(f(\boldsymbol{u}), f(\boldsymbol{v})) = g(\boldsymbol{u}, \boldsymbol{v})$.

14.12. Definice. Buď (V,g) unitární prostor. Pro každý vektor $\boldsymbol{u} \in V$ označme $\|\boldsymbol{u}\|_g = \sqrt{g_2(\boldsymbol{u})}$. Číslo $\|\boldsymbol{u}\|_g$ nazýváme *normou vektoru* $\boldsymbol{u}$ (vzhledem ke skalárnímu součinu g).

14.13. Poznámka. Protože skalární součin g bývá většinou pevně dán, budeme písmeno g zpravidla vynechávat a budeme používat zjednodušené označení $\boldsymbol{uv}$ místo $g(\boldsymbol{u}, \boldsymbol{v})$ a $\|\boldsymbol{u}\|$ místo $\|\boldsymbol{u}\|_g$. Připomeňme, že zobrazení $\varrho : M \times M \to R$, kde M je neprázdná množina, se nazývá *metrika* na M, jestliže

(i) $\varrho(\boldsymbol{u}, \boldsymbol{v}) \geq 0$ pro všechna $\boldsymbol{u}, \boldsymbol{v} \in M$ a $\varrho(\boldsymbol{u}, \boldsymbol{v}) = 0$, právě když $\boldsymbol{u} = \boldsymbol{v}$;

(ii) $\varrho(\boldsymbol{v}, \boldsymbol{u}) = \varrho(\boldsymbol{u}, \boldsymbol{v})$ pro všechna $\boldsymbol{u}, \boldsymbol{v} \in M$;

(iii) $\varrho(\boldsymbol{u}, \boldsymbol{v}) + \varrho(\boldsymbol{v}, \boldsymbol{w}) \geq \varrho(\boldsymbol{u}, \boldsymbol{w})$ pro všechna $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in M$.

Podmínka (iii) se nazývá *trojúhelníková nerovnost* a množina M spolu s metrikou ϱ se nazývá *metrický prostor* a značí se (M, ϱ).

14.14. Věta. *Pro každé dva vektory $\boldsymbol{u}, \boldsymbol{v}$ z unitárního prostoru V platí*

(i) $|\boldsymbol{uv}| \leq \|\boldsymbol{u}\|\|\boldsymbol{v}\|$ (Cauchyho nerovnost);

(ii) $\|\boldsymbol{u} - \boldsymbol{v}\| \leq \|\boldsymbol{u}\| + \|\boldsymbol{v}\|$ (trojúhelníková nerovnost);

(iii) zobrazení $\varrho : V \times V \to R$ definované pro libovolné vektory $\boldsymbol{u}, \boldsymbol{v} \in V$ předpisem $\varrho(\boldsymbol{u}, \boldsymbol{v}) = \|\boldsymbol{u} - \boldsymbol{v}\|$ je metrika na V.

Důkaz. (i) Je-li $\boldsymbol{v}$ nulový vektor, je tvrzení zřejmé. V opačném případě jest $\|\boldsymbol{u} - \frac{(\boldsymbol{uv})}{\|\boldsymbol{v}\|^2}\boldsymbol{v}\|^2 = \|\boldsymbol{u}\|^2 - 2\frac{(\boldsymbol{uv})^2}{\|\boldsymbol{v}\|^2} + \frac{(\boldsymbol{uv})^2}{\|\boldsymbol{v}\|^4}\|\boldsymbol{v}\|^2 = \|\boldsymbol{u}\|^2 - \frac{(\boldsymbol{uv})^2}{\|\boldsymbol{v}\|^2} \geq 0$, odkud tvrzení ihned plyne.

(ii) Podle (i) máme $\|\boldsymbol{u} - \boldsymbol{v}\|^2 = \|\boldsymbol{u}\|^2 - 2\boldsymbol{uv} + \|\boldsymbol{v}\|^2 \leq \|\boldsymbol{u}\|^2 + 2\|\boldsymbol{u}\|\|\boldsymbol{v}\| + \|\boldsymbol{v}\|^2 = (\|\boldsymbol{u}\| + \|\boldsymbol{v}\|)^2$ a $\|\boldsymbol{u} - \boldsymbol{v}\| \leqq \|\boldsymbol{u}\| + \|\boldsymbol{v}\|$.

(iii) Podle (ii) platí $\varrho(\boldsymbol{u},\boldsymbol{v})+\varrho(\boldsymbol{v},\boldsymbol{w}) = \|\boldsymbol{u}-\boldsymbol{v}\|+\|\boldsymbol{v}-\boldsymbol{w}\| = \|\boldsymbol{u}-\boldsymbol{v}\|+\|\boldsymbol{w}-\boldsymbol{v}\| \geq \|\boldsymbol{u}-\boldsymbol{w}\| = \varrho(\boldsymbol{u},\boldsymbol{w})$ a zbytek je zřejmý. ∎

14.15. Definice. Metrika ϱ z předchozí věty definovaná pro $\boldsymbol{u},\boldsymbol{v}\in V$ předpisem $\varrho(\boldsymbol{u},\boldsymbol{v}) = \|\boldsymbol{u}-\boldsymbol{v}\|$, $\boldsymbol{u},\boldsymbol{v}\in V$, se nazývá *metrika indukovaná skalárním součinem.*

14.16. Definice. Buďte (M,ϱ) a (N,σ) dva metrické prostory. Zobrazení $f: M\to N$ množiny M do množiny N se nazývá *izometrie*, jestliže $\sigma(f,(\boldsymbol{u}),f(\boldsymbol{v})) = \varrho(\boldsymbol{u},\boldsymbol{v})$ pro každé dva prvky $\boldsymbol{u},\boldsymbol{v}\in M$.

14.17. Věta. *Buď $f: V\to V'$ unitární zobrazení unitárního prostoru (V,g) do unitárního prostoru (V',g'). Pak*

(i) f je injektivní homomorfismus vektorového prostoru V do vektorového prostoru V';

(ii) f je izometrie metrického prostoru (V,ϱ_g) do vektorového prostoru $(V',\varrho_{g'})$, kde ϱ_g a $\varrho_{g'}$ jsou metriky příslušných prostorů indukované skalárním součinem.

Důkaz. (i) Z definice unitárního zobrazení plyne $g'_2(f(\boldsymbol{u})+f(\boldsymbol{v})) = g'_2(f(\boldsymbol{u})) + 2g'(f(\boldsymbol{u}),f(\boldsymbol{v})) + g'_2(f(\boldsymbol{v})) = g_2(\boldsymbol{u})+2g(\boldsymbol{u},\boldsymbol{v})+g_2(\boldsymbol{v}) = g_2(\boldsymbol{u}+\boldsymbol{v})$ pro libovolné dva vektory $\boldsymbol{u},\boldsymbol{v}\in V$. Dále z $f(\boldsymbol{u}) = f(\boldsymbol{v})$ dostáváme $0 = g'_2(f(\boldsymbol{u})-f(\boldsymbol{v})) = g_2(\boldsymbol{u}-\boldsymbol{v})$ a $\boldsymbol{u}=\boldsymbol{v}$ vzhledem k tomu, že forma g_2 je pozitivně definitní, a f je tedy prosté zobrazení. Nakonec $g'_2(f(\boldsymbol{u}+\boldsymbol{v})-f(\boldsymbol{u})-f(\boldsymbol{v})) = g_2(\boldsymbol{u}+\boldsymbol{v}-\boldsymbol{u}-\boldsymbol{v}) = 0$, $g'_2(f(r\boldsymbol{u})-rf(\boldsymbol{u})) = g'_2(f(r\boldsymbol{u})) - 2rg'(f(r\boldsymbol{u}),f(\boldsymbol{u})) + r^2g'_2(f(\boldsymbol{u})) = g_2(r\boldsymbol{u}) - 2rg(r\boldsymbol{u},\boldsymbol{u}) + r^2g_2(\boldsymbol{u}) = 0$, a tedy $f(\boldsymbol{u}+\boldsymbol{v}) = f(\boldsymbol{u})+f(\boldsymbol{v})$, $f(r\boldsymbol{u}) = rf(\boldsymbol{u})$ a f je homomorfismus.

(ii) Pro libovolné dva vektory $\boldsymbol{u},\boldsymbol{v}$ z V zde máme $\varrho_{g'}(f(\boldsymbol{u}),f(\boldsymbol{v})) = \|f(\boldsymbol{u})-f(\boldsymbol{v})\|_{g'} = \sqrt{g'_2(f(\boldsymbol{u})-f(\boldsymbol{v}))} = \sqrt{g_2(\boldsymbol{u}-\boldsymbol{v})} = \|\boldsymbol{u}-\boldsymbol{v}\|_g = \varrho_g(\boldsymbol{u},\boldsymbol{v})$ podle důkazu části (i). ∎

14.18. Věta. *Buď M ortonormální báze unitárního prostoru (V_n,g). Pak zobrazení $\varphi: V_n\to R^n$ definované pro každé $\boldsymbol{u}\in V_n$ předpisem $\varphi(\boldsymbol{u}) = \{\boldsymbol{u}\}_M$ je unitární zobrazení unitárního prostoru (V_n,g) na unitární prostor (R^n,ω), a tedy izometrie metrického prostoru (V_n,ϱ_g) na metrický prostor (R^n,ϱ_ω). Speciálně je tedy každý unitární prostor izometrický s unitárním prostorem (R^n,ω).*

Důkaz. Vzhledem k předchozí větě stačí ověřit, že φ je unitární zobrazení. Nechť tedy $\boldsymbol{u},\boldsymbol{v}\in V_n$ jsou libovolné prvky, $\{\boldsymbol{u}\}_M = (x_1,x_2,\dots,x_n)$, $\{\boldsymbol{v}\}_M = (y_1,y_2,\dots,y_n)$ jejich souřadnice vzhledem k ortonormální bázi M. Pak ale $\omega(\varphi(\boldsymbol{u}),\varphi(\boldsymbol{v})) = \omega((x_1,\ x_2,\ \dots,x_n),\ (y_1,y_2,\dots,y_n)) = \sum_{i=1}^n x_iy_i = g(\boldsymbol{u},\boldsymbol{v})$ a věta je dokázána, neboť zbytek tvrzení je zřejmý. ∎

14.19. Poznámka. Poznamenejme předně, že poslední věta předchozího tvrzení znamená, že existuje izometrie metrického prostoru (V_n,ϱ_g) na metrický prostor (R^n,ϱ_ω) s příslušnými indukovanými metrikami. Dále si ve smyslu poznámky 14.5 připomeňme, že je-li $M = \{\boldsymbol{u}_1,\boldsymbol{u}_2,\dots,\boldsymbol{u}_n\}$ ortonormální báze unitárního prostoru V a $\boldsymbol{u},\boldsymbol{v}\in V$ jsou vektory takové, že $\{\boldsymbol{u}\}_M = (x_1,x_2,\dots,x_n)$ a $\{\boldsymbol{v}\}_M = (y_1,y_2,\dots,y_n)$, pak $\|\boldsymbol{u}\| = \sqrt{\boldsymbol{u}\boldsymbol{u}} = \sqrt{\sum_{i=1}^n x_i^2}$ a tedy $\varrho(\boldsymbol{u},\boldsymbol{v}) = \|\boldsymbol{u}-\boldsymbol{v}\| = \sqrt{\sum_{i=1}^n (x_i-y_i)^2}$.

15.1. Definice. Buď $\boldsymbol{A} = (a_{ij}) \in T_n$ čtvercová matice stupně n nad tělesem T. Polynom $f(\lambda) = \det(\boldsymbol{A} - \lambda\boldsymbol{E})$ se nazývá *charakteristický polynom matice* $\boldsymbol{A}$. Prvek $\lambda \in T$ takový, že $\det(\boldsymbol{A} - \lambda\boldsymbol{E}) = 0$ se nazývá *vlastní hodnota* matice $\boldsymbol{A}$. V případě, že T je číselné těleso (např. těleso racionálních, reálných, komplexních čísel), pak místo vlastní hodnota obvykle říkáme *vlastní číslo*. Říkáme dále, že nenulový vektor $\boldsymbol{u} \in T^n$ je *vlastní vektor* matice $\boldsymbol{A}$ příslušný vlastní hodnotě λ, jestliže $\boldsymbol{A}\boldsymbol{u}^T = \lambda\boldsymbol{u}^T$.

15.2. Poznámka. Buď $\boldsymbol{A} = (a_{ij}) \in T_n$ čtvercová matice stupně n nad tělesem T a buď $\boldsymbol{u} = (x_1, x_2, \ldots, x_n)$ vlastní vektor matice $\boldsymbol{A}$ příslušný vlastní hodnotě λ. To znamená, že platí rovnost $\boldsymbol{A}\boldsymbol{u}^T = \lambda\boldsymbol{u}^T$, což rozepsáno ve složkách znamená

$$\begin{array}{ccccccccc}
(a_{11}-\lambda)x_1 & + & a_{12}x_2 & + & \ldots & + & a_{1n}x_n & = & 0, \\
a_{21}x_1 & + & (a_{22}-\lambda)x_2 & + & \ldots & + & a_{2n}x_n & = & 0, \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
a_{n1}x_1 & + & a_{n2}x_2 & + & \ldots & + & (a_{nn}-\lambda)x_n & = & 0.
\end{array}$$

Vidíme tedy, že vlastní vektor $\boldsymbol{u}$ je řešením homogenní soustavy lineárních rovnic s maticí $\boldsymbol{A} - \lambda\boldsymbol{E}$. Uvědomme si, že tato soustava má podle důsledku 5.9 a věty 8.4 netriviální řešení, právě když $\det(\boldsymbol{A} - \lambda\boldsymbol{E}) = 0$, tj. právě když λ je vlastní hodnota matice $\boldsymbol{A}$.

15.3. Důsledek. *Buď $\boldsymbol{A} = (a_{ij}) \in T_n$ čtvercová matice stupně n nad tělesem T. Pak $\boldsymbol{u} = (x_1, x_2, \ldots, x_n)$ je vlastní vektor matice $\boldsymbol{A}$ příslušný vlastní hodnotě λ, právě když pro každé $j = 1, 2, \ldots, n$ platí $\sum_{i=1}^{n} a_{ji}x_i = \lambda x_j$.*

Důkaz. Dokazovaná rovnost neříká nic jiného, než j-tá rovnice homogenní soustavy lineárních rovnic z předchozí poznámky. ∎

15.4. Definice. Říkáme, že dvě čtvercové matice $\boldsymbol{A}, \boldsymbol{B}$ stupně n nad tělesem T jsou *podobné*, jestliže existuje regulární čtvercová matice $\boldsymbol{C}$ stupně n nad tělesem T taková, že $\boldsymbol{B} = \boldsymbol{C}^{-1}\boldsymbol{A}\boldsymbol{C}$.

15.5. Věta. *Relace podobnosti matic je ekvivalence na množině všech čtvercových matic stupněm nad tělesem T.*

Důkaz. Lze přenechat čtenáři jako snadné cvičení. ∎

15.6. Věta. *Buď $\boldsymbol{A} \in T_n$ čtvercová matice stupně n nad tělesem T a buď $\boldsymbol{C} \in T_n$ regulární. Pak*

(i) matice $\boldsymbol{B} = \boldsymbol{C}^{-1}\boldsymbol{A}\boldsymbol{C}$ podobná matici $\boldsymbol{A}$ má stejný charakteristický polynom jako matice $\boldsymbol{A}$;

(ii) matice $\boldsymbol{B}$ má stejné vlastní hodnoty jako matice $\boldsymbol{A}$;

(iii) Je-li $\boldsymbol{u} \in V_n$ vlastní vektor matice $\boldsymbol{A}$ příslušný vlastní hodnotě λ, pak $\boldsymbol{u}(\boldsymbol{C}^T)^{-1}$ je vlastní vektor matice $\boldsymbol{B}$ příslušný λ.

Důkaz. (i) Věta o násobení determinantů 7.21 dává $\det(\boldsymbol{B} - \lambda\boldsymbol{E}) = \det(\boldsymbol{C}^{-1}\boldsymbol{A}\boldsymbol{C} - \lambda\boldsymbol{E}) = \det\boldsymbol{C}^{-1}\det(\boldsymbol{A} - \lambda\boldsymbol{E})\det\boldsymbol{C} = \det(\boldsymbol{A} - \lambda\boldsymbol{E})$.

(ii) Plyne ihned z (i).

(iii) Podle důsledku 15.3, vět 8.6 a 4.14 jest $\boldsymbol{B}(\boldsymbol{u}(\boldsymbol{C}^T)^{-1})^T = \boldsymbol{C}^{-1}\boldsymbol{A}\boldsymbol{C}(\boldsymbol{C}^{-1}\boldsymbol{u}^T) = \boldsymbol{C}^{-1}\boldsymbol{A}\boldsymbol{u}^T = \boldsymbol{C}^{-1}\lambda\boldsymbol{u}^T = \lambda(\boldsymbol{u}(\boldsymbol{C}^T)^{-1})^T$ a stačí znovu použít důsledek 15.3. ∎

15.7. Poznámka. Buď M báze vektorového prostoru V_n a buď $\boldsymbol{A}$ matice endomorfismu f prostoru V_n vzhledem k bázi M. Je-li $\boldsymbol{C}$ matice přechodu od báze M k bázi M', je podle věty 10.17 matice $\boldsymbol{B} = \boldsymbol{C}^{-1}\boldsymbol{A}\boldsymbol{C}$ maticí homomorfismu f vzhledem k bázi M'. S ohledem na větu 10.16 tedy vidíme, že množina matic daného endomorfismu f prostoru V_n je právě jedna třída ekvivalence podobnosti matic. Podle věty 15.6 mají všechny tyto matice stejné vlastní hodnoty.

15.8. Definice. Buď f endomorfismus vektorového prostoru V_n. Jestliže pro nějaké $\boldsymbol{u} \in V_n$ a nějaké $\lambda \in T$ je $f(\boldsymbol{u}) = \lambda\boldsymbol{u}$, pak říkáme, že λ je *vlastní hodnota endomorfismu* f a $\boldsymbol{u}$ je *vlastní vektor endomorfismu* f příslušný vlastní hodnotě λ.

15.9. Věta. *Buď M báze vektorového prostoru V_n a buď $\boldsymbol{A}$ matice endomorfismu f vzhledem k bázi M. Pak*

(i) prvek $\lambda \in T$ je vlastní hodnotou endomorfismu f, právě když λ je vlastní hodnotou matice $\boldsymbol{A}$;

(ii) vektor $\boldsymbol{u} \in V_n$ je vlastním vektorem endomorfismu f příslušným vlastní hodnotě λ, právě když $\{\boldsymbol{u}\}_M$ je vlastním vektorem matice $\boldsymbol{A}$ příslušným λ.

Důkaz. Nechť $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ je báze prostoru V_n a nechť $\{\boldsymbol{u}\}_M = (x_1, x_2, \dots, x_n)$ jsou souřadnice vektoru $\boldsymbol{u}$ vzhledem k bázi M. Podle předpokladu je $f(\boldsymbol{u}_i) = \sum_{j=1}^n a_{ji}\boldsymbol{u}_j$ pro každé $i = 1, 2, \dots, n$ a $\boldsymbol{u} = \sum_{i=1}^n x_i\boldsymbol{u}_i$. Pak ale $f(\boldsymbol{u}) = \lambda\boldsymbol{u}$, právě když $f(\boldsymbol{u}) = f(\sum_{i=1}^n x_i\boldsymbol{u}_i) = \sum_{i=1}^n x_i f(\boldsymbol{u}_i) = \sum_{i=1}^n x_i \sum_{j=1}^n a_{ji}\boldsymbol{u}_j = \sum_{j=1}^n(\sum_{i=1} a_{ji}x_i)\boldsymbol{u}_j = \lambda\sum_{j=1}^n(x_j\boldsymbol{u}_j)$, což je ekvivalentní s tím, že $\sum_{i=1}^n a_{ji}x_i = \lambda x_j$ pro každé $j = 1, 2, \dots, n$, odkud obě tvrzení plynou podle důsledku 15.3. ■

15.10. Věta. *Buď $\boldsymbol{A}$ čtvercová matice stupně n nad tělesem reálných čísel. Je-li $\boldsymbol{A}$ symetrická, jsou všechna její vlastní čísla reálná.*

Důkaz. Nechť komplexní číslo λ je vlastní číslo matice $\boldsymbol{A}$ a buď $\boldsymbol{u} = (x_1, x_2, \dots, x_n)$ nějaké komplexní netriviální řešení homogenní soustavy lineárních rovnic z poznámky 15.2. Pak podle důsledku 15.3. máme jednak $\lambda\sum_{j=1}^n x_j\overline{x_j} = \sum_{j=1}\overline{x_j}\sum_{i=1}^n a_{ji}x_i = \sum_{j=1}^n\sum_{i=1}^n a_{ji}x_i\overline{x_j}$, jednak $\overline{\lambda}\sum_{j=1}^n x_j\overline{x_j} = \sum_{j=1}^n x_j\overline{\sum_{i=1}^n a_{ji}x_i} = \sum_{j=1}^n\sum_{i=1}^n a_{ji}\overline{x_i}x_j$, odkud dostáváme $(\lambda - \overline{\lambda})\sum_{j=1}^n x_j\overline{x_j} = 0$ vzhledem k tomu, že matice $\boldsymbol{A}$ je symetrická. Protože vektor $\boldsymbol{u}$ je nenulový, je $\sum_{j=1}^n x_j\overline{x_j} > 0$, takže $\lambda = \overline{\lambda}$ je reálné číslo a jsme hotovi. ■

Začneme tím, že si shrneme některé základní algebraické pojmy, které v té či oné formě již znáte z dřívějška. Tak *binární operací* na neprázdné množině M rozumíme každé zobrazení $\omega : M \times M \to M$, tj. předpis, který každé uspořádáné dvojici (a, b) prvků množiny M jednoznačně přiřazuje prvek $\omega(a, b) \in M$. Místo symbolu $\omega(a, b)$ se v praxi užívá zejména $a \cdot b = ab$, tzv.*multiplikativní zápis*, $a + b$, tzv. *aditivní zápis*, případně další, $a \circ b, a * b$ apod.

16.1. Definice. Neprázdná množina G spolu s operací násobení $\cdot$ se nazývá *grupoid*. *Pologrupa* je grupoid splňující *asociativní zákon*, tj. rovnost $a(bc) = (ab)c$ pro každé tři prvky $a, b, c, \in G$. Jestliže existuje prvek $1 \in G$ takový, že $1a = a1 = a$ pro každé $a \in G$, pak říkáme, že 1 je *jednotkový prvek* grupoidu G a pologrupa s jednotkovým prvkem se nazývá *monoid.* Konečně *grupou* rozumíme monoid, v němž ke každému prvku existuje *prvek inverzní*, tj. ke každému $a \in G$ existuje $a^{-1} \in G$ tak, že $aa^{-1} = a^{-1}a = 1$. *Komutativní grupoid* je grupoid, v němž pro každé dva prvky $a, b \in G$ platí $ab = ba$. Podobně se definuje komutativní pologrupa, monoid, grupa.

16.2.Poznámka. Pro komutativní grupu se též používá název Abelova grupa a zpravidla se volí *aditivní zápis* $(G, +)$. V tomto případě pak hovoříme o *nulovém prvku* 0 místo prvku jednotkového a o *prvku opačném* $-a$ místo prvku inverzního a^{-1}.

Nyní můžeme přejít ke stručnému přehledu algebraických struktur se dvěma binárními operacemi.

16.3. Definice. *Okruhem* $(R, +, \cdot)$ rozumíme neprázdnou množinu R spolu se dvěma binárními operacemi sčítání $+$ a násobení $\cdot$ takovou, že $(R, +)$ je Abelova grupa, $(R, \cdot)$ je monoid a jsou splněny tzv. *distributivní zákony*, tj. pro každé tři prvky $a, b, c \in R$ platí $a(b + c) = ab + ac$ a $(b + c)a = ba + ca$. Je-li navíc monoid $(R, \cdot)$ komutativní, pak hovoříme o *komutativním okruhu*. Komutativní okruh bez *dělitelů nuly*, tj. takový, že z rovnosti $ab = 0$ plyne buď $a = 0$, nebo $b = 0$, se nazývá *obor integrity*. Komutativní okruh s alespoň dvěma prvky, v němž ke každému nenulovému prvku a existuje prvek inverzní a^{-1} (tj. $(R \setminus \{0\}, \cdot)$ je Abelova grupa), se nazývá *těleso*. V literatuře se zpravidla v definici tělesa nepožaduje platnost komutativního zákona pro násobení a těleso, ve kterém tento zákon platí, se pak nazývá *komutativní těleso*. Protože zde budeme pracovat výhradně s komutativními tělesy, zavedli jsme tento pojem tak, abychom mohli pro stručnost hovořit pouze o tělese.

16.4. Definice. Buď R okruh a x neurčitá (tj. nějaký nový symbol). *Okruhem $R[x]$ polynomů jedné neurčité x nad okruhem R* rozumíme množinu $R[x]$ všech polynomů $f(x) = \sum_{i=0}^{n} a_i x^i$, kde $a_i \in R, i = 0, 1, \ldots, n$, jsou koeficienty polynomu f a kde klademe $x^0 = 1$, spolu s operacemi sčítání a násobení definovanými obvyklým způsobem pro $f(x) = \sum_{i=0}^{n} a_i x^i$ a $g(x) = \sum_{j=0}^{m} b_i x^i$ takto: $f(x) + g(x) = \sum_{i=0}^{t}(a_i + b_i)x^i$, kde $t = \max\,(n, m)$ a kde klademe $a_j = 0$ pro $j > n$ a $b_j = 0$ pro $j > m$, a $f(x)g(x) = \sum_{i=0}^{n+m} c_i x^i$, kde $c_i = \sum_{r+s=i} a_r b_s$ při platnosti předchozí úmluvy o nulovosti koeficientů s vyššími indexy. Polynom $f(x)$, jehož všechny koeficienty jsou rovny nule, se nazývá *nulový* a polynom $0 \neq f(x) = \sum_{i=0}^{n} a_i x^i$ je *stupně* n, st $f(x) = n$, je-li $a_n \neq 0$. Nulovému polynomu se často nepřiřazuje žádný stupeň, pro naše účely však bude výhodné položit st $0 = -1$.

16.5. Úmluva. Vzhledem k tomu, že v dalším textu budeme pracovat s celou řadou polynomů, domluvme se, že pro větší přehlednost budeme používat pro polynomy zkráceného zápisu f, g atd., namísto $f(x), g(x)$ atd.

16.6. Věta. *Je-li R obor integrity, pak okruh polynomů $R[x]$ je rovněž oborem integrity. V tomto případě je* $\operatorname{st} fg = \operatorname{st} f + \operatorname{st} g$, *kdykoliv* $f \neq 0 \neq g$.

Důkaz. Potřebujeme ověřit, že součin dvou polynomů je opět nenulový polynom. Buď tedy $f = \sum_{i=0}^{n} a_i x^i, a_n \neq 0$ a $g = \sum_{i=0}^{m} b_i x^i, b_m \neq 0$. Pak pro $h = fg = \sum_{i=0}^{n+m} c_i x^i$ je $c_{n+m} = a_n b_m \neq 0$ a věta je dokázána. ∎

16.7. Věta. *Buď T těleso a buďte $f, g, \in T$ dva polynomy, $f \neq 0$. Pak existují jednoznačně určené polynomy $q, r \in T$ takové, že $g = fq + r$, přičemž* $\operatorname{st} r < \operatorname{st} f$.

Důkaz. Dokažme nejprve existenci uvedených polynomů. Je-li $\operatorname{st} g < \operatorname{st} f$, pak stačí položit $q = 0$ a $r = g$. V opačném případě položme $s = \operatorname{st} g - \operatorname{st} f \geq 0$ a postupujme úplnou indukcí podle s. Nechť tedy $f = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$, $g = \sum_{i=0}^{m} b_i x^i, b_m \neq 0$, a buď nejprve $s = 0$. V tomto případě stačí položit $q = b_n a_n^{-1}, r = g - fq$ a ověřit, že $\operatorname{st} r < \operatorname{st} f$. Protože $\operatorname{st} q = 0$, je $\operatorname{st}(fq) = \operatorname{st} f = n = \operatorname{st} g$ podle předchozí věty, tedy $\operatorname{st} r \leq n$ a stačí ukázat, že koeficient u x^n v polynomu r je roven nule. Avšak tento koeficient je roven $b_n - a_n b_n a_n^{-1} = 0$ a můžeme přejít k indukčnímu kroku. Buď tedy $s > 0$ a předpokládejme, že pro každé $0 \leq t < s$ již tvrzení platí. Položíme-li $q_1 = b_m a_n^{-1} x^s$, pak polynom $g_1 = g - fq_1$ je stupně menšího než m, neboť koeficient u x^m je roven $b_m - a_n b_m a_n^{-1} = 0$. Použitím indukčního předpokladu na polynomy g_1 a f dostaneme existenci polynomů q_2, r takových, že $g_1 = fq_2 + r$, kde $\operatorname{st} r < \operatorname{st} f$. Pak ale dosazením dostaneme $g = g_1 + fq_1 = f(q_1 + q_2) + r$ a jsme hotovi.

Přejděme k důkazu jednoznačnosti. Nechť tedy $g = fq_1 + r_1$ a $g = fq_2 + r_2$, kde $\operatorname{st} r_1, \operatorname{st} r_2 < \operatorname{st} f$. Odečtením dostaneme rovnost $f(q_1 - q_2) = r_2 - r_1$. Je-li nyní $q_1 - q_2 \neq 0$, je na levé straně polynom stupně alespoň $n = \operatorname{st} f$, zatímco na pravé straně je polynom stupně ostře menšího než n. Získaný spor dokazuje rovnost $q_1 = q_2$, a tedy i $r_1 = r_2$ a věta je dokázána. ∎

16.8. Definice. Buď T těleso a buďte $f, g \in T[x]$ dva polynomy nad T. Říkáme, že *polynom f dělí polynom g*, $f|g$, jestliže existuje polynom $h \in T[x]$ takový, že $g = fh$. Dále říkáme, že polynom f je *ireducibilní*, jestliže $\operatorname{st} f \geq 1$ a jestliže $g|f$, pak buď $\operatorname{st} g = 0$, nebo $\operatorname{st} g = \operatorname{st} f$. Polynom $f = \sum_{i=0}^{n} a_i x^i$ se nazývá *normovaný*, jestliže $a_n = 1$.

16.9. Věta. *Nechť f, g jsou dva polynomy z $T[x]$ takové, že f je ireducibilní a nedělí g. Pak existují polynomy $\alpha, \beta \in T[x]$ tak, že $f\alpha + g\beta = 1$.*

Důkaz. V množině $M = \{f\alpha + g\beta \mid \alpha, \beta \in T[x]\}$ vezměme nenulový polynom $h = f\alpha + g\beta$ nejmenšího možného nezáporného stupně. Ukažme nejprve, že polynom h dělí jak polynom f, tak i g. Podle věty 16.6 existují polynomy $q, r \in T[x]$ takové, že $f = hq + r$, kde $\operatorname{st} r < \operatorname{st} h$. Pak ale $r = f - hq = f - (f\alpha + g\beta)q = f(1 - \alpha q) + g\beta q \in M$, což je pro $r \neq 0$ spor s volbou polynomu h, neboť $r \in M$ je menšího stupně než h. Podobně pro $g = hq + r$, $\operatorname{st} r < \operatorname{st} h$ máme $r = g - hq = g - (f\alpha + g\beta)q = f(-\alpha q) + g(1 - \beta q) \in M$, což jest opět pro $r \neq 0$ spor s volbou polynomu h. Protože f je ireducibilní a $h|f$, je vzhledem k větě 16.6 buď $h = af$ pro nějaké $0 \neq a \in T$, nebo $0 \neq h = a \in T$. V prvém případě dostáváme z $h|g$ rovnost $g = hk$ pro nějaké

$k \in T[x]$, odkud $g = afk$, a tedy $f|g$, což jest spor s předpokladem věty. Vidíme tedy, že $h = a \in T$, takže $1 = a^{-1}h = a^{-1}(f\alpha + g\beta) = f(\alpha a^{-1}) + g(\beta a^{-1})$ a jsme hotovi. ■

16.10. Lemma. *Nechť $f, f_1, \dots, f_r$ jsou normované ireducibilní polynomy z $T[x]$. Jestliže $f|f_1f_2\dots, f_r$, pak existuje index $i \in \{1, 2, \dots, r\}$ tak, že $f = f_i$.*

Důkaz. Ukažme nejprve, že pokud polynom f dělí součin polynomů gh, $gh = fk$ pro nějaké $k \in T[x]$, pak f dělí buď g, nebo h. Předpokládejme tedy, že f nedělí g. Podle předchozí věty 16.9 existují polynomy $\alpha, \beta \in T[x]$ takové, že $f\alpha + g\beta = 1$. Pak ale $h = (f\alpha + g\beta)h = f\alpha h + f\beta k = f(\alpha h + \beta k)$ a $f|h$. Nyní se již důkaz snadno dokončí úplnou indukcí podle r. Pro $r = 1$ je $f = f_1$. Buď tedy $r > 1$. Protože $f|(f_1 \dots, f_{r-1})f_r$ platí podle první části důkazu buď $f|f_1, \dots, f_{r-1}$, nebo $f|f_r$. V prvém případě existuje podle indukčního předpokladu index $i \in \{1, 2, \dots, r-1\}$ takový, že $f = f_i$, ve druhém případě je $f_r = fa$, kde $a \in T$ podle definice ireducibilního polynomu 16.8. Protože f a f_r jsou normované, je nutně $a = 1$ a jsme hotovi. ■

16.11. Věta. *Buď T těleso a buď $f \in T[x]$ polynom kladného stupně. Pak polynom f lze rozložit na součin $f = af_1^{k_1}f_2^{k_2}\dots f_r^{k_r}$, kde $a \in T$, $f_1, f_2, \dots, f_r$ jsou navzájem různé normované ireducibilní polynomy z $T[x]$ a $k_1, k_2, \dots, k_r$ jsou kladná celá čísla. Prvek $a \in T$ a polynomy $f_1, f_2, \dots, f_r$ jsou přitom polynomem f určeny jednoznačně.*

Důkaz. Vzhledem k tomu, že každý nenulový polynom $f = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$, lze napsat ve tvaru $f = a_n f_1$, kde polynom $f_1 = \sum_{i=0}^{n} a_n^{-1} a_i x^i$ je normovaný, můžeme bez újmy na obecnosti předpokládat, že všechny polynomy v tomto důkaze jsou normované. Začneme s důkazem existence daného rozkladu. Ukažme nejprve, že polynom f je dělitelný alespoň jedním ireducibilním polynomem. Jestliže f není ireducibilní, pak $f = f_1 g_1$, kde f_1 je polynom takový, že $0 < \operatorname{st} f_1 < \operatorname{st} f$. Předpokládejme, že polynom f_1 v tomto rozkladu má nejmenší možný stupeň, tj. kdykoliv je $f = f_2 g_2$, pak $\operatorname{st} f_1 \leq \operatorname{st} f_2$. Nyní je patrné, že polynom f_1 je ireducibilní, neboť v opačném případě můžeme f_1 rozložit na součin $f_1 = f_2 g_2$, kde $0 < \operatorname{st} f_2 < \operatorname{st} f_1$. Pak ale $f = f_1 g_1 = f_2(g_2 g_1)$, kde $\operatorname{st} f_2 < \operatorname{st} f_1$, což je spor s volbou polynomu f_1. Nyní se již důkaz snadno dokončí úplnou indukcí podle stupně n polynomu f. Pro $n = 1$ plyne ireducibilita polynomu f ihned z věty 16.6. Pro $n > 1$ je buď f ireducibilní, nebo jej lze podle první části důkazu rozložit v součin $f = f_1 g$, kde f_1 je ireducibilní polynom. Podle věty 16.6. je $\operatorname{st} g < n$, takže podle indukčního předpokladu lze g rozložit na součin ireducibilních polynomů, odkud existence rozkladu již snadno plyne.

Přejděme k důkazu jednoznačnosti. Nechť tedy $f = af_1f_2\dots f_k = bg_1g_2\dots g_l$, $a, b \in T$, jsou dva rozklady polynomu f na součin normovaných ireducibilních polynomů, budeme postupovat indukcí podle k. Předně je patrné, že $a = b$, můžeme tedy předpokládat, že $a = b = 1$. Pro $k = 1$ je f ireducibilní, a tedy $f = f_1 = g_1$. Buď tedy $k > 1$. Pak $f_k|g_1g_2\dots g_l$, takže podle lemmatu 16.10 je $f_k = g_i$ pro nějaké $i \in \{1, 2, \dots, l\}$. Vzhledem ke komutativitě násobení můžeme bez újmy předpokládat, že $i = l$, tedy $f_k = g_l$. Po zkrácení polynomem f_k dostaneme rovnost $f_1\dots f_{k-1} = g_1\dots g_{l-1}$. Podle indukčního předpokladu je tedy $k - 1 = l - 1$ a při vhodném očíslování prvků $g_1, g_2, \dots, g_{k-1}$ je $f_i = g_i$ pro každé $i = 1, 2, \dots, k-1$. Protože také $f_k = g_k$, je důkaz dokončen. ∎

16.12. Věta. *Buď $f \in T[x]$ polynom kladného stupně, $f = af_1^{k_1} f_2^{k_2} \dots f_r^{k_r}, a \in T$, kde $f_i \in T[x]$ jsou navzájem různé normované ireducibilní polynomy a k_i jsou celá kladná čísla, $i = 1, 2, \dots, r$. Označíme-li pro každé $i = 1, 2, \dots, r$ symbolem $\bar{f}_i$ součin všech $f_j^{k_j}$ s výjimkou $f_i^{k_i}$, je $f = f_i^{k_i} \bar{f}_i$ a platí*

(i) pro každé $i = 1, 2, \dots, r$ existují polynomy $\beta_i, \gamma_i \in T[x]$ takové, že $f_i^{k_i}\beta_i + \bar{f}_i\gamma_i = 1$;

(ii) existují prvky $\alpha_1, \alpha_2, \dots, \alpha_r \in T[x]$ takové, že $\bar{f}_1\alpha_1 + \bar{f}_2\alpha_2 + \dots + \bar{f}_r\alpha_r = 1$.

Důkaz. (i) Zřejmě můžeme předpokládat, že polynom f je normovaný, tj. že $a = 1$. Podobně jako v důkazu věty 16.9 vyšetřujme množinu $M_i = \{f_i^{k_i}\alpha + \bar{f}^i\beta \mid \alpha, \beta \in T[x]\}$ pro libovolné $i \in \{1, 2, \dots, r\}$. Buď $h_i = f_i^{k_i}\beta_i + \bar{f}_i\gamma_i$ normovaný polynom z M_i nejmenšího možného nezáporného stupně. Stejným způsobem jako v důkazu věty 16.9 se ukáže, že h_i dělí jak $f_i^{k_i}$, tak $\bar{f}_i$. Pak ale nutně buď $h_i = f_i$, nebo $h_i = 1$. Avšak pro $h_i = f_i$ máme $f_i | \bar{f}_i$, podle lemmatu 16.10 tedy $f_i = f_j$ pro nějaké $j \neq i$, což podle předpokladu není možné.

(ii) Toto tvrzení se dokáže podobně jako předchozí. Vezmeme polynom $h = \bar{f}_1\alpha_1 + \bar{f}_2\alpha_2 + \dots + \bar{f}_r\alpha_r$ nejmenšího možného nezáporného stupně v množině všech polynomů tvaru $\sum_{i=1}^r \bar{f}_i\beta_i$ a ukážeme, že $h | \bar{f}_i$ pro každé $i = 1, 2, \dots, r$. To však znamená, že buďto $h = 1$, nebo je h rovno podle lemmatu 16.10 některému z polynomů $f_1, f_2, \dots, f_r$, řekněme $h = f_i$. To však vzhledem k tomu, že $h | \bar{f}_i$, není zřejmě možné. ∎

16.13. Poznámka. Připomeňme si na tomto místě některá fakta týkající se pojmu vektorového prostoru. Jak víme z definice 1.1 a z poznámky 1.2, vektorový prostor je Abelova grupa $(V, +)$, na které je definováno násobení vektorů prvky z tělesa T tak, že jsou splněny podmínky 4.–7. Jak víme z definice 16.3, těleso je velmi speciálním případem okruhu, přičemž žádné speciální vlastnosti tělesa nejsou v definici vektorového prostoru využity. To nás vede k zavedení následujícího pojmu.

16.14. Definice. Buď R libovolný okruh. *Levým modulem M nad okruhem R*, nebo *levým R-modulem* rozumíme Abelovu grupu $(M, +)$, na níž je definováno násobení zleva prvky z okruhu R (tj. každému prvku $u \in M$ a každému $r \in R$ je jednoznačně přiřazen prvek $ru \in M$) tak, že pro všechna $u, v \in M$ a všechna $r, s \in R$ platí

$$r(u+v) = ru + rv, \qquad (r+s)u = ru + su,$$
$$r(su) = (rs)u, \qquad 1u = u.$$

16.15. Definice. Neprázdná podmnožina K R-modulu M se nazývá *podmodul*, jestliže pro všechna $u, v \in K$ je $u + v \in K$ a pro všechna $u \in K$ a všechna $r \in R$ je $ru \in K$. Říkáme, že modul M je *direktním součtem svých podmodulů* $M_1, M_2, \dots, M_k$, jestliže každý prvek $u \in M$ lze jednoznačně zapsat ve tvaru $u = u_1 + u_2 + \dots + u_k$, kde $u_i \in M_i, i = 1, 2, \dots, k$. Pro direktní součet používáme označení $M = M_1 \oplus M_2 \oplus \dots \oplus M_k = \oplus_{i=1}^k M_i$.

16.16. Poznámka. Stejným způsobem jako ve větě 1.8 lze dokázat, že průnik libovolného neprázdného systému podmodulů modulu M je opět podmodul v M.

To nám umožňuje definovat podmodul $\langle M \rangle$ generovaný množinou M stejně jako v definici 1.9 a spojení či součet podmodulů $\vee_{i=1}^k M_i = \sum_{i=1}^k M_i$ jako podmodul generovaný množinou $\cup_{i=1}^k M_i$. Stejně jako v poznámce 1.14 lze ukázat, že $\sum_{i=1}^k M_i = \{\sum_{i=1}^k u_i \mid u_i \in M_i, i = 1, 2, \dots, k\}$.

16.17. Věta. *Modul M je direktním součtem svých podmodulů $M_1, M_2, \dots, M_k$, $M = \oplus_{i=1}^k M_i$, právě když $M = \sum_{i=1}^k M_i$ a $M_i \cap \sum_{j \neq i} M_j = 0$ pro každé $i = 1, 2, \dots, k$.*

Důkaz. Je-li $M = \oplus_{i=1}^k M_i$ direktním součtem svých podmodulů $M_1, M_2, \dots, M_k$ je zřejmě $M = \sum_{i=1}^k M_i$. Pro $u \in M_i \cap \sum_{j \neq i} M_j$ je $u = u_1 + \dots + u_{i-1} + u_{i+1} + \dots + u_k$, odkud použitím jednoznačnosti zápisu dostáváme $u = 0$. Buď tedy naopak splněna podmínka věty. Pak každý prvek $u \in M$ lze zapsat ve tvaru $u = u_1 + u_2 + \dots + u_k$, $u_i \in M_i, i = 1, 2, \dots, k$, a zbývá dokázat jednoznačnost. Jestliže $u = v_1 + v_2 + \dots + v_k$ je jiný zápis prvku u, pak odečtením dostaneme pro každé $i = 1, 2, \dots, k$ rovnost $u_i - v_i = v_1 - u_1 + \dots + v_{i-1} - u_{i-1} + v_{i+1} - u_{i+1}, + \dots v_k - u_k \in M_i \cap \sum_{j \neq i} M_j = 0$, takže $u_i = v_i$ a jsme hotovi. ∎

16.18. Definice. Buď V_n vektorový prostor dimenze n nad tělesem T a buď φ endomorfismus prostoru V_n. Na Abelově grupě $(V_n, +)$ můžeme nyní definovat strukturu *$T[x]$-modulu* tak, že pro $f = \sum_{i=0}^m a_i x^i$ a $\boldsymbol{u} \in V_n$ položíme

$$f\boldsymbol{u} = \sum_{i=0}^{m} a_i \varphi^i(\boldsymbol{u}).$$

Snadno se ověří, že takto definované násobení splňuje podmínky z definice 16.14 (viz pozn. 16.19). Buď $\boldsymbol{u} \in V_n$ libovolný vektor. Normovaný polynom $m_{\boldsymbol{u}}$ nejmenšího možného stupně takový, že $m_{\boldsymbol{u}}\boldsymbol{u} = 0$ se nazývá *minimální polynom vektoru $\boldsymbol{u}$*. Podobně, normovaný polynom m_V nejmenšího možného stupně takový, že $m_V \boldsymbol{u} = 0$ pro každé $\boldsymbol{u} \in V_n = V$ se nazývá *minimální polynom prostoru V*. Existence obou polynomů bude dokázána v následující větě.

16.19. Poznámka. Ověřme, že násobení vektorů polynomy z $T[x]$ splňuje podmínky z definice 16.14. S výjimkou rovnosti $r(s\boldsymbol{u}) = (rs)\boldsymbol{u}$ jsou zbývající podmínky buď zřejmé, nebo plynou z definice endomorfismu. Ověřme tedy zbývající rovnost. Buďte tedy $f = \sum_{i=0}^m a_i x^i, g = \sum_{i=0}^k b_i x^i$ libovolné polynomy, $fg = \sum_{r=0}^{m+k} c_r x^r$, kde $c_r = \sum_{i+j=r} a_i b_j$. Potom máme $f(g\boldsymbol{u}) = f(\sum_{j=0}^k b_j \varphi^j(\boldsymbol{u})) = \sum_{j=0}^k b_j f \varphi^j(\boldsymbol{u}) = \sum_{j=0}^k b_j \sum_{i=0}^m a_i \varphi^i(\varphi^j(\boldsymbol{u})) = \sum_{j=0}^k \sum_{i=0}^m a_i b_j \varphi^{i+j}(\boldsymbol{u}) = \sum_{r=0}^{k+m} c_r \varphi^r(\boldsymbol{u}) = (fg)\boldsymbol{u}$.

16.20. Věta. *Buď $V_n = V$ vektorový prostor dimenze n nad tělesem T. Pak*

(i) pro každý vektor $\boldsymbol{u} \in V$ existuje minimální polynom $m_{\boldsymbol{u}}$;
(ii) $g\boldsymbol{u} = 0$ pro nějaké $g \in T[x]$, právě když $m_{\boldsymbol{u}} | g$;
(iii) existuje minimální polynom m_V prostoru V;
(iv) $g(\boldsymbol{u}) = 0$ pro každé $\boldsymbol{u} \in V$, právě když $m_V | g$.

Důkaz. (i) Buď $\boldsymbol{u} \in V_n$ libovolný vektor. Pak vektory $\boldsymbol{u}, \varphi(\boldsymbol{u}), \dots, \varphi^n(\boldsymbol{u})$ jsou lineárně závislé podle věty 2.17, takže $\sum_{i=0}^n a_i \varphi^i(\boldsymbol{u}) = 0$ pro nějaké, ne vesměs nulové, koeficienty $a_0, a_1, \dots, a_n$. Pak ale polynom $f = \sum_{i=0}^n a_i x^i$ je nenulový a

$fu = \sum_{i0}^{n} a_i\varphi^i(u) = 0$. Nyní stačí v množině všech nenulových polynomů f takových, že $fu = 0$ vzít normovaný polynom nejmenšího stupně.

(ii) Jestliže $m_u|g$, je $g = m_u h$ pro nějaké $h \in T[x]$, takže $gu = hm_u u = 0$. Buď tedy naopak $gu = 0$. Podle věty 16.7 existují polynomy $q, r \in T[x]$ takové, že $g = m_u q + r, \operatorname{st} r < \operatorname{st} m_u$. Přitom $ru = gu - qm_u u = 0$, takže $r = 0$, neboť v opačném případě dostáváme spor s minimalitou stupně polynomu m_u. Vidíme tedy, že $m_u|g$.

(iii) Podobně jako v (i) stačí ukázat existenci nenulového polynomu f takového, že $fu = 0$ pro každé $u \in V$. Buď $\{v_1, v_2, \dots, v_n\}$ báze prostoru V a buď $f = m_{v_1} m_{v_2} \dots m_{v_n} = m_{v_i} \bar{m}_{v_i}$. Je-li nyní $u \in V$ libovolný vektor, $u = \sum_{i=1}^{n} r_i v_i$, pak $fu = \sum_{i=1}^{n} r_i f v_i = \sum_{i=1}^{n} r_i \bar{m}_{v_i} m_{v_i} v_i = 0$.

(iv) Důkaz tohoto tvrzení je stejný jako důkaz tvrzení (ii), a lze jej tudíž přenechat čtenáři jako snadné cvičení. ■

16.21. Věta. *Buď f normovaný ireducibilní polynom nad tělesem T a buď M vektorový prostor nad T takový, že pro M jakožto $T[x]$-modul platí, že $f^k M = \{f^k u | u \in M\} = 0 \neq f^{k-1} M$ pro nějaké přirozené číslo k. Je-li $u \in M$ takový, že $f^{k-1} u \neq 0$, pak $M = \langle u \rangle \oplus N$ pro vhodný $T[x]$-podmodul N modulu M.*

Důkaz. Položme $v = f^{k-1} u \neq 0$ a buď $N \subseteq M$ podmodul maximální vzhledem k $v \notin N$ (Zornovo lemma). Nejprve ukážeme, že

$$\langle u \rangle \cap N = 0. \tag{16.1}$$

K tomuto cíli začneme s ověřením následujících dvou ekvivalencí

$$sv \in N \iff f|s \iff sv = 0. \tag{16.2}$$

Jestliže $f|s$ je $s = fh$ pro nějaké $h \in T[x]$, takže $sv = hfv = hf^k u = 0 \in N$. Jestliže f nedělí s, je podle věty 16.9 $f\alpha + s\beta = 1$ pro vhodné polynomy $\alpha, \beta \in T[x]$, takže $v = \alpha f v + \beta s v \in N$ a první ekvivalence je dokázána. K dokončení důkazu druhé ekvivalence ukažme nejprve, že

$$m_u = f^k. \tag{16.3}$$

Podle věty 16.20 (ii) víme, že $f^k = m_u h$, takže $m_u = f^l$ pro nějaké $l \leq k$ podle věty 16.11. Pro $l < k$ však je $f^{k-1} u = 0$, což jest spor s předpokladem.

Nyní již důkaz ekvivalencí (16.2) snadno dokončíme. Je-li $sv = 0$, je $sf^{k-1} u = 0$, takže $f^k | sf^{k-1}$ podle (16.3) a věty 16.20 (ii). Tedy $sf^{k-1} = f^k t$ pro nějaké $t \in T[x]$, odkud po zkrácení dostáváme $s = ft$, a tedy $f|s$.

Vraťme se nyní k důkazu formule (16.1). Pro $a \in \langle u \rangle \cap N$ je $a = ru \in N$ pro nějaké $r \in T[x]$. Pak $f^{k-1} a = rv \in N$, a tedy $f^{k-1} a = 0$ podle (16.2). Dále budeme pokračovat indukcí. Předpokládejme tedy, že $f^i a = 0$ pro nějaké $i \in \{1, 2, \dots, k-1\}$, a ukažme, že potom $f^{i-1} a = 0$. Jest $f^i a = f^i r u = 0$, takže podle (16.3) a věty (16.20) je $f^k | f^i r$, tedy $f^i r = f^k s$ pro nějaké $s \in T[x]$, a po zkrácení máme $r = f^{k-i}s$. Pak ale $f^{i-1}\boldsymbol{a} = f^{i-1}r\boldsymbol{u} = f^{i-1}f^{k-i}s\boldsymbol{u} = f^{k-1}s\boldsymbol{u} = s\boldsymbol{v} \in N$, a podle (16.2) je $s\boldsymbol{v} = 0$. Speciálně tedy pro $i = 1$ dostáváme $\boldsymbol{a} = 0$ a (16.1) je dokázáno.

K dokončení důkazu zbývá podle věty 16.17 ukázat, že

$$M = \langle \boldsymbol{u} \rangle \oplus N. \tag{16.4}$$

Předpokládejme tedy naopak, že $\langle \boldsymbol{u} \rangle \oplus N \subsetneq M$, a ukažme, že pak existuje prvek $\boldsymbol{a} \in M \setminus (\langle \boldsymbol{u} \rangle \oplus N)$ takový, že $f\boldsymbol{a} \in \langle \boldsymbol{u} \rangle \oplus N$. Je-li totiž $a \in M \setminus (\langle \boldsymbol{u} \rangle \oplus N)$ libovolný prvek, pak z $f^k\boldsymbol{a} = 0$ plyne existence přirozeného čísla r takového, že $f^r\boldsymbol{a} \in \langle \boldsymbol{u} \rangle \oplus N$ a $f^{r-1}a \notin \langle \boldsymbol{u} \rangle \oplus N$, takže prvek $f^{r-1}\boldsymbol{a}$ má požadovanou vlastnost. Máme tedy $f\boldsymbol{a} = r\boldsymbol{u} + \boldsymbol{w}$ pro nějaké $r \in T[x]$ a $\boldsymbol{w} \in N$. Pak $f^k\boldsymbol{a} = f^{k-1}r\boldsymbol{u} + f^{k-1}\boldsymbol{w} = r\boldsymbol{v} + f^{k-1}\boldsymbol{w} = 0$, odkud dostáváme $r\boldsymbol{v} = -f^{k-1}\boldsymbol{w} \in N$, a tedy $r = fs$ podle (16.2). Pak ale $f\boldsymbol{a} = fs\boldsymbol{u} + \boldsymbol{w}$, $\boldsymbol{a} - s\boldsymbol{u} \notin \langle \boldsymbol{u} \rangle \oplus N$ a $f(\boldsymbol{a} - s\boldsymbol{u}) = \boldsymbol{w} \in N$. Vidíme tedy, že $N \subsetneq \langle \boldsymbol{a} - s\boldsymbol{u} \rangle + N$, a jelikož N je maximální vzhledem k podmínce $\boldsymbol{v} \in N$, je $\boldsymbol{v} \in \langle \boldsymbol{a} - s\boldsymbol{u} \rangle + N$. Tedy $\boldsymbol{v} = t(\boldsymbol{a} - s\boldsymbol{u}) + \bar{\boldsymbol{w}}$ pro nějaké $t \in T[x]$ a $\bar{\boldsymbol{w}} \in N$. Jestliže nyní $f|t, t = fq$ pro vhodné $q \in T[x]$, je $\boldsymbol{v} = qf(\boldsymbol{a} - s\boldsymbol{u}) + \bar{\boldsymbol{w}} = q\boldsymbol{w} + \bar{\boldsymbol{w}} \in N$, což vzhledem k volbě podmodulu N není možné. Tedy f nedělí t, takže podle věty 16.9 je $f\alpha + t\beta = 1$ pro nějaká $\alpha, \beta \in T[x]$. Odtud máme $\boldsymbol{a} - s\boldsymbol{u} = \alpha f(\boldsymbol{a} - s\boldsymbol{u}) + \beta t(\boldsymbol{a} - s\boldsymbol{u}) = \alpha\boldsymbol{w} + \beta\boldsymbol{v} - \beta\bar{\boldsymbol{w}} \in \langle \boldsymbol{u} \rangle \oplus N$, neboť $\boldsymbol{v} \in \langle \boldsymbol{u} \rangle$. Získaný spor dokazuje (16.4), a tedy i větu. ∎

16.22. Důsledek. *Buď V vektorový prostor dimenze n nad tělesem T a buď f normovaný ireducibilní polynom z $T[x]$. Je-li na V definována struktura $T[x]$-modulu tak, $f^kV = 0$ pro nějaké přirozené číslo k, pak existují prvky $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_r$ z V tak, že $T[x]$-modul V je direktním součtem podmodulů $\langle \boldsymbol{u}_1 \rangle, \langle \boldsymbol{u}_2 \rangle, \ldots, \langle \boldsymbol{u}_r \rangle$, $V = \oplus_{i=1}^r \langle \boldsymbol{u}_r \rangle$.*

Důkaz. Předně je bezprostředně patrné, že každý podmodul $T[x]$-modulu V je podprostorem vektorového prostoru V. Postupujme nyní úplnou indukcí podle dimenze n prostoru V. Pro $n = 1$ je $V = \langle \boldsymbol{u} \rangle$ pro každé $0 \neq \boldsymbol{u} \in V$. Je-li $n > 1$, je podle předchozí věty $V = \langle \boldsymbol{u}_1 \rangle \oplus N$ pro vhodný $T[x]$-podmodul N modulu V. Protože N je vlastním podprostorem vektorového prostoru V, je $\dim N < \dim V$ podle věty 2.22, takže $N = \langle \boldsymbol{u}_2 \rangle \oplus \cdots \oplus \langle \boldsymbol{u}_r \rangle$ podle indukčního předpokladu a $V = \langle \boldsymbol{u}_1 \rangle \oplus \langle \boldsymbol{u}_2 \rangle \oplus \cdots \oplus \langle \boldsymbol{u}_r \rangle$. ∎

16.23. Poznámka. V odstavci 16.8 jsme zavedli pojem dělitelnosti polynomů tak, že polynom f dělí polynom g, $f|g$ v $T[x]$, jestliže existuje polynom $q \in T[x]$ takový, že $g = fq$. V opačném případě píšeme $f \nmid g$. Poznamenejme, že pro každý polynom $f \in T[x]$ je $f|0$, neboť $0 = f \cdot 0$, zatímco $0|f$ právě tehdy, když $f = 0$.

16.24. Definice. Říkáme, že polynomy $f, g \in T[x]$ jsou *asociované*, $f\|g$, jestliže $f|g$ a zároveň $g|f$. V opačném případě píšeme $f \nparallel g$. Polynom $f \in T[x]$ se nazývá *jednotka*, jestliže $f\|1$. Dále polynom $d \in T[x]$ je *společným dělitelem polynomů* $f_1, f_2, \ldots, f_n$, jestliže $d|f_i$ pro každé $i = 1, 2, \ldots, n$, a nazývá se *největším společným dělitelem*, jestliže je jejich společným dělitelem a každý jiný společný dělitel těchto prvků dělí d, tj. jestliže $t|f_i, i = 1, 2, \ldots, n$, pak $t|d$. Pro největšího společného dělitele polynomů $f_1, f_2, \ldots, f_n$ používáme označení $d = (f_1, f_2, \ldots, f_n)$.

16.25. Věta. *Buď T libovolné těleso. Pak platí*

(i) polynom $j \in T[x]$ je jednotkou, právě když j je nenulovým prvkem tělesa T;

(ii) polynomy f a g jsou asociovány, právě když existuje jednotka $j \in T[x]$ tak, že $g = fj$;

(iii) je-li $d = (f_1, f_2, \dots, f_n)$ největším společným dělitelem polynomů $f_1, f_2, \dots, f_n$, pak prvek $d' \in T[x]$ je největším společným dělitelem těchto polynomů, právě když $d' \| d$;

(iv) je-li $d = (f_1, f_2, \dots, f_n)$ největším společným dělitelem polynomů $f_1, f_2, \dots, f_n$, pak existují polynomy $\alpha_1, \alpha_2, \dots, \alpha_n \in T[x]$ tak, že $\sum_{i=1}^{n} \alpha_i f_i = d$;

(v) pro libovolné polynomy $f_1, f_2, \dots, f_n \in T[x]$ platí $(f_1, f_2, \dots, f_n) = ((f_1, f_2, \dots, f_{n-1}), f_n)$.

Důkaz. (i) Protože zřejmě $1|j$ pro každé $j \in T[x]$, je j jednotka, právě když $j|1$. Je-li tedy j jednotka, je $j \neq 0$ a $\operatorname{st} j = 0$ podle věty 16.6, takže $j \in T$. Naopak, pro $0 \neq j \in T$ je $jj^{-1} = 1$ a j je jednotka.

(ii) Jestliže $f|g$ a $g|f$, je podle poznámky 16.23 $f = 0$, právě když $g = 0$ a $g = f \cdot 1$. V opačném případě existují prvky $j, k \in T[x]$ tak, že $g = fj$ a $f = gk$. Pak ale $f = fjk$, takže po zkrácení $jk = 1$ a j je jednotka. Naopak, je-li $g = fj$, kde j je jednotka, je předně f dělitelem g, a protože podle (i) je $jj^{-1} = 1$, je $gj^{-1} = f$ a $g|f$.

(iii) Je-li $d' = (f_1, f_2, \dots, f_n)$, pak $d|d'$ a $d'|d$ podle definice 16.24, a tedy $d' \| d$. Naopak, je-li $d' \| d$, je podle (ii) $d' = dj$, kde j je jednotka. Jestliže nyní $t \in T[x]$ je společným dělitelem polynomů $f_1, f_2, \dots, f_n$, pak $t|d$ podle definice 16.24, a tedy $t|d'$ vzhledem k tomu, že $d|d'$. Prvek d' je tedy největším společným dělitelem polynomů $f_1, f_2, \dots, f_n$ opět podle definice 16.24.

(iv) Postup je podobný důkazu věty 16.9. Je-li $f_1 = f_2 = \dots = f_n = 0$, plyne snadno z poznámky 16.23, že $(f_1, f_2, \dots, f_n) = 0 = \sum_{i=1}^{n} 0 \cdot f_i$. V opačném případě buď' $d' = \sum_{i=1}^{n} \beta_i f_i$ normovaný polynom nejmenšího možného stupně v množině $M = \{\sum_{i=1}^{n} \gamma_i f_i \mid \gamma_1, \gamma_2, \dots, \gamma_n \in T[x]\}$. Pak pro každé $i \in \{1, 2, \dots, n\}$ existují podle věty 16.7 polynomy $q_i, r_i \in T[x]$ takové, že $f_i = d'q_i + r_i$, kde $\operatorname{st} r_i < \operatorname{st} d'$. Přitom $r_i = f_i - \sum_{j=1}^{n} \beta_j f_j \in M$, takže $r_i = 0$, neboť v opačném případě nerovnost $\operatorname{st} r_i < \operatorname{st} d'$ vede ke sporu s volbou polynomu d'. Vidíme tedy, že d' je společným dělitelem polynomů $f_1, f_2, \dots, f_n$. Je-li $t \in T[x]$ jiný společný dělitel těchto polynomů, plyne z $t|f_i$, $i = 1, 2, \dots, n$, snadno, že $t|(\sum_{i=1}^{n} \beta_i f_i)$, tj. $t|d'$ a d' je největší společný dělitel polynomů $f_1, f_2, \dots, f_n$. Podle (iii) a (i) existuje jednotka $j \in T[x]$ tak, že $d = d'j$ a stačí položit $\alpha_i = \beta_i j$ pro každé $i = 1, 2, \dots, n$.

(v) Označme $d = (f_1, f_2, \dots, f_n)$, $t = (f_1, f_2, \dots, f_{n-1})$ a $d' = (t, f_n)$. Předně vidíme, že $d|f_i$, $i = 1, 2, \dots, n$, takže $d|t$, $d|f_n$, a tedy i $d|d'$. Na druhé straně $d'|t$, $d'|f_n$, tedy $d'|f_i$, $i = 1, 2, \dots, n$, odkud $d'|d$ a stačí použít tvrzení (iii). ■

16.26. Věta. *Buď $f = af_1^{k_1} f_2^{k_2} \dots f_r^{k_r}$, $0 \neq a \in T$, polynom kladného stupně z $T[x]$, kde $f_1, f_2, \dots, f_r$ jsou navzájem různé normované ireducibilní polynomy a $k_1, k_2, \dots, k_r$ jsou kladná celá čísla. Jestliže polynom $d \in T[x]$ dělí polynom f, pak $d = bf_1^{l_1} f_2^{l_2} \dots f_r^{l_r}$, kde $0 \neq b \in T$ a $0 \leq l_i \leq k_i$ pro každé $i = 1, 2, \dots, r$.*

Důkaz. Podle věty 16.11 lze polynom d zapsat jednoznačně ve tvaru $d = bh_1^{s_1} h_2^{s_2} \dots h_t^{s_t}$, kde $h_1, h_2, \dots, h_t$ jsou navzájem různé normované ireducibilní polynomy z $T[x]$, $s_1, s_2, \dots, s_t$ jsou celá kladná čísla a $0 \neq b \in T$. Pro každé $i \in \{1, 2, \dots, t\}$

polynom h_i dělí d, takže $h_i|f$ vzhledem k tomu, že $d|f$ (viz též pozn. 18.3 níže). Podle lemmatu 16.10 je h_i rovno některému $f_j, j = 1, 2, \dots, r$, odkud snadno dostáváme, že d můžeme psát ve tvaru $d = df_1^{l_1} f_2^{l_2} \dots f_r^{l_r}$, kde l_i, $i = 1, 2, \dots, r$, jsou celá nezáporná čísla, a zbývá ukázat, že $l_i \leq k_i$ pro každé $i = 1, 2, \dots, r$. Podle předpokladu existuje $h \in T[x]$ tak, že $f = dh$ a podle předchozí části důkazu je $h = cf_1^{m_1} f_2^{m_2} \dots f_r^{m_r}$, kde $0 \neq c \in T$ a $m_1, m_2, \dots, m_r$ jsou celá nezáporná čísla. Pak ale $f = af_1^{k_1} f_2^{k_2} \dots f_r^{k_r} = bcf_1^{l_1+m_1} f_2^{l_2+m_2} \dots f_r^{l_r+m_r} = dh$, takže $l_i + m_i = k_i$, $i = 1, 2, \dots, r$, vzhledem k tomu, že rozklad polynomu f v součin ireducibilních prvků je podle věty 16.11 jednoznačný. Tedy $l_i \leq k_i$ a jsme hotovi. ■

16.27. Věta. *Nechť $f = af_1^{k_1} f_2^{k_2} \dots f_n^{k_n}$ a $g = bf_1^{l_1} f_2^{l_2} \dots f_n^{l_n}$, kde $0 \neq a \in T$, $0 \neq b \in T$, jsou dva rozklady polynomů $f, g \in T[x]$ na součin ireducibilních prvků. Označíme-li $m_i = \min(k_i, l_i)$, $i = 1, 2, \dots, n$, pak $d = (f, g) = f_1^{m_1} f_2^{m_2} \dots f_n^{m_n}$.*

Důkaz. Protože $m_i \leq k_i$ a $m_i \leq l_i$ pro všechna $i = 1, 2, \dots, n$, je polynom d zřejmě společným dělitelem polynomů f a g. Je-li nyní $t \in T[x]$ libovolný společný dělitel polynomů f a g, je podle předchozí věty $t = cf_1^{r_1} f_2^{r_2} \dots f_n^{r_n}$, kde $0 \neq c \in T$ a $0 \leq r_i \leq k_i$, $0 \leq r_i \leq l_i$ pro každé $i = 1, 2, \dots, n$. Pak ale $0 \leq r_i \leq m_i$ pro všechna $i = 1, 2, \dots, n$, takže $t|d$ a věta je dokázána. ■

16.28. Poznámka. Uvědomme si, že věta 16.27 nám dává konkrétní metodu (jednu z možných), jak spočítat největšího společného dělitele dvou polynomů f a g s koeficienty z tělesa T. Jsou-li $f_1, f_2, \dots, f_n \in T[x]$ libovolné polynomy, pak věta 16.25 (v) dává návod, jak pomocí úplné indukce spočítat největšího společného dělitele $d = (f_1, f_2, \dots, f_n)$ těchto polynomů. Označíme-li totiž $d_2 = (f_1, f_2)$, $d_3 = (d_2, f_3), \dots, d_{i+1} = (d_i, f_{i+1})$, $i = 1, \dots, n-1$, pak zřejmě $d_n = (d_{n-1}, f_n)$ je hledaný největší společný dělitel daných polynomů.

Definice 17.1. Matice $\boldsymbol{A}(\lambda) = (a_{ij}(\lambda))$, kde $a_{ij}(\lambda)$ je nějaký polynom v neurčité λ nad tělesem T pro každé $i = 1, \ldots, m$ a každé $j = 1, \ldots, n$, se nazývá *λ-matice* typu (m, n) nad tělesem T. Je patrné, že každou λ-matici lze psát ve tvaru $\boldsymbol{A}(\lambda) = \boldsymbol{A}_0 + \lambda \boldsymbol{A}_1 + \cdots + \lambda^k \boldsymbol{A}_k$, kde $\boldsymbol{A}_0, \ldots \boldsymbol{A}_k$ jsou matice typu (m, n) nad tělesem T, tj. $\boldsymbol{A}_0, \ldots, \boldsymbol{A}_k \in T_{m,n}$. Je-li speciálně $\boldsymbol{A}(\lambda)$ čtvercová matice stupně n a je-li $\boldsymbol{B} \in T_n$ libovolná čtvercová matice, jsou všechny matice $\boldsymbol{A}_0 \ldots, \boldsymbol{A}_k$ rovněž čtvercové stupně n a můžeme definovat matici $\boldsymbol{A}(\boldsymbol{B}) \in T_n$ předpisem $\boldsymbol{A}(\boldsymbol{B}) = \boldsymbol{A}_0 + \boldsymbol{B}\boldsymbol{A}_1 + \cdots + \boldsymbol{B}^k \boldsymbol{A}_k$.

Poznámka 17.2. Uvědomme si, že v předchozí definici jsme mohli namísto zápisu $\boldsymbol{A}(\lambda) = \sum_{i=0}^{k} \lambda^i \boldsymbol{A}_i$ zvolit zápis $\boldsymbol{A}(\lambda) = \sum_{i=0}^{k} \boldsymbol{A}_i \lambda^i$ a poté položit $\boldsymbol{A}(\boldsymbol{B}) = \boldsymbol{A}_0 + \boldsymbol{A}_1 \boldsymbol{B} + \cdots + \boldsymbol{A}_k \boldsymbol{B}^k$. Zatímco oba zápisy matice $\boldsymbol{A}(\lambda)$ se od sebe svým významem prakticky neliší, jsou matice $\boldsymbol{A}(\boldsymbol{B})$ vzhledem k nekomutativnosti operace násobení matic obecně různé. Z tohoto důvodu musíme tedy předem rozhodnout, zda budeme v matici $\boldsymbol{A}(\lambda)$ psát neurčitou λ zleva či zprava a tento způsob zápisu v dalším důsledně respektovat. Dříve než budeme pokračovat, zdůrazněme, že v našich dalších úvahách budeme používat zápis z předchozí definice, tj. neurčitá λ bude psána zleva. Poznamenejme ještě, že pro zjednodušení vyjadřování budeme v dalším někdy maticím $\boldsymbol{A} \in T_{m,n}$ na rozdíl od λ-matic říkat *skalární matice.*

Věta 17.3. *Je-li $\boldsymbol{A}(\lambda)$ čtvercová matice stupně n nad tělesem T a $\boldsymbol{B} \in T_n$ libovolná skalární matice, pak existuje právě jedna λ-matice $\boldsymbol{C}(\lambda)$ a právě jedna skalární matice $\boldsymbol{D} \in T_n$ tak, že*

$$\boldsymbol{A}(\lambda) = (\boldsymbol{B} - \lambda \boldsymbol{E})\boldsymbol{C}(\lambda) + \boldsymbol{D}.$$

Přitom $\boldsymbol{D} = \boldsymbol{A}(\boldsymbol{B})$.

Důkaz. Přímým vynásobením snadno ověříme, že pro každé $i = 1, 2, \ldots$ platí rovnost $\boldsymbol{B}^i - \lambda^i \boldsymbol{E} = (\boldsymbol{B} - \lambda \boldsymbol{E})(\boldsymbol{B}^{i-1} + \lambda \boldsymbol{B}^{i-2} + \cdots + \lambda^{i-2}\boldsymbol{B} + \lambda^{i-1}\boldsymbol{E})$. Odtud nyní snadno dostaneme $\boldsymbol{A}(\lambda) - \boldsymbol{A}(\boldsymbol{B}) = \sum_{i=0}^{k} \lambda^i \boldsymbol{A}_i - \sum_{i=0}^{k} \boldsymbol{B}^i \boldsymbol{A}_i = -\sum_{i=0}^{k} (\boldsymbol{B}^i - \lambda^i \boldsymbol{E})\boldsymbol{A}_i = (\boldsymbol{B} - \lambda \boldsymbol{E})\boldsymbol{C}(\lambda)$ pro vhodnou λ-matici $\boldsymbol{C}(\lambda)$, a tedy i rovnost $\boldsymbol{A}(\lambda) = (\boldsymbol{B} - \lambda \boldsymbol{E})\boldsymbol{C}(\lambda) + \boldsymbol{A}(\boldsymbol{B})$ dokazující existenci matic $\boldsymbol{C}(\lambda)$ a $\boldsymbol{D}$. K důkazu jednoznačnosti předpokládejme jednak, že $\boldsymbol{A}(\lambda) = (\boldsymbol{B} - \lambda \boldsymbol{E})\boldsymbol{C}(\lambda) + \boldsymbol{A}(\boldsymbol{B})$, jednak, že $\boldsymbol{A}(\lambda) = (\boldsymbol{B} - \lambda \boldsymbol{E})\boldsymbol{C}_1(\lambda) + \boldsymbol{D}$. Odečtením dostaneme rovnost $(\boldsymbol{B} - \lambda \boldsymbol{E})(\boldsymbol{C}(\lambda) - \boldsymbol{C}_1(\lambda)) = \boldsymbol{D} - \boldsymbol{A}(\boldsymbol{B})$. Pro $\boldsymbol{C}(\lambda) \neq \boldsymbol{C}_1(\lambda)$ je na levé straně λ-matice, která jistě není skalární, zatímco na pravé straně je matice skalární. Získaný spor dokazuje, že $\boldsymbol{C}(\lambda) = \boldsymbol{C}_1(\lambda)$, $\boldsymbol{D} = \boldsymbol{A}(\boldsymbol{B})$ a jednoznačnost je dokázána. ∎

17.4. Věta. (Hamilton–Cayley.) *Je-li $\boldsymbol{A} \in T_n$ čtvercová matice stupně n a $g(\lambda) = |\boldsymbol{A} - \lambda \boldsymbol{E}|$ její charakteristický polynom, pak $g(\boldsymbol{A}) = 0$.*

Důkaz. Podle předchozí věty existuje λ-matice $\boldsymbol{C}(\lambda)$ taková, že $g(\lambda)\boldsymbol{E} = (\boldsymbol{A} - \lambda \boldsymbol{E})\boldsymbol{C}(\lambda) + g(\boldsymbol{A})$. Je-li $\boldsymbol{B}(\lambda)$ matice adjungovaná k matici $\boldsymbol{A} - \lambda \boldsymbol{E}$ (definice 8.11), je podle věty 8.12 $(\boldsymbol{A} - \lambda \boldsymbol{E})\boldsymbol{B}(\lambda) = \det(\boldsymbol{A} - \lambda \boldsymbol{E})\boldsymbol{E} = g(\lambda)\boldsymbol{E}$. Pak ale jednoznačnost v předchozí větě dává $\boldsymbol{C}(\lambda) = \boldsymbol{B}(\lambda)$ a $g(\boldsymbol{A}) = 0$, což jsme chtěli dokázat. ∎

17.5. Poznámka. Při důkazu Hamiltonovy–Cayleyho věty jsme použili větu 17.3, a můžeme se tedy ptát, zda by nebylo možno do charakteristického polynomu dosadit matici $\boldsymbol{A}$. Ukažme si na jednoduchém příkladě, v čem problém spočívá. Pro matici $A = \begin{pmatrix} 2, & 1 \\ 0, & 1 \end{pmatrix}$ (nad tělesem R reálných čísel) máme $g(\lambda) = |A - \lambda E| = \begin{vmatrix} 2-\lambda, & 1 \\ 1, & -\lambda \end{vmatrix} = \lambda^2 - 2\lambda - 1$, a tedy $g(A) = A^2 - 2A - E = \begin{pmatrix} 5, & 2 \\ 2, & 1 \end{pmatrix} - \begin{pmatrix} 4, & 2 \\ 2, & 0 \end{pmatrix} - \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix} = \begin{pmatrix} 0, & 0 \\ 0, & 0 \end{pmatrix}$. Na druhé straně ale do $|A - \lambda E| = \begin{vmatrix} 2-\lambda, & 1 \\ 1, & -\lambda \end{vmatrix}$ nelze za λ dosadit matici A, neboť výraz, který bychom dosazením dostali nemá žádný rozumný smysl.

17.6. Definice. Čtvercovou matici

$$B(\lambda) = \begin{pmatrix} \lambda, & 1, & 0, & \dots, & 0, & 0 \\ 0, & \lambda, & 1, & \dots, & 0, & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0, & 0, & 0, & \dots, & \lambda, & 1 \\ 0, & 0, & 0, & \dots, & 0, & \lambda \end{pmatrix}$$

stupně n nazýváme *Jordanovou buňkou stupně n příslušnou prvku λ* z tělesa T. *Jordanovou maticí* rozumíme matici tvaru

$$\begin{pmatrix} B_1, & 0, & 0, & \dots, & 0 \\ 0, & B_2, & 0, & \dots, & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0, & 0, & 0, & \dots, & B_k \end{pmatrix},$$

kde B_i je Jordanova buňka stupně n_i příslušná prvku λ_i, $i = 1, 2, \dots, k$, a symbol 0 značí nulovou matici příslušného typu. Matice uvedeného tvaru se též nazývá *bloková matice.*

17.7. Příklad. Matice

$$\begin{pmatrix} 2, & 1, & 0, & 0, & 0 \\ 0, & 2, & 1, & 0, & 0 \\ 0, & 0, & 2, & 0, & 0 \\ 0, & 0, & 0, & 3, & 1 \\ 0, & 0, & 0, & 0, & 3 \end{pmatrix} \quad \text{a} \quad \begin{pmatrix} 2, & 1, & 0, & 0, & 0 \\ 0, & 2, & 0, & 0, & 0 \\ 0, & 0, & 2, & 0, & 0 \\ 0, & 0, & 0, & 3, & 1 \\ 0, & 0, & 0, & 0, & 3 \end{pmatrix}$$

jsou Jordanovy matice, první sestává ze dvou Jordanových buněk, druhá ze třech.

17.8. Věta. *Buď $A \in T_n$ čtvercová matice stupně n nad tělesem T mající v T n vlastních hodnot (ne nutně různých). Pak matice A je podobná Jordanově matici.*

Důkaz. Buď V_n vektorový prostor dimenze n nad tělesem T, $\bar{N} = \{v_1, v_2, \dots, v_n\}$ buď jeho báze a buď φ endomorfismus prostoru V_n příslušný matici A^T vzhledem k bázi $\bar{N}$ podle věty 10.7. Definujme na V_n strukturu $T[x]$-modulu podle definice 16.18. Je-li m_V minimální polynom prostoru $V = V_n$, existuje podle věty 16.11 rozklad $m_V = f_1^{k_1} f_2^{k_2} \dots f_r^{k_r} = f_i^{k_i} \bar{f}_i$, kde $f_i \in T[x]$ jsou normované ireducibilní polynomy a k_i jsou přirozená čísla. Položme

$$M_i = \{u \in V \mid f_i^{k_i} u = 0\} \tag{17.1}$$

a ukažme, že

$$V = M_1 \oplus M_2 \oplus \dots \oplus M_r. \tag{17.2}$$

Předně pro $\boldsymbol{u} \in M_i \cap \sum_{j \neq i} M_j$ je $f_i^{k_i}\boldsymbol{u} = \bar{f}_i\boldsymbol{u} = 0$. Podle věty 16.12 (i) existují prvky $\beta_i, \gamma_i \in T[x]$ tak, že $f_i^{k_i}\beta_i + \bar{f}_i\gamma_i = 1$. Pak ale $\boldsymbol{u} = \beta_i f_i^{k_i}\boldsymbol{u} + \gamma_i\bar{f}_i\boldsymbol{u} = 0$ a $M_i \cap \sum_{j \neq i} M_j = 0$. Konečně, opět podle věty 16.12 (ii), existují polynomy $\alpha_1, \alpha_2 \ldots, \alpha_r \in T[x]$ takové, že $\sum_{i=1}^r \bar{f}_i\alpha_i = 1$. Pak pro každé $\boldsymbol{u} \in V$ máme $\boldsymbol{u} = \sum_{i=1}^r \alpha_i\bar{f}_i\boldsymbol{u} \in \sum_{i=1}^r M_i$ vzhledem k tomu, že z $0 = m_v\boldsymbol{u} = f_i^{k_i}\bar{f}_i\boldsymbol{u}$ plyne $\bar{f}_i\boldsymbol{u} \in M_i$ podle (17.1). Tím je rovnost (17.2) podle věty 16.17 dokázána.

Protože podle (17.1) je $f_i^{k_i}M_i = 0$, je každé M_i podle důsledku 16.22 direktním součtem cyklických (generovaných jedním prvkem) $T[x]$-podmodulů, takže ze (17.2) dostáváme, že V lze psát ve tvaru

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_k, \tag{17.3}$$

kde $W_i = \langle \boldsymbol{u}_i \rangle$ jsou $T[x]$-podmoduly na V takové, že $f_i^k\langle \boldsymbol{u}_i \rangle = 0$ pro nějaký normovaný ireducibilní polynom f_i dělící m_V.

Vzhledem k tomu, že každý $T[x]$-podmodul $T[x]$-modulu V je podprostorem vektorového prostoru V, můžeme v každém W_i zvolit bázi N_i a pak podle věty 2.29 je $N = N_1 \cup N_2 \cup \cdots \cup N_k$ báze prostoru V. Protože podle definice 16.18 pro každé $\boldsymbol{u} \in W_i$ je $\varphi(\boldsymbol{u}) = x\boldsymbol{u} \in W_i$, je matice endomorfismu φ vzhledem k bázi N bloková matice tvaru

$$\begin{pmatrix} \boldsymbol{B}_1, & 0, & \ldots, & 0 \\ 0, & \boldsymbol{B}_2, & \ldots, & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0, & 0, & \ldots, & \boldsymbol{B}_k \end{pmatrix}.$$

K dokončení důkazu tedy nyní stačí v každém podprostoru W_i, $i = 1, 2, \ldots, k$, nalézt takovou bázi N_i, aby matice endomorfismu φ vzhledem k této bázi byla Jordanova buňka, a použít větu 10.17.

Buď tedy $\langle \boldsymbol{u} \rangle$ $T[x]$-podmodul na V takový, že $f^k\langle \boldsymbol{u} \rangle = 0 \neq f^{k-1}\langle \boldsymbol{u} \rangle$, kde $f|m_V$ je ireducibilní polynom. Předně podle věty 10.5 máme $\{\varphi(\boldsymbol{u})\}_{\bar{N}} = \{\boldsymbol{u}\}_{\bar{N}}\boldsymbol{A}$, odkud úplnou indukcí dostáváme $\{\varphi^i(\boldsymbol{u})\}_{\bar{N}} = \{\varphi(\varphi^{i-1}(\boldsymbol{u}))\}_{\bar{N}} = \{\varphi^{i-1}(\boldsymbol{u})\}_{\bar{N}}\boldsymbol{A} = \{\boldsymbol{u}\}_{\bar{N}}\boldsymbol{A}^{i-1}\cdot \boldsymbol{A} = \{\boldsymbol{u}\}_{\bar{N}}\boldsymbol{A}^i$. Je-li nyní $h = \sum_{i=0}^m a_i x^i \in T[x]$ libovolný polynom, je podle definice 16.18 $\{h\boldsymbol{u}\}_{\bar{N}} = \{\sum_{i=0}^m a_i\varphi^i(\boldsymbol{u})\}_{\bar{N}} = \sum_{i=0}^m a_i\{\varphi^i(\boldsymbol{u})\}_{\bar{N}} = \sum_{i=0}^m a_i\{\boldsymbol{u}\}_{\bar{N}}\boldsymbol{A}^i = \{\boldsymbol{u}\}_{\bar{N}}\sum_{i=0}^m a_i\boldsymbol{A}^i = \{\boldsymbol{u}\}_{\bar{N}}h(\boldsymbol{A})$. Dále, je-li $g \in T[x]$ charakteristický polynomem matice $\boldsymbol{A}$, je podle Hamiltonovy–Cayleyho věty 17.4 $g(\boldsymbol{A}) = 0$, takže $\{g\boldsymbol{u}\}_{\bar{N}} = \{\boldsymbol{u}\}_{\bar{N}}g(\boldsymbol{A}) = 0$ pro každé $\boldsymbol{u} \in V$, a tedy $gV = 0$. Podle věty 16.20 tedy m_V dělí polynom g. Protože zároveň $f|m_V$ a protože podle předpokladu věty je $g = (x - \lambda_1)(x - \lambda_2)\ldots(x - \lambda_n)$, plyne z věty 16.11 a z ireducibility polynomu f, že

$$f = x - \lambda \quad \text{pro některé} \quad \lambda = \lambda_i,\ i \in \{1, 2, \ldots, n\}. \tag{17.4}$$

Uvažujme nyní množinu

$$N = \{\boldsymbol{u}, f\boldsymbol{u}, \ldots, f^{k-1}\boldsymbol{u}\} \subseteq \langle \boldsymbol{u} \rangle. \tag{17.5}$$

Jestliže ukážeme, že N je báze podprostoru $\langle \boldsymbol{u} \rangle$ vektorového prostoru V, pak podle (17.4) a definice 16.18 máme

$$
\begin{array}{lllllll}
\varphi(\boldsymbol{u}) & = & x\boldsymbol{u} & = & \lambda\boldsymbol{u} & + & f\boldsymbol{u}, \\
\varphi(f\boldsymbol{u}) & = & xf\boldsymbol{u} & = & \lambda f\boldsymbol{u} & + & f^2\boldsymbol{u}, \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\varphi(f^{k-2}\boldsymbol{u}) & = & xf^{k-2}\boldsymbol{u} & = & \lambda f^{k-2}\boldsymbol{u} & + & f^{k-1}\boldsymbol{u}, \\
\varphi(f^{k-1}\boldsymbol{u}) & = & xf^{k-1}\boldsymbol{u} & = & \lambda f^{k-1}\boldsymbol{u}, & &
\end{array}
$$

takže matice endomorfismu $\varphi|\langle\boldsymbol{u}\rangle$ vzhledem k bázi N je Jordanova buňka stupně k příslušná k prvku λ.

Dokažme nejprve lineární nezávislost množiny N ze (17.5). Pro $r_0\boldsymbol{u}+r_1f\boldsymbol{u}\cdots+r_if^i\boldsymbol{u}+\cdots+r_{k-1}f^{k-1}\boldsymbol{u}=0$ dostaneme vynásobením polynomem f^{k-1} rovnost $r_0f^{k-1}\boldsymbol{u}=0$ vzhledem k tomu, že podle předpokladu je $f^k\boldsymbol{u}=0$. Vidíme tedy, že $r_0=0$, a můžeme dále postupovat indukcí. Předpokládejme tedy, že pro nějaké $i=\{0,1,\ldots,k-2\}$ je $r_0=r_1=\cdots=r_i=0$. Vynásobením výše uvedené lineární kombinace polynomem f^{k-i-2} dostáváme $r_{i+1}f^{k-1}\boldsymbol{u}=0$, takže $r_{i+1}=0$ a množina N je nad T lineárně nezávislá.

Zbývá ověřit, že množina N generuje $\langle\boldsymbol{u}\rangle$ jako vektorový prostor nad T. Je-li tedy $0\neq g\boldsymbol{u}\in\langle\boldsymbol{u}\rangle$ pro nějaké $g\in T[x]$ libovolný prvek, je podle věty 16.7 $g=f^kq+r$ pro vhodné prvky $q,r\in T[x]$, kde st $r<k$. Přitom $r\boldsymbol{u}=g\boldsymbol{u}-qf^k\boldsymbol{u}=g\boldsymbol{u}$, takže můžeme předpokládat, že st $g<k$. Protože podle (17.4) je $f=x-\lambda$, je $x=f+\lambda$ a pro $g=g_1+a_{k-1}x^{k-1}$ máme $g=g_1+a_{k-1}(f+\lambda)^{k-1}=\bar{g}_1+a_{k-1}f^{k-1}$, kde st $\bar{g}_1<k-1$. Odtud úplnou indukcí snadno dostaneme $g=b_0+b_1f+\cdots+b_{k-1}f^{k-1}$, takže konečně $g\boldsymbol{u}=b_0\boldsymbol{u}+b_1f\boldsymbol{u}+\cdots+b_{k-1}f^{k-1}\boldsymbol{u}$, pro $b_0,b_1,\ldots,b_{k-1}\in T$ a jsme hotovi. ■

17.9. Důsledek. *Buď T algebraicky uzavřené těleso (speciálně těleso komplexních čísel). Pak každá čtvercová matice nad T je podobná Jordanově matici.*

Důkaz. Nad algebraicky uzavřeným tělesem má každý polynom stupně n právě n kořenů. ■

18.1. Věta. *Buď $\boldsymbol{B}$ čtvercová matice tvaru*

$$\boldsymbol{B} = \begin{pmatrix} \boldsymbol{B}_1, & \boldsymbol{0}_1 \\ \boldsymbol{0}_2, & \boldsymbol{B}_2 \end{pmatrix},$$

kde $\boldsymbol{B}_1$ je čtvercová matice stupně n_1, $\boldsymbol{B}_2$ čtvercová matice stupně n_2, $\boldsymbol{0}_1$ nulová matice typu (n_1, n_2) a $\boldsymbol{0}_2$ nulová matice typu (n_2, n_1). Pak $\det \boldsymbol{B} = \det \boldsymbol{B}_1 \det \boldsymbol{B}_2$.

Důkaz. Označme $n = n_1+n_2$. Podle definice determinantu 7.1 je $\det \boldsymbol{B} = \sum_{\pi\in S_n} \operatorname{zn}\pi\, b_{1i_1} b_{2i_2} \dots b_{ni_n}$, kde sčítáme přes všechny permutace

$$\pi = \begin{pmatrix} 1, & 2, & \dots, & n \\ i_1, & i_2, & \dots, & i_n \end{pmatrix} \in S_n.$$

Rozdělme množinu S_n všech permutací do dvou skupin, P_1 sestává ze všech permutací $\pi \in S_n$, $\pi = \pi_1\pi_2$, kde

$$\pi_1 = \begin{pmatrix} 1, & 2, & \dots, & n_1, & n_1+1, & \dots, & n \\ i_1, & i_2, & \dots, & i_{n_1}, & n_1+1, & \dots, & n \end{pmatrix},$$

$$\pi_2 = \begin{pmatrix} 1, & 2, & \dots, & n_1, & n_1+1, & \dots, & n \\ 1, & 2, & \dots, & n_1, & j_{n_1+1}, & \dots, & j_n \end{pmatrix}$$

a $P_2 = S_n \backslash P_1$. Je-li $\pi \in P_2$ libovolná permutace, existuje index $i \in \{1, 2, \dots, n_1\}$, takový, že $\pi(i) \in \{n_1+1, \dots, n\}$, neboť v opačném případě by π leželo v P_1. Sčítanec determinantu příslušný permutaci π obsahuje činitel $b_{i\pi(i)} = 0$, takže $\det \boldsymbol{B} = \sum_{\pi\in P_1} \operatorname{zn}\pi\, b_{1i_1} b_{2i_2} \dots b_{ni_n} = \sum_{\pi_1} \operatorname{zn}\pi_1 b_{1i_1} b_{2i_2} \dots b_{n_1 i_{n_1}} \cdot \sum_{\pi_2} \operatorname{zn}\pi_2 b_{n_1+1, j_{n_1+1}} \dots b_{nj_n} = \det \boldsymbol{B}_1 \det \boldsymbol{B}_2$ vzhledem k tomu, že $\operatorname{zn}\pi = \operatorname{zn}\pi_1 \operatorname{zn}\pi_2$ podle věty 6.13. ∎

18.2. Definice. Říkáme, že čtvercová λ-matice $\boldsymbol{A}(\lambda)$ je *v kanonickém tvaru*, jestliže

$$\boldsymbol{A}(\lambda) = \begin{pmatrix} a_1(\lambda), & 0, & \dots, & 0 \\ 0, & a_2(\lambda), & \dots, & 0 \\ \dots & \dots & \dots & \dots \\ 0, & 0, & \dots, & a_n(\lambda) \end{pmatrix},$$

kde $a_i(\lambda) | a_{i+1}(\lambda)$ pro každé $i = 1, 2, \dots, n-1$.

18.3. Poznámka. Na tomto místě je vhodné si uvědomit některé zcela elementární důsledky definice dělitelnosti 16.8, které budeme v dalším často, zpravidla mlčky používat. Předně, jestliže $f|g$ a $g|h$, $g = f\alpha$, $h = g\beta$, $\alpha, \beta \in T[x]$, pak $h = f\alpha\beta$ a $f|h$. Dále, když $f|g_i$, a $\alpha_i \in T[x]$, $i = 1, 2, \dots, n$, jsou libovolné prvky, pak $f | \sum_{i=1}^n g_i\alpha_i$, neboť z $g_i = fh_i$, $h_i \in T[x]$ dostáváme $\sum_{i=1}^n g_i\alpha_i = f(\sum_{i=1}^n h_i\alpha_i)$.

18.4. Věta. *Každou čtvercovou λ-matici $\boldsymbol{A}(\lambda)$ lze konečným počtem elementárních transformací na řádky a sloupce převést na kanonický tvar.*

Důkaz. Důkaz rozdělíme do čtyř kroků.

(a) Jestliže prvek $a_{11}(\lambda)$ nedělí všechny prvky prvního řádku, pak konečným počtem elementárních transformací na sloupce matice $\boldsymbol{A}(\lambda)$ dostaneme λ-matici $\boldsymbol{B}(\lambda)$, kde $\operatorname{st} b_{11}(\lambda) < \operatorname{st} a_{11}(\lambda)$.

Nechť tedy $a_{11}(\lambda) \nmid a_{1i}(\lambda)$ pro některé $i = 2, 3, \dots, n$. Podle věty 16.7 existují polynomy $q_i(\lambda)$ a $r_i(\lambda)$ v $T[\lambda]$ takové, že $a_{1i}(\lambda) = a_{11}(\lambda)q_i(\lambda) + r_i(\lambda)$, přičemž $\operatorname{st} r_i(\lambda) < \operatorname{st} a_{11}(\lambda)$. Odečtením $q_i(\lambda)$-násobku prvního sloupce od sloupce i-tého dostaneme matici $\boldsymbol{C}(\lambda)$, kde $c_{1i}(\lambda) = r_i(\lambda)$. Podle věty 3.3 lze vzájemnou výměnu dvou sloupců realizovat konečným počtem elementárních transformací. Vyměníme-li tedy navzájem první a i-tý sloupec matice $\boldsymbol{C}(\lambda)$, dostaneme matici $\boldsymbol{B}(\lambda)$ požadovaných vlastností.

(b) Jestliže prvek $a_{11}(\lambda)$ nedělí všechny prvky prvního sloupce, pak konečným počtem elementárních transformací na řádky matice $\boldsymbol{A}(\lambda)$ dostaneme λ-matici $\boldsymbol{B}(\lambda)$, kde $\operatorname{st} b_{11}(\lambda) < \operatorname{st} a_{11}(\lambda)$.

Důkaz je stejný jako v předchozím případě, a proto jej lze přenechat čtenáři jako cvičení.

(c) Jestliže prvek $a_{11}(\lambda)$ nedělí některý prvek matice $\boldsymbol{A}(\lambda)$, pak konečným počtem elementárních tranformací na řádky a sloupce matice $\boldsymbol{A}(\lambda)$ dostaneme matici $\boldsymbol{B}(\lambda)$ takovou, že $\operatorname{st} b_{11}(\lambda) < \operatorname{st} a_{11}(\lambda)$.

Vzhledem k částem (a) a (b) můžeme předpokládat, že prvek $a_{11}(\lambda)$ dělí všechny prvky v prvním řádku i v prvním sloupci. Nechť tedy $a_{11}(\lambda) \nmid a_{ik}(\lambda)$ pro některá $i, k \in \{2, 3, \dots, n\}$ a nechť $a_{1i} = a_{11}\alpha_i$ a $a_{j1} = a_{11}\beta_j$ pro nějaké polynomy $\alpha_i, \beta_j \in T[\lambda]$, $i, j \in \{2, 3, \dots, n\}$. Odečtením α_i-násobku prvního sloupce od i-tého pro $i = 2, 3, \dots, n$ dostaneme λ-matici $\boldsymbol{C}(\lambda)$, kde $c_{11}(\lambda) = a_{11}(\lambda)$, $c_{1i}(\lambda) = 0$ pro všechna $i = 2, 3, \dots, n$ a $c_{ik}(\lambda) = a_{ik}(\lambda) - \alpha_k a_{i1}(\lambda)$. Dále, odečtením β_j-násobku prvního řádku od řádku j-tého pro $j = 2, 3, \dots, n$ dostaneme matici $\boldsymbol{D}(\lambda)$, kde $d_{11}(\lambda) = a_{11}(\lambda)$, všechny ostatní prvky v prvním řádku a prvním sloupci jsou nulové, $d_{1i}(\lambda) = d_{j1}(\lambda) = 0$, $i, j \in \{2, 3, \dots, n\}$, a $d_{ik}(\lambda) = c_{ik}(\lambda) = a_{ik}(\lambda) - \alpha_k a_{i1}(\lambda)$. Nyní přičtením i-tého řádku k řádku prvnímu dostaneme matici $\boldsymbol{F}(\lambda)$, kde $f_{11}(\lambda) = a_{11}(\lambda)$ a $f_{1k}(\lambda) = d_{ik}(\lambda) = a_{ik}(\lambda) - \alpha_k a_{i1}(\lambda)$. Protože podle předpokladu $a_{11}(\lambda) | a_{i1}(\lambda)$ a $a_{11}(\lambda) \nmid a_{ik}(\lambda)$, dostáváme pomocí poznámky 18.3 snadno, že $a_{11}(\lambda) \nmid f_{1k}(\lambda)$ a matici $\boldsymbol{B}(\lambda)$ dostaneme použitím kroku (a).

(d) Úplnou indukcí podle stupně n matice $\boldsymbol{A}(\lambda)$ nyní již důkaz snadno dokončíme. Pro $n = 1$ je tvrzení zřejmé. Předpokládejme tedy, že $n > 1$ a že pro $n-1$ již tvrzení platí. Dále můžeme předpokládat, že matice $\boldsymbol{A}(\lambda)$ je nenulová, neboť v opačném případě je tvrzení opět zřejmé. Nyní je patrné, že po konečném počtu použití kroku (c) dostaneme matici $\boldsymbol{C}(\lambda)$ takovou, že prvek $c_{11}(\lambda)$ dělí všechny prvky této matice. Podobně jako v důkazu předchozí části dostaneme odečtením vhodných násobků prvního řádku a prvního sloupce od řádků a sloupců ostatních matici

$$\boldsymbol{B}(\lambda) = \begin{pmatrix} b_{11}(\lambda), & 0, & \dots, & 0 \\ 0, & b_{22}(\lambda), & \dots, & b_{2n}(\lambda) \\ \dots & \dots & \dots & \dots \\ 0, & b_{n2}(\lambda), & \dots, & b_{nn}(\lambda) \end{pmatrix} = \begin{pmatrix} b_{11}(\lambda), & 0 \\ 0, & \boldsymbol{B}'(\lambda) \end{pmatrix}.$$

Podle indukčního předpokladu lze λ-matici $\boldsymbol{B}'(\lambda)$ konečným počtem elementárních transformací převést na kanonický tvar, tj. diagonální matici s diagonálními prvky $a_2(\lambda), \dots, a_n(\lambda)$, kde $a_i(\lambda) | a_{i+1}(\lambda)$ pro každé $i = 2, 3, \dots, n-1$. K dokončení důkazu si nyní stačí uvědomit, že prvek $a_1(\lambda) = b_{11}(\lambda) = c_{11}(\lambda)$ dělí $a_2(\lambda)$. Vzhledem k tomu, že polynom $c_{11}(\lambda)$ dělí všechny prvky matice $\boldsymbol{C}(\lambda)$, plyne z poznámky

18.3, že prvek $b_{11}(\lambda)$ dělí všechny prvky matice $\boldsymbol{B}'(\lambda)$. Z téhož důvodu dělí prvek $a_1(\lambda)$ prvek $a_2(\lambda)$. ■

18.5. Definice. Buď $\boldsymbol{A}(\lambda)$ čtvercová λ-matice stupně n nad tělesem T. Symbolem $D_k^{\boldsymbol{A}(\lambda)}$ označíme největšího společného dělitele všech subdeterminantů stupně k matice $\boldsymbol{A}(\lambda)$, $k = 1, 2, \dots, n$. Je-li $\boldsymbol{A} \in T_n$ čtvercová matice stupně n nad tělesem T, pak symbolem $D_k^{\boldsymbol{A}}(\lambda)$ označíme největšího společného dělitele všech subdeterminantů stupně k matice $\boldsymbol{A} - \lambda \boldsymbol{E}$, $k = 1, 2, \dots, n$.

18.6. Příklad. Uvažujme matici $\boldsymbol{A} = \begin{pmatrix} \lambda+1, & \lambda \\ \lambda+2, & \lambda+1 \end{pmatrix}$. Jest $\det \boldsymbol{A}(\lambda) = (\lambda + 1)^2 - \lambda(\lambda+2) = 1$, takže matice $\boldsymbol{A}(\lambda)$ je regulární (pro každé λ) a existuje k ní tudíž inverzní matice $(\boldsymbol{A}(\lambda))^{-1} = \begin{pmatrix} \lambda+1, & -\lambda \\ -\lambda-2, & \lambda+1 \end{pmatrix}$. V dalším budeme pod *regulární λ-maticí* rozumět takovou λ-matici $\boldsymbol{A}(\lambda)$, k níž existuje λ-matice inverzní, tj. taková λ-matice $(\boldsymbol{A}(\lambda))^{-1}$, pro kterou platí $\boldsymbol{A}(\lambda)(\boldsymbol{A}(\lambda))^{-1} = \boldsymbol{E}$.

18.7. Věta. *Buďte $\boldsymbol{A}(\lambda)$, $\boldsymbol{P}(\lambda)$, $\boldsymbol{Q}(\lambda)$ čtvercové λ-matice stupně n, $\boldsymbol{P}(\lambda)$, $\boldsymbol{Q}(\lambda)$ regulární. Označíme-li $\boldsymbol{B}(\lambda) = \boldsymbol{P}(\lambda)\boldsymbol{A}(\lambda)\boldsymbol{Q}(\lambda)$, pak $D_k^{\boldsymbol{A}(\lambda)} = D_k^{\boldsymbol{B}(\lambda)}$ pro každé $k = 1, 2, \dots, n$.*

Důkaz. Podle věty 4.10 jsou řádky matice $\boldsymbol{P}(\lambda)\boldsymbol{A}(\lambda)$ lineárními kombinacemi řádků matice $\boldsymbol{A}(\lambda)$. Je-li nyní $\boldsymbol{C}(\lambda)$ libovolná dílčí matice matice $\boldsymbol{P}(\lambda)\boldsymbol{A}(\lambda)$ stupně k, jejíž sloupce jsou obsaženy ve sloupcích $i_1 < i_2 < \dots < i_k$ matice $\boldsymbol{P}(\lambda)\boldsymbol{A}(\lambda)$, pak je patrné, že řádky matice $\boldsymbol{C}(\lambda)$ jsou lineárními kombinacemi vektorů, jejichž komponenty leží právě ve sloupcích $i_1, i_2, \dots, i_k$. Z vět 7.12 a 7.13 pak snadno plyne, že $\det \boldsymbol{C}(\lambda)$ je lineární kombinací subdeterminantů matice $\boldsymbol{A}(\lambda)$ stupně k. Z poznámky 18.3 nyní ihned vidíme, že každý společný dělitel všech subdeterminantů matice $\boldsymbol{A}(\lambda)$ stupně k dělí každý subdeterminant matice $\boldsymbol{P}(\lambda)\boldsymbol{A}(\lambda)$ stupně k, a tedy $D_k^{\boldsymbol{A}(\lambda)} | D_k^{\boldsymbol{P}(\lambda)\boldsymbol{A}(\lambda)}$. Provedeme-li stejnou úvahu na matice $\boldsymbol{P}(\lambda)\boldsymbol{A}(\lambda)$ a $(\boldsymbol{P}(\lambda))^{-1}\boldsymbol{P}(\lambda)\boldsymbol{A}(\lambda) = \boldsymbol{A}(\lambda)$, dostaneme $D_k^{\boldsymbol{P}(\lambda)\boldsymbol{A}(\lambda)} | D_k^{\boldsymbol{A}(\lambda)}$, a tedy $D_k^{\boldsymbol{A}(\lambda)} || D_k^{\boldsymbol{P}(\lambda)\boldsymbol{A}(\lambda)}$. Zcela analogickou úvahou pro sloupce namísto řádků dostaneme $D_k^{\boldsymbol{P}(\lambda)\boldsymbol{A}(\lambda)} || D_k^{\boldsymbol{B}(\lambda)}$, odkud již tvrzení bezprostředně plyne. ■

18.8. Věta. *Nechť $\boldsymbol{A}(\lambda)$ je čtvercová λ-matice stupně n nad tělesem T. Potom $D_k^{\boldsymbol{A}(\lambda)} | D_{k+1}^{\boldsymbol{A}(\lambda)}$ pro každé $k = 1, 2, \dots, n-1$.*

Důkaz. Buď $\boldsymbol{B}(\lambda)$ libovolná čtvercová dílčí matice stupně $k+1$ matice $\boldsymbol{A}(\lambda)$. Označíme-li $b_1(\lambda), b_2(\lambda), \dots, b_{k+1}(\lambda)$ prvky prvního řádku matice $\boldsymbol{B}(\lambda)$ a $\boldsymbol{B}_1(\lambda)$, $\boldsymbol{B}_2(\lambda), \dots, \boldsymbol{B}_{k+1}(\lambda)$ jejich algebraické doplňky v matici $\boldsymbol{B}(\lambda)$, pak rozvojem podle prvního řádku dostaneme $\det \boldsymbol{B}(\lambda) = \sum_{i=1}^{k+1} b_i(\lambda)\boldsymbol{B}_i(\lambda)$. Protože $D_k^{\boldsymbol{A}(\lambda)} | \boldsymbol{B}_i(\lambda)$ pro každé $i = 1, 2, \dots, k+1$, plyne z definice největšího společného dělitele 16.24 ihned, že $D_k^{\boldsymbol{A}(\lambda)} | D_{k+1}^{\boldsymbol{A}(\lambda)}$, což jsme chtěli dokázat. ■

18.9. Věta. *Buď $\boldsymbol{B} = \boldsymbol{B}(\lambda_0)$ Jordanova buňka stupně n příslušná prvku $\lambda_0 \in T$. Pak $D_n^{\boldsymbol{B}}(\lambda) = (\lambda_0 - \lambda)^n$ a $D_k^{\boldsymbol{B}}(\lambda) = 1$ pro všechna $k = 1, 2, \dots, n-1$.*

Důkaz. Předně $D_n^{\boldsymbol{B}}(\lambda) = \det(\boldsymbol{B} - \lambda\boldsymbol{E}) = (\lambda_0 - \lambda)^n$ vzhledem k tomu, že matice $\boldsymbol{B} - \lambda\boldsymbol{E}$ má následující tvar

$$B - \lambda E = \begin{pmatrix} \lambda_0 - \lambda, & 1, & 0, & \dots, & 0, & 0 \\ 0, & \lambda_0 - \lambda, & 1, & \dots, & 0, & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0, & 0, & 0, & \dots, & \lambda_0 - \lambda, & 1 \\ 0, & 0, & 0, & \dots, & 0, & \lambda_0 - \lambda \end{pmatrix}.$$

Vynecháním prvního sloupce a posledního řádku dostaneme dílčí matici stupně $n-1$, jejíž determinant je zřejmě roven 1, takže $D^B_{n-1}(\lambda) = 1$. Jelikož zřejmě $D^B_1(\lambda) = 1$, plyne z předchozí věty ihned, že $D^B_1(\lambda) = D^B_2(\lambda) = \dots = D^B_{n-1}(\lambda) = 1$. ∎

18.10. Věta. *Buď B Jordanova matice mající*
s_1 Jordanových buněk příslušných prvku $\lambda_1 \in T$ řádů $n^1_1 \geq n^1_2 \geq \dots \geq n^1_{s_1}$,
s_2 Jordanových buněk příslušných prvku $\lambda_2 \in T$ řádů $n^2_1 \geq n^2_2 \geq \dots \geq n^2_{s_2}$,
....
s_k Jordanových buněk příslušných prvku $\lambda_k \in T$ řádů $n^k_1 \geq n^k_2 \geq \dots \geq n^k_{s_k}$.
Pak platí

$$D^B_n(\lambda) = (\lambda_1 - \lambda)^{\sum_{i=1}^{s_1} n^1_i} \cdot (\lambda_2 - \lambda)^{\sum_{i=1}^{s_2} n^2_i} \dots (\lambda_k - \lambda)^{\sum_{i=1}^{s_k} n^k_i},$$

$$D^B_{n-l}(\lambda) = (\lambda_1 - \lambda)^{\sum_{i=l+1}^{s_1} n^1_i} \cdot (\lambda_2 - \lambda)^{\sum_{i=l+1}^{s_2} n^2_i} \dots (\lambda_k - \lambda)^{\sum_{i=l+1}^{s_k} n^k_i},$$

$l = 1, 2, \dots, n-1$, kde klademe $\sum_{i=j}^{k} n^r_i = 0$ kdykoliv $k < j$.

Důkaz. Z věty 18.1 úplnou indukcí snadno plyne, že $\det(B - \lambda E)$ je součinem determinantů $\det(B_i - \lambda E)$, kde B_i jsou jednotlivé Jordanovy buňky matice B, takže výraz pro $D^B_n(\lambda)$ plyne ihned z předchozí věty.

Buď tedy $l > 0$. Protože podle věty 18.8 (a poznámky 18.3) $D^B_{n-l}(\lambda) | D^B_n(\lambda)$ a polynomy $\lambda_i - \lambda$, $i = 1, 2, \dots, k$, jsou zřejmě ireducibilní, plyne z věty 16.26, že $D^B_{n-l}(\lambda)$ je součinem mocnin polynomů $\lambda_i - \lambda$, $i = 1, 2, \dots, k$. Naším úkolem je tedy zjistit, jaká nejmenší mocnina jednotlivých $\lambda_i - \lambda$, $i = 1, 2, \dots, k$, se může vyskytnout v subdeterminantech stupně $n - l$ matice $B - \lambda E$. Každý takový subdeterminant vznikne vynecháním l řádků a l sloupců. V důkazu předchozí věty jsme viděli, že vynecháme-li v Jordanově buňce první sloupec a poslední řádek, je příslušný subdeterminant roven 1. Vynecháme-li tedy příslušné sloupce a řádky v Jordanových buňkách řádů $n^i_1, n^i_2, \dots, n^i_l$, $i = 1, 2, \dots, k$, dostaneme pomocí věty 18.1 snadno dokazovanou rovnost. ∎

18.11. Definice. Buď $A(\lambda)$ čtvercová λ-matice stupně n nad tělesem T. *Invariantními faktory matice* $A(\lambda)$ nazýváme výrazy $E^{A(\lambda)}_k = \frac{D^{A(\lambda)}_k}{D^{A(\lambda)}_{k-1}}$, $k = 1, 2, \dots, n$, kde klademe $D^{A(\lambda)}_0 = 1$. Je-li $A \in T_n$ čtvercová matice stupně n nad tělesem T, pak *invariantními faktory matice* A rozumíme invariantní faktory λ-matice $A - \lambda E$, tj. $E^A_k(\lambda) = \frac{D^A_k(\lambda)}{D^A_{k-1}(\lambda)}$, $D^A_0(\lambda) = 1$.

18.12. Věta. *Buďte* $\boldsymbol{A}(\lambda), \boldsymbol{P}(\lambda), \boldsymbol{Q}(\lambda)$ *čtvercové* λ*-matice stupně* n*,* $\boldsymbol{P}(\lambda), \boldsymbol{Q}(\lambda)$ *regulární. Označíme-li* $\boldsymbol{B}(\lambda) = \boldsymbol{P}(\lambda)\boldsymbol{A}(\lambda)\boldsymbol{Q}(\lambda)$*, pak matice* $\boldsymbol{A}(\lambda)$ *a* $\boldsymbol{B}(\lambda)$ *mají stejné invariantní faktory.*

Důkaz. Tvrzení plyne okamžitě z věty 18.7. ■

18.13. Věta. *Podobné matice mají stejné invariantní faktory.*

Důkaz. Buďte $\boldsymbol{A}, \boldsymbol{C}$ čtvercové matice stupně n nad tělesem T, $\boldsymbol{C}$ regulární. Položíme-li $\boldsymbol{B} = \boldsymbol{C}^{-1}\boldsymbol{A}\boldsymbol{C}$, je $\boldsymbol{B} - \lambda\boldsymbol{E} = \boldsymbol{C}^{-1}\boldsymbol{A}\boldsymbol{C} - \lambda\boldsymbol{E} = \boldsymbol{C}^{-1}(\boldsymbol{A} - \lambda\boldsymbol{E})\boldsymbol{C}$ a stačí použít předchozí větu. ■

18.14. Věta. *Buď* $\boldsymbol{B}$ *Jordanova matice z věty 18.10. Pak pro každé* $l = 0, 1, \ldots, n-1$ *je* $E^B_{n-l}(\lambda) = (\lambda_1 - \lambda)^{n^1_{l+1}} \cdot (\lambda_2 - \lambda)^{n^2_{l+1}} \cdot \ldots \cdot (\lambda_k - \lambda)^{n^k_{l+1}}$*, kde klademe* $n^j_i = 0$ *pro* $i > s_j$*.*

Důkaz. Plyne bezprostředně z věty 18.10. ■

18.15. Poznámka. V důsledku 17.9 jsme viděli, že každá čtvercová matice nad algebraicky uzavřeným tělesem je podobná Jordanově matici. Toto tvrzení neplatí nad obecným, ne algebraicky uzavřeným tělesem, jak si ukážeme v příkladu 18.18. Pro zjednodušení vyjadřování budeme do konce tohoto článku říkat, že matice $\boldsymbol{A}$ má Jordanovu matici místo toho, že matice $\boldsymbol{A}$ je podobná Jordanově matici. Skutečnost, že matice $\boldsymbol{A}$ a $\boldsymbol{B}$ jsou podobné, budeme pro stručnost značit symbolem $\boldsymbol{A} \sim \boldsymbol{B}$.

18.16. Věta. *Buď* $\boldsymbol{A}$ *čtvercová matice stupně* n *nad tělesem* T*. Jestliže* $\boldsymbol{A}$ *má Jordanovu matici* $J(\boldsymbol{A})$*, pak matice* $J(\boldsymbol{A})$ *je až na pořadí buněk určena jednoznačně.*

Důkaz. Protože $\boldsymbol{A} \sim J(\boldsymbol{A})$, mají matice $\boldsymbol{A}$ a $J(\boldsymbol{A})$ stejné invariantní faktory podle věty 18.13. Z věty 18.14 však vyplývá, že invariantní faktory matice $J(\boldsymbol{A})$ jsou jednoznačně určeny stupni jednotlivých Jordanových buněk. ■

18.17. Metoda pro nalezení Jordanovy matice.

Buď $\boldsymbol{A} \in T_n$ čtvercová matice stupně n nad tělesem T mající Jordanovu matici $J(\boldsymbol{A})$. Podle věty 18.13 mají matice $\boldsymbol{A}$ a $J(\boldsymbol{A})$ stejné invariantní faktory, takže potřebujeme nalézt invariantní faktory λ-matice $\boldsymbol{A} - \lambda\boldsymbol{E}$. Podle věty 18.4 lze matici $\boldsymbol{A} - \lambda\boldsymbol{E}$ převést konečným počtem elementárních transformací na řádky a sloupce na kanonický tvar

$$\boldsymbol{A}(\lambda) = \begin{pmatrix} a_1(\lambda), & 0, & \ldots, & 0 \\ 0, & a_2(\lambda), & \ldots, & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0, & 0, & \ldots, & a_n(\lambda) \end{pmatrix},$$

kde $a_i(\lambda) | a_{i+1}(\lambda)$ pro každé $i = 1, 2, \ldots, n-1$. Protože provádění elementárních transformací na řádky (sloupce) matice znamená podle věty 8.8 násobení zleva (zprava) regulární maticí dané transformace, je $\boldsymbol{A}(\lambda) = \boldsymbol{P}(\lambda)(\boldsymbol{A} - \lambda\boldsymbol{E})\boldsymbol{Q}(\lambda)$ pro nějaké regulární čtvercové λ-matice stupně n. Podle věty 18.12 mají tedy matice $\boldsymbol{A} - \lambda\boldsymbol{E}$ a $\boldsymbol{A}(\lambda)$ stejné invariantní faktory. Z vlastností kanonického tvaru a z definice 18.5 snadno dostáváme, že

$D^A_1(\lambda) = a_1(\lambda)$,

$$D_2^A(\lambda) = a_1(\lambda)a_2(\lambda),$$
$$\dots\dots\dots\dots\dots\dots\dots\dots$$
$$D_k^A(\lambda) = a_1(\lambda)a_2(\lambda)\dots a_k(\lambda),$$
$$\dots\dots\dots\dots\dots\dots\dots\dots$$
$$D_n^A(\lambda) = a_1(\lambda)a_2(\lambda)\dots a_n(\lambda),$$

takže $E_k^A(\lambda) = a_k(\lambda)$ pro každé $k = 1, 2, \dots, n$. Z věty 18.14 pak snadno dostaneme jednotlivé Jordanovy buňky, a tedy i Jordanovu matici $\boldsymbol{J}(\boldsymbol{A})$ matice $\boldsymbol{A}$.

18.18. Příklad. Buď

$$\boldsymbol{A} = \begin{pmatrix} 3, & -1, & 0 \\ 6, & -3, & 2 \\ 8, & -6, & 5 \end{pmatrix}$$

čtvercová matice stupně 3 nad tělesem reálných čísel R. Ukážeme, že matice $\boldsymbol{A}$ nemá nad R Jordanovu matici. Nad tělesem K komplexních čísel má $\boldsymbol{A}$ Jordanovu matici podle důsledku 16.9. Matici $J(\boldsymbol{A})$ nalezneme metodou z předchozího odstavce. Jest

$$\boldsymbol{A} - \lambda\boldsymbol{E} = \begin{pmatrix} 3-\lambda, & -1, & 0 \\ 6, & -3-\lambda, & 2 \\ 8, & -6, & 5-\lambda \end{pmatrix} \sim \begin{pmatrix} -1, & 3-\lambda, & 0 \\ -3-\lambda, & 6, & 2 \\ -6, & 8, & 5-\lambda \end{pmatrix} \sim$$

$$\begin{pmatrix} -1, & 0, & 0 \\ -3-\lambda, & \lambda^2-3, & 2 \\ -6, & 6\lambda-10, & 5-\lambda \end{pmatrix} \sim \begin{pmatrix} 1, & 0, & 0 \\ 0, & \lambda^2-3, & 2 \\ 0, & 6\lambda-10, & 5-\lambda \end{pmatrix} \sim$$

$$\begin{pmatrix} 1, & 0, & 0 \\ 0, & 2, & \lambda^2-3 \\ 0, & 5-\lambda, & 6\lambda-10 \end{pmatrix} \sim \begin{pmatrix} 1, & 0, & 0 \\ 0, & 2, & \lambda^2-3 \\ 0, & 0, & \lambda^3-5\lambda^2+9\lambda-5 \end{pmatrix} \sim$$

$$\begin{pmatrix} 1, & 0, & 0 \\ 0, & 1, & 0 \\ 0, & 0, & (\lambda-1)(\lambda^2-4\lambda+5) \end{pmatrix}.$$

Vidíme tedy, že $a_3(\lambda) = (\lambda-1)(\lambda-(2+i))(\lambda-(2-i))$, takže Jordanova matice $J(\boldsymbol{A})$ matice $\boldsymbol{A}$ nad tělesem komplexních čísel je

$$J(\boldsymbol{A}) = \begin{pmatrix} 1, & 0, & 0 \\ 0, & 2+i, & 0 \\ 0, & 0, & 2-i \end{pmatrix}.$$

Předpokládejme nyní, že matice $\boldsymbol{A}$ má Jordanovu matici $\widetilde{J}(\boldsymbol{A})$ nad tělesem reálných čísel R. Existuje tedy regulární matice $\boldsymbol{C} \in R_3$ taková, že $\widetilde{J}(\boldsymbol{A}) = \boldsymbol{C}^{-1}\boldsymbol{A}\boldsymbol{C}$. Protože těleso reálných čísel R je podtělesem tělesa komplexních čísel K, je $\widetilde{J}(\boldsymbol{A})$ Jordanova matice nad K, a je to tudíž Jordanova matice matice $\boldsymbol{A}$ nad K vzhledem k tomu, že $\widetilde{J}(\boldsymbol{A}) \sim \boldsymbol{A}$. Podle věty 18.16 o jednoznačnosti Jordanovy matice se matice $J(\boldsymbol{A})$ a $\widetilde{J}(\boldsymbol{A})$ mohou lišit pouze pořadím diagonálních prvků. To je však spor, protože $J(\boldsymbol{A})$ není matice nad R, a tedy $\boldsymbol{A}$ nemá Jordanovu matici nad R.

18.19. Lemma. *Buď $\boldsymbol{B}$ čtvercová matice stupně n nad tělesem T, která vznikne z matice $\boldsymbol{A}$ vzájemnou výměnou i-tého a j-tého řádku, $i \neq j$. Pak existuje čtvercová matice $\boldsymbol{C}$ stupně n taková, že $\boldsymbol{B} = \boldsymbol{C}\boldsymbol{A}$, přičemž $\boldsymbol{C}^2 = \boldsymbol{E}$. Speciálně je tedy matice $\boldsymbol{C}$ regulární a $\boldsymbol{C}^{-1} = \boldsymbol{C}$.*

Důkaz. Bez újmy na obecnosti můžeme předpokládat, že $i < j$. Snadno se ověří, že matice

$$\boldsymbol{C} = \begin{pmatrix} 1, & 0, & \dots, & 0, & \dots, & 0, & \dots, & 0, & 0 \\ 0, & 1, & \dots, & 0, & \dots, & 0, & \dots, & 0, & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0, & 0, & \dots, & 0, & \dots, & 1, & \dots, & 0, & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0, & 0, & \dots, & 1, & \dots, & 0, & \dots, & 0, & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & ,0, & \dots, & 0, & \dots, & 0, & \dots, & 0, & 1 \end{pmatrix},$$

kde $c_{11} = c_{22} = \cdots = c_{i-1,i-1} = c_{i+1,i+1} = \cdots = c_{nn} = c_{ij} = c_{ji} = 1$ a ostatní prvky matice matice $\boldsymbol{C}$ jsou rovny 0, má všechny požadované vlastnosti. ∎

18.20. Věta. *Nechť $\boldsymbol{A}, \boldsymbol{B}$ jsou čtvercové matice stupně n nad tělesem T mající Jordanovu matici. Pak matice $\boldsymbol{A}$ a $\boldsymbol{B}$ jsou podobné, právě když mají stejné invariantní faktory.*

Důkaz. Podobné matice mají stejné invariantní faktory podle věty 18.13. Jestliže tedy naopak matice $\boldsymbol{A}$ a $\boldsymbol{B}$ mají stejné invariantní faktory, pak Jordanovy matice $J(\boldsymbol{A})$ a $J(\boldsymbol{B})$ mají stejné invariantní faktory opět podle věty 18.13 vzhledem k tomu, že $\boldsymbol{A} \sim J(\boldsymbol{A})$, $\boldsymbol{B} \sim J(\boldsymbol{B})$. Z věty 18.14 nyní plyne, že matice $J(\boldsymbol{A})$ a $J(\boldsymbol{B})$ jsou až na pořadí Jordanových buněk stejné. Několikanásobným použitím předchozího lemmatu snadno zjistíme, že $J(\boldsymbol{A}) = \boldsymbol{C}J(\boldsymbol{B})\boldsymbol{C} = \boldsymbol{C}^{-1}J(\boldsymbol{B})\boldsymbol{C}$ pro vhodnou matici $\boldsymbol{C}$ takovou, že $\boldsymbol{C}^2 = \boldsymbol{E}$, takže $J(\boldsymbol{A}) \sim J(\boldsymbol{B})$, odkud snadno plyne podobnost matic $\boldsymbol{A}$ a $\boldsymbol{B}$. ∎

18.21. Věta. *Buď $\boldsymbol{A}$ čtvercová matice stupně n nad tělesem T mající Jordanovu matici. Pak matice $\boldsymbol{A}$ je podobná diagonální matici, právě když invariantní faktory matice $\boldsymbol{A}$ mají vesměs jednoduché kořeny.*

Důkaz. Buď nejprve matice $\boldsymbol{A}$ podobná diagonální matici $\boldsymbol{D}$. Podle věty 18.13 mají matice $\boldsymbol{A}$ a $\boldsymbol{D}$ stejné invariantní faktory. Protože $\boldsymbol{D}$ je Jordanova matice, jejíž Jordanovy buňky mají všechny stupeň 1, plyne z věty 18.14, že invariantní faktory matice $\boldsymbol{D}$, a tedy i matice $\boldsymbol{A}$, mají vesměs jednoduché kořeny. Naopak, jestliže invariantní faktory matice $\boldsymbol{A}$ mají vesměs jednoduché kořeny, má stejnou vlastnost podle věty 18.13 i matice $J(\boldsymbol{A})$. Z věty 18.14 nyní plyne, že všechny Jordanovy buňky matice $J(\boldsymbol{A})$ jsou stupně 1, a matice $J(\boldsymbol{A}) \sim \boldsymbol{A}$ je tudíž diagonální. ∎

18.22. Důsledek. *Buď T algebraicky uzavřené těleso (speciálně těleso K komplexních čísel), $\boldsymbol{A}, \boldsymbol{B}$ buďte čtvercové matice stupně n nad tělesem T. Pak*

(i) matice $\boldsymbol{A}$ má až na pořadí Jordanových buněk jednoznačně určenou Jordanovu matici;

(ii) matice $\boldsymbol{A}$ a $\boldsymbol{B}$ jsou podobné, právě když mají stejné invariantní faktory;

(iii) matice $\boldsymbol{A}$ je podobná diagonální matici, právě když její invariantní faktory mají vesměs jednoduché kořeny.

Důkaz. (i) Matice $\boldsymbol{A}$ má Jordanovu matici podle důsledku 16.9, a to jedinou až na pořadí Jordanových buněk podle věty 18.16.

(ii) Podle (i) a věty 18.20.

(iii) Podle (i) a věty 18.21. ∎

18.23. Příklad. Najděme Jordanovu matici čtvercové matice $\boldsymbol{A} \in R_6$, jestliže

$$\boldsymbol{A} = \begin{pmatrix} 0, & 3, & -1, & 1, & 0, & -1 \\ 0, & 3, & -1, & 1, & 0, & -1 \\ 0, & 1, & 1, & 1, & 0, & -1 \\ 0, & 0, & 0, & 3, & 0, & -1 \\ 0, & 0, & 0, & 1, & 2, & -1 \\ 0, & 0, & 0, & 0, & 1, & 1 \end{pmatrix}.$$

Ř e š e n í : Nejprve převedeme λ-matici

$$\boldsymbol{A} - \lambda \boldsymbol{E} = \begin{pmatrix} -\lambda, & 3, & -1, & 1, & 0, & -1 \\ 0, & 3-\lambda, & -1, & 1, & 0, & -1 \\ 0, & 1, & 1-\lambda, & 1, & 0, & -1 \\ 0, & 0, & 0, & 3-\lambda, & 0, & -1 \\ 0, & 0, & 0, & 1, & 2-\lambda, & -1 \\ 0, & 0, & 0, & 0, & 1, & 1-\lambda \end{pmatrix}$$

na kanonický tvar. Vyměníme vzájemně 1. a 4. sloupec, přičteme vhodné násobky prvního řádku k ostatním, pak vhodné násobky prvního sloupce k ostatním, čímž dostaneme matici

$$\begin{pmatrix} 1, & 0, & 0, & 0, & 0, & 0 \\ 0, & -\lambda, & 0, & \lambda, & 0, & 0 \\ 0, & -2, & 2-\lambda, & \lambda, & 0, & 0 \\ 0, & 3\lambda-9, & 3-\lambda, & 3\lambda-\lambda^2, & 0, & 2-\lambda \\ 0, & -3, & 1, & \lambda, & 2-\lambda, & 0 \\ 0, & 0, & 0, & 0, & 1, & 1-\lambda \end{pmatrix}.$$

Provedeme nejprve vzájemnou výměnu 2. a 6. řádku, potom 2. a 5. sloupce, odečteme vhodné násobky 2. řádku a 2. sloupce od ostatních a získáme matici

$$\begin{pmatrix} 1, & 0, & 0, & 0, & 0, & 0 \\ 0, & 1, & 0, & 0, & 0, & 0 \\ 0, & 0, & 2-\lambda, & \lambda, & -2, & 0 \\ 0, & 0, & 3-\lambda, & 3\lambda-\lambda^2, & 3\lambda-9, & 2-\lambda \\ 0, & 0, & 1, & \lambda, & -3, & (2-\lambda)(\lambda-1) \\ 0, & 0, & 0, & \lambda, & -\lambda, & 0 \end{pmatrix}.$$

Podobně vzájemnou výměnou 3. a 5. řádku po příslušných úpravách dostaneme matici

$$\begin{pmatrix} 1, & 0, & 0, & 0, & 0, & 0 \\ 0, & 1, & 0, & 0, & 0, & 0 \\ 0, & 0, & 1, & 0, & 0, & 0 \\ 0, & 0, & 0, & 0, & 0, & (2-\lambda)^3 \\ 0, & 0, & 0, & \lambda(\lambda-1), & -3\lambda+4, & (\lambda-2)^2(1-\lambda) \\ 0, & 0, & 0, & \lambda, & -\lambda, & 0 \end{pmatrix}.$$

Nyní odečteme trojnásobek posledního řádku od předposledního, provedeme vzájemnou výměnu 4. a 5. řádku a poté 4. a 5. sloupce a po příslušných úpravách dostaneme

$$\begin{pmatrix} 1, & 0, & 0, & 0, & 0, & 0 \\ 0, & 1, & 0, & 0, & 0, & 0 \\ 0, & 0, & 1, & 0, & 0, & 0 \\ 0, & 0, & 0, & 1, & 0, & 0 \\ 0, & 0, & 0, & 0, & 0, & (2-\lambda)^3 \\ 0, & 0, & 0, & 0, & \lambda(\lambda-2)^2, & \lambda(\lambda-2)^2(1-\lambda) \end{pmatrix}.$$

Vzhledem ke tvaru matice je nyní patrné, že se stačí omezit na úpravy λ-matice stupně 2 v pravém dolním rohu. Provedeme postupně tyto úpravy: $(\lambda-1)$-násobek prvního sloupce přičteme k druhému, vyměníme vzájemně řádky, vynásobíme druhý řádek -1 a přičteme k prvnímu, odečteme první sloupec od druhého, $\frac{\lambda}{2}$-násobek druhého sloupce přičteme k prvnímu, první řádek vydělíme -2, odečteme $(\lambda-2)$-násobek od druhého a druhý řádek vynásobíme 2 a konečně vyměníme sloupce. Jest

$$\begin{pmatrix} 0, & (2-\lambda)^3 \\ \lambda(\lambda-2)^2, & \lambda(\lambda-2)^2(1-\lambda) \end{pmatrix} \sim \begin{pmatrix} 0, & (2-\lambda)^3 \\ \lambda(\lambda-2)^2, & 0 \end{pmatrix} \sim$$

$$\begin{pmatrix} \lambda(\lambda-2)^2, & (\lambda-2)^3 \\ 0, & (\lambda-2)^3 \end{pmatrix} \sim \begin{pmatrix} \lambda(\lambda-2)^2, & -2(\lambda-2)^2 \\ 0, & (\lambda-2)^3 \end{pmatrix} \sim$$

$$\begin{pmatrix} 0, & -2(\lambda-2)^2 \\ \frac{\lambda}{2}(\lambda-2)^3, & (\lambda-2)^3 \end{pmatrix} \sim \begin{pmatrix} 0, & (\lambda-2)^2 \\ \lambda(\lambda-2)^3, & 0 \end{pmatrix} \sim \begin{pmatrix} (\lambda-2)^2, & 0 \\ 0, & \lambda(\lambda-2)^3 \end{pmatrix}.$$

Celkem tedy vidíme, že matice $\boldsymbol{A}$ má invariantní faktory $1, 1, 1, 1, (\lambda-2)^2, \lambda(\lambda-2)^3$, takže podle věty 18.14 je podobná Jordanově matici

$$J(\boldsymbol{A}) = \begin{pmatrix} 2, & 1, & 0, & 0, & 0, & 0 \\ 0, & 2, & 1, & 0, & 0, & 0 \\ 0, & 0, & 2, & 0, & 0, & 0 \\ 0, & 0, & 0, & 2, & 1, & 0 \\ 0, & 0, & 0, & 0, & 2, & 0 \\ 0, & 0, & 0, & 0, & 0, & 0, \end{pmatrix}.$$

19. Afinní prostor

Ve zbývajících kapitolách těchto skript se budeme věnovat některým geometrickým aplikacím lineární algebry. Začneme s nejjednodušší takovou geometrickou strukturou, s afinním prostorem. Idea tohoto pojmu spočívá na prostém faktu, že dva body určují jednoznačně vektor a naopak, „umístíme-li" vektor do daného bodu, dostaneme jednoznačně určený „koncový" bod.

19.1. Definice. *Afinním prostorem* $A = A(V)$ nad vektorovým prostorem V (nad tělesem T) rozumíme trojici (A, V, f), kde A je neprázdná množina a $f : A \times V \to A$ je zobrazení splňující tyto dvě podmínky:

(a) $f(a, 0) = a$, $f(f(a, \boldsymbol{u}), \boldsymbol{v}) = f(a, \boldsymbol{u} + \boldsymbol{v})$ pro všechna $a \in A$ a $\boldsymbol{u}, \boldsymbol{v} \in V$;

(b) ke každé dvojici prvků $a, b \in A$ existuje právě jeden vektor $\boldsymbol{u} \in V$ tak, že $f(a, \boldsymbol{u}) = b$.

Dimenzí afinního prostoru $A(V)$ rozumíme dimenzi příslušného vektorového prostoru V, místo $A(V_n)$ budeme často používat kratší zápis A_n. Prvky množiny A se nazývají *body* příslušného afinního prostoru.

19.2. Poznámka. Afinní prostor jsme definovali jako trojici (A, V, f). Protože jak zobrazení f, tak vektorový prostor V bývají zpravidla pevně dány, používáme pro afinní prostor zkrácené označení A. V některých případech, zejména u zobrazení mezi afinními prostory, kde se mohou vyskytovat různé vektorové prostory (nad týmž tělesem, pochopitelně), pak používáme označení $A(V)$. Dále, zápis a vlastnosti zobrazení f jsou dosti těžkopádně zapisovatelné, a proto budeme místo $f(a, \boldsymbol{u})$ psát krátce $a + \boldsymbol{u}$. Při tomto způsobu zápisu dostávají podmínky (a),(b) z předchozí definice tento tvar:

(a) $a + 0 = a$, $(a + \boldsymbol{u}) + \boldsymbol{v} = a + (\boldsymbol{u} + \boldsymbol{v})$ pro všechna $a \in A$ a $\boldsymbol{u}, \boldsymbol{v} \in V$;

(b) ke každé dvojici bodů $a, b \in A$ existuje právě jeden vektor $\boldsymbol{u} \in V$ tak, že $a + \boldsymbol{u} = b$. Pro tento jednoznačně určený vektor $\boldsymbol{u}$ můžeme tedy zvolit zápis $\boldsymbol{u} = b - a$.

Přirozenost tohoto zápisu vysvitne z tohoto jednoduchého příkladu. Pro $A = V = R^2$, kde R značí jako obvykle těleso reálných čísel, snadno ověříme, že zobrazení $f(a, \boldsymbol{u}) = a + \boldsymbol{u}$ definuje na množině A strukturu afinního prostoru. Přitom $a + \boldsymbol{u}$ značí obvyklé sčítání v aritmetickém vektorovém prostoru R^2. Podmínky (a) a (b) v tomto případě neříkají nic jiného než vlastnost nulového vektoru, asociativní zákon pro sčítání a vlastnost opačného vektoru. Takže např. pro $a = (3, 5)$, $b = (7, 1)$, $\boldsymbol{u} = (4, 2)$ máme $a + \boldsymbol{u} = (7, 7)$ a $b - a = (4, -4)$.

19.3. Definice. Říkáme, že afinní prostor (B, W, f_B) je *podprostorem* afinního prostoru (A, V, f_A), jestliže B je neprázdná podmnožina množiny A, W je podprostor vektorového prostoru V a f_B je restrikce zobrazení f_A na množinu $B \times W$, tj. $B \subseteq A$, $W \leq V$ a $f_B = f_A | (B \times W)$.

19.4. Věta. *Afinní prostor $B(W)$ je podprostorem afinního prostoru $A(V)$, právě když pro každé dva body $a, b \in B$ a každý vektor $\boldsymbol{u} \in W$ je $a + \boldsymbol{u} \in B$ a $b - a \in W$.*

Důkaz. Zřejmé. ■

19.5. Příklad. Podobně jako v poznámce 19.2 vezměme $A_n = V = T^n$ a buď f obvyklé sčítání vektorů v T^n. Čtenář snadno sám ověří, že $A_n(T^n)$ je afinní prostor dimenze n nad T^n. Je-li $W \leq T^n$ libovolný podprostor a $a \in A_n$ libovolný bod, pak množina $B = a + W = \{a + \boldsymbol{w} | \boldsymbol{w} \in W\}$ je podprostor afinního prostoru A_n. Skutečně, jsou-li $b = a + \boldsymbol{w}_1$, $c = a + \boldsymbol{w}_2$ libovolné body z B a $\boldsymbol{w} \in W$ je libovolný vektor, je $b + \boldsymbol{w} = a + (\boldsymbol{w}_1 + \boldsymbol{w}) \in B$, $c - b = a + \boldsymbol{w}_2 - a + \boldsymbol{w}_1 = \boldsymbol{w}_2 - \boldsymbol{w}_1 \in W$ a stačí použít předchozí větu.

V následující části ukážeme, že tento příklad je pro podprostory typický, tj. že každý podprostor v obecném afinním prostoru je tohoto tvaru. K tomu však potřebujeme následující spíše technické, leč užitečné lemma.

19.6. Lemma. *Buď $A(V)$ afinní prostor, $a, b, c, d \in A$ libovolné body a $\boldsymbol{u}, \boldsymbol{v} \in V$ libovolné vektory. Pak platí*

(i) $(a + \boldsymbol{u}) - (b + \boldsymbol{v}) = (a - b) + \boldsymbol{u} - \boldsymbol{v}$;

(ii) $(a - b) + (b - c) = a - c$;

(iii) $(a - b) + (c - d) = (a - d) + (c - b)$.

Důkaz. (i) Označíme-li $\boldsymbol{w} = (a+\boldsymbol{u}) - (b+\boldsymbol{v})$, je $a + \boldsymbol{u} = (b+\boldsymbol{v}) + \boldsymbol{w} = b + (\boldsymbol{v} + \boldsymbol{w})$, takže $a = (a + \boldsymbol{u}) - \boldsymbol{u} = b + (\boldsymbol{v} + \boldsymbol{w} - \boldsymbol{u})$, odkud $a - b = \boldsymbol{v} + \boldsymbol{w} - \boldsymbol{u}$. a tedy $\boldsymbol{w} = (a - b) + \boldsymbol{u} - \boldsymbol{v}$.

(ii) Označme $\boldsymbol{u} = a - b$ a $\boldsymbol{v} = b - c$. Pak $a = b + \boldsymbol{u}$ a $b = c + \boldsymbol{v}$, a tedy po dosazení $a = c + (\boldsymbol{u} + \boldsymbol{v})$, odkud $a - c = \boldsymbol{u} + \boldsymbol{v}$.

(iii) Označme $\boldsymbol{u} = a - b$, $\boldsymbol{v} = c - d$ a ukažme, že vektor na pravé straně dokazované rovnosti je právě $\boldsymbol{u} + \boldsymbol{v}$. Podle (i) a (ii) máme $(a - d) + (c - b) = ((b + \boldsymbol{u}) - d) + ((d + \boldsymbol{v}) - b) = (b - d) + \boldsymbol{u} + (d - b) + \boldsymbol{v} = \boldsymbol{u} + \boldsymbol{v}$.

∎

19.7. Věta. *Buď $A(V)$ afinní prostor, W podprostor vektorového prostoru V a $a \in A$ libovolný bod. Pak $B(W)$, kde $B = \{b \in A | b = a + \boldsymbol{u},\ \boldsymbol{u} \in W\}$ je podprostor afinního prostoru $A(V)$. Obráceně, je-li $B(W)$ podprostor prostoru $A(V)$ a $a \in B$ je libovolný bod, pak $B = \{b \in A | b = a + \boldsymbol{u},\ \boldsymbol{u} \in W\}$.*

Speciálně je $A = \{b \in A | b = a + \boldsymbol{u},\ \boldsymbol{u} \in V\}$ pro libovolný bod $a \in A$.

Důkaz. Nejprve ukažme, že $B(W)$, kde $B = \{b \in A | b = a + \boldsymbol{u},\ \boldsymbol{u} \in W\}$ je podprostor afinního prostoru $A(V)$. Jsou-li $a + \boldsymbol{u}$, $a + \boldsymbol{v} \in B$ a $\boldsymbol{w} \in W$ libovolné prvky, je předně $(a + \boldsymbol{u}) + \boldsymbol{w} = a + (\boldsymbol{u} + \boldsymbol{w}) \in B$. Dále podle lemmatu 19.6 (i) máme $(a + \boldsymbol{u}) - (a + \boldsymbol{v}) = \boldsymbol{u} - \boldsymbol{v} \in W$ a $B(W)$ je podprostor v $A(V)$ podle věty 19.4. Obráceně, buď $B(W)$ podprostor v $A(V)$ a $a \in B$ buď libovolný bod. Označíme-li $C = \{b \in A | b = a + \boldsymbol{u},\ \boldsymbol{u} \in W\}$ je $C \subseteq B(W)$ podle věty 19.4. Naopak pro libovolný bod $b \in B(W)$ je podle téže věty $b - a = \boldsymbol{u} \in W$, takže $b = a + \boldsymbol{u} \in C$ a jsme hotovi. Speciální tvrzení je nyní zřejmé. ∎

19.8. Definice. Jednorozměrný afinní prostor se nazývá *afinní přímka*, dvojrozměrný prostor se nazývá *afinní rovina*. *Nadrovinou* afinního prostoru A_n rozumíme každý podprostor dimenze $n - 1$.

19.9. Definice. Na základě věty 19.7 můžeme každý podprostor $B(W)$ afinního prostoru $A(V)$ zapisovat formálně ve tvaru $B = a + W$, kde $a \in B$ je libovolný bod. Je-li $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k\}$ nějaká báze podprostoru W, můžeme každý prvek $b \in B$ napsat jednoznačně ve tvaru $b = a + \sum_{i=1}^{k} t_i \boldsymbol{u}_i$, kde $t_1, t_2, \ldots, t_k \in T$. Toto vyjádření se nazývá *parametrické vyjádření* nebo *parametrická rovnice* podprostoru B. Říkáme též, že podprostor B je *dán parametricky*.

19.10. Definice. Množina $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$, kde $a \in A(V_n)$ a $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ je báze vektorového prostoru V_n, se nazývá *soustava souřadnic* v afinním prostoru $A(V_n)$. Bod a se nazývá *počátek soustavy souřadnic* a přímka $a + \langle \boldsymbol{u}_i \rangle$ se nazývá *i-tá souřadnicová osa*, $i = 1, 2, \dots, n$. Pro libovolný bod $b \in A$ je $b - a = \sum_{i=1}^{n} x_i \boldsymbol{u}_i$, přičemž koeficienty $x_1, x_2, \dots, x_n$ jsou podle věty 2.10 prvkem b určeny jednoznačně. Prvek $(x_1, x_2, \dots, x_n) \in T^n$ nazýváme *souřadnicemi prvku b* vzhledem k soustavě souřadnic S a značíme $\{b\}_S$. *Souřadnicemi vektoru $\boldsymbol{u} \in V_n$* vzhledem k S rozumíme jeho souřadnice vzhledem k bázi M, tj. $\{\boldsymbol{u}\}_S = \{\boldsymbol{u}\}_M$.

19.11. Věta. *Buď $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ soustava souřadnic v afinním prostoru $A(V_n)$. Pak pro každé dva body $b, c \in A$ a každý vektor $\boldsymbol{u} \in V_n$ je*

$$\{b - c\}_S = \{b\}_S - \{c\}_S \quad a \quad \{b + \boldsymbol{u}\}_S = \{b\}_S + \{\boldsymbol{u}\}_S.$$

Důkaz. Označíme-li $\{b\}_S = (x_1, x_2, \dots, x_n)$, $\{c\}_S = (y_1, y_2, \dots, y_n)$ a $\{\boldsymbol{u}\}_S = (z_1, z_2, \dots, z_n)$, je $b = a + \sum_{i=1}^{n} x_i \boldsymbol{u}_i$, $c = a + \sum_{i=1}^{n} y_i \boldsymbol{u}_i$ a $\boldsymbol{u} = \sum_{i=1}^{n} z_i \boldsymbol{u}_i$. Podle lemmatu 19.6 (ii) je $b - c = (b-a) - (c-a) = \sum_{i=1}^{n} (x_i - y_i) \boldsymbol{u}_i$, takže $\{b-c\}_S = (x_1 - y_1, x_2 - y_2, \dots, x_n - y_n) = \{b\}_S - \{c\}_S$. Podobně $b + \boldsymbol{u} = a + \sum_{i=1}^{n} x_i \boldsymbol{u}_i + \sum_{i=1}^{n} z_i \boldsymbol{u}_i = a + \sum_{i=1}^{n} (x_i + z_i) \boldsymbol{u}_i$, odkud $\{b + \boldsymbol{u}\}_S = (x_1 + z_1, x_2 + z_2, \dots, x_n + z_n) = \{b\}_S + \{\boldsymbol{u}\}_S$. ■

19.12. Poznámka. Buď $p = a + \langle \boldsymbol{u} \rangle$ afinní přímka v afinním prostoru A_n a buď S soustava souřadnic v A_n. Buď dále $x \in p$ libovolný bod a nechť $\{x\}_S = (x_1, x_2, \dots, x_n)$, $\{a\}_S = (a_1, a_2, \dots, a_n)$ a $\{\boldsymbol{u}\}_S = (z_1, z_2, \dots, z_n)$ jsou souřadnice bodů x, a a vektoru $\boldsymbol{u}$ vzhledem k soustavě souřadnic S. Jelikož $x = a + t\boldsymbol{u}$ pro nějaký parametr $t \in T$, je podle předchozí věty $(x_1, x_2, \dots, x_n) = (a_1, a_2, \dots, a_n) + t(z_1, z_2, \dots, z_n)$, takže $x_i = a_i + tz_i$ pro každé $i = 1, 2, \dots, n$. Tyto rovnosti můžeme zapsat též formálně ve tvaru

$$\frac{x_1 - a_1}{z_1} = \frac{x_2 - a_2}{z_2} = \dots = \frac{x_n - a_n}{z_n} = t.$$

Tomuto zápisu budeme říkat *parametrické vyjádření přímky p* vzhledem k soustavě souřadnic S. Zdůrazněme, že se jedná skutečně o ryze formální zápis, tj. má smysl i výraz $\frac{r}{0}$, $r \in T$.

19.13. Věta. (Transformace souřadnic.) *Buďte $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ a $S' = \{a', \boldsymbol{u}'_1, \boldsymbol{u}'_2, \dots, \boldsymbol{u}'_n\}$ dvě soustavy souřadnic v afinním prostoru $A(V_n)$ a buď $\boldsymbol{B} = (b_{ij})$ matice přechodu od báze $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ k bázi $M' = \{\boldsymbol{u}'_1, \boldsymbol{u}'_2, \dots, \boldsymbol{u}'_n\}$. Pak pro každý bod $b \in A$ platí*

$$\{b\}_S = \{a'\}_S + \{b\}_{S'} \boldsymbol{B}^T$$

a pro každý vektor $\boldsymbol{u} \in V_n$ platí

$$\{\boldsymbol{u}\}_S = \{\boldsymbol{u}\}_{S'} \boldsymbol{B}^T.$$

Důkaz. Podle věty 10.14 je $\{\boldsymbol{u}\}_S = \{\boldsymbol{u}\}_M = \{\boldsymbol{u}\}_{M'} \boldsymbol{B}^T = \{\boldsymbol{u}\}_{S'} \boldsymbol{B}^T$. Z definice 19.10 je zřejmé, že $\{b\}_S = \{b - a\}_M$, takže použitím lemmatu 19.6 a věty 19.11 dostaneme $\{b\}_S = \{b - a\}_S = \{b - a'\}_S + \{a' - a\}_S = \{a'\}_S + \{b - a'\}_{S'} \boldsymbol{B}^T = \{a'\}_S + \{b\}_{S'} \boldsymbol{B}^T$. ■

19.14. Poznámka. Pro praktické počítání je účelné mít transformační vzorce vyjádřené v explicitním tvaru. Označíme-li tedy $\{a'\}_S = (a_1, a_2, \ldots, a_n)$, $\{b\}_S = (x_1, x_2, \ldots, x_n)$ a $\{b\}_{S'} = (x'_1, x'_2, \ldots, x'_n)$, pak rozepsáním tvrzení věty do složek dostaneme transformační vzorce

$$x_i = a_i + \sum_{j=1}^{n} x'_j \cdot b_{ij}, \quad i = 1, 2, \ldots, n.$$

19.15. Věta. (Popis podprostorů rovnicemi.) *Buď $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ soustava souřadnic v afinním prostoru $A(V_n)$ a buď $B = b + W$ podprostor prostoru $A(V_n)$ dimenze $n - k$. Pak existují prvky a_{ij}, $b_i \in T$, $i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, n$ tak, že bod $c \in S$ o souřadnicích $\{c\}_S = (x_1, x_2, \ldots, x_n)$ leží v B, právě když*

$$\sum_{j=1}^{n} a_{ij} x_j = b_i \quad \text{pro každé} \quad i = 1, 2, \ldots, k.$$

Důkaz. Při označení z definice 11.23 je $\Phi(W) = \{f \in \tilde{V}_n | W \subseteq \operatorname{Ker} f\}$, takže podle věty 11.25 (v) je $\dim \Phi(W) = k$. Buď $\{f_1, f_2, \ldots, f_k\}$ báze podprostoru $\Phi(W)$ prostoru $\tilde{V}_n$. Použitím věty 11.25 (i) a věty 11.24 (iv) dostaneme $W = \Psi\Phi(W) = \Psi(\langle f_1, f_2, \ldots, f_k\rangle| = \Psi(\{f_1, f_2, \ldots, f_k\})$, takže $W = \cap_{i=1}^{k} \operatorname{Ker} f_i$. Nechť $f_i(\boldsymbol{u}) = \sum_{j=1}^{n} a_{ij} x_j$, $i = 1, 2, \ldots, k$, je analytické vyjádření formy f_i vzhledem k bázi $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ prostoru V_n a $\{b\}_S = (y_1, y_2, \ldots, y_n)$. Z věty 19.4 snadno plyne, že bod $c \in A$ leží v B, právě když vektor $c - b$ leží ve W. S použitím věty 19.11 tedy vidíme, že $b \in C$, právě když $\sum_{j=1}^{n} a_{ij}(x_j - y_j) = 0$ pro každé $i = 1, 2, \ldots, k$. Položíme-li nakonec $b_i = \sum_{j=1}^{n} a_{ij} y_j$ vidíme, že $c \in B$, právě když $\sum_{j=1}^{n} a_{ij} x_j = b_i$ pro každé $i = 1, 2, \ldots, k$. ■

19.16. Definice. Buďte $B(W)$ a $C(W')$ dva podprostory afinního prostoru $A(V)$. Řekneme, že podprostory $B(W)$ a $C(W')$ jsou

- *rovnoběžné*, jestliže buďto $W \subseteq W'$, nebo $W' \subseteq W$;
- *různoběžné*, jestliže nejsou rovnoběžné a mají aspoň jeden společný bod;
- *mimoběžné*, jestliže nejsou ani rovnoběžné, ani různoběžné.

19.17. Poznámka. Speciálním případem rovnoběžných podprostorů $B(W)$ a $C(W)$ je to, že jeden z nich je obsažen ve druhém, např. $B \subseteq C$, nebo že dokonce splývají, $B = C$. Mimoběžnost dvou podprostorů znamená, že tyto podprostory nemají společný žádný bod a nejsou přitom rovnoběžné. V následujících dvou větách dokážeme kritéria, kdy jsou dva rovnoběžné podprostory různé a kdy jsou dva nerovnoběžné podprostory různoběžné.

19.18. Věta. *Nechť $B(W)$ a $C(W')$ jsou dva rovnoběžné podprostory afinního prostoru $A(V)$ takové, že $W' \subseteq W$. Pak následující podmínky jsou ekvivalentní:*
(i) podprostory B a C jsou disjunktní;
(ii) pro každé $b \in B$ a každé $c \in C$ je $b - c \notin W$;
(iii) existují prvky $b \in B$ a $c \in C$ takové, že $b - c \notin W$.

Důkaz. Z (i) plyne (ii). Předpokládejme naopak, že existují prvky $b \in B$ a $c \in C$ takové, že $b - c \in W$, a ukažme, že potom $C \subseteq B$. Je-li $d \in C$ libovolný bod, je $C = d + W'$ podle věty 19.7. Pro libovolný vektor $\boldsymbol{w}' \in W'$ je podle lemmatu 19.6

$d + \boldsymbol{w}' = b + (d - c) + (c - b) \in b + W = B$, neboť $d - c \in W' \subseteq W$ podle věty 19.7 a $c - b \in W$ podle předpokladu. Tedy $C \subseteq B$, což je spor s předpokladem.

Z (ii) plyne zřejmě (iii).

Z (iii) plyne (i). Předpokládejme naopak, že podprostory B a C mají společný bod d. Jsou-li nyní $b \in B$ a $c \in C$ body z podmínky (iii), je $b - d \in W$ a $d - c \in W' \subseteq W$ podle věty 19.7. Pak ale podle lemmatu 19.6 je $b - c = (b - d) + (d - c) \in W$, což je spor. ■

19.19. Věta. *Buďte $B(W)$ a $C(W')$ dva nerovnoběžné podprostory afinního prostoru $A(V)$. Pak následující podmínky jsou ekvivalentní:*

(i) podprostory B a C jsou různoběžné;

(ii) pro každé $b \in B$ a každé $c \in C$ je $b - c \in W \vee W'$;

(iii) existují prvky $b \in B$ a $c \in C$ takové, že $b - c \in W \vee W'$.

Důkaz. Z (i) plyne (ii). Buď $d \in B \cap C$ libovolný bod. Podle věty 19.7 leží pro každé $b \in B$ vektor $b - d$ v podprostoru W a pro každé $c \in C$ vektor $d - c$ v podprostoru W'. Pak ale podle lemmatu 19.6 je $b - c = (b - d) + (d - c) \in W \vee W'$.

Z (ii) plyne zřejmě (iii).

Z (iii) plyne (i). Podle předpokladu a věty 1.13 je $b - c = \boldsymbol{w} + \boldsymbol{w}'$, kde $\boldsymbol{w} \in W$ a $\boldsymbol{w}' \in W'$. Odtud podle lemmatu 19.6 (i) máme $b - \boldsymbol{w} = c + \boldsymbol{w}' \in B \cap C$ a podprostory B a C jsou různoběžné. ■

19.20. Důsledek. *Dvě přímky $p = a + \langle \boldsymbol{u} \rangle$ a $q = b + \langle \boldsymbol{v} \rangle$ trojrozměrného afinního prostoru $A_3(V_3)$ jsou mimoběžné, právě když $\langle a - b, \boldsymbol{u}, \boldsymbol{v} \rangle = V_3$, tj. právě když vektory $a - b, \boldsymbol{u}, \boldsymbol{v}$ tvoří bázi vektorového prostoru V_3.*

Důkaz. Jsou-li přímky p a q mimoběžné, je jednak $\langle \boldsymbol{u} \rangle \neq \langle \boldsymbol{v} \rangle$, jednak $a - b \notin \langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$ podle předchozí věty, takže $\dim \langle a - b, \boldsymbol{u}, \boldsymbol{v} \rangle = 3$ a $\langle a - b, \boldsymbol{u}, \boldsymbol{v} \rangle = V_3$ podle věty 2.22. Obráceně, je-li $\langle a - b, \boldsymbol{u}, \boldsymbol{v} \rangle = V_3$ je $\langle \boldsymbol{u} \rangle \neq \langle \boldsymbol{v} \rangle$ a $a - b \notin \langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$ a stačí opět použít předchozí větu. ■

19.21. Poznámka. V předchozím důsledku jsme zkoumali mimoběžnost dvou přímek v trojrozměrném afinním prostoru $A_3(V_3)$. Uvědomme si, že tento předpoklad není nikterak omezující. Jsou-li totiž $p = a + \langle \boldsymbol{u} \rangle$ a $q = b + \langle \boldsymbol{v} \rangle$ dvě přímky v nějakém afinním prostoru $A(V)$, leží obě přímky v podprostoru $a + \langle a - b, \boldsymbol{u}, \boldsymbol{v} \rangle$, jehož dimenze je nejvýše 3. Přesněji, tato dimenze je 3, právě když jsou přímky p a q mimoběžné, je rovna 2, právě když jsou přímky p a q buď různoběžné, nebo rovnoběžné různé a je rovno 1, právě když přímky p a q splývají.

Z toho, co bylo právě řečeno, plyne, že nejmenší možná dimenze afinního prostoru, ve kterém existují mimoběžné přímky, je rovna 3. Podívejme se na tuto otázku obecně, tj. zjistěme nejmenší možnou dimenzi n afinního prostoru, v němž existují dva mimoběžné podprostory dimenzí k a l. Nechť tedy $B = b + W$, $C = c + W'$, kde $\dim W = k$ a $\dim W' = l$ jsou dva mimoběžné podprostory, $k \leq l$. Protože B a C nejsou rovnoběžné, není ani $W \subseteq W'$, ani $W' \subseteq W$. Podle věty o dimenzi spojení a průniku 2.23 je $\dim W + \dim W' = \dim (W \cap W') + \dim (W \vee W')$ a vzhledem k tomu, že hledáme co možná nejmenší spojení $W \vee W'$, potřebujeme podprostory W a W' tak, aby $\dim (W \cap W') = k - 1$. Pak $\dim (W \vee W') = k + l - (k - 1) = l + 1$. Protože podle věty 19.19 je $b - c \notin W \vee W'$, je hledané minimální n rovno $l + 2$, tedy $n = \max(k, l) + 2$. Speciálně tedy dvě mimoběžné roviny existují v afinních prostorech A_n, $n \geq 4$.

Ukažme si na závěr, jak takové dvě mimoběžné roviny můžeme sestrojit. V prostoru $A_4(V_4)$ vezměme libovolný bod a a bázi $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4\}$ vektorového prostoru V_4. Položme $b = a + \boldsymbol{u}_4$ a uvažujme roviny $\varrho = a + \langle \boldsymbol{u}_1, \boldsymbol{u}_2 \rangle$, $\sigma = b + \langle \boldsymbol{u}_1, \boldsymbol{u}_3 \rangle$. Pak $\boldsymbol{u}_3 \notin \langle \boldsymbol{u}_1, \boldsymbol{u}_2 \rangle$, $\boldsymbol{u}_2 \notin \langle \boldsymbol{u}_1, \boldsymbol{u}_3 \rangle$, takže roviny ϱ a σ nejsou rovnoběžné. Kromě toho $b - a = \boldsymbol{u}_4 \notin \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3 \rangle = \langle \boldsymbol{u}_1, \boldsymbol{u}_2 \rangle \vee \langle \boldsymbol{u}_1, \boldsymbol{u}_3 \rangle$ a roviny ϱ a σ jsou mimoběžné podle věty 19.19.

19.22. Vzájemná poloha přímek v afinní rovině $A_2(V_2)$. Buďte $p = a + \langle \boldsymbol{u} \rangle$ a $q = b + \langle \boldsymbol{v} \rangle$ dvě přímky v afinní rovině $A_2(V_2)$. Je-li $\langle \boldsymbol{u} \rangle = \langle \boldsymbol{v} \rangle$, jsou přímky p a q rovnoběžné, přičemž podle věty 19.18 je $p = q$, právě když $a - b \in \langle \boldsymbol{u} \rangle = \langle \boldsymbol{v} \rangle$. Jestliže přímky p, q nejsou rovnoběžné, je $\langle \boldsymbol{u} \rangle \neq \langle \boldsymbol{v} \rangle$, takže $V_2 = \langle \boldsymbol{u}, \boldsymbol{v} \rangle$. Pak ale $a - b \in \langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$ a přímky p, q jsou různoběžné podle věty 19.19. Vidíme tedy, že v afinní rovině jsou každé dvě přímky buď rovnoběžné, nebo různoběžné.

19.23. Vzájemná poloha přímek a rovin v afinním prostoru $A_3(V_3)$. Nechť $p = a + \langle \boldsymbol{u} \rangle$, $q = b + \langle \boldsymbol{v} \rangle$ jsou dvě přímky v afinním prostoru $A_3(V_3)$. Podobně jako v afinní rovině A_2 přímky p, q jsou rovnoběžné, právě když $\langle \boldsymbol{u} \rangle = \langle \boldsymbol{v} \rangle$, přičemž podle věty 19.18 je $p = q$, právě když $a - b \in \langle \boldsymbol{u} \rangle = \langle \boldsymbol{v} \rangle$. Jestliže $\langle \boldsymbol{u} \rangle \neq \langle \boldsymbol{v} \rangle$, pak podle věty 19.19 jsou přímky p, q různoběžné, právě když $a - b \in \langle \boldsymbol{u}, \boldsymbol{v} \rangle$ a jsou mimoběžné, právě když $a - b \notin \langle \boldsymbol{u}, \boldsymbol{v} \rangle$, tj. vzhledem k důsledku 19.20, právě když $\langle a - b, \boldsymbol{u}, \boldsymbol{v} \rangle = V_3$.

Buď nyní $p = a + \langle \boldsymbol{u} \rangle$ přímka a $\varrho = b + W$ rovina v A_3. Jestliže $\langle \boldsymbol{u} \rangle \subseteq W$, je přímka p rovnoběžná s rovinou ϱ, přičemž (věta 19.18) $p \subseteq \varrho$, právě když $a - b \in W$. Jestliže přímka p není rovnoběžná s rovinou ϱ, je $\langle \boldsymbol{u} \rangle \nsubseteq W$, takže $W \vee \langle \boldsymbol{u} \rangle = V_3$. Pak ale $a - b \in W \vee \langle \boldsymbol{u} \rangle$ a podle věty 19.19 přímka p protíná rovinu ϱ. Přitom přímka p má s rovinou ϱ společný právě jeden bod, neboť v opačném případě pro $c \neq d \in p \cap \varrho$ je $c - d \in \langle \boldsymbol{u} \rangle \cap W$, takže $\langle \boldsymbol{u} \rangle \subseteq W$ a přímka p by byla rovnoběžná s rovinou ϱ.

Přejděme ke vzájemné poloze dvou rovin $\varrho = a + W$ a $\sigma = b + W'$ v afinním prostoru $A_3(V_3)$. Jestliže $W = W'$, jsou roviny ϱ, σ rovnoběžné, přičemž $\varrho = \sigma$, právě když $a - b \in W = W'$. Nechť tedy $W \neq W'$. Pak $W \subsetneqq W \vee W'$, a tedy $W \vee W' = V_3$ podle věty 2.22. Podle věty o dimenzi spojení a průniku 2.23 je $\dim(W \cap W') = \dim W + \dim W' - \dim (W \vee W') = 1$, tj. $W \cap W' = \langle \boldsymbol{w} \rangle$ pro nějaké $0 \neq \boldsymbol{w} \in W \cap W'$. Protože zřejmě $a - b \in W \vee W' = V_3$, mají roviny ϱ a σ společný alespoň jeden bod c. Pak ale přímka $p = c + \langle \boldsymbol{w} \rangle$ je společná oběma rovinám. Je patrné, že $p = \varrho \cap \sigma$, neboť v opačném případě by roviny ϱ a σ měly společnou rovinu, a tudíž by splývaly. Přímka p se nazývá *průsečnice rovin ϱ a σ.*

19.24. Definice. Každý jednorozměrný podprostor vektorového prostoru V nazýváme *směrem.* Buďte $p = a + \langle \boldsymbol{u} \rangle$ a $q = b + \langle \boldsymbol{v} \rangle$ dvě mimoběžky v trojrozměrném afinním prostoru A_3. Každou přímku $r = c + \langle \boldsymbol{w} \rangle$ prostoru A_3, která protíná jak p, tak q, nazýváme *příčkou* těchto *mimoběžek.* V tomto případě hovoříme někdy o *příčce ve směru $\boldsymbol{w}$* (přesněji ve směru $\langle \boldsymbol{w} \rangle$) nebo o *příčce procházející bodem c.*

19.25. Poznámka. V následujících dvou větách budeme zkoumat otázky existence a jednoznačnosti příček dvou mimoběžek v daném směru či procházejících daným bodem. Zdůrazněme na tomto místě ještě jednou, že podle poznámky 19.21 řeší tyto věty problematika příček dvou mimoběžek zcela obecně, tj. v libovolném afinním prostoru $A(V)$.

19.26. Věta. *Buďte $p = a + \langle \boldsymbol{u} \rangle$ a $q = b + \langle \boldsymbol{v} \rangle$ dvě mimoběžky v trojrozměrném afinním prostoru $A_3(V_3)$ a $\boldsymbol{w} \in V_3$ buď nenulový vektor. Pak příčka mimoběžek p a q ve směru $\boldsymbol{w}$ existuje, právě když $\boldsymbol{w} \notin \langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$. V tomto případě je příčka ve směru $\boldsymbol{w}$ určena jednoznačně.*

Důkaz. Předpokládejme nejprve, že $\boldsymbol{w} \notin \langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$. Pak jsou vektory $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$ zřejmě lineárně nezávislé, takže $\boldsymbol{v} \notin W = \langle \boldsymbol{u}, \boldsymbol{w} \rangle$. Podle odstavce 19.23 protíná přímka q rovinu $\sigma = a + W$ (rovina procházející přímkou p a obsahující směr $\langle \boldsymbol{w} \rangle$) v jediném bodě c. Přímka $r = c + \langle \boldsymbol{w} \rangle$ leží celá v rovině ϱ a protíná přímku q v bodě c. Protože přímka p leží rovněž v rovině ϱ a není rovnoběžná s přímkou r, neboť $\langle \boldsymbol{u} \rangle \neq \langle \boldsymbol{w} \rangle$, protíná přímka r přímku p podle odstavce 19.22 v jediném bodě d a $r = c + \langle \boldsymbol{w} \rangle$ je tudíž příčka mimoběžek p a q ve směru $\boldsymbol{w}$. Dokažme nyní jednoznačnost. Buď tedy $r' = c' + \langle \boldsymbol{w} \rangle$ libovolná příčka mimoběžek p a q ve směru $\boldsymbol{w}$ taková, že $r' \cap q = c'$ a $r' \cap p = d'$. Pak máme jednak $c' - d' = s\boldsymbol{w}$ pro nějaké $s \in T$, jednak s pomocí lemmatu 19.6 $c' - d' = (c' - c) + (c - d) + (d - d') = \alpha\boldsymbol{v} + \beta\boldsymbol{w} + \gamma\boldsymbol{u}$. Odtud porovnáním dostáváme $s\boldsymbol{w} = \alpha\boldsymbol{v} + \beta\boldsymbol{w} + \gamma\boldsymbol{u}$ neboli $\alpha\boldsymbol{v} + (\beta - s)\boldsymbol{w} + \gamma\boldsymbol{u} = 0$, odkud $\alpha = \gamma = 0$ a $\beta = s$ vzhledem k lineární nezávislosti vektorů $\boldsymbol{u}, \boldsymbol{v}$ a $\boldsymbol{w}$. To ale znamená, že $c' = c, d' = d$, a tedy $r = r'$.

K dokončení důkazu předpokládejme, že existuje příčka $r = c + \langle \boldsymbol{w} \rangle$ mimoběžek p a q ve směru $\boldsymbol{w}$. Na základě věty 19.7 můžeme bez újmy na obecnosti předpokládat, že bod c je průsečíkem přímek p a r. Pak ale rovina $\varrho = c + \langle \boldsymbol{u}, \boldsymbol{w} \rangle$ obsahuje přímku p a podle odstavce 19.22 nemůže obsahovat přímku q, neboť v opačném případě by přímky p a q byly buď rovnoběžné, nebo různoběžné. Dále, rovina ϱ obsahuje přímku r, přímky q a r jsou podle předpokladu různoběžné (r je příčka mimoběžek p a q), takže přímka q je různoběžná s rovinou ϱ. Podle odstavce 19.23 to však znamená, že $\boldsymbol{v} \notin \langle \boldsymbol{u}, \boldsymbol{w} \rangle$, takže vektory $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$ jsou lineárně nezávislé, a tedy $\boldsymbol{w} \notin \langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$, což jsme chtěli dokázat. ∎

19.27. Věta. *Buďte $p = a + \langle \boldsymbol{u} \rangle$ a $q = b + \langle \boldsymbol{v} \rangle$ dvě mimoběžky v trojrozměrném afinním prostoru $A_3(V_3)$ a buď $c \in A_3$ bod neležící na žádné z nich. Pak existuje jediná příčka mimoběžek p a q procházející bodem c, právě když ani jeden z vektorů $c - a$, $c - b$ neleží ve spojení $\langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$.*

Důkaz. Předpokládejme nejprve, že ani $c - a$, ani $c - b$ neleží v $\langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$. Pak vektory $c - a, \boldsymbol{u}, \boldsymbol{v}$ jsou lineárně nezávislé, takže $\boldsymbol{v} \notin \langle c - a, \boldsymbol{u} \rangle$ a podle odstavce 19.23 přímka q protne rovinu $\varrho = c + \langle c - a, \boldsymbol{u} \rangle$ v jediném bodě d. Podle lemmatu 19.6 (ii) je $c - d = (c - b) + (b - d)$, takže vzhledem k tomu, že $b - d \in \langle \boldsymbol{v} \rangle$, je $c - d \notin \langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$, právě když $c - b \notin \langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$. Podle předchozí věty existuje tedy jediná příčka r mimoběžek p a q ve směru $\boldsymbol{w} = c - d$. Protože přímka p a body c, d leží v rovině ϱ, leží v této rovině i příčka r. Dále, přímka q protíná rovinu ϱ v jediném bodě d, takže z $r \subseteq \varrho$ a $r \cap q \neq \emptyset$ ihned plyne $d = r \cap q$, tj. bod d leží na příčce r. Pak ale $r = d + \langle c - d \rangle$, tedy $c \in r$ a r je příčka mimoběžek p a q procházející bodem c.

Obráceně, jestliže existuje příčka r mimoběžek p a q procházející bodem c, pak rovina $\varrho = c + \langle c - a, \boldsymbol{u} \rangle$ protíná přímku q v jediném bodě d. Skutečně podle odstavce 19.23 je přímka q buď rovnoběžná s rovinou ϱ, nebo s ní má jediný průsečík d. V prvním případě však z $p \subseteq \varrho$, $c \in \varrho$ a $r \cap p \neq \emptyset$ plyne $r \subseteq \varrho$, a protože $r \cap q \neq \emptyset$, leží přímka q v rovině ϱ. To je ale podle odstavce 19.22 spor s mimoběžností přímek p a q. Nyní z odstavce 19.23 vyplývá, že $\boldsymbol{v} \notin \langle c - a, \boldsymbol{u} \rangle$, a tedy i $c - a \notin \langle \boldsymbol{u}, \boldsymbol{v} \rangle$. Jelikož příčka r má nutně směr $\boldsymbol{w} = c - d$, platí podle předchozí věty, že $c - d \notin \langle \boldsymbol{u}, \boldsymbol{v} \rangle$. V první části důkazu jsme však ukázali, že v této situaci je $c - d \notin \langle \boldsymbol{u}, \boldsymbol{v} \rangle$, právě když $c - b \notin \langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$, a jsme hotovi. ■

19.28. Příklady. Důkazy dvou předchozích vět jsou zároveň metodou pro řešení konkrétních numerických úloh. Pro dvě mimoběžky $p = a + \langle \boldsymbol{u} \rangle$ a $q = b + \langle \boldsymbol{v} \rangle$ a daný směr $\langle \boldsymbol{w} \rangle$ či daný bod c splňující příslušné podmínky z předchozích dvou vět utvoříme rovinu $\varrho = a + \langle \boldsymbol{u}, \boldsymbol{w} \rangle$, resp. $\varrho = a + \langle c - a, \boldsymbol{u} \rangle$ procházející přímkou p a obsahující $\boldsymbol{w}$, resp. c, nalezneme průsečík $d = \varrho \cap q$ a dostaneme hledanou příčku $r = d + \langle \boldsymbol{w} \rangle$, resp. $r = d + \langle c - d \rangle$.

1. V afinním prostoru $A(T^3)$ (viz příklad 19.5) nalezněme příčku mimoběžek $p = (1, 2, -1) + \langle (1, -1, 1) \rangle$ a $q = (0, 9, -2) + \langle (1, 0, 0) \rangle$ rovnoběžnou se směrem $\boldsymbol{w} = (1, 2, 0)$.

Ř e š e n í : Při označení z předchozích vět je

$$\begin{pmatrix} 1, & -1, & 1 \\ 1, & 0, & 0 \\ 1, & -7, & 1 \end{pmatrix} \sim \begin{pmatrix} 1, & 0, & 0 \\ 0, & -1, & 1 \\ 0, & -7, & 1 \end{pmatrix} \sim \begin{pmatrix} 1, & 0, & 0 \\ 0, & 1, & -1 \\ 0, & 0, & -6 \end{pmatrix},$$

vektory $\boldsymbol{u}, \boldsymbol{v}, a - b$ jsou lineárně nezávislé a přímky p a q jsou mimoběžné podle důsledku 19.20. Stejným způsobem snadno ověříme, že vektory $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$ jsou lineárně nezávislé a příčka mimoběžek p a q ve směru $\boldsymbol{w}$ existuje podle věty 19.26. Jak bylo řečeno v úvodu tohoto odstavce, stačí nyní nalézt průsečík d přímky p s rovinou $\varrho = (1, 2, -1) + \langle (1, -1, 1), (1, 2, 0) \rangle$. Parametrické vyjádření přímky q je $(0, 9, -2) + \alpha(1, 0, 0)$ a rovina ϱ má parametrické vyjádření $(1, 2, -1) + \beta(1, -1, 1) + \gamma(1, 2, 0)$. K tomu, abychom nalezli průsečík d, musíme řešit rovnici $(0, 9, -2) + \alpha(1, 0, 0) = (1, 2, -1) + \beta(1, -1, 1) + \gamma(1, 2, 0)$, přičemž nám zřejmě stačí znát hodnotu parametru α. Rozepsáním do složek dostaneme nehomogenní soustavu tří lineárních rovnic o třech neznámých

$$\begin{aligned} \alpha - \beta - \gamma &= 1, \\ \beta - 2\gamma &= -7, \\ -\beta &= 1. \end{aligned}$$

Odtud vidíme ihned, že $\beta = -1$, $\gamma = 3$ a $\alpha = 3$, takže bod $d = (3, 9, -2)$ je průsečík přímky q s rovinou ϱ a hledaná příčka pak je $r = (3, 9, -2) + \langle (1, 2, 0) \rangle$.

Proberme si ještě jeden způsob řešení naší úlohy. Rovina ϱ je nadrovina v A^3, takže podle věty 19.15 ji lze zapsat jednou rovnicí tvaru $\alpha x + \beta y + \gamma z = \delta$. Z důkazu této věty vyplývá, že body nadroviny splňují tuto rovnici, zatímco vektory z této roviny splňují příslušnou homogenní rovnici. Tedy

$$\begin{aligned} \alpha - \beta + \gamma &= 0, \\ \alpha + 2\beta &= 0 \end{aligned}$$

je soustava homogenních rovnic (pro vektory $\boldsymbol{u}$ a $\boldsymbol{w}$), která má řešení $\langle (2, -1, -3) \rangle$. Odtud dostáváme rovnici roviny ϱ ve tvaru $2x - y - 3z = \delta$, kde δ spočteme dosazením bodu $a = (1, 2, -1)$, tedy $2x - y - 3z = 3$. Průsečík d nyní snadno spočteme dosazením parametrické rovnice přímky q do rovnice roviny ϱ. Máme $2\alpha - 9 + 6 = 3$, tedy $\alpha = 3$ a zbytek již známe.

2. V afinním prostoru $A(T^3)$ nalezněme příčku mimoběžek $p = (3,3,3)+\langle(2,2,1)\rangle$ a $q = (0,5,-1) + \langle(1,1,1)\rangle$, která prochází bodem $c = (4,5,3)$.

Řešení: Snadno ověříme, že vektory $\boldsymbol{u} = (2,2,1)$, $\boldsymbol{v} = (1,1,1)$ a $a - b = (3,-2,4)$ jsou lineárně nezávislé, takže přímky p a q jsou skutečně mimoběžné. Dále lehce zjistíme, že jak vektory $(1,2,0), (2,2,1), (1,1,1)$, tak vektory $(4,0,4), (2,2,1)$, $(1,1,1)$ jsou rovněž nezávislé, takže příčka procházející bodem c existuje podle věty 19.27. Jak víme, stačí nám nyní nalézt průsečík d přímky q s rovinou $\varrho = (4,5,3) + \langle(1,2,0),(2,2,1)\rangle$. Porovnáme-li nyní parametrické rovnice $(0,5,-1) + \alpha(1,1,1) = (4,5,3) + \beta(1,2,0) + \gamma(2,2,1)$, dostaneme soustavu rovnic

$$\begin{aligned}
\alpha \; - \;\; \beta \;\; - 2\gamma &= 4,\\
\alpha \; - 2\beta \;\; - 2\gamma &= 0,\\
\alpha \qquad\quad - \;\; \gamma &= 4,
\end{aligned}$$

odkud například použitím Cramerova pravidla 8.13 dostaneme $\alpha = 0$. Průsečík přímky q s rovinou ϱ tedy je $d = (0,-5,1)$ a hledaná příčka $r = d + \langle c - d\rangle = (0,-5,1) + \langle(4,0,4)\rangle = (0,-5,1) + \langle(1,0,1)\rangle$.

19.29. Definice. Buďte a, b, c tři různé body afinní přímky A_1. Vektory $c-a$, $c-b$ jsou lineárně závislé, takže $c - a = \lambda(c - b)$ pro nějaký prvek $\lambda \in T$. Tento prvek se nazývá *dělicí poměr bodu c vzhledem k bodům a, b* (v tomto pořadí!) a značí se symbolem $(c; a, b)$. Jestliže těleso T je charakteristiky různé od 2 a $(c; a, b) = -1$, pak říkáme, že bod c je *středem dvojice*, nebo *středem úsečky* (a, b).

19.30 Věta. *Buďte a, b, c tři různé body afinní přímky A_1. Pak platí*

(i) $(c; a, b) \neq 0, 1$;

(ii) jestliže $(c; a, b) = \lambda$, pak $(c; b, a) = \frac{1}{\lambda}$, $(a; b, c) = \frac{\lambda-1}{\lambda}$, $(a; c, b) = \frac{\lambda}{\lambda-1}$, $(b; a, c) = 1 - \lambda$, $(b; c, a) = \frac{1}{1-\lambda}$;

(iii) je-li těleso T charakteristiky různé od 2, pak bod c je středem dvojice (a, b), právě když $c = a + \frac{1}{2}(b - a) = b + \frac{1}{2}(a - b)$.

Důkaz. (i) Vzhledem k tomu, že body a, b, c jsou navzájem různé, jsou vektory $c-a$ a $c - b$ nenulové, a tedy $\lambda = (c; a, b) \neq 0$. Dále, pro $(c; a, b) = 1$ je $c - a = c - b$, takže podle lemmatu 19.6 je $a = a + 0 = a + (c - a) - (c - b) = a + (b - a) = b$, což je spor s předpokladem.

(ii) Nechť $(c; a, b) = \lambda$, tj. $c - a = \lambda(c - b)$. Pak $c - b = \frac{1}{\lambda}(c - a)$ a $(c; b, a) = \frac{1}{\lambda}$. Dále z $a - c = \lambda(b - c)$ pomocí lemmatu 19.6 dostaneme $a - c = \lambda((b - a) + (a - c))$, odkud $(1 - \lambda)(a - c) = \lambda(b - a)$, tedy $a - c = \frac{\lambda}{\lambda-1}(a - b)$ a $(a; c, b) = \frac{\lambda}{\lambda-1}$. Vidíme tedy, že vzájemnou výměnou prvních dvou bodů se dělicí poměr změní z λ na $\frac{\lambda}{\lambda-1}$ a vzájemnou výměnou druhého a třetího bodu se dělicí poměr změní z λ na $\frac{1}{\lambda}$. Odtud již všechny požadované hodnoty snadno dostaneme. Tedy $(a; b, c) = \frac{\lambda-1}{\lambda}$, $(b; a, c) = \frac{\lambda-1}{\lambda} : (\frac{\lambda-1}{\lambda} - 1) = \frac{\lambda-1}{-1} = 1 - \lambda$ a $(b; c, a) = \frac{1}{1-\lambda}$.

(iii) Buď nejprve $(c; a, b) = -1$, tj. $c - a = -(c - b) = b - c = (b - a) + (a - c) = (b - a) - (c - a)$ a tedy $c - a = \frac{1}{2}(b - a)$. Podobně $c - b = (c - a) + (a - b) = \frac{1}{2}(b - a) + (a - b) = \frac{1}{2}(a - b)$. Odtud je zřejmé, že $c = a + \frac{1}{2}(b - a) = b + \frac{1}{2}(a - b)$.

Obráceně, je-li $c = a + \frac{1}{2}(b-a)$, je $c - a = \frac{1}{2}(b-a)$, tedy $2(c-a) = (b-a)$ a z $c - a = (b-a) + (a-c) = b - c$ dostáváme $(c; a, b) = -1$. ■

19.31. Definice. Buďte $A(V)$, $A'(V')$ dva afinní prostory, kde V a V' jsou vektorové prostory nad tělesem T. Jsou-li $a \in A$, $a' \in A'$ body a je-li $f : V \to V'$ homomorfismus, pak zobrazení $F : A \to A'$ definované předpisem $F(a + \boldsymbol{u}) = a' + f(\boldsymbol{u})$, $\boldsymbol{u} \in V$, se nazývá *afinní zobrazení vytvořené homomorfismem* f. Je-li homomorfismus f navíc injektivní, nazývá se F *regulární afinní zobrazení.* Afinní zobrazení prostoru $A(V)$ do něho samého se nazývá *afinita.*

19.32. Poznámka. Z definice afinního zobrazení $F(a+\boldsymbol{u}) = a' + f(\boldsymbol{u})$ plyne pro $\boldsymbol{u} = 0$, že $F(a) = a'$. Uvědomme si, že místo bodu a můžeme v definici afinního zobrazení vzít libovolný bod $b \in A$ a místo $a' = F(a) \in A'$ vzít obraz $b' = F(b)$. Skutečně $b = a + \boldsymbol{v}$ pro nějaký, jednoznačně určený, vektor $\boldsymbol{v} \in V$. Pak $b' = F(b) = a' + f(\boldsymbol{v})$, takže $F(b + \boldsymbol{u}) = F(a + \boldsymbol{v} + \boldsymbol{u}) = a' + f(\boldsymbol{v} + \boldsymbol{u}) = a' + f(\boldsymbol{v}) + f(\boldsymbol{u}) = b' + f(\boldsymbol{u})$, což jsme chtěli ověřit.

Dále nechť $B = b + W$ a $C = c + W'$ jsou dva rovnoběžné podprostory afinního prostoru $A(V)$ takové, že $W' \subseteq W$, a buď $F : A \to A'$ afinní zobrazení vytvořené homomorfismem $f : V \to V'$, $F(a+\boldsymbol{u}) = a' + f(\boldsymbol{u})$ pro nějaké body $a \in A$, $a' \in A'$. Předně je $b = a + \boldsymbol{v}$ pro nějaký, jednoznačně určený, vektor $\boldsymbol{v}$. Dále pro libovolné $\boldsymbol{w} \in W$ platí $F(b + \boldsymbol{w}) = F(a + \boldsymbol{u} + \boldsymbol{w}) = a' + f(\boldsymbol{u}) + f(\boldsymbol{w}) = F(b) + f(\boldsymbol{w})$, takže $F(B) = F(b) + f(W)$. Protože $f(W') \subseteq f(W)$ jsou podprostory $F(B)$ a $F(C)$ rovnoběžné. Jinými slovy, afinní zobrazení zachovává rovnoběžnost podprostorů. Na závěr tohoto odstavce ještě dokážeme, že nad tělesem charakteristiky různé od 2 je afinní zobrazení charakterizováno tím, že zachovává dělicí poměr a že dimenze konečně rozměrného afinního prostoru je charakterizována existencí surjektivního regulárního afinního zobrazení. Tato skutečnost je analogická stejné vlastnosti vektorových prostorů tak, jak je to ukázáno ve větě 10.3.

19.33. Věta. *Buďte $F : A(V) \to A'(V')$ a $G : A'(V') \to A''(V'')$ dvě afinní zobrazení vytvořené homomorfismy $f : V \to V'$ a $g : V' \to V''$. Pak platí*

(i) složené zobrazení $GF : A(V) \to A''(V'')$ je afinní zobrazení vytvořené homomorfismem $gf : V \to V''$;

(ii) jsou-li F i G regulární, je i GF regulární;

(iii) je-li F regulární afinní zobrazení prostoru $A(V)$ na prostor $A'(V')$, pak $F^{-1} : A'(V') \to A(V)$ je regulární afinní zobrazení vytvořené izomorfismem $f^{-1} : V' \to V$.

Důkaz. Vzhledem k poznámce 19.32 můžeme předpokládat, že $F(a + \boldsymbol{u}) = a' + f(\boldsymbol{u})$, kde $a \in A$ a $\boldsymbol{u} \in V$ je libovolný vektor, přičemž $a' = F(a)$, a podobně, že $G(a' + \boldsymbol{v}') = a'' + g(\boldsymbol{v}')$, $a'' = G(a')$, $\boldsymbol{v}' \in V'$.

(i) Zřejmě jest $GF(a + \boldsymbol{u}) = G(a' + f(\boldsymbol{u})) = a'' + g(f(\boldsymbol{u}))$, tj. platí (i).

(ii) Protože f i g jsou monomorfismy, je složený homomorfismus gf rovněž injektivní podle věty 9.7 (i).

(iii) Zobrazení $F^{-1} : A'(V') \to A(V)$ dané předpisem $F^{-1}(a' + \boldsymbol{u}') = a + f^{-1}(\boldsymbol{u}')$ je vzhledem k tomu, že f a f^{-1} jsou izomorfismy, regulární afinní zobrazení. Přitom $F^{-1}F(a + \boldsymbol{u}) = F^{-1}(a' + f(\boldsymbol{u})) = a + \boldsymbol{u}$, $FF^{-1}(a' + \boldsymbol{u}') = F(a + f^{-1}(\boldsymbol{u}')) = a' + \boldsymbol{u}'$, takže $F^{-1}F = 1_A$, $FF^{-1} = 1_{A'}$ a F^{-1} je regulární afinní zobrazení inverzní k zobrazení F. ■

19.34. Věta. *Buďte $A(V)$ a $A'(V')$ dva afinní prostory nad tělesem charakteristiky různé od 2. Zobrazení $F : A \to A'$ je afinní zobrazení, právě když pro každé tři body $b, c, d \in A$ ležící na přímce je buď $F(b) = F(c) = F(d)$, nebo $(F(b); F(c), F(d)) = (b; c, d)$.*

Důkaz. Buď nejprve $F : A \to A'$ afinní zobrazení vytvořené homomorfismem $f : V \to V'$, tj. $F(a + \boldsymbol{v}) = a' + f(\boldsymbol{v})$ pro nějaké body $a \in A$, $a' \in A'$ a libovolný vektor $\boldsymbol{v} \in V$. Buďte dále b, c, d tři navzájem různé body na afinní přímce $b + \langle \boldsymbol{u} \rangle$. Označíme-li $b' = F(b)$, pak podle poznámky 19.32 je $F(b + \boldsymbol{v}) = b' + f(\boldsymbol{v})$ pro každé $\boldsymbol{v} \in V$. Dále je $c = b + \lambda \boldsymbol{u}$ a $d = b + \mu \boldsymbol{u}$ pro nějaké nenulové prvky λ, $\mu \in T$, $\lambda \neq \mu$. Je-li nyní $F(b) = F(c)$ je $b' = b' + \lambda f(\boldsymbol{u})$, takže nutně $f(\boldsymbol{u}) = 0$ a $F(d) = F(c) = F(b) = b'$. Stejná situace zřejmě nastane, jestliže $F(b) = F(d)$. Předpokládáme-li konečně rovnost $F(c) = F(d)$, je $b' + \lambda f(\boldsymbol{u}) = b' + \mu f(\boldsymbol{u})$, tedy $(\lambda - \mu) f(\boldsymbol{u}) = 0$ a $f(\boldsymbol{u}) = 0$ vzhledem k nerovnosti $\lambda \neq \mu$. Opět tedy $F(b) = F(c) = F(d)$. Jsou-li nyní body $F(b), F(c), F(d)$ navzájem různé, leží všechny tři na afinní přímce $b' + \langle f(\boldsymbol{u}) \rangle$ a platí $F(b) - F(c) = -\lambda f(\boldsymbol{u})$, $F(b) - F(d) = -\mu f(\boldsymbol{u})$. Pak ale $(F(b); F(c), F(d)) = \frac{\lambda}{\mu} = (b; c, d)$.

Buď tedy naopak $F : A \to A'$ zobrazení splňující podmínku věty. Zvolme libovolně bod $a \in A$ a ukažme, že pro každé dva vektory $\boldsymbol{u}, \boldsymbol{v} \in V$ platí rovnost

$$(*) \qquad F(a + \boldsymbol{u} + \boldsymbol{v}) - F(a + \boldsymbol{v}) = F(a + \boldsymbol{u}) - F(a).$$

Označme b střed dvojice $(a, a + \boldsymbol{u} + \boldsymbol{v})$. Podle věty 19.30 (iii) s použitím lemmatu 19.6 je $b = a + \frac{1}{2}(\boldsymbol{u} + \boldsymbol{v}) = a + \boldsymbol{u} + \frac{1}{2}(\boldsymbol{v} - \boldsymbol{u})$, takže b je zároveň středem dvojice $(a + \boldsymbol{u}, a + \boldsymbol{v})$, a tedy $(b; a, a + \boldsymbol{u} + \boldsymbol{v}) = (b, a + \boldsymbol{u}, a + \boldsymbol{v}) = -1$. Vzhledem k podmínce věty nyní rozlišíme čtyři případy.

1. $F(b) = F(a) = F(a + \boldsymbol{u} + \boldsymbol{v}) = F(a + \boldsymbol{u}) = F(a + \boldsymbol{v})$. V tomto případě zřejmě máme $F(a + \boldsymbol{u} + \boldsymbol{v}) - F(a + \boldsymbol{v}) = 0 = F(a + \boldsymbol{u}) - F(a)$.

2. $F(b) = F(a) = F(a + \boldsymbol{u} + \boldsymbol{v})$ a $(F(b); F(a + \boldsymbol{u}), F(a + \boldsymbol{v})) = -1$. Zde jest $F(a + \boldsymbol{u}) - F(b) = F(b) - F(a + \boldsymbol{v})$, odkud $F(a + \boldsymbol{u} + \boldsymbol{v}) - F(a + \boldsymbol{v}) = F(b) - F(a + \boldsymbol{v}) = F(a + \boldsymbol{u}) - F(b)$.

3. $(F(b); F(a), F(a + \boldsymbol{u} + \boldsymbol{v})) = -1$ a $F(b) = F(a + \boldsymbol{u}) = F(a + \boldsymbol{v})$. Máme $F(a) - F(b) = F(b) - F(a + \boldsymbol{u} + \boldsymbol{v})$, a tedy $F(a + \boldsymbol{u} + \boldsymbol{v}) - F(a + \boldsymbol{v}) = F(a + \boldsymbol{u} + \boldsymbol{v}) - F(b) = F(b) - F(a) = F(a + \boldsymbol{u}) - F(a)$.

4. $(F(b); F(a), F(a + \boldsymbol{u} + \boldsymbol{v})) = (F(b); F(a + \boldsymbol{u}), F(a + \boldsymbol{v})) = -1$. V tomto případě jest $F(b) = F(a) + \frac{1}{2}(F(a + \boldsymbol{u} + \boldsymbol{v}) - F(a)) = F(a + \boldsymbol{u}) + \frac{1}{2}(F(a + \boldsymbol{v}) - F(a + \boldsymbol{u}))$, odkud podle lemmatu 19.6 máme $F(a + \boldsymbol{u}) - F(a) = \frac{1}{2}[(F(a + \boldsymbol{u} + \boldsymbol{v}) - F(a)) + (F(a + \boldsymbol{u}) - F(a + \boldsymbol{v}))]$. Pak ale $2(F(a + \boldsymbol{u}) - F(a)) = (F(a + \boldsymbol{u} + \boldsymbol{v}) - F(a)) + (F(a + \boldsymbol{u}) - F(a + \boldsymbol{v}))$, takže $F(a + \boldsymbol{u}) - F(a) = (F(a + \boldsymbol{u} + \boldsymbol{v}) - F(a)) + (F(a + \boldsymbol{u}) - F(a + \boldsymbol{v})) + (F(a) - F(a + \boldsymbol{u})) = F(a + \boldsymbol{u} + \boldsymbol{v}) - F(a + \boldsymbol{v})$.

Nyní se již důkaz snadno dokončí. Pro libovolný vektor $\boldsymbol{u} \in V$ položme $f(\boldsymbol{u}) = F(a + \boldsymbol{u}) - F(a)$. Pak f je zobrazení vektorového prostoru V do vektorového prostoru V', $F(a + \boldsymbol{u}) = F(a) + f(\boldsymbol{u})$, takže zbývá pouze ověřit, že zobrazení f je homomorfismus. Předně pro libovolné dva vektory $\boldsymbol{u}, \boldsymbol{v} \in V$ pomocí rovnosti (*) dostáváme $f(\boldsymbol{u} + \boldsymbol{v}) = F(a + \boldsymbol{u} + \boldsymbol{v}) - F(a) = (F(a + \boldsymbol{u} + \boldsymbol{v}) - F(a + \boldsymbol{v})) + (F(a + \boldsymbol{v}) - F(a)) = (F(a + \boldsymbol{u}) - F(a)) + (F(a + \boldsymbol{v}) - F(a)) = f(\boldsymbol{u}) + f(\boldsymbol{v})$. Buď dále $r \in T$ libovolný prvek. Pro $r = 0, 1$ je zřejmě $f(r\boldsymbol{u}) = r f(\boldsymbol{u})$. Je-li vektor $\boldsymbol{u}$ nulový, je jistě $f(r\boldsymbol{u}) = r f(\boldsymbol{u})$

pro každé $r \in T$. Nechť tedy $\boldsymbol{u}$ je nenulový vektor a $r \in T$ libovolný prvek, $r \neq 0, 1$. V tomto případě jsou $a, a+\boldsymbol{u}$ a $a + r\boldsymbol{u}$ tři různé body z A ležící na přímce a $(a; a+r\boldsymbol{u}, a+\boldsymbol{u}) = r$. Podle předpokladu tedy je buď $F(a) = F(a+r\boldsymbol{u}) = F(a+\boldsymbol{u})$ a $f(r\boldsymbol{u}) = 0 = f(\boldsymbol{u}) = rf(\boldsymbol{u})$, nebo $(F(a); F(a+r\boldsymbol{u}), F(a+\boldsymbol{u})) = r$. Pak ale $f(r\boldsymbol{u}) = F(a+r\boldsymbol{u}) - F(a) = r(F(a+\boldsymbol{u}) - F(a)) = rf(\boldsymbol{u})$ a věta je dokázána. ■

19.35. Věta. *Buď $A(V_n)$ afinní prostor dimenze n a buď $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ soustava souřadnic v $A(V_n)$. Pak zobrazení $F : A(V_n) \to A(T^n)$ definované pro $b \in A(V_n)$ vztahem $F(b) = \{b\}_S$ je regulární afinní afinního prostoru $A(V_n)$ na afinní prostor $A(T^n)$ (viz příklad 19.5).*

Důkaz. Zobrazení $f : V_n \to T^n$ definované předpisem $f(\boldsymbol{u}) = \{\boldsymbol{u}\}_S$ je ve smyslu definice 19.10 izomorfismus podle věty 10.2 (ii). Kromě toho pro každý bod $b \in A$ je $b = a + \boldsymbol{u}$ pro nějaký vektor $\boldsymbol{u} \in V_n$, přičemž podle věty 19.11 je $F(b) = \{a+\boldsymbol{u}\}_S = \{a\}_S + f(\boldsymbol{u})$, a F je tudíž regulární afinní zobrazení afinního prostoru $A(V_n)$ na afinní prostor $A(T^n)$ vytvořené izomorfismem f. ■

19.36. Důsledek. *Afinní prostory $A(V_n)$ a $A'(V'_m)$ mají stejnou dimenzi, právě když existuje regulární afinní zobrazení prostoru $A(V_n)$ na prostor $A'(V'_m)$.*

Důkaz. Buď nejprve $F : A \to A'$ regulární afinní zobrazení prostoru A na prostor A' vytvořené monomorfismem $f : V_n \to V'_m$. Protože F je surjektivní, je f nutně epimorfismus a $\dim V_n = \dim V'_m$ podle věty 10.3.

Jestliže naopak prostory $A(V_n)$ a $A'(V'_n)$ mají stejnou dimenzi n, existují podle předchozí věty regulární afinní zobrazení $F : A(V_n) \to A(T^n)$ a $G : A'(V'_n) \to A(T^n)$ a zobrazení $G^{-1}F : A(V_n) \to A'(V'_n)$ je regulární afinní zobrazení podle věty 19.33. ■

V tomto odstavci budeme pokračovat ve studiu dalších vlastností afinních prostorů, avšak s tím rozdílem, že místo obecného vektorového prostoru budeme uvažovat prostor unitární. Proto bude v dalším T značit těleso reálných čísel. Naším cílem bude studium tzv. metrických vlastností, tj. vzdáleností, úhlů apod., což je umožněno právě přítomností skalárního součinu na unitárním prostoru.

20.1. Definice. Afinní prostor $A((V_n, g))$ nad n-rozměrným unitárním prostorem (V_n, g) nazýváme *n-rozměrným euklidovským prostorem* a značíme E_n nebo $E(V_n)$. Ve smyslu poznámky 14.13 budeme v dalším výkladu zpravidla předpokládat, že skalární součin g na prostoru V_n je pevně dán, a tedy budeme místo $g(\boldsymbol{u}, \boldsymbol{v})$ psát jen $\boldsymbol{uv}$.

20.2. Definice. Soustava souřadnic $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ euklidovského prostoru $E(V_n)$, kde $\{\boldsymbol{u}_1, \boldsymbol{u}_2 \dots, \boldsymbol{u}_n\}$ je ortonormální báze unitárního prostoru V_n, se nazývá *kartézská soustava souřadnic*. *Úhlem* dvou nenulových vektorů $\boldsymbol{u}, \boldsymbol{v} \in V_n$ rozumíme ostrý úhel α takový, že

$$\cos\alpha = \frac{|\boldsymbol{uv}|}{\|\boldsymbol{u}\|\|\boldsymbol{v}\|}.$$

Vzdáleností dvou bodů $a, b \in E(V_n)$ rozumíme číslo $\|a - b\|$, tj. normu vektoru $a - b$.

20.3. Poznámka. Abychom si co nejvíce zjednodušili zápis, učiníme úmluvu, že místo $\boldsymbol{u} \in V_n$ budeme prostě psát $\boldsymbol{u} \in E_n$. Z kontextu je totiž vždy zcela zřejmé, kdy se jedná o body a kdy o vektory. Uvědomme si, že podle Cauchyovy nerovnosti 14.14 (i) je vždy $\cos\alpha \leq 1$, takže každé dva vektory svírají nějaký ostrý úhel. Nakonec poznamenejme, že je-li S nějaká kartézská soustava souřadnic v E_n a $b, c \in E$ jsou dva body o souřadnicích $\{b\}_S = (x_1, x_2, \dots, x_n)$, $\{c\}_S = (y_1, y_2, \dots, y_n)$ vzhledem k soustavě S, je podle věty 19.11 $\{b - c\}_S = (x_1 - y_1, x_2 - y_2, \dots, x_n - y_n)$, a tedy vzdálenost $\|b - c\|$ bodů b a c je podle poznámky 14.19 rovna $\sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}$.

20.4. Definice. Buď S kartézská soustava souřadnic v euklidovském prostoru E_3 a buďte $\boldsymbol{u}, \boldsymbol{v} \in E_3$ dva vektory. Jestliže $\{\boldsymbol{u}\}_S = (x_1, x_2, x_3)$, $\{\boldsymbol{v}\}_S = (y_1, y_2, y_3)$, pak vektor $\boldsymbol{w} \in E_3$ takový, že $\{\boldsymbol{w}\}_S = (x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_1)$ nazýváme *vektorovým součinem vektorů* $\boldsymbol{u}, \boldsymbol{v}$ (v tomto pořadí!) a značíme $\boldsymbol{u} \times \boldsymbol{v}$.

20.5. Poznámka. Vektorový součin vektorů v euklidovském prostoru E_3 jsme definovali pomocí jeho souřadnic vzhledem k předem dané kartézské soustavě souřadnic S. Aby takto zavedený pojem měl vůbec nějaký praktický význam, je zapotřebí, aby se choval „rozumně" při přechodu od dané soustavy S k jiné kartézské soustavě souřadnic. V následující části si předně ukážeme, že vektorový součin se sice při změně kartézské soustavy souřadnic změní, ale tak, že nejvýše změní znaménko. To tedy v podstatě znamená, že předchozí definicí je jednoznačně určen směr $\langle \boldsymbol{u} \times \boldsymbol{v} \rangle$ vektorového součinu vektorů $\boldsymbol{u}, \boldsymbol{v}$ a jeho velikost. Nicméně je tento pojem v praxi velmi důležitý, neboť jak brzy uvidíme, vektor $\boldsymbol{u} \times \boldsymbol{v}$ je buď vektor nulový, nebo je kolmý k oběma vektorům $\boldsymbol{u}$ a $\boldsymbol{v}$. Přitom $\boldsymbol{u} \times \boldsymbol{v} = 0$, právě když $\langle \boldsymbol{u} \rangle = \langle \boldsymbol{v} \rangle$, takže pro lineárně nezávislé vektory $\boldsymbol{u}, \boldsymbol{v}$ je $\langle \boldsymbol{u} \times \boldsymbol{v} \rangle$ ortogonální doplněk podprostoru $\langle \boldsymbol{u}, \boldsymbol{v} \rangle$ ve V_3.

20.6. Poznámka. Vraťme se ještě jednou k definici vektorového součinu 20.4 a podívejme se, jak si lze snadno výraz pro souřadnice vektorového součinu zapamatovat. Buď $\boldsymbol{a} = (a_1, a_2, a_3) \in R^3$ vektor a vyšetřujme determinant

$$[\![\{\boldsymbol{u}\}_S, \{\boldsymbol{v}\}_S, \boldsymbol{a}]\!] = \begin{vmatrix} x_1, & x_2, & x_3 \\ y_1, & y_2, & y_3 \\ a_1, & a_2, & a_3 \end{vmatrix}.$$

Bezprostředně je patrné, že i-tá souřadnice w_i, $i = 1, 2, 3$, vektorového součinu $\boldsymbol{u} \times \boldsymbol{v}$ je rovna algebraickému doplňku i-tého prvku třetího řádku. Odtud pak plynou dvě skutečnosti. Předně determinant $[\![\{\boldsymbol{u}\}_S, \{\boldsymbol{v}\}_S, \boldsymbol{a}]\!] = a_1 w_1 + a_2 w_2 + a_3 w_3 = \boldsymbol{a} \cdot \{\boldsymbol{u} \times \boldsymbol{v}\}_S$ je roven skalárnímu součinu vektorů $\boldsymbol{a}$ a $\{\boldsymbol{u} \times \boldsymbol{v}\}_S$ v unitárním prostoru (R^3, ω) (viz poznámku 14.2). Dále, zvolíme-li za $\boldsymbol{a}$ postupně jednotkové vektory $\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3$, je uvedený determinant postupně roven složkám w_1, w_2, w_3 souřadnic vektorového součinu $\{\boldsymbol{u} \times \boldsymbol{v}\}_S$. Jinými slovy $w_i = [\![\{\boldsymbol{u}\}_S, \{\boldsymbol{v}\}_S, \boldsymbol{e}_i]\!]$, $i = 1, 2, 3$.

20.7. Definice. Buďte $S = \{\boldsymbol{a}, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ a $S' = \{\boldsymbol{a}', \boldsymbol{u}'_1, \boldsymbol{u}'_2, \dots, \boldsymbol{u}'_n\}$ dvě kartézské soustavy souřadnic v euklidovském prostoru E_n. *Maticí přechodu od soustavy S k soustavě S'* rozumíme matici přechodu od báze $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ k bázi $\{\boldsymbol{u}'_1, \boldsymbol{u}'_2, \dots, \boldsymbol{u}'_n\}$.

20.8. Definice. Čtvercová matice $\boldsymbol{A} = (a_{ij}) \in R_n$ se nazývá *ortogonální*, jestliže její řádkové vektory tvoří ortonormální bázi unitárního prostoru (R^n, ω).

20.9. Poznámka. Připomeňme si, že v poznámce 14.2 jsme ověřili, že zobrazení ω, definované pro $\boldsymbol{u} = (x_1, x_2, \dots, x_n)$ a $\boldsymbol{v} = (y_1, y_2, \dots, y_n)$ z R^n předpisem $\omega(\boldsymbol{u}, \boldsymbol{v}) = \sum_{i=1}^n x_i y_i$ je skalární součin na aritmetickém vektorovém prostoru R^n. Ortogonálnost matice $\boldsymbol{A}$ ve smyslu předchozí definice neznamená nic jiného, než že její řádkové vektory jsou navzájem kolmé a mají normu 1 v unitárním prostoru (R^n, ω). Jak uvidíme, ortogonální matice jsou právě matice přechodu mezi ortonormálními bázemi unitárního prostoru. Zároveň ukážeme, že sloupce ortogonální matice tvoří rovněž ortonormální bázi prostoru (R^n, ω), tj. že matice transponovaná $\boldsymbol{A}^T$ je rovněž ortogonální a rovná se $\boldsymbol{A}^{-1}$.

20.10. Věta. *Buď $\boldsymbol{A} \in R_n$ ortogonální čtvercová matice stupně n. Pak* $\det \boldsymbol{A} = \pm 1$, *matice $\boldsymbol{A}$ je regulární, $\boldsymbol{A}^{-1} = \boldsymbol{A}^T$ a matice $\boldsymbol{A}^T$ je ortogonální.*

Důkaz. Označíme-li $\boldsymbol{C} = (c_{ij}) = \boldsymbol{A}\boldsymbol{A}^T$ je $c_{ij} = \sum_{k=1}^n a_{ik} a_{kj}^T = \sum_{k=1}^n a_{ik} a_{jk} = \omega(\boldsymbol{a}_i, \boldsymbol{a}_j) = \delta_{ij}$, kde $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n$ jsou řádkové vektory matice $\boldsymbol{A}$. Vidíme tedy, že $\boldsymbol{C} = \boldsymbol{E}$ je jednotková matice. Podle důsledku 8.5 je matice $\boldsymbol{A}$ regulární a $\boldsymbol{A}^{-1} = \boldsymbol{A}^T$. Dále podle věty o násobení determinantů 7.21 máme $1 = \det \boldsymbol{E} = \det \boldsymbol{A} \cdot \det \boldsymbol{A}^T = (\det \boldsymbol{A})^2$, takže $\det \boldsymbol{A} = \pm 1$. Nakonec z rovnosti $\boldsymbol{A}^T \boldsymbol{A} = \boldsymbol{E}$ dostáváme $\delta_{ij} = \sum_{k=1}^n a_{ik}^T a_{kj} = a_{ki} a_{kj}$, což znamená, že matice $\boldsymbol{A}^T$ je ortogonální. ■

20.11. Věta. *Buď (V_n, g) unitární prostor a M, M' dvě ortonormální báze tohoto prostoru. Pak matice přechodu od báze M k bázi M' je ortogonální. Obráceně, je-li $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ ortonormální báze unitárního prostoru (V_n, g) a $\boldsymbol{A} = (a_{ij})$ je ortogonální matice, pak množina $M' = \{\boldsymbol{u}'_1, \boldsymbol{u}'_2, \dots, \boldsymbol{u}'_n\}$, kde $\boldsymbol{u}'_i = \sum_{n=1}^n a_{ji} \boldsymbol{u}_i$, $i = 1, 2, \dots, n$, je ortonormální báze prostoru (V_n, g).*

Důkaz. Je-li $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ a $M' = \{\boldsymbol{u}'_1, \boldsymbol{u}'_2, \dots, \boldsymbol{u}'_n\}$, pak $\boldsymbol{u}'_i = \sum_{k=1}^n a_{ki} \boldsymbol{u}_k$. Dále je $g(\boldsymbol{u}'_i, \boldsymbol{u}'_j) = g(\sum_{k=1}^n a_{ki} \boldsymbol{u}_k, \sum_{l=1}^n a_{lj} \boldsymbol{u}_l) = \sum_{k=1}^n \sum_{l=1}^n a_{ki} a_{lj} g(\boldsymbol{u}_k, \boldsymbol{u}_l) =$

$\sum_{k=1}^{n}\sum_{l=1}^{n} a_{ki}a_{lj}\delta_{kl} = \sum_{k=1}^{n} a_{ki}a_{kj} = \omega(\boldsymbol{b}_i, \boldsymbol{b}_j)$, kde $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n$ jsou sloupcové vektory matice $\boldsymbol{A}$. Je-li nyní M' ortonormální báze ve (V_n, g), je $g(\boldsymbol{u}'_i, \boldsymbol{u}'_j) = \omega(\boldsymbol{b}_i, \boldsymbol{b}_j) = \delta_{ij}$ a matice $\boldsymbol{A}^T$, a tedy podle předchozí věty i matice $\boldsymbol{A}$ je ortogonální. Obráceně, je-li matice $\boldsymbol{A}$ ortogonální, je ortogonální i transponovaná matice $\boldsymbol{A}^T$, takže $\omega(\boldsymbol{b}_i, \boldsymbol{b}_j) = g(\boldsymbol{u}'_i, \boldsymbol{u}'_j) = \delta_{ij}$ a M' je ortonormální báze unitárního prostoru (V_n, g). ■

20.12. Poznámka. Ve větě 4.10 a poznámce 4.11 jsme ukázali, že násobit matici $\boldsymbol{B}$ maticí $\boldsymbol{A}$ zleva znamená totéž, jako provádět lineární kombinace na řádky matice $\boldsymbol{B}$, a to tak, že i-tý řádek součinu $\boldsymbol{AB}$ dostaneme jako lineární kombinaci řádků matice $\boldsymbol{B}$ s koeficienty v i-tém řádku matice $\boldsymbol{A}$. Vzhledem k tomu, že této skutečnosti použijeme dvakrát v následujícím důkazu, proveďme tuto úvahu poněkud podrobněji. Buď tedy $\boldsymbol{A} = (a_{ij})$ matice typu (m, n) s řádkovými vektory $\boldsymbol{a}_i$, $i = 1, 2, \ldots, m$, a $\boldsymbol{B} = (b_{ij})$ matice typu (n, k) s řádkovými vektory $\boldsymbol{b}_j$, $j = 1, 2, \ldots, n$. Pak $\boldsymbol{C} = \boldsymbol{AB} = (c_{ij})$ je matice typu (m, k) s řádkovými vektory $\boldsymbol{c}_i$, $i = 1, 2, \ldots, m$. Pohlížíme-li jako obvykle, na vektor $\boldsymbol{a}_i \in T^n$ jako na matici typu $(1, n)$, je součin matic $\boldsymbol{a}_i\boldsymbol{B}$ roven i-tému řádku $\boldsymbol{c}_i$ matice $\boldsymbol{C} = \boldsymbol{AB}$. Jinými slovy, matice $\boldsymbol{AB}$ má řádky $\boldsymbol{a}_1\boldsymbol{B}, \boldsymbol{a}_2\boldsymbol{B}, \ldots, \boldsymbol{a}_m\boldsymbol{B}$. Speciálně, jsou-li $\boldsymbol{A}, \boldsymbol{B}$ čtvercové matice stupně n, můžeme větu o násobení determinantů 7.21 interpretovat také takto: $\det \boldsymbol{C} = [\![\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n]\!] = [\![\boldsymbol{a}_1\boldsymbol{B}, \boldsymbol{a}_2\boldsymbol{B}, \ldots, \boldsymbol{a}_n\boldsymbol{B}]\!] = [\![\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n]\!] \det \boldsymbol{B} = \det \boldsymbol{A} \det \boldsymbol{B}$.

20.13. Věta. *Buďte $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3\}$ a $S' = \{a', \boldsymbol{u}'_1, \boldsymbol{u}'_2, \boldsymbol{u}'_3\}$ dvě kartézské soustavy souřadnic v euklidovském prostoru E_3, $\boldsymbol{u}, \boldsymbol{v} \in E_3$ buďte dva vektory. Označíme-li $\boldsymbol{w}$ vektorový součin vektorů $\boldsymbol{u}, \boldsymbol{v}$ vzhledem k soustavě S a $\boldsymbol{w}'$ jejich vektorový součin vzhledem k S', pak $\boldsymbol{w} = \boldsymbol{w}' \det \boldsymbol{B}$, kde $\boldsymbol{B}$ je matice přechodu od soustavy S k soustavě S'.*

Důkaz. Označíme-li $\{w\}_S = (w_1, w_2, w_3)$ a $\{w'\}_{S'} = (w'_1, w'_2, w'_3)$ a uvědomíme-li si, že $\{\boldsymbol{u}_i\}_S = \boldsymbol{e}_i$, $i = 1, 2, 3$, dostaneme podle poznámky 20.6, že $w_i = [\![\{\boldsymbol{u}\}_S, \{\boldsymbol{v}\}_S, \boldsymbol{e}_i]\!] = [\![\{\boldsymbol{u}\}_S, \{\boldsymbol{v}\}_S, \{\boldsymbol{u}_i\}_S]\!]$. Použitím věty 10.14 (i), předchozí poznámky, věty o násobení determinantů 7.21 a věty 7.3 postupně máme $w_i = [\![\{\boldsymbol{u}\}_S, \{\boldsymbol{v}\}_S, \{\boldsymbol{u}_i\}_S]\!] = [\![\{\boldsymbol{u}\}_{S'}\boldsymbol{B}^T, \{\boldsymbol{v}\}_{S'}\boldsymbol{B}^T, \{\boldsymbol{u}_i\}_{S'}\boldsymbol{B}^T]\!] = [\![\{\boldsymbol{u}\}_{S'}, \{\boldsymbol{v}\}_{S'}, \{\boldsymbol{u}_i\}_{S'}]\!] \det \boldsymbol{B}^T = [\![\{\boldsymbol{u}\}_{S'}, \{\boldsymbol{v}\}_{S'}, \{\boldsymbol{u}_i\}_{S'}]\!] \det \boldsymbol{B}$. Nyní podle vět 10.14 (ii) a 20.10 je $\boldsymbol{B}^T$ matice přechodu od soustavy souřadnic S' k soustavě S, a tedy $\{\boldsymbol{u}_i\}_{S'} = (b^T_{1i}, b^T_{2i}, b^T_{3i}) = (b_{i1}, b_{i2}, b_{i3})$, odkud podle poznámky 20.6 plyne $w_i = (b_{i1}w'_1 + b_{i2}w'_2 + b_{i3}w'_3) \det \boldsymbol{B}$ neboli $\{\boldsymbol{w}\}_S = \{\boldsymbol{w}'\}_{S'}\boldsymbol{B}^T \det \boldsymbol{B}$ podle předchozí poznámky. Na druhé straně věta 7.14 (i) dává $\{\boldsymbol{w}\}_S = \{\boldsymbol{w}\}_{S'}\boldsymbol{B}^T$, odkud porovnáním a vynásobením maticí $\boldsymbol{B}$ inverzní k $\boldsymbol{B}^T$ podle věty 20.10 dostaneme $\{\boldsymbol{w}\}_{S'} = \{\boldsymbol{w}'\}_{S'} \det \boldsymbol{B} = \{\boldsymbol{w}' \det \boldsymbol{B}\}_{S'}$. Protože podle věty 10.2 (ii) je zobrazení $\boldsymbol{w} \to \{\boldsymbol{w}\}_{S'}$ izomorfismus, je $\boldsymbol{w} = \boldsymbol{w}' \det \boldsymbol{B}$. ■

20.14. Věta. *Buď $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3\}$ kartézská soustava souřadnic v euklidovském prostoru E_3 a buďte $\boldsymbol{u}, \boldsymbol{v} \in E_3$ dva vektory. Označíme-li $\boldsymbol{u} \times \boldsymbol{v}$ vektorový součin těchto vektorů vzhledem k soustavě S, platí*

(i) $\boldsymbol{u} \times \boldsymbol{v} = -(\boldsymbol{v} \times \boldsymbol{u}) = (-\boldsymbol{v}) \times \boldsymbol{u} = \boldsymbol{v} \times (-\boldsymbol{u})$;

(ii) $\boldsymbol{u} \times \boldsymbol{v} = 0$, *právě když jsou vektory $\boldsymbol{u}$ a $\boldsymbol{v}$ lineárně závislé;*

(iii) $(\boldsymbol{u} \times \boldsymbol{v}) \perp \boldsymbol{u}$, $(\boldsymbol{u} \times \boldsymbol{v}) \perp \boldsymbol{v}$;

(iv) $\|\boldsymbol{u} \times \boldsymbol{v}\| = \|\boldsymbol{u}\|\|\boldsymbol{v}\| \sin\alpha$, *kde α je úhel vektorů $\boldsymbol{u}$ a $\boldsymbol{v}$, pokud $\boldsymbol{u}$ a $\boldsymbol{v}$ jsou nenulové;*

(v) $[\![\{u\}_S, \{v\}_S, \{u \times v\}]\!] \geq 0$, *přičemž rovnost nastává, právě když* $u \times v$ · *tj. právě když vektory* u *a* v *jsou lineárně závislé.*

Důkaz. Nechť $\{u\}_S = (x_1, x_2, x_3)$ a $\{v\}_S = (y_1, y_2, y_3)$ a $\{u \times v\}_S = (w_1, w_2, w_3)$.

(i) Podle poznámky 20.6 $w_i = [\![\{u\}_S, \{v\}_S, e_i]\!]$, kde $e_i \in R^3$ je jednotkový vektor, $i = 1, 2, 3$. Označíme-li $\{v \times u\}_S = (w'_1, w'_2, w'_3)$, je $w'_i = [\![\{v\}_S, \{u\}_S, e_i]\!] = -[\![\{u\}_S, \{v\}_S, e_i]\!] = -w_i$ podle věty 7.6 a zbytek tvrzení je zřejmý.

(ii) Jsou-li vektory u, v lineárně závislé, jsou lineárně závislé i vektory $\{u\}_S$, $\{v\}_S$ a $w_i = [\![\{u\}_S, \{v\}_S, e_i]\!] = 0$ pro každé $i = 1, 2, 3$ podle věty 7.18.

Předpokládejme tedy naopak, že $u \times v = 0$ a ukažme, že vektory u, v jsou lineárně závislé. Zvolme libovolně vektor $z \notin \langle u, v \rangle$. Podle poznámky 19.6 je $[\![\{u\}_S, \{v\}_S, \{z\}_S]\!] = \{z\}_S \cdot \{u \times v\}_S = 0$, takže vektory $\{u\}_S, \{v\}_S$ a $\{z\}_S$ jsou lineárně závislé podle věty 7.18. Protože zobrazení $u \to \{u\}_S$ je podle věty 10.2 (ii) izomorfismus, jsou vektory u, v, z lineárně závislé podle věty 9.20, takže existuje netriviální lineární kombinace $ru + sv + tz = 0$. Pro $t \neq 0$ dostáváme $z = -\frac{r}{t}u - \frac{s}{t}v \in \langle u, v \rangle$, což jest spor s volbou vektoru z. Je tedy nutně $t = 0$, lineární kombinace $ru + sv = 0$ je netriviální, a vektory u, v jsou tudíž lineárně závislé.

(iii) Podle poznámky 20.6 a věty 7.8 je $\{u\}_S \cdot \{u \times v\}_S = [\![\{u\}_S, \{v\}_S, \{u\}_S]\!] = 0$ a $\{v\}_S \cdot \{u \times v\}_S = [\![\{u\}_S, \{v\}_S, \{v\}_S]\!] = 0$. Podle věty 14.18 je zobrazení $\varphi(u) = \{u\}_S$ unitární, takže $u(u \times v) = v(u \times v) = 0$.

(iv) Podle poznámky 14.19 je $\|u \times v\|^2 = w_1^2 + w_2^2 + w_3^2 = (x_2y_3 - x_3y_2)^2 + (x_3y_1 - x_1y_3)^2 + (x_1y_2 - x_2y_1)^2 = \|u\|^2\|v\|^2 - x_1^2y_1^2 - x_2^2y_2^2 - x_3^2y_3^2 - 2x_1x_2y_1y_2 - 2x_1x_3y_1y_3 - 2x_2x_3y_2y_3 = \|u\|^2\|v\|^2 - (uv)^2 = \|u\|^2\|v\|^2(1 - \frac{(uv)^2}{\|u\|^2\|v\|^2}) = \|u\|^2\|v\|^2(1 - \cos^2\alpha) = \|u\|^2\|v\|^2 \sin^2\alpha$, a tedy $\|u \times v\| = \|u\|\|v\| \sin\alpha$.

(v) Podle poznámek 20.6 a 14.19 je $[\![\{u\}_S, \{v\}_S, \{u \times v\}_S]\!] = \{u \times v\}_S \{u \times v\}_S = \|u \times v\|^2 = w_1^2 + w_2^2 + w_3^2$ a jsme hotovi. ∎

20.15 *Poznámka.* Přihlédneme-li k poznámce 20.6, můžeme pojem vektorového součinu rozšířit na euklidovské prostory E_n pro $n \geq 2$. Buď S kartézská soustava souřadnic v euklidovském prostoru E_n. Jsou-li $u_1, u_2, \ldots, u_{n-1}$ vektory z E_n, pak rozvojem determinantu $[\![\{u_1\}_S, \{u_2\}_S, \ldots, \{u_{n-1}\}_S, a]\!]$, kde $a = (a_1, a_2, \ldots, a_n) \in R^n$, podle posledního řádku dostaneme číslo $\sum_{i=1}^n a_i w_i$. Vektor w takový, že $\{w\}_S = (w_1, w_2, \ldots, w_n)$ se nazývá *vnější součin vektorů* $u_1, u_2, \ldots, u_{n-1}$. Analogicky jako u vektorového součinu čtenář snadno sám ověří, že platí

(i) při změně kartézské soustavy souřadnic změní vnější součin nejvýše znaménko;

(ii) je-li $\pi \in S_{n-1}$ libovolná permutace, pak vnější součin vektorů $u_{\pi(1)}, u_{\pi(2)}, \ldots, u_{\pi(n-1)}$ dostaneme z vnějšího součinu vektorů $u_1, u_2, \ldots, u_{n-1}$ vynásobením číslem zn π;

(iii) vnější součin je roven nulovému vektoru, právě když jsou vektory $u_1, u_2, \ldots, u_{n-1}$ lineárně závislé;

(iv) vnější součin je kolmý ke všem vektorům $u_1, u_2, \ldots, u_{n-1}$;

(v) $[\![\{u_1\}_S, \{u_2\}_S, \ldots, \{u_{n-1}\}_S, \{w\}_S]\!] \geq 0$, přičemž rovnost nastane, právě když vnější součin w je roven nulovému vektoru.

20.16. Věta. *Buď S kartézská soustava souřadnic v euklidovském prostoru E_3 a buďte u, v, u', v' čtyři vektory z E_3. Pak platí*

$$(\boldsymbol{u}\times\boldsymbol{v})(\boldsymbol{u}'\times\boldsymbol{v}') = (\boldsymbol{u}\boldsymbol{u}')(\boldsymbol{v}\boldsymbol{v}') - (\boldsymbol{v}\boldsymbol{u}')(\boldsymbol{u}\boldsymbol{v}') = \begin{vmatrix} \boldsymbol{u}\boldsymbol{u}', & \boldsymbol{v}\boldsymbol{u}' \\ \boldsymbol{u}\boldsymbol{v}', & \boldsymbol{v}\boldsymbol{v}' \end{vmatrix}.$$

Důkaz. Jsou-li vektory $\boldsymbol{u}, \boldsymbol{v}$ lineárně závislé, $\boldsymbol{v} = r\boldsymbol{u}$, pak podle věty 20.14 (ii) je $\boldsymbol{u}\times\boldsymbol{v} = 0$, takže $(\boldsymbol{u}\boldsymbol{u}')r(\boldsymbol{u}\boldsymbol{v}') - r(\boldsymbol{u}\boldsymbol{u}')(\boldsymbol{u}\boldsymbol{v}') = \begin{vmatrix} \boldsymbol{u}\boldsymbol{u}', & r\boldsymbol{u}\boldsymbol{u}' \\ \boldsymbol{u}\boldsymbol{v}', & r\boldsymbol{u}\boldsymbol{v}' \end{vmatrix} = 0$.

Nechť tedy vektory $\boldsymbol{u}, \boldsymbol{v}$ jsou lineárně nezávislé. Z věty 14.8 plyne, že můžeme zvolit kartézskou soustavu souřadnic $S' = \{a', \boldsymbol{u}_1', \boldsymbol{u}_2', \boldsymbol{u}_3'\}$ tak, aby $\boldsymbol{u} \in \langle \boldsymbol{u}_1' \rangle$ a $\boldsymbol{v} \in \langle \boldsymbol{u}_1', \boldsymbol{u}_2' \rangle$. Přitom vhodnou volbou znaménka u vektoru $\boldsymbol{u}_3'$ můžeme dosáhnout toho, aby determinant matice přechodu od soustavy S k soustavě S' byl roven jedné. Podle věty 20.13 jsou pak vektorové součiny $\boldsymbol{u}\times\boldsymbol{v}$ a $\boldsymbol{u}'\times\boldsymbol{v}'$ vzhledem k oběma soustavám souřadnic S a S' stejné. Přitom $\{\boldsymbol{u}\}_{S'} = (x_1, 0, 0)$, $\{\boldsymbol{v}\}_{S'} = (y_1, y_2, 0)$, $\{\boldsymbol{u}'\}_{S'} = (x_1', x_2', x_3')$, $\{\boldsymbol{v}'\}_{S'} = (y_1', y_2', y_3')$, $\{\boldsymbol{u}\times\boldsymbol{v}\}_{S'} = (0, 0, x_1y_2)$ a tedy $(\boldsymbol{u}\times\boldsymbol{v})(\boldsymbol{u}'\times\boldsymbol{v}') = x_1y_2(x_1'y_2' - x_2'y_1')$. Na druhé straně máme $\boldsymbol{u}\boldsymbol{u}' = x_1x_1'$, $\boldsymbol{v}\boldsymbol{v}' = y_1y_1' + y_2y_2'$, $\boldsymbol{u}\boldsymbol{v}' = x_1y_1'$, $\boldsymbol{v}\boldsymbol{u}' = y_1x_1' + y_2x_2'$, odkud dostáváme $(\boldsymbol{u}\boldsymbol{u}')(\boldsymbol{v}\boldsymbol{v}') - (\boldsymbol{v}\boldsymbol{u}')(\boldsymbol{u}\boldsymbol{v}') = x_1x_1'(y_1y_1' + y_2y_2') - x_1y_1'(y_1x_1' + y_2x_2') = x_1y_2(x_1'y_2' - x_2'y_1')$ a jsme hotovi. ∎

20.17. Definice. Buď $\varrho = a + W$ nadrovina euklidovského prostoru E_n. Podle věty 14.7 je ortogonální doplněk podprostoru W ve V_n jednorozměrným podprostorem $\langle \boldsymbol{u} \rangle$ ve V_n. Směr $\langle \boldsymbol{u} \rangle$ (nebo pro jednoduchost stručně každý nenulový vektor z $\langle \boldsymbol{u} \rangle$) nazýváme *směrem normály* nadroviny ϱ. Každou přímku v E_n o směru $\langle \boldsymbol{u} \rangle$ nazýváme normálou nadroviny ϱ.

20.18. Věta. *Buď $\sum_{i=1}^n a_ix_i = b$ rovnice nadroviny ϱ euklidovského prostoru E_n vzhledem k nějaké kartézské soustavě souřadnic S (viz věta 19.15). Pak směr $\langle \boldsymbol{u} \rangle$, kde $\{\boldsymbol{u}\}_S = (a_1, a_2, \ldots, a_n)$ je směrem normály nadroviny ϱ.*

Důkaz. Buď $\boldsymbol{v}$ libovolný vektor z nadroviny ϱ a $a \in \varrho$ buď libovolný bod. Položme $c = a + v$ a nechť $\{a\}_S = (x_1, x_2, \ldots, x_n)$, $\{c\}_S = (y_1, y_2, \ldots, y_n)$. Podle věty 19.11 je $\{\boldsymbol{v}\}_S = \{c - a\}_S = (y_1 - x_1, y_2 - x_2, \ldots, y_n - x_n)$. Přitom podle věty 19.15 je $\sum_{i=1}^n a_ix_i = b$, $\sum_{i=1}^n a_iy_i = b$, takže $\sum_{i=1}^n a_i(y_i - x_i) = 0$. To však znamená, že $\boldsymbol{u}\boldsymbol{v} = 0$, vektor $\boldsymbol{u}$ je kolmý ke každému vektoru nadroviny ϱ, a $\boldsymbol{u}$ je tedy vektor normály této nadroviny. ∎

Ve zbytku tohoto odstavce se budeme věnovat jednak úhlům, jednak dvěma aspektům vzdálenosti v euklidovském prostoru. Předně probereme vzdálenost dvou rovnoběžných podprostorů a poté se budeme zabývat vzdáleností dvou mimoběžek. Připomeňme, že studium těchto pojmů je umožněno díky skalárnímu součinu a že něco podobného nelze provádět v prostoru afinním.

20.19. Lemma. *Buď α úhel dvou nenulových vektorů $\boldsymbol{u}$ a $\boldsymbol{v}$ v euklidovském prostoru E_n. Jestliže $\boldsymbol{u}' = r\boldsymbol{u}$ a $\boldsymbol{v}' = s\boldsymbol{v}$, kde $rs \neq 0$, pak úhel vektorů $\boldsymbol{u}'$ a $\boldsymbol{v}'$ je rovněž roven α.*

Důkaz. Označíme-li β úhel vektorů $\boldsymbol{u}'$ a $\boldsymbol{v}'$, pak podle definice 20.2 je

$$\cos\beta = \frac{|\boldsymbol{u}'\boldsymbol{v}'|}{\|\boldsymbol{u}'\|\|\boldsymbol{v}'\|} = \frac{|(r\boldsymbol{u})(s\boldsymbol{v})|}{\|r\boldsymbol{u}\|\|s\boldsymbol{v}\|} = \frac{|rs||\boldsymbol{u}\boldsymbol{v}|}{|rs|\|\boldsymbol{u}\|\|\boldsymbol{v}\|} = \cos\alpha,$$

takže $\alpha = \beta$ vzhledem k tomu, že úhly α a β jsou ostré. ∎

20.20. Definice. *Úhlem směrů* $\langle \boldsymbol{u} \rangle$, $\langle \boldsymbol{v} \rangle$ euklidovského prostoru E_n rozumíme úhel vektorů $\boldsymbol{u}$, $\boldsymbol{v}$. *Úhel dvou přímek* $a + \langle \boldsymbol{u} \rangle$ a $b + \langle \boldsymbol{v} \rangle$ v E_n je úhel směrů $\langle \boldsymbol{u} \rangle$ a $\langle \boldsymbol{v} \rangle$. *Úhel přímky* $a + \langle \boldsymbol{u} \rangle$ *a nadroviny* ϱ v E_n je doplněk úhlu směru $\langle \boldsymbol{u} \rangle$ a směru normály nadroviny ϱ (připomeňme, že úhel α je doplňkem úhlu β, jestliže $\alpha + \beta = \frac{\pi}{2}$). Konečně *úhlem dvou nadrovin* rozumíme úhel směrů jejich normál.

20.21. Věta. *Nechť $a + W$, $b + W'$, $W' \subseteq W$ jsou dva rovnoběžné podprostory euklidovského prostoru E_n. Pak platí*

(i) pro každý bod $c \in b + W'$ se podprostory $c + W^{\perp}$ a $a + W$ protínají v jediném bodě;

(ii) označíme-li $F(c)$ průsečík podprostorů z tvrzení (i), je F izometrické afinní zobrazení podprostoru $b + W'$ na podprostor $F(b) + W'$ prostoru $a + W$ vytvořené identickým automorfismem $1_{W'}$ vektorového prostoru W';

(iii) pro každé dva body $b_1, b_2 \in b + W'$ je $\|b_1 - F(b_1)\| = \|b_2 - F(b_2)\|$;

(iv) je-li $c \in F(b) + W'$ libovolný bod, pak $\|c - b\| \geq \|F(b) - b\|$, přičemž rovnost platí, právě když $c = F(b)$.

Důkaz. (i) Podle věty 14.7 (i) je $W \vee W^{\perp} = V_n$, takže $a - c \in W \vee W^{\perp}$ a podprostory $c + W^{\perp}$ a $a + W$ jsou různoběžné podle věty 19.19. Přitom se tyto podprostory protínají v jediném bodě, neboť v opačném případě by existovala přímka $d + \langle \boldsymbol{u} \rangle \subseteq (c + W^{\perp}) \cap (a + W)$, což by vedlo ke sporu $0 \neq \boldsymbol{u} \in W^{\perp} \cap W = 0$.

(ii) Podle (i) existují vektory $\boldsymbol{u}_1 \in W^{\perp}$ a $\boldsymbol{u}_2 \in W$ takové, že $F(b) = b + \boldsymbol{u}_1 = a + \boldsymbol{u}_2$. Pro každé $\boldsymbol{u} \in W'$ pak je $F(b) + \boldsymbol{u} = b + \boldsymbol{u}_1 + \boldsymbol{u} = a + \boldsymbol{u}_2 + \boldsymbol{u} \in ((b + \boldsymbol{u}) + W^{\perp}) \cap (a + W)$, a tudíž $F(b + \boldsymbol{u}) = F(b) + \boldsymbol{u}$. Vidíme tedy, že F je afinní zobrazení vytvořené identickým automorfismem prostoru W' a zbývá ukázat, že F je izometrie. Jsou-li $b_1 = b + \boldsymbol{v}_1$, $b_2 = b + \boldsymbol{v}_2$ dva body z $b + W'$, je $F(b_i) = F(b) + \boldsymbol{v}_i = b + \boldsymbol{u}_1 + \boldsymbol{v}_i$, $i = 1, 2$, a podle lemmatu 20.6 máme $\|F(b_2) - F(b_1)\| = \|(b + \boldsymbol{u}_1 + \boldsymbol{v}_2) - (b + \boldsymbol{u}_1 + \boldsymbol{v}_1)\| = \|(b + \boldsymbol{v}_2) - (b + \boldsymbol{v}_1)\| = \|b_2 - b_1\|$.

(iii) Při stejném označení jako v předchozí části je $\|b_1 - F(b_1)\| = \|(b + \boldsymbol{v}_1) - (b + \boldsymbol{u}_1 + \boldsymbol{v}_1)\| = \|\boldsymbol{u}_1\|$ a $\|b_2 - F(b_2)\| = \|(b + \boldsymbol{v}_2) - (b + \boldsymbol{u}_1 + \boldsymbol{v}_2)\| = \|\boldsymbol{u}_1\|$.

(iv) Buď $c = F(b) + \boldsymbol{u} = b + \boldsymbol{u}_1 + \boldsymbol{u}$, kde $\boldsymbol{u}_1 \in W^{\perp}$ a $\boldsymbol{u} \in W' \leq W$. Protože $\boldsymbol{u} \perp \boldsymbol{u}_1$, je $\|F(b) - b\|^2 = \|\boldsymbol{u}_1\|^2 = \|\boldsymbol{u}_1 + \boldsymbol{u} - \boldsymbol{u}\|^2 = ((\boldsymbol{u}_1 + \boldsymbol{u}) - \boldsymbol{u})((\boldsymbol{u}_1 + \boldsymbol{u}) - \boldsymbol{u}) = \|\boldsymbol{u}_1 + \boldsymbol{u}\|^2 - \|\boldsymbol{u}\|^2 - \|\boldsymbol{u}\|^2 + \|\boldsymbol{u}\|^2 = \|\boldsymbol{u}_1 + \boldsymbol{u}\|^2 - \|\boldsymbol{u}\|^2 \leq \|\boldsymbol{u}_1 + \boldsymbol{u}\|^2 = \|c - b\|^2$. Přitom rovnost nastane, právě když $\boldsymbol{u} = 0$, tj. právě když $c = F(b)$. ■

20.22. Definice. Nechť $a + W$, $b + W'$, $W' \subseteq W$ jsou dva rovnoběžné podprostory euklidovského prostoru E_n. *Vzdáleností těchto podprostorů* rozumíme číslo $\|b - F(b)\|$, kde F je zobrazení z předchozí věty.

20.23. Věta. *Buď $r = c + \langle \boldsymbol{w} \rangle$ příčka mimoběžek $p = a + \langle \boldsymbol{u} \rangle$ a $q = b + \langle \boldsymbol{v} \rangle$ v euklidovském prostoru E_3. Pak r je nejkratší příčka mimoběžek p a q, právě když $\boldsymbol{w} \perp \boldsymbol{u}$ a $\boldsymbol{w} \perp \boldsymbol{v}$, tj. právě když $\langle \boldsymbol{u}, \boldsymbol{v} \rangle^{\perp} = \langle \boldsymbol{w} \rangle$.*

Důkaz. Bez újmy na obecnosti můžeme předpokládat, že $r \cap p = a$, $r \cap q = b$. Buď $\boldsymbol{w} \perp \boldsymbol{u}$, $\boldsymbol{w} \perp \boldsymbol{v}$. Protože $\langle \boldsymbol{u} \rangle \neq \langle \boldsymbol{v} \rangle$, je $\langle \boldsymbol{u}, \boldsymbol{v} \rangle^{\perp} = \langle \boldsymbol{w} \rangle$ podle věty 14.7 (ii), takže příčka $r = c + \langle \boldsymbol{w} \rangle$ mimoběžek p a q ve směru $\boldsymbol{w}$ existuje podle věty 19.26. Abychom dokázali, že tato příčka je nejkratší, potřebujeme zjevně ověřit, že pro každou příčku $r' = c' + \langle \boldsymbol{w}' \rangle$ mimoběžek p, q takovou, že $p \cap r' = a'$, $q \cap r' = b'$ je $\|a' - b'\| \geq \|a - b\|$, přičemž rovnost nastává, právě když $a' = a$ a $b' = b$. Protože

$a' \in p$, $b' \in q$, je $a' = a + \alpha\boldsymbol{u}$ a $b' = b + \beta\boldsymbol{v}$ pro nějaká reálná čísla α, β. Dále vektor $a - b$ leží ve $\langle \boldsymbol{w} \rangle$, tedy $a - b = \gamma\boldsymbol{w}$, odkud vzhledem k tomu, že $\boldsymbol{w} \perp \boldsymbol{u}$, $\boldsymbol{w} \perp \boldsymbol{v}$ pomocí lemmatu 19.6 dostáváme $\|a' - b'\|^2 = \|(a + \alpha\boldsymbol{u}) - (b + \beta\boldsymbol{v})\|^2 = \|\gamma\boldsymbol{w} + \alpha\boldsymbol{u} - \beta\boldsymbol{v}\|^2 = \|\gamma\boldsymbol{w}\|^2 + \|\alpha\boldsymbol{u} - \beta\boldsymbol{v}\|^2 \geq \|a - b\|^2$. Přitom rovnost zřejmě platí, právě když $\alpha\boldsymbol{u} - \beta\boldsymbol{v} = 0$, tj. právě když $\alpha = \beta = 0$ vzhledem k tomu, že vektory $\boldsymbol{u}, \boldsymbol{v}$ jsou lineárně nezávislé. To je však ekvivalentní s tím, že $a' = a$ a $b' = b$. ∎

20.24. Definice. Buďte $p = a + \langle \boldsymbol{u} \rangle$ a $q = b + \langle \boldsymbol{v} \rangle$ dvě mimoběžky v euklidovském prostoru E_3. Je-li $r = c + \langle \boldsymbol{w} \rangle$ nejkratší příčka mimoběžek p a q taková, že $r \cap p = a$ a $r \cap q = b$, pak číslo $\|a - b\|$ se nazývá *vzdálenost mimoběžek* p a q.

20.25. Příklady. 1. V euklidovském prostoru $E_3 = E(R^3)$ nalezněme nejkratší příčku a spočtěme vzdálenost mimoběžek

$$p : \frac{x-1}{2} = \frac{y+8}{3} = \frac{z-11}{-6} \quad \text{a} \quad q : \frac{x-8}{6} = \frac{y-3}{-1} = \frac{z-13}{12}.$$

Ř e š e n í : Podle poznámky 19.12 je $p = a + \langle \boldsymbol{u} \rangle$ a $q = b + \langle \boldsymbol{v} \rangle$, kde $a = (1, -8, 11)$, $\boldsymbol{u} = (2, 3, -6)$, $b = (8, 3, 13)$ a $\boldsymbol{v} = (6, -1, 12)$. Snadno se ověří, že vektory $a - b$, $\boldsymbol{u}$, $\boldsymbol{v}$ jsou lineárně nezávislé, takže přímky p a q jsou skutečně mimoběžné podle důsledku 19.20. Směr $\boldsymbol{w}$ kolmý k oběma vektorům $\boldsymbol{u}$, $\boldsymbol{v}$ můžeme podle věty 20.14 (iii) nalézt pomocí vektorového součinu $\boldsymbol{w}' = \boldsymbol{u} \times \boldsymbol{v} = (30, -60, -20)$. Musíme tedy nejprve nalézt příčku mimoběžek p a q o směru $\boldsymbol{w} = (3, -6, -2)$. Podobně jako v odstavci 19.28 proložíme rovinu ϱ přímkou p a směrem $\boldsymbol{w}$. Směr normály roviny ϱ je určen vektorovým součinem $\boldsymbol{u} \times \boldsymbol{w} = (-42, -14, -21)$, takže rovina ϱ má podle věty 20.18 rovnici $6x + 2y + 3z = d$, kde pravou stranu d spočteme dosazením složek bodu a, $d = 23$. Dále, průsečík c přímky $q = b + t\boldsymbol{v}$ s rovinou ϱ spočteme opět dosazením. Máme $6(8+6t)+2(3-t)+3(13+12t) = 23$, $48+36t+6-2t+39+36t-23 = 0$, odkud $t = -1$ a $c = (2, 4, 1)$. Hledaná příčka tedy je $r = c + \langle \boldsymbol{w} \rangle = (2, 4, 1) + \langle (3, -6, -2) \rangle$. Ke stanovení vzdálenosti mimoběžek p a q potřebujeme ještě spočítat průsečík $d = r \cap p$ a poté vzdálenost $\|c - d\|$. Pro průsečík d musí platit $(1, -8, 11) + t(2, 3, -6) = (2, 4, 1) + s(3, -6, -2)$ pro vhodné hodnoty parametrů t, s. Po rozepsání do složek dostaneme soustavu tří rovnic, která, jak se snadno zjistí, má řešení $t = 2$, $s = 1$. Tedy $d = (5, -2, -1)$ a $\|c - d\| = \|(-3, 6, 2)\| = \sqrt{9 + 36 + 4} = 7$, což je vzdálenost mimoběžek p a q.

2. V euklidovském prostoru $E_4 = E(R^4)$ určeme vzdálenost rovnoběžných rovin

$$\varrho = (1, 2, 0, 1) + \langle (4, 1, -1, -1), (4, -2, 2, -1) \rangle \quad \text{a}$$

$$\sigma = (6, 7, 3, 4) + \langle (8, -1, 1, -2), (0, 1, -1, 0) \rangle.$$

Ř e š e n í : Nejprve ověřme, že roviny ϱ a σ jsou skutečně rovnoběžné, tj. že při našem obvyklém značení je $W \vee W'$. Protože zřejmě $\dim W = \dim W' = 2$, stačí nám ukázat, že $\dim\,(W \vee W') = 2$. Jest

$$\begin{pmatrix} 4, & 1, & -1, & -1 \\ 4, & -2, & 2, & -1 \\ 8, & -1, & 1, & -2 \\ 0, & 1, & -1, & 0 \end{pmatrix} \sim \begin{pmatrix} 4, & 1, & -1, & -1 \\ 0, & -3, & 3, & 0 \\ 0, & -3, & 3, & 0 \\ 0, & 1, & -1, & 0 \end{pmatrix},$$

odkud je již rovnoběžnost rovin ϱ a σ zřejmá. Podle věty 20.21 nyní potřebujeme nalézt ortogonální doplněk $W^{\perp}$ a spočítat průsečík $F(b) = (b + W^{\perp}) \cap (a + W)$. Uvědomíme-li si, že $W = W'$, tvoří poslední dva řádky matice vlevo matici homogenní soustavy rovnic, jejíž řešení je $W^{\perp}$. Vidíme tedy ihned, že $W^{\perp} = \langle(1,0,0,4),(0,1,1,0)\rangle$. Z rovnosti $(6,7,3,4)+\alpha(1,0,0,4)+\beta(0,1,1,0) = (1,2,0,1)+\gamma(4,1,-1,-1)+\delta(4,-2,2,-1)$ dostaneme nehomogenní soustavu lineárních rovnic a máme

$$\left(\begin{array}{cccc|c} 1, & 0, & -4, & -4 & -5 \\ 0, & 1, & -1, & 2 & -5 \\ 0, & 1, & 1, & -2 & -3 \\ 4, & 0, & 1, & 1 & -3 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1, & 0, & -4, & -4 & -5 \\ 0, & 1, & -1, & 2 & -5 \\ 0, & 0, & 2, & -4 & 2 \\ 0, & 0, & 17, & 17 & 17 \end{array}\right) \sim$$

$$\left(\begin{array}{cccc|c} 1, & 0, & -4, & -4 & -5 \\ 0, & 1, & -1, & 2 & -5 \\ 0, & 0, & 1, & -2 & 1 \\ 0, & 0, & 0, & 3 & 0 \end{array}\right).$$

Tedy $\delta = 0$, $\gamma = 1$, $\beta = -4$, $\alpha = -1$ a $F(b) = (5,3,-1,0)$. Nakonec spočteme vzdálenost rovin ϱ a σ. Jest $\|b - F(b)\| = \|(1,4,4,4)\| = \sqrt{1+16+16+16} = 7$.

3. Určeme úhel přímky p dané soustavou rovnic $x + y + 3z = 0$, $x - y - z = 0$ s rovinou ϱ danou rovnicí $2x + y + z = -1$.

Ř e š e n í : Řešením soustavy rovnic, které určují přímku p, dostaneme, že p má směr $\langle \boldsymbol{u} \rangle$, kde $\boldsymbol{u} = (1,2,-1)$ a prochází bodem $(0,0,0)$. Podle věty 20.18 je vektor $\boldsymbol{v} = (2,1,1)$ vektorem normály roviny ϱ. Pro úhel β vektorů $\boldsymbol{u}, \boldsymbol{v}$ platí $\cos\beta = \frac{|2+2-1|}{\sqrt{6}\sqrt{6}} = \frac{1}{2}$, takže $\beta = 60^o$ a hledaný úhel je podle definice 20.20 $\alpha = 30^o$.

Metodami popsanými v tomto odstavci můžeme řešit nejrůznější další geometrické úlohy. Pro ilustraci uvedeme následující příklad.

4. Bodem $b = (-1,1,-1)$ veďme v rovině ϱ o rovnici $x + y + z = -1$ přímku kolmou k přímce p dané soustavou rovnic $y - z = -1$, $x + 2y = 0$.

Ř e š e n í : Dosazením složek bodu b do rovnice roviny ϱ snadno ověříme, že bod b v rovině ϱ leží, a úloha má tedy smysl. Hledaná přímka $q = b + \langle \boldsymbol{u} \rangle$ musí procházet daným bodem b a vektor $\boldsymbol{u}$ musí být kolmý ke směrovému vektoru $\boldsymbol{v}$ přímky p, a protože přímka q má ležet v rovině ϱ, musí být vektor $\boldsymbol{u}$ kolmý k vektoru normály $\boldsymbol{w}$ roviny ϱ. Řešením soustavy rovnic pro p dostaneme $p = (0,0,1) + \langle(-2,1,1)\rangle$, takže $\boldsymbol{v} = (-2,1,1)$ a $\boldsymbol{w} = (1,1,1)$ podle věty 20.18. Vektor $\boldsymbol{u}$ kolmý jak k $\boldsymbol{v}$, tak k $\boldsymbol{w}$ dostaneme jako vektorový součin $\boldsymbol{u} = \boldsymbol{v} \times \boldsymbol{w} = (0,3,-3)$. Hledaná přímka tedy je $q = (-1,1,-1) + \langle(0,1,-1)\rangle$ nebo parametricky $\frac{x+1}{0} = \frac{y-1}{1} = \frac{z+1}{-1}$.

21.1. Poznámka. Dříve než přistoupíme k vlastnímu studiu projektivních prostorů, podívejme se ve stručnosti na jednu ze základních motivací k jejich zkoumání. V afinní rovině $A_2(R^2)$ zvolme soustavu souřadnic $S = \{(0,0),(1,0),(0,1)\}$. Přímka p o rovnici $x - 1 = 0$ je rovnoběžná s osou $y : (0,0) + \langle(0,1)\rangle$ a prochází bodem $(0,1)$. Na přímce p zvolme soustavu souřadnic $S' = \{(1,0),(0,1)\}$ a buď $a = (1,x)$ libovolný bod přímky p. Protože $(1,x)-(1,0) = x(0,1)$, je $\{a\}_{S'} = (x)$. Bod a spolu s počátkem soustavy souřadnic S, bodem $(0,0)$, určuje přímku $q : (0,0) + \langle(1,x)\rangle$, která podle odstavce 19.22 protíná přímku p v jediném bodě a. Daný bod a tedy jednoznačně určuje směr $\langle(1,x)\rangle$ v právě uvedeném smyslu. Jestliže je naopak dán směr $\langle(r,s)\rangle$, $r \neq 0$, v rovině A_2, pak přímka $(0,0) + \langle(r,s)\rangle$ protne přímku p v jediném bodě, a to zřejmě v bodě $a = (1, \frac{s}{r})$. Vidíme tedy, že mezi body přímky p a směry $\langle(r,s)\rangle$ v rovině A_2 pro které je $r \neq 0$, existuje vzájemně jednoznačná korespondence. Kromě toho směr $\langle(0,1)\rangle$ je směrem přímky p.

Jestliže shrneme a zobecníme získané poznatky, vidíme, že afinní prostor A_n můžeme také zkoumat pomocí směrů v afinním prostoru o jednotku větší dimenze. Preciznější popis tohoto postupu odložíme na pozdější dobu a nyní se začneme věnovat práci se směry ve vektorovém prostoru, tj. s projektivním prostorem.

21.2. Definice. Řekneme, že je dán n-rozměrný *projektivní prostor* $P_n(V_{n+1})$, je-li dáno:

(1) množina P_n;

(2) vektorový prostor V_{n+1};

(3) vzájemně jednoznačné zobrazení φ množiny $\{\langle \boldsymbol{u}\rangle | 0 \neq \boldsymbol{u} \in V_{n+1}\}$ na množinu P_n.

Speciálně je tedy P_0 jednoprvková množina, a abychom si v dalším výkladu usnadnili vyjadřování, označme ještě P_{-1} jako prázdnou množinu.

Prvky množiny P_n se nazývají *geometrické body*, nenulové vektory z V_{n+1} se nazývají *aritmetické body*. Vektorový prostor V_{n+1} se nazývá *aritmetický základ* prostoru P_n. Každý vektor $0 \neq \boldsymbol{u} \in V_{n+1}$ se nazývá *aritmetický zástupce* geometrického bodu $\varphi(\langle \boldsymbol{u}\rangle)$.

21.3. Poznámka. V projektivním prostoru $P_n(V_{n+1})$ tedy každému aritmetickému bodu $0 \neq \boldsymbol{u} \in V_{n+1}$ odpovídá jediný geometrický bod $\varphi(\langle \boldsymbol{u}\rangle)$, zatímco geometrické body mohou mít více aritmetických zástupců. Přitom je-li $\boldsymbol{u}$ jeden z nich, jsou všechny ostatní tvaru $r\boldsymbol{u}$, kde $0 \neq r \in T$. Například je-li V_{n+1} reálný vektorový prostor, má každý geometrický bod nekonečně mnoho aritmetických zástupců.

21.4. Definice. *Podprostorem* $P_k(V_{k+1})$ projektivního prostoru $P_n(V_{n+1})$ rozumíme projektivní prostor takový, že $P_k \subseteq P_n$, $V_{k+1} \leq V_{n+1}$, a zobrazení ψ příslušné prostoru $P_k(V_{k+1})$ je restrikcí zobrazení φ na množinu $\{\langle \boldsymbol{u}\rangle | 0 \neq \boldsymbol{u} \in V_{k+1}\}$.

21.5. Poznámka. V definici 21.2 hraje podstatnou roli množina $\{\langle \boldsymbol{u}\rangle | 0 \neq \boldsymbol{u} \in V_{n+1}\}$ všech směrů vektorového prostoru V_{n+1}. Zobrazení φ pak zcela mechanicky přenáší vlastnosti této množiny na množinu P_n. Z tohoto důvodu se můžeme při studiu abstraktních vlastností projektivního prostoru omezit pouze na množinu $\{\langle \boldsymbol{u}\rangle | 0 \neq \boldsymbol{u} \in V_{n+1}\}$ a pokládat zobrazení φ za identické. Nebude-li tedy v dalším výkladu řečeno jinak, budeme projektivním prostorem rozumět vždy množinu $P_n = \{\langle \boldsymbol{u}\rangle | 0 \neq \boldsymbol{u} \in V_{n+1}\}$.

21.6. Věta. *Buďte $P_k(V_{k+1})$ a $P_l(V_{l+1})$ dva podprostory projektivního prostoru $P_n(V_{n+1})$. Pak platí*

(i) množina $P_k \vee P_l = \{\langle \boldsymbol{u} \rangle | 0 \neq \boldsymbol{u} \in V_{k+1} \vee V_{l+1}\}$ je podprostorem prostoru $P_n(V_{n+1})$;

(ii) průnik $P_k \cap P_l$ je podprostorem prostoru P_n, přičemž $P_k \cap P_l = \{\langle \boldsymbol{u} \rangle | 0 \neq \boldsymbol{u} \in V_{k+1} \cap V_{l+1}\}$;

(iii) $\dim(P_k \vee P_l) + \dim(P_k \cap P_l) = k + l$.

Důkaz. Tvrzení (i) a (ii) jsou zřejmá.

(iii) Podle věty o dimenzi spojení a průniku 2.23 je $\dim(P_k \vee P_l) + \dim(P_k \cap P_l) = \dim(V_{k+1} \vee V_{l+1}) - 1 + \dim(V_{k+1} \cap V_{l+1}) - 1 = k + 1 + l + 1 - 2 = k + l$. ∎

21.7. Definice. Podprostor $P_k \vee P_l$ projektivního prostoru $P_n(V_{n+1})$ nazýváme *spojením podprostorů* P_k a P_l. Říkáme, že podprostor $P_l(V_{l+1})$ je doplňkem podprostoru $P_k(V_{k+1})$ v prostoru $P_l(V_{l+1})$, jestliže V_{l+1} je doplňkem V_{k+1} v prostoru V_{n+1}. Projektivní prostor P_1 dimenze 1 se nazývá *projektivní přímka*, projektivní prostor P_2 dimenze 2 se nazývá *projektivní rovina*. Každý podprostor P_{n-1} projektivního podprostoru P_n se nazývá *nadrovina*.

21.8. Definice. Je-li $M = \{\boldsymbol{u}_0, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$ báze vektorového prostoru V_{n+1}, pak množinu M nazýváme *aritmetickou bází* projektivního podprostoru $P_n(V_{n+1})$. Množina $\{\langle \boldsymbol{u}_0 \rangle, \langle \boldsymbol{u}_1 \rangle, \ldots, \langle \boldsymbol{u}_n \rangle, \langle \boldsymbol{u}_{n+1} \rangle\}$ $n+2$ bodů projektivního prostoru $P_n(V_{n+1})$ se nazývá *geometrická báze*, jestliže žádných $n+1$ z těchto bodů neleží v nadrovině.

21.9. Věta. *Buď $\{\langle \boldsymbol{u}_0 \rangle, \langle \boldsymbol{u}_1 \rangle, \ldots, \langle \boldsymbol{u}_n \rangle, \langle \boldsymbol{u}_{n+1} \rangle\}$ geometrická báze projektivního prostoru $P_n(V_{n+1})$. Pak existují aritmetičtí zástupci $\boldsymbol{v}_i$ bodů $\langle \boldsymbol{u}_i \rangle$, $i = 0, 1, \ldots, n+1$, tak, že $\boldsymbol{v}_{n+1} = \sum_{i=0}^{n} \boldsymbol{v}_i$. Přitom $\{\boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ je aritmetická báze prostoru P_n.*

Důkaz. Podle definice geometrické báze neleží vektory $\boldsymbol{u}_0, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ v žádné nadrovině prostoru V_{n+1}, a tvoří tedy bázi tohoto prostoru. Pak existují prvky $r_0, r_1, \ldots, r_n \in T$ takové, že $\boldsymbol{u}_{n+1} = \sum_{i=0}^{n} r_i \boldsymbol{u}_i$. K dokončení důkazu nyní stačí ověřit, že všechny prvky $r_0, r_1, \ldots, r_n$ jsou nenulové, a položit $\boldsymbol{v}_i = r_i \boldsymbol{u}_i$, $i = 0, 1, \ldots, n$, a $\boldsymbol{v}_{n+1} = \boldsymbol{u}_{n+1}$. Předpokládejme tedy, že existuje nějaký index $i \in \{0, 1, \ldots, n\}$ takový, že $r_i = 0$. Pak ale $\boldsymbol{u}_{n+1} \in \langle \boldsymbol{u}_0, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_{i+1}, \ldots, \boldsymbol{u}_n \rangle$, takže $\dim\langle \boldsymbol{u}_0, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_{i+1}, \ldots, \boldsymbol{u}_n, \boldsymbol{u}_{n+1} \rangle \leq n$ a body $\langle \boldsymbol{u}_0 \rangle, \langle \boldsymbol{u}_1 \rangle, \ldots, \langle \boldsymbol{u}_{i-1} \rangle, \langle \boldsymbol{u}_{i+1} \rangle, \ldots, \langle \boldsymbol{u}_{n+1} \rangle$ leží v nadrovině, což jest spor s předpokladem. ∎

21.10. Definice. Buď $M = \{\boldsymbol{u}_0, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$ aritmetická báze projektivního prostoru $P_n(V_{n+1})$. Je-li $0 \neq \boldsymbol{u} \in V_{n+1}$, pak $\{\boldsymbol{u}\}_M$ nazýváme *homogenními souřadnicemi* geometrického bodu $\langle \boldsymbol{u} \rangle$ vzhledem k bázi M.

21.11. Poznámka. Název homogenní souřadnice pochází z toho, že dva aritmetické vektory lišící se pouze násobkem, jsou homogenními souřadnicemi téhož geometrického bodu. Přesněji tedy nechť $M = \{\boldsymbol{u}_0, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$ je aritmetická báze projektivního prostoru $P_n(V_{n+1})$ a nechť pro $0 \neq \boldsymbol{u} \in V_{n+1}$ je $\{\boldsymbol{u}\}_M = (x_0, x_1, \ldots, x_n)$. Protože pro $0 \neq r \in T$ je $\langle \boldsymbol{u} \rangle = \langle r\boldsymbol{u} \rangle$, jsou obě $(n+1)$-tice $(x_0, x_1, \ldots, x_n)$ a $(rx_0, rx_1, \ldots, rx_n)$ homogenními souřadnicemi geometrického bodu $\langle \boldsymbol{u} \rangle$. Této skutečnosti lze v některých případech využít při řešení úloh k vhodné volbě homogenních souřadnic daného geometrického bodu.

21.12. Definice. $P_n(V_{n+1})$ a $P_m(V_{m+1})$ dva projektivní prostory a $f : V_{n+1} \to V_{m+1}$ buď prostý homomorfismus. Zobrazení $K : P_n \to P_m$ definované pro $0 \neq \boldsymbol{u} \in V_{n+1}$ předpisem $K(\langle \boldsymbol{u} \rangle) = \langle f(\boldsymbol{u}) \rangle$ se nazývá *kolineární zobrazení vytvořené monomorfismem* f a značí se $K = \langle f \rangle$. Kolineární zobrazení prostoru P_n na sebe se nazývá *kolineace*.

21.13. Poznámka. Buď $0 \neq r \in T$ libovolný prvek. Pak $rf : V_{n+1} \to V_{m+1}$ je opět monomorfismus a platí $K(\langle \boldsymbol{u} \rangle) = \langle f(\boldsymbol{u}) \rangle = \langle rf(\boldsymbol{u}) \rangle = \langle (rf)(\boldsymbol{u}) \rangle$ pro každé $0 \neq \boldsymbol{u} \in V_{n+1}$, takže $K = \langle f \rangle = \langle rf \rangle$. Vidíme tedy, že kolineární zobrazení K je v souladu s označením generováno směrem určeným monomorfismem f.

V definici kolineárního zobrazení se požaduje, aby f byl monomorfismus, a to z toho důvodu, že body $\langle \boldsymbol{u} \rangle \in P_n$, kde $\boldsymbol{u} \in \operatorname{Ker} f$ by neměly obraz v P_m, neboť $K(\langle \boldsymbol{u} \rangle) = \langle f(\boldsymbol{u}) \rangle = 0$, což není geometrický bod. Dále, podle vět 9.4 a 9.27 je $\dim \operatorname{Im} f = n + 1$, takže obrazem prostoru P_n při kolineárním zobrazení K je podprostor prostoru P_m dimenze n. Odtud je patrné, že při studiu kolineárního zobrazení se můžeme omezit na případ $m = n$, tj. na případ, kdy $f : V_{n+1} \to V_{m+1}$ je izomorfismus. Nyní ukážeme, že význam geometrických bází spočívá v tom, že jednoznačně určují kolineární zobrazení.

21.14. Věta. *Nechť $\{\langle \boldsymbol{u}_0 \rangle, \langle \boldsymbol{u}_1 \rangle, \dots, \langle \boldsymbol{u}_{n+1} \rangle\}$ je geometrická báze projektivního prostoru $P_n(V_{n+1})$ a $\{\langle \boldsymbol{u}'_0 \rangle, \langle \boldsymbol{u}'_1 \rangle, \dots, \langle \boldsymbol{u}'_{n+1} \rangle\}$ geometrická báze projektivního prostoru $P'_n(V'_{n+1})$. Pak existuje právě jedno kolineární zobrazení $K : P_n \to P'_n$ takové, že $K(\langle \boldsymbol{u}_i \rangle) = \langle \boldsymbol{u}'_i \rangle$ pro každé $i = 0, 1, \dots, n + 1$.*

Důkaz. Začněme s důkazem existence. Podle věty 21.9 existují aritmetičtí zástupci $\boldsymbol{v}_i$ geometrických bodů $\langle \boldsymbol{u}_i \rangle$, $i = 0, 1, \dots, n+1$, tak, že $\{\boldsymbol{v}_0, \boldsymbol{v}_1, \dots, \boldsymbol{v}_n\}$ je aritmetická báze prostoru P_n taková, že $\boldsymbol{v}_i \in \langle \boldsymbol{u}_i \rangle$ pro každé $i = 0, 1, \dots, n + 1$ a $\boldsymbol{v}_{n+1} = \sum_{i=1}^{n} \boldsymbol{v}_i$. Podobně existuje aritmetická báze $\{\boldsymbol{v}'_0, \boldsymbol{v}'_1, \dots, \boldsymbol{v}'_n\}$ prostoru P'_n taková, že $\boldsymbol{v}'_{n+1} = \sum_{i=1}^{n} \boldsymbol{v}'_i$ a $\boldsymbol{v}'_i \in \langle \boldsymbol{u}'_i \rangle$ pro každé $i = 0, 1, \dots, n + 1$. Podle věty 9.24 existuje izomorfismus $f : V_{n+1} \to V'_{n+1}$ takový, že $f(\boldsymbol{v}_i) = \boldsymbol{v}'_i$ pro každé $i = 0, 1, \dots, n$. Pak také $f(\boldsymbol{v}_{n+1}) = f(\sum_{i=0}^{n} \boldsymbol{v}_i) = \sum_{i=0}^{n} f(\boldsymbol{v}_i) = \sum_{i=0}^{n} \boldsymbol{v}'_i = \boldsymbol{v}'_{n+1}$, takže pro kolineární zobrazení $K = \langle f \rangle$ platí $K(\langle \boldsymbol{u}_i \rangle) = K(\langle \boldsymbol{v}_i \rangle) = \langle f(\boldsymbol{v}_i) \rangle = \langle \boldsymbol{v}'_i \rangle = \langle \boldsymbol{u}'_i \rangle$ pro všechna $i = 0, 1, \dots, n + 1$.

Přejděme nyní k důkazu jednoznačnosti. Buď tedy $L = \langle g \rangle$ libovolné kolineární zobrazení prostoru P_n na prostor P'_n takové, že $L(\langle \boldsymbol{u}_i \rangle) = \boldsymbol{u}'_i$ pro každé $i = 0, 1, \dots, n+1$. Odtud dostáváme $\langle f(\boldsymbol{v}_i) \rangle = \langle \boldsymbol{u}'_i \rangle = \langle g(\boldsymbol{v}_i) \rangle$, takže $g(\boldsymbol{v}_i) = r_i f(\boldsymbol{v}_i)$ pro nějaký nenulový prvek $r_i \in T$, $i = 0, 1, \dots, n + 1$. Pak ale $\sum_{i=0}^{n} r_{n+1} \boldsymbol{v}'_i = r_{n+1} \boldsymbol{v}'_{n+1} = r_{n+1} f(\boldsymbol{v}_{n+1}) = g(\boldsymbol{v}_{n+1}) = g(\sum_{i=0}^{n} \boldsymbol{v}_i) = \sum_{i=0}^{n} g(\boldsymbol{v}_i) = \sum_{i=0}^{n} r_i f(\boldsymbol{v}_i) = \sum_{i=0}^{n} r_i \boldsymbol{v}'_i$ odkud $r_0 = r_1 = \dots = r_{n+1} = r$ podle věty 2.10. Nyní se již důkaz snadno dokončí. Je-li $0 \neq \boldsymbol{u} \in V_{n+1}$ libovolný vektor, je $\boldsymbol{u} = \sum_{i=0}^{n} x_i \boldsymbol{v}_i$, $x_i \in T$. Pak $L(\langle \boldsymbol{u} \rangle) = \langle g(\boldsymbol{u}) \rangle = \langle g(\sum_{i=0}^{n} x_i \boldsymbol{v}_i) \rangle = \langle \sum_{i=0}^{n} x_i g(\boldsymbol{v}_i) \rangle = \langle \sum_{i=0}^{n} r x_i f(\boldsymbol{v}_i) \rangle = \langle rf(\sum_{i=0}^{n} x_i \boldsymbol{v}_i) \rangle = \langle rf(\boldsymbol{u}) \rangle = \langle f(\boldsymbol{u}) \rangle = K(\langle \boldsymbol{u} \rangle)$, takže $L = K$ a jsme hotovi. ∎

21.15. Definice. Buď K kolineace projektivního prostoru P_n. Bod $\langle \boldsymbol{u} \rangle \in P_n$ nazýváme *samodružným bodem kolineace* K, jestliže $K(\langle \boldsymbol{u} \rangle) = \langle \boldsymbol{u} \rangle$. Říkáme, že podmnožina $M \subseteq P_n$ je *samodružná* při kolineaci K, jestliže $K(\langle \boldsymbol{u} \rangle) \in M$ pro každé $\langle \boldsymbol{u} \rangle \in M$, a *bodově samodružná*, je-li každý bod množiny M samodružným bodem kolineace K.

21.16. Poznámka. Každá bodově samodružná množina při kolineaci K je zřejmě samodružná. Obrácené tvrzení ovšem neplatí, jak ukazuje tento příklad. Buď $M = \{\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2\}$ báze vektorového prostoru V_3 a buď K kolineace projektivního prostoru $P_2(V_3)$ vytvořená automorfismem f prostoru V_3, jehož matice vzhledem k bázi M je

$$\boldsymbol{A} = \begin{pmatrix} 2, & 1, & 0 \\ 1, & 2, & 0 \\ 0, & 0, & 1 \end{pmatrix}.$$

Pak projektivní přímka $P_1(\langle \boldsymbol{u}_0, \boldsymbol{u}_1 \rangle)$ je zřejmě samodružná při kolineaci K, ale není bodově samodružná, neboť např. $K(\langle \boldsymbol{u}_0 \rangle) = \langle f(\boldsymbol{u}_0) \rangle = \langle 2\boldsymbol{u}_0 + \boldsymbol{u}_1 \rangle \neq \langle \boldsymbol{u}_0 \rangle$.

21.17. Věta. *Buď K kolineace projektivního prostoru $P_n(V_{n+1})$, kde V_{n+1} je vektorový prostor nad tělesem T. Jestliže těleso T je algebraicky uzavřené (speciálně je $T = K$ těleso komplexních čísel), nebo je T těleso reálných čísel a n je sudé číslo, pak kolineace K má alespoň jeden samodružný bod.*

Důkaz. Nechť kolineace K je vytvořena automorfismem f prostoru V_{n+1} a buď $\boldsymbol{A} = (a_{ij})$ matice automorfismu f vzhledem k nějaké aritmetické bázi $M = \{\boldsymbol{u}_0, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$ prostoru P_n. Nechť $\langle \boldsymbol{u} \rangle$ je samodružným bodem kolineace K, $K(\langle \boldsymbol{u} \rangle) = \langle f(\boldsymbol{u}) \rangle = \langle \boldsymbol{u} \rangle$ a buďte $\{\boldsymbol{u}\}_M = (x_0, x_1, \ldots, x_n)$ homogenní souřadnice bodu $\langle \boldsymbol{u} \rangle$. Pak existuje nenulový prvek $\lambda \in T$ takový, že $f(\boldsymbol{u}) = \lambda \boldsymbol{u}$ a platí $f(\boldsymbol{u}) = f(\sum_{i=0}^n x_i \boldsymbol{u}_i) = \sum_{i=0}^n x_i f(\boldsymbol{u}_i) = \sum_{i=0}^n \sum_{j=0}^n x_i a_{ji} \boldsymbol{u}_j = \sum_{j=0}^n (\sum_{i=0}^n x_i a_{ji}) \boldsymbol{u}_j = \sum_{j=0}^n \lambda x_j \boldsymbol{u}_j = \lambda \boldsymbol{u}$. Porovnáním koeficientů (věta 2.10) dostaneme pro každé $j = 0, 1, \ldots, n$ rovnost $\sum_{i=0}^n a_{ji} x_i = \lambda x_j$. Zatím jsme tedy odvodili nutnou podmínku pro to, aby geometrický bod $\langle \boldsymbol{u} \rangle$ byl samodružným bodem kolineace K. Pohlížíme-li nyní na získané rovnosti jako homogenní soustavu lineárních rovnic s maticí $\boldsymbol{A} - \lambda \boldsymbol{E}$, stačí nám k dokončení důkazu nalézt nenulový prvek $\lambda \in T$ tak, aby tato soustava měla netriviální řešení $(x_0, x_1, \ldots, x_n)$. Z předchozích úvah pak totiž bezprostředně vyplývá, že geometrický bod $\langle \boldsymbol{u} \rangle$, kde $\{\boldsymbol{u}\}_M = (x_0, x_1, \ldots, x_n)$ je samodružným bodem kolineace K. Avšak podle důsledku 5.9 má homogenní soustava lineárních rovnic s maticí $\boldsymbol{A} - \lambda \boldsymbol{E}$ netriviální řešení, právě když $h(\boldsymbol{A} - \lambda \boldsymbol{E}) < n + 1$, tj. podle věty 8.4, právě když $\det(\boldsymbol{A} - \lambda \boldsymbol{E}) = 0$. Nyní $\det(\boldsymbol{A} - \lambda \boldsymbol{E})$ je polynom v λ stupně $n + 1$, jehož absolutní člen je zřejmě roven $\det \boldsymbol{A}$. Podle věty 10.10 je matice $\boldsymbol{A}$ regulární, takže $\det \boldsymbol{A} \neq 0$ opět podle věty 8.4. To však znamená, že polynom $\det(\boldsymbol{A} - \lambda \boldsymbol{E})$ má všechny kořeny nenulové. Je-li nyní těleso T algebraicky uzavřené, má polynom $\det(\boldsymbol{A} - \lambda \boldsymbol{E})$ alespoň jeden (dokonce všechny) svůj kořen v T. Je-li $T = R$ těleso reálných čísel a n je sudé, je tento polynom lichého stupně, a má tudíž alespoň jeden reálný kořen. Tím je důkaz věty dokončen. ∎

21.18. Poznámka. Právě dokončený důkaz je zároveň jednou z metod, jak v konkrétních příkladech hledat samodružné body kolineace. K tomu stačí nalézt kořeny polynomu $\det(\boldsymbol{A} - \lambda \boldsymbol{E})$ a pro každý takový kořen λ nalézt (všechna) netriviální řešení homogenní soustavy lineárních rovnic $(\boldsymbol{A} - \lambda \boldsymbol{E})\{\boldsymbol{u}\}_M^T = 0$.

21.19. Příklad. Nalezněme samodružné body kolineace K projektivního prostoru $P_2(R^3)$ vytvořené automorfismem f, jestliže $f((x_1, x_2, x_3)) = (2x_1 - x_3, 2x_1 + x_2 - 2x_3, 3x_1 - 2x_3)$.

Ř e š e n í : Jest $f(e_1) = (2, 2, 3)$, $f(e_2) = (0, 1, 0)$, $f(e_3) = (-1, -2, -2)$, takže

$$A = \begin{pmatrix} 2, & 0, & -1 \\ 2, & 1, & -2 \\ 3, & 0, & -2 \end{pmatrix}$$

je matice automorfismu f vzhledem ke kanonické bázi prostoru R^3. Dále

$$\det(A - \lambda E) = \begin{vmatrix} 2-\lambda, & 0, & -1 \\ 2, & 1-\lambda, & -2 \\ 3, & 0, & -2-\lambda \end{vmatrix} = (1-\lambda) \begin{vmatrix} 2-\lambda, & -1 \\ 3, & -2-\lambda \end{vmatrix} =$$

$$(\lambda-1) \begin{vmatrix} 2-\lambda, & 1 \\ 3, & 2+\lambda \end{vmatrix} = (\lambda-1)(4-\lambda^2-3) = (1-\lambda)(\lambda^2-1) = (1-\lambda)(\lambda-1)(\lambda+1),$$

takže polynom $\det(A - \lambda E)$ má dva reálné kořeny 1 a -1. Pro $\lambda = -1$ jest

$$\begin{pmatrix} 3, & 0, & -1 \\ 2, & 2, & -2 \\ 3, & 0, & -1 \end{pmatrix} \sim \begin{pmatrix} 1, & 1, & -1 \\ 0, & -3, & 2 \end{pmatrix},$$

takže příslušná homogenní soustava má řešení $(1,2,3)$ a $\langle(1,2,3)\rangle$ je samodružným bodem kolineace K. Pro $\lambda = 1$ pak máme

$$\begin{pmatrix} 1, & 0, & -2 \\ 2, & 0, & -2 \\ 3, & 0, & -3 \end{pmatrix} \sim \begin{pmatrix} 1, & 0, & -1 \end{pmatrix}$$

a příslušná soustava má řešení $\langle(1,0,1),(0,1,0)\rangle$. Tedy projektivní přímka $P_1 = \langle(1,0,1),(0,1,0)\rangle$ je bodově samodružná při kolineaci K.

21.20. Poznámka. Dříve než přistoupíme k zavedení pojmu projektivního rozšíření afinního prostoru, vraťme se na okamžik k úvahám z úvodního odstavce 21.1. Mějme nyní dva body a, b na přímce p o souřadnicích $\{a\}_{S'} = (x)$, $\{b\}_{S'} = (y)$. Bodu a odpovídá směr $\langle(1,x)\rangle$ a bodu b odpovídá směr $\langle(1,y)\rangle$. Podívejme se nyní, který bod odpovídá směru $\langle(r,rx)+(s,sy)\rangle$, $rs \neq 0$. Nejprve předpokládejme, že $r+s \neq 0$. V tomto případě máme $\langle(r+s, rx+sy)\rangle = \langle(r+s),(r+s)(x+\frac{s}{r+s}(y-x))\rangle = \langle 1, x+\frac{s}{r+s}(y-x)\rangle$, takže tomuto směru odpovídá bod $c = a + \frac{s}{r+s}(b-a)$ na přímce p. Je-li nyní $r+s=0$, je $\langle(r+s, rx+sy)\rangle = \langle(0, r(x-y))\rangle$ a v tomto případě nedostáváme žádný bod přímky p, ale její směr $\langle a-b\rangle$. Z této úvahy je patrná, jak uvidíme, motivace následující konstrukce.

21.21. Projektivní rozšíření afinního prostoru.

V tomto odstavci vyjdeme z afinního $A_n(V_n)$ a sestrojíme k němu projektivní prostor $\bar{A}_n(\overline{V}_{n+1})$ obsahující A_n jako svou podmnožinu a to tak, aby vlastnosti prostoru A_n zůstaly v $\bar{A}_n$ zachovány v maximální možné míře. Poznamenejme ještě, že v tomto případě bude zobrazení φ z definice projektivního prostoru 21.2 neidentické.

Označme N množinu všech směrů vektorového prostoru V_n a položme $\bar{A}_n = A_n \cup N$. Pro každý bod $a \in A_n$ a každý prvek $0 \neq r \in T$ uvažujme formální symbol ra, který můžeme chápat např. jako zkrácený zápis uspořádané dvojice (r,a). Místo

$1a$ budeme psát krátce a. Nyní na množině $\overline{V}_{n+1} = V_n \cup \{ra | 0 \neq r \in T, a \in A_n\}$ definujme následujícím způsobem operace sčítání a násobku prvky z tělesa T (viz motivace z předchozí poznámky). Pro libovolné prvky $a, b \in A_n$, $\boldsymbol{u} \in V_n$ a nenulové prvky $r, s \in T$ položme

$$\begin{aligned}
ra + sb &= r(a-b) \quad \text{pro} \quad r+s=0;\\
ra + sb &= (r+s)(a + \tfrac{s}{r+s}(b-a)) \quad \text{pro} \quad r+s \neq 0;\\
ra + \boldsymbol{u} &= r(a + \tfrac{1}{r}\boldsymbol{u});\\
s(ra) &= (sr)a;\\
0(ra) &= 0 \in V_n.
\end{aligned}$$

Přitom operace na podmnožině V_n množiny $\overline{V}_{n+1}$ zůstávají stejné. Přenecháme čtenáři jako snadné cvičení ověření toho, že množina $\overline{V}_{n+1}$ s právě zavedenými operacemi je vektorovým prostorem. Dříve než budeme definovat zobrazení φ z definice 21.2 ukažme, že vektorový prostor $\overline{V}_{n+1}$ má dimenzi $n+1$. Buď tedy $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ libovolná báze prostoru V_n a $a \in A_n$ buď libovolný bod. Ukážeme, že množina $\{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ je bází vektorového prostoru $\overline{V}_{n+1}$.

Je-li předně $ra + \sum_{i=1}^n r_i\boldsymbol{u}_i = 0$, je $r = 0$, neboť v opačném případě bychom dostali $ra + \sum_{i=1}^n r_i\boldsymbol{u}_i = r(a + \frac{1}{r}\sum_{i=1}^n r_i\boldsymbol{u}_i)$, tedy nenulový násobek nějakého bodu z A_n, a nikoli nulový vektor z V_n. Nyní z $r = 0$ dostáváme $\sum_{n=i}^n r_i\boldsymbol{u}_i = 0$, tedy $r_1 = r_2 = \dots = r_n = 0$ vzhledem k tomu, že vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n$ jsou lineárně nezávislé. Ukázali jsme, že množina $\{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ je lineárně nezávislá, a zbývá ověřit, že tato množina generuje $\overline{V}_{n+1}$. Je-li $\boldsymbol{u} \in V_n$ libovolný vektor, je $\boldsymbol{u} = \sum_{i=1}^n r_i\boldsymbol{u}_i = 0 \cdot a + \sum_{i=1}^n r_i\boldsymbol{u}_i$. Je-li nakonec $b \in A_n$ libovolný bod a $0 \neq r \in T$ libovolný prvek, je $b = a + \sum_{i=1}^n r_i\boldsymbol{u}_i$, tedy $rb = ra + \sum_{i=1}^n rr_i\boldsymbol{u}_i$ a vektory $a, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n$ generují prostor $\overline{V}_{n+1}$.

Položíme-li nakonec $\varphi(\langle\boldsymbol{u}\rangle) = \langle\boldsymbol{u}\rangle$ pro $\boldsymbol{u} \in V_n$ a $\varphi(\langle ra\rangle) = a$ pro $a \in A_n$ a $0 \neq r \in T$, je φ zřejmě vzájemné jednoznačné zobrazení množiny všech směrů vektorového prostoru $\overline{V}_{n+1}$ na množinu $\bar{A}_n$.

21.22. Definice. Projektivní prostor $\bar{A}_n(\overline{V}_{n+1})$ nazýváme *projektivním rozšířením afinního prostoru* $A_n(V_n)$. Body z A_n se nazývají *vlastní body* prostoru $\bar{A}_n(\overline{V}_{n+1})$ a body z N se nazývají *nevlastní body* tohoto prostoru.

21.23. Věta. *Množina N všech nevlastních bodů projektivního rozšíření $\bar{A}_n(\overline{V}_{n+1})$ afinního prostoru $A_n(V_n)$ je nadrovina v $\bar{A}_n(\overline{V}_{n+1})$.*

Důkaz. Stačí si uvědomit, že n-rozměrný podprostor V_n prostoru $\overline{V}_{n+1}$ je kromě nulového vektoru množinou právě všech aritmetických zástupců množiny N. ∎

21.24. Definice. Nadrovina N projektivního rozšíření $\bar{A}_n(\overline{V}_{n+1})$ afinního prostoru $A_n(V_n)$ se nazývá *nevlastní nadrovina.*

21.25. Věta. *Buď $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ soustava souřadnic v afinním prostoru $A_n(V_n)$. Pak $\bar{S} = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$, kde a má ve smyslu odstavce 21.21 význam prvku $1a$, je aritmetická báze projektivního prostoru $\bar{A}_n(\overline{V}_{n+1})$. Přitom pro $b \in A_n$, $\{b\}_S = (x_1, x_2, \dots, x_n)$ a $0 \neq r \in T$ je*

$$\{rb\}_{\bar{S}} = (r, rx_1, rx_2, \dots, rx_n)$$

a pro $\boldsymbol{u} \in V_n$, $\{\boldsymbol{u}\}_S = (y_1, y_2, \dots, y_n)$ a $r \in T$ je

$$\{ru\}_{\bar{S}} = (0, ry_1, ry_2, \ldots, ry_n).$$

Důkaz. V odstavci 21.21 jsme ukázali, že množina $\bar{S}$ je aritmetická báze projektivního rozšíření $\bar{A}_n(\overline{V}_{n+1})$. Je-li $\{b\}_S = (x_1, x_2, \ldots, x_n)$, je $b - a = \sum_{i=1}^n x_i \boldsymbol{u}_i$, takže $r(b-a) = \sum_{i=1}^n rx_i\boldsymbol{u}_i$, a tedy $rb = ra + \sum_{i=1}^n rx_i\boldsymbol{u}_i$, odkud máme $\{rb\}_{\bar{S}} = (r, rx_1, rx_2, \ldots, rx_n)$. Zbytek tvrzení je zřejmý. ■

21.26. Definice. Buď $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ soustava souřadnic v afinním prostoru $A_n(V_n)$. Pak aritmetickou bázi $\bar{S} = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ projektivního rozšíření $\bar{A}_n(\overline{V}_{n+1})$ nazýváme *soustavou souřadnic indukovanou* S.

21.27. Věta. *Buďte $A_n(V_n)$, $A'_n(V'_n)$ dva afinní prostory a buď $F : A_n \to A'_n$ regulární afinní zobrazení vytvořené izomorfismem $f : V_n \to V'_n$. Pak existuje právě jedno kolineární zobrazení $K : \bar{A}_n \to \bar{A}'_n$ takové, že $K|A_n = F$. Přitom $K = \langle g \rangle$, kde $g|V_n = f$ a $g(ra) = rF(a)$ pro každé $a \in A_n$ a každé $0 \neq r \in T$.*

Důkaz. K důkazu existence stačí ověřit, že zobrazení g popsané ve větě je izomorfismus vektorového prostoru $(\overline{V}_{n+1})$ na vektorový prostor$(\overline{V}'_{n+1})$. Je-li totiž φ' vzájemné jednoznačné zobrazení množiny všech směrů prostoru $(\overline{V}_{n+1})$ na množinu $\bar{A}'_n$ definované v odstavci 21.21, je $K(a) = \varphi'(\langle g(a)\rangle) = \varphi'(\langle F(a)\rangle) = F(a)$, pro každé $a \in A_n$, takže $K|A_n = F$. Nejprve ověřme, že g je homomorfismus. Jsou-li $a, b \in A_n$ libovolné body a r, s libovolné nenulové prvky z tělesa T, pak podle odstavce 21.21 pro $r+s \neq 0$ máme $g(ra+sb) = g((r+s)(a+\frac{s}{r+s}(b-a)) = (r+s)F(a+\frac{s}{r+s}(b-a)) = (r+s)(F(a)+\frac{s}{r+s}f(b-a)) = (r+s)(F(a)+\frac{s}{r+s}(F(b)-F(a))) = rF(a)+sF(b) = g(ra)+g(sb)$ a pro $r+s = 0$ je $g(ra+sb) = g(r(a-b)) = rf(a-b) = r(F(a)-F(b)) = rF(a)+sF(b) = g(ra)+g(sb)$. Dále pro libovolný bod $a \in A_n$, libovolný vektor $\boldsymbol{u} \in V_n$ a libovolný nenulový prvek $r \in T$ jest $g(ra+\boldsymbol{u}) = g(r(a+\frac{1}{r}\boldsymbol{u})) = rF(a+\frac{1}{r}\boldsymbol{u}) = r(F(a)+\frac{1}{r}f(\boldsymbol{u})) = r(F(a)+\frac{1}{r}g(\boldsymbol{u})) = rF(a)+g(\boldsymbol{u}) = g(ra)+g(\boldsymbol{u})$. Odtud již plyne, že g je homomorfismus vzhledem k tomu, že $g|V_n = f$ a že zřejmě $g(ra) = rF(a) = rg(a)$. Protože F je surjektivní zobrazení množiny A_n na množinu A'_n a $g|V_n = f$ je rovněž surjektivní homomorfismus prostoru V_n na prostor V'_n, je g zřejmě epimorfismus, a tedy izomorfismus podle věty 9.27.

Nyní můžeme přejít k důkazu jednoznačnosti kolineárního zobrazení požadovaných vlastností. Buď tedy $L = \langle h \rangle : \bar{A}_n \to \bar{A}'_n$ kolineární zobrazení vytvořené izomorfismem $h : \overline{V}_{n+1} \to \overline{V}'_{n+1}$ takové, že $L|A_n = F$, a buď $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ soustava souřadnic v $A_n(V_n)$. Podle předpokladu je $\varphi'(\langle h(a)\rangle) = L(a) = F(a) = K(a) = \varphi'(\langle g(a)\rangle)$, takže $h(a) = rg(a)$ pro nějaké $0 \neq r \in T$. Podobně pro každé $i = 1, 2, \ldots, n$ je $\varphi'(\langle h(a+\boldsymbol{u}_i)\rangle) = L(a+\boldsymbol{u}_i) = F(a+\boldsymbol{u}_i) = K(a+\boldsymbol{u}_i) = \varphi'(\langle g(a+\boldsymbol{u}_i)\rangle)$, odkud $h(a+\boldsymbol{u}_i) = r_i g(a+\boldsymbol{u}_i)$, $0 \neq r_i \in T$. Odtud dostáváme $rg(a)+h(\boldsymbol{u}_i) = h(a)+h(\boldsymbol{u}_i) = h(a+\boldsymbol{u}_i) = r_i g(a+\boldsymbol{u}_i) = r_i g(a)+r_i g(\boldsymbol{u}_i)$, čili $(r-r_i)g(a) = r_i g(\boldsymbol{u}_i) - h(\boldsymbol{u}_i)$. Protože vzájemné jednoznačné zobrazení L zobrazuje množinu A_n na množinu A'_n, musí zobrazovat nevlastní nadrovinu prostoru $\bar{A}_n(\overline{V}_{n+1})$ na nevlastní nadrovinu prostoru $\bar{A}'_n(\overline{V}'_{n+1})$. Pak ale nutně $r = r_i$, neboť v opačném případě je $\varphi'(\langle(r-r_i)g(a)\rangle) = \varphi'(\langle g(a)\rangle) = F(a)$ vlastním bodem, zatímco $\varphi(\langle r_i g(\boldsymbol{u}_i) - h(\boldsymbol{u}_i)\rangle)$ je nevlastním bodem, což je spor s rovností $(r-r_i)g(a) = r_i g(\boldsymbol{u}_i) - h(\boldsymbol{u}_i)$. Vidíme tedy, že $h(a) = rg(a)$ a $h(\boldsymbol{u}_i) = rg(\boldsymbol{u}_i)$ pro každé $i = 1, 2, \dots, n$. Protože $\bar{S} = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ je podle věty 21.25 aritmetická báze prostoru $\bar{A}_n(\overline{V}_{n+1})$, je $h = rg$ podle věty 9.22, a tedy $L = \langle h \rangle = \langle rg \rangle = \langle g \rangle = K$. ■

21.28. Definice. Kolineární zobrazení z předchozí věty se nazývá *projektivní rozšíření afinního zobrazení F.*

21.29. Věta. *Buď K projektivní rozšíření afinity F afinního prostoru $A_n(V_n)$. Pak nevlastní nadrovina $N \subseteq A_n(V_n)$ je samodružná nadrovina kolineace K.*

Důkaz. Protože $K|A_n = F$, zobrazuje vzájemně jednoznačné zobrazení K množinu všech vlastních bodů $A_n \subseteq \bar{A}_n$ na sebe, a tedy množina N všech nevlastních bodů se nutně musí zobrazit také na sebe. ■

21.30. Definice. Buďte $\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4$ vektory z vektorového prostoru V_2 takové, že každé dva z nich jsou lineárně nezávislé. Pak existují prvky $r_3, s_3, r_4, s_4 \in T$ takové, že $\boldsymbol{u}_3 = r_3\boldsymbol{u}_1 + s_3\boldsymbol{u}_2$, $\boldsymbol{u}_4 = r_4\boldsymbol{u}_1 + s_4\boldsymbol{u}_2$. Prvek $\frac{s_3r_4}{s_4r_3} \in T$ nazýváme *dvojpoměrem čtveřice vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4$* (v tomto pořadí) a značíme $(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4)$.

21.31. Věta. *Buďte $\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4$ po dvou lineárně nezávislé vektory z vektorového prostoru V_2 a t_1, t_2, t_3, t_4 buďte nenulové prvky z tělesa T. Pak $(t_1\boldsymbol{u}_1, t_2\boldsymbol{u}_2, t_3\boldsymbol{u}_3, t_4\boldsymbol{u}_4) = (\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4)$.*

Důkaz. Jestliže $\boldsymbol{u}_3 = r_3\boldsymbol{u}_1 + s_3\boldsymbol{u}_2$, $\boldsymbol{u}_4 = r_4\boldsymbol{u}_1 + s_4\boldsymbol{u}_2$, pak $t_3\boldsymbol{u}_3 = \frac{r_3t_3}{t_1} \cdot t_1\boldsymbol{u}_1 + \frac{s_3t_3}{t_2} \cdot t_2\boldsymbol{u}_2$, $t_4\boldsymbol{u}_4 = \frac{r_4t_4}{t_1} \cdot t_1\boldsymbol{u}_1 + \frac{s_4t_4}{t_2} \cdot t_2\boldsymbol{u}_2$, takže $(t_1\boldsymbol{u}_1, t_2\boldsymbol{u}_2, t_3\boldsymbol{u}_3, t_4\boldsymbol{u}_4) = (\frac{s_3t_3}{t_2} \cdot \frac{r_4t_4}{t_1}) : (\frac{s_4t_4}{t_2} \cdot \frac{r_3t_3}{t_1}) = \frac{s_3r_4}{s_4r_3} = (\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4)$. ■

21.32. Definice. Buďte $\langle \boldsymbol{u}_1 \rangle$, $\langle \boldsymbol{u}_2 \rangle$, $\langle \boldsymbol{u}_3 \rangle$, $\langle \boldsymbol{u}_4 \rangle$ čtyři navzájem různé body na projektivní přímce $P_1(V_2)$. *Dvojpoměrem čtveřice $\langle \boldsymbol{u}_1 \rangle$, $\langle \boldsymbol{u}_2 \rangle$, $\langle \boldsymbol{u}_3 \rangle$, $\langle \boldsymbol{u}_4 \rangle$ (v tomto pořadí) rozumíme prvek $(\langle \boldsymbol{u}_1 \rangle, \langle \boldsymbol{u}_2 \rangle, \langle \boldsymbol{u}_3 \rangle, \langle \boldsymbol{u}_4 \rangle) = (\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4)$ tělesa T.*

21.33. Věta. *Nechť $\langle \boldsymbol{u}_1 \rangle$, $\langle \boldsymbol{u}_2 \rangle$, $\langle \boldsymbol{u}_3 \rangle$ jsou po dvou různé body projektivní přímky $P_1(V_2)$ a buď $\lambda \in T$ prvek takový, že $0 \neq \lambda \neq 1$. Pak existuje právě jeden bod $\langle \boldsymbol{u}_4 \rangle$ na přímce P_1 takový, že $(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4) = \lambda$. Obráceně, dvojpoměr $(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4)$ čtyř po dvou různých bodů $\langle \boldsymbol{u}_1 \rangle$, $\langle \boldsymbol{u}_2 \rangle$, $\langle \boldsymbol{u}_3 \rangle$, $\langle \boldsymbol{u}_4 \rangle$ na projektivní přímce P_1 je vždy různý od $0, 1$.*

Důkaz. Protože dané body jsou navzájem různé, neleží žádné dva z nich v nadrovině P_0, takže body $\langle \boldsymbol{u}_1 \rangle$, $\langle \boldsymbol{u}_2 \rangle$, $\langle \boldsymbol{u}_3 \rangle$ tvoří geometrickou bázi přímky P_1. Podle věty 21.9 můžeme volit aritmetické zástupce těchto bodů tak, aby $\boldsymbol{u}_3 = \boldsymbol{u}_1 + \boldsymbol{u}_2$. Položíme-li $\boldsymbol{u}_4 = \lambda\boldsymbol{u}_1 + \boldsymbol{u}_2$, je $\langle \boldsymbol{u}_4 \rangle \neq \langle \boldsymbol{u}_1 \rangle$, $\langle \boldsymbol{u}_4 \rangle \neq \langle \boldsymbol{u}_2 \rangle$, protože $\lambda \neq 0$, a $\langle \boldsymbol{u}_4 \rangle \neq \langle \boldsymbol{u}_3 \rangle$, protože $\lambda \neq 1$, a zřejmě je $(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4) = \lambda$. Je-li nyní $\boldsymbol{u}_4' = r\boldsymbol{u}_1 + s\boldsymbol{u}_2$ libovolný vektor z V_2 takový, že bod $\langle \boldsymbol{u}_4' \rangle$ je různý od bodů $\langle \boldsymbol{u}_1 \rangle$, $\langle \boldsymbol{u}_2 \rangle$, $\langle \boldsymbol{u}_3 \rangle$, pak z $(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4') = \frac{r}{s} = \lambda$ plyne $r = s\lambda$, takže $\boldsymbol{u}_4' = s(\lambda\boldsymbol{u}_1 + \boldsymbol{u}_2) = s\boldsymbol{u}_4$, a tedy $\langle \boldsymbol{u}_4' \rangle = \langle \boldsymbol{u}_4 \rangle$.

K důkazu obráceného tvrzení si stačí uvědomit, že je-li $\boldsymbol{u}_3 = r_3\boldsymbol{u}_1 + s_3\boldsymbol{u}_2$, $\boldsymbol{u}_4 = r_4\boldsymbol{u}_1 + s_4\boldsymbol{u}_2$ a $(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4) = \frac{s_3r_4}{s_4r_3} = 0$, je buď $s_3 = 0$, a tedy $\langle \boldsymbol{u}_3 \rangle = \langle \boldsymbol{u}_1 \rangle$, nebo $r_4 = 0$, a tedy $\langle \boldsymbol{u}_4 \rangle = \langle \boldsymbol{u}_2 \rangle$, což je spor s předpokladem. Podobně pro $\frac{s_3r_4}{s_4r_3} = 1$ je $s_3r_4 = s_4r_3$, odkud $s_4\boldsymbol{u}_3 = s_4r_3\boldsymbol{u}_1 + s_4s_3\boldsymbol{u}_2 = s_3r_4\boldsymbol{u}_1 + s_3s_4\boldsymbol{u}_2 = s_3\boldsymbol{u}_4$, takže $\langle \boldsymbol{u}_3 \rangle = \langle s_4\boldsymbol{u}_3 \rangle = \langle s_3\boldsymbol{u}_4 \rangle = \langle \boldsymbol{u}_4 \rangle$, což je opět spor s předpokladem. ■

21.34. Věta. *Buďte $\langle \boldsymbol{u}_1\rangle$, $\langle \boldsymbol{u}_2\rangle$, $\langle \boldsymbol{u}_3\rangle$, $\langle \boldsymbol{u}_4\rangle$ po dvou různé body projektivní přímky $P_1(V_2)$ a buď $\lambda = (\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4)$ jejich dvojpoměr. Pak platí*

(i) $(\boldsymbol{u}_2, \boldsymbol{u}_1, \boldsymbol{u}_3, \boldsymbol{u}_4) = \frac{1}{\lambda}$;

(ii) $(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_4, \boldsymbol{u}_3) = \frac{1}{\lambda}$;

(iii) $(\boldsymbol{u}_1, \boldsymbol{u}_3, \boldsymbol{u}_2, \boldsymbol{u}_4) = 1 - \lambda$.

Důkaz. Podle věty 21.9 můžeme zvolit aritmetické zástupce bodů $\langle \boldsymbol{u}_1\rangle$, $\langle \boldsymbol{u}_2\rangle$, $\langle \boldsymbol{u}_3\rangle$ tak, aby $\boldsymbol{u}_3 = \boldsymbol{u}_1 + \boldsymbol{u}_2$. Vzhledem k jednoznačnosti dokázané v předchozí větě, můžeme zvolit aritmetického zástupce bodu $\langle \boldsymbol{u}_4\rangle$ ve tvaru $\boldsymbol{u}_4 = \lambda \boldsymbol{u}_1 + \boldsymbol{u}_2$. Nyní z $\boldsymbol{u}_3 = \boldsymbol{u}_2 + \boldsymbol{u}_1$, $\boldsymbol{u}_4 = \boldsymbol{u}_2 + \lambda \boldsymbol{u}_1$ dostáváme $(\boldsymbol{u}_2, \boldsymbol{u}_1, \boldsymbol{u}_3, \boldsymbol{u}_4) = \frac{1}{\lambda}$ a zřejmě je $(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_4, \boldsymbol{u}_3) = \frac{1}{\lambda}$. Nakonec $\boldsymbol{u}_2 = -\boldsymbol{u}_1 + \boldsymbol{u}_3$ a $\boldsymbol{u}_4 = \lambda \boldsymbol{u}_1 + \boldsymbol{u}_2 = (\lambda - 1)\boldsymbol{u}_1 + \boldsymbol{u}_3$, takže $(\boldsymbol{u}_1, \boldsymbol{u}_3, \boldsymbol{u}_2, \boldsymbol{u}_4) = 1 - \lambda$. ■

21.35. Věta. *Nechť $\langle \boldsymbol{u}_1\rangle$, $\langle \boldsymbol{u}_2\rangle$, $\langle \boldsymbol{u}_3\rangle$, $\langle \boldsymbol{u}_4\rangle$ jsou po dvou různé body projektivní přímky $P_1(V_2)$ a buď $(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4) = \lambda$ jejich dvojpoměr. Potom dvojpoměry sestavené ze všech možných pořadí těchto čtyř bodů (je jich 24) nabývají pouze 6 hodnot, a to λ, $\frac{1}{\lambda}$, $1 - \lambda$, $\frac{1}{1-\lambda}$, $\frac{\lambda-1}{\lambda}$, $\frac{\lambda}{\lambda-1}$.*

Důkaz. Snadno se ověří, že libovolné pořadí daných čtyř bodů dostaneme tak, že postupně provedeme některou z těchto tří operací: (i) vzájemná výměna 1. a 2. bodu; (ii) vzájemná výměna 2. a 3. bodu; (iii) vzájemná výměna 3. a 4. bodu. Přitom podle předchozí věty se dvojpoměr μ změní buď na $\frac{1}{\mu}$, nebo na $1 - \mu$. Vyjdeme-li tedy od dvojpoměru λ, dostaneme prováděním těchto operací právě 6 hodnot vypsaných ve formulaci věty. Čtenář sám bez obtíží ověří, že je-li μ některý z těchto 6 prvků, jsou i $\frac{1}{\mu}$ a $1 - \mu$ některé z těchto prvků. ■

21.36. Poznámka. Zamysleme se nyní nad tím, zda se některé ze 6 hodnot dvojpoměru mohou rovnat. Pro snažší orientaci si utvořme tabulku

	λ	$\frac{1}{\lambda}$	$1-\lambda$	$\frac{1}{1-\lambda}$	$\frac{\lambda-1}{\lambda}$	$\frac{\lambda}{\lambda-1}$
λ	$-$	-1	$\frac{1}{2}$	$*$	$*$	2
$\frac{1}{\lambda}$	-1	$-$	$*$	$\frac{1}{2}$	2	$*$
$1-\lambda$	$\frac{1}{2}$	$*$	$-$	2	-1	$*$
$\frac{1}{1-\lambda}$	$*$	$\frac{1}{2}$	2	$-$	$*$	-1
$\frac{\lambda-1}{\lambda}$	$*$	2	-1	$*$	$-$	$\frac{1}{2}$
$\frac{\lambda}{\lambda-1}$	2	$*$	$*$	-1	$\frac{1}{2}$	$-$

kde v průsečíku daného řádku a daného sloupce je hodnota λ, pro kterou se příslušné hodnoty rovnají. Symbolem $*$ je označeno, že λ je kořenem polynomu $\lambda^2 - \lambda + 1$. Pro $\lambda = -1$ vypadá 6 hodnot vypsaných v předchozí větě takto: $-1, -1, 2, \frac{1}{2}, 2, \frac{1}{2}$. Podobně pro $\lambda = 2$ a $\lambda = \frac{1}{2}$ dostáváme $2, \frac{1}{2}, -1, -1, \frac{1}{2}, 2$ a $\frac{1}{2}, 2, \frac{1}{2}, 2, -1, -1$. Podobným způsobem se snadno ověří, že je-li λ kořenem polynomu $\lambda^2 - \lambda + 1$, jsou všechny ostatní hodnoty rovněž kořeny tohoto polynomu.

21.37. Definice. Uspořádaná čtveřice $\langle \boldsymbol{u}_1\rangle$, $\langle \boldsymbol{u}_2\rangle$, $\langle \boldsymbol{u}_3\rangle$, $\langle \boldsymbol{u}_4\rangle$ navzájem různých bodů projektivní přímky $P_1(V_2)$ se nazývá *harmonická*, jestliže $(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4) = -1$. V tomto případě nabývá dvojpoměr při všech možných pořadích těchto bodů pouze hodnot $-1, 2, \frac{1}{2}$.

21.38. Věta. *Nechť $\langle \boldsymbol{u}_1\rangle$, $\langle \boldsymbol{u}_2\rangle$, $\langle \boldsymbol{u}_3\rangle$, $\langle \boldsymbol{u}_4\rangle$, $\langle \boldsymbol{u}_5\rangle$ jsou po dvou různé body na projektivní přímce $P_1(V_2)$. Pak platí*

$$(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4)(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_4, \boldsymbol{u}_5) = (\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_5).$$

Důkaz. Podle vět 21.9 a 21.33 můžeme zvolit aritmetické zástupce daných bodů tak, že $\boldsymbol{u}_3 = \boldsymbol{u}_1 + \boldsymbol{u}_2$, $\boldsymbol{u}_4 = \lambda\boldsymbol{u}_1 + \boldsymbol{u}_2$, $\boldsymbol{u}_5 = \mu\boldsymbol{u}_1 + \boldsymbol{u}_2$. Pak $(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4)(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_4, \boldsymbol{u}_5)$ $= \lambda \cdot \frac{\mu}{\lambda} = \mu = (\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_5)$. ∎

21.39. Věta. *Buďte a, b, c tři různé body afinní přímky $A_1(V_1)$. Pak v projektivním rozšíření $\bar{A}_1(\bar{V}_2)$ platí*

$$(a, b, c, \langle \boldsymbol{u}\rangle) = (c; a, b),$$

kde $\langle \boldsymbol{u}\rangle$ je nevlastní bod projektivní přímky $\bar{A}_1(\bar{V}_2)$.

Důkaz. Označíme-li $\lambda = (c; a, b)$ dělicí poměr bodu c vzhledem k bodům a, b, je podle definice 19.29 $c - a = \lambda(c - b)$. Položíme-li $\boldsymbol{u} = c - b$, je podle lemmatu 19.6 $c = a + \lambda\boldsymbol{u}$ a $b = a + (b - a) = a + (b - c) + (c - a) = a - \boldsymbol{u} + \lambda\boldsymbol{u} = a + (\lambda - 1)\boldsymbol{u}$, takže $(a, \langle \boldsymbol{u}\rangle, b, c) = \frac{\lambda - 1}{\lambda}$. Podle věty 21.34 pak je $(a, b, \langle \boldsymbol{u}\rangle, c) = 1 - \frac{\lambda-1}{\lambda} = \frac{1}{\lambda}$ a konečně $(a, b, c, \langle \boldsymbol{u}\rangle) = \lambda$. ∎

21.40. Věta. *Buďte a, b, c, d čtyři navzájem různé body afinní přímky $A_1(V_1)$. Pak dvojpoměr (a, b, c, d) v projektivním rozšíření $\bar{A}_1(\bar{V}_2)$ je roven podílu dělicích poměrů $\frac{(c;a,b)}{(d;a,b)}$ (odtud také pochází název dvojpoměr).*

Důkaz. Označíme-li $\langle \boldsymbol{u}\rangle = V_1$ nevlastní bod projektivní roviny $\bar{A}_1(\bar{V}_2)$, pak podle věty 21.38 platí $(a, b, c, d) = (a, b, c, \langle \boldsymbol{u}\rangle)(a, b, \langle \boldsymbol{u}\rangle, d)$. Podle předchozí věty je $(a, b, c, \langle \boldsymbol{u}\rangle) = (c; a, b,)$ a $(a, b, d, \langle \boldsymbol{u}\rangle) = (d; a, b)$. Pak ale podle věty 21.34 máme $(a, b, \langle \boldsymbol{u}\rangle, d)$ $= \frac{1}{(d;a,b)}$, a tedy $(a, b, c, d) = \frac{(c;a,b)}{(d;a,b)}$. ∎

21.41. Věta. *Buďte a, b, c tři různé body afinní přímky $A_1(V_1)$, kde V_1 je vektorový prostor nad tělesem charakteristiky různé od 2. Pak bod c je středem dvojice a, b, právě když $a, b, c, \langle \boldsymbol{u}\rangle$ je harmonická čtveřice bodů projektivní přímky $\bar{A}_1(\bar{V}_2)$ s nevlastním bodem $\langle \boldsymbol{u}\rangle$.*

Důkaz. Podle definice 19.29 je $(c; a, b) = -1$ a stačí použít větu 21.39. ∎

22.1. Definice. Buď f_2 kvadratická forma na vektorovém prostoru V. Množina $Q(f_2)$ všech vektorů $\boldsymbol{u} \in V$ takových, že $f_2(\boldsymbol{u}) = 0$ se nazývá *nulová množina kvadratické formy* f_2.

22.2. Věta. *Buď f_2 kvadratická forma na vektorovém prostoru V a buď W doplněk jejího vrcholu $V(f_2)$ ve V. Označíme-li $g_2 = f_2|W$ restrikci formy f_2 na podprostor W, pak forma g_2 je regulární a platí*

$$Q(f_2) = \bigcup_{\boldsymbol{u}\in Q(g_2)} \langle V(f_2) \cup \{\boldsymbol{u}\}\rangle = \bigcup_{\boldsymbol{u}\in Q(g_2)} (V(f_2) \vee \langle \boldsymbol{u}\rangle) =$$

$$\bigcup \{\langle \boldsymbol{v}\rangle \vee \langle \boldsymbol{u}\rangle | \boldsymbol{v} \in V(f_2), \boldsymbol{u} \in Q(g_2)\}.$$

Důkaz. Forma g_2 je regulární podle věty 12.21. Stačí dokázat první rovnost, neboť druhá je zřejmá, zatímco třetí plyne bezprostředně z věty 1.13. Buď tedy nejprve $\boldsymbol{v} \in Q(f_2)$. Podle věty 9.25 je $\boldsymbol{v} = \boldsymbol{w} + \boldsymbol{u}$, kde $\boldsymbol{w} \in V(f_2)$ a $\boldsymbol{u} \in W$. Přitom $g_2(\boldsymbol{u}) = f_2(\boldsymbol{u}) = f_2(\boldsymbol{v} - \boldsymbol{w}) = f_2(\boldsymbol{v}) - 2f(\boldsymbol{v}, \boldsymbol{w}) + f_2(\boldsymbol{w}) = 0$, takže $\boldsymbol{u} \in Q(g_2)$. Tedy $\boldsymbol{v} \in V(f_2) \vee \langle \boldsymbol{u}\rangle$ a $Q(f_2) \subseteq \cup_{\boldsymbol{u}\in Q(g_2)}\langle V(f_2) \cup \langle \boldsymbol{u}\rangle\rangle$.

Obráceně, je-li $\boldsymbol{v} \in \cup_{\boldsymbol{u}\in Q(g_2)}(V(f_2) \vee \langle \boldsymbol{u}\rangle)$, je $\boldsymbol{v} = \boldsymbol{w} + r\boldsymbol{u}$ pro nějaké $\boldsymbol{w} \in V(f_2)$, $\boldsymbol{u} \in Q(g_2)$, $r \in T$. Přitom platí $f_2(\boldsymbol{v}) = f_2(\boldsymbol{w}+r\boldsymbol{u}) = f_2(\boldsymbol{w})+2rf(\boldsymbol{w}, \boldsymbol{u})+r^2f_2(\boldsymbol{u}) = r^2g_2(\boldsymbol{u}) = 0$, a tedy $\boldsymbol{v} \in Q(f_2)$. ■

22.3. Věta. *Buď f_2 kvadratická forma na reálném vektorovém prostoru V_n a buď W podprostor prostoru V_n. Jestliže $W \subseteq Q(f_2)$, pak $\dim W \le \min(n(f_2)+p(f_2), n(f_2) +q(f_2)) = n(f_2)+\min(p(f_2), q(f_2))$, kde $\langle n(f_2), p(f_2), q(f_2)\rangle$ je signatura formy f_2.*

Důkaz. Předpokládejme nejprve, že forma f_2 je regulární, tj. $n(f_2) = 0$. Označme $k = \min(p(f_2), q(f_2))$, $\bar{k} = \max(p(f_2), q(f_2))$. Podle definice signatury 13.10 existuje podprostor W' prostoru V_n dimenze $\bar{k}$, na němž je forma f_2 definitivní (buď pozitivně, nebo negativně). Pak ale nutně $W \cap W' = 0$, takže použitím věty o dimenzi spojení a průniku 2.23 dostáváme $\dim W + \dim W' \le n$, a tedy $\dim W \le n - \bar{k} = k$.

Nechť tedy forma f_2 je singulární. Označme $W_1 = W \cap V(f_2)$ a buď W_2 doplněk W_1 ve W, tj. $W_1 \cap W_2 = 0$ a $W_1 \vee W_2 = W$. Protože $W_2 \cap V(f_2) \subseteq W_2 \cap W \cap V(f_2) = W_2 \cap W_1 = 0$, plyne snadno z věty 2.21 existence doplňku W' vrcholu $V(f_2)$ obsahujícího W_2. Označíme-li $g_2 = f_2|W'$ restrikci formy f_2 na podprostor W', je forma g_2 regulární podle věty 12.21 a její signatura je zřejmě $\langle 0, p(f_2), q(f_2)\rangle$. Protože $W_2 \subseteq Q(g_2)$, je podle první části důkazu $\dim W_2 \le \min(p(f_2), q(f_2))$. Mimoto $\dim W_1 \le n(f_2)$, odkud použitím věty 9.24 dostáváme $\dim W = \dim W_1 + \dim W_2 \le n(f_2) + \min(p(f_2), q(f_2))$. ■

22.4. Věta. *Buď f_2 kvadratická forma na reálném vektorovém prostoru V_n. Pak $Q(f_2)$ obsahuje podprostor prostoru V_n dimenze $k = n(f_2) + \min(p(f_2), q(f_2))$.*

Důkaz. Předpokládejme opět nejprve, že forma f_2 je regulární a buď $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ polární báze formy f_2. Zřejmě můžeme předpokládat, že všechna čísla $f_2(\boldsymbol{u}_i)$, $i = 1, 2, \dots, k$, mají totéž znaménko a všechna čísla $f_2(\boldsymbol{u}_i)$, $i = k+1, \dots, n$, mají totéž znaménko opačné k předchozímu. Pro každé $i = 1, 2, \dots, k$ položme $\boldsymbol{v}_i = \boldsymbol{u}_i + c_i\boldsymbol{u}_{k+i}$, kde $c_i = \sqrt{\frac{-f_2(\boldsymbol{u}_i)}{f_2(\boldsymbol{u}_{k+i})}}$. Poznamenejme, že podle předchozího je zlomek pod odmocninou kladný, takže c_i je reálné číslo. Ověřme, že vektory $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$ jsou lineárně nezávislé. Skutečně, z rovnosti $\sum_{i=1}^k r_i \boldsymbol{v}_i = 0$ dostáváme $\sum_{i=1}^k r_i(\boldsymbol{u}_i + c_i \boldsymbol{u}_{k+i}) = 0$, a tedy $r_1 = r_2 = \cdots = r_k = 0$ vzhledem k lineární nezávislosti vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$. Vidíme tedy, že podprostor $W = \langle \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k \rangle$ prostoru V_n má dimenzi k, a zbývá ukázat, že $W \subseteq Q(f_2)$. Předně pro všechna $i, j \in \{1, 2, \ldots, k\}$, $i \neq j$, je $f(\boldsymbol{v}_i, \boldsymbol{v}_j) = f(\boldsymbol{u}_i + c_i \boldsymbol{u}_{k+i}, \boldsymbol{u}_j + c_j \boldsymbol{u}_{k+j}) = 0$, neboť M je polární báze formy f_2. Je-li nyní $\boldsymbol{u} \in W$, $\boldsymbol{u} = \sum_{i=1}^k r_i \boldsymbol{v}_i$ libovolný vektor, je $f_2(\boldsymbol{u}) = f_2(\sum_{i=1}^k r_i \boldsymbol{v}_i) = \sum_{i=1}^k r_i^2 f_2(\boldsymbol{v}_i) = \sum_{i=1}^k r_i^2 f_2(\boldsymbol{u}_i + c_i \boldsymbol{u}_{k+i}) = \sum_{i=1}^k r_i^2 (f_2(\boldsymbol{u}_i) + c_i^2 f_2(\boldsymbol{u}_{k+i})) = 0$ vzhledem k volbě čísel $c_1, c_2, \ldots, c_k$.

Je-li nyní forma f_2 singulární, označíme W' doplněk vrcholu $V(f_2)$ ve V_n a $g_2 = f_2|W'$ restrikci formy f_2 na W'. Podle věty 12.21 je forma g_2 regulární, má zřejmě signaturu $\langle 0, p(f_2), q(f_2) \rangle$ a podle první části důkazu nulová množina $Q(g_2)$ obsahuje podprostor W'' prostoru W' dimenze $\min(p(f_2), q(f_2))$. Nakonec podle věty 22.2 je $W = V(f_2) \vee W'' \subseteq Q(f_2)$, přičemž podle věty 9.24 je $\dim W = \dim V(f_2) + \dim W'' = n(f_2) + \min(p(f_2), q(f_2))$, a věta je dokázána. ■

22.5. Poznámka. V předchozích dvou větách jsme ukázali, jak „velké" v závislosti na signatuře mohou být podprostory ležící v nulové množině kvadratické formy a že tato nulová množina skutečně obsahuje podprostory této maximální dimenze. V následující části uvidíme, že platí daleko silnější tvrzení. Ukážeme totiž, že podprostory maximální dimenze obsažené v nulové množině kvadratické formy jsou „všudypřítomné" v tom smyslu, že každý podprostor prostoru V_n ležící v nulové množině kvadratické formy je obsažen v podprostoru maximální dimenze $n(f_2) + \min(p(f_2), q(f_2))$, který leží celý v nulové množině kvadratické formy $Q(f_2)$.

22.6. Věta. *Buď f definitní symetrická bilineární forma na reálném vektorovém prostoru V_n a buď W_1 podprostor prostoru V_n. Pak existuje doplněk W_2 podprostoru W_1 ve V_n takový, že $f(\boldsymbol{u}, \boldsymbol{v}) = 0$ pro všechna $\boldsymbol{u} \in W_1$ a $\boldsymbol{v} \in W_2$.*

Důkaz. Bilineární forma f je buď pozitivně, nebo negativně definitní. V prvém případě je (V_n, f) unitární prostor a podle věty 14.7 (i) stačí vzít $W_2 = W_1^{\perp}$. Je-li f negativně definitní, je forma $g = -f$ zřejmě pozitivně definitní, takže ortogonální doplněk W_2 podprostoru W_1 v unitárním prostoru (V_n, g) je hledaným doplňkem vzhledem k tomu, že $g(\boldsymbol{u}, \boldsymbol{v}) = 0$, právě když $f(\boldsymbol{u}, \boldsymbol{v}) = 0$. ■

22.7. Věta. *Buď f_2 kvadratická forma na reálném vektorovém prostoru V_n a buď W podprostor prostoru V_n takový, že $W \subseteq Q(f_2)$. Označíme-li $\dim W = l$, $l \leq k = n(f_2) + \min(p(f_2), q(f_2))$, pak existuje podprostor W' prostoru V_n takový, že $W \subseteq W' \subseteq Q(f_2)$ a $\dim W' = k$.*

Důkaz. Předpokládejme nejprve, že forma f_2 je regulární, a rozdělme důkaz pro lepší přehlednost do pěti kroků.

1. Buď $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ polární báze formy f_2 taková, že všechna čísla $f_2(\boldsymbol{u}_i)$, $i = 1, 2, \ldots, k$, mají stejná znaménka a všechna čísla $f_2(\boldsymbol{u}_i)$, $i = k+1, \ldots, n$, mají stejná, ale opačná znaménka. Označíme-li $W_1 = \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle$ a $W_2 = \langle \boldsymbol{u}_{k+1}, \ldots, \boldsymbol{u}_n \rangle$, je zřejmé, že $V_n = W_1 \oplus W_2$ a že restrikce $f_2|W_1$ a $f_2|W_2$ jsou definitní kvadratické formy. Je-li nyní $\{\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_l\}$ libovolná báze podprostoru W, existují podle věty 2.28 vektory $\boldsymbol{u}_i' \in W_1$ a $\boldsymbol{v}_i' \in W_2$ (dokonce jednoznačně určené) takové, že $\boldsymbol{w}_i = \boldsymbol{u}_i' + \boldsymbol{v}_i'$ pro každé $i = 1, 2, \ldots, l$.

2. Položme $W_1' = \langle u_1', u_2', \ldots, u_l' \rangle \leq W_1$, $W_2' = \langle v_1', v_2', \ldots, v_l' \rangle \leq W_2$, a ukažme, že $\dim W_1' = \dim W_2' = l$. K tomuto cíli stačí zřejmě ověřit, že vektory $u_1', u_2', \ldots, u_l'$ a $v_1', v_2', \ldots, v_l'$ jsou lineárně nezávislé. Nechť tedy $\sum_{i=1}^l r_i u_i' = 0$. Pak $\sum_{i=1}^l r_i(w_i - v_i') = 0$, takže $\sum_{i=1}^l r_i w_i = \sum_{i=1}^l r_i v_i' \in W \cap W_2$. Protože forma f_2 je nulová na W a definitní na W_2, je $W \cap W_2 = 0$, $\sum_{i=1}^l r_i w_i = 0$, a tedy $r_1 = r_2 = \cdots = r_l = 0$ vzhledem k lineární nezávislosti vektorů $w_1, w_2, \ldots, w_l$. Stejným způsobem se ověří, že $\dim W_2' = l$.

3. Forma f_2 je definitní na W_1, takže podle předchozí věty existuje doplněk W_1'' podprostoru W_1' ve W_1, $W_1 = W_1' \oplus W_1''$, takový, že $f(u, v) = 0$ kdykoliv $u \in W_1'$ a $v \in W_1''$. Ze stejného důvodu je $W_2 = W_2' \oplus W_2''$ tak, že $f(u, v) = 0$ pro každé $u \in W_2'$ a každé $v \in W_2''$. Přitom zřejmě $\dim W_1'' = k - l$ a $\dim W_2' = n - k - l$.

4. Forma $f_2|(W_1'' \vee W_2'')$ má zřejmě signaturu buď $\langle 0, k - l, n - k - l \rangle$, nebo $\langle 0, n - k - l, k - l \rangle$. Protože $k \leq \frac{n}{2}$, je $k \leq n - k$, a tedy $k - l \leq n - k - l$. Podle věty 22.4 obsahuje nulová množina $Q(f_2|(W_1'' \vee W_2''))$ podprostor W'' dimenze $k - l$.

5. Označme $W' = W \vee W''$. Předně je $W \cap W'' \subseteq (W_1' \vee W_2') \cap W'' \subseteq (W_1' \vee W_2') \cap (W_1'' \vee W_2'')$. Je-li $w_1' + w_2' = w_1'' + w_2''$, $w_1' \in W_1'$, $w_2' \in W_2'$, $w_1'' \in W_1''$, $w_2'' \in W_2''$ libovolný prvek tohoto průniku, je $w_1' - w_1'' = w_2'' - w_2' \in W_1 \cap W_2 = 0$, takže $w_1' = w_1'' \in W_1' \cap W_1'' = 0$, $w_2' = w_2'' \in W_2' \cap W_2'' = 0$. Vidíme tedy, že $W \cap W'' = 0$, a podle věty o dimenzi spojení a průniku 2.23 je $\dim W' = \dim W + \dim W'' = k$. K dokončení důkazu tedy zbývá ověřit, že W' leží v nulové množině $Q(f_2)$ formy f_2. Buď tedy $w' \in W'$, $w' = w + w''$, $w \in W$, $w'' \in W''$, libovolný prvek. Protože jak W, tak W'' leží v nulové množině formy f_2, je $f_2(w) = f_2(w'')$, takže $f_2(w') = f_2(w + w'') = 2f(w, w'')$, a potřebujeme ukázat, že $f(w, w'') = 0$. Jelikož $w = \sum_{i=1}^l r_i w_i = \sum_{i=1}^l r_i(u_i' + v_i') = w_1' + w_2'$, $w_1' \in W_1'$, $w_2' \in W_2'$ a $w'' = w_1'' + w_2''$, $w_1'' \in W_1''$, $w_2'' \in W_2''$ (protože $W'' \subseteq W_1'' \vee W_2''$), je $f(w, w'') = f(w_1' + w_2', w_1'' + w_2'') = f(w_1', w_1'') + f(w_1', w_2'') + f(w_2', w_1'') + f(w_2', w_2'') = 0$, a to z následujících důvodů. První a čtvrtý sčítanec je nulový podle volby podprostorů W_1'' a W_2'' v části 3. tohoto důkazu a prostřední dva sčítance jsou rovné nule vzhledem k tomu, že $W_1', W_2'' \subseteq W_1$, $W_2', W_2'' \subseteq W_2$ a že z definice polární báze bezprostředně plyne $f(u, v) = 0$, kdykoliv $u \in W_1$ a $v \in W_2$.

Zbývá dokončit důkaz věty v případě, že forma f_2 je singulární. Označme $W_1 = W \cap V(f_2)$ a buď W_2 doplněk W_1 ve W, $W = W_1 \oplus W_2$. Protože $W_2 \cap V(f_2) = W_2 \cap W \cap V(f_2) = W_2 \cap W_1 = 0$, plyne z věty 2.21 existence doplňku W_3 vrcholu $V(f_2)$, který obsahuje W_2, tj. $V_n = V(f_2) \oplus W_3$, $W_2 \leq W_3$. Restrikce $f_2|W_3$ formy f_2 je regulární kvadratická forma na W_3 podle věty 12.21 a má zřejmě signaturu $\langle 0, p(f_2), q(f_2) \rangle$. Podle první části důkazu tedy existuje podprostor $W'' \leq W_3$ takový, že $W_2 \leq W''$, $W'' \subseteq Q(f_2|W_3)$ a $\dim W'' = \min(p(f_2), q(f_2))$. Položíme-li nyní $W' = V(f_2) \vee W''$, je $V(f_2) \cap W'' \subseteq V(f_2) \cap W_3 = 0$, a tedy $\dim W' = n(f_2) + \min(p(f_2), q(f_2))$ podle věty o dimenzi spojení a průniku 2.23. Přitom podle věty 22.2 je $W' \subseteq Q(f_2)$ a zároveň $W = W_1 \vee W_2 \subseteq V(f_2) \vee W'' = W'$, čímž je důkaz věty dokončen.

V následující části tohoto článku se podíváme na některé vzájemné vztahy mezi kvadratickými formami a automorfismy vektorového prostoru V_n. ■

22.8. Věta. *Buď h automorfismus vektorového prostoru V_n a buď f_2 kvadratická forma na V_n. Pak zobrazení $h(f_2) : V_n \to T$ definované pro $u \in V_n$ předpisem $(h(f_2))(h(u)) = f_2(u)$, je kvadratická forma na V_n. Mimoto formy f_2 a $h(f_2)$ mají* *stejnou nulitu.*

Důkaz. Buď f polární bilineární forma kvadratické formy f_2. Pro libovolné dva vektory $\boldsymbol{u}, \boldsymbol{v} \in V_n$ definujme $(h(f))(h(\boldsymbol{u}), h(\boldsymbol{v})) = f(\boldsymbol{u}, \boldsymbol{v})$ a ukažme, že $h(f)$ je symetrická bilineární forma na V_n. Pro libovolné tři vektory $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in V_n$ a libovolný prvek $r \in T$ je $(h(f))(h(\boldsymbol{u}), h(\boldsymbol{v})) = f(\boldsymbol{u}, \boldsymbol{v}) = f(\boldsymbol{v}, \boldsymbol{u}) = (h(f))(h(\boldsymbol{v}), h(\boldsymbol{u}))$, $(h(f))(h(\boldsymbol{u})+h(\boldsymbol{w}), h(\boldsymbol{v})) = (h(f))(h(\boldsymbol{u}+\boldsymbol{w}), h(\boldsymbol{v}) = f(\boldsymbol{u}+\boldsymbol{w}, \boldsymbol{v}) = f(\boldsymbol{u}, \boldsymbol{v})+f(\boldsymbol{w}, \boldsymbol{v})$ $= (h(f))(h(\boldsymbol{u}), h(\boldsymbol{v})) + (h(f))(h(\boldsymbol{w}), h(\boldsymbol{v}))$ a $(h(f))(rh(\boldsymbol{u}), h(\boldsymbol{v})) = (h(f))(h(r\boldsymbol{u}), h(\boldsymbol{v})) = f(r\boldsymbol{u}, \boldsymbol{v}) = rf(\boldsymbol{u}, \boldsymbol{v}) = r(h(f))(h(\boldsymbol{u}), h(\boldsymbol{v}))$. Dále $(h(f))_2(h(\boldsymbol{u})) = (h(f))(h(\boldsymbol{u}), h(\boldsymbol{u})) = f_2(\boldsymbol{u}) = (h(f_2))(h(\boldsymbol{u}))$, takže $h(f)$ je polární bilineární forma kvadratické formy $h(f_2)$. Nakonec z rovnosti $(h(f))(h(\boldsymbol{u}), h(\boldsymbol{v})) = f(\boldsymbol{u}, \boldsymbol{v})$ bezprostředně plyne, že $\boldsymbol{u} \in V(f_2)$ právě když $h(\boldsymbol{u}) \in V(h(f_2))$. Vidíme tedy, že vrcholy $V(f_2)$ a $V(h(f_2))$ jsou izomorfní (prostřednictvím h), a formy f_2 a $h(f_2)$ mají tudíž stejnou nulitu. ∎

22.9. Poznámka. V právě dokázané větě jsme definovali kvadratickou formu $h(f_2)$ a její polární bilineární formu $h(f)$ zdánlivě poněkud netradičním způsobem, totiž $(h(f))(h(\boldsymbol{u}), h(\boldsymbol{v})) = f(\boldsymbol{u}, \boldsymbol{v})$. Uvědomíme-li si však, že h je automorfismus prostoru V_n, tedy speciálně bijekce množiny V_n na sebe samu a že tudíž existuje automorfismus h^{-1} prostoru V_n inverzní k h vidíme, že jak formu $h(f)$, tak formu $h(f_2)$ bychom mohli definovat ekvivalentním způsobem pro vektory $\boldsymbol{u}, \boldsymbol{v} \in V_n$ takto: $(h(f))(\boldsymbol{u}, \boldsymbol{v}) = f(h^{-1}(\boldsymbol{u}), h^{-1}(\boldsymbol{v}))$ a $(h(f_2))(\boldsymbol{u}) = f_2(h^{-1}(\boldsymbol{u}))$. Ekvivalence obou zápisů vyplývá okamžitě z rovností $(h(f))(\boldsymbol{u}, \boldsymbol{v}) = (h(f))(h(h^{-1}(\boldsymbol{u})), h(h^{-1}(\boldsymbol{v})) = f(h^{-1}(\boldsymbol{u}), h^{-1}(\boldsymbol{v}))$, podobně pro $h(f_2)$.

22.10. Věta. *Buď h automorfismus reálného vektorového prostoru V_n a buď f_2 kvadratická forma na V_n. Pak formy f_2 a $h(f_2)$ mají stejnou signaturu.*

Důkaz. Buď $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ polární báze formy f_2. Podle věty 9.21 je množina $\{h(\boldsymbol{u}_1), h(\boldsymbol{u}_2), \ldots, h(\boldsymbol{u}_n)\}$ rovněž bází prostoru V_n. Přitom pro všechna $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$, je $h(f)(h(\boldsymbol{u}_i), h(\boldsymbol{u}_j) = f(\boldsymbol{u}_i, \boldsymbol{u}_j) = 0$, takže množina $\{h(\boldsymbol{u}_1), h(\boldsymbol{u}_2), \ldots, h(\boldsymbol{u}_n)\}$ je polární báze formy $h(f_2)$. Protože zároveň $(h(f_2))(h(\boldsymbol{u}_i)) = f_2(\boldsymbol{u}_i)$ pro každé $i = 1, 2, \ldots, n$, mají formy f_2 a $h(f_2)$ stejnou signaturu podle definice 13.10. ∎

22.11. Věta. *Buďte f, g regulární symetrické bilineární formy na vektorovém prostoru V_n. Jestliže* $\operatorname{Ker} \Phi^f(\boldsymbol{u}) = \operatorname{Ker} \Phi^g(\boldsymbol{u})$ *pro každé $\boldsymbol{u} \in V_n$, pak existuje nenulový prvek $r \in T$ tak, že $g_2 = rf_2$.*

Důkaz. Buď $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ báze vektorového prostoru V_n. Pro každé $i = 1, 2, \ldots, n$ existuje podle věty 11.14 (iii) nenulový prvek $r_i \in T$ tak, že $\Phi^g(\boldsymbol{u}_i) = r_i \Phi^f(\boldsymbol{u}_i)$. Z téhož důvodu existuje prvek $0 \neq r \in T$ tak, že $\Phi^g(\sum_{i=1}^n \boldsymbol{u}_i) = r\Phi^f(\sum_{i=1}^n \boldsymbol{u}_i)$. Protože forma f je regulární, je zobrazení $\Phi^f : V_n \to \widetilde{V}_n$ izomorfismus podle věty 12.15, takže podle věty 9.21 je množina $\{\Phi^f(\boldsymbol{u}_1), \Phi^f(\boldsymbol{u}_2), \ldots, \Phi^f(\boldsymbol{u}_n)\}$ báze duálního prostoru V_n. Pak ale z $\sum_{i=1}^n r\Phi^f(\boldsymbol{u}_i) = r\Phi^f(\sum_{i=1}^n \boldsymbol{u}_i) = \Phi^g(\sum_{i=1}^n \boldsymbol{u}_i) = \sum_{i=1}^n \Phi^g(\boldsymbol{u}_i) = \sum_{i=1}^n r_i \Phi^f(\boldsymbol{u}_i)$ dostáváme $r_1 = r_2 = \cdots = r_n = r$, takže pro libovolný vektor $\boldsymbol{u} = \sum_{i=1}^n s_i \boldsymbol{u}_i$ je $\Phi^g(\boldsymbol{u}) = \Phi^g(\sum_{i=1}^n s_i \boldsymbol{u}_i) = \sum_{i=1}^n s_i \Phi^g(\boldsymbol{u}_i) = \sum_{i=1}^n s_i r \Phi^f(\boldsymbol{u}_i) = r\Phi^f(\sum_{i=1}^n s_i \boldsymbol{u}_i) = r\Phi^f(\boldsymbol{u})$. Speciálně tedy pro každé $\boldsymbol{u} \in V_n$ je $g_2(\boldsymbol{u}) = (\Phi^g(\boldsymbol{u}))(\boldsymbol{u}) = (r\Phi^f(\boldsymbol{u}))(\boldsymbol{u}) = rf_2(\boldsymbol{u})$, tj. $g_2 = rf_2$. ∎

V závěru tohoto odstavce se budeme zabývat některými vlastnostmi symetrických bilineárních a kvadratických forem na unitárních prostorech. Začněme s následujícím užitečným tvrzením o regulárních symetrických bilineárních formách.

22.12. Lemma. *Buď f regulární symetrická bilineární forma na unitárním prostoru (V_n, g). Pak existuje nenulový vektor $\boldsymbol{u} \in V_n$ takový, že* $\operatorname{Ker} \Phi^f(\boldsymbol{u}) = \operatorname{Ker} \Phi^g(\boldsymbol{u})$ *a $f_2(\boldsymbol{u}) \neq 0$.*

Důkaz. Buď $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ libovolná ortonormální báze prostoru (V_n, g) a buď $\boldsymbol{A} = (a_{ij})$ matice formy f vzhledem k bázi M. Podle věty 11.14 mají lineární formy $\Phi^g(\boldsymbol{u})$ a $\Phi^f(\boldsymbol{u})$ stejnou nulovou množinu, právě když $\Phi^f(\boldsymbol{u}) = \lambda \Phi^g(\boldsymbol{u})$ pro nějaké nenulové reálné číslo λ. Jsou-li $\{\boldsymbol{u}\}_M = (x_1, x_2, \dots, x_n)$ a $\{\boldsymbol{v}\}_M = (y_1, y_2, \dots, y_n)$ souřadnice vektorů $\boldsymbol{u}$ a $\boldsymbol{v}$ vzhledem k bázi M, jsou $(\Phi^f(\boldsymbol{u}))(\boldsymbol{v}) = f(\boldsymbol{u}, \boldsymbol{v}) = \sum_{ij=1}^n a_{ij} x_i y_j = \sum_{j=1}^n (\sum_{i=1}^n a_{ij} x_i) y_j$ a $(\Phi^g(\boldsymbol{u}))(\boldsymbol{v}) = g(\boldsymbol{u}, \boldsymbol{v}) = \sum_{j=1}^n x_j y_j$ analytická vyjádření lineárních forem $\Phi^f(\boldsymbol{u})$ a $\Phi^g(\boldsymbol{u})$ vzhledem k ortonormální bázi M prostoru (V_n, g). Vidíme tedy, že pro každé $\boldsymbol{v} \in V_n$ musí platit rovnost $(\Phi^f(\boldsymbol{u}))(\boldsymbol{v}) = \lambda(\Phi^g(\boldsymbol{u}))(\boldsymbol{v})$, takže pro každé $j = 1, 2, \dots, n$ dostáváme rovnost $\sum_{i=1}^n a_{ij} x_i = \lambda x_j$. Odtud je patrné, že souřadnice vektoru $\boldsymbol{u}$ vzhledem k bázi M musí být pro nějaké $0 \neq \lambda \in R$ řešením homogenní soustavy lineárních rovnic

$$(*)\qquad \begin{array}{ccccccccc}
(a_{11} - \lambda)x_1 & + & a_{21}x_2 & + & \dots & + & a_{n1}x_n & = & 0, \\
a_{12}x_1 & + & (a_{22} - \lambda)x_2 & + & \dots & + & a_{n2}x_n & = & 0, \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
a_{1n}x_1 & + & a_{2n}x_2 & + & \dots & + & (a_{nn} - \lambda)x_n & = & 0
\end{array}$$

s maticí $\boldsymbol{A}^T - \lambda \boldsymbol{E} = \boldsymbol{A} - \lambda \boldsymbol{E}$ vzhledem k tomu, že matice $\boldsymbol{A}$ je symetrická. Podle důsledku 5.9 má soustava (*) netriviální řešení, právě když matice $\boldsymbol{A} - \lambda \boldsymbol{E}$ je singulární, což jest podle věty 8.4 ekvivalentní s tím, že $\det(\boldsymbol{A} - \lambda \boldsymbol{E}) = 0$. Podle věty 15.10 má symetrická matice všechna vlastní čísla reálná. Přitom absolutní člen polynom $\det(\boldsymbol{A} - \lambda \boldsymbol{E})$ je zřejmě roven $\det \boldsymbol{A}$, což je s ohledem na regularitu formy f nenulové číslo, takže všechna vlastní čísla matice $\boldsymbol{A}$ jsou rovněž nenulová. Pro libovolné vlastní číslo $\lambda \in R$ matice $\boldsymbol{A}$ tedy existuje nenulový vektor $\boldsymbol{u} \in V_n$, jehož souřadnice vzhledem k M, $\{\boldsymbol{u}\}_M = (x_1, x_2, \dots, x_n)$, jsou řešením soustavy (*). Nakonec je $f_2(\boldsymbol{u}) = \sum_{i,j=1}^n a_{ij} x_i x_j = \sum_{j=1}^n x_j \sum_{i=1}^n a_{ij} x_i = \lambda \sum_{j=1}^n x_j^2 \neq 0$ a lemma je dokázáno. ■

22.13 Věta. *Ke každé symetrické bilineární formě f na unitárním prostoru (V_n, g) existuje ortonormální polární báze, tj. báze, která je ortonormální bází prostoru (V_n, g) a zároveň polární bází bilineární formy f.*

Důkaz. Začneme opět s případem, kdy forma f je regulární, a budeme postupovat úplnou indukcí podle dimenze n. Pro $n = 1$ stačí vzít libovolný nenulový vektor $\boldsymbol{v} \in V_1$ a ve smyslu poznámky 14.5 položit $\boldsymbol{u} = \frac{\boldsymbol{v}}{\|\boldsymbol{v}\|}$. Buď tedy $n > 1$ a předpokládejme, že pro $n - 1$ již tvrzení platí. Podle předchozího lemmatu existuje nenulový vektor $\boldsymbol{u}_n \in V_n$ takový, že $\operatorname{Ker} \Phi^f(\boldsymbol{u}_n) = \operatorname{Ker} \Phi^g(\boldsymbol{u}_n) = W$ a $f_2(\boldsymbol{u}_n) \neq 0$. Podle věty 11.14 je W nadrovina ve V_n a podle věty 12.22 je restrikce $f|W$ regulární symetrická bilineární forma na unitárním prostoru (W, g). Pak ale podle indukčního předpokladu existuje ortonormální polární báze $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_{n-1}\}$ formy $f|W$

na (W, g). Vzhledem k poznámce 14.5 můžeme předpokládat, že $||\boldsymbol{u}_n|| = 1$. Protože vektory $\boldsymbol{u}_i$, $i = 1, 2, \ldots, n-1$, leží v nadrovině $\operatorname{Ker}\Phi^f(\boldsymbol{u}_n) = \operatorname{Ker}\Phi^g(\boldsymbol{u}_n)$, je $f(\boldsymbol{u}_n, \boldsymbol{u}_i) = (\Phi^f(\boldsymbol{u}_n))(\boldsymbol{u}_i) = 0$, $g(\boldsymbol{u}_n, \boldsymbol{u}_i) = (\Phi^g(\boldsymbol{u}_n))(\boldsymbol{u}_i) = 0$ a $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ je ortonormální polární báze formy f na (V_n, g).

Zbývá dokončit důkaz pro případ, že forma f je singulární. Podle věty 14.7 je ortogonální doplněk $W = V(f)^{\perp}$ vrcholu $V(f)$ doplňkem vrcholu $V(f)$, $V_n = V(f) \oplus W$. Je-li $\dim W = k$, je podle věty 9.24 $\dim V(f) = n-k$, přičemž podle věty 12.21 je restrikce $f|W$ regulární symetrická bilineární forma na unitárním prostoru (W, g). Podle první části důkazu existuje ortonormální polární báze $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k\}$ formy $f|W$ a podle věty 14.6 existuje ortonormální báze $\{\boldsymbol{u}_{k+1}, \ldots, \boldsymbol{u}_n\}$ unitárního prostoru $(V(f), g)$. Podle věty 2.29 je množina $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ báze prostoru V_n. Protože $V(f) \perp W$, je báze M ortonormální, a jelikož $f(\boldsymbol{u}, \boldsymbol{v}) = 0$ pro každé $\boldsymbol{u} \in V(f)$ a každé $\boldsymbol{v} \in V_n$, je množina M polární bází formy f. ■

22.14. Věta. *Buď $\boldsymbol{A} = (a_{ij}) \in R_n$ symetrická čtvercová matice stupně n a buďte $\mu, \nu \in R$, $\mu \neq \nu$, vlastní čísla matice $\boldsymbol{A}$. Je-li $\boldsymbol{u} \in R^n$ vlastní vektor matice $\boldsymbol{A}$ příslušný číslu μ a $\boldsymbol{v} \in R^n$ vlastní vektor této matice příslušný číslu ν, pak $\omega(\boldsymbol{u}, \boldsymbol{v}) = 0$, tj. vektory $\boldsymbol{u}, \boldsymbol{v}$ jsou kolmé v unitárním prostoru (R^n, ω).*

Důkaz. Označme $\boldsymbol{u} = (x_1, x_2, \ldots, x_n)$, $\boldsymbol{v} = (y_1, y_2, \ldots, y_n)$. Podle důsledku 15.3 platí $\sum_{i=1}^n a_{ji}x_i = \mu x_j$ pro každé $j = 1, 2, \ldots, n$ a $\sum_{y=1}^n a_{ij}y_j = \nu y_i$ pro každé $i = 1, 2, \ldots, n$. Pak ale máme jednak $\sum_{i,j=1}^n a_{ij}x_iy_j = \sum_{i=1}^n x_i \sum_{j=1}^n a_{ij}y_j = \nu \sum_{i=1}^n x_iy_i$, jednak, vzhledem k symetričnosti matice $\boldsymbol{A}$, $\sum_{i,j=1}^n a_{ij}x_iy_j = \sum_{j=1}^n y_j \sum_{i=1}^n a_{ji}x_i = \mu \sum_{j=1}^n x_jy_j$, odkud porovnáním dostáváme $(\mu - \nu)\sum_{i=1}^n x_iy_i = 0$ a tedy $\sum_{i=1}^n x_iy_i = \omega(\boldsymbol{u}, \boldsymbol{v}) = 0$ vzhledem k tomu, že $\mu - \nu \neq 0$. ■

22.15. Věta. *Buď $\lambda \in T$ vlastní hodnota čtvercové matice $\boldsymbol{A} = (a_{ij}) \in T_n$. Pak množina všech vlastních vektorů matice $\boldsymbol{A}$ příslušných prvku λ tvoří podprostor prostoru T^n.*

Důkaz. Jsou-li $\boldsymbol{u}, \boldsymbol{v}$ dva vlastní vektory matice $\boldsymbol{A}$ příslušné prvku $\lambda \in T$ a je-li $r \in T$ libovolný prvek, pak podle věty 4.7 jest $\boldsymbol{A}(\boldsymbol{u}+\boldsymbol{v})^T = \boldsymbol{A}(\boldsymbol{u}^T + \boldsymbol{v}^T) = \boldsymbol{A}\boldsymbol{u}^T + \boldsymbol{A}\boldsymbol{v}^T = \lambda\boldsymbol{u}^T + \lambda\boldsymbol{v}^T = \lambda(\boldsymbol{u}+\boldsymbol{v})^T$, $\boldsymbol{A}(r\boldsymbol{u})^T = r\boldsymbol{A}\boldsymbol{u}^T = r\lambda\boldsymbol{u}^T = \lambda(r\boldsymbol{u})^T$ a jsme hotovi. ■

22.16. Definice. Buď $\lambda \in T$ vlastní hodnota čtvercové matice $\boldsymbol{A} = (a_{ij}) \in T_n$. Podprostor $W(\lambda) = \{\boldsymbol{u} \in T^n |\, \boldsymbol{u}$ je vlastní vektor matice $\boldsymbol{A}$ příslušný prvku $\lambda\}$ se nazývá *vlastní podprostor matice* $\boldsymbol{A}$ příslušný prvku λ.

22.17. Věta. *Buď M ortonormální báze unitárního prostoru (V_n, g) a $\boldsymbol{A}$ matice regulární symetrické bilineární formy f na V_n vzhledem k bázi M. Nechť dále $\lambda_1, \lambda_2, \ldots, \lambda_k$ jsou právě všechny navzájem různé reálné kořeny charakteristického polynomu $\det(\boldsymbol{A} - \lambda\boldsymbol{E})$ matice $\boldsymbol{A}$ a označme $\boldsymbol{B}_i = \boldsymbol{A} - \lambda_i\boldsymbol{E}$ a $W(\boldsymbol{B}_i) = \{\boldsymbol{u} \in V_n | \{\boldsymbol{u}\}_M \in W(\lambda_i)\}$, $i = 1, 2, \ldots, k$. Pak platí*

(i) je-li $\boldsymbol{u} \in W(\boldsymbol{B}_i)$ pro nějaké $i \in \{1, 2, \ldots, k\}$, pak $\operatorname{Ker}\Phi^g(\boldsymbol{u}) = \operatorname{Ker}\Phi^f(\boldsymbol{u})$;
(ii) je-li $\operatorname{Ker}\Phi^g(\boldsymbol{u}) = \operatorname{Ker}\Phi^f(\boldsymbol{u})$, pak $\boldsymbol{u} \in W(\boldsymbol{B}_i)$ pro nějaké $i \in \{1, 2, \ldots, k\}$;
(iii) $W(\boldsymbol{B}_i) \perp W(\boldsymbol{B}_j)$, kdykoliv $i, j \in \{1, 2, \ldots, k\}$, $i \neq j$;
(iv) $V_n = \oplus_{i=1}^n W(\boldsymbol{B}_i)$;
(v) je-li N_i, $i = 1, 2, \ldots, k$, ortonormální báze prostoru $W(\boldsymbol{B}_i)$, pak $N = \bigcup_{i=1}^k N_i$ je ortonormální polární báze formy f.

Důkaz. Pro vektory $\boldsymbol{u}$, $\boldsymbol{v} \in V_n$ označme $\{\boldsymbol{u}\}_M = (x_1, x_2, \dots, x_n)$ a $\{\boldsymbol{v}\}_M = (y_1, y_2, \dots, y_n)$.

(i) Je-li $\boldsymbol{u} \in W(\boldsymbol{B}_i)$, je $\{\boldsymbol{u}\}_M \in W(\lambda_i)$, takže $\boldsymbol{A}\{\boldsymbol{u}\}_M^T = \lambda_i\{\boldsymbol{u}\}_M^T$ podle důsledku 15.3. Pro každý vektor $\boldsymbol{v} \in V_n$ nyní podle věty 12.3 a 14.8 máme $(\Phi^f(\boldsymbol{u})(\boldsymbol{v}) = f(\boldsymbol{v}, \boldsymbol{u}) = \{\boldsymbol{v}\}_M \boldsymbol{A}\{\boldsymbol{u}\}_M^T = \lambda_i\{\boldsymbol{v}\}_M\{\boldsymbol{u}\}_M = \lambda_i g(\boldsymbol{u}, \boldsymbol{v}) = (\lambda_i \Phi^g(\boldsymbol{u}))(\boldsymbol{v})$, takže $\Phi^f(\boldsymbol{u}) = \lambda_i \Phi^g(\boldsymbol{u})$ a $\operatorname{Ker} \Phi^f(\boldsymbol{u}) = \operatorname{Ker} \Phi^g(\boldsymbol{u})$ podle věty 11.14 (iii).

(ii) Podle věty 11.14 (iii) existuje $\lambda \in R$ takové, že $\Phi^f(\boldsymbol{u}) = \lambda \Phi^g(\boldsymbol{u})$, odkud podle předchozí části důkazu a věty 12.3 plyne $f(\boldsymbol{u}, \boldsymbol{v}) = \sum_{i,j=1}^n a_{ij} x_i y_j = \sum_{j=1}^n (\sum_{i=1}^n a_{ij} x_i) y_j = \lambda g(\boldsymbol{u}, \boldsymbol{v}) = \lambda \sum_{j=1}^n x_j y_j$ pro každý vektor $\boldsymbol{v} \in V_n$. Pak ale pro každé $j = 1, 2, \dots, n$ musí platit $\sum_{i=1}^n a_{ij} x_i = \lambda x_j$, souřadnice vektoru $\boldsymbol{u}$ vzhledem k bázi M tedy splňují homogenní soustavu lineárních rovnic $(*)$ z důkazu lemmatu 22.12, tj. soustavu rovnic s maticí $\boldsymbol{A} - \lambda \boldsymbol{E}$. Odtud stejně jako v důkazu lemmatu 22.12 plyne, že λ musí být vlastní číslo matice $\boldsymbol{A}$ a $\{\boldsymbol{u}\}_M$ vlastní vektor příslušný číslu λ. Protože podle věty 15.10 jsou všechny vlastní hodnoty matice $\boldsymbol{A}$ reálná čísla, je $\lambda = \lambda_i$ pro některé $i \in \{1, 2, \dots, k\}$ podle předpokladu.

(iii) Podle věty 14.18 je zobrazení $\varphi : (V_n, g) \to (R_n, \omega)$, kde $\varphi(\boldsymbol{u}) = \{\boldsymbol{u}\}_M$ pro každé $\boldsymbol{u} \in V_n$, unitární zobrazení. Jsou-li tedy $\boldsymbol{u} \in W(\boldsymbol{B}_i)$ a $\boldsymbol{v} \in W(\boldsymbol{B}_j)$, $i \neq j$, libovolné vektory, je $g(\boldsymbol{u}, \boldsymbol{v}) = \omega(\{\boldsymbol{u}\}_M, \{\boldsymbol{v}\}_M)$, přičemž $\{\boldsymbol{u}\}_M \in W(\lambda_i)$ a $\{\boldsymbol{v}\}_M \in W(\lambda_j)$. Pak ale $\omega(\{\boldsymbol{u}\}_M, \{\boldsymbol{v}\}_M) = 0$ podle věty 22.14 a vektory $\boldsymbol{u}$ a $\boldsymbol{v}$ jsou kolmé.

(iv) Podle věty 22.13 existuje ortonormální polární báze $N = \{\boldsymbol{v}_1, \boldsymbol{v}_2 \dots, \boldsymbol{v}_n\}$ bilineární formy f na unitárním prostoru (V_n, g). Je-li $j \in \{1, 2, \dots, n\}$ libovolný prvek, pak pro každé $i \neq j$ je $f(\boldsymbol{v}_j, \boldsymbol{v}_i) = 0 = g(\boldsymbol{v}_j, \boldsymbol{v}_i)$, a tedy $\operatorname{Ker} \Phi^f(\boldsymbol{v}_j) = \operatorname{Ker} \Phi^g(\boldsymbol{v}_j) = \langle \boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_{j-1}, \boldsymbol{v}_{j+1}, \dots, \boldsymbol{v}_n \rangle$. Podle tvrzení (ii) leží každý vektor $\boldsymbol{v}_j$ v některém podprostoru $W(\boldsymbol{B}_i)$, $i = 1, 2, \dots, k$, což znamená, že $V_n = \langle \boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n \rangle \subseteq \langle \bigcup_{j=1}^k W(\boldsymbol{B}_i) \rangle \subseteq V_n$, a tedy $V_n = \bigvee_{i=1}^k W(\boldsymbol{B}_i)$. Na druhé straně, je-li $\boldsymbol{u} \in W(\boldsymbol{B}_i) \cap (\bigvee_{j \neq i} W(\boldsymbol{B}_j))$, $\boldsymbol{u} = \boldsymbol{w}_1 + \boldsymbol{w}_2 + \dots + \boldsymbol{w}_{i-1} + \boldsymbol{w}_{i+1} + \dots + \boldsymbol{w}_k$, $\boldsymbol{w}_j \in W(\boldsymbol{B}_j)$, libovolný prvek, je $g_2(\boldsymbol{u}) = g(\boldsymbol{u}, \sum_{j \neq i} \boldsymbol{w}_j) = \sum_{j \neq i} g(\boldsymbol{u}, \boldsymbol{w}_j) = 0$ podle tvrzení (iii), takže $\boldsymbol{u} = 0$, a stačí si uvědomit definici direktního součtu 2.27.

(v) Množina N je báze prostoru V_n podle věty 2.29. Pro každé $\boldsymbol{u} \in N$ je podle (i) $\operatorname{Ker} \Phi^f(\boldsymbol{u}) = \operatorname{Ker} \Phi^g(\boldsymbol{u})$, takže $f(\boldsymbol{u}, \boldsymbol{v}) = 0$, právě když $g(\boldsymbol{u}, \boldsymbol{v}) = 0$, a stačí tudíž ověřit, že N je ortonormální báze prostoru (V_n, g). Tato skutečnost však bezprostředně plyne jednak z volby N_i, $i = 1, 2, \dots, k$, jednak z tvrzení (iii). ■

23.1. Definice. Buď $P_n(V_{n+1})$ n-rozměrný projektivní prostor a buď f_2 kvadratická forma na V_{n+1}. Množinu $Q_{f_2} = \{\langle \boldsymbol{u} \rangle \in P_n | f_2(\boldsymbol{u}) = 0\}$ nazýváme *kvadrikou v* P_n *vytvořenou kvadratickou formou* f_2. Říkáme, že kvadrika Q_{f_2} je *regulární*, jestliže je regulární forma f_2, a že Q_{f_2} je *singulární*, je-li forma f_2 singulární. Je-li přitom V_{k+1} vrchol kvadratické formy f_2, pak podprostor $P_k(V_{k+1})$ prostoru $P_n(V_{n+1})$ nazýváme *vrcholem kvadriky* Q_{f_2}.

23.2. Poznámka. V definici 22.1 jsme zavedli nulovou množinu kvadratické formy f_2 jako množinu $Q(f_2) = \{\boldsymbol{u} \in V | f_2(\boldsymbol{u}) = 0\}$. Kvadrika Q_{f_2} v projektivním prostoru $P_n(V_{n+1})$ je tedy množina právě těch geometrických bodů $\langle \boldsymbol{u} \rangle \in P_n$, jejichž aritmetičtí zástupci leží v nulové množině $Q(f_2)$ kvadratické formy f_2, tedy $Q_{f_2} = \{\langle \boldsymbol{u} \rangle \in P_n | \boldsymbol{u} \in Q(f_2)\}$. Aplikací věty 22.2 nyní převedeme otázku singulárních kvadrik na studium kvadrik regulárních a těm se budeme věnovat do konce této kapitoly.

23.3. Věta. *Buď* Q_{f_2} *singulární kvadrika v projektivním prostoru* $P_n(V_{n+1})$ *a* $P_k(V_{k+1})$ *buď její vrchol. Je-li* $P_l(V_{l+1})$ *(libovolný) doplněk vrcholu* $P_k(V_{k+1})$ *v prostoru* $P_n(V_{n+1})$, *pak* $Q_{f_2} \cap P_l(V_{l+1}) = Q_{g_2}$ *je regulární kvadrika v* $P_l(V_{l+1})$ *vytvořená kvadratickou formou* $g_2 = f_2 | V_{l+1}$ *a*

$$Q_{f_2} = \bigcup_{\langle \boldsymbol{v} \rangle \in Q_{g_2}} (P_k \vee \langle \boldsymbol{v} \rangle) = \bigcup_{\substack{\langle \boldsymbol{u} \rangle \in P_k \\ \langle \boldsymbol{v} \rangle \in Q_{g_2}}} (\langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle).$$

Jinými slovy, Q_{f_2} *je sjednocením množiny všech přímek spojujících libovolný bod z vrcholu kvadriky* Q_{f_2} *s libovolným bodem regulární kvadriky* Q_{f_2} *v doplňku vrcholu* P_k.

Důkaz. Plyne bezprostředně z věty 22.2. ∎

23.4. Definice. Buď Q_{f_2} regulární kvadrika v projektivním prostoru $P_n(V_{n+1})$ a buď f polární bilineární forma kvadratické formy f_2. Říkáme, že body $\langle \boldsymbol{u} \rangle$, $\langle \boldsymbol{v} \rangle \in P_n$ jsou *konjugovány* vzhledem ke kvadrice Q_{f_2}, jestliže $f(\boldsymbol{u}, \boldsymbol{v}) = 0$.

23.5. Věta. *Buď* $Q(f_2)$ *regulární kvadrika v projektivním prostoru* $P_n(V_{n+1})$. *Pak platí*

(i) množina všech bodů $\langle \boldsymbol{v} \rangle \in P_n$ *konjugovaných s daným bodem* $\langle \boldsymbol{u} \rangle \in P_n$ *je nadrovina v* P_n*;*

(ii) je-li $P_{n-1}(V_n)$ *libovolná nadrovina v* P_n, *pak existuje právě jeden bod* $\langle \boldsymbol{u} \rangle \in P_n$ *takový, že daná nadrovina* $P_{n-1}(V_n)$ *je množina právě všech bodů z* P_n, *které jsou konjugovány s bodem* $\langle \boldsymbol{u} \rangle$.

Důkaz. (i) Buď f polární bilineární forma kvadratické formy f_2. Podle věty 12.15 je zobrazení $\Phi^f : V_{n+1} \to \widetilde{V}_{n+1}$, definované pro $\boldsymbol{u}, \boldsymbol{v} \in V_{n+1}$ vztahem $(\Phi^f(\boldsymbol{u}))(\boldsymbol{v}) = f(\boldsymbol{u}, \boldsymbol{v})$, izomorfismus. Přitom $f(\boldsymbol{u}, \boldsymbol{v}) = 0$, právě když $\boldsymbol{v} \in \operatorname{Ker} \Phi^f(\boldsymbol{u})$. Protože $\boldsymbol{u}$ je nenulový vektor, je lineární forma $\Phi^f(\boldsymbol{u})$ rovněž nenulová a $\operatorname{Ker} \Phi^f(\boldsymbol{u})$ je podle věty 11.14 nadrovina ve V_{n+1} a tvrzení (i) je dokázáno.

(ii) Buď tedy naopak $P_{n-1}(V_n)$ nadrovina v P_n. Podle věty 11.14 existuje netriviální lineární forma $g \in \widetilde{V}_{n+1}$ taková, že $\operatorname{Ker} g = V_n$ a forma g je přitom až na násobek určena jednoznačně. Protože Φ^f je izomorfismus, existuje jednoznačně určený vektor $u \in V_{n+1}$ takový, že $\Phi^f(u) = g$. Protože forma g je netriviální, je vektor u nenulový a určuje tedy geometrický bod $\langle u \rangle$. Přitom geometrický bod $\langle v \rangle \in P_n$ je konjugován s bodem $\langle u \rangle$, právě když $\Phi^f(u)(v) = f(u, v) = 0$, tj. právě když $v \in \operatorname{Ker} \Phi^f(u) = \operatorname{Ker} g = V_n$, což je ekvivalentní s tím, že $\langle v \rangle \in P_{n-1}(V_n)$. ■

23.6. Definice. Buď Q_{f_2} regulární kvadrika v projektivním prostoru $P_n(V_{n+1})$. Množinu $\varrho_{\langle u \rangle}$ všech bodů $\langle v \rangle \in P_n$ konjugovaných s bodem $\langle u \rangle$ vzhledem ke kvadrice Q_{f_2} nazýváme *polární nadrovinou bodu* $\langle u \rangle$ vzhledem ke kvadrice Q_{f_2} a bod $\langle u \rangle$ nazýváme *pólem* této nadroviny. Jestliže bod $\langle u \rangle$ leží na kvadrice, $\langle u \rangle \in Q_{f_2}$, pak místo polární nadrovina říkáme *tečná nadrovina* a místo pól říkáme *bod dotyku*. Pro $n = 2$ pak hovoříme o *poláře* a *tečně*.

23.7. Poznámka. Právě zavedené pojmy mají zásadní důležitost, a nebude proto na škodu, když si je pro větší přehlednost napíšeme ve tvaru formulí. Je-li tedy Q_{f_2} regulární kvadrika na $P_n(V_{n+1})$, pak pro každý bod $\langle u \rangle$ je

$$\varrho_{\langle u \rangle} = \{\langle v \rangle \in P_n | f(u, v) = 0\} = \{\langle v \rangle \in P_n | 0 \neq v \in \operatorname{Ker} \Phi^f(u)\}$$

jeho polární nadrovina. Naopak, je-li $P_{n-1}(V_n)$ libovolná nadrovina v P_n, pak bod $\langle u \rangle \in P_n$ takový, že $\operatorname{Ker} \Phi^f(u) = V_n$, neboli $f(u, v) = 0$, právě když $v \in V_n$, je pólem nadroviny $P_{n-1}(V_n)$.

23.8. Věta. *Buď Q_{f_2} regulární kvadrika v projektivním prostoru $P_n(V_{n+1})$. Pak platí*

(i) ke každému geometrickému bodu $\langle u \rangle \in P_n$ existuje jednoznačně určená polární nadrovina $\varrho_{\langle u \rangle}$ vzhledem ke Q_{f_2};

(ii) ke každé nadrovině $P_{n-1}(V_n)$ existuje v P_n jednoznačně určený pól vzhledem ke Q_{f_2};

(iii) leží-li bod $\langle v \rangle \in P_n$ v polární nadrovině $\varrho_{\langle u \rangle}$ bodu $\langle u \rangle$, pak bod $\langle u \rangle$ leží v polární nadrovině $\varrho_{\langle v \rangle}$ bodu $\langle v \rangle$.

Důkaz. Tvrzení (i) a (ii) plynou bezprostředně z věty 23.5. K důkazu posledního tvrzení si stačí uvědomit, že vzhledem k symetričnosti formy f je rovnost $f(u, v) = 0$ ekvivalentní jak s $\langle v \rangle \in \varrho_{\langle u \rangle}$, tak s $\langle u \rangle \in \varrho_{\langle v \rangle}$. ■

23.9. Poznámka. Právě dokázané tvrzení (iii) předchozí věty je, jak jsme viděli, zcela triviální. Nicméně má toto tvrzení zejména pro početní techniku obrovský význam. Ukažme si to na několika konkrétních příkladech, v nichž budeme řešit úlohy z afinních prostorů v jejich projektivních rozšířeních. Pochopitelně lze tyto úlohy řešit přímo v příslušných afinních prostorech a čtenář se může sám přesvědčit, oč je takové řešení delší a složitější.

23.10. Příklady. Ve všech třech následujících příkladech předpokládáme, že je dána afinní rovina $A(V_2)$, kde V_2 je vektorový prostor nad tělesem T charakteristiky 0 (speciálně nad tělesem R reálných čísel), a že všechny souřadnice, ať bodů nebo vektorů, jsou vztaženy k nějaké dané soustavě souřadnic $S = \{a, u_1, u_2\}$.

1. Určeme tečnu křivky dané rovnicí $16x^2 - 25y^2 = 400$ v bodech, jejichž druhá souřadnice je rovna 4.

Ř e š e n í : Bod $b \in A_2$, v němž tečnu hledáme, musí ležet na dané křivce. Jestliže tedy $\{b\}_S = (x, 4)$, pak $16x^2 - 25 \cdot 16 = 400$, takže $16x^2 = 800$, $x^2 = 50$ a $x = \pm 5\sqrt{2}$.

Vzhledem k soustavě souřadnic $\bar{S} = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2\}$ projektivního rozšíření $\bar{A}_2(\bar{V}_3)$ indukované soustavou S má podle věty 21.25 aritmetický zástupce $x_0 c$ bodu c o souřadnicích $\{c\}_S = (x, y)$ homogenní souřadnice $\{x_0 c\}_{\bar{S}} = (x_0, x_1, x_2) = (x_0, x x_0, y x_0)$, takže $x = \frac{x_1}{x_0}$, $y = \frac{x_2}{x_0}$. Dosadíme-li toto do rovnice křivky, dostaneme po úpravě její rovnici v homogenních souřadnicích $400x_0^2 - 16x_1^2 + 25x_2^2 = 0$. Příslušná polární bilineární forma má analytické vyjádření $f(\boldsymbol{u}, \boldsymbol{v}) = 400x_0y_0 - 16x_1y_1 + 25x_2y_2$, kde $\{\boldsymbol{u}\}_{\bar{S}} = (x_0, x_1, x_2)$, $\{\boldsymbol{v}\}_{\bar{S}} = (y_0, y_1, y_2)$. Tečna v bodě b_1 o souřadnicích $\{b_1\}_{\bar{S}} = (1, 5\sqrt{2}, 4)$, tedy polára bodu $b_1 \in A_2(\widetilde{V}_3)$, má v homogenních souřadnicích rovnici $(\Phi^f(b_1))(\boldsymbol{u}) = f(b_1, \boldsymbol{u}) = 400x_0 - 80\sqrt{2}x_1 + 100x_2 = 0$. Přejdeme-li zpět k soustavě souřadnic S, tj. vydělíme celou rovnost x_0 a místo $\frac{x_1}{x_0}$ píšeme x a místo $\frac{x_2}{x_0}$ píšeme y, dostaneme rovnici tečny v bodě b_1, $\{b_1\}_S = (5\sqrt{2}, 4)$, ve tvaru $4\sqrt{2x} - 5y = 20$. Podobným způsobem dostaneme i rovnici tečny v bodě b_2, $\{b_2\}_S = (-5\sqrt{2}, 4)$, ve tvaru $4\sqrt{2}x + 5y = -20$.

2. Ke křivce v afinní rovině A_2 dané rovnicí $9x^2 + 16y^2 = 144$ veďme tečny z bodu o souřadnicích $(5, 9)$.

Řešení: V homogenní soustavě souřadnic $\bar{S}$ indukované S v projektivním rozšíření $\bar{A}_2(\bar{V}_3)$ jde o kvadriku vytvořenou kvadratickou formou $f_2(\boldsymbol{u}) = 144x_0^2 - 9x_1^2 - 16x_2^2$, přičemž hledáme tečny z bodu b o homogenních souřadnicích $(1, 5, 9)$. Je-li c bod dotyku tečny vedené ke kvadrice Q_{f_2} z bodu b, je tato tečna polára ϱ_c bodu c. Protože bod b leží na této tečně, $b \in \varrho_c$ je $c \in \varrho_b$ podle 23.8 (iii). Jinými slovy to znamená, že body dotyku hledaných tečen najdeme jako průsečíky poláry ϱ_b bodu b s kvadrikou. Protože polární bilineární forma f formy f_2 má vzhledem k $\bar{S}$ analytické vyjádření $f(\boldsymbol{u}, \boldsymbol{v})) = 144x_0y_0 - 9x_1y_1 - 16x_2y_2$, dostaneme dosazením souřadnic bodu b za vektor $\boldsymbol{v}$ rovnici poláry ϱ_b v homogenních souřadnicích ve tvaru $144x_0 - 45x_1 - 144x_2 = 0$ neboli po zkrácení $16x_0 - 5x_1 - 16x_2 = 0$. Spočtěme průsečíky poláry ϱ_b s kvadrikou. Vynásobíme-li rovnici kvadriky 16, dostaneme $2304x_0^2 - 144x_1^2 - 256x_2^2 = 0$. Z rovnice poláry dále máme $16x_2 = 16x_0 - 5x_1$, odkud dosazením do předchozí rovnice jest $2304x_0^2 - 144x_1^2 - (16x_0 - 5x_1)^2 = 2048x_0^2 + 160x_0x_1 - 169x_1^2 = 0$. Odtud pro $x = \frac{x_1}{x_0}$ dostáváme kvadratickou rovnici $169x^2 - 160x - 2048 = 0$, která má kořeny $\frac{80 \pm 144\sqrt{17}}{169}$. Položíme-li $x_0 = 169$, $x_1 = 80 \pm 144\sqrt{17}$ a dopočteme-li x_2 z rovnice $16x_2 = 16x_0 - 5x_1$, dostaneme průsečíky poláry ϱ_b s kvadrikou v homogenních souřadnicích $\{c_1\}_{\bar{S}} = (169, 80 - 144\sqrt{17}, 144 + 45\sqrt{17})$ a $\{c_2\}_{\bar{S}} = (169, 80 + 144\sqrt{17}, 144 - 45\sqrt{17})$. Tečny (poláry) v těchto bodech mají pak po zkrácení v homogenních souřadnicích rovnice $169x_0 - (5 - 9\sqrt{17})x_1 - (16 + 5\sqrt{17})x_2 = 0$ a $169x_0 - (5 + 9\sqrt{17})x_1 - (16 - 5\sqrt{17})x_2 = 0$. Přejdeme-li zpět k soustavě souřadnic S v $A_2(V_2)$, dostáváme rovnice tečen z bodu o souřadnicích $(5, 9)$ ve tvaru $(5 - 9\sqrt{17})x + (16 + 5\sqrt{17})y = 169$ a $(5 + 9\sqrt{17})x + (16 - 5\sqrt{17})y = 169$.

3. Ke křivce v afinní rovině $A_2(V_2)$ dané rovnicí $\frac{x^2}{25} + \frac{y^2}{10} = 1$ veďme tečny rovnoběžné s přímkou o rovnici $3x - 2y + 5 = 0$.

Řešení: Daná přímka má v homogenních souřadnicích rovnici $5x_0 + 3x_1 - 2x_2 = 0$, takže obsahuje nevlastní bod $\langle \boldsymbol{u} \rangle$, kde $\{\boldsymbol{u}\}_{\bar{S}} = (0, 2, 3)$. Protože hledané tečny mají být rovnoběžné s danou přímkou, musí mít týž směr, tj. musí procházet nevlastním bodem $\langle \boldsymbol{u} \rangle$. Další postup je tudíž stejný jako v předchozím příkladě. Polára bodu $\langle \boldsymbol{u} \rangle$ má rovnici $4x_1 + 15x_2 = 0$, protíná kvadriku o rovnici $-50x_0^2 + 2x_1^2 + 5x_2^2 = 0$ v bodech $\{b_1\}_{\bar{S}} = (53, -15\sqrt{265}, 4\sqrt{265})$, $\{b_2\}_{\bar{S}} =$

$(53, 15\sqrt{265}, -4\sqrt{265})$. Poláry v těchto bodech mají rovnice $-2650x_0 - 30\sqrt{265}x_1 + 20\sqrt{265}x_2 = 0$, $-2650x_0 + 30\sqrt{265}x_1 - 20\sqrt{265}x_2 = 0$ a přechodem zpět k soustavě souřadnic S dostáváme rovnice hledaných tečen ve tvaru $3x - 2y + \sqrt{265} = 0$, $3x - 2y - \sqrt{265} = 0$.

23.11. Věta. *Buď Q_{f_2} regulární kvadrika v projektivním prostoru $P_n(V_{n+1})$ a buď $P_{n-1}(V_n)$ nadrovina v P_n. Pak kvadrika $P_{n-1} \cap Q_{f_2}$ je regulární, právě když nadrovina P_{n-1} není tečnou nadrovinou kvadriky Q_{f_2}. Je-li P_{n-1} tečnou nadrovinou kvadriky Q_{f_2} s bodem dotyku $\langle \boldsymbol{u} \rangle$, pak $\langle \boldsymbol{u} \rangle$ je vrcholem kvadriky $P_{n-1} \cap Q_{f_2}$ v P_{n-1}.*

Důkaz. Buď $\langle \boldsymbol{u} \rangle$ pól nadroviny P_{n-1} vzhledem ke kvadrice Q_{f_2}. Podle věty 12.22 je kvadrika $P_{n-1} \cap Q_{f_2} = Q_{g_2}$, kde $g_2 = f_2|V_n$, regulární, právě když bod $\langle \boldsymbol{u} \rangle$ neleží na Q_{f_2}, tj. právě když P_{n-1} není tečná nadrovina kvadriky Q_{f_2}. Je-li $\langle \boldsymbol{u} \rangle$ bod dotyku tečné nadroviny P_{n-1} kvadriky Q_{f_2}, je $\langle \boldsymbol{u} \rangle$ vrcholem kvadriky Q_{g_2} opět podle věty 12.22. ■

23.12 Věta. *Buď Q_{f_2} regulární kvadrika v projektivním prostoru $P_n(V_{n+1})$ a buďte $\langle \boldsymbol{u} \rangle \in Q_{f_2}$, $\langle \boldsymbol{v} \rangle \in P_n$ dva různé body. Pak platí*

(i) přímka $\langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$ leží celá na kvadrice Q_{f_2}, právě když $\langle \boldsymbol{v} \rangle \in Q_{f_2}$ a body $\langle \boldsymbol{u} \rangle, \langle \boldsymbol{v} \rangle$ jsou konjugovány vzhledem ke Q_{f_2};

(ii) přímka $\langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$ protne kvadriku Q_{f_2} v jediném bodě, právě když $\langle \boldsymbol{v} \rangle \notin Q_{f_2}$ a body $\langle \boldsymbol{u} \rangle, \langle \boldsymbol{v} \rangle$ jsou konjugovány vzhledem ke Q_{f_2};

(iii) přímka $\langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$ protne kvadriku Q_{f_2} ve dvou různých, právě když body $\langle \boldsymbol{u} \rangle$ a $\langle \boldsymbol{v} \rangle$ nejsou konjugovány vzhledem ke Q_{f_2}.

Důkaz. Buď $\langle \boldsymbol{w} \rangle$ libovolný bod přímky $\langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$ různý od bodu $\langle \boldsymbol{u} \rangle$. Pak $\boldsymbol{w} = r\boldsymbol{u} + s\boldsymbol{v}$, kde $s \neq 0$, takže můžeme zvolit aritmetického zástupce $\boldsymbol{w}$ bodu $\langle \boldsymbol{w} \rangle$ tak, aby $\boldsymbol{w} = x\boldsymbol{u} + \boldsymbol{v}$, $x \in T$. Pak $f_2(\boldsymbol{w}) = x^2 f_2(\boldsymbol{u}) + 2xf(\boldsymbol{u}, \boldsymbol{v}) + f_2(\boldsymbol{v}) = 2xf(\boldsymbol{u}, \boldsymbol{v}) + f_2(\boldsymbol{v})$. Odtud vidíme, že každý bod přímky $\langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$ leží na Q_{f_2}, právě když $f(\boldsymbol{u}, \boldsymbol{v}) = f_2(\boldsymbol{v}) = 0$, tj. platí tvrzení (i). Přímka $\langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$ protne kvadriku Q_{f_2} pouze v bodě $\langle \boldsymbol{u} \rangle$, právě když $f(\boldsymbol{u}, \boldsymbol{v}) = 0$ a $f_2(\boldsymbol{v}) \neq 0$, tj. platí (ii). Nakonec přímka $\langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{u} \rangle$ protne kvadriku Q_{f_2} ve dvou různých bodech, právě když $f(\boldsymbol{u}, \boldsymbol{v}) \neq 0$, neboť v tomto případě má rovnice $2xf(\boldsymbol{u}, \boldsymbol{v}) + f_2(\boldsymbol{u}) = 0$ jediné řešení $x = \frac{-f_2(\boldsymbol{u})}{2f(\boldsymbol{u}, \boldsymbol{v})}$ a bod $\boldsymbol{w}$ s touto hodnotou parametru je druhým průsečíkem přímky $\langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$ s kvadrikou Q_{f_2}. ■

23.13. Poznámka. Předchozí věta řeší vzájemnou polohu přímky a kvadriky zcela obecně. Je-li kvadrika Q_{f_2} regulární, pak buďto projektivní přímka P_1 nemá s Q_{f_2} žádný společný bod, nebo s ním má alespoň jeden společný bod $\langle \boldsymbol{u} \rangle$. V tomto případě stačí použít předchozí větu. Nechť tedy Q_{f_2} je singulární kvadrika a nechť přímka P_1 obsahuje bod $\langle \boldsymbol{u} \rangle$ ležící ve vrcholu $P_k(V_{k+1})$ kvadriky Q_{f_2}. Pokud $\langle \boldsymbol{u} \rangle$ není jediným společným bodem přímky a kvadriky, buď $\langle \boldsymbol{v} \rangle \in Q_{f_2} \cap P_1$, $\langle \boldsymbol{v} \rangle \neq \langle \boldsymbol{u} \rangle$. Protože $\langle \boldsymbol{u} \rangle \in P_k$, je $f(\boldsymbol{u}, \boldsymbol{v}) = 0$ a z důkazu předchozí věty snadno plyne, že přímka P_1 leží celá na kvadrice. Zbývá poslední případ, totiž že přímka $P_1(V_2)$ neprotíná vrchol $P_k(V_{k+1})$ kvadriky Q_{f_2}. Pak ale $V_{k+1} \cap V_2 = 0$, takže je-li M báze V_{k+1} a N báze V_2, plyne z věty 9.25, že $M \cup N$ je lineárně nezávislá množina ve V_{n+1}. Podle věty 2.21 existuje lineárně nezávislá množina $L \subseteq V_{n+1}$ taková, že $M \cup N \cup L$ je bází V_{n+1}. Z věty o dimenzi spojení a průniku 2.23 plyne, že $V_{l+1} = \langle N \cup L \rangle$ je doplňkem $V_{k+1} = \langle M \rangle$ ve V_{n+1}, takže projektivní přímka P_1 leží v doplňku $P_l(V_{l+1})$ vrcholu

$P_k(V_{k+1})$ kvadriky Q_{f_2}. Podle věty 23.3 je kvadrika $Q_{f_2} \cap P_l$ regulární kvadrika v P_l, a tedy přímka P_1 buďto kvadriku Q_{f_2} neprotíná, nebo můžeme pro stanovení vzájemné polohy použít předchozí větu.

23.14. Poznámka. Přejděme nyní k otázce, do jaké míry určuje kvadrika příslušnou kvadratickou formu. Jinými slovy, budeme se zajímat o to, jak vypadají všechny kvadratické formy, které vytvářejí tutéž kvadriku. Při tomto zkoumání se omezíme na projektivní prostory nad algebraicky uzavřenými tělesy, k nimž patří těleso komplexních čísel, a samozřejmě nad tělesem čísel reálných. Vzhledem k již známým výsledkům týkajících se nulových množin lineárních a kvadratických forem (věty 11.14 a 22.11) můžeme očekávat, že kvadratické formy vytvářející tutéž kvadriku se budou lišit pouze násobkem. K důkazu těchto tvrzení budeme potřebovat některé další poznatky o vzájemné poloze přímky a kvadriky.

23.15. Věta. *Buď Q_{f_2} kvadrika v projektivním prostoru $P_n(V_{n+1})$, $n \geq 1$, nad algebraicky uzavřeným tělesem (speciálně v komplexním projektivním prostoru). Pak každá přímka $P_1 \subseteq P_n$ protíná kvadriku Q_{f_2} alespoň v jednom bodě.*

Důkaz. Buď $P_1 = \langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$ a předpokládejme, že bod $\langle \boldsymbol{u} \rangle$ neleží na kvadrice Q_{f_2}. Je-li $\langle \boldsymbol{w} \rangle \in P_1$, $\langle \boldsymbol{w} \rangle \neq \langle \boldsymbol{u} \rangle$, můžeme zvolit aritmetické zástupce bodů $\langle \boldsymbol{u} \rangle$, $\langle \boldsymbol{v} \rangle$ tak, aby $\boldsymbol{w} = x\boldsymbol{u} + \boldsymbol{v}$ pro nějaké $x \in T$. Pak máme $f_2(\boldsymbol{w}) = x^2 f_2(\boldsymbol{u}) + 2xf(\boldsymbol{u}, \boldsymbol{v}) + f_2(\boldsymbol{v})$. Protože $f_2(\boldsymbol{u}) \neq 0$ a těleso T je algebraicky uzavřené, má kvadratická rovnice $f_2(\boldsymbol{w}) = 0$ alespoň jeden kořen x, který určuje průsečík $\langle \boldsymbol{w} \rangle$ přímky P_1 s kvadrikou Q_{f_2}. ■

23.16. Věta. *Buď Q_{f_2} kvadrika v reálném projektivním prostoru $P_n(V_{n+1})$. Jestliže $\langle \boldsymbol{u} \rangle$ a $\langle \boldsymbol{v} \rangle$ jsou dva body z P_n takové, že čísla $f_2(\boldsymbol{u})$ a $f_2(\boldsymbol{v})$ mají opačná znaménka, pak přímka $P_1 = \langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$ protíná kvadriku Q_{f_2} ve dvou různých bodech.*

Důkaz. Buď $\langle \boldsymbol{w} \rangle \neq \langle \boldsymbol{u} \rangle$ libovolný bod přímky P_1. Aritmetické zástupce bodů $\langle \boldsymbol{w} \rangle$, $\langle \boldsymbol{v} \rangle$ a $\langle \boldsymbol{u} \rangle$ můžeme zvolit tak, aby $\boldsymbol{w} = x\boldsymbol{u} + \boldsymbol{v}$. Pak ale $f_2(\boldsymbol{w}) = x^2 f_2(\boldsymbol{u}) + 2xf(\boldsymbol{u}, \boldsymbol{v}) + f_2(\boldsymbol{v})$. Kvadratická rovnice $f_2(\boldsymbol{w}) = 0$ má diskriminant $D = 4((f(\boldsymbol{u}, \boldsymbol{v}))^2 - f_2(\boldsymbol{u}) f_2(\boldsymbol{v}))$. Protože součin $f_2(\boldsymbol{u}) f_2(\boldsymbol{v})$ je podle předpokladu záporný, je $D > 0$, rovnice má dva různé reálné kořeny, které určují dva různé průsečíky přímky P_1 s kvadrikou Q_{f_2}. ■

23.17. Věta. *Nechť Q_{f_2}, Q_{g_2} jsou dvě regulární kvadriky v projektivním prostoru $P_n(V_{n+1})$ takové, že pro každý bod $\langle \boldsymbol{u} \rangle \in P_n$ je polární nadrovina bodu $\langle \boldsymbol{u} \rangle$ vzhledem ke Q_{f_2} totožná s polární nadrovinou bodu $\langle \boldsymbol{u} \rangle$ vzhledem ke Q_{g_2}. Pak existuje prvek $0 \neq r \in T$ takový, že $g_2 = rf_2$.*

Důkaz. Nechť f a g jsou polární bilineární formy kvadratických forem f_2 a g_2. Je-li $\langle \boldsymbol{u} \rangle \in P_n$ libovolný, je podle poznámky 23.7 $\operatorname{Ker} \Phi^f(\boldsymbol{u})$ aritmetický základ polární nadroviny bodu $\langle \boldsymbol{u} \rangle$ vzhledem ke Q_{f_2} a $\operatorname{Ker} \Phi^g(\boldsymbol{u})$ aritmetický základ polární nadroviny bodu $\langle \boldsymbol{u} \rangle$ vzhledem ke Q_{g_2}. Podle předpokladu je $\operatorname{Ker} \Phi^f(\boldsymbol{u}) = \operatorname{Ker} \Phi^g(\boldsymbol{u})$ a stačí použít větu 22.11. ■

23.18. Věta. *Buďte $\langle \boldsymbol{u}_1 \rangle$, $\langle \boldsymbol{u}_2 \rangle$ dva různé body regulární kvadriky Q_{f_2} v projektivním prostoru $P_n(V_{n+1})$ nad tělesem T charakteristiky různé od 2. Jsou-li $\langle \boldsymbol{v} \rangle$, $\langle \boldsymbol{w} \rangle$ dva různé body přímky $P_1 = \langle \boldsymbol{u}_1 \rangle \vee \langle \boldsymbol{u}_2 \rangle$, která neleží na kvadrice Q_{f_2}, pak body*

$\langle v\rangle$ a $\langle w\rangle$ jsou konjugovány vzhledem ke Q_{f_2}, právě když $(u_1, u_2, v, w) = -1$, tj. právě když čtveřice $\langle u_1\rangle$, $\langle u_2\rangle$, $\langle v\rangle$, $\langle w\rangle$ je harmonická.

Důkaz. Zvolme aritmetické zástupce bodů $\langle u_1\rangle$, $\langle u_2\rangle$, $\langle v\rangle$, $\langle w\rangle$, tak, aby $v = u_1 + u_2$, $w = \lambda u_1 + u_2$. Tato volba je umožněna tím, že všechny čtyři body jsou navzájem různé, neboť $\langle u_1\rangle$, $\langle u_2\rangle$ leží na Q_{f_2} a $\langle v\rangle$, $\langle w\rangle$ nikoliv. Je-li nyní $(u_1, u_2, v, w) = \lambda = -1$, je $f(v, w) = f(u_1+u_2, \lambda u_1+u_2) = \lambda f_2(u_1)+\lambda f(u_2, u_1)+f(u_1, u_2)+f_2(u_2) = 0$ a body $\langle v\rangle$, $\langle w\rangle$ jsou konjugovány vzhledem ke Q_{f_2}. Předpokládejme tedy naopak, že body $\langle v\rangle$, $\langle w\rangle$ jsou konjugovány vzhledem ke Q_{f_2}. Protože přímka P_1 obsahuje podle předpokladu alespoň dva body kvadriky Q_{f_2}, totiž $\langle u_1\rangle$ a $\langle u_2\rangle$, a neleží celá na Q_{f_2}, nejsou body $\langle u_1\rangle$ a $\langle u_2\rangle$ konjugovány vzhledem ke Q_{f_2} podle věty 23.12. Pak ale z $f(v, w) = \lambda f(u_2, u_1) + f(u_1, u_2) = (\lambda + 1) f(u_1, u_2) = 0$ plyne $(u_1, u_2, v, w) = \lambda = -1$. ∎

23.19. Věta. *Buď Q_{f_2} regulární kvadrika v projektivním prostoru $P_n(V_{n+1})$ nad algebraicky uzavřeným tělesem T charakteristiky různé od 2 (speciálně v komplexním projektivním prostoru) a buď $\langle u\rangle \in P_n$ libovolný bod. Pak geometrický bod $\langle v\rangle \in P_n$ leží v polární nadrovině $\varrho_{\langle u\rangle}$ bodu $\langle u\rangle$, právě když nastane jedna z následujících čtyř možností:*

(a) $\langle u\rangle \in Q_{f_2}$ a přímka $\langle u\rangle \vee \langle v\rangle$ má s Q_{f_2} jediný společný bod $\langle u\rangle$;

(b) $\langle u\rangle \in Q_{f_2}$ a přímka $\langle u\rangle \vee \langle v\rangle$ leží celá na kvadrice Q_{f_2};

(c) $\langle u\rangle \notin Q_{f_2}$ a přímka $\langle u\rangle \vee \langle v\rangle$ má s Q_{f_2} jediný společný bod $\langle v\rangle$;

(d) $\langle u\rangle \notin Q_{f_2}$, přímka $\langle u\rangle \vee \langle v\rangle$ protíná kvadriku Q_{f_2} ve dvou bodech $\langle w_1\rangle$, $\langle w_2\rangle$ a $(w_1, w_2, u, v) = -1$.

Důkaz. Nejprve ukažme, že podmínky (a)–(d) jsou postačující. Platí-li (a) nebo (c), jsou body $\langle u\rangle$, $\langle v\rangle$ konjugovány vzhledem ke Q_{f_2} podle věty 23.12 (ii), je-li splněno (b), platí totéž podle věty 23.12 (i). V případě podmínky (d) stačí použít větu 23.18.

Předpokládejme tedy naopak, že bod $\langle v\rangle$ leží v polární nadrovině $\varrho_{\langle u\rangle}$ bodu $\langle u\rangle$, tj. že body $\langle u\rangle$, $\langle v\rangle$ jsou konjugovány vzhledem ke kvadrice Q_{f_2}. Jestliže $\langle u\rangle \in Q_{f_2}$, pak podle věty 23.12 je splněna buď podmínka (a), nebo podmínka (b). Jestliže $\langle u\rangle \notin Q_{f_2}$, pak přímka $\langle u\rangle \vee \langle v\rangle$ protíná podle věty 23.15 kvadriku Q_{f_2} alespoň v jednom bodě. Je-li $\langle w\rangle$ jediný průsečík této přímky s Q_{f_2}, pak pro $\langle w\rangle = \langle v\rangle$ je podle věty 23.12 splněna podmínka (c). V případě, že $\langle w\rangle \neq \langle v\rangle$, můžeme volit aritmetické zástupce bodů $\langle u\rangle$, $\langle v\rangle$ a $\langle w\rangle$ tak, že $u = v + w$. Protože body $\langle u\rangle$, $\langle w\rangle$ jsou podle věty 23.12 konjugovány vzhledem ke Q_{f_2}, je $0 \neq f_2(u) = f(u, v + w) = f(u, v)$, což je spor s konjugovaností bodů $\langle u\rangle$ a $\langle v\rangle$. Zbývá tedy poslední možnost, kdy kvadrika Q_{f_2} protíná přímku $\langle u\rangle \vee \langle v\rangle$ ve dvou různých bodech $\langle w_1\rangle$, $\langle w_2\rangle$. Přitom $\langle w_1\rangle \neq \langle v\rangle \neq \langle w_2\rangle$, neboť v opačném případě by body $\langle u\rangle$ a $\langle v\rangle$ nebyly podle věty 23.12 konjugovány vzhledem ke Q_{f_2}. Pak je ale podle věty 23.18 splněna podmínka (d) a důkaz je dokončen. ∎

23.20. Věta. *Buď Q_{f_2} regulární kvadrika v reálném projektivním prostoru $P_n(V_{n+1})$ a buď $\langle u\rangle \in P_n$ libovolný geometrický bod. Pak platí*

(i) Je-li $\langle u\rangle \in Q_{f_2}$, pak bod $\langle v\rangle \in P_n$ leží v polární nadrovině $\varrho_{\langle u\rangle}$ bodu $\langle u\rangle$, právě když přímka $\langle u\rangle \vee \langle v\rangle$ buď leží celá na Q_{f_2}, nebo má s Q_{f_2} jediný společný bod $\langle u\rangle$;

(ii) je-li $\langle u \rangle \notin Q_{f_2}$ a jsou-li body $\langle w_1 \rangle$, $\langle w_2 \rangle$, $\langle w \rangle \in P_n$ takové, že $\langle u \rangle$, $\langle v \rangle \in \langle w_1 \rangle \vee \langle w_2 \rangle$, body $\langle w_1 \rangle$, $\langle w_2 \rangle$ jsou jedinými průsečíky přímky $\langle w_1 \rangle \vee \langle w_2 \rangle$ s kvadrikou Q_{f_2} a $(w_1, w_2, u, v) = -1$, pak $\varrho_{\langle u \rangle} = (\varrho_{\langle w_1 \rangle} \cap \varrho_{\langle w_2 \rangle}) \vee \langle v \rangle$ je polární nadrovina bodu $\langle u \rangle$ vzhledem ke kvadrice Q_{f_2}.

Důkaz. (i) Je-li $\langle u \rangle \in Q_{f_2}$, jsou body $\langle u \rangle$ a $\langle v \rangle$ podle věty 23.12 konjugovány vzhledem ke Q_{f_2}, právě když přímka $\langle u \rangle \vee \langle v \rangle$ buď leží celá na Q_{f_2}, nebo má s Q_{f_2} jediný společný bod $\langle u \rangle$.

(ii) Nechť tedy $\langle u \rangle \notin Q_{f_2}$. Podle věty 23.12 nejsou body $\langle w_1 \rangle$ a $\langle w_2 \rangle$ konjugovány vzhledem ke Q_{f_2}, takže $\langle w_1 \rangle \notin \varrho_{\langle w_2 \rangle}$, nadroviny $\varrho_{\langle w_1 \rangle}$ a $\varrho_{\langle w_2 \rangle}$ jsou s ohledem na skutečnost, že $\langle w_1 \rangle \in \varrho_{\langle w_1 \rangle}$ navzájem různé, a tedy $\dim(\varrho_{\langle w_1 \rangle} \cap \varrho_{\langle w_2 \rangle}) = n - 2$ podle věty 21.6 (iii). Označíme-li nyní $P_{n-2} = \varrho_{\langle w_1 \rangle} \cap \varrho_{\langle w_2 \rangle}$, je zřejmě bod $\langle w_1 \rangle$ konjugován s každým bodem z P_{n-2} a stejně je i bod $\langle w_2 \rangle$ konjugován s každým bodem z P_{n-2}. Pak ale každý bod přímky $\langle w_1 \rangle \vee \langle w_2 \rangle$, speciálně bod $\langle u \rangle$, je konjugován s každým bodem z P_{n-2}, takže $P_{n-2} \subseteq \varrho_{\langle u \rangle}$. Protože bod $\langle v \rangle$ je podle věty 23.18 konjugován s bodem $\langle u \rangle$, je zřejmé, že $P_{n-2} \vee \langle v \rangle \subseteq \varrho_{\langle u \rangle}$. K dokončení důkazu je zapotřebí si pouze uvědomit, že $\langle v \rangle \notin P_{n-2}$, neboť potom $P_{n-2} \vee \langle v \rangle$ je nadrovina v P_n podle věty 21.6, a tedy $P_{n-2} \vee \langle v \rangle = \varrho_{\langle u \rangle}$. Avšak podle věty 23.12 bod $\langle v \rangle$ není konjugován s bodem $\langle w_1 \rangle$ vzhledem ke Q_{f_2}, takže $\langle v \rangle \notin \varrho_{\langle w_1 \rangle}$, a tedy $\langle v \rangle \notin P_{n-2}$. ■

23.21. Věta. *Buďte Q_{f_2} a Q_{g_2} dvě kvadriky v projektivním prostoru $P_n(V_{n+1})$ nad algebraicky uzavřeným tělesem T charakteristiky různé od 2 (speciálně v komplexním projektivním prostoru). Pak $Q_{f_2} = Q_{g_2}$, právě když $g_2 = r f_2$ pro nějaký nenulový prvek r tělesa T.*

Důkaz. Je-li $g_2 = r f_2$, pak zřejmě $Q_{f_2} = Q_{g_2}$. Předpokládejme tedy naopak, že $Q_{f_2} = Q_{g_2}$, a buď nejprve tato kvadrika regulární. S ohledem na větu 23.17 potřebujeme popsat polární nadrovinu každého bodu $\langle u \rangle \in P_n$ pomocí samotné množiny Q_{f_2}, tj. bez použití kvadratické formy f_2. Je-li $\langle u \rangle \in Q_{f_2}$, pak podle věty 23.19 sestává polární nadrovina $\varrho_{\langle u \rangle}$ právě ze všech bodů $\langle v \rangle \in P_n$ takových, že přímka $\langle u \rangle \vee \langle v \rangle$ buď leží celá na kvadrice Q_{f_2}, nebo s ní má jediný společný bod $\langle u \rangle$. Jestliže $\langle u \rangle \notin Q_{f_2}$, pak podle téže věty polární nadrovina $\varrho_{\langle u \rangle}$ sestává právě z těch bodů $\langle v \rangle \in P_n$, pro něž přímka $\langle u \rangle \vee \langle v \rangle$ buď protíná kvadriku Q_{f_2} právě v bodě $\langle v \rangle$, nebo ji protíná ve dvou různých bodech $\langle w_1 \rangle$, $\langle w_2 \rangle$, a platí $(w_1, w_2, u, v) = -1$. Aplikací věty 23.17 je tvrzení v případě regulární kvadriky dokázáno.

Buď tedy Q_{f_2} singulární kvadrika, buď $P_k(V_{k+1})$ její vrchol a $P_l(V_{l+1})$ buď doplněk vrcholu v prostoru $P_n(V_{n+1})$. Podle věty 23.3 je $Q_{f_2} \cap P_l$ regulární kvadrika v P_l, takže podle první části důkazu je $g_2(u) = r f_2(u)$ pro každý vektor $u \in V_{l+1}$ a vhodný nenulový prvek r z tělesa T. Je-li nyní $u \in V_{n+1}$ libovolný vektor, lze u podle věty 9.25 psát dokonce jednoznačně ve tvaru $u = u_1 + u_2$, kde $u_1 \in V_{k+1}$, $u_2 \in V_{l+1}$. Pak ale podle definice vrcholu 12.8 máme $g_2(u) = g_2(u_1 + u_2) = g_2(u_1) + 2g(u_1, u_2) + g_2(u_2) = r f_2(u_2) = r f_2(u)$, a tedy $g_2 = r f_2$, což jsme chtěli dokázat. ■

23.22. Věta. *Nechť Q_{f_2} a Q_{g_2} jsou dvě kvadriky v reálném projektivním prostoru $P_n(V_{n+1})$, které obsahují alespoň jeden bod neležící ve vrcholu. Pak $Q_{f_2} = Q_{g_2}$, právě když existuje nenulové reálné číslo r takové, že $g_2 = r f_2$.*

Důkaz. Podobně jako v předchozí větě stačí zřejmě dokázat, že z rovnosti $Q_{f_2} = Q_{g_2}$ plyne existence nenulového reálného čísla r takového, že $g_2 = rf_2$. Buď nejprve Q_{f_2} regulární kvadrika. Podle věty 23.20 je polární nadrovina $\varrho_{\langle u \rangle}$ libovolného bodu $\langle \boldsymbol{u} \rangle \in P_n$ určena pomocí množiny Q_{f_2} bez použití formy f_2. Pak ale podle věty 23.17 je $g_2 = rf_2$ pro nějaké $0 \neq r \in R$.

Je-li Q_{f_2} singulární kvadrika, buď $P_k(V_{k+1})$ její vrchol a $P_l(V_{l+1})$ buď doplněk vrcholu P_k v prostoru P_n. Stejně jako v důkazu předchozí věty je podle věty 23.3 kvadrika $Q_{f_2} \cap P_l$ regulární kvadrika v P_l, takže $g_2 = rf_2$ na V_{l+1}. Nyní libovolný vektor $\boldsymbol{u} \in V_{n+1}$ lze psát ve tvaru $\boldsymbol{u} = \boldsymbol{u}_1 + \boldsymbol{u}_2$, $\boldsymbol{u}_1 \in V_{k+1}$, $\boldsymbol{u}_2 \in V_{l+1}$, takže $g_2(\boldsymbol{u}) = g_2(\boldsymbol{u}_1 + \boldsymbol{u}_2) = g_2(\boldsymbol{u}_2) = rf_2(\boldsymbol{u}_2) = rf_2(\boldsymbol{u})$ a jsme hotovi. ∎

23.23. Poznámka. V právě dokázané větě jsme viděli, že v reálném vektorovém prostoru $P_n(V_{n+1})$ každá kvadrika obsahující alespoň jeden bod mimo vrchol určuje vytvářející kvadratickou formu až na nenulový násobek jednoznačně. Velice snadno se nahlédne, že pokud podmínka existence bodu mimo vrchol není splněna, tvrzení neplatí. Jsou-li totiž $f_2(\boldsymbol{u}) = x_0^2 + x_1^2 + x_2^2$ a $g_2(\boldsymbol{u}) = x_0^2 + 2x_1^2 + x_2^2$ analytická vyjádření kvadratických forem f_2 a g_2 vzhledem ke kanonické bázi aritmetického vektorového R^3, je $Q_{f_2} = Q_{g_2} = \emptyset$, avšak forma g_2 není násobkem formy f_2. Mohlo by se tedy na první pohled zdát, že věta 23.21 řeší studovanou problematiku nad algebraicky uzavřeným tělesem charakteristiky různé od 2 daleko obecněji než věta 23.22 nad tělesem reálných čísel. Ve skutečnosti se však obě tvrzení liší jen nepatrně. Je-li totiž ve větě 23.21 Q_{f_2} kvadrika, jejíž vrchol není nadrovina, pak doplněk P_l vrcholu kvadriky Q_{f_2} má dimenzi alespoň 1, takže kvadrika $Q_{f_2} \cap P_l$ obsahuje podle věty 23.15 alespoň jeden bod, a kvadrika Q_{f_2} obsahuje tudíž alespoň jeden bod neležící ve vrcholu. Zbývá tedy jediný případ, kdy vrchol kvadriky Q_{f_2} je nadrovina $P_{n-1}(V_n)$ v $P_n(V_{n+1})$. Je-li $\langle \boldsymbol{u} \rangle \in P_n \setminus P_{n-1}$ libovolný bod, je $\langle \boldsymbol{u} \rangle \notin Q_{f_2}$, neboť v opačném případě bychom podle věty 23.3 měli $Q_{f_2} = Q_{g_2} = P_n$, tedy $g_2 = f_2 = 0$ a vrcholem kvadriky by byl celý prostor P_n. Opětovným použitím věty 23.3 tedy vidíme, že $Q_{f_2} = Q_{g_2} = P_{n-1}$, a označíme-li $r = \frac{f_2(\boldsymbol{u})}{g_2(\boldsymbol{u})} \neq 0$, pak pro každý vektor $\boldsymbol{v} \in V_{n+1}$ platí $\boldsymbol{v} = s\boldsymbol{u} + \boldsymbol{w}$ pro nějaké $s \in T$ a nějaké $\boldsymbol{w} \in V_n$, a tedy $g_2(\boldsymbol{v}) = g_2(r\boldsymbol{u} + \boldsymbol{w}) = s^2 g_2(\boldsymbol{u}) = rs^2 f_2(\boldsymbol{u}) = rf_2(s\boldsymbol{u} + \boldsymbol{w})$ a $g_2 = rf_2$.

23.24. Definice. Řekněme, že dvě kvadriky Q_{f_2} a Q_{g_2} jsou *téhož projektivního typu*, jestliže existuje kolineace K prostoru P_n převádějící kvadriku Q_{f_2} na kvadriku Q_{g_2}.

23.25. Věta. *Buď $P_n(V_{n+1})$ projektivní prostor nad algebraicky uzavřeným tělesem T charakteristiky různé od 2 (speciálně nad tělesem komplexních čísel K). Dvě kvadriky Q_{f_2} a Q_{g_2} jsou téhož projektivního typu, právě když jejich vrcholy mají stejnou dimenzi.*

Důkaz. Předpokládejme nejprve, že kvadriky Q_{f_2} a Q_{g_2} jsou téhož projektivního typu. Existuje tedy kolineace $K = \langle h \rangle$ prostoru P_n vytvořená automorfismem $h : V_{n+1} \to V_{n+1}$ taková, že $K(Q_{f_2}) = Q_{g_2}$. To znamená, že pro nulové množiny kvadratických forem f_2 a g_2 je $h(Q(f_2)) = Q(g_2)$ neboli $\boldsymbol{u} \in Q(f_2)$, právě když $h(\boldsymbol{u}) \in Q(g_2)$. Ve větě 22.8 bylo definována kvadratická forma $h(f_2)$ na V_{n+1} předpisem $h(f_2)(h(\boldsymbol{u})) = f_2(\boldsymbol{u})$ pro každé $\boldsymbol{u} \in V_{n+1}$. Celkem tedy vidíme, že $g_2(h(\boldsymbol{u})) = 0$, právě když $f_2(\boldsymbol{u}) = h(f_2)(h(\boldsymbol{u})) = 0$, tj. $\langle h(\boldsymbol{u}) \rangle \in Q_{f_2}$, právě když $\langle h(\boldsymbol{u}) \rangle \in Q_{h(f_2)}$, takže $Q_{f_2} = Q_{h(f_2)}$ vzhledem k tomu, že h je automorfismus prostoru V_{n+1}. Podle věty 23.21 existuje prvek $0 \neq r \in T$ takový, že $h(f_2) = rg_2$. Pak ale formy g_2 a $h(f_2)$ mají stejnou nulitu, a tedy podle věty 22.8 i formy f_2 a g_2 mají stejnou nulitu.

Nechť tedy naopak vrcholy kvadrik Q_{f_2} a Q_{g_2} mají stejnou dimenzi k, tj. nechť $n(f_2) = n(g_2) = k+1$. Buď nyní $\{\boldsymbol{u}_0, \boldsymbol{u}_1, \dots, \boldsymbol{u}_n\}$ polární báze formy f_2 taková, že $f_2(\boldsymbol{u}_0) = f_2(\boldsymbol{u}_1) = \dots = f_2(\boldsymbol{u}_k) = 0$ a $\{\boldsymbol{v}_0, \boldsymbol{v}_1, \dots, \boldsymbol{v}_n\}$ polární báze formy g_2 taková, že $g_2(\boldsymbol{v}_0) = g_2(\boldsymbol{v}_1) = \dots = g_2(\boldsymbol{v}_k) = 0$. Podle věty 13.8 je $V(f_2) = \langle \boldsymbol{u}_0, \boldsymbol{u}_1, \dots, \boldsymbol{u}_k \rangle$, $V(g_2) = \langle \boldsymbol{v}_0, \boldsymbol{v}_1, \dots, \boldsymbol{v}_k \rangle$ a $f_2(\boldsymbol{u}_i) \neq 0 \neq g_2(\boldsymbol{v}_i)$ pro všechna $i = k+1, \dots, n$. Podle věty 9.22 existuje právě jeden automorfismus h prostoru V_{n+1} takový, že $h(\boldsymbol{u}_i) = \boldsymbol{v}_i$ pro každé $i = 0, 1, \dots, k$ a $h(\boldsymbol{u}_i) = \sqrt{\frac{f_2(\boldsymbol{u}_i)}{g_2(\boldsymbol{v}_i)}}\boldsymbol{v}_i$ pro všechna $i = k+1, \dots, n$. Je-li nyní $\boldsymbol{u} \in V_{n+1}$ libovolný vektor, je $\boldsymbol{u} = \sum_{i=1}^n x_i \boldsymbol{u}_i$ a platí $g_2(h(\boldsymbol{u})) = g_2(h(\sum_{i=0}^n x_i \boldsymbol{u}_i)) = g_2(\sum_{i=0}^n x_i h(\boldsymbol{u}_i)) = g_2(\sum_{i=0}^k x_i \boldsymbol{v}_i + \sum_{i=k+1}^n x_i \sqrt{\frac{f_2(\boldsymbol{u}_i)}{g_2(\boldsymbol{v}_i)}} v_i) = \sum_{i=k+1}^n x_i^2 f_2(\boldsymbol{u}_i) = \sum_{i=0}^n x_i^2 f_2(\boldsymbol{u}_i) = f_2(\sum_{i=0}^n x_i \boldsymbol{u}_i) = f_2(\boldsymbol{u})$. Odtud je patrné, že $\langle \boldsymbol{u} \rangle \in Q_{f_2}$, právě když $\langle h(\boldsymbol{u}) \rangle \in Q_{g_2}$. Jinými slovy kolineace $K = \langle h \rangle$ vytvořená automorfismem h prostoru V_{n+1} převádí kvadriku Q_{f_2} na kvadriku Q_{g_2}, a kvadriky Q_{f_2} a Q_{g_2} jsou tudíž téhož projektivního typu. ■

23.26. Věta. *Dvě kvadriky Q_{f_2} a Q_{g_2} v reálném projektivním prostoru $P_n(V_{n+1})$ jsou téhož projektivního typu, právě když jejich vrcholy mají stejnou dimenzi a* $\min(p(f_2), q(f_2)) = \min(p(g_2), q(g_2))$.

Důkaz. Předpokládejme nejprve, že kvadriky Q_{f_2} a Q_{g_2} jsou téhož projektivního typu a buď $K = \langle h \rangle$ kolineace převádějící kvadriku Q_{f_2} na kvadriku Q_{g_2}. Protože $(h(f_2))(h(\boldsymbol{u})) = f_2(\boldsymbol{u}) = 0$, právě když $g_2(h(\boldsymbol{u})) = 0$, vytvářejí formy $h(f_2)$ a g_2 tutéž kvadriku v P_n. Jestliže kvadrika Q_{f_2} obsahuje alespoň jeden bod neležící ve vrcholu, pak podle věty 23.22 existuje nenulové reálné číslo r takové, že $g_2 = rh(f_2)$. Podle věty 22.10 mají formy f_2 a $h(f_2)$ stejnou signaturu $\langle k+1, p, q \rangle$, $k \geq -1$. Je-li nyní $r > 0$, má forma g_2 tutéž signaturu $\langle k+1, p, q \rangle$, zatímco pro $r < 0$ má g_2 zřejmě signaturu $\langle k+1, q, p \rangle$, takže v každém případě mají obě formy f_2 a g_2 stejnou nulitu a $\min(p(f_2), q(f_2)) = \min(p(g_2), q(g_2))$.

Jestliže kvadrika Q_{g_2} neobsahuje žádný bod neležící na vrcholu, pak Q_{g_2} splývá se svým vrcholem $P_k(V_{k+1})$. Je-li $P_l(V_{l+1})$ doplněk vrcholu P_k v prostoru P_n, je $Q_{f_2} \cap P_l$ regulární kvadrika v P_l podle věty 23.3 a neobsahuje žádný bod. Pak ale z věty 22.4 vyplývá, že $\min(p(g_2), q(g_2)) = 0$. Protože formy g_2 a $h(f_2)$ vytvářejí tutéž kvadriku, mají tyto formy stejnou nulitu a $\min(p(h(f_2)), q(h(f_2))) = 0$. Jelikož formy f_2 a $h(f_2)$ mají podle věty 22.10 stejnou signaturu, jsme i v tomto případě hotovi.

Předpokládejme tedy naopak, že $n(f_2) = n(g_2)$ a $\min(p(f_2), q(f_2)) = \min(p(g_2), q(g_2))$. Protože formy g_2 a $-g_2$ určují tutéž kvadriku, můžeme bez újmy na obecnosti předpokládat, že formy f_2 a g_2 mají stejnou signaturu $\langle k+1, p, q \rangle$. Existuje tedy polární báze $\langle \boldsymbol{u}_0, \boldsymbol{u}_1, \dots, \boldsymbol{u}_n \rangle$ formy f_2 taková, že $f_2(\boldsymbol{u}_i) = 0$ pro $i = 0, 1, \dots, k$, $f_2(\boldsymbol{u}_i) > 0$ pro $i = k+1, \dots, k+p$ a $f_2(\boldsymbol{u}_i) < 0$ pro $i = k+p+1, \dots, n$. Podobně existuje polární báze $\{\boldsymbol{v}_0, \boldsymbol{v}_1, \dots, \boldsymbol{v}_n\}$ formy g_2 taková, že $g_2(\boldsymbol{v}_i) = 0$ pro $i = 0, 1, \dots, k$, $g_2(\boldsymbol{v}_i) > 0$ pro $i = k+1, \dots, k+p$ a $g_2(\boldsymbol{v}_i) < 0$ pro $i = k+p+1, \dots, n$. Podle věty 9.22 existuje právě jeden automorfismus h prostoru V_{n+1} takový, že $h(\boldsymbol{u}_i) = \boldsymbol{v}_i$, $i = 0, 1, \dots, k$ a $h(\boldsymbol{u}_i) = \sqrt{\frac{f_2(\boldsymbol{u}_i)}{g_2(\boldsymbol{v}_i)}} v_i$, $i = k+1, \dots, n$. Uvědomme si, že výrazy $\sqrt{\frac{f_2(\boldsymbol{u}_i)}{g_2(\boldsymbol{v}_i)}}$ mají smysl, neboť pro $i = k+1, \dots, n$ mají obě čísla $f_2(\boldsymbol{u}_i)$ a $g_2(\boldsymbol{v}_i)$ vždy stejná znaménka. Nyní pro libovolný vektor $u \in V_{n+1}$ je $u = \sum_{i=0}^{n} x_i u_i$ a platí $g_2(h(u)) = g_2(h(\sum_{i=0}^{n} x_i u_i)) = g_2(\sum_{i=0}^{n} x_i h(u_i)) = g_2(\sum_{i=0}^{k} x_i v_i + \sum_{i=k+1}^{n} x_i \sqrt{\frac{f_2(u_i)}{g_2(v_i)}} v_i) = \sum_{i=k+1}^{n} x_i^2 f_2(u_i) = \sum_{i=0}^{n} x_i^2 f_2(u_i) = f_2(\sum_{i=0}^{n} x_i u_i) = f_2(u)$. Odtud je ihned patrné, že $\langle u \rangle \in Q_{f_2}$, právě když $\langle h(u) \rangle \in Q_{g_2}$, takže kolineace $K = \langle h \rangle$ vytvořená automorfismem h převádí kvadriku Q_{f_2} na kvadriku Q_{g_2}, a obě kvadriky jsou tudíž téhož projektivního typu. ■

23.27. Věta. *Nechť Q_{f_2}, Q_{g_2} jsou dvě kvadriky v reálném projektivním prostoru $P_n(V_{n+1})$. Pak kvadriky Q_{f_2} a Q_{g_2} jsou téhož projektivního typu, právě když jejich vrcholy mají stejnou dimenzi a když dimenze maximálního podprostoru prostoru P_n ležícího na Q_{f_2} je rovna dimenzi maximálního podprosotur P_n ležícího na Q_{g_2}.*

Důkaz. Podle vět 22.3 a 22.4 je dimenze maximálního podprostoru ležícího na kvadrice Q_{f_2} rovna $n(f_2) + \min(p(f_2), q(f_2)) - 1$, takže stačí použít předchozí větu. ■

23.28. Definice. Řekneme, že regulární kvadrika Q_{f_2} v reálném projektivním prostoru $P_n(V_{n+1})$ je *projektivního typu* l, je-li $l - 1$ dimenze maximální podprostoru prostoru P_n ležícího na kvadrice Q_{f_2}.

23.29. Poznámka. Z vět 22.3 a 22.4 ihned plyne, že regulární kvadrika Q_{f_2} v reálném projektivním prostoru $P_n(V_{n+1})$ je projektivního typu l, právě když $l = \min(p(f_2), q(f_2))$. To znamená, že pro n sudé existuje právě $\frac{n}{2} + 1$ a pro n liché právě $\frac{n+1}{2} + 1$ různých projektivních typů regulárních kvadrik. Vzhledem k tomu, že pod *projektivní vlastností* se rozumí každá vlastnost, která je invariantní vůči kolineacím, provedli jsme v předcházející části tzv. projektivní klasifikaci kvadrik. Viděli jsme, že v projektivním prostoru nad algebraicky uzavřeným tělesem charakteristiky různé od 2 jsou každé dvě regulární kvadriky téhož projektivního typu, takže projektivní klasifikace kvadrik je v tomto případě velmi chudá. V reálných projektivních prosotrech je, jak jsme viděli, tato klasifikace jen o málo bohatší.

V následujících dvou kapitolách budeme studovat kvadriky v afinních a euklidovských prostorech, přesněji řečeno v jejich projektivních rozšířeních. To nám umožní, podstatně jemnější klasifikace, totiž tzv. afinní klasifikaci, vztahující se k vlastnostem invariantním vzhledem k afinitám a tzv. metrickou klasifikaci v euklidovských prostorech, která se vztahuje ke skalárnímu součinu, a tedy k příslušné indukované metrice.

24.1. Definice. *Kvadrikou v afinním prostoru* $A_n(V_n)$ rozumíme kvadriku v projektivním rozšíření $\bar{A}_n(\overline{V}_{n+1})$.

24.2. Definice. Buď Q_{f_2} regulární kvadrika v afinním prostoru $A_n(V_n)$. Říkáme, že kvadrika Q_{f_2} je *středová*, jestliže nevlastní nadrovina N v $\bar{A}_n(\overline{V}_{n+1})$ není tečnou nadrovinou kvadriky Q_{f_2}. Pól nevlastní nadroviny se v tomto případě nazývá *střed kvadriky* Q_{f_2}. Jestliže nevlastní nadrovina N je tečnou nadrovinou kvadriky Q_{f_2}, pak říkáme, že Q_{f_2} je *nestředová kvadrika* nebo *paraboloid*. Bod dotyku nevlastní nadroviny s Q_{f_2}, tj. pól této nadroviny se nazývá *směr osy paraboloidu*.

24.3. Definice. Buď $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ soustava souřadnic v afinním prostoru $A_n(V_n)$ a buď $\bar{S}$ soustava souřadnic v $\bar{A}_n(\overline{V}_{n+1})$ indukovaná S (viz definice 21.26). Je-li $\sum_{i,j=0}^{n} a_{ij}x_i x_j$ analytické vyjádření kvadratické formy f_2 na $\overline{V}_{n+1}$ vzhledem k bázi $\bar{S}$ pak $a_{00}+\sum_{i=1}^{n}(a_{0i}+a_{i0})x_i+\sum_{i,j=1}^{n} a_{ij}x_i x_j = 0$ nazýváme *rovnicí kvadriky* Q_{f_2} vzhledem k soustavě souřadnic S. Přitom matice $\boldsymbol{A} = (a_{ij}) \in T_{n+1}$ se nazývá *matice kvadriky* Q_{f_2} vzhledem k S.

24.4. Věta. *Buď S soustava souřadnic v afinním prostoru $A_n(V_n)$. Buď dále $\boldsymbol{A} = (a_{ij})$ matice kvadriky Q_{f_2} vzhledem k S a buď $\boldsymbol{B} = (a_{ij})$, $i, j = 1, 2, \ldots, n$, matice vzniklá z matice $\boldsymbol{A}$ vynecháním prvního řádku a prvního sloupce. Pak platí:*
(i) kvadrika Q_{f_2} je regulární, právě když $\det \boldsymbol{A} \neq 0$*;*
(ii) kvadrika Q_{f_2} je středová, právě když $\det \boldsymbol{B} \neq 0$.

Důkaz. (i) Kvadrika Q_{f_2} je podle poznámky 12.12 regulární, právě když je regulární matice $\boldsymbol{A}$, takže stačí použít větu 8.4.

(ii) Kvadrika Q_{f_2} je středová, právě když nevlastní nadrovina N není tečnou nadrovinou Q_{f_2}. To je podle věty 23.11 ekvivalentní s tím, že kvadrika $Q_{f_2} \cap N$ je regulární kvadrika v N. Protože $x_0 = 0$ je zřejmě rovnice nevlastní nadroviny N, je $\boldsymbol{B}$ matice kvadriky $Q_{f_2} \cap N$ a stačí použít tvrzení (i). ■

24.5. Věta. *Buď Q_{f_2} regulární nestředová kvadrika v afinním prostoru $A_n(V_n)$ a buď $\langle \boldsymbol{u} \rangle$ směr osy této kvadriky. Pak pro každý bod $c \in A_n$ přímka $c + \langle \boldsymbol{u} \rangle$ protne kvadriku Q_{f_2} v jediném vlastním bodě.*

Důkaz. V projektivním rozšíření $\bar{A}_n(\overline{V}_{n+1})$ prostoru $A_n(V_n)$ přejde $c+\langle \boldsymbol{u} \rangle$ v přímku $c \vee \langle \boldsymbol{u} \rangle$. Podle předpokladu je $\langle \boldsymbol{u} \rangle \in Q_{f_2}$ a body $\langle \boldsymbol{u} \rangle, c$ nejsou konjugovány vzhledem k tomu, že polární nadrovina bodu $\langle \boldsymbol{u} \rangle$ je nevlastní nadrovina N. Podle věty 23.12 (iii) protne přímka $c \vee \langle \boldsymbol{u} \rangle$ kvadriku Q_{f_2} ve dvou různých bodech, z nichž jeden je nevlastní bod $\langle \boldsymbol{u} \rangle$. ■

24.6. Věta. *Buď Q_{f_2} regulární středová kvadrika v afinním prostoru $A_n(V_n)$ nad tělesem T, $\operatorname{char} T \neq 2$. Pak v $A_n(V_n)$ existuje soustava souřadnic $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$, vzhledem k níž má kvadrika Q_{f_2} rovnici*

$$\sum_{i=1}^{n} \varepsilon_i x_i^2 = 1,$$

kde ε_i jsou nenulové prvky z tělesa T.

Důkaz. Buď a střed kvadriky Q_{f_2} a buď $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ polární báze kvadratické formy $f_2|V_n$. Protože a je podle definice pólem nevlastní nadroviny N vzhledem ke Q_{f_2}, je množina $\bar{S} = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ polární bází formy f_2. Podle věty 13.8 je $f_2(a) = x_0^2 + \sum_{i=1}^n f_2(\boldsymbol{u}_i)x_i^2$ analytické vyjádření formy f_2 vzhledem k bázi $\bar{S}$, takže stačí položit $\varepsilon_i = \frac{-f_2(\boldsymbol{u}_i)}{f_2(a)}$, $i = 1, 2, \dots, n$. Přitom $f_2(a) \neq 0$ a $\varepsilon_i \neq 0$, neboť kvadrika Q_{f_2} je podle předpokladu regulární. ■

24.7. Věta. *Buď Q_{f_2} regulární nestředová kvadrika v afinním prostoru $A_n(V_n)$ nad tělesem T, $\operatorname{char} T \neq 2$. Pak v $A_n(V_n)$ existuje soustava souřadnic $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$, vzhledem k níž má kvadrika Q_{f_2} rovnici*

$$\sum_{i=1}^{n-1} \varepsilon_i x_i^2 = 2x_n,$$

kde ε_i, $i = 1, 2, \dots, n-1$, jsou nenulové prvky tělesa T.

Důkaz. Protože Q_{f_2} je nestředová, je podle věty 23.11 kvadrika $Q_{f_2} \cap N$ singulární a její vrchol je směr osy $\langle \boldsymbol{u}_n \rangle$ paraboloidu Q_{f_2}. Z důkazu věty 12.25 tedy plyne existence polární báze $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ restrikce $f|V_n$. Podle věty 12.15 je zobrazení $\Phi^f : V_{n+1} \to \widetilde{V}_{n+1}$ izomorfismus, takže podle věty 9.20 jsou lineární formy $\Phi^f(\boldsymbol{u}_1), \Phi^f(\boldsymbol{u}_2), \dots, \Phi^f(\boldsymbol{u}_{n-1})$ lineárně nezávislé. Pak ale podle věty 12.15 je $\dim \bigcap_{i=1}^{n-1} \operatorname{Ker} \Phi^f(\boldsymbol{u}_i) = 2$, takže $\bigcap_{i=1}^{n-1} \varrho_{\langle \boldsymbol{u}_i \rangle}$ je projektivní přímka v $\bar{A}_n(\overline{V}_{n+1})$. Je-li nyní $\langle \boldsymbol{v} \rangle$ nějaký nevlastní bod této přímky, je bod $\langle \boldsymbol{v} \rangle$ konjugován nejen se všemi body $\langle \boldsymbol{u}_i \rangle$, $i = 1, 2, \dots, n-1$, ale i s $\langle \boldsymbol{u}_n \rangle$, neboť $\langle \boldsymbol{u}_n \rangle$ je směrem osy paraboloidu Q_{f_2}, tj. pólem nevlastní nadroviny. To však znamená, že bod $\langle \boldsymbol{v} \rangle$ je pólem nevlastní nadroviny, takže $\langle \boldsymbol{v} \rangle = \langle \boldsymbol{u}_n \rangle$. Vidíme tedy, že přímka $\bigcap_{i=1}^{n-1} \varrho_{\langle \boldsymbol{u}_i \rangle}$ obsahuje jediný nevlastní bod $\langle \boldsymbol{u}_n \rangle$, takže podle věty 24.5 protíná kvadriku Q_{f_2} v jediném vlastním bodě a. Vezměme nyní soustavu souřadnic $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$. Protože bod a leží jednak na kvadrice Q_{f_2}, jednak na přímce $\bigcap_{i=1}^{n-1} \varrho_{\langle \boldsymbol{u}_i \rangle}$, je konjugován vzhledem ke Q_{f_2} jednak sám se sebou, jednak se všemi body $\langle \boldsymbol{u}_1 \rangle, \langle \boldsymbol{u}_2 \rangle, \dots, \langle \boldsymbol{u}_{n-1} \rangle$. To však znamená, že analytické vyjádření formy f_2 vzhledem k soustavě souřadnic $\bar{S}$ indukované S je tvaru $2x_0x_n f(a, \boldsymbol{u}_n) + \sum_{i=1}^{n-1} x_i^2 f_2(\boldsymbol{u}_i)$. K dokončení důkazu tedy stačí položit $\varepsilon_i = \frac{-f_2(\boldsymbol{u}_i)}{f(a, \boldsymbol{u}_n)}$, $i = 1, 2, \dots, n-1$, a uvědomit si, že $f_2(\boldsymbol{u}_i) \neq 0$ vzhledem k tomu, že $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ je polární báze formy $f_2|V_n$ s vrcholem $\langle \boldsymbol{u}_n \rangle$ a $f(a, \boldsymbol{u}_n) \neq 0$, neboť v opačném případě bod a byl pólem nevlastní nadroviny N, což není podle předpokladu možné. ■

24.8. Definice. Rovnice $\sum_{i=1}^n \varepsilon_i x_i^2 = 1$ z věty 24.6 se nazývá *kanonická rovnice regulární středové kvadriky Q_{f_2}* a rovnice $\sum_{i=1}^{n-1} \varepsilon_i x_i^2 = 2x_n$ z věty 24.7 se nazývá *kanonická rovnice regulárního paraboloidu Q_{f_2}*. U singulárních kvadrik rozumíme *kanonickou rovnicí* její rovnici vzhledem k nějaké polární bázi formy f_2.

V následujících třech odstavcích bude V_{f_2} značit vrchol kvadriky Q_{f_2} a všechna čísla ε_i v kanonických rovnicích jednotlivých kvadrik budou kladná reálná čísla.

24.9. Klasifikace kvadrik na reálné projektivní přímce.

Je-li Q_{f_2} regulární kvadrika na projektivní přímce P_1 projektivního typu 1, je forma f_2 indefinitní, takže nutně existují body $\langle \boldsymbol{u} \rangle, \langle \boldsymbol{v} \rangle \in P_1$ takové, že reálná čísla $f_2(\boldsymbol{u})$ a $f_2(\boldsymbol{v})$ mají opačná znaménka. Podle věty 23.12 pak přímka $P_1 = \langle \boldsymbol{u} \rangle \vee \langle \boldsymbol{v} \rangle$ protne kvadriku Q_{f_2} ve dvou různých bodech. Je-li Q_{f_2} singulární a jejím vrcholem je bod $\langle \boldsymbol{u} \rangle$, pak libovolný bod $\langle \boldsymbol{v} \rangle \neq \langle \boldsymbol{u} \rangle$ je doplňkem vrcholu $\langle \boldsymbol{u} \rangle$ v P_1. Přitom bod $\langle \boldsymbol{v} \rangle$ nemůže ležet na kvadrice Q_{f_2}, nebo v opačném případě by podle věty 23.3 platilo $Q_{f_2} = P_1$. Pomocí těchto úvah můžeme nyní provést úplnou klasifikaci kvadrik na reálné projektivní přímce P_1.

a) *Regulární kvadriky:*

α) projektivní typ 0: *prázdná množina:* $-\varepsilon_1 x_1^2 = 1$;
β) projektivní typ 1: *dva různé body:* $\varepsilon_1 x_1^2 = 1$.

b) *Singulární kvadriky:*

α) $\dim V_{f_2} = 0$: *jeden bod:* $\varepsilon_0 x_0^2 = 0$;
β) $\dim V_{f_2} = 1$: *celá přímka:* $(f_2 = 0)$.

24.10. Afinní klasifikace kvadrik v reálné afinní rovině $A_2(V_2)$.

Kvadriky v afinní rovině se nazývají *kuželosečky*. Je-li kvadrika Q_{f_2} singulární a její vrchol je bod, pak doplněk vrcholu v $\bar{A}_2(\bar{V}_3)$ je projektivní přímka P_1 a kvadrika $Q_{f_2} \cap P_1$ je regulární kvadrika v P_1 podle věty 23.3. Podle předchozího odstavce je $Q_{f_2} \cap P_1$ buď prázdná množina, nebo sestává ze dvou bodů. Pak ale, opět podle věty 23.3, kvadrika Q_{f_2} buď splývá s vrcholem, nebo je tvořena dvojicí přímek. Je-li kvadrika Q_{f_2} singulární a její vrchol je přímka P_1, potom doplněk vrcholu je libovolný bod $\langle \boldsymbol{v} \rangle \in \bar{A}_2 \setminus V_{f_2}$. Pak $\langle \boldsymbol{v} \rangle \notin Q_{f_2}$, neboť v opačném případě by podle věty 23.3 bylo $Q_{f_2} = \bar{A}_2$. V tomto případě tedy kvadrika splývá se svým vrcholem. Nyní můžeme přistoupit ke klasifikaci kuželoseček.

a) *Regulární kuželosečky:*

a$_1$) středové:
α) projektivní typ 0: *prázdná množina:* $-\varepsilon_1 x_1^2 - \varepsilon_2 x_2^2 = 1$;
β) projektivní typ 1:
β_1) $Q_{f_2} \cap N$ projektivního typu 0: *elipsa:* $\varepsilon_1 x_1^2 + \varepsilon_2 x_2^2 = 1$;
β_2) $Q_{f_2} \cap N$ projektivního typu 1: *hyperbola:* $\varepsilon_1 x_1^2 - \varepsilon_2 x_2^2 = 1$;

a$_2$) nestředové: *parabola:* $2x_2 = \varepsilon_1 x_1^2$.

b) *Singulární kuželosečky:*

α) $\dim V_{f_2} = 0$, doplněk vrcholu je přímka P_1:
α_1) $Q_{f_2} \cap P_1$ projektivního typu 0: *bod* (vrchol): $\varepsilon_0 x_0^2 + \varepsilon_1 x_1^2 = 0$;
α_2) $Q_{f_2} \cap P_1$ projektivního typu 1: *dvojice přímek* protínajících se ve vrcholu: $\varepsilon_0 x_0^2 - \varepsilon_1 x_1^2 = 0$;
α_{21}) vrchol je vlastní bod: 2 *různoběžky;*
α_{22}) vrchol je nevlastní bod: 2 *rovnoběžky;*
β) $\dim V_{f_2} = 1$: *přímka* (vrchol): $\varepsilon_0 x_0^2 = 0$;
γ) $\dim V_{f_2} = 2$: *celá rovina* $(f_2 = 0)$.

24.11. Afinní klasifikace kvadrik v reálném afinním prostoru $A_3(V_3)$.

Podobně jako v předchozích dvou odstavcích plyne klasifikace singulárních kvadrik v A_3 z těchto úvah: Je-li vrchol Q_{f_2} bod, je doplněk vrcholu rovina P_2 a kvadrika $Q_{f_2} \cap P_2$ je regulární podle věty 23.3. Klasifikace v bodě b α) pak plyne z této věty a z předchozího odstavce. Je-li vrchol Q_{f_2} přímka, je doplněk opět projektivní přímka a v bodě b β) se použije věta 23.3 a odstavec 24.9. Konečně v bodě b γ) je vrchol

Q_{f_2} rovina P_2, takže doplněk vrcholu je libovolný bod $\langle \boldsymbol{v} \rangle \in \bar{A}_3 \setminus P_2$, který neleží na Q_{f_2}, neboť v opačném případě věta 23.3 dává $Q_{f_2} = \bar{A}_3$.

a) *Regulární kvadriky:*

a$_1$) středové:

α) projektivní typ 0: *prázdná množina:* $\quad -\varepsilon_1 x_1^2 - \varepsilon_2 x_2^2 - \varepsilon_3 x_3^2 = 1$;

β) projektivní typ 1:

β_1) $Q_{f_2} \cap N$ proj. typu 0: *elipsoid* $\quad \varepsilon_1 x_1^2 + \varepsilon_2 x_2^2 + \varepsilon_3 x_3^2 = 1$;

β_2) $Q_{f_2} \cap N$ proj. typu 1: *dvojdílný hyperboloid:* $\quad \varepsilon_1 x_1^2 - \varepsilon_2 x_2^2 - \varepsilon_3 x_3^2 = 1$;

γ) proj. typ 2: *jednodílný (přímkový) hyperboloid:* $\quad \varepsilon_1 x_1^2 + \varepsilon_2 x_2^2 - \varepsilon_3 x_3^2 = 1$;

a$_2$) nestředové:

α) projektivní typ 1: *eliptický paraboloid:* $\quad \varepsilon_1 x_1^2 + \varepsilon_2 x_2^2 = 2x_3$;

β) projektivní typ 2: *hyperbolický paraboloid:* $\quad \varepsilon_1 x_1^2 - \varepsilon_2 x_2^2 = 2x_3$.

b) *Singulární kvadriky:*

α) $\dim V_{f_2} = 0$, doplněk vrcholu je rovina P_2:

α_1) $Q_{f_2} \cap P_2$ projektivního typu 0: *bod* (vrchol): $\quad \varepsilon_0 x_0^2 + \varepsilon_1 x_1^2 + \varepsilon_2 x_2^2 = 0$;

α_2) $Q_{f_2} \cap P_2$ projektivního typu 1: $\quad \varepsilon_0 x_0^2 + \varepsilon_1 x_1^2 - \varepsilon_2 x_2^2 = 0$;

α_{21}) V_{f_2} vlastní bod: *kuželová plocha;*

α_{22}) V_{f_2} nevlastní bod: *válcová plocha;*

β) $\dim V_{f_2} = 1$, doplněk vrcholu je přímka P_1:

β_1) $Q_{f_2} \cap P_1$ projektivního typu 0: *přímka* (vrchol): $\quad \varepsilon_0 x_0^2 - \varepsilon_1 x_1^2 = 0$;

β_{21}) V_{f_2} vlastní přímka: *2 různoběžné roviny;*

β_{22}) V_{f_2} nevlastní přímka: *2 rovnoběžné roviny;*

γ) $\dim V_{f_2} = 2$: *rovina* (vrchol): $\quad \varepsilon_0 x_0^2 = 0$;

δ) $\dim V_{f_2} = 3$: *celý prostor* ($f_2 = 0$).

24.12. Věta. *Buď Q_{f_2} regulární nestředová kvadrika v reálném afinním prostoru $A_3(V_3)$. Pak platí*

(i) Q_{f_2} je eliptický paraboloid, právě když kvadrika $Q_{f_2} \cap N$ je tvořena jediným bodem;

(ii) Q_{f_2} je eliptický paraboloid, právě když $Q_{f_2} \cap N$ je dvojice přímek.

Důkaz. Protože Q_{f_2} je nestředová kvadrika, je kvadrika $Q_{f_2} \cap N$ podle věty 23.11 singulární a její vrchol je směr osy $\langle \boldsymbol{u} \rangle$ paraboloidu Q_{f_2}. Z klasifikace kuželoseček z odstavce 24.10 plyne, že $Q_{f_2} \cap N$ je buď bod $\langle \boldsymbol{u} \rangle$, nebo dvojice přímek protínajících se v bodě $\langle \boldsymbol{u} \rangle$. Je-li nyní Q_{f_2} eliptický paraboloid, je projektivního typu 1, takže podle definice 23.28 kvadrika Q_{f_2} obsahuje body, ale neobsahuje žádnou přímku, takže nutně $Q_{f_2} \cap N = \langle \boldsymbol{u} \rangle$. Je-li Q_{f_2} hyperbolický paraboloid, je projektivního typu 2, takže obsahuje přímky. Z věty 22.7 pak plyne, že bodem $\langle \boldsymbol{u} \rangle \in Q_{f_2}$ prochází přímka ležící celá na Q_{f_2}. Tato přímka je nevlastní, protože podle věty 24.5 každá vlastní přímka procházející bodem $\langle \boldsymbol{u} \rangle$ protne paraboloid v jediném vlastním bodě. Tedy $Q_{f_2} \cap N$ je nutně dvojice přímek protínajících se v bodě $\langle \boldsymbol{u} \rangle$. Odtud již obě tvrzení bezprostředně plynou. ∎

24.13. Příklady. Proveďme afinní klasifikaci kuželoseček v afinní rovině $A_2(R^2)$ daných vzhledem k soustavě souřadnice $S = \{(0,0), \boldsymbol{e}_1, \boldsymbol{e}_2\}$ rovnicemi:

a) $x^2 + 4y^2 + 4xy + 4x + 2y + 3 = 0$;

b) $4x^2 + 2y^2 + 6xy + 2x + 2y + 3 = 0$;
c) $2x^2 + 3y^2 + 2xy - 10x - 10y + 15 = 0$;
d) $9x^2 + y^2 - 6xy + 12x - 4y + 3 = 0$.

Pokud je kuželosečka regulární, nalezněme střed, případně směr osy.

Ř e š e n í : a) Abychom dostali analytické vyjádření formy f_2 vzhledem k indukované soustavě souřadnic $\bar{S}$ v $\bar{A}_2(\bar{V}_3)$, stačí s přihlédnutím k větě 21.25 položit $x = \frac{x_1}{x_0}$, $y = \frac{x_2}{x_0}$ a vynásobit levou stranu číslem x_0^2. Tedy $f_2(\boldsymbol{u}) = 3x_0^2 + 4x_0x_1 + 2x_0x_2 + x_1^2 + 4x_1x_2 + 4x_2^2$. Matice dané kuželosečky tedy je

$$\boldsymbol{A} = \begin{pmatrix} 3, & 2, & 1 \\ 2, & 1, & 2 \\ 1, & 2, & 4 \end{pmatrix}.$$

Protože $\det A = -9$ a $\det B = \begin{vmatrix} 1, & 2 \\ 2, & 4 \end{vmatrix} = 0$, je kuželosečka regulární a nestředová, tedy parabola. Je-li $\langle \boldsymbol{u} \rangle$ směr osy této paraboly, jsou jeho homogenní souřadnice $(0, z_1, z_2)$. Dosazením do polární bilineární formy f dostaneme rovnici poláry bodu $\langle \boldsymbol{u} \rangle$, $(2z_1 + z_2)x_0 + (z_1 + 2z_2)x_1 + (2z_1 + 4z_2)x_2 = 0$. Protože tato polára je nevlastní přímka o rovnici $x_0 = 0$, musí podle věty 11.14 platit $z_1 + 2z_2 = 0$, $2z_1 + 4z_2 = 0$. Odtud je již patrné, že vektor $\boldsymbol{u}$ o homogenních souřadnicích $(0, 2, -1)$ je aritmetickým zástupcem směru osy paraboly. Přejdeme-li zpět k soustavě souřadnic S v A_2, dostaneme směr osy $\langle (2, -1) \rangle$.

b) Podobně jako v a) je matice kuželosečky

$$\boldsymbol{A} = \begin{pmatrix} 3, & 1, & 1 \\ 1, & 4, & 3 \\ 1, & 3, & 2 \end{pmatrix},$$

$\det A = -3, \det B = -1$ a jedná se o regulární středovou kuželosečku. Při označení z věty 13.16 je $D_1 = 3, D_2 = 11, D_3 = |A| = -3$, takže signatura formy f_2 je $\langle 0, 2, 1 \rangle$, kuželosečka je tedy projektivního typu 1 a podle odstavce 24.10 je to tedy hyperbola. Jsou-li $(1, a, b)$ homogenní souřadnice středu S hyperboly vzhledem k $\bar{S}$, je podobně jako v předchozím příkladu $(a + b + 3)x_0 + (4a + 3b + 1)x_1 + (3a + 2b + 1)x_2 = 0$ rovnice poláry bodu S. Protože tato polára je podle definice 24.2 nevlastní přímka o rovnici $x_0 = 0$, musí podle věty 11.14 platit $4a + 3b + 1 = 0$ a $3a + 2b + 1 = 0$. Řešením této soustavy snadno zjistíme, že bod $S = (-1, 1)$ je středem hyperboly.

c) Matice kuželosečky je

$$\boldsymbol{A} = \begin{pmatrix} 15, & -5, & -5 \\ -5, & 2, & 1 \\ -5 & 1, & 3 \end{pmatrix}.$$

Protože $\det A = 0$, je kuželosečka singulární a její vrchol dostaneme podle věty 12.10 jako řešení homogenní soustavy lineárních rovnic s maticí $\boldsymbol{A}$. Jest

$$\begin{pmatrix} 15, & -5, & -5 \\ -5, & 2, & 1 \\ -5, & 1, & 3 \end{pmatrix} \sim \begin{pmatrix} 3, & -1, & -1 \\ -5, & 2, & 1 \\ -5, & 1, & 3 \end{pmatrix} \sim \begin{pmatrix} 3, & -1, & -1 \\ 0, & 1, & -2 \\ 0, & -2, & 4 \end{pmatrix} \sim \begin{pmatrix} 3, & -1, & -1 \\ 0, & 1, & -2 \end{pmatrix},$$

takže $\langle(1,2,1)\rangle$ je vrchol kuželosečky. Doplněk vrcholu je např. $\langle(0,1,0),(0,0,1)\rangle$, tj. nevlastní přímka N o rovnici $x_0 = 0$, takže kvadrika $Q_{f_2} \cap N$ je vytvořena formou $g_2(\boldsymbol{u}) = 2x_1^2 + 2x_1x_2 + 3x_2^2$, a má tudíž matici $\begin{pmatrix} 2, & 1 \\ 1, & 3 \end{pmatrix}$. Protože $D_1 = 2, D_2 = 5$, je forma g_2 podle 13.16 pozitivně definitní, kvadrika $Q_{f_2} \cap N$ je prázdná množina a $Q_{f_2} = \{(2,1)\}$.

d) Matice kuželosečky je

$$\boldsymbol{A} = \begin{pmatrix} 3, & 6, & -2 \\ 6, & 9, & -3 \\ -2, & -3, & 1 \end{pmatrix},$$

$\det A = 0$, takže Q_{f_2} je singulární a z

$$\begin{pmatrix} 3, & 6, & -2 \\ 6, & 9, & -3 \\ -2, & -3, & 1 \end{pmatrix} \sim \begin{pmatrix} 3, & 6, & -2 \\ 0, & -3, & 1 \\ 0, & 3, & -1 \end{pmatrix} \sim \begin{pmatrix} 1, & 0, & 0 \\ 0, & 3, & -1 \end{pmatrix}$$

dostaneme vrchol $V_{f_2} = \langle(0,1,3)\rangle$. Doplněk vrcholu je např. projektivní přímka $P_1 = \langle(1,0,0),(0,1,0)\rangle$, kvadrika $Q_{f_2} \cap P_1$ je vytvořena formou $g_2(\boldsymbol{u}) = 3x_0^2 + 12x_0x_1 + 9x_1^2$ s maticí $\begin{pmatrix} 3, & 6 \\ 6, & 9 \end{pmatrix}$. Protože $D_1 = 3$ a $D_2 = -9$, je kvadrika Q_{g_2} podle odstavce 24.9 tvořena dvěma body. Položíme-li $x = \frac{x_1}{x_0}$, pak po vydělení $g_2(\boldsymbol{u})$ výrazem x_0^2 a dosazení dostaneme kvadratickou rovnici $9x^2 + 12x + 3 = 0$ neboli $3x^4 + 4x + 1 = 0$, která má dvě řešení $x = -\frac{1}{3}$ a $x = -1$. Kvadrika Q_{g_2} je tedy tvořena body $\langle(1,-\frac{1}{3},0)\rangle$ a $\langle(1,-1,0)\rangle$. Přechodem zpět k soustavě souřadnic S a použitím věty 23.3 snadno dostaneme, že Q_{f_2} je dvojice rovnoběžných přímek $(-\frac{1}{3},0) + \langle(1,3)\rangle$ a $(-1,0) + \langle(1,3)\rangle$. Podle věty 19.15 můžeme tyto přímky popsat rovnicemi $3x - y + 1 = 0$ a $3x - y + 3 = 0$.

24.14. Příklady. Proveďme afinní klasifikaci kvadrik v afinním prostoru $A_3(R^3)$ daných vzhledem k soustavě souřadnic $S = \{(0,0,0), \boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3\}$ rovnicemi

a) $5x^2 - 4xy + 2xz + y^2 + 2z^2 - 8x - 14z - 1 = 0$;
b) $x^2 + 4xy - 6xz + 5y^2 - 12yz + 9z^2 + 4x + 2y + 10z - 4 = 0$,
c) $3x^2 + 4xy - 2xz + y^2 - 4yz + z^2 - 22x - 22y + 14z + 54 = 0$;
d) $2x^2 - 3xy + 5xz - 2y^2 + 10yz - 12z^2 - 5y + 11z - 2 = 0$;
e) $x^2 - 4xy + 6xz + 4y^2 - 12yz + 9z^2 + 2x - 4y + 6z - 3 = 0$.

Pokud je kvadrika regulární, nalezněme střed, případně směr osy.

Řešení: a) Matice kvadriky vzhledem k soustavě souřadnic S (indukované soustavě souřadnic $\bar{S}$) je

$$\boldsymbol{A} = \begin{pmatrix} -1, & -4, & 0, & -7 \\ -4, & 5, & -2, & 1 \\ 0, & -2, & 1, & 0 \\ -7, & 1, & 0, & 2 \end{pmatrix}.$$

Jest $\det A = -26$, $\det B = 1$, takže Q_{f_2} je regulární středová kvadrika. Pro matici $\boldsymbol{A}$ máme (viz odst. 13.16) $D_1 = -1, D_2 = -21, D_3 = -17, D_4 = |A| = -26$, takže forma f_2 má signaturu $\langle 0,3,1\rangle$ a kvadrika Q_{f_2} je projektivního typu 1. Dále víme, že $\boldsymbol{B}$ je matice kvadriky $Q_{f_2} \cap N$, přičemž pro matici $\boldsymbol{B}$ analogicky máme $D_1 = 5, D_2 = 1, D_3 = |B| = 1$, forma $f_2|V_n$ má signaturu $\langle 0, 3, 0\rangle$, kvadrika $Q_{f_2} \cap N$ je tudíž projektivního typu 0 a Q_{f_2} je podle odstavce 24.11 elipsoid. Jak je patrno z definice středu či směru osy 24.2, plyne z věty 11.14, že matice $\boldsymbol{B}$ je maticí soustavy lineárních rovnic pro nalezení středu či směru osy. Pro nalezení směru osy se jedná o soustavu homogenní, zatímco pro hledání středu jde o soustavu nehomogenní, kde $(-a_{10}, -a_{20}, \dots, -a_{n0})$ je sloupec pravých stran soustavy (viz též příklady v předchozím odstavci). V našem případě tedy dostáváme nehomogenní soustavu lineárních rovnic s rozšířenou maticí

$$\left(\begin{array}{ccc|c} 5, & -2, & 1 & 4 \\ -2, & 1, & 0 & 0 \\ 1, & 0, & 2 & 7 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1, & 0, & 2 & 7 \\ 0, & 1, & 4 & 14 \\ 0, & -2, & -9 & -31 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1, & 0, & 2 & 7 \\ 0, & 1, & 4 & 14 \\ 0, & 0, & -1 & -3 \end{array}\right).$$

Odtud dostáváme, že řešení $(1, 2, 3)$ této soustavy je středem elipsoidu Q_{f_2}.

b) Podobně jako v předchozím příkladu máme

$$\boldsymbol{A} = \begin{pmatrix} -4, & 2, & 1, & 5 \\ 2, & 1, & 2, & -3 \\ 1, & 2, & 5, & -6 \\ 5, & -3, & -6, & 9 \end{pmatrix}.$$

Dále, $\det A = -121, \det B = 0$, takže kvadrika Q_{f_2} je paraboloid. Protože $D_1 = -4, D_2 = -8, D_3 = -19, D_4 = |A| = -121$, je Q_{f_2} projektivního typu 1, a je to tedy eliptický paraboloid. Dále

$$\begin{pmatrix} 1, & 2, & -3 \\ 2, & 5, & -6 \\ -3, & -6, & 9 \end{pmatrix} \sim \begin{pmatrix} 1, & 2, & -3 \\ 0, & 1, & 0 \\ 0, & 0, & 0 \end{pmatrix},$$

takže homogenní soustava lineárních rovnic s maticí $\boldsymbol{B}$ má řešení $\langle(3, 0, 1)\rangle$ a nevlastní bod $\langle(3, 0, 1)\rangle$ je tedy směrem osy tohoto eliptického paraboloidu.

c) Jest

$$\boldsymbol{A} = \begin{pmatrix} 54, & -11, & -11, & 7 \\ -11, & 3, & 2, & -1 \\ -11, & 2, & 1, & -2 \\ 7, & -1, & -2, & 1 \end{pmatrix},$$

takže $\det A = 0$ a kvadrika je singulární. Její vrchol dostaneme podle věty 12.10 jako řešení homogenní soustavy lineárních rovnic s maticí $\boldsymbol{A}$. Máme (pětinásobek třetího řádku přičteme k prvnímu a třetí řádek odečteme od druhého, zbytek je jasný)

$$\boldsymbol{A} \sim \begin{pmatrix} -1, & -1, & -6, & -3 \\ 0, & 1, & 1, & 1 \\ -11, & 2, & 1, & -2 \\ 7, & -1, & -2, & 1 \end{pmatrix} \sim \begin{pmatrix} 1, & 1, & 6, & 3 \\ 0, & 1, & 1, & 1 \\ 0, & 13, & 67, & 31 \\ 0, & -8, & -44, & -20 \end{pmatrix} \sim \begin{pmatrix} 1, & 1, & 6, & 3 \\ 0, & 1, & 1, & 1 \\ 0, & 0, & 54, & 18 \\ 0, & 0, & -36, & -12 \end{pmatrix} \sim$$

$$\begin{pmatrix} 1, & 1, & 6, & 3 \\ 0, & 1, & 1, & 1 \\ 0, & 0, & 3, & 1 \end{pmatrix},$$

takže soustava má řešení $\langle(1,2,1,-3)\rangle$ a vlastní bod $(2,1,-3)$ je vrcholem kvadriky Q_{f_2}. Doplněk vrcholu V_{f_2} je např. nevlastní nadrovina N, kvadrika $Q_{f_2} \cap N$ má matici

$$\boldsymbol{B} = \begin{pmatrix} 3, & 2, & -1 \\ 2, & 1, & -2 \\ -1, & -2, & 1 \end{pmatrix}$$

a platí $D_1 = 3, D_2 = -1, D_3 = -6$, kvadrika $Q_{f_2} \cap N$ je projektivního typu 1, a Q_{f_2} je tedy podle odstavce 24.11 kuželová plocha s vrcholem $(2,1,-3)$.

d) Abychom nemuseli pracovat se zlomky, budeme uvažovat formu $2f_2$. Pak příslušná matice je

$$\boldsymbol{A} = \begin{pmatrix} -4, & 0, & -5, & 11 \\ 0, & 4, & -3, & 5 \\ -5, & -3, & -4, & 10 \\ 11, & 5, & 10, & -24 \end{pmatrix}.$$

Přičteme-li dvojnásobek třetího řádku ke čtvrtému a dáme-li čtvrtý řádek na první místo, dostaneme

$$\boldsymbol{A} \sim \begin{pmatrix} 1, & -1, & 2, & -4 \\ -4, & 0, & -5, & 11 \\ 0, & 4, & -3, & 5 \\ -5, & -3, & -4, & 10 \end{pmatrix} \sim \begin{pmatrix} 1, & -1, & 2, & -4 \\ 0, & -4, & 3, & -5 \\ 0, & 4, & -3, & 5 \\ 0, & -8, & 6, & -10 \end{pmatrix} \sim \begin{pmatrix} 1, & -1, & 2, & -4 \\ 0, & 4, & -3, & 5 \end{pmatrix},$$

takže kvadrika Q_{f_2} je singulární a její vrchol je přímka $\langle(-5,3,4,0),(11,-5,0,4)\rangle = \langle(1,1,8,4),(0,2,11,5)\rangle$. Doplněk vrcholu je např. přímka $P_1 = \langle \boldsymbol{e}_3, \boldsymbol{e}_4\rangle$, matice kvadriky $Q_{f_2} \cap P_1$ je zřejmě $\begin{pmatrix} -4, & 10 \\ 10, & -24 \end{pmatrix}$. Protože $D_1 = -4, D_2 = -4$, je $Q_{f_2} \cap P_1$ projektivního typu 1 a podle odstavce 24.9 sestává ze dvou bodů. Podobně jako v příkladu 4.13 d) máme $-4x^2 + 20x - 24 = 0$, tedy $x^2 - 5x + 6 = 0$, kde $x = \frac{x_2}{x_3}$. Pak $x = 3, 2$, takže $Q_{f_2} \cap P_1 = \{\langle(0,0,3,1)\rangle, \langle(0,0,2,1)\rangle\}$. Přejdeme-li zpět k soustavě souřadnic S v A_2, vidíme, že kvadrika Q_{f_2} je dvojice rovin protínajících se ve vrcholu V_{f_2}, tj. dvojice rovin $(1,8,4) + \langle(2,11,5),(0,3,1)\rangle$ a $(1,8,4) + \langle(2,11,5),(0,2,1)\rangle$. Použitím věty 19.15 snadno tyto roviny vyjádříme pomocí rovnic, $2x+y-3z+2 = 0$ a $x - 2y + 4z - 1 = 0$.

e) Podobně jako v předchozím příkladu máme

$$\boldsymbol{A} = \begin{pmatrix} -3, & 1, & -2, & 3 \\ 1, & 1, & -2, & 3 \\ -2, & -2, & 4, & -6 \\ 3, & 3, & -6, & 9 \end{pmatrix},$$

$$A \sim \begin{pmatrix} 1, 1, -2, & 3 \\ 0, 4, -8, & 12 \end{pmatrix} \sim \begin{pmatrix} 1, 1, -2, 3 \\ 0, 1, -2, 3 \end{pmatrix} \sim \begin{pmatrix} 1, 0, & 0, 0 \\ 0, 1, & -2, 3 \end{pmatrix},$$

takže vrchol V_{f_2} je projektivní přímka obsažená v nevlastní rovině N, totiž $\langle(0,-3, 0,1), (0,2,1,0)\rangle$. Doplněk vrcholu je např. přímka $P_1 = \langle(1,0,0,0),(0,1,0,0)\rangle$, $Q_{f_2} \cap P_1$ má matici $\begin{pmatrix} -3, 1 \\ 1, 1 \end{pmatrix}$, přičemž $D_1 = -3, D_2 = -4$, takže $Q_{f_2} \cap P_1$ je projektivního typu jedna a je tvořena dvěma body. Pro $x = \frac{x_1}{x_0}$ máme $x^2 + 2x - 3 = 0$ s kořeny 1 a -3, takže $Q_{f_2} \cap P_1 = \langle(1,1,0,0),(1,-3,0,0)\rangle$. Vidíme tedy, že Q_{f_2} je dvojice rovnoběžných rovin $(1,0,0) + \langle(-3,0,1),(2,1,0)\rangle$ a $(-3,0,0) + \langle(-3,0,1),(2,1,0)\rangle$, nebo v rovnicovém tvaru $x-2y+3z-1 = 0$ a $x-2y+3z+3 = 0$.

V této kapitole se budeme zabývat regulárními kvadrikami v euklidovském prostoru E_n. Jak jsme již naznačili v poznámce 23.29, budeme zkoumat otázky související se skalárním součinem, tj. problematiku týkající se kolmosti a velikosti úsečky (vzdálenost bodů).

25.1. Definice. Buď Q_{f_2} regulární středová kvadrika v euklidovském prostoru E_n. Nevlastní bod $\langle \boldsymbol{u} \rangle$ se nazývá *směr osy kvadriky* Q_{f_2}, jestliže vektor $\boldsymbol{u}$ je kolmý na polární nadrovinu $\varrho_{\langle \boldsymbol{u} \rangle}$ bodu $\langle \boldsymbol{u} \rangle$. Každá přímka jdoucí středem kvadriky Q_{f_2} a mající směr osy se nazývá *osa kvadriky* Q_{f_2}.

25.2. Věta. *Buď Q_{f_2} regulární středová kvadrika v euklidovském prostoru E_n. Pak v E_n existuje soustava souřadnic $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ taková, že*

(i) a je středem kvadriky Q_{f_2};

(ii) $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ je ortonormální polární báze kvadratické formy $f_2|V_n$;

(iii) kvadrika Q_{f_2} má vzhledem k S rovnici $\sum_{i=1}^n \eta_i \frac{x_i^2}{a_i^2} = 1$, kde $\eta_i = \pm 1$ a čísla $a_i > 0$ jsou kvadrikou Q_{f_2} určena až na pořadí jednoznačně, tj. nezávisí na volbě soustavy souřadnic S mající vlastnosti (i) a (ii).

Důkaz. Existence soustavy souřadnic S s vlastnostmi (i) a (ii) plyne ihned z věty 22.13. Přitom Q_{f_2} má vzhledem k S zřejmě rovnici $\sum_{i=1}^n \varepsilon_i x_i^2 = 1$, kde $\varepsilon_i = \frac{-f_2(\boldsymbol{u}_i)}{f_2(a)}$. Nyní stačí položit $a_i = \frac{1}{\sqrt{\eta_i \varepsilon_i}}$, kde $\eta_i = 1$ pro $\varepsilon_i > 0$ a $\eta_i = -1$ pro $\varepsilon_i < 0$ a zbývá dokázat nezávislost čísel $a_i, i = 1, 2, \dots, n$, na volbě soustavy souřadnic S s vlastnostmi (i) a (ii). K tomu zřejmě stačí ověřit, že čísla $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$ jsou kvadrikou Q_{f_2} určena až na pořadí jednoznačně. Označme $\lambda_0 = f_2(a)$, $\lambda_i = f_2(\boldsymbol{u}_i), i = 1, 2, \dots, n$, a ukažme jednoznačnost čísel $\lambda_1, \lambda_2, \dots, \lambda_n$. Forma f_2 má vzhledem k aritmetické bázi $\bar{S} = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ diagonální matici

$$\boldsymbol{A} = \begin{pmatrix} \lambda_0, & 0, & \dots, & 0 \\ 0, & \lambda_1, & \dots, & 0 \\ \dots & \dots & \dots & \dots \\ 0, & 0, & \dots, & \lambda_n \end{pmatrix},$$

a je-li $S' = \{a, \boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n\}$ jiná soustava souřadnic v E_n mající vlastnosti (i) a (ii), pak matice přechodu od $\bar{S}$ k $\bar{S}'$ má zřejmě tvar $\boldsymbol{B} = \begin{pmatrix} 1, & 0 \\ 0, & \boldsymbol{C} \end{pmatrix}$, kde $\boldsymbol{C}$ je podle věty 20.11 ortogonální matice stupně n. Protože podle věty 20.10 je $\boldsymbol{C}^{-1} = \boldsymbol{C}^T$, je i $\boldsymbol{B}^{-1} = \boldsymbol{B}^T$. Podle věty 12.7 je matice formy f vzhledem k bázi $\bar{S}'$ rovna $\boldsymbol{B}^T \boldsymbol{A} \boldsymbol{B}$. Tato matice je opět diagonální a má podle věty 15.6 stejná vlastní čísla jako matice $\boldsymbol{A}$. Tím je jednoznačnost čísel $a_1, a_2, \dots, a_n$ až na pořadí dokázána. ∎

25.3. Důsledek. *Každá regulární středová kvadrika Q_{f_2} v euklidovském prostoru E_n má alespoň jednu n-tici navzájem kolmých směrů.*

Důkaz. Je-li $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ soustava souřadnic z předchozí věty, pak pro každé $i \in \{1, 2, \dots, n\}$ je $f(\boldsymbol{u}_i, a) = f(\boldsymbol{u}_i, \boldsymbol{u}_j) = 0$ pro $j = 1, 2, \dots, n$, $j \neq i$, takže polární nadrovina geometrického bodu $\langle \boldsymbol{u}_i \rangle$ je $\varrho_{\langle \boldsymbol{u}_i \rangle} = \langle a, \boldsymbol{u}_1, \dots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_{i+1}, \dots, \boldsymbol{u}_n \rangle$. Protože vektor $\boldsymbol{u}_i$ je zároveň kolmý k této nadrovině, je $\langle \boldsymbol{u}_i \rangle$ směr osy kvadriky Q_{f_2}. ∎

25.4. Definice. Čísla $a_i, i = 1, 2, \dots, n$, z věty 25.2 se nazývají *velikosti poloos* regulární středové kvadriky Q_{f_2}, rovnice $\sum_{i=1}^{n} \eta_i \frac{x_i^2}{a_i^2} = 1$ se nazývá *kanonická rovnice kvadriky* Q_{f_2}.

25.5. Metrická klasifikace regulárních středových kuželoseček v E_2.

V souladu s odstavcem 24.10 rozlišujeme následujících šest typů regulárních středových kuželoseček:

a) Kuželosečka Q_{f_2} o rovnici $\frac{x_1^2}{a_1^2} + \frac{x_2^2}{a_2^2} = 1$ se pro $a_1 \neq a_2$ nazývá *elipsa* a pro $a_1 = a_2$ *kružnice* (o poloměru a_1).

b) Kuželosečka o rovnici $-\frac{x_1^2}{a_1^2} - \frac{x_2^2}{a_2^2} = 1$ se pro $a_1 \neq a_2$ nazývá *imaginární elipsa* a pro $a_1 = a_2$ *imaginární kružnice.*

c) Kuželosečka o rovnici $\frac{x_1^2}{a_1^2} - \frac{x_2^2}{a_2^2} = 1$ se pro $a_1 \neq a_2$ nazývá *hyperbola* a pro $a_1 = a_2$ *rovnoosá hyperbola.*

25.6. Metrická klasifikace regulárních středových kvadrik v E_3.

a) $\frac{x_1^2}{a_1^2} + \frac{x_2^2}{a_2^2} + \frac{x_3^2}{a_3^2} = 1$:

$a_1 = a_2 = a_2$	*kulová plocha* (o poloměru a_1);
$a_1 = a_2 < a_3$	*protáhlý rotační elipsoid*;
$a_1 = a_2 > a_3$	*zploštělý rotační elipsoid*;
$a_1 \neq a_2, a_2 \neq a_3, a_1 \neq a_3$	*trojosý elipsoid.*

b) $-\frac{x_1^2}{a_1^2} - \frac{x_2^2}{a_2^2} - \frac{x_3^2}{a_3^2} = 1$: Jak víme z odstavce 24.11, tato kvadrika neobsahuje žádný bod. Podle vzájemného vztahu velikosti poloos v tomto případě rozlišujeme podobně jako v bodě a) *imaginární kulovou plochu* a tři typy *imaginárních elipsoidů.*

c) $\frac{x_1^2}{a_1^2} - \frac{x_2^2}{a_2^2} - \frac{x_3^2}{a_3^2} = 1$:

$a_1 = a_2 = a_3$	*rovnoosý dvojdílný hyperboloid*;
$a_1 = a_2 \neq a_3$	*rotační dvojdílný hyperboloid*;
$a_1 \neq a_2, a_2 \neq a_3, a_1 \neq a_3$	*trojosý dvojdílný hyperboloid.*

d) $\frac{x_1^2}{a_1^2} + \frac{x_2^2}{a_2^2} - \frac{x_3^2}{a_3^2} = 1$: Metrická klasifikace *jednodílného hyperboloidu* je stejná jako v předchozím případě u hyperboloidu dvojdílného.

25.7. Definice. Bod a paraboloidu Q_{f_2} se nazývá *vrchol paraboloidu*, jestliže tečná nadrovina ϱ_a v bodě a je kolmá na směr osy paraboloidu. Přímka, která prochází vrcholem a má směr osy paraboloidu, se nazývá *osa paraboloidu.*

25.8. Věta. *Každá regulární nestředová kvadrika Q_{f_2} v euklidovském prostoru E_n má právě jeden vrchol.*

Důkaz. Začněme s důkazem existence. Podle věty 12.22 je kvadratická forma $f_2|V_n$ singulární a její vrchol je směr osy paraboloidu $\langle \boldsymbol{u}_n \rangle$. Podle věty 22.13 pak existuje ortonormální báze $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$ formy $f_2|V_n$. Označme $W = \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_{n-1} \rangle$ ortogonální doplněk směru osy $\langle \boldsymbol{u}_n \rangle$ ve V_n a buď $b \in E_n$ libovolný bod. Podle věty 23.8 má nadrovina $b + W$ jednoznačně určený pól c, přičemž přímka $c + \langle \boldsymbol{u}_n \rangle$ protne kvadriku Q_{f_2} podle věty 24.5 v jediném vlastním bodě a. Pak $a = c + r\boldsymbol{u}_n$ pro nějaké reálné číslo r, takže $f(a, \boldsymbol{u}_i) = f(c + r\boldsymbol{u}_n, \boldsymbol{u}_i) = 0$ pro každé $i = 1, 2, \dots, n-1$.

Protože však $a \in Q_{f_2}$, je $a + W$ tečná nadrovina kvadriku Q_{f_2} v bodě a a tento bod je vrcholem paraboloidu Q_{f_2} vzhledem k tomu, že $\boldsymbol{u}_n \perp W$.

K důkazu jednoznačnosti předpokládejme, že a, b jsou dva vrcholy paraboloidu Q_{f_2}. Protože $f(b, \boldsymbol{u}_i) = 0$ pro každé $i = 1, 2, \ldots, n-1$, je $f(b, \boldsymbol{u}_n) \neq 0$, neboť v opačném případě by bod b byl pólem nevlastní nadroviny. Existuje tedy reálné číslo r takové, že $f(a, \boldsymbol{u}_n) = rf(b, \boldsymbol{u}_n)$. Pak ale bod $\langle a - rb \rangle \in \bar{E}_n$ je pólem nevlastní nadroviny, takže $\langle a - rb \rangle = \langle \boldsymbol{u}_n \rangle$. Podle definice sčítání ve $(\overline{V}_{n+1})$ (viz odstavec 21.11) je nutně $r = 1$, takže $a \in b + \langle \boldsymbol{u}_n \rangle$. Vidíme tedy, že body a, b jsou průsečíky přímky $b + \langle \boldsymbol{u}_n \rangle$ s paraboloidem Q_{f_2}, odkud podle věty 24.5 dostáváme $a = b$. ∎

25.9. Věta. *Buď Q_{f_2} regulární nestředová kvadrika v euklidovském prostoru E_n. Pak v E_n existuje soustava souřadnic $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ taková, že*

(i) bod a je vrchol paraboloidu Q_{f_2} a $\langle \boldsymbol{u}_n \rangle$ je směr jeho osy;

(ii) $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ je ortonormální polární báze kvadratické formy $f_2|V_n$;

(iii) kvadrika Q_{f_2} má vzhledem k soustavě S kanonickou rovnici $\sum_{i=1}^{n-1} \varepsilon_i x_i^2 = 2x_n$, kde čísla $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{n-1}$ jsou kvadrikou Q_{f_2} určena až na pořadí jednoznačně, tj. nezávisí na volbě soustavy souřadnic S mající vlastnosti (i) a (ii).

Důkaz. Existence soustavy souřadnic S s vlastnostmi (i) a (ii) plyne bezprostředně z vět 25.8 a 22.13, přičemž kvadrika Q_{f_2} má vzhledem k S rovnici $\sum_{i=1}^{n-1} \varepsilon_i x_i^2 = 2x_n$, kde $\varepsilon_i = -\frac{f_2(\boldsymbol{u}_i)}{f(a, \boldsymbol{u}_n)}, i = 1, 2, \ldots, n-1$. K důkazu jednoznačnosti stačí ověřit, že číslo $f_2(\boldsymbol{u}_1), f_2(\boldsymbol{u}_2), \ldots, f_2(\boldsymbol{u}_{n-1})$ nezávisí na volbě soustavy souřadnic S splňující podmínky (i) a (ii). Důkaz tohoto tvrzení je stejný jako v případě věty 25.2 a lze jej tudíž přenechat čtenáři jako cvičení. ∎

25.10. Metrická klasifikace regulárních nestředových kvadrik v E_2 a E_3.

I. *Kuželosečky.* Jediná nestředová kuželosečka je *parabola* s kanonickou rovnicí $\varepsilon_1 x_1^2 = 2x_2$, číslo $p = \frac{1}{|\varepsilon_1|}$ se nazývá *parametr paraboly.*

II. *Kvadriky v E_3.*

a) $\varepsilon_1 x_1^2 + \varepsilon_2 x_2^2 = 2x_3$ — *eliptický paraboloid;*

b) $\varepsilon_1 x_1^2 - \varepsilon_2 x_2^2 = 2x_3$ — *hyperbolický paraboloid.*

V případě $\varepsilon_1 = \varepsilon_2$ hovoříme o rotačních paraboloidech a v případě $\varepsilon_1 \neq \varepsilon_2$ o dvojosých paraboloidech.

25.11. Příklady. Proveďme metrickou klasifikaci kuželoseček v euklidovské rovině $E_2(R^2)$:

(a) $3x^2 + 2xy + 3y^2 - 10x - 14y + 7 = 0$;
(b) $x^2 - 6xy + 9y^2 + 14x - 2y - 27 = 0$.

Ř e š e n í : (a) Pro matici

$$\boldsymbol{A} = \begin{pmatrix} 7, & -5, & -7 \\ -5, & 3, & 1 \\ -7, & 1, & 3 \end{pmatrix}$$

máme $\det \boldsymbol{A} = -96$, $\det \boldsymbol{B} = 8$, odkud snadno vidíme, že se jedná o elipsu. Podobně jako v příkladech předchozí kapitoly nalezneme řešením soustavy rovnic

$$3x + \ \ y = 5,$$

$$x + 3y = 7,$$

střed elipsy $a = (1, 2)$. Směry os budeme hledat pomocí věty 22.17. Rovnice $\det(\boldsymbol{B} - \lambda \boldsymbol{E}) = \lambda^2 - 6\lambda + 8 = 0$ má kořeny $\lambda_1 = 2, \lambda_2 = 4$ a příslušné homogenní soustavy lineárních rovnic s maticemi $\boldsymbol{B} - \lambda_1 \boldsymbol{E}$ a $\boldsymbol{B} - \lambda_2 \boldsymbol{E}$ mají řešení $\boldsymbol{v}_1 = (1, -1)$ a $\boldsymbol{v}_2 = (1, 1)$. Tak dostáváme soustavu souřadnic $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2\}$, kde $a = (1, 2)$, $\boldsymbol{u}_1 = \frac{1}{\sqrt{2}}(1, -1)$, $\boldsymbol{u}_2 = \frac{1}{\sqrt{2}}(1, 1)$. Protože $f_2(a) = -12, f_2(\boldsymbol{u}_1) = 2$ a $f_2(\boldsymbol{u}_2) = 4$, má daná elipsa rovnici $x^2 + 2y^2 = 6$, a tedy kanonickou rovnici $\frac{x^2}{6} + \frac{y^2}{3} = 1$. Velikosti poloos tudíž jsou $\sqrt{6}$ a $\sqrt{3}$.

(b) Podobně jako v předchozím příkladě máme

$$\boldsymbol{A} = \begin{pmatrix} -27, & 7, & -1 \\ 7, & 1, & -3 \\ -1, & -3, & 9 \end{pmatrix},$$

$\det \boldsymbol{A} = -400, \det \boldsymbol{B} = 0$, takže se jedná o parabolu o směru osy $\boldsymbol{v}_2 = (3, 1)$ (řešení homogenní soustavy rovnic s maticí $\boldsymbol{B}$). Ortogonální doplněk směru osy je generován vektorem $\boldsymbol{v}_1 = (1, -3)$. Podle definice vrcholu paraboloidu 25.7 leží nevlastní bod $\langle \boldsymbol{v}_1 \rangle$ na poláře ϱ_a bodu a, takže podle věty 23.8 leží bod a na poláře $\varrho_{\langle \boldsymbol{v}_1 \rangle}$ bodu $\langle \boldsymbol{v}_1 \rangle$. Z matice $\boldsymbol{A}$ snadno dostaneme rovnici $10x_0 + 10x_1 - 30x_2 = 0$ poláry $\varrho_{\langle \boldsymbol{v}_1 \rangle}$ neboli v E_2 $x - 3y + 1 = 0$. Podle věty 24.5 protne tato přímka parabolu v jediném bodě, tedy ve vrcholu a. Dosazením do rovnice paraboly snadno dostaneme vrchol $a = (2, 1)$ paraboly Q_{f_2}. Máme tedy soustavu souřadnic $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2\}$, kde $a = (2, 1)$, $\boldsymbol{u}_1 = \frac{1}{\sqrt{10}}(1, -3)$, $\boldsymbol{u}_2 = \frac{1}{\sqrt{10}}(3, 1)$. Rovnice paraboly vzhledem k S pak je $10x^2 + \frac{40}{\sqrt{10}}y = 0$ neboli $2y = -\frac{\sqrt{10}}{2}x^2$ a parabola má parametr $p = \frac{\sqrt{10}}{5}$.

25.12. Příklady. Proveďme metrickou klasifikaci kvadrik v euklidovském prostoru $E_3(R^3)$:

(a) $10x^2 + 4xy + 4xz + 13y^2 + 8yz + 13z^2 + 88x - 40y - 22z + 262 = 0$;
(b) $4x^2 - 4xz + 2y^2 - 4yz - 3z^2 - 28x - 40y - 54z + 33 = 0$.

Řešení: (a) Jest

$$\boldsymbol{A} = \begin{pmatrix} 262, & 44, & -20, & -11 \\ 44, & 10, & 2, & 2 \\ -20, & 2, & 13, & 4 \\ -11, & 2, & 4, & 13 \end{pmatrix},$$

$\det \boldsymbol{A} = -129\,762, \det \boldsymbol{B} = 1458$. Protože pro subdeterminanty matice $\boldsymbol{B}$ je $D_1 = 10, D_2 = 126$ a $D_3 = |\boldsymbol{B}| = 1458$, je forma $f_2|R^3$ pozitivně definitní a Q_{f_2} je elipsoid. Střed a spočteme ze soustavy rovnic

$$10x^2 + 2y + 2z = -44,$$

$$2x + 13y + 4z = 20,$$

$$2x + 4y + 13z = 11,$$

takže $a = (-5, 2, 1)$. Pro nalezení směrů os musíme nejprve nalézt vlastní čísla matice $\boldsymbol{B} - \lambda \boldsymbol{E}$. Předně jest

$$|\boldsymbol{B} - \lambda \boldsymbol{E}| = \begin{vmatrix} 10-\lambda, & 2, & 2 \\ 2, & 13-\lambda, & 4 \\ 2, & 4, & 13-\lambda \end{vmatrix} = -\lambda^3 + 36\lambda^2 - 405\lambda + 1458.$$

Přitom je ihned patrné, že pro $\lambda_1 = 9$ jsou poslední dva řádky stejné, takže pak již snadno najdeme zbývající vlastní čísla $\lambda_2 = 9$ a $\lambda_3 = 18$. Pro $\lambda = 9$ dostáváme jedinou rovnici $x + 2y + 2z = 0$, jejíž řešení tvoří dvojrozměrný podprostor s ortogonální bází $\boldsymbol{v}_1 = (2, 1, -2), \boldsymbol{v}_2 = (2, -2, 1)$. Pro $\lambda = 18$ dostáváme homogenní soustavu lineárních rovnic s maticí

$$\begin{pmatrix} -8, & 2, & 2 \\ 2, & -5, & 4 \\ 2, & 4, & -5 \end{pmatrix} \sim \begin{pmatrix} 2, & 4, & -5 \\ 0, & -9, & 9 \\ 0, & 18, & -18 \end{pmatrix} \sim \begin{pmatrix} 2, & 4, & -5 \\ 0, & 1, & -1 \end{pmatrix}$$

a s řešením $\boldsymbol{v}_3 = (1, 2, 2)$

Tím jsme získali soustavu souřadnic $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3\}$, kde $a = (-5, 2, 1), \boldsymbol{u}_1 = \frac{1}{3}(2, 1, -2), \boldsymbol{u}_2 = \frac{1}{3}(2, -2, 1), \boldsymbol{u}_3 = \frac{1}{3}(1, 2, 2)$. Přitom $f_2(a) = -9, f_2(\boldsymbol{u}_1) = 9, f_2(\boldsymbol{u}_2) = 9$ a $f_2(\boldsymbol{u}_3) = 18$, takže kvadrika Q_{f_2} je zploštělý elipsoid se středem $a = (-5, 2, 1)$, kanonickou rovnicí $x^2 + y^2 + 2z^2 = 1$ a velikostmi poloos $1, 1, \frac{\sqrt{2}}{2}$.

(b) Jest

$$\boldsymbol{A} = \begin{pmatrix} 33, & -14, & -20, & -27 \\ -14, & 4, & 0, & -2 \\ -20, & 0, & 2, & -2 \\ -27, & -2, & -2, & 3 \end{pmatrix},$$

$\det \boldsymbol{A} \neq 0, \det \boldsymbol{B} = 0$. Ze soustavy rovnic s maticí $\boldsymbol{B}$ spočteme směr osy $\boldsymbol{v}_3 = (1, 2, 2)$. Podobně jako v příkladu 25.11 (b) nalezneme vrchol paraboloidu $a = (1, -1, 1)$. Ortogonální doplněk $\boldsymbol{v}_3$ v R^3 je $W = \langle (2, 1, -2), (2, -2, 1) \rangle$, přičemž, jak se snadno ověří, vektory $\boldsymbol{v}_1 = (2, 1, -2)$ a $\boldsymbol{v}_2 = (2, -2, 1)$ tvoří polární bázi formy $f_2|W$. Tím dostáváme soustavu souřadnic $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3\}$, kde $a = (1, -1, 1), \boldsymbol{u}_1 = \frac{1}{3}(2, 1, -2), \boldsymbol{u}_2 = \frac{1}{3}(2, -2, 1), \boldsymbol{u}_3 = \frac{1}{3}(1, 2, 2)$. Dále $f(a, \boldsymbol{u}_3) = -36$, $f_2(\boldsymbol{u}_1) = 6, f_2(\boldsymbol{u}_2) = 3$, takže paraboloid Q_{f_2} má vzhledem k soustavě souřadnic S rovnici $6x^2 + 3y^2 = 72z$ neboli kanonickou rovnici $\frac{x^2}{6} + \frac{y^2}{12} = 2z$. Odtud vidíme, že kvadrika Q_{f_2} je dvojosý eliptický paraboloid s vrcholem $(1, -1, 1)$, směrem osy $(1, 2, 2)$ a $\varepsilon_1 = 6, \varepsilon_2 = 12$.

26.1. Poznámka. Na tomto místě je účelné připomenout si některé poznatky z teorie lineárních forem a duálních vektorových prostorů. Duální prostor $\tilde{V}$ k vektorovému prostoru V je množina všech lineárních forem na prostoru V spolu s operacemi sčítání a skalárního násobku homomorfismů z definice 9.6. Je-li f netriviální lineární forma na vektorovém prostoru V_n, pak podle věty 11.14 je $\operatorname{Ker} f$ nadrovina ve V_n a obráceně každá nadrovina je nulovou množinou nějaké netriviální lineární formy na V_n. Přitom každá nadrovina $\operatorname{Ker} f \leq V_n$ je jednoznačně určena směrem $\langle f \rangle \leq \tilde{V}_n$. Dále, v definici 11.23 jsme každé podmnožině $M \subseteq V_n$ přiřadili podprostor $\Phi(M) = \{f \in \tilde{V}_n | f(M) = 0\}$ podprostoru $\tilde{V}_n$ a každé podmnožině $N \subseteq \tilde{V}_n$ podprostor $\Psi(N) = \cap_{f \in N} \operatorname{Ker} f$. Přitom podle věty 11.25 jsou Φ a Ψ vzájemně inverzní zobrazení mezi množinami všech podprostorů prostorů V_n a $\tilde{V}_n$. Je-li $W \leq V_{n+1}$ libovolný podprostor, budeme pro jednoduchost zápisu symbolem $P(W)$ rozumět podprostor projektivního prostoru $P_n(V_{n+1})$ vytvořený prostorem W, tj. $P(W) = \{\varphi(\langle \boldsymbol{u} \rangle) | 0 \neq \boldsymbol{u} \in W\}$.

26.2. Definice. Buď $P_n(V_{n+1})$ projektivní prostor. Označíme-li $\tilde{P}_n$ množinu všech nadrovin prostoru P_n a přiřadíme-li každému směru $\langle f \rangle$ z prostoru $\tilde{V}_{n+1}$ nadrovinu $P_{n-1}(\operatorname{Ker} f)$, dostaneme projektivní prostor $\tilde{P}_n(\tilde{V}_{n+1})$. Tento projektivní prostor se nazývá *duální projektivní prostor k prostoru* $P_n(V_{n+1})$.

26.3. Definice. Buď $P_n(V_{n+1})$ projektivní prostor a $\tilde{P}_n(\tilde{V}_{n+1})$ prostor k němu duální. Pro každý podprostor $P_k(V_{k+1})$ prostoru $P_n(V_{n+1})$ označíme $\Phi^*(P_k) = \tilde{P}(\Phi(V_{k+1}))$ a pro každý podprostor $\tilde{P}_l(\tilde{V}_{l+1})$ prostoru $P_n(V_{n+1})$ označíme $\Psi^*(\tilde{P}_l) = P(\Psi(\tilde{V}_{l+1}))$.

26.4. Věta. *Buď $P_n(V_{n+1})$ projektivní prostor a $\tilde{P}_n(\tilde{V}_{n+1})$ prostor k němu duální. Pak platí*

(i) zobrazení Φ^* je vzájemně jednoznačné zobrazení množiny všech podprostorů prostoru P_n na množinu všech podprostorů prostoru $\tilde{P}_n$ a zobrazení Ψ^* je k němu inverzní;

(ii) $\dim \Phi^*(P_k) = n - k - 1$, $\dim \Psi^*(\tilde{P}_l) = n - l - 1$;

(iii) $\Phi^*(P_k \vee P_l) = \Phi^*(P_k) \cap \Phi^*(P_l), \Phi^*(P_k \cap P_l) = \Phi^*(P_k) \vee \Phi^*(P_l)$;

(iv) $\Psi^*(\tilde{P}_k \vee \tilde{P}_l) = \Psi^*(\tilde{P}_k) \cap \Psi^*(\tilde{P}_l), \Psi^*(\tilde{P}_k \cap \tilde{P}_l) = \Psi^*(\tilde{P}_k) \vee \Psi^*(\tilde{P}_l)$.

Důkaz. (i) Plyne ihned z věty 11.25 (viz poznámka 26.1).

(ii) Plyne bezprostředně z věty 11.25 (iv) a (v).

(iii) Potřebujeme ověřit rovnosti $\Phi(V_{k+1} \vee V_{l+1}) = \Phi(V_{k+1}) \cap \Phi(V_{l+1})$ a $\Phi(V_{k+1} \cap V_{l+1}) = \Phi(V_{k+1} \vee \Phi(V_{l+1})$. Zřejmě platí $\Phi(V_{k+1} \vee V_{l+1}) = \{f \in \tilde{V}_{n+1} | V_{k+1} \vee V_{l+1} \subseteq \operatorname{Ker} f\} = \{f \in \tilde{V}_{n+1} | V_{k+1} \subseteq \operatorname{Ker} f\} \cap \{f \in \tilde{V}_{n+1} | V_{l+1} \subseteq \operatorname{Ker} f\} = \Phi(V_{k+1}) \cap \Phi(V_{l+1})$ a $\Phi(V_{k+1}) \vee \Phi(V_{l+1}) = \{f \in \tilde{V}_{n+1} | V_{k+1} \subseteq \operatorname{Ker} f\} \vee \{f \in \tilde{V}_{n+1} | V_{l+1} \subseteq \operatorname{Ker} f\} \subseteq \{f \in \tilde{V}_{n+1} | V_{k+1} \cap V_{l+1} \subseteq \operatorname{Ker} f\} = \Phi(V_{k+1} \cap V_{l+1})$. Přitom podle věty 11.25 (v) a podle věty o dimenzi spojení a průniku 2.23 je $\dim \Phi(V_{k+1} \cap V_{l+1}) = n + 1 - \dim(V_{k+1} \cap V_{l+1}) = n + 1 - (k + 1 + l + 1 - \dim(V_{k+1} \vee V_{l+1})) = n - k + n - l - (n + 1 - \dim(V_{k+1} \vee V_{l+1})) = n - k + n - l - \dim \Phi(V_{k+1} \vee V_{l+1}) = \dim \Phi(V_{k+1}) + \dim \Phi(V_{l+1}) - \dim(\Phi(V_{k+1}) \cap \Phi(V_{l+1})) = \dim(\Phi(V_{k+1}) \vee \Phi(V_{l+1}))$ (zde jsme použili již dokázanou rovnost). Podle věty 2.22 tedy je $\Phi(V_{k+1} \cap V_{l+1}) = \Phi(V_{k+1}) \vee \Phi(V_{l+1})$.

(iv) Podobně jako v předchozí části potřebujeme ověřit, že $\Psi(\tilde{V}_{k+1} \vee \tilde{V}_{l+1}) = \Psi(\tilde{V}_{k+1}) \cap \Psi(\tilde{V}_{l+1})$ a $\Psi(\tilde{V}_{k+1} \cap \tilde{V}_{l+1}) = \Psi(\tilde{V}_{k+1}) \vee \Psi(\tilde{V}_{l+1})$. Zřejmě platí $\Psi(\tilde{V}_{k+1} \vee \tilde{V}_{l+1}) = \bigcap_{f \in \tilde{V}_{k+1} \vee \tilde{V}_{l+1}} \operatorname{Ker} f = \bigcap_{f \in \tilde{V}_{k+1}} \operatorname{Ker} f \cap \bigcap_{f \in \tilde{V}_{l+1}} \operatorname{Ker} f = \Psi(\tilde{V}_{k+1}) \cap \Psi(\tilde{V}_{l+1})$ a $\Psi(\tilde{V}_{k+1}) \vee \Psi(\tilde{V}_{l+1}) = (\bigcap_{f \in \tilde{V}_{k+1}} \operatorname{Ker} f) \vee (\bigcap_{f \in \tilde{V}_{l+1}} \operatorname{Ker} f) \subseteq \bigcap_{f \in \tilde{V}_{k+1} \cap \tilde{V}_{l+1}} \operatorname{Ker} f = \Psi(\tilde{V}_{k+1} \cap \tilde{V}_{l+1})$. Přitom podle věty 11.25 (iv) a podle věty o dimenzi spojení a průniku 2.23 je $\dim \Psi(\tilde{V}_{k+1} \cap \tilde{V}_{l+1}) = n + 1 - \dim(\tilde{V}_{k+1} \cap \tilde{V}_{l+1}) = n + 1 - (k + 1 + l + 1 - \dim(\tilde{V}_{k+1} \vee \tilde{V}_{l+1}) = n - k + n - l - (n + 1 - \dim(\tilde{V}_{k+1} \vee \tilde{V}_{l+1})) = \dim \Psi(\tilde{V}_{k+1}) + \dim \Psi(\tilde{V}_{l+1}) - \dim \Psi(\tilde{V}_{k+1} \vee \tilde{V}_{l+1}) = \dim \Psi(\tilde{V}_{k+1}) - \dim(\Psi(\tilde{V}k + 1) \cap \Psi(\tilde{V}_{l+1})) = \dim(\Psi(\tilde{V}_{k+1}) \vee \Psi(\tilde{V}_{l+1}))$ a tedy $\Psi(\tilde{V}_{k+1} \cap \tilde{V}_{l+1}) = \Psi(\tilde{V}_{k+1}) \vee \Psi(\tilde{V}_{l+1})$ podle věty 2.22. ∎

26.5. Definice. Buď V nějaké tvrzení platné v libovolném projektivním prostoru $P_n(V_{n+1})$. Nahradíme-li v tvrzení V každý podprostor dimenze k podprostorem dimenze $n - k - 1$, každé spojení podprostorů průnikem odpovídajících podprostorů a naopak každý průnik podprostorů spojením odpovídajících podprostorů, dostaneme nové tvrzení $\tilde{V}$, které se nazývá *tvrzení duální k V*.

26.6. Princip duality. Jestliže tvrzení V je dokazatelné v projektivním prostoru $P_n(V_{n+1})$, pak i tvrzení duální $\tilde{V}$ je v tomto prostoru dokazatelné.

26.7. Poznámka. Princip duality není matematickou větou, ale, jak je patrné ze samotné formulace, větou o větách čili *metavětou*. Je to vlastně návod, jak dokazovat více vět najednou. Při důkazu duálního tvrzení $\tilde{V}$ můžeme totiž postupovat takto: Provedeme důkaz tvrzení V v duálním prostoru $\tilde{P}_n$ a pomocí zobrazení Ψ^* přeneseme tento důkaz do prostoru P_n.

Pojem dualizace si můžeme ilustrovat na tomto jednoduchém příkladě. Duální větou k větě „Každé dvě různé přímky v projektivní rovině P_2 se protínají v jediném bodě" je věta „Každými dvěma různými body v P_2 lze vést jedinou přímku". Dualita těchto dvou tvrzení je okamžitě patrná, jestliže použijeme obvyklou matematickou symboliku. Tvrzení V lze totiž zapsat takto: $(P_1 \neq P_1' \Rightarrow P_1 \cap P_1' = P_0)$ a tvrzení $\tilde{V}$ má tento zápis: $(P_0 \neq P_0' \Rightarrow P_0 \vee P_0' = P_1)$.

26.8. Věta. *Buď f_2 regulární kvadratická forma na vektorovém prostoru V_n nad tělesem T, $\operatorname{char} T \neq 2$, a buď f polární bilineární forma formy f_2. Pak zobrazení $\tilde{f}_2 : \tilde{V}_n \to T$ definované pro $\tilde{u} \in \tilde{V}_n$ předpisem $\tilde{f}_2(\tilde{u}) = f_2((\Phi^f)^{-1}(\tilde{u}))$ je kvadratická forma na prostoru $\tilde{V}_n$.*

Důkaz. Podle věty 12.15 je zobrazení $\Phi^f : V_n \to \tilde{V}_n$ izomorfismus, takže $\tilde{f}_2(\tilde{u})$ má smysl pro každé $\tilde{u} \in \tilde{V}_n$. Jestliže nyní položíme $\tilde{f}(\tilde{u}, \tilde{v}) = f((\Phi^f)^{-1}(\tilde{u}), (\Phi^f)^{-1}(\tilde{v}))$ pro libovolné dva prvky $\tilde{u}, \tilde{v} \in \tilde{V}$, pak není obtížné ověřit, že $\tilde{f}$ je symetrická bilineární forma na $\tilde{V}_n$ vytvářející kvadratickou formu $\tilde{f}_2$. ∎

26.9. Definice. *Duální kvadrikou* rozumíme kvadriku v duálním projektivním prostoru $\tilde{P}_n(\tilde{V}_{n+1})$. Je-li Q_{f_2} regulární kvadrika v projektivním prostoru $P_n(V_{n+1})$ nad tělesem T charakteristiky různé od 2, pak duální kvadriku $Q_{\tilde{f}_2}$ v duálním prostoru $\tilde{P}_n(\tilde{V}_{n+1})$ nazýváme *dualizací kvadriky Q_{f_2}*.

26.10. Věta. *Buď Q_{f_2} regulární kvadrika v projektivním prostoru $P_n(V_{n+1})$ nad tělesem T charakteristiky různé od 2. Je-li $\boldsymbol{A}$ matice formy f_2 vzhledem k nějaké* *aritmetické bázi M prostoru P_n, pak A^{-1} je matice formy $\tilde{f}_2$ vzhledem k aritmetické bázi $\tilde{M}$ prostoru $\tilde{P}_n$ duální k M.*

Důkaz. Nechť $M = \{u_0, u_1, \ldots, u_n\}$ a $\tilde{M} = \{\tilde{u}_0, \tilde{u}_1, \ldots, \tilde{u}_n\}$. Podle věty 12.15 je A matice izomorfismu $\Phi^f : V_{n+1} \to \tilde{V}_{n+1}$ vzhledem k bázím M a $\tilde{M}$, takže podle věty 10.8 je $A^{-1} = B = (b_{ij})$ matice izomorfismu $(\Phi^f)^{-1} : \tilde{V}_{n+1} \to V_{n+1}$ vzhledem k bázím $\tilde{M}$ a M. K dokončení důkazu zbývá nyní ověřit, že B je matice formy $\tilde{f}_2$ vzhledem k bázi $\tilde{M}$. Jest $\tilde{f}(\tilde{u}_i, \tilde{u}_j) = f((\Phi^f)^{-1}(u_i), (\Phi^{\tilde{f}})^{-1}(\tilde{u}_j))$ $= f(\sum_{k=0}^n b_{ki}u_k, \sum_{l=0}^n b_{lj}u_l) = \sum_{k=0}^n \sum_{l=0}^n b_{ki}b_{lj}a_{kl} = \sum_{k=0}^n b_{ki}\delta_{kj} = b_{ji} = b_{ij}$ vzhledem k tomu, že $AB = E$ a že podle věty 8.12 je matice B symetrická. ■

26.11. Poznámka. Buď Q_{f_2} regulární kvadrika v projektivním prostoru $A_n(V_n)$. Je-li $\langle u \rangle \in P_n$ libovolný bod, pak podle poznámky 23.7 je $P(\operatorname{Ker} \Phi^f(u))$ polární nadrovina bodu u vzhledem ke Q_{f_2}. Je-li speciálně $\langle u \rangle \in Q_{f_2}$, je $P(\operatorname{Ker}\Phi^f(u))$ tečná nadrovina kvadriky Q_{f_2} v bodě $\langle u \rangle$. Protože $\tilde{f}_2(\Phi^f(u)) = f_2(u)$, je $\langle u \rangle \in Q_{f_2}$, právě když $P(\operatorname{Ker} \Phi^f(u)) \in Q_{\tilde{f}_2}$, tedy dualizace $Q_{\tilde{f}_2}$ kvadriky Q_{f_2} je množina právě všech tečných nadrovin kvadriky Q_{f_2}. Protože obecná rovnice kuželosečky má šest koeficientů, které jsou určeny jednoznačně až na (nenulový) násobek, stačí k určení kuželosečky pět prvků, mezi které patří body a tečny, případně pól a polára. Použití předchozí věty nám tak umožňuje například určovat kuželosečky dané pěti tečnami. Protože u paraboly je nevlastní přímka tečnou, stačí k určení paraboly čtyři body.

26.12. Příklady. V afinní rovině $A_2(R^2)$ nalezněme rovnici kuželosečky Q_{f_2} vzhledem k soustavě souřadnic S sestávající z bodu $(0,0)$ a kanonické báze $K = \{e_1, e_2\}$ prostoru R^2, víme-li, že:

(a) Q_{f_2} je parabola dotýkající se souřadnicových os a přímek o rovnicích $x - y + 2 = 0, x + y - 1 = 0$;

(b) Q_{f_2} prochází bodem $(1, -1)$ a dotýká se přímek $y - 1 = 0$ a $2x + y + 1 = 0$ v bodech $(0, 1)$ a $(0, -1)$.

Ř e š e n í : (a) V homogenní soustavě souřadnic $\bar{S}$ indukované S v projektivním rozšíření $\bar{A}_2$ mají souřadnicové osy a dané přímky rovnice $x_1 = 0, x_2 = 0, 2x_0 + x_1 - x_2 = 0, x_0 - x_1 - x_2 = 0$. Tečnou paraboly je podle definice ještě nevlastní přímka o rovnici $x_0 = 0$. Podle věty 11.7 jsou souřadnice daných lineárních forem vzhledem k bázi $\tilde{\bar{S}}$ duální k $\bar{S}$ rovny $(0,1,0), (0,0,1), (2,1,-1), (1,-1-1)$ a $(1,0,0)$. Dualizace $Q_{\tilde{f}_2}$ dané paraboly tedy musí procházet těmito pěti body. Jestliže tedy rovnice této kuželosečky vzhledem k bázi $\tilde{\bar{S}}$ je $ax^2 + 2bx_0x_1 + 2cx_0x_2 + dx_1^2 + 2ex_1x_2 + fx_2^2 = 0$, pak dosazením jednotlivých bodů dostaneme homogenní soustavu lineárních rovnic

$$\begin{aligned} d \qquad\qquad &= 0, \\ f &= 0, \\ 4a + 4b - 4c + d - 2e + f &= 0, \\ a - 2b - 2c + d + 2e + f &= 0, \\ a \qquad\qquad &= 0. \end{aligned}$$

Řešením této soustavy je např. $a = d = f = 0$, $b = 3, c = 1, e = 4$, takže dualizace $Q_{\tilde{f}_2}$ je vytvořena kvadratickou formou $\tilde{f}_2$, mající vzhledem k $\tilde{\bar{S}}$ matici

$$A = \begin{pmatrix} 0, & 3, & 1 \\ 3, & 0, & 4 \\ 1, & 4, & 0 \end{pmatrix}.$$

Podle věty 26.10 je matice A^{-1} maticí dané paraboly vzhledem k bázi $\bar{S}$. Protože rovnice kvadriky je určena jednoznačně až na násobek, stačí nám vzhledem k větě 8.12 nalézt matici adjungovanou $\bar{A}$. Jest

$$\bar{A} = \begin{pmatrix} -16, & 4, & 12 \\ 4, & -1, & 3 \\ 12, & 3, & -9 \end{pmatrix},$$

hledaná rovnice paraboly tedy je $-16x_0^2 + 8x_0x_1 + 24x_0x_2 - x_1^2 + 6x_1x_2 - 9x_2^2 = 0$, a tedy v soustavě souřadnic S $x^2 - 6xy + 9x^2 - 8x - 24y + 16 = 0$.

(b) Podobně jako v předchozím příkladě dostaneme dosazením bodů $(1, 0, 1)$, $(1, 0, -1)$ a $(1, 1, -1)$ do obecné rovnice homogenní soustavu lineárních rovnic

$$\begin{aligned} a \quad\quad + 2c \quad\quad\quad\quad + f &= 0, \\ a \quad\quad - 2c \quad\quad\quad\quad + f &= 0, \\ a + 2b - 2c + d - 2e + f &= 0, \end{aligned}$$

odkud plyne $c = 0, f = -a, d = 2(e - b)$. Matice kuželosečky Q_{f_2} má tedy tvar

$$A = \begin{pmatrix} a, & b, & 0 \\ b, & 2(e-b), & e \\ 0, & e, & -a \end{pmatrix}.$$

Pro dualizaci $Q_{\bar{f}_2}$ kvadriky Q_{f_2} můžeme použít matici adjungovanou $\bar{A}$, přičemž víme, že $Q_{\bar{f}_2}$ prochází body $(1, 0, -1)$ a $(1, 2, 1)$. Máme tedy

$$\bar{A} = \begin{pmatrix} -2a(e-b) - e^2, & ab, & be \\ ab, & -a^2, & -ae \\ be, & -ae, & 2a(e-b) - b^2 \end{pmatrix}$$

a soustavu rovnic

$$\begin{aligned} -2a(e-b) - e^2 - 2be + 2a(e-b) - b^2 &= 0, \\ -2a(e-b) - e^2 + 4ab + 2be - 4a^2 - 4ae + 2a(e-b) - b^2 &= 0, \end{aligned}$$

neboli $(e + b)^2 = 0$, a tedy $e = -b$. Dosazením do druhé rovnice pak máme $-b^2 + 4ab - 2b^2 - 4a^2 + 4ab - b^2 = 0$, tedy $-4(a - b)^2 = 0$ a $a = b$. Zvolíme-li nyní např. $a = -1$, dostaneme

$$A = \begin{pmatrix} -1, & -1, & 0 \\ -1, & 4, & 1 \\ 0, & 1, & 1 \end{pmatrix},$$

takže hledaná rovnice kuželosečky Q_{f_2} je $-x_0^2 - 2x_0x_1 + 4x_1^2 + 2x_1x_2 + x_2^2 = 0$, a tedy v soustavě souřadnic S $4x^2 + 2xy + y^2 - 2x - 1 = 0$.

27.1. Poznámka. Vektorové prostory můžeme vyšetřovat nad libovolným tělesem. V předchozím textu jsme však viděli, že reálné a komplexní vektorové prostory mají v některých případech zvláštní postavení. U prostorů reálných se jedná zejména o možnost rozlišování kladných a záporných prvků, což se projevilo zejména při zkoumání signatury kvadratických forem. Na druhé straně všude tam, kde se vyskytují kořeny polynomů, jsme pracovali nad tělesem komplexních čísel nebo nad tělesem algebraicky uzavřeným. V tomto směru připomeňme např. kanonický tvar matice, nebo samodružné body kolineace. Zvláštní postavení tělesa reálných čísel a tělesa komplexních čísel je navíc zvýrazněno ještě tím, že těleso R je podtělesem tělesa K. Jak víme, těleso komplexních čísel vznikne poměrně jednoduchou konstrukcí z tělesa čísel reálných. Ukážeme si nyní, že stejný postup lze aplikovat i na konstrukci komplexního vektorového prostoru z vektorového prostoru reálného.

27.2. Komplexní rozšíření reálného vektorového prostoru.
Buď V vektorový prostor nad tělesem reálných čísel. Množina V^* všech uspořádaných dvojic $(\boldsymbol{u}_1, \boldsymbol{u}_2)$ vektorů z V tvoří, jak se snadno ověří, spolu s operacemi sčítání vektorů $(\boldsymbol{u}_1, \boldsymbol{u}_2) + (\boldsymbol{v}_1, \boldsymbol{v}_2) = (\boldsymbol{u}_1 + \boldsymbol{v}_1, \boldsymbol{u}_2 + \boldsymbol{v}_2)$ a násobení komplexním číslem $(r + is)(\boldsymbol{u}_1, \boldsymbol{u}_2) = (r\boldsymbol{u}_1 - s\boldsymbol{u}_2, s\boldsymbol{u}_1 + r\boldsymbol{u}_2)$ komplexní vektorový prostor, který se nazývá *komplexní rozšíření vektorového prostoru V*. Protože každý komplexní vektorový prostor je zároveň reálným vektorovým prostorem, můžeme zkoumat zobrazení $f : V \to V^*$ definované předpisem $f(\boldsymbol{u}) = (\boldsymbol{u}, 0)$. Jelikož $f(\boldsymbol{u} + \boldsymbol{v}) = (\boldsymbol{u} + \boldsymbol{v}, 0) = (\boldsymbol{u}, 0) + (\boldsymbol{v}, 0) = f(\boldsymbol{u}) + f(\boldsymbol{v})$ a $f(r\boldsymbol{u}) = (r\boldsymbol{u}, 0) = r(\boldsymbol{u}, 0) = rf(\boldsymbol{u})$ je f zřejmě monomorfismus reálného vektorového prostoru V do reálného vektorového prostoru V^*. Proto můžeme podobně jako v případě komplexních čísel dvojici $(\boldsymbol{u}, 0)$ ztotožnit s vektorem $\boldsymbol{u}$ a dvojici $(0, \boldsymbol{u})$ označit jako $i\boldsymbol{u}$. Pak pro vektor $(\boldsymbol{u}_1, \boldsymbol{u}_2) \in V^*$ dostaneme analogický zápis jako pro komplexní čísla, totiž $\boldsymbol{u}_1 + i\boldsymbol{u}_2$.

27.3. Věta. *Buďte V, V' vektorové prostory nad tělesem reálných čísel R a buď $f : V \to V'$ homomorfismus. Pak existuje právě jeden homomorfismus f^* komplexního rozšíření V^* vektorového prostoru V do komplexního rozšíření V'^* vektorového prostoru V' takový, že $f^*|V = f$. Homomorfismus f^* je přitom dán předpisem $f^*(\boldsymbol{u}_1 + i\boldsymbol{u}_2) = f(\boldsymbol{u}_1) + if(\boldsymbol{u}_2)$ a platí $\operatorname{Ker} f^* = (\operatorname{Ker} f)^*$.*

Důkaz. Protože pro $\boldsymbol{u} \in V$ je $f^*(\boldsymbol{u}) = f(\boldsymbol{u})$, je jednoznačnost zřejmá a jediné, co je potřeba ověřit, je, že $f^* : V^* \to V'^*$ je homomorfismus komplexních vektorových prostorů. Jest $f^*((\boldsymbol{u}_1 + i\boldsymbol{u}_2) + (\boldsymbol{v}_1 + i\boldsymbol{v}_2)) = f^*(\boldsymbol{u}_1 + \boldsymbol{v}_1 + i(\boldsymbol{u}_2 + \boldsymbol{v}_2)) = f(\boldsymbol{u}_1 + \boldsymbol{v}_1) + if(\boldsymbol{u}_2 + \boldsymbol{v}_2) = f(\boldsymbol{u}_1) + f(\boldsymbol{v}_1) + if(\boldsymbol{u}_2) + if(\boldsymbol{v}_2) = f^*(\boldsymbol{u}_1 + i\boldsymbol{u}_2) + f^*(\boldsymbol{v}_1 + i\boldsymbol{v}_2)$ a $f^*((r+is)(\boldsymbol{u}_1 + i\boldsymbol{u}_2)) = f^*(r\boldsymbol{u}_1 - s\boldsymbol{u}_2 + i(s\boldsymbol{u}_1 + r\boldsymbol{u}_2)) = f(r\boldsymbol{u}_1 - s\boldsymbol{u}_2) + if(s\boldsymbol{u}_1 + r\boldsymbol{u}_2) = rf(\boldsymbol{u}_1) - sf(\boldsymbol{u}_2) + isf(\boldsymbol{u}_1) + irf(\boldsymbol{u}_2) = (r+is)(f(\boldsymbol{u}_1) + if(\boldsymbol{u}_2)) = (r+is)f^*(\boldsymbol{u}_1 + i\boldsymbol{u}_2)$. Přitom $f^*(\boldsymbol{u}_1 + i\boldsymbol{u}_2) = 0$, právě když $f(\boldsymbol{u}_1) = f(\boldsymbol{u}_2) = 0$, takže $\operatorname{Ker} f^* = (\operatorname{Ker} f)^*$. ■

27.4. Věta. *Buď V_n n-rozměrný reálný vektorový prostor. Pak platí*
(i) dimenze V_n^* nad tělesem komplexních čísel $\dim_K V_n^*$ je rovna n;
(ii) dimenze V_n^* nad tělesem reálných čísel $\dim_R V_n^*$ je rovna $2n$.

Důkaz. (i) Nechť $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ je nějaká báze vektorového prostoru V_n. Je-li $\boldsymbol{u} + i\boldsymbol{v} \in V_n^*$ libovolný vektor, je $\boldsymbol{u} = \sum_{j=1}^n r_j \boldsymbol{u}_j$ a $\boldsymbol{v} = \sum_{j=1}^n s_j \boldsymbol{u}_j$ pro nějaká reálná čísla $r_j, s_j, j = 1, 2, \ldots, n$. Pak ale $\boldsymbol{u} + i\boldsymbol{v} = \sum_{j=1}^{n} r_j \boldsymbol{u}_j + i \sum_{j=1}^{n} s_j \boldsymbol{u}_j = \sum_{j=1}^{n} (r_j + is_j)\boldsymbol{u}_j$ a množina M generuje prostor V_n^*. Kromě toho pro $\sum_{j=1}^{n}(r_j + is_j)\boldsymbol{u}_j = 0$ je $\sum_{j=1}^{n} r_j \boldsymbol{u}_j = 0$ a $\sum_{j=1}^{n} s_j \boldsymbol{u}_j = 0$, takže $r_j + is_j = 0$ pro každé $j = 1, 2, \ldots, n$ a M je báze prostoru V_n^*.

(ii) Ukážeme si, že množina $N = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n, i\boldsymbol{u}_1, i\boldsymbol{u}_2, \ldots, i\boldsymbol{u}_n\}$ je bází prostoru V_n^* nad tělesem reálných čísel R. Protože pro každé $\boldsymbol{u} + i\boldsymbol{v} \in V_n^*$ je $\boldsymbol{u} + i\boldsymbol{v} = \sum_{j=1}^{n}(r_j + is_j)\boldsymbol{u}_j$ pro nějaká reálná čísla $r_j, s_j, j = 1, 2, \ldots, n$, množina N zřejmě generuje V_n^* nad R. Jestliže nyní $\sum_{j=1}^{n} r_j \boldsymbol{u}_j + \sum_{j=1}^{n} s_j i\boldsymbol{u}_j = 0$ pro nějaká reálná čísla $r_j, s_j, j = 1, 2, \ldots, n$, pak $\sum_{j=1}^{n}(r_j + is_j)\boldsymbol{u}_j = 0$, takže $r_j = s_j = 0$, $j = 1, 2, \ldots, n$, a množina N je lineárně nezávislá nad R. ■

27.5. Definice. Buď $P_n(V_{n+1})$ reálný projektivní prostor. Komplexní projektivní prostor $P_n(V_{n+1}^*)$ nazýváme *komplexním rozšířením projektivního prostoru* $P_n(V_{n+1})$.

27.6. Věta. *Buď f bilineární forma na reálném vektorovém prostoru V. Definujeme-li zobrazení $f^* : V^* \times V^* \to K$ předpisem $f^*(\boldsymbol{u}_1 + i\boldsymbol{u}_2, \boldsymbol{v}_2 + i\boldsymbol{v}_2) = f(\boldsymbol{u}_1, \boldsymbol{v}_1) - f(\boldsymbol{u}_2, \boldsymbol{v}_2) + i(f(\boldsymbol{u}_1, \boldsymbol{v}_2) + f(\boldsymbol{u}_2, \boldsymbol{v}_1))$, pak platí*

(i) f^* je bilineární forma na V^*;

(ii) f^* je symetrická, právě když f je symetrická;

(iii) je-li $\dim V = n$ a $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ je polární báze formy f, pak M je polární báze formy f^*.

Důkaz. (i) Tvrzení se snadno ověří přímým výpočtem, takže důkaz lze přenechat čtenáři jako snadné cvičení.

(ii) Je-li f^* symetrická, pak pro libovolné dva vektory $\boldsymbol{u}, \boldsymbol{v} \in V$ platí $f(\boldsymbol{v}, \boldsymbol{u}) = f^*(\boldsymbol{v}, \boldsymbol{u}) = f^*(\boldsymbol{u}, \boldsymbol{v}) = f(\boldsymbol{u}, \boldsymbol{v})$. Buď tedy naopak forma f symetrická. Pak $f^*(\boldsymbol{v}_1 + i\boldsymbol{v}_2, \boldsymbol{u}_1 + i\boldsymbol{u}_2) = f(\boldsymbol{v}_1, \boldsymbol{u}_1) - f(\boldsymbol{v}_2, \boldsymbol{u}_2) + i(f(\boldsymbol{v}_1, \boldsymbol{u}_2) + f(\boldsymbol{v}_2, \boldsymbol{u}_1)) = f(\boldsymbol{u}_1, \boldsymbol{v}_1) - f(\boldsymbol{u}_2, \boldsymbol{v}_2) + i(f(\boldsymbol{u}_2, \boldsymbol{v}_1) + f(\boldsymbol{u}_1, \boldsymbol{v}_1)) = f^*(\boldsymbol{u}_1 + i\boldsymbol{u}_2, \boldsymbol{v}_1 + i\boldsymbol{v}_2)$.

(iii) Pro všechna $j, k \in \{1, 2, \ldots, n\}$, $j \neq k$, je zřejmě $f^*(\boldsymbol{u}_j, \boldsymbol{u}_k) = f(\boldsymbol{u}_j, \boldsymbol{u}_k) = 0$.
■

27.7. Definice. Je-li f bilineární forma na reálném vektorovém prostoru V, pak forma f^* na prostoru V^* definovaná v předchozí větě se nazývá *komplexní rozšíření formy f*. Je-li Q_{f_2} kvadrika v reálném projektovém prostoru $P_n(V_{n+1})$, pak *komplexním rozšířením této kvadriky* rozumíme kvadriku $Q_{f_2^*}$ v komplexním rozšíření $P_n(V_{n+1}^*)$ projektivního prostoru $P_n(V_{n+1})$.

27.8. Poznámka. Ve větě 23.21 jsme ukázali, že v komplexním projektivním prostoru $P_n(V_{n+1})$ určuje každá kvadrika Q_{f_2} vytvářející kvadratickou formu f_2 až na násobek jednoznačně. Stručně řečeno $Q_{f_2} = Q_{g_2}$, právě když $f_2 = rg_2$ pro nějaké nenulové komplexní číslo r. Podle věty 23.22 platí stejné tvrzení i v reálných projektivních prostorech za předpokladu, že kvadriky Q_{f_2} a Q_{g_2} obsahují alespoň jeden bod ležící mimo vrchol. Zatímco tedy množina všech reálných bodů obecně neurčuje vytvořující formu f_2 jednoznačně (viz poznámka 23.23), množina všech komplexních bodů tuto formu určuje jednoznačně.

27.9. Věta. *Nechť Q_{f_2} a Q_{g_2} jsou dvě kvadriky v reálném projektivním prostoru $P_n(V_{n+1})$. Pak $Q_{f_2^*} = Q_{g_2^*}$ v komplexním rozšíření $P_n(V_{n+1}^*)$, právě když $g_2 = rf_2$ pro nějaké nenulové reálné číslo r.*

Důkaz. Je-li $g_2 = rf_2$ pro nějaké $0 \neq r \in R$, pak $g_2^* = rf_2^*$, a tedy zřejmě $Q_{f_2}^* = Q_{g_2}^*$. Nechť tedy naopak $Q_{f_2}^* = Q_{g_2}^*$. Podle věty 23.21 existuje nenulové komplexní číslo $r + is$ takové, že $g_2^* = (r + is)f_2^*$. Pak ale pro každé $\boldsymbol{u} \in V_{n+1}$ je $g_2(\boldsymbol{u}) = g_2^*(\boldsymbol{u}) = (r + is)f_2^*(\boldsymbol{u}) = rf_2(\boldsymbol{u}) + isf_2(\boldsymbol{u})$, odkud předně plyne $s = 0$, takže $r \neq 0$, $g_2(\boldsymbol{u}) = rf_2(\boldsymbol{u})$ a $g_2 = rf_2$. ■

27.10. Věta. *Buď $A(V)$ afinní prostor nad reálným vektorovým prostorem V. Označíme-li $A^* = A \times V$ množinu všech uspořádaných dvojic $(a, \boldsymbol{u})$, $a \in A$, $\boldsymbol{u} \in V$, pak $A^*(V^*)$ je afinní prostor nad komplexním rozšířením V^* vektorového prostoru V, jestliže definujeme $(a, \boldsymbol{u}) + (\boldsymbol{v}, \boldsymbol{w}) = (a + \boldsymbol{v}, \boldsymbol{u} + \boldsymbol{w})$ a $(a, \boldsymbol{u}) - (b, \boldsymbol{v}) = (a - b, \boldsymbol{u} - \boldsymbol{v})$. Přitom zobrazení $F : A \to A^*$ definované pro každé $a \in A$ a každé $\boldsymbol{u} \in V$ předpisem $F(a + \boldsymbol{u}) = (a + \boldsymbol{u}, 0)$ je regulární afinní zobrazení vytvořené homomorfismem $f : V \to V^*$ z odstavce 27.2.*

Důkaz. Skutečnost, že $A^*(V^*)$ je afinní prostor, se s ohledem na poznámku 19.2 ověří velmi snadno. Protože $f : V \to V^*, f(\boldsymbol{u}) = (\boldsymbol{u}, 0)$, je podle odstavce 27.2 injektivní homomorfismus reálného vektorového prostoru V do reálného vektorového prostoru V^* a $F(a + \boldsymbol{u}) = (a + \boldsymbol{u}, 0) = (a, 0) + (\boldsymbol{u}, 0) = (a, 0) + f(\boldsymbol{u})$, je F regulární afinní zobrazení vytvořené monomorfismem f. ■

27.11. Definice. Komplexní afinní prostor $A^*(V^*)$ z předchozí věty se nazývá *komplexní rozšíření afinního prostoru $A(V)$*. Podobně jako v odstavci 27.2 budeme místo $(a, \boldsymbol{u})$ psát $a + i\boldsymbol{u}$.

27.12. Věta. *Buď g pozitivně definitní bilineární forma na reálném vektorovém prostoru V_n. Pak zobrazení $g^* : V_n^* \times V_n^* \to K$ definované předpisem $g^*(\boldsymbol{u}_1 + i\boldsymbol{u}_2, \boldsymbol{v}_1 + i\boldsymbol{v}_2) = g(\boldsymbol{u}_1, \boldsymbol{v}_1) + g(\boldsymbol{u}_2, \boldsymbol{v}_2) + i(g(\boldsymbol{u}_2, \boldsymbol{v}_1) - g(\boldsymbol{u}_1, \boldsymbol{v}_2))$ splňuje pro všechna $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in V_n^*$ a všechna $\alpha \in K$ následující podmínky:*

(1) $g^*(\boldsymbol{u} + \boldsymbol{v}, \boldsymbol{w}) = g^*(\boldsymbol{u}, \boldsymbol{w}) + g^*(\boldsymbol{v}, \boldsymbol{w})$;
(2) $g^*(\boldsymbol{u}, \boldsymbol{v} + \boldsymbol{w}) = g^*(\boldsymbol{u}, \boldsymbol{v}) + g^*(\boldsymbol{u}, \boldsymbol{w})$;
(3) $g^*(\alpha \boldsymbol{u}, \boldsymbol{v}) = \alpha g^*(\boldsymbol{u}, \boldsymbol{v})$;
(4) $g^*(\boldsymbol{u}, \alpha \boldsymbol{v}) = \bar{\alpha} g^*(\boldsymbol{u}, \boldsymbol{v})$;
(5) $g^*(\boldsymbol{v}, \boldsymbol{u}) = \overline{g^*(\boldsymbol{u}, \boldsymbol{v})}$;
(6) $g_2^*(\boldsymbol{u}) \geq 0$, *přičemž* $g_2^*(\boldsymbol{u}) = 0$, *právě když* $\boldsymbol{u} = 0$.

Důkaz. Nechť $\boldsymbol{u} = \boldsymbol{u}_1 + i\boldsymbol{u}_2, \boldsymbol{v} = \boldsymbol{v}_1 + i\boldsymbol{v}_2, \boldsymbol{w} = \boldsymbol{w}_1 + i\boldsymbol{w}_2$ a $\alpha = r + is, r, s \in R$.

(1) Jest $g^*(\boldsymbol{u}+\boldsymbol{v}, \boldsymbol{w}) = g^*(\boldsymbol{u}_1+\boldsymbol{v}_1+i(\boldsymbol{u}_2+\boldsymbol{v}_2), \boldsymbol{w}_1+\boldsymbol{w}_2) = g(\boldsymbol{u}_1+\boldsymbol{v}_1, \boldsymbol{w}_1)+g(\boldsymbol{u}_2+\boldsymbol{v}_2, \boldsymbol{w}_2) + i(g(\boldsymbol{u}_2 + \boldsymbol{v}_2, \boldsymbol{w}_2) - g(\boldsymbol{u}_1 + \boldsymbol{v}_1, \boldsymbol{w}_2)) = g(\boldsymbol{u}_1, \boldsymbol{w}_1) + g(\boldsymbol{v}_1, \boldsymbol{w}_1) + g(\boldsymbol{u}_2, \boldsymbol{w}_2) + g(\boldsymbol{v}_2, \boldsymbol{w}_2) + i(g(\boldsymbol{u}_2, \boldsymbol{w}_1) + g(\boldsymbol{v}_2, \boldsymbol{w}_1) - g(\boldsymbol{u}_1, \boldsymbol{w}_2) - g(\boldsymbol{v}_1, \boldsymbol{w}_2)) = g^*(\boldsymbol{u}, \boldsymbol{w}) + g^*(\boldsymbol{v}, \boldsymbol{w})$.

(2) Analogicky jako (1).

(3) Máme $g^*(\alpha\boldsymbol{u}, \boldsymbol{v}) = g^*((r + is)(\boldsymbol{u}_1 + i\boldsymbol{u}_2), \boldsymbol{v}_1 + i\boldsymbol{v}_2) = g(r\boldsymbol{u}_1 - s\boldsymbol{u}_2, \boldsymbol{v}_1) + g(s\boldsymbol{u}_1 + r\boldsymbol{u}_2, \boldsymbol{v}_2) + i(g(s\boldsymbol{u}_1 + r\boldsymbol{u}_2, \boldsymbol{v}_1) - g(r\boldsymbol{u}_1 - s\boldsymbol{u}_2, \boldsymbol{v}_2)) = rg(\boldsymbol{u}_1, \boldsymbol{v}_1) - sg(\boldsymbol{u}_2, \boldsymbol{v}_1) + sg(\boldsymbol{u}_1, \boldsymbol{v}_2) + rg(\boldsymbol{u}_2, \boldsymbol{v}_2) + i(sg(\boldsymbol{u}_1, \boldsymbol{v}_1) + rg(\boldsymbol{u}_2, \boldsymbol{v}_1) - rg(\boldsymbol{u}_1, \boldsymbol{v}_2) + sg(\boldsymbol{u}_2, \boldsymbol{v}_2))$. Podobně $\alpha g^*(\boldsymbol{u}, \boldsymbol{v}) = (r + is)(g(\boldsymbol{u}_1, \boldsymbol{v}_1) + g(\boldsymbol{u}_2, \boldsymbol{v}_2) + i(g(\boldsymbol{u}_2, \boldsymbol{v}_1) - g(\boldsymbol{u}_1, \boldsymbol{v}_2)) = rg(\boldsymbol{u}_1, \boldsymbol{v}_1) + rg(\boldsymbol{u}_2, \boldsymbol{v}_2) - sg(\boldsymbol{u}_2, \boldsymbol{v}_1) + sg(\boldsymbol{u}_1, \boldsymbol{v}_2) + i(sg(\boldsymbol{u}_1, \boldsymbol{v}_1) + sg(\boldsymbol{u}_2, \boldsymbol{v}_2) + rg(\boldsymbol{u}_2, \boldsymbol{v}_2) - rg(\boldsymbol{u}_1, \boldsymbol{v}_2))$, odkud porovnáním dostáváme požadovanou rovnost.

(4) Analogicky jako v předchozím případě jest $g^*(\boldsymbol{u}, \alpha\boldsymbol{v}) = g^*(\boldsymbol{u}_1 + i\boldsymbol{u}_2, (r + is)(\boldsymbol{v}_1 + i\boldsymbol{v}_2)) = g(\boldsymbol{u}_1, r\boldsymbol{v}_1 - s\boldsymbol{v}_2) + g(\boldsymbol{u}_2, s\boldsymbol{v}_1 + r\boldsymbol{v}_2) + i(g(\boldsymbol{u}_2, r\boldsymbol{v}_1 - s\boldsymbol{v}_2) - g(\boldsymbol{u}_1, s\boldsymbol{v}_1 + r\boldsymbol{v}_2)) = rg(\boldsymbol{u}_1, \boldsymbol{v}_1) - sg(\boldsymbol{u}_1, \boldsymbol{v}_2) + sg(\boldsymbol{u}_2, \boldsymbol{v}_1) + rg(\boldsymbol{u}_2, \boldsymbol{v}_2) + i(rg(\boldsymbol{u}_2, \boldsymbol{v}_1) - sg(\boldsymbol{u}_2, \boldsymbol{v}_2) -$

$sg(\boldsymbol{u}_1, \boldsymbol{v}_1) - rg(\boldsymbol{u}_1, \boldsymbol{v}_2))$ a $\bar{\alpha}g^*(\boldsymbol{u}, \boldsymbol{v}) = (r - is)(g(\boldsymbol{u}_1, \boldsymbol{v}_1) + g(\boldsymbol{u}_2, \boldsymbol{v}_2) + i(g(\boldsymbol{u}_2, \boldsymbol{v}_1) - g(\boldsymbol{u}_1, \boldsymbol{v}_1) = rg(\boldsymbol{u} - 1, \boldsymbol{v}_1) + rg(\boldsymbol{u}_2, \boldsymbol{v}_2) + sg(\boldsymbol{u}_2, \boldsymbol{v}_1) - sg(\boldsymbol{u}_1, \boldsymbol{v}_2) + i(-sg(\boldsymbol{u}_1, \boldsymbol{v}_1) - sg(\boldsymbol{u}_2, \boldsymbol{v}_2) + rg(\boldsymbol{u}_2, \boldsymbol{v}_1) - rg(\boldsymbol{u}_1, \boldsymbol{v}_2)$, odkud daná rovnost plyne.

(5) Jest $g^*(\boldsymbol{v}, \boldsymbol{u}) = g(\boldsymbol{v}_1, \boldsymbol{u}_1) + g(\boldsymbol{v}_2, \boldsymbol{u}_2) + i(g(\boldsymbol{v}_2, \boldsymbol{u}_1) - g(\boldsymbol{v}_1, \boldsymbol{u}_2)) = g(\boldsymbol{u}_1, \boldsymbol{v}_1) + g(\boldsymbol{u}_2, \boldsymbol{v}_2) - i(g(\boldsymbol{u}_2, \boldsymbol{v}_1) - g(\boldsymbol{u}_1, \boldsymbol{v}_1)) = \overline{g^*(\boldsymbol{u}, \boldsymbol{v})}$.

(6) Máme $g_2^*(\boldsymbol{u}) = g^*(\boldsymbol{u}, \boldsymbol{u}) = g_2(\boldsymbol{u}_1) + g_2(\boldsymbol{u}_2) \geq 0$ vzhledem k tomu, že forma g je pozitivně definitní. Přitom $g_2^*(\boldsymbol{u}) = 0$, právě když $g_2(\boldsymbol{u}_1) = g_2(\boldsymbol{u}_2) = 0$, tj. právě když $\boldsymbol{u} = 0$. ■

27.13. Definice. Buď (V_n, g) unitární prostor. Funkce g^* z předchozí věty se nazývá *komplexní rozšíření skalárního součinu* g na V_n a dvojice (V_n^*, g^*) se nazývá *komplexní rozšíření unitárního prostoru* (V_n, g). Vektory $\boldsymbol{u}, \boldsymbol{v} \in V_n^*$ se nazývají *ortogonální* nebo *kolmé*, jestliže $g^*(\boldsymbol{u}, \boldsymbol{v}) = 0$. Je-li $E_n((V_n, g))$ n-rozměrný euklidovský prostor, pak afinní prostor $E_n^*((V_n^*, g^*))$ se nazývá *komplexní rozšíření prostoru* E_n.

27.14. Věta. *Je-li $M = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ ortonormální polární báze symetrické bilineární formy f na unitárním prostoru (V_n, g), pak M je ortonormální polární báze formy f^* na komplexním rozšíření (V_n^*, g^*) unitárního prostoru (V_n, g).*

Důkaz. Podle definice formy f^* z věty 27.12 jest $f^*(\boldsymbol{u}_i, \boldsymbol{u}_j) = f(\boldsymbol{u}_i, \boldsymbol{u}_j) = 0$ pro $i \neq j$ a $g^*(\boldsymbol{u}_i, \boldsymbol{u}_j) = g(\boldsymbol{u}_i, \boldsymbol{u}_j) = \delta_{ij}$ pro $i, j = 1, 2, \ldots, n$. ■

27.15. Věta. *Buď (V_n, g) unitární prostor a buď (V_n^*, g^*) komplexní rozšíření tohoto prostoru. Označíme-li $\|\boldsymbol{u}\| = \sqrt{g_2(\boldsymbol{u})}$ pro každé $\boldsymbol{u} \in V_n$, $\|\boldsymbol{u}\|_g = \sqrt{g_2^*(\boldsymbol{u})}$ pro každé $\boldsymbol{u} \in V_n^*$ a $\varrho(\boldsymbol{u}, \boldsymbol{v}) = \|\boldsymbol{u} - \boldsymbol{v}\|_g$ pro libovolné $\boldsymbol{u}, \boldsymbol{v} \in V_n^*$, pak ϱ je metrika na V_n^*.*

Důkaz. Podle věty 27.12 (6) je $\varrho(\boldsymbol{u}\boldsymbol{v}) \geq 0$, přičemž $\varrho(\boldsymbol{u}, \boldsymbol{v}) = 0$ právě když $\boldsymbol{u} = \boldsymbol{v}$. Dále z $g_2^*(\boldsymbol{u}) = g_2(\boldsymbol{u}_1) + g_2(\boldsymbol{u}_2)$, $\boldsymbol{u} = \boldsymbol{u}_1 + i\boldsymbol{u}_2$, plyne $g_2^*(-\boldsymbol{u}) = g_2(-\boldsymbol{u}_1) + g_2(-\boldsymbol{u}_2) = g_2^*(\boldsymbol{u})$, takže $\varrho(\boldsymbol{u}, \boldsymbol{v}) = \varrho(\boldsymbol{v}, \boldsymbol{u})$ a zbývá ověřit trojúhelníkovou nerovnost (viz poznámka 14.3). Protože $(\|\boldsymbol{u}_1\|\|\boldsymbol{v}_2\| - \|\boldsymbol{u}_2\|\|\boldsymbol{v}_1\|)^2 \geq 0$, je $2\|\boldsymbol{u}_1\|\|\boldsymbol{u}_2\|\|\boldsymbol{v}_1\|\|\boldsymbol{v}_2\| \leq \|\boldsymbol{u}_1\|^2\|\boldsymbol{v}_2\|^2 + \|\boldsymbol{u}_2\|^2\|\boldsymbol{v}_1\|^2$, odkud $(\|\boldsymbol{u}_1\|\|\boldsymbol{v}_1\| + \|\boldsymbol{u}_2\|\|\boldsymbol{v}_2\|)^2 = \|\boldsymbol{u}_1\|^2\|\boldsymbol{v}_1\|^2 + 2\|\boldsymbol{u}_1\|\|\boldsymbol{u}_2\| \|\boldsymbol{v}_1\|\|\boldsymbol{v}_2\| + \|\boldsymbol{u}_2\|^2\|\boldsymbol{v}_2\|^2 \leq \|\boldsymbol{u}_1\|^2\|\boldsymbol{v}_1\|^2 + \|\boldsymbol{u}_2\|^2\|\boldsymbol{v}_2\|^2 + \|\boldsymbol{u}_1\|^2\|\boldsymbol{v}_2\|^2 + \|\boldsymbol{u}_2\|^2\|\boldsymbol{v}_1\|^2 = (\|\boldsymbol{u}_1\|^2 + \|\boldsymbol{u}_2\|^2)(\|\boldsymbol{v}_1\|^2 + \|\boldsymbol{v}_2\|^2) = \|\boldsymbol{u}\|_*^2\|\boldsymbol{v}\|_*^2$ a tedy $\|\boldsymbol{u}_1\|\|\boldsymbol{v}_1\| + \|\boldsymbol{u}_2\|\|\boldsymbol{v}_2\| \leq \|\boldsymbol{u}\|_*\|\boldsymbol{v}\|_*$. Podle věty 14.14 (ii) nyní máme $\|\boldsymbol{u} - \boldsymbol{v}\|_* = \sqrt{\|\boldsymbol{u}_1 - \boldsymbol{v}_1\|^2 + \|\boldsymbol{u}_2 - \boldsymbol{v}_2\|^2} \leq \sqrt{(\|\boldsymbol{u}_1\| + \|\boldsymbol{v}_1\|)^2 + (\|\boldsymbol{u}_2\| + \|\boldsymbol{v}_2\|)^2} = \sqrt{\|\boldsymbol{u}\|_*^2 + \|\boldsymbol{v}\|_*^2 + 2(\|\boldsymbol{u}_1\|\|\boldsymbol{v}_1\| + \|\boldsymbol{u}_2\|\|\boldsymbol{v}_2\|)} \leq \sqrt{\|\boldsymbol{u}\|_*^2 + \|\boldsymbol{v}\|_*^2 + 2\|\boldsymbol{u}\|_*\|\boldsymbol{v}\|_*} = \|\boldsymbol{u}\|_* + \|\boldsymbol{v}\|_*$. Pak ale $\varrho(\boldsymbol{u}, \boldsymbol{v}) + \varrho(\boldsymbol{v}, \boldsymbol{w}) = \varrho(\boldsymbol{u}, \boldsymbol{v}) + \varrho(\boldsymbol{w}, \boldsymbol{v}) = \|\boldsymbol{u} - \boldsymbol{v}\|_* + \|\boldsymbol{w} - \boldsymbol{v}\|_* \geq \|\boldsymbol{u} - \boldsymbol{v} - (\boldsymbol{w} - \boldsymbol{v})\|_* = \|\boldsymbol{u} - \boldsymbol{w}\|_* = \varrho(\boldsymbol{u}, \boldsymbol{w})$ a jsme hotovi. ■

27.16. Definice. Buď $A_n(V_n)$ afinní prostor dimenze n nad tělesem reálných čísel. Projektivní rozšíření $\overline{A_n^*}(\overline{V_{n+1}^*})$ komplexního rozšíření $A_n^*(V_n^*)$ afinního prostoru $A_n(V_n)$ se nazývá *komplexní projektivní rozšíření prostoru* $A_n(V_n)$.

27.17. Poznámka. Podle odstavců 27.10 a 27.2 sestává A_n^* z bodů tvaru $a + i\boldsymbol{u}$, kde $a \in A_n$ a $\boldsymbol{u} \in V_n$ a V_n^* sestává z vektorů tvaru $\boldsymbol{v} + i\boldsymbol{w}, \boldsymbol{v}, \boldsymbol{w} \in V_n$. Z definice projektivního rozšíření afinního prostoru 21.21 pak dostáváme, že prostor $\overline{V_{n+1}^*}$ je tvořen vektory tvaru $\alpha(a + i\boldsymbol{u}) + \boldsymbol{v} + i\boldsymbol{w}$, kde α je nějaké komplexní číslo. V předchozí definici jsme zavedli komplexní projektivní rozšíření afinního prostoru v právě popsaných dvou krocích v daném pořadí. Je tudíž přirozené položit si otázku, co se stane, jestliže pořadí obou kroků vyměníme. Z odstavce 21.21 víme, že $\overline{V_{n+1}}$ sestává z vektorů tvaru $ra + \boldsymbol{u}$, kde $a \in A_n$, $\boldsymbol{u} \in V_n$ a r je nějaké reálné číslo. Pak vektorový prostor $\left(\overline{V_{n+1}}\right)^*$ je podle 27.2 tvořen prvky tvaru $ra + \boldsymbol{u} + i(sb + \boldsymbol{v})$, $a, b \in A_n$, $\boldsymbol{u}, \boldsymbol{v} \in V_n$, $r, s \in R$. Není obtížné ověřit, že zobrazení $\varphi : \overline{V_{n+1}^*} \to (\overline{V_{n+1}})^*$ definované pro $\alpha = r + is \in K$, $a \in A_n$ a $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in V_n$ předpisem $\varphi(\alpha a + i\boldsymbol{u} + \boldsymbol{v} + i\boldsymbol{w}) = ra + \boldsymbol{v} + i(sa + \boldsymbol{u} + \boldsymbol{w})$ je izomorfismus vytvářející kanonické kolineární zobrazení projektivního prostoru $\overline{A_n^*}(\overline{V_{n+1}^*})$ na projektivní prostor $(\overline{A}_n)^*((\overline{V_{n+1}})^*)$. Podívejme se na celou tuto problematiku ještě z jiné strany. Buď $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ nějaká soustava souřadnic v afinním prostoru $A_n(V_n)$. Podle věty 21.25 je $\bar{S} = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ (kde a je zkrácené označení pro $1a$) aritmetická báze projektivního prostoru $\overline{A}_n(\overline{V_{n+1}})$ a podle důkazu věty 27.4 (i) je $\bar{S}$ báze komplexního rozšíření $(\overline{V_{n+1}})^*$. Obrátíme-li nyní pořadí obou kroků, pak podle 27.4 je $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ báze komplexního rozšíření V_n^*, takže $S = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ je soustava souřadnic afinního prostoru $A_n^*(V_n^*)$ a podle věty 21.25 je $\bar{S} = \{a, \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ aritmetická báze projektivního rozšíření $\overline{A_n^*}(\overline{V_{n+1}^*})$. Výše popsaný izomorfismus $\varphi : \overline{V_{n+1}^*} \to \left(\overline{V_{n+1}}\right)^*$ je tedy ve smyslu věty 9.22 indukován identickým zobrazením na množině $\bar{S}$.

27.18. Poznámka. Z předcházející teorie víme, že obecná rovnice kuželosečky v euklidovské rovině E_2 obsahuje šest koeficientů, které jsou určeny jednoznačně až na nenulový násobek. To znamená, že znalost pěti bodů ležících na dané kuželosečce stačí k jejímu jednoznačnému určení. Na druhé straně víme, že kružnice je jednoznačně určena pouze třemi body. Podívejme se tedy, v čem tato zvláštnost u kružnice spočívá. Z odstavce 25.2 víme, že kanonická rovnice kružnice v kartézské soustavě souřadnic tvořené středem a směry os je $x^2 + y^2 = a^2$. V projektivním rozšíření roviny E_2 má tato kružnice rovnici $x_1^2 + x_2^2 - ax_0^2 = 0$ a průnik $Q_{f_2} \cap N$ s nevlastní nadrovinou pak rovnici $x_1^2 + x_2^2 = 0$. Vidíme tedy, že $Q_{f_2} \cap N$ neobsahuje žádné reálné body. Přejdeme-li však ke komplexnímu rozšíření, pak $Q_{f_2} \cap N$ sestává ze dvou imaginárních bodů v souřadnicích $(0, 1, i)$ a $(0, 1, -i)$. Vidíme tedy, že každá kružnice v E_2 prochází těmito dvěma nevlastními komplexními body, a proto k jejímu určení stačí udat pouze tři body. Právě popsané nevlastní body se nazývají *izotropické směry.*

LINEÁRNÍ ALGEBRA A GEOMETRIE
prof. RNDr. LADISLAV BICAN, DrSc.

Vydala Academia
nakladatelství Akademie věd České republiky
Legerova 61, 120 00 Praha 2

Obálku navrhl Oleg Man
Redaktorka publikace Jitka Zykánová

Vydání 1., dotisk 2002
Ed. číslo 1562
Tisk ACADEMIA

ISBN 80-200-0843-8