Теореме за усмени из алгебре

2023/2024.

- Релација (2)

  +2.14
  +2.15

- Булове алгебре (14)

  4.5 4.12
  4.6 4.13
  4.7 4.18
  4.8 4.20
  4.9 4.22
  4.10 4.23
  4.11 4.52

- Групоиди и групе (2)

  5.32
  5.41

- Прстени и поља (1)

  6.6

- Комплексни бројеви (5)

  7.6
  7.28
  7.29
  7.32
  7.48

- Полиноми (10)

  8.19 8.53
  8.24 8.54
  8.34 8.55
  8.39 8.69
  8.49 8.70

- Конструкција поља (2)

  9.1
  9.2

- Детерминанте (1)

  10.18

- Системи линеарних једначина (1)

  11.12

- Аналитичка геометрија (6)

  13.3 13.11
  13.4 13.20
  13.5 13.21

- Векторски простори (8)

  14.4 14.22
  14.10 14.23
  14.13 14.26 (17.26)
  14.21 14.28 (17.28)

- Линеарне трансформације (4)

  15.13
  15.14
  15.15
  15.17

- Матрице и линеарне трансформације (1)

  16.33

- Ранг матрице и инверзна матрица (5)

  17.12
  17.15
  17.19
  17.24
  17.25

Релације

2.14 Ако је ρ релација еквиваленције скупа A, тада је:

$$(\forall x,y \in A)\ (x\rho y \Leftrightarrow C_x = C_y)$$

Доказ:

($\Rightarrow$) Нека је $x\rho y$. За $z \in C_x$ важи $x\rho z$, а даље

$(x\rho y \wedge x\rho z) \overset{S}{\Rightarrow} (y\rho x \wedge x\rho z) \overset{T}{\Rightarrow} y\rho z \Rightarrow z \in C_y \Rightarrow C_x \subseteq C_y$.

Аналогно се доказује и да $C_y \subseteq C_x$ па је $C_x = C_y$

($\Leftarrow$) Нека је $C_x = C_y$. Из $x \in C_x$ и $C_x = C_y$ следи $x \in C_y$, а одатле по дефиницији класе еквиваленције (2.13) следи $y\rho x$, а због симетричности релације важи и $x\rho y$.

$\square$

2.15 Нека су C_x и C_y класе еквиваленције скупа A с обзиром на релацију еквиваленције ρ. Тада је:

$$C_x \cap C_y = \emptyset \ \vee \ C_x = C_y$$

Доказ:

Ако је $C_x \cap C_y = \emptyset$ тврђење теореме је тачно.

Претпоставимо да је $C_x \cap C_y \neq \emptyset$. Тада постоји $z \in C_x \cap C_y$ тј. $z \in C_x \wedge z \in C_y$, одакле следи $x\rho z \wedge y\rho z$, односно из симетричности следи $x\rho z \wedge z\rho y$ па на основу транзитивности $x\rho y$. Из теореме 2.14 ($x\rho y \Leftrightarrow C_x = C_y$) следи да је $C_x = C_y$ па је тврђење поново тачно.

$\square$

Булове алгебре

Аксиоми Булових алгебри:

B_1: $a+b=b+a$ $\quad a\cdot b=b\cdot a$ — комутативност

B_2: $a(b+c)=(a\cdot b)+(a\cdot c)$ $\quad a+(b\cdot c)=(a+b)\cdot(a+c)$ — дистрибутивност

B_3: $a+0=a$ $\quad a\cdot 1=a$ — постојање неутралног елемента

B_4: $a+a'=1$ $\quad a\cdot a'=0$ — постојање инверзног елемента

4.5 $a+a=a$; $a\cdot a=a$ идентоентност

Доказ:

$$\underline{\underline{a}} \overset{B3}{=} a+0 \overset{B4}{=} a+a\cdot a' \overset{B2}{=} (a+a)\cdot(a+a') \overset{B4}{=} (a+a)\cdot 1 \overset{B3}{=} \underline{\underline{a+a}}$$

Због дуалности теорема важи и $a\cdot a=a$ □

4.6 $a+1=1$; $a\cdot 0=0$ ограниченост

Доказ:

$$\underline{\underline{a+1}} \overset{B3}{=} (a+1)\cdot 1 \overset{B1}{=} 1\cdot(a+1) \overset{B4}{=} (a+a')(a+1) \overset{B2}{=} a+a'\cdot 1 \overset{B3}{=} a+a' \overset{B4}{=} \underline{\underline{1}}$$ □

4.7 $a+ab=a$; $a\cdot(a+b)=a$ апсорбција

Доказ:

$$\underline{\underline{a+ab}} \overset{B3}{=} a\cdot 1+a\cdot b \overset{B2}{=} a(1+b) \overset{4.6}{=} a\cdot 1 \overset{B3}{=} \underline{\underline{a}}$$ □

4.8 $a+a'b=a+b$; $a(a'+b)=ab$

Доказ:

$$\underline{\underline{a+a'b}} \overset{B2}{=} \underbrace{(a+a')}_{1}(a+b) \overset{B4}{=} 1\cdot(a+b) \overset{B1}{=} (a+b)\cdot 1 \overset{B3}{=} \underline{\underline{a+b}}$$ □

4.9 $(a+b)+c = a+(b+c)$; $(ab)c = a(bc)$ асоцијативност

Доказ:

$$\underline{\underline{(a+b)+c}} \overset{B3,B1}{=} 1\cdot((a+b)+c) \overset{B4}{=} (a+a')((a+b)+c) \overset{B2}{=} (\overbrace{a(a+b)}^{a}+ac)+(\overbrace{a'(a+b)}^{0+a'b}+ac)$$

$$\overset{4.7,4.8}{=} a+(a'b+a'c) \overset{B2}{=} a+a'(b+c) \overset{4.8}{=} \underline{\underline{a+(b+c)}}$$

$\square$

4.10 Систем једначина $a+x=1 \wedge a\cdot x=0$ по непознатој x, има јединствено решење за све вредности параметра a из скупа B.

Доказ:

На основу аксиома B_4 следи да $\underline{x=a'}$ јесте решење датог система. Потребно је доказати да нема више решења. То ће се урадити контрадикцијом.

Претпоставити да је $b\neq a'$ такође решење датог система. Тада систем изгледа:

$$a+b=1 \quad (*)$$
$$a\cdot b=0 \quad (\#)$$

и важи:

$$\underline{\underline{b}} \overset{B3,B1}{=} b\cdot 1 \overset{B4}{=} b\cdot(a+a') \overset{B2}{=} \overbrace{ba}^{0}+ba' \overset{B1,\#}{=} 0+ba' \overset{B4}{=} a\cdot a'+ba' \overset{B2}{=} a'\overbrace{(a+b)}^{1}$$

$$\overset{*}{=} a'\cdot 1 \overset{B3}{=} \underline{\underline{a'}}$$ ↯ контрадикција са $b\neq a'$ па не постоји друга решења

$\square$

4.11 $0'=1$; $1'=0$

Доказ:

Систем $0+x=1 \wedge 0\cdot x=0$ на основу B_4 има за решење $x=0'$, а због B_3 $x=1$, а како по теореми 4.10 систем има јединствено решење, следи да је $\underline{\underline{0'=1.}}$

$\square$

4.12 $(a')'=a$; Да ли је $f(x)=x'$ бијективна функција? Зашто?

Доказ:

Систем $a'+x=1 \wedge a'\cdot x=0$ на основу B_1 и B_4 има за решење $x=a$ и $x=(a')'$, а како на основу теореме 4.10 систем има јединствено решење, следи да је $\underline{\underline{(a')'=a}}$.

$f(x)=x'$ јесте бијективна функција јер сваком елементу x одговара тачно један x'

$f(f(x))=f(x')=(x')'\overset{4.12}{=}x \Rightarrow f: B \underset{на}{\overset{1-1}{\Rightarrow}} B$

$\square$

4.13 $(a+b)'=a'b'$; $(ab)'=a'+b'$ Де Морганови закони

Доказ:

Систем $(a+b)+x=1$ $(*)$

$(a+b)x=0$ $(\#)$

Због B_4 има решење $x=(a+b)'$ и решење $x=a'b'$ јер важи:

$\underline{\underline{(a+b)+a'b'}}\overset{B_2}{=}(a+b+a')+(a+b+b')\overset{B_1,B_4}{=}(b+1)(a+1)\overset{4.6}{=}1\cdot 1\overset{B_3}{=}\underline{\underline{1}}$ $(*)$

$\underline{\underline{(a+b)\cdot a'b'}}\overset{B_2}{=}a\cdot a'b'+b\cdot a'b'\overset{B_1,B_4}{=}0\cdot a'+0\cdot b'\overset{4.6}{=}0+0\overset{B_9}{=}\underline{\underline{0}}$ $(\#)$

Како на основу теореме 4.10 систем има јединствено решење, следи да је $\underline{\underline{(a+b)'=a'b'}}$.

$\square$

4.18 У Буловој алгебри B следећи искази су еквивалентни:

a) $x+y=y$ b) $xy=x$ c) $x'+y=1$ d) $xy'=0$

Доказ:

Да би доказали теорему довољно је доказати да важе:

a) $\Rightarrow$ b) $\Rightarrow$ c) $\Rightarrow$ d) $\Rightarrow$ a)

a) $\Rightarrow x+y=y \,/\cdot x \Rightarrow x(x+y)=xy \overset{4.7}{\Rightarrow} x=xy \Rightarrow$ b) a) $\Rightarrow$ b)

b) $\Rightarrow xy=x \,/+x' \Rightarrow x'+xy=x+x' \overset{4.8,B_4}{\Rightarrow} x'+y=1 \Rightarrow$ c) b) $\Rightarrow$ c)

c) $\Rightarrow x'+y=1 \,/'\overset{4.13}{\Rightarrow} xy'=0 \Rightarrow$ d) c) $\Rightarrow$ d)

d) $\Rightarrow xy'=0 \,/+y \Rightarrow xy'+y=y \overset{4.8}{\Rightarrow} x+y=y \Rightarrow$ a) d) $\Rightarrow$ a) $\square$

Бинарна релација $\lesssim$: $(\forall x\in B)(\forall y\in B)\ x\lesssim y \Leftrightarrow x+y=y$

4.20 Релација $\lesssim$ у Буловој алгебри $B=(B,+,\cdot,',0,1)$ јесте релација поретка тј. за свако $x,y,z\in B$ важи:

a) $\underset{R}{x\lesssim x}$ b) $(x\lesssim y \wedge \underset{A}{y\lesssim x}) \Rightarrow x=y$ c) $(x\lesssim y \wedge \underset{T}{y\lesssim z}) \Rightarrow x\lesssim z$

Доказ:

a) $x\lesssim x \Leftrightarrow \underset{\text{апсорпција}}{x+x=x}$ T рефлексивна

b) $(x\lesssim y \wedge y\lesssim x) \Rightarrow (x+y=y \wedge y+x=x) \Rightarrow x=y$ антисиметрична

c) $(x\lesssim y \wedge y\lesssim z) \Rightarrow x+y=y \wedge y+z=z \Rightarrow x+\underbrace{y+z}_{z}=\underbrace{y+z}_{z} \Rightarrow x+z=z \Rightarrow x\lesssim z$

транзитивна

Пошто важе a), b) и c) релација је рефлексивна, антисиметрична, транзитивна па је релација $\lesssim$ релација поретка у Буловој алгебри B. $\square$

4.22. У Буловој алгебри B за свако x и y из B важи:

a) $x \leq x+y$ b) $y \leq x+y$ c) $xy \leq x$ d) $xy \leq y$

Доказ:

a) $x \leq x+y \iff \overbrace{x+x}^{\text{идемпотентност}}+y = x+y \iff x+y = x+y$ ✓

b) $y \leq x+y \iff \overbrace{y+x+y}^{\text{идемпотентност}} = x+y \iff x+y = x+y$ ✓

c) $xy \leq x \iff \overbrace{xy+x}^{\text{апсорпција}} = x \iff x = x$ ✓

d) $xy \leq y \iff \overbrace{xy+y}^{\text{апсорпција}} = y \iff y = y$ ✓ $\square$

4.23 У Буловој алгебри B за свако x, y и z из B важи:

a) $(x \leq z \wedge y \leq z) \Rightarrow x+y \leq z$

b) $(z \leq x \wedge z \leq y) \Rightarrow z \leq xy$

c) $(x \leq z \wedge y \leq z) \Rightarrow xy \leq z$

d) $(z \leq x \wedge z \leq y) \Rightarrow z \leq x+y$

Доказ:

a) $(x \leq z \wedge y \leq z) \Rightarrow (x+z = z \wedge y+z = z) \Rightarrow x+y+z = z \Rightarrow x+y \leq z$

b) $(z \leq x \wedge z \leq y) \Rightarrow (zx = z \wedge zy = z) \Rightarrow xyz = z \Rightarrow z \leq xy$

c) $(x \leq z \wedge y \leq z) \Rightarrow (x+z = z \wedge y+z = z) \Rightarrow (x+z)(y+z) = \overbrace{z \cdot z}^{\text{идемпотентност}} = z$

$\overset{B2}{\Rightarrow} xy + z = z \Rightarrow xy \leq z$

d) $(z \leq x \wedge z \leq y) \Rightarrow (zx = z \wedge zy = z) \Rightarrow zx + zy = \overbrace{z+z}^{\text{идемпотентност}} = z$

$\overset{B2}{\Rightarrow} z(x+y) = z \Rightarrow z \leq x+y$ $\square$

4.52 Репрезентација Булових функција помоћу SDNF.

$$f(x_1, x_2, \dots, x_n) = \sum_{(\alpha_1, \alpha_2, \dots, \alpha_n) \in \{0,1\}^n} f(\alpha_1, \alpha_2, \dots, \alpha_n)\, x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

Доказ:

Доказаћемо теорему за $n=3$. На примеру три независне променљиве, односно за $n=3$ претходна теорема има облик:

$$f(x,y,z) = f(0,0,0)x^0y^0z^0 + f(0,0,1)x^0y^0z^1 + f(0,1,0)x^0y^1z^0 + f(0,1,1)x^0y^1z^1 + f(1,0,0)x^1y^0z^0 + f(1,0,1)x^1y^0z^1 + f(1,1,0)x^1y^1z^0 + f(1,1,1)x^1y^1z^1$$

Проверићемо сада да ли је ова једнакост тачна на примеру за $(x,y,z)=(0,1,1)$. Ако се уврсти $(x,y,z)=(0,1,1)$, тада ће на десној страни сви сабирци (елементарне конјукције), изузев четвртог, бити нуле јер у свим тим сабирцима ће се на бар једном месту разликовати основа од експонента па ће због 4.51 сабирци бити једнаки 0, а четврти ће бити $f(0,1,1)$. Тиме је наша једнакост постала $f(0,1,1)=f(0,1,1)$ односно тачна. Како ће се ово очевидно увек десити за сваку тројку $(x,y,z) \in \{0,1\}^3$ тиме је теорема доказана.

Доказ је спроведен за $n=3$, међутим то очевидно важи и за свако $n \in \mathbb{N}$. $\square$

Групоиди и групе

5.32 Нека је ρ конгруенција групоида $(G,\cdot)$. Тада једнакост $C_x * C_y = C_{xy}$, где су x и y из G а C_x, C_y и C_{xy} из G/ρ, дефинише операцију $*$ у скупу G/ρ односно $(G/\rho, *)$ је групоид.

Доказ:

Треба проверити да ли $*$ јесте функција која пару (C_x, C_y) придружује C_{xy}, тј. да ли пар (C_x, C_y) може да се пресликa са $*$ и у неки елемент различит од C_{xy}, јер ако узмемо $u \in C_x$ и $v \in C_y$, тада је због 2.13 и 2.14 $(C_x, C_y) = (C_u, C_v)$, а питање је да ли ће бити и $C_{xy} = C_{uv}$? Одговор је потврдан само зато што је ρ конгруенција па важи:

$$\underline{(C_x, C_y) = (C_u, C_v)} \Rightarrow (C_u = C_x \wedge C_v = C_y) \overset{2.14}{\Longrightarrow} (u \rho x \wedge v \rho y) \overset{5.30}{\Rightarrow} uv \rho xy$$

$$\Rightarrow \underline{\underline{C_{uv} = C_{xy}}}$$

$\square$

5.41 Свака група $(G,\cdot)$ изоморфна је некој подгрупи групе пермутација скупа G.

Доказ:

Лако се проверава да функција $\delta_a : G \to G$ дефинисана са:

$$(*) \quad (\forall x \in G)\ \delta_a(x) = ax, \quad a \in G \qquad \text{(једна пермутација)}$$

јесте бијекција, тј. пермутација скупа G. Уочимо сада скуп свих пермутација скупа G које су облика $(*)$ и означимо га са H односно

$$H = \{\delta_a \mid \delta_a : G \xrightarrow[\text{на}]{1-1} G \wedge a \in G \wedge (\forall x \in G)\ \delta_a(x) = ax\}.$$

Лако се показује да $(H, \circ)$ јесте група, где је $\circ$ операција композиције функција. Да би се доказало да су $(G,\cdot)$ и $(H,\circ)$ изоморфни, мора се конструисати (дефинисати) нека функција $\psi : G \to H$ која ће бити бијекција и хомоморфизам, односно изоморфизам.

Нека је функција $\psi: G \to H$ дефинисана са:

$$(\forall a \in G)\ \psi(a) = \delta_a.$$

Функција ψ је инјективна јер за све p и q из G важи:

$$\psi(p) = \psi(q) \Rightarrow \delta_p = \delta_q \Rightarrow (\forall x \in G)\ \delta_p(x) = \delta_q(x) \Rightarrow (\forall x \in G)\ px = qx \Rightarrow p = q$$

Сурјективност следи из чињенице да за свако $\delta_a \in H$ постоји такав $a \in G$ да је $\psi(a) = \delta_a$. И коначно доказимо да је ψ изоморфизам. Треба доказати да је $\psi(ab) = \psi(a) \circ \psi(b)$.

$$(\forall a, b \in G)\ \psi(ab) = \delta_{ab}(x) = \underbrace{(ab)x = a(bx)}_{\text{асоцијативност операције}} = \delta_a(bx) = \delta_a(\delta_b(x)) = (\delta_a \circ \delta_b)(x) = \psi(a) \circ \psi(b)$$

$\square$

Прстени и поља

6.6 Сваки коначан дачен интегритета $(R,+,\cdot)$ је поље.

Доказ:

Нека је $R=\{a_1,a_2,\dots,a_n\}$ скуп од n елемената у којем су свака два различита, и нека су $a\in R$ и $a\neq 0$. Доказаће се да постоји инверзни елемент за елемент a, што ће онда значити да је $(R,+,\cdot)$ поље. Формирати скуп $S=\{aa_1,aa_2,\dots,aa_n\}\subseteq R$ и доказати да скуп S има n елемената, тј. да је $aa_i\neq aa_j$ за $i\neq j$. Доказ се изводи контрадикцијом.

Претпоставимо да је $aa_i=aa_j$ за $i\neq j$. Тада је:

$aa_j=aa_i \Rightarrow aa_j-aa_i=0 \Rightarrow a(a_j-a_i)=0 \Rightarrow a_j-a_i=0$ јер је $a\neq 0$ и R без делитеља нуле. То је контрадикција јер се добило да је $a_i=a_j$ и $i\neq j$, а у скупу $R=\{a_1,a_2,\dots,a_n\}$ свака два су различита.

Како су R и S коначни скупови, $S\subseteq R$ и $Card(S)=Card(R)$ следи да је $S=R$. Пошто у домену интегритета R постоји јединица и како је $S=R$, то је за неко $k\in\{1,2,3,\dots,n\}$ $aa_k=e$, то јесте постоји инверзна за $a\neq 0$ односно $\underline{a^{-1}=a_k}$ $\square$

Комплексни бројеви

7.6 За произвољне комплексне бројеве z, z_1, z_2 важи:

a) $Re(z)=\frac{1}{2}(z+\bar{z})$

b) $Im(z)=\frac{1}{2i}(z-\bar{z})$

c) $\overline{z_1 \pm z_2}=\bar{z_1} \pm \bar{z_2}$

d) $Re(z_1+z_2)=Re(z_1)+Re(z_2)$

e) $\alpha \in R \Rightarrow \bar{\alpha}=\alpha$

f) $\overline{z_1 z_2}=\bar{z_1}\,\bar{z_2}$

g) $\overline{\left(\frac{z_1}{z_2}\right)}=\frac{\bar{z_1}}{\bar{z_2}}$

h) $Im(z_1+z_2)=Im(z_1)+Im(z_2)$

i) Четвороугао O, z_1, z_1+z_2, z_2 јесте паралелограм, где је $O=0+0i$

Доказ:

$z=x+iy$, $Re(z)=x$, $Im(z)=y$, $\bar{z}=x-iy$

$z_1=x+iy$, $Re(z_1)=x$, $Im(z_1)=y$, $\bar{z_1}=x-iy$

$z_2=a+ib$, $Re(z_2)=a$, $Im(z_2)=b$, $\bar{z_2}=a-ib$

a) $z+\bar{z}=x+\cancel{iy}+x-\cancel{iy}=2x \Rightarrow x=\frac{1}{2}(z+\bar{z}) \Rightarrow \underline{Re(z)=\frac{1}{2}(z+\bar{z})}$

b) $z-\bar{z}=x+iy-(x-iy)=\cancel{x}+iy-\cancel{x}+iy=2iy \Rightarrow y=\frac{1}{2i}(z-\bar{z}) \Rightarrow \underline{Im(z)=\frac{1}{2i}(z-\bar{z})}$

c) $\underline{\overline{z_1+z_2}}=\overline{x+iy+a+ib}=\overline{(x+a)+(y+b)i}=(x+a)-(y+b)i=x+a-yi-bi$

$=(x-yi)+(a-bi)=\underline{\bar{z_1}+\bar{z_2}}$

$\underline{\overline{z_1-z_2}}=\overline{x+iy-(a+ib)}=\overline{x+iy-a-ib}=\overline{(x-a)+(y-b)i}=(x-a)-(y-b)i$

$=x-a-yi+bi=(x-iy)-(a-bi)=\underline{\bar{z_1}-\bar{z_2}}$

d) $\underline{Re(z_1+z_2)}=Re(x+iy+a+ib)=Re((x+a)+i(y+b))=x+a=\underline{Re(z_1)+Re(z_2)}$

e) $\underline{\alpha \in R} \Rightarrow (w \in \mathbb{C} \wedge w=\alpha+0i=\alpha) \Rightarrow \bar{w}=\alpha-0i=\alpha \Rightarrow \bar{w}=w \Rightarrow \underline{\bar{\alpha}=\alpha}$

f) $\overline{z_1 \cdot z_2} = \overline{(x+iy)(a+ib)} = \overline{xa + xbi + yai - yb} = \overline{(xa-yb) + (xb+ya)i}$

$= (xa-yb) - (xb+ya)i = xa - yb - xbi - yai = x(a-bi) - yi\left(\frac{b}{i}\cdot\frac{i}{i^2} + a\right)$

$= x(a-bi) - yi(a-bi) = (a-bi)(x-yi) = \overline{z_2}\cdot\overline{z_1} = \overline{z_1}\,\overline{z_2}$

g) $\overline{\left(\frac{z_1}{z_2}\right)} = \overline{\left(\frac{x+iy}{a+ib}\cdot\frac{a-ib}{a-ib}\right)} = \overline{\left(\frac{xa-xbi+yai+yb}{a^2+b^2}\right)} = \overline{\left(\frac{(xa+yb)+(-xb+ya)i}{a^2+b^2}\right)}$

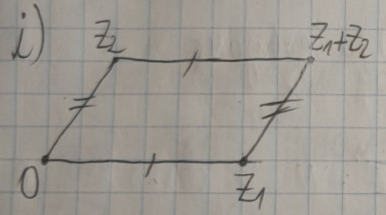
$= \frac{xa+yb}{a^2+b^2} + \frac{-xb+ya}{a^2+b^2}i = \frac{xa+yb}{a^2+b^2} - \frac{-xb+ya}{a^2+b^2}i = \frac{xa+yb+xbi-yai}{a^2+b^2}$

$= \frac{x(a+bi) - yi\left(-\frac{b}{i}\cdot\frac{i}{i^2} + a\right)}{a^2+b^2} = \frac{x(a+bi) - yi(a+bi)}{a^2+b^2} = \frac{(x-yi)(a+bi)}{a^2+b^2}\cdot\frac{a-bi}{a-bi}$

$= \frac{(x-yi)\cancel{(a^2+b^2)}}{\cancel{(a^2+b^2)}(a-bi)} = \frac{x-yi}{a-bi} = \frac{\overline{z_1}}{\overline{z_2}}$

h) $\mathrm{Im}(z_1+z_2) = \mathrm{Im}(x+iy+a+ib) = \mathrm{Im}((x+a)+(y+b)i) = y+b = \mathrm{Im}(z_1) + \mathrm{Im}(z_2)$

i)



$(z_1+z_2) - z_2 = z_1 - 0$

$(z_1+z_2) - z_1 = z_2 - 0$

$\cancel{x}+iy+a+ib-(a+ib) = x+iy-(0+0i)$

$x+iy+a+ib-(x+ib) = a+ib-(0+0i)$

$\cancel{x}+\cancel{iy}+\cancel{a}+\cancel{ib}-\cancel{a}-\cancel{ib} = \cancel{x}+\cancel{iy}-0-0i$

$\cancel{x}+\cancel{iy}+\cancel{a}+\cancel{ib}-\cancel{x}-\cancel{ib} = \cancel{a}+\cancel{ib}-0-0i$

$0=0$

$0=0$ ✓

$R_S = \{(z_1, z_2) \mid z_1, z_2 \in \mathbb{C}\}$

$\square$

7.28 За конвексно оријентисани угао $\varphi = \sphericalangle z_1 O z_2$ важи:

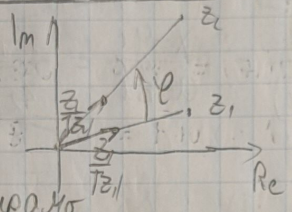
$$\sphericalangle z_1 O z_2 = \arg \frac{z_2}{z_1}$$

Доказ:

Нека је $\varphi \in (-\pi, \pi]$ мерни број оријентисаног угла $\sphericalangle z_1 O z_2$ односно $\varphi = \sphericalangle z_1 O z_2$. Тада је због 7.27 (ротација)

$$\frac{z_2}{|z_2|} \overset{①}{=} \frac{z_1}{|z_1|} e^{i\varphi} \iff e^{i\varphi} = \frac{z_2}{z_1} \frac{|z_1|}{|z_2|} \Rightarrow \arg e^{i\varphi} = \arg \frac{z_2}{z_1} \frac{|z_1|}{|z_2|}$$

$$\iff \varphi \overset{②}{=} \arg \frac{z_2}{z_1} \iff \underline{\underline{\sphericalangle z_1 O z_2 = \arg \frac{z_2}{z_1}}}$$



Напомена ①:

Пошто $|z_1| \neq$ не мора да буде једнак $|z_2|$ мораћемо да ротирамо комплексне бројеве истог аргумента као и полазни z_1 и z_2 али интензитет 1 односно ротирамо хомотетију $H_{0,|z_1|}(z_1)$ и добијамо хомотетију $H_{0,|z_2|}(z_2)$.

Напомена ②:

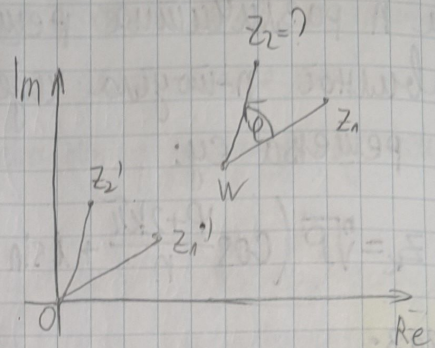
Хомотетија не мења аргумент, односно $\arg \rho z = \arg z$ за $\rho \in \mathbb{R}^+$ и $z \in \mathbb{C} \setminus \{0\}$. Одатле следи да је $\arg \frac{z_2}{z_1} \cdot \frac{|z_1|}{|z_2|} = \arg \frac{z_2}{z_1}$ јер $\frac{z_2}{z_1} \in \mathbb{C} \setminus \{0\}$ и $\frac{|z_1|}{|z_2|} \in \mathbb{R}^+$

$\square$

7.29 Ако је комплексни број z_2 добијен ротацијом комплексног броја z_1 око центра ротације, броја w, за угао φ, тада је:

$$z_2 = w + (z_1 - w)e^{i\varphi}$$

Доказ:



Пошто познајемо само ротацију око координатног почетка морамо прво да транслирамо z_1, z_2, w тако да центар ротације буде у координатни почетак. $T(z) = z + t$

Пошто је $w' = 0 = T(w) = t + w$ одавде следи да је $\boxed{t = -w}$ па транслација T има облик $\boxed{T(z) = z - w}$ па се добија

$z_1' = T(z_1) = z_1 - w$

$z_2' = T(z_2) = z_2 - w$

а по формули ротације око кординатног почетка за угао φ: $R_{0,\varphi}(z) = ze^{i\varphi}$ знамо да је $z_2' = R_{0,\varphi}(z_1') \iff z_2 - w = (z_1 - w)e^{i\varphi}$

$\implies \underline{z_2 = w + (z_1 - w)e^{i\varphi}}$

Одавде добијамо функцију за ротацију комплексног броја z око центра ротације w за угао φ: $\underline{R_{w,\varphi}(z) = w + (z - w)e^{i\varphi}}$

$\square$

7.32 Једначина $z^n = w = \rho e^{i\varphi}$, где је z непозната, n произвољан природни број и w произвољни комплексни број различит од нуле, има n различитих решења која су у комплексној равни темена правилног n-тогла чије је тежиште у координатном почетку, тј. решења су:

$$z_k = \sqrt[n]{\rho}\left(\cos\frac{\varphi+2k\pi}{n} + i\sin\frac{\varphi+2k\pi}{n}\right) = \sqrt[n]{\rho}\, e^{i\frac{\varphi+2k\pi}{n}} \qquad k=0,\dots,n-1$$

Доказ:

Дата једначина $z^n = w$ решава се увођењем смена $z = re^{i\psi}$ и $w = \rho e^{i\varphi}$, где су r и ψ непознате, а ρ и φ дати бројеви, јер је w дати број. Сада следи $z^n = w \iff r^n e^{in\psi} = \rho e^{i\varphi} \iff r = \sqrt[n]{\rho} \wedge n\psi = \varphi + 2k\pi \wedge k \in \mathbb{Z}$. Да се нека решења не би понављала узима се да је $\psi = \frac{\varphi+2k\pi}{n} \in (-\pi, \pi]$ па је онда довољно да је $k \in \{0, 1, \dots, n-1\}$ односно:

$$z^n = w = \rho e^{i\varphi} \iff z \in \left\{\sqrt[n]{\rho}\, e^{i\frac{\varphi+2k\pi}{n}} \,\middle|\, k=0,\dots,n-1\right\} = S$$

Значи, $z_k = \sqrt[n]{\rho}\, e^{i\frac{\varphi+2k\pi}{n}}$ су решења једначине $z^n = w$ за свако $k=0,\dots,n-1$. Показати да су свака два z_k из S различита тј. да их има бар n. Ако је $k_1 \neq k_2$ тада је $z_{k_1} \neq z_{k_2}$ јер је

$$z_k = \sqrt[n]{\rho}\, e^{i\frac{\varphi+2k\pi}{n}} = \sqrt[n]{\rho}\, e^{i\frac{\varphi}{n}} \cdot e^{i\frac{2k\pi}{n}} = \sqrt[n]{\rho} \cdot e^{i\frac{\varphi}{n}} \left(e^{i\frac{2\pi}{n}}\right)^{k-1} \cdot e^{i\frac{2\pi}{n}} = \sqrt[n]{\rho} \cdot e^{i\frac{\varphi+2(k-1)\pi}{n}} \cdot e^{i\frac{2\pi}{n}}$$

$$= \underline{\underline{z_{k-1}\, e^{i\frac{2\pi}{n}}}}$$

тј. $z_k = z_{k-1} e^{i\frac{2\pi}{n}}$, што значи да је z_k добијен ротацијом броја z_{k-1} око координатног почетка за угао $\frac{2\pi}{n}$, па следи да су $z_0, z_1, \dots, z_{n-1}$ на истој централној кружници полупречника $\sqrt[n]{\rho}$ и сваки од њих се добија од претходног, ротацијом за угао $\frac{2\pi}{n}$, јер множење са $e^{i\theta}$ је ротација за угао θ око координатног почетка, а пун угао износи 2π па се ниједан од $z_0, z_1, \dots, z_{n-1}$ неће поклапати. Значи пронашли смо бар n решења. $\square$

7.48 Дока
дефи
осну
почет
Одред

Доказ:

Примети
реална о
ротацује
симетрија
$f(z) = (R_{0,\frac{\varphi}{2}} \circ$
$z e^{i}$
Значи f
почетак
Скуп ко
где се
Напомен

7.48 Доказати да функција $f_\theta : \mathbb{C} \to \mathbb{C}$, где је $\theta \in (-\pi, \pi]$, дефинисана са $f_\theta(z) = \bar{z} e^{i\theta}$ у комплексној равни одређује једну осну симетрију чија оса је права која пролази кроз координатни почетак и образује угао $\frac{\theta}{2}$ са позитивном делом реалне осе. Одредити скуп свих комплексних бројева који припадају тој оси.

Доказ:

Приметимо да је $g(z) = \bar{z}$ осна симетрија чија је оса симетрије реална оса. Такође је познато (из група) да композиција ротације $R_{0,-\frac{\theta}{2}}$, осне симетрије $g(z) = \bar{z}$ и ротације $R_{0,\frac{\theta}{2}}$ јесте осна симетрија чија оса гради угао $\frac{\theta}{2}$ са реалном осом односно:

$$\underline{f_\theta(z)} = (\underbrace{R_{0,-\frac{\theta}{2}} \circ g \circ R_{0,\frac{\theta}{2}}}(z) = R_{0,-\frac{\theta}{2}}\left(g\left(R_{0,\frac{\theta}{2}}(z)\right)\right) = R_{0,-\frac{\theta}{2}}\left(g\left(ze^{i\frac{\theta}{2}}\right)\right) = R_{0,-\frac{\theta}{2}}\left(\overline{ze^{i\frac{\theta}{2}}}\right) =$$

$$ze^{-i\frac{\theta}{2}} \cdot e^{-i\frac{\theta}{2}} = \bar{z}e^{-i\frac{\theta}{2}} \cdot e^{i\frac{\theta}{2}} = \underline{\bar{z}e^{i\theta}}$$

Значи f_θ јесте осна симетрија чија оса пролази кроз координатни почетак и образује угао $\frac{\theta}{2}$ са позитивним делом реалне осе.

Скуп тачака праве осе је $\{z \mid z \in \mathbb{C} \wedge (\arg z = \frac{\theta}{2} \vee \arg z = \pm\pi + \frac{\theta}{2})\} \cup \{0\}$ где се знак + или − бира тако да буде $\pm\pi + \frac{\theta}{2} \in (-\pi, \pi]$

Напомена: $R_{0,\theta}$ је ознака за ротацију око кординатног почетка за угао θ у дефиницији $R_{0,\theta}(z) = ze^{i\theta}$

$\square$

Полиноми

8.19 Теорема о дељењу полинома. За свака два полинома S и $T \neq 0$, постоје такви јединствени полиноми Q и R, да је:

$$S = QT + R \quad \wedge \quad (R = 0 \ \vee \ dgR < dgT)$$

Уобичајено је да се $S = QT + R$ пише и у облику:

$$\frac{S}{T} = Q + \frac{R}{T} \quad \text{или} \quad S : T = Q + \frac{R}{T}$$

Доказ:

- Ако је $S = 0$, тада је $-QT = R$, одакле следи $Q = 0$ и $R = 0$ јер би у противном степен полинома на левој страни једнакости $-QT = R$ био већи од степена полинома на десној страни.
- Ако је $S \neq 0$ и $dgS < dgT$, тада очевидно мора бити $Q = 0$ и $S = R$ јер би се опет добили полиноми различитих степена на левој и десној страни једнакости $S = QT + R$
- Ако су $S \neq 0$ и $dgS \geq dgT$, тада се узима да је $S = a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n$ и $T = b_0 + b_1 t + b_2 t^2 + \ldots + b_m t^m$.

Сада ће бити дефинисан коначни низ полинома $S_1, S_2, \ldots, S_k$ чији су водећи коефицијенти означени са S_i, на следећи начин:

$$S_1 = S - a_n b_m^{-1} t^{n-m} T$$
$$S_2 = S_1 - s_1 b_m^{-1} t^{dgS_1 - m} T$$
$$\vdots$$
$$S_k = S_{k-1} - s_{k-1} b_m^{-1} t^{dg(S_{k-1}) - m} T$$

где је k најмањи природни број за који ће бити $S_k = 0$ или $dg(S_k) < dgT$.

Доказати да такав број k постоји. Ако је $S_k=0$ за неки природан број k, онда је доказ готов. У супротном случају је $dg(S)>dg(S_1)$, јер су полинома S и $a_n b_m^{-1} t^{n-m} T$ очевидно истог степена и имају једнаке водеће коефицијенте. На исти начин закључује се да је $dg(S_1)>dg(S_2)>dg(S_3)>\dots$, што значи да ће постојати такав природан број k за који је $dg(S_k)<dg(T)$. Заменом S_1 из прве у другу једнакост, затим заменом S_2 из друге у трећу једначину, ..., и, на крају заменом S_{k-1} из $k-1$-ве у k-ту једнакост следи да је $S=QT+R$, где је $R=S_k$ и $Q=a_n b_m^{-1} t^{n-m}+s_1 b_m^{-1} t^{dg(S_1)-m}+\dots+s_{k-1} b_m^{-1} t^{dg(S_{k-1})-m}$.

Ако би поред полинома Q и R који задовољавају услове теореме постојали и полиноми Q_1 и R_1 који задовољавају услове теореме, тада би се добило $S=QT+R$ и $S=Q_1T+R_1$, одакле одузимањем следи да је $-(Q-Q_1)T=R-R_1$, а одавде обавезно следи да је $R-R_1=0$ и $Q-Q_1=0$ јер би у противном у једнакости $-(Q-Q_1)T=R-R_1$ било да је степен полинома на левој страни виши од степена полинома на десној страни једнакости. Овиме је доказана и јединственост полинома Q и R. $\square$

8.24 Постоји тачно један такав нормализовани полином W да је $W = NZD(S,T)$, где су S и T такви полиноми да је бар један од њих различит од нуле.

Доказ:

- Ако је $S=0 \wedge T\neq 0$, тада је $NZD(S,T) = a^{-1}T$, где је a водећи коефицијент полинома T. Аналогно се доказује и случај када је $S\neq 0 \wedge T=0$.
- Нека је сада $dg(S) \geq dg(T)$. На основу претходне теореме (8.19 – теорема о дељењу полинома) важи:

$$S = QT + R_1 \quad \wedge \quad (R_1 = 0 \vee dg(R_1) < dg(T))$$
$$T = Q_1 R_1 + R_2 \quad \wedge \quad (R_2 = 0 \vee dg(R_2) < dg(R_1))$$
$$\vdots$$
$$R_{k-2} = Q_{k-1} R_{k-1} + R_k \quad \wedge \quad (R_k = 0 \vee dg(R_k) < dg(R_{k-1}))$$
$$R_{k-1} = Q_k R_k$$

Из приложеног алгоритма (познат као Еуклидов алгоритам) за добијање низа полинома $R_1, R_2, \ldots$ очевидно је да постоји природан број k за који је $R_{k+1}=0$ или $dg(R_k)=0$ јер је $dg(T) > dg(R_1) > dg(R_2) > \cdots > dg(R_{i-1}) > dg(R_i) \ldots$ Показаће се да је R_k заједнички делилац полинома S и T. Из последње једнакости следи $R_k | R_{k-1}$, што на основу претпоследње, имплицира да $R_k | R_{k-2}, \ldots$, а даље на основу друге следи да $R_k | T$, што на основу прве, имплицира $R_k | S$. Значи да је R_k заједнички делилац за S и T. Доказати сад да је R_k и највећи заједнички делилац S и T. Претпоставимо да су $W_1 | S$ и $W_1 | T$. Тада из прве једнакости и следи да $W_1 | R_1$, што заједно са другом имплицира $W_1 | R_2, \ldots$, а заједно с претпоследњом имплицира да $W_1 | R_k$ па је дакле $R_k = NZD(S,T)$, а тражени

нормализовани полином је $W=a^{-1}R_k$, где је a водећи коефицијент уз R_k. Јединственост полинома W једноставно се доказује контрадикцијом коришћењем последице 8.21.

$W_1 \neq W_2 \Rightarrow (W_1 | S \wedge W_1 \nmid T \wedge W_2 | S \wedge W_2 \nmid T \Rightarrow W_2 | W_1$ анализом и $W_1 | W_2$ из $(W_1 = aW_2$ и нормализ. $W_1 = W_2 \wedge a = 1)$ $\square$

8.34 (Безуова теорема) Вредност полинома P над полем F у тачки α, то јесте $(\Psi(P)(\alpha))$, једнака је остатку при дељењу полинома P полиномом $(-\alpha, 1) = t-\alpha = -\alpha+t$.

Доказ:

На основу теореме 8.19 (теорема о дељењу полинома) постоје јединствени полиноми Q и R $(R=0 \vee dg(R) < dg(t-\alpha))$ такви да је $P=(t-\alpha)Q+R$ одакле је због 8.30 (теорема о функцији Ψ): $\Psi(P)=\Psi(t-\alpha)\Psi(Q)+\Psi(R)$ односно:

$$(\forall x \in F)\ \Psi(P)(x) = (x-\alpha)\Psi(Q)+R.$$

Треба уочити да се у претходне три једнакости појављује шест бинарних операција: сабирање и множење полинома, функција и у пољу F. Такође је $R \in F$ због $R=0 \vee dg(R) < dg(t-\alpha)=1$ односно $R=0 \vee dg R=0$. Ако се узме да је $x=\alpha$, добија се:

$$\Psi(P)(\alpha)=(\alpha-\alpha)\Psi(\alpha)+R \text{ односно } \underline{\Psi(P)(\alpha)=R} \quad \square$$

8.39 Сваки полином P_n n-тог степена има највише n корена.

Доказ: Полином нултог степена очевидно има „нула" корена па је тврђење тачно за $n=0$. Ако P_n нема корена, доказ је завршен. Ако је $n>0$ и P_n има бар један корен α, доказ се изводи индукцијом по n. За $n=1$ следи да полином $P_1=a_0+a_1t$ има тачно један корен $-a_1^{-1}a_0$ јер једначина $a_0+a_1x=0$ има тачно једно решење у пољу F, па тврђење је тачно. Претпоставимо да је тврђење тачно за $n-1$ и докажимо да важи и за n. Како је $P_n=(t-\alpha)Q_{n-1}$ због теореме 8.35 и како по индуктивној претпоставци $dg(Q_{n-1})=n-1$, на основу индуктивне претпоставке следи да Q_{n-1} има највише $n-1$ корена, а из једнакости $P_n=(t-\alpha)Q_{n-1}$ тада следи да P_n има највише n корена.

$\square$

8.49 Нека је $P \in F_{[t]}$ полином другог или трећег степена. Тада је полином P сводљив над F акко ($\Leftrightarrow$) полином P има бар један корен у пољу F.

Доказ:

($\Rightarrow$) Ако је P полином другог или трећег степена и сводљив над пољем F, тада је дељив линеарним полиномом због дефиниције сводљивости и због 8.14 ($PQ \neq 0 \Rightarrow dg(PQ) = dg(P) + dg(Q)$) и чињенице да су једини начини представљања двојке и тројке као збира природних бројева: $2=1+1$, $3=2+1$, $3=1+2$. Како P има линеарни фактор, а сваки линеарни полином има један корен, следи да полином P има бар један корен.

($\Leftarrow$) Ако P има корен α, због теореме 8.35 тада следи да је $t-\alpha$ фактор полинома P (односно $P=(t-\alpha)Q$), тј. P је сводљив. $\square$

8.53 Сваки полином $P_n = a_0 + a_1 t + a_2 t^2 + \dots + a_n t^n$, n-тог степена, за $n>0$, над пољем комплексних бројева може се написати у облику $P = a_n (t-t_1)(t-t_2)\dots(t-t_n)$, где је t полином $(0,1)$, а $t_1, t_2, \dots t_n$ и a_n комплексни бројеви, односно константни полиноми.

Доказ: На основу основног става алгебре (8.52), полином P има бар један корен t_1 из скупа комплексних бројева, па због теореме 8.35 $P = (t-t_1)P_{n-1}$, где је P_{n-1} полином степена $n-1$. Сада се на полином P_{n-1} примени 8.52 и добија се да је $P_n = (t-t_1)(t-t_2)P_{n-2}$. Наставком овог поступка добија се да је $P_n = (t-t_1)(t-t_2)\dots(t-t_{n-1})P_1$. Како се сваки линеарни полином може написати у облику $a(t-\alpha)$, заменом $P_1 = a(t-t_n)$ у претходну једнакост и изједначавањем коефицијената уз t^n добија се да је $a = a_n$, односно тврђење теореме. $\square$

8.54 Ако су P полином над пољем реалних бројева P и α корен полинома P, тада је и конјуговани број $\bar{\alpha}$ корен полин. P.

Доказ:

Ако је a реалан број, јасно је да је тада $\bar{a}=a$. Како су структуре полинома и полиномских функција изоморфне над бесконачним пољем (8.43), онда је оправдано, само у том случају, да се $\psi(P)$ краће пише само са P, односно $\psi(P)(x)=P(x)$ за свако x из тог бесконачног поља. Нека је $P(x)=a_0+a_1x+a_2x^2+\dots+a_nx^n=a_n(x-x_1)(x-x_2)\dots(x-x_n)$, тада је:

$\overline{P(x)}=a_0+a_1\bar{x}+a_2\bar{x}^2+\dots+a_n\bar{x}^n=P(\bar{x})=a_n(\bar{x}-x_1)(\bar{x}-x_2)\dots(\bar{x}-x_n)$, па је

$P(x)=\overline{\overline{P(x)}}=\overline{a_n(\bar{x}-x_1)(\bar{x}-x_2)\dots(\bar{x}-x_n)}=a_n(x-\bar{x}_1)(x-\bar{x}_2)\dots(x-\bar{x}_n)$, одакле је очевидно да $P(\alpha)=0$ имплицира $P(\bar{\alpha})=0$. □

8.55 Сваки полином $P=a_0+a_1t+\dots+a_nt^n$ над пољем реалних бројева, може се написати у облику производа полинома степена нижих од 3, чији су коефицијенти реални бројеви.

Доказ: На основу теореме 8.53 полином P може се написати у облику $P_n=a_n(t-t_1)(t-t_2)\dots(t-t_n)$, где су $t_1,t_2,\dots t_n$ комплексни корени полинома P. Међутим ако је α корен полинома P над пољем реалних бројева, тада је и $\bar{\alpha}$ корен полинома P, па ако се помноже полиноми $(t-\alpha)$ и $(t-\bar{\alpha})$, добија се полином $t^2-2Re(\alpha)t+|\alpha|^2$ чији су коефицијенти реални бројеви. Настави ли се овај поступак докле год у полиному $P=a_n(t-t_1)(t-t_2)\dots(t-t_n)$ има комплексних бројева који нису реални, очевидно се добија полином P у облику који тврди теорема:

$$P_n=a_n(t^2+p_1t+q_1)\dots(t^2+p_kt+q_k)(t-t_{r_1})\dots(t-t_{r_m}),$$ где су

$p_i, q_i, t_{r_j}\in R$ и $t_{r_j}\in\{t_1,t_2,\dots,t_n\}$ за свако $i=1,2,3,\dots,k$ и $j=1,2,3,\dots,m$. □

8.69 Нула (корен) реда $k \geq 2$ полинома P је нула (корен) реда $k-1$ полинома P'. Број α је корен реда k полинома P акко је α заједнички корен полинома $P, P', P'', \dots, P^{(k-1)}$ и α није корен полинома $P^{(k)}$.

Доказ: Ако је α нула реда k полинома P, то значи да је

$$P(x) = (x-\alpha)^k Q(x) \text{ где } Q(\alpha) \neq 0.$$

Израчунати извод леве и десне стране претходне једнакости,

$$P'(x) = (x-\alpha)^{k-1}\left(kQ(x) + (x-\alpha)Q'(x)\right),$$ одакле следи да је α нула реда $k-1$ полинома P'. Други део тврђења теореме је последица првог дела, који је доказан. □

8.70 Нека је $\frac{p}{q}$ [redacted] рационалан број, где су p и q узајамно прости цели бројеви и нека су коефицијенти полинома $P = a_n t^n + a_{n-1} t^{n-1} + \dots + a_1 t + a_0$ цели бројеви. Тада ако је $\frac{p}{q}$ корен полинома P, онда су $p \mid a_0$ и $q \mid a_n$.

Доказ: Како је $\frac{p}{q}$ корен полинома P то је

$$(1) \quad a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \dots + a_1\frac{p}{q} + a_0 = 0 \quad / \cdot q^{n-1} \quad / \cdot \frac{q^n}{p}$$

$$(2) \quad a_n \frac{p^n}{q} + a_{n-1} p^{n-1} + \dots + a_1 p q^{n-2} + a_0 q^{n-1} = 0$$

$$(3) \quad a_n p^{n-1} + a_{n-1} p^{n-2} q + \dots + a_1 q^{n-1} + a_0 \frac{q^n}{p} = 0$$

где су једнакости (2) и (3) добијене из једнакости (1) множењем редом са q^{n-1} и $\frac{q^n}{p}$. Број $a_n \frac{p^n}{q}$ мора бити цео јер сви остали сабирци у једнакости (2) су цели бројеви. Како је $a_n \frac{p^n}{q}$ цео број тада a_n мора бити дељив са q јер су p и q узајамно прости бројеви. Аналогно се закључује да је a_0 дељив са p. □

Конструкција поља

9.1 Релација $\equiv_P$ дефинисана у скупу свих полинома $F[t]$ као $(\forall Q, S \in F[t])\ Q \equiv_P S \Leftrightarrow P \mid Q-S$ јесте конгруенција у односу на сабирање и множење полинома, где је P неки ненула полином из $F[t]$.

Доказ: Значи Q и S су у релацији $\equiv_P$ ако и само ако је њихова разлика дељива са P, тј. акко полиноми Q и S имају исте остатке при дељењу полинома P.

Релација је рефлексивна јер је $Q \equiv_P Q \Leftrightarrow P \mid Q-Q \Leftrightarrow P \mid 0 \Leftrightarrow$ тачно

Симетричност следи из $Q \equiv S \Rightarrow P \mid Q-S \Rightarrow P \mid S-Q \Rightarrow S \equiv_P Q$.

Релација је транзитивна јер $(Q \equiv_P S \wedge S \equiv_P R) \Rightarrow (P \mid Q-S \wedge P \mid S-R) \Rightarrow P \mid Q-R \Rightarrow Q \equiv_P R$. Релација $\equiv_P$ јесте релација еквиваленције. Релација $\equiv_P$ је конгруенција у односу на сабирање и множење полинома, јер је: $(Q \equiv_P S \wedge R \equiv_P T) \Rightarrow (P \mid (Q-S) \wedge P \mid (R-T)) \Rightarrow P \mid ((Q+R)-(S+T)) \Rightarrow Q+R \equiv_P S+T$ као и $(Q \equiv_P S \wedge R \equiv_P T) \Rightarrow (P \mid (Q-S) \wedge P \mid (R-T)) \Rightarrow (P \mid (QR-SR) \wedge P \mid (SR-ST)) \Rightarrow P \mid (QR-ST) \Rightarrow QR \equiv_P ST$.

Класа еквиваленције, с обзиром на релацију $\equiv_P$ којој припада полином Q, означиће се са $[Q]$, а фактор скуп са $F[t]/_{\equiv_P}$.

$\square$

9.2 Уређена тројка $(F[t]/_{\equiv_P}, +, \cdot)$ је комутативни прстен са јединицом, где су операције $+$ и $\cdot$ дефинисане са $(\forall Q, S \in F[t])$ $[Q]+[S]=[Q+S]$ и $[Q][S]=[QS]$.

Доказ:

Операције $+$ и $\cdot$ су логички добро дефинисане због теореме 5.32 (конгруенција $\ast$ са фактор скупом $G/_\ast$ чини групоид $(G/_\ast, \cdot)$). Асоцијативност операција следи из $([Q]+[R])+[S]=[Q+R]+[S]$ $=[(Q+R)+S]=[Q+(R+S)]=[Q]+[R+S]=[Q]+([R]+[S])$ и $([Q][R])[S]=[QR][S]=[(QR)S]=[Q(RS)]=[Q][RS]=[Q]([R][S])$, где су коришћене дефиниције операција у скупу $F[t]/_{\equiv_P}$ и асоцијативност операција $+$ и $\cdot$ у скупу полинома $F[t]$. Аналогно се доказују и комутативност операција $+$ и $\cdot$ и дистрибутивност операције $\cdot$ према операцији $+$ скупа $F[t]/_{\equiv_P}$. Неутрални елемент за операцију $+$ је $[0]$, односно класа којој припадају сви полиноми деливи са P која се може означити и са $[P]$, па је значи $0=[0]=[P]$. Неутрални елемент мултипликативне операције је $[1]$ јер $[1][Q]=[1\cdot Q]=[Q]$. Инверзни елемент, с обзиром на операцију $+$ увек постоји јер је $[Q]+[-Q]=[Q+(-Q)]=[0]=[P]$

$\square$

Детерминанте

10.18 Детерминанта је линеарна функција по свакој врсти, односно $\det A_{x_i+y_i} = \det A_{x_i} + \det A_{y_i}$ и важи теорема 10.13 ($\det_{\alpha x_i} = \alpha \det A_{x_i}$), где је $A=[a_{ij}]_{nn}$ нека матрица.

Доказ:

$$\underline{\det A_{x_i+y_i}} = \sum_{\sigma\in S_n} (-1)^{\operatorname{Inv}\sigma} a_{1\sigma(1)} a_{2\sigma(2)} \dots (x_{i\sigma(i)} + y_{i\sigma(i)}) \dots a_{n\sigma(n)} =$$

$$= \sum_{\sigma\in S_n} (-1)^{\operatorname{Inv}\sigma} a_{1\sigma(1)} a_{2\sigma(2)} \dots x_{i\sigma(i)} \dots a_{n\sigma(n)} + \sum_{\sigma\in S_n} (-1)^{\operatorname{Inv}\sigma} a_{1\sigma(1)} a_{2\sigma(2)} \dots y_{i\sigma(i)} \dots a_{n\sigma(n)}$$

$$= \det A_{x_i} + \det A_{y_i}$$

□

Системи линеарних једначина

11.12 Квадратни систем једначина S одређен је ако и само ако је детерминанта система различита од нуле.

Доказ: Дати систем S еквивалентним трансформацијама сведемо на њему еквивалентни систем S_1, који је у троугаоном облику. На основу особина детерминанти следи да је $\det S=0 \Leftrightarrow \det S_1=0$. Према томе, ако је $\det S\neq 0$, тада је и $\det S_1\neq 0$, па у троугаоном облику систем S_1, због теореме 17.15 постоји алгоритам

$$S_1: \begin{array}{l} a_{11}x + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ \quad\quad a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \quad\quad\quad \vdots \\ \quad\quad\quad a_{nn}x_n = b_n \end{array}$$

одакле следи да је систем одређен јер је $\det S_1 = a_{11}\dots a_{nn} \neq 0$. Обратно, ако је квадратни систем S одређен, тада је и њему еквивалентан троугаони систем S_1 обавезно квадратни и одређен, па матрица система S_1 на главној дијагонали има све елементе различите од нуле, а испод ње једнаке нули, што значи да је $\det S_1\neq 0$ односно $\det S\neq 0$.

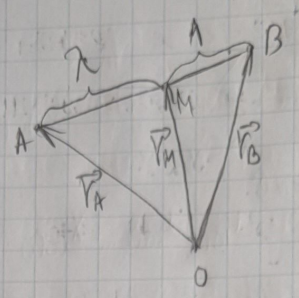
□

Аналитичка геометрија

13.3 (Деоба дужи у датој размери) Ако тачка M дели дуж AB у размери $\lambda:1$, тј. $\overrightarrow{AM}=\lambda\overrightarrow{MB}$, тада $\vec{r}_M=\dfrac{\vec{r}_A+\lambda\vec{r}_B}{1+\lambda}$

Доказ:

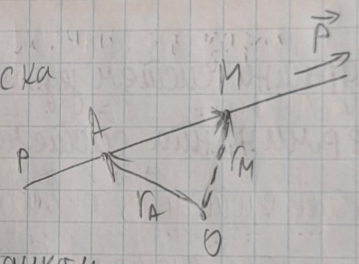
$$\overrightarrow{AM}=\lambda\overrightarrow{MB}$$
$$\vec{r}_M-\vec{r}_A=\lambda(\vec{r}_B-\vec{r}_M)$$
$$\vec{r}_M-\vec{r}_A=\lambda\vec{r}_B-\lambda\vec{r}_M$$
$$\vec{r}_M+\lambda\vec{r}_M=\vec{r}_A+\lambda\vec{r}_B$$
$$\vec{r}_M(1+\lambda)=\vec{r}_A+\lambda\vec{r}_B$$
$$\vec{r}_M=\frac{\vec{r}_A+\lambda\vec{r}_B}{1+\lambda}$$



□

13.4 Једначина праве p

Доказ: Нека је $\overrightarrow{OM}=\vec{r}_M=\vec{r}=(x,y,z)$ векторска променљива, односно променљива вектор положаја тачке на правој p.



Права p одређена је једном њеном тачком $A(x_A,y_A,z_A)\in p$ и вектором правца $\vec{p}=(p_1,p_2,p_3)\parallel p$. Тада је

$$\overrightarrow{AM}\parallel\vec{p}\iff(\overrightarrow{AM}=t\vec{p}\ \wedge\ t\in R)\iff\vec{r}_M-\vec{r}_A=t\vec{p}\iff\vec{r}_M=\vec{r}_A+t\vec{p}$$

$\vec{r}=\vec{r}_A+t\vec{p}$, $t\in R$ векторски облик једначине праве.

Ако уврстимо $\vec{r}=(x,y,z)$, $\vec{r}_A=(x_A,y_A,z_A)$, $p=(p_1,p_2,p_3)$ у претходну једначину добија се:

$$(x,y,z)=(x_A,y_A,z_A)+t(p_1,p_2,p_3)\iff(x,y,z)=(x_A+tp_1,\ y_A+tp_2,\ z_A+tp_3)\iff$$

$(x=x_A+tp_1\ \wedge\ y=y_A+tp_2\ \wedge\ z=z_A+tp_3)$ параметарски облик

Ако се изрази t из све три једнакости добија се:

$$t=\frac{x-x_A}{p_1}=\frac{y-y_A}{p_2}=\frac{z-z_A}{p_3}$$ канонички облик

□

13.5 Једна

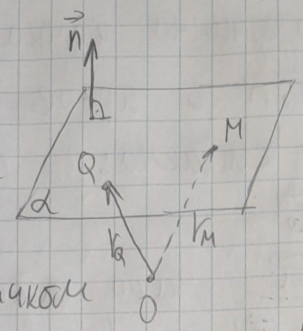
Доказ:

Нека је $\overrightarrow{OM}$
променљива
било које
Раван α
$Q(x_Q,y_Q,z_Q)$
$\vec{n}=(A,B,C$
$\overrightarrow{QM}\parallel\alpha$
$\iff\vec{r}_M$
$\vec{r}\vec{n}=$

Ако у пр
добијамо:
и ако за
другу стр
једначине
$(\vec{r}-\vec{r}_Q$
$\iff($
тј. доб

13.5 Једначина равни α

Доказ:



Нека је $\overrightarrow{OM} = \vec{r_M} = \vec{r} = (x, y, z)$ вектореки променљива, односно $\vec{r_M}$ је вектор положаја било које тачке са равни α.

Раван α одређена је једном својом тачком $Q(x_Q, y_Q, z_Q) \in \alpha$ и једним вектором нормалним на раван $\vec{n} = (A, B, C) \perp \alpha$. Тада је

$$\overrightarrow{QM} \parallel \alpha \iff \overrightarrow{QM} \perp \vec{n} \iff \overrightarrow{QM}\,\vec{n} = 0 \iff (\vec{r_M} - \vec{r_Q})\vec{n} = 0$$

$$\iff \vec{r_M}\vec{n} - \vec{r_Q}\vec{n} \iff \vec{r_M}\vec{n} = \vec{r_Q}\vec{n}$$

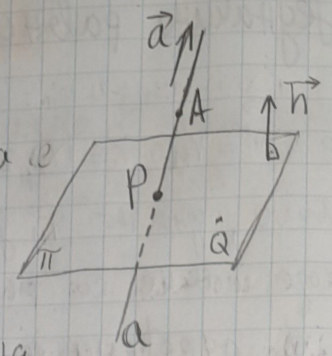
$\underline{\underline{\vec{r}\vec{n} = \vec{r_Q}\vec{n}}}$ векторски облик једначине равни α

Ако у претходној једначини заменимо $\vec{r} = (x, y, z)$, $\vec{n} = (A, B, C)$ и $r_Q = (x_Q, y_Q, z_Q)$ добијамо: $(x, y, z) \cdot (A, B, C) = (x_Q, y_Q, z_Q)(A, B, C) \iff Ax + By + Cz = Ax_Q + By_Q + Cz_Q$ и ако заменимо $Ax_Q + By_Q + Cz_Q$, тј. $\vec{r_Q} \cdot \vec{n}$ са $-D$ и пребацимо на другу страну добијамо $\underline{\underline{Ax + By + Cz + D = 0}}$ што је општи облик једначине равни, а ако заменимо исте векторе у једнакости $(\vec{r} - \vec{r_Q})\vec{n} = 0$ добијамо: $((x, y, z) - (x_Q, y_Q, z_Q))(A, B, C) = 0$

$\iff (x - x_Q, y - y_Q, z - z_Q)(A, B, C) = 0 \iff \underline{A(x - x_Q) + B(y - y_Q) + C(z - z_Q) = 0}$

тј. добијамо једначину равни кроз тачку Q. $\square$

13.11 Продор праве кроз раван



Доказ: Заједничка тачка P равни $\pi: \vec{r}\vec{n} = \vec{r_Q}\vec{n}$ и праве $a: \vec{r} = \vec{r_A} + t\vec{a}$ добија се решавањем система:

$$\begin{aligned} \vec{n}\vec{r_P} &= \vec{n}\vec{r_Q} \\ \vec{r_P} &= \vec{r_A} + t\vec{a} \end{aligned}$$

зато што вектор положаја тачке P, $\vec{r_P}$ задовољава обе једначине. Систем се решава тако што се $\vec{r_P}$ из једначине праве уврсти у једначину равни и из тако добијене једначине се изрази t које се после замени у једначину праве.

$$\begin{aligned} \vec{n}\vec{r_P} &= \vec{n}\vec{r_Q} \\ \vec{r_P} &= \vec{r_A} + t\vec{a} \end{aligned} \overset{①}{\Rightarrow} \vec{n}(\vec{r_A} + t\vec{a}) = \vec{n}\vec{r_Q} \Rightarrow \underline{\underline{\vec{r_P} = \vec{r_A} + \frac{(\vec{r_Q} - \vec{r_A})\vec{n}}{\vec{a}\vec{n}}\vec{a}}}$$

$$\vec{n}\vec{r_A} + t\vec{n}\vec{a} = \vec{n}\vec{r_Q}$$

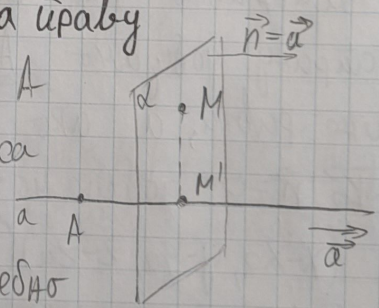
$$③ \quad t\vec{n}\vec{a} = \vec{n}\vec{r_Q} - \vec{n}\vec{r_A}$$

$$t = \frac{\vec{n}(\vec{r_Q} - \vec{r_A})}{\vec{n}\vec{a}} \quad ②$$

тачка продора P

□

13.20 Ортогонална пројекција тачке на праву



Доказ: Нека је права a одређена тачком A која јој припада и вектором правца $\vec{a}$ са којом је паралелна. Да би се добила пројекција тачке M, тј тачка M' потребно је конструисати раван α кроз тачку M нормалну на праву a, тј $\vec{n} = \vec{a}$. Сада тачка M' представља продор праве $a: \vec{r} = \vec{r_A} + t\vec{a}$ кроз раван $\alpha: \vec{a}\vec{r} = \vec{a}\vec{r_M}$ односно вектор положаја $\vec{r_M}$ исказан је формулом:

$$\underline{\underline{\vec{r_{M'}} = \vec{r_A} + \frac{(\vec{r_M} - \vec{r_A})\vec{a}}{\vec{a}\vec{a}}\vec{a}}}$$

која се добија уврштавањем одговарајућих вектора у формулу продора.

□

13.21

Доказ

тачко

норма

као о

на ра

на р

Сада

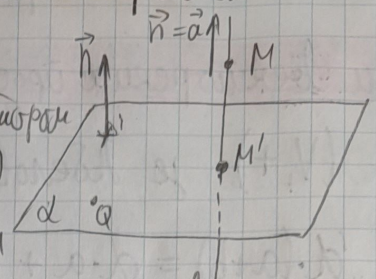
кроз

форм

тачке

13.21 Ортогонална пројекција тачке на раван

Доказ: Нека је раван α одређена тачком Q која јој припада и вектором нормале $\vec{n}$. За би се добило тачка M' као ортогонална пројекција тачке M на раван α потребно је конструисати праву a нормалну на раван α ($\vec{a}=\vec{n}$) која пролази кроз тачку M ($M \in a$). Сада тачка M' представља тачку продора праве a кроз раван α и увршћавањем одговарајућих вектора у формулу тачке продора, добијамо да је вектор положаја $\vec{r_{M'}}$ тачке M' исказан формулом: $\vec{r_{M'}} = \vec{r_M} + \frac{(\vec{r_Q}-\vec{r_M})\vec{n}}{\vec{n}\vec{n}}\vec{n}$



$\square$

Векторски простори

Аксиоми векторских простора:

V_1: $(V,+)$ је Абелова група

V_2: $\alpha\cdot(a+b) = \alpha\cdot a + \alpha\cdot b$

V_3: $(\alpha+\beta)\cdot a = \alpha\cdot a + \beta\cdot a$

V_4: $(\alpha\cdot\beta)\cdot a = \alpha\cdot(\beta\cdot a)$

V_5: $1\cdot a = a$

$(V,F,+,\cdot)$ - векторски простор

$\alpha,\beta\in F \ \wedge \ a,b\in V$

14.4 Ако је $(V,F,+,\cdot)$ векторски простор, тада за свако α из F и свако a из V важи:

1. $\alpha\cdot 0 = 0$
2. $0\cdot a = 0$
3. $\alpha\cdot a = 0 \iff a=0 \vee \alpha=0$
4. $(-\alpha)\cdot a = -(\alpha\cdot a)$
5. $\alpha(-a) = -(\alpha\cdot a)$
6. $(-\alpha)(-a) = \alpha\cdot a$
7. $-a = (-1)\cdot a$

Доказ:

1. $\underline{\alpha\cdot 0} \overset{V_1}{=} \alpha\cdot 0 + 0 \overset{V_1}{=} \alpha\cdot 0 + (\alpha\cdot 0 - (\alpha\cdot 0)) \overset{V_1}{=} (\alpha\cdot 0 + \alpha\cdot 0) - (\alpha\cdot 0) \overset{V_2}{=} \alpha(0+0) - (\alpha\cdot 0) \overset{V_1}{=} \alpha\cdot 0 - \alpha\cdot 0 \overset{V_1}{=} \underline{\underline{0}}$

2. $\underline{0\cdot a} \overset{V_1}{=} 0\cdot a + 0 \overset{V_1}{=} 0\cdot a + (0\cdot a - (0\cdot a)) \overset{V_1}{=} (0\cdot a + 0\cdot a) - (0\cdot a) \overset{V_3}{=} (0+0)\cdot a - (0\cdot a) \overset{V_1}{=} 0\cdot a - (0\cdot a) \overset{V_1}{=} \underline{\underline{0}}$

3. ($\Leftarrow$) На основу претходна два доказа следи $\underline{\alpha=0 \vee a=0 \Rightarrow \alpha\cdot a=0}$

($\Rightarrow$) Нека је $\alpha\cdot a=0$. Скалар α може бити једнак нули или различит од нуле. Ако је $\alpha=0$ тврђење је тачно, а ако је $\alpha\neq 0$ тада постоји њему инверзни α^{-1} у односу на множење у пољу F. Помножи ли се једнакост $\alpha\cdot a=0$ са α^{-1} добија се:

$$\alpha^{-1}\cdot(\alpha\cdot a)=\alpha^{-1}\cdot 0 \overset{1,V_4}{\Rightarrow} (\alpha^{-1}\cdot\alpha)\cdot a=0 \overset{F}{\Rightarrow} 1\cdot a=0 \overset{V_5}{\Rightarrow} a=0,$$

па важи $\underline{\alpha\cdot a=0 \Rightarrow \alpha=0 \vee a=0}$.

4. $\underline{(-\alpha)\cdot a} \overset{V_1}{=} (-\alpha)\cdot a+0 \overset{V_1}{=} (-\alpha)\cdot a+(\alpha\cdot a-(\alpha\cdot a)) \overset{V_1}{=} ((-\alpha)\cdot a+\alpha\cdot a)-(\alpha\cdot a)$
$\overset{V_3}{=} (-\alpha+\alpha)\cdot a-(\alpha\cdot a) \overset{F}{=} 0\cdot a-(\alpha\cdot a) \overset{1}{=} 0-(\alpha\cdot a) \overset{V_1}{=} \underline{-(\alpha\cdot a)}$

5. $\underline{\alpha\cdot(-a)} \overset{V_1}{=} \alpha\cdot(-a)+0 \overset{V_1}{=} \alpha(-a)+(\alpha a-(\alpha\cdot a)) \overset{V_1}{=} (\alpha(-a)+\alpha a)-(\alpha\cdot a)$
$\overset{V_2}{=} \alpha(-a+a)-(\alpha a) \overset{V_1}{=} \alpha\cdot 0-(\alpha a) \overset{2}{=} 0-(\alpha a) \overset{V_1}{=} \underline{-(\alpha\cdot a)}$

свако 6. $\underline{(-\alpha)(-a)} \overset{4}{=} -(\alpha(-a)) \overset{5}{=} -(-(\alpha a)) \overset{V_1}{=} \underline{\alpha a}$

7. $\underline{(-1)a} \overset{4}{=} -(1\cdot a) \overset{V_5}{=} \underline{-a}$ $\square$

14.10 Скуп свих линеарних комбинација n-торке вектора $A=(a_1,a_2,\dots,a_n)$ простора V јесте потпростор простора V. (тј. линеал $L(a_1,a_2,\dots,a_n)$ је потпростор простора V генерисан n-торком вектора A).

Доказ: На основу теореме 14.6 да би скуп $W=L(a_1,a_2,\dots,a_n)$ био потпростор простора V довољно је доказати:

$$(\forall x,y\in W)(\forall\alpha\in F)\quad x+y\in W \wedge \alpha x\in W.$$

Збир две линеарне комбинације је поново линеарна комбинација:

$(\alpha_1a_1+\alpha_2a_2+\dots+\alpha_na_n)+(\beta_1a_1+\beta_2a_2+\dots+\beta_na_n)=(\alpha_1+\beta_n)a_1+(\alpha_2+\beta_2)a_2+\dots+(\alpha_n+\beta_n)a_n$
$=\gamma_1a_1+\gamma_2a_2+\dots+\gamma_na_n$ где је $\gamma_i=\alpha_i+\beta_i$ за свако $i=1,2,\dots,n$.

Производ линеарне комбинације и скалара је линеарна комбинација:

$\beta(\alpha_1a_1+\alpha_2a_2+\dots+\alpha_na_n)=\beta\alpha_1a_1+\beta\alpha_2a_2+\dots+\beta\alpha_na_n=\gamma_1a_1+\gamma_2a_2+\dots+\gamma_na_n$ где је $\gamma_i=\beta\alpha_i$ за свако $i=1,2,\dots,n$. $\square$

14.13 Произвољна n-торка вектора $(a_1, a_2, \dots, a_n)$ је линеарно зависна ако и само ако је бар један од њених вектора линеарна комбинација преосталих вектора.

Доказ:

($\Rightarrow$) Ако је n-торка $(a_1, a_2, \dots, a_n)$ зависна, тада је у линеарној комбинацији n-торке која је једнака нули, бар један скалар различит од нуле. Вектор уз тај скалар очевидно се може написати као линеарна комбинација преосталих вектора.

($\Leftarrow$) Ако је неки вектор n-торке $(a_1, a_2, \dots, a_n)$ линеарна комбинација преосталих вектора, тада се пребацивањем свих вектора на једну страну добија линеарна комбинација n-торке $(a_1, a_2, \dots, a_n)$ једнака нули, а један скалар је јединица, односно различит од нуле, па је n-торка зависна. $\square$

14.21 (Теорема о максималној линеарној n-торки) Произвољна n-торка вектора јесте база простора V ако и само ако је та n-торка максимално линеарно независна.

Доказ:

($\Rightarrow$) Ако је n-торка B база простора V, тада додавањем произвољног вектора она постоје зависна, јер се тај вектор може изразити преосталим векторима, па је B заиста максимална линеарна независна n-торка.

($\Leftarrow$) Ако је n-торка $B = (a_1, a_2, \dots, a_n)$ максимално линеарно независна, а да би она била база, треба још доказати да генерише простор V. Доказати то контрадикцијом. Претпоставити ли се супротно, тј. да постоји вектор $x \notin \{a_1, a_2, \dots, a_n\}$ који се не може изразити као линеарна комбинација n-торке B, тада из $\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n + \alpha x = 0$ следи да је $\alpha = 0$ јер би се у супротном вектор x могао изразити као линеарна комбинација n-торке B), па се добија $\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n = 0$, а из тога, следи

$\alpha_1 = \alpha_2 = \dots = \alpha_n = 0$ јер је B линеарно независна. Добија се да је $B' = (a_1, a_2, \dots, a_n, x)$ линеарно независна $(n+1)$-торка, што је контрадикција са условом да је $B = (a_1, a_2, \dots, a_n)$ максимална линеарно независна n-торка, па је B генераторна, односно база. □

14.22 (Теорема о минималној n-торки генератора) Произвољна n-торка вектора B јесте база простора V ако и само ако је n-торка минимална n-торка генератора.

Доказ:

($\Rightarrow$) Ако је B база простора V, избацивањем произвољног вектора x из B добија се $(n-1)$-торка чијом се линеарном комбинацијом не може добити вектор x јер би тада B била зависна, па је B заиста минимална n-торка генератора.

($\Leftarrow$) Ако је B минимална n-торка генератора, тада да би она била и база простора V, треба доказати да је линеарно независна. Доказ се изводи контрадикцијом. Претпоставимо ли супротно, тј. да је B линеарно зависна, тада се бар један вектор n-торке B може представити као линеарна комбинација преосталих вектора, и они очевидно генеришу простор V, што је контрадикција са условом да је B минимална n-торка генератора, односно B је независна, а самим тим и база. □

14.23 (Теорема о јединственој репрезентацији) Произвољна n-торка вектора B јесте база простора V ако и само ако се сваки вектор простора V може на јединствен начин представити као линеарна комбинација вектора n-торке B.

Доказ:

($\Rightarrow$) Нека је $B=(a_1,a_2,\dots,a_n)$ база простора V. Доказаћа контрадикцијом да се сваки вектор x простора V може на јединствен начин представити као линеарна комбинација вектора базе B.:
Ако се претпостави супротно, тј. да постоје две различите репрезентације вектора вектора x у бази B, онда следи:
$x=\alpha_1 a_1+\alpha_2 a_2+\dots+\alpha_n a_n=\beta_1 a_1+\beta_2 a_2+\dots+\beta_n a_n$. Ово је даље еквивалентно са: $(\alpha_1-\beta_1)a_1+(\alpha_2-\beta_2)a_2+\dots+(\alpha_n-\beta_n)a_n=0$.
Како је B линеарно независна n-торка простора V, следи:
$\alpha_1-\beta_1=0 \wedge \alpha_2-\beta_2=0 \wedge \dots \wedge \alpha_n-\beta_n=0 \Leftrightarrow \alpha_1=\beta_1 \wedge \dots \wedge \alpha_n=\beta_n$.
Ово је у контрадикцији са претпоставком да постоје две различите репрезентације вектора x у бази B.

($\Leftarrow$) Поћи ће се од исказа да сваки вектор има јединствену репрезентацију у бази B. Тада и нула вектор има јединствену репрезентацију у бази B:
$0=\alpha_1 a_1+\alpha_2 a_2+\dots+\alpha_n a_n$ што имплицира $\alpha_1=\alpha_2=\dots=\alpha_n$ односно B је линеарно независна n-торка. Ка је по услову n-торка B и ченераторна, она је уједно и база простора V.

$\square$

14.26 Нека
векторско
$M=(\lambda_{11} a_1$
ако је
$(\forall \lambda_{ij} \in R)($

Доказ:
Раздвојимо
1° $m>n$
Уређена
простор
броју
$\dim W \leq$
вектора
$m>n$
може пр
бити мањ
M мора
2° $m \leq n$
Нека је
17.15 Мо

$B'_{mn}=\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$

i-та вр
k-та

Произвољна
и само ако се
н начин представља

а контрадикција
тивен начин
базе B.
раничите
нда следи:
е даље еквива-

V, следи:
... $\lambda_n \alpha_n = \beta_n$.
тоје две

има
или вектор

$= \alpha_n$ односно
n-торка
V.

$\square$

14.26 Нека је $(a_1, a_2, \dots, a_n)$ произвољна n-торка вектора из векторског простора $V = (V, R, +, \cdot)$. Тада уређена m-торка из V $M = (\lambda_{11} a_1 + \lambda_{12} a_2 + \dots + \lambda_{1n} a_n, \dots, \lambda_{m1} a_1 + \lambda_{m2} a_2 + \dots + \lambda_{mn} a_n)$ је зависна ако је $\operatorname{rang} [\lambda_{ij}]_{mn} < m$ за све $\lambda_{ij} \in R$, односно $(\forall \lambda_{ij} \in R)(\forall a_i \in V)\ (\operatorname{rang} [\lambda_{ij}]_{mn} < m \Rightarrow M$ је зависна.

Доказ:

Раздвојимо доказ на 2 случаја $1^\circ\ m > n$ $2^\circ\ m \leq n$

$1^\circ\ m > n$

Уређена n-торка вектора $(a_1, a_2, \dots, a_n)$ генерише неки потпростор $W = L(a_1, a_2, \dots, a_n)$ простора V. По теореми о броју генератора у односу на димензију простора важи $\dim W \leq n$. Сваки вектор m_i из M је линеарна комбинација вектора $a_1, a_2, \dots, a_n$ па свака од вектора m_i припада W. Како је $m > n \geq \dim W$ односно број вектора m је већи од простора које припадају па с обзиром да независних вектора мора бити мање или једнако од димензије простора закључујемо да M мора бити зависна n-торка.

$2^\circ\ m \leq n$

Нека је $\operatorname{rang} [\lambda_{ij}]_{mn} = r < m$. Матрица $B_{mn} = [\lambda_{ij}]_{mn}$ се на основу теореме 17.15 може написати у продужном облику који има исти rang

$$B'_{mn} = \begin{bmatrix} 1 & a_{12} & a_{13} & \dots & a_{1r+1} & \dots & a_{1n} \\ 0 & 1 & a_{23} & \dots & a_{2r+1} & \dots & a_{2n} \\ \vdots & \vdots & & & \vdots & & \vdots \\ 0 & 0 & \dots & 1 & a_{rr+1} & \dots & a_{rn} \\ 0 & 0 & 0 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 & \dots & 0 \end{bmatrix}$$

а како је $r < m$ онда постоји макар једна врста (k-та) која је потпуно попуњена 0. Из овога следи да постоје скалари $\alpha_1, \alpha_2, \dots, \alpha_{n-1}$ такви да кад се i-та врста помножи са α_i и дода k-тој врсти за свако $i = 1, 2, \dots, n-1$ k-та врста постане 0 вектор.

Свакој врсти i одговара вектор m_i из M, па скаларима $\alpha_1, \alpha_2, \dots, \alpha_{n-1}$ можемо множити векторе m_i, а додавати вектору m_k. Без губитка општости можемо узети да је $k=n$ јер заменом места врстама rang се не мења. На основу овога важи $\alpha_1 m_1 + \alpha_2 m_2 + \dots + \alpha_{n-1} m_{n-1} + m_n = 0$ и с обзиром да постоји скалар различит од нуле, односно уз m_n стоји 1 и на основу теореме 14.13 следи да је m-торка M зависна. $\square$

14.28 Нека је $(a_1, a_2, \dots, a_n)$ не зависна n-торка вектора из векторског простора $V=(V, R, +, \cdot)$. Тада $\operatorname{rang}[\lambda_{ij}]_{mn} < m$ ако и само ако је m-торка $M = (\lambda_{11}a_1 + \lambda_{12}a_2 + \dots + \lambda_{1n}a_n, \dots, \lambda_{m1}a_1 + \lambda_{m2}a_2 + \dots + \lambda_{mn}a_n)$ зависна, односно $(\forall \lambda_{ij} \in R)(\forall a_i \in V)$ $(\operatorname{rang}[\lambda_{ij}]_{mn} < m \iff M$ је зависна$)$.

Доказ:

($\Longrightarrow$) Директна последица претходне теореме (14.26) Како теорема важи за произвољну n-торку $(a_1, a_2, \dots, a_n)$ тако важи и за независну n-торку.

($\Longleftarrow$) Нека је m-торка M зависна ($n \geq m$). То значи да постоје скалари $\alpha_1, \alpha_2, \dots, \alpha_n$ од којих је макар један различит од нуле такви да је $\alpha_1 m_1 + \alpha_2 m_2 + \dots + \alpha_n m_n = 0$ односно ако би се вектор m_k уз који је $\alpha_k \neq 0$ написао као комбинација осталих вектора и цела једнакост поделила са α_k добило би се

$$m_k = \beta_1 m_1 + \beta_2 m_2 + \dots + \beta_{k-1} m_{k-1} + \beta_{k+1} m_{k+1} + \dots + \beta_n m_n \quad \text{где је } \beta_i = \frac{\alpha_i}{\alpha_k}$$

за $i = 1, 2, \dots, k-1, k+1, \dots, n$. Ако би се сада у матрици $B_{mn} = [\lambda_{ij}]_{mn}$ i-та врста помножила са β_i и додала k-тој врсти, k-та врста би постала 0 вектор, па пошто је једна врста матрице B_{mn} једнака нули, следи да сваки минор реда m (уколико постоји, односно ако је $n \geq m$) по особина детерминанте има вредност 0, односно rang никад неће бити m тј $\operatorname{rang}[\lambda_{ij}]_{mn} < m$. Ако је $n < m$, $\operatorname{rang}[\lambda_{ij}]_{mn} \in \{1, 2, \dots, n\}$

да је rang $[\lambda_{ij}]_{mn}$ свакако $< m$. $\square$

Линеарне трансформације

15.13 Уређена четворка $(Hom(V_1,V_2), F, +, \cdot)$ јесте векторски простор, где су $+$ и $\cdot$ бинарне операције из претходне дефиниције.

Доказ: Прво треба проверити да ли је $f+g \in Hom(V_1,V_2)$ ако су f и g из $Hom(V_1,V_2)$, односно да је збир два хомоморфизма опет хомоморфизам. Како је:

$(f+g)(\alpha x+\beta y) = f(\alpha x+\beta y) + g(\alpha x+\beta y) = \alpha f(x) + \beta f(y) + \alpha g(x) + \beta g(x)$
$= \alpha(f(x)+g(x)) + \beta(f(y)+g(y)) = \alpha(f+g)(x) + \beta(f+g)(y)$, то је $f+g \in Hom(V_1,V_2)$. Значи $(Hom(V_1,V_2),+)$ јесте групоид, и даље се показује да је и Абелова група.

Асоцијативност операције $+$ једноставно се проверава по дефиницији те операције: $((f+g)+h)(x) = (f+g)(x) + h(x) = (f(x)+g(x)) + h(x)$
$= f(x) + (g(x)+h(x)) = f(x) + (g+h)(x) = (f+(g+h))(x)$

Неутрални елемент је функција $O: V_1 \to V_2$ дефинисана са $O(x)=0$. Наравно треба проверити да ли $O \in Hom(V_1,V_2)$ тј да ли је $O(\alpha x+\beta y) = \alpha O(x) + \beta O(y)$ за све x и y из V_1 и α и β из F. Очигледно је да је једнакост увек тачна јер је увек еквивалентна са $0=0$

Пре испитивања постојања инверзног елемента доказаће се да λf јесте хаманорфизам за ска ко λ из F и f из $Hom(V_1,V_2)$. Како је:

$(\lambda f)(\alpha x+\beta y) = \lambda f(\alpha x+\beta y) = \lambda(\alpha f(x) + \beta f(y)) = \alpha\lambda f(x) + \beta\lambda f(y)$
$= \alpha(\lambda f)(x) + \beta(\lambda f)(y)$ тј $\lambda f \in Hom(V_1,V_2)$.

Како се инверзни елемент за f у односу на сабирање у сваком векторском простору обележава са $-f$, то треба доказати да за сваки $f \in Hom(V_1,V_2)$ постоји $-f \in Hom(V_1,V_2)$ такав да за свако $x \in V_1$ важи $f(x) + (-f)(x) = O(x)$ тј $f + (-f) = O$.

Доказати и да тражени хомоморфизам $-f$ јесте $-f=(-1)f$.
Показано је да $\lambda f \in Hom(V_1,V_2)$ за свако $\lambda \in F$ и $f \in Hom(V_1,V_2)$, па је онда и $-f=(-1)f \in Hom(V_1,V_2)$, што значи да остаје још само доказати да је $f+(-f)=\mathcal{O}$, што следи из:

$(f+(-1)f)(x) = f(x)+((-1)f)(x) = f(x)+(-1)f(x) = f(x)-(1\cdot f(x))$
$= f(x)-f(x) = 0 = \mathcal{O}(x)$.

Комутативност операције $+$ очевидна је из дефиниције.
Доказаће се још друга аксиома векторског простора, то јесте аксиома $\alpha(f+g)=\alpha f+\alpha g$. Како је за свако x из V_1:

$(\alpha(f+g))(x) = \alpha(f+g)(x) = \alpha(f(x)+g(x)) = \alpha f(x)+\alpha g(x) = (\alpha f)(x)+(\alpha g)(x)$
$= (\alpha f+\alpha g)(x)$, то јесте $\alpha(f+g)=\alpha f+\alpha g$.

Преостале три аксиоме аналогно се проверавају по дефиницији операција $+$ и $\cdot$ и дефиницији хомоморфизма. $\square$

15.14 Уређена тројка $(Hom(V),+,\circ)$ јесте прстен, где је операција $+$ сабирање хомоморфизама, а $\circ$ композиција функција

Доказ: Доказ да је $(Hom(V),+)$ као из 15.13. Познато је да је композиција асоцијативна. Преостало је да се докаже да $f\circ g \in Hom(V)$ за све f и g из $Hom(V)$ и да важи закон дистрибутивности.
Нека су f и g из $Hom(V)$. Тада је

$(f\circ g)(\alpha x+\beta y) = f(g(\alpha x+\beta y)) = f(\alpha g(x)+\beta g(y)) = \alpha f(g(x))+\beta f(g(x))$
$= \alpha(f\circ g)(x)+\beta(f\circ g)(y)$, што значи да је $f\circ g \in Hom(V)$.

Доказати сада дистрибутивност. Како је за свако x из V:

$(f\circ(g+h))(x) = f((g+h)(x)) = f(g(x)+h(x)) = f(g(x))+f(h(x)) = (f\circ g)(x)+(f\circ h)(x)$
$= (f\circ g+f\circ h)(x)$, то је $f\circ(g+h) = f\circ g+f\circ h$. $\square$

15.15 (Основни став линеарне алгебре) Нека су V_1 и V_2 векторски простора над телом F и нека је $(a_1, \dots, a_n)$ база простора V_1. Тада је за сваку n-торку вектора $(b_1, b_2, \dots, b_n) \in V_2^n$ једнозначно одређена линеарна трансформација $f: V_1 \to V_2$ за коју важи $f(a_i) = b_i$ за све $i \in \{1, 2, \dots, n\}$

Доказ: Доказаће се прво јединственост такве линеарне трансформације. Претпоставимо да постоје две такве линеарне трансформације f и g за које важи $f(a_i) = g(a_i) = b_i$. Сада за произвољни вектор $x = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n \in V_1$ важи:

$$f(x) = f(\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n) = \alpha_1 f(a_1) + \alpha_2 f(a_2) + \dots + \alpha_n f(a_n) =$$
$$= \alpha_1 g(a_1) + \alpha_2 g(a_2) + \dots + \alpha_n g(a_n) = g(\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n) = g(x)$$

што значи да је $f = g$.

Доказати постојање такве линеарне трансформације f. Функција $f: V_1 \to V_2$ дефинисаће се на следећи начин:

$$f(x) = f(\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n) \overset{def}{=} \alpha_1 b_1 + \alpha_2 b_2 + \dots + \alpha_n b_n$$

за произвољни вектор $x = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n \in V_1$. Да би f била линеарна трансформација мора да важи $f(\theta x + \psi y) = \theta f(x) + \psi f(y)$ за свако θ и ψ из F и свака два вектора $x = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n$ и $y = \beta_1 a_1 + \beta_2 a_2 + \dots + \beta_n a_n$ из V_1.

$$\underline{f(\theta x + \psi y)} = f(\theta(\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n) + \psi(\beta_1 a_1 + \beta_2 a_2 + \dots + \beta_n a_n))$$
$$= f(\theta \alpha_1 a_1 + \theta \alpha_2 a_2 + \dots + \theta \alpha_n a_n + \psi \beta_1 a_1 + \psi \beta_2 a_2 + \dots + \psi \beta_n a_n))$$
$$= f((\theta \alpha_1 + \psi \beta_1) a_1 + (\theta \alpha_2 + \psi \beta_2) a_2 + \dots + (\theta \alpha_n + \psi \beta_n) a_n)$$
$$= (\theta \alpha_1 + \psi \beta_1) b_1 + (\theta \alpha_2 + \psi \beta_2) b_2 + \dots + (\theta \alpha_n + \psi \beta_n) b_n$$
$$= \theta \alpha_1 b_1 + \theta \alpha_2 b_2 + \dots + \theta \alpha_n b_n + \psi \beta_1 b_1 + \psi \beta_2 b_2 + \dots + \psi \beta_n b_n$$
$$= \theta(\alpha_1 b_1 + \alpha_2 b_2 + \dots + \alpha_n b_n) + \psi(\beta_1 b_1 + \beta_2 b_2 + \dots + \beta_n b_n)$$
$$= \theta f(\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n) + \psi f(\beta_1 a_1 + \beta_2 a_n + \dots + \beta_n a_n)$$
$$= \underline{\underline{\theta f(x) + \psi f(y)}} \Rightarrow f(x) \text{ јесте ЛТ}$$

$\square$

15.17 Нека
n-торка ве
$f: V_1 \to V_2$ л
ако и сам
база про
Доказ: (
1. Доказа
Из $\alpha_1 f(a_1)$
$f(\alpha_1 a_1 + \alpha_n$
следи да
$(a_1, a_2, \dots,$
независн
2. Доказ
Узета про
функције
база про
да је x
$y = f(x)$
у прос
($\Leftarrow$) Нек
3. Доказ
Из $f(x) = f$
линеарнос
а због н
$\alpha_1 - \beta_1 =$
однос

15.17 Нека су V_1 и V_2 векторски простори над пољем F и нека је n-торка вектора $(a_1, a_2, \dots, a_n)$ база простора V_1 и нека је функција $f: V_1 \to V_2$ линеарна трансформација. Тада f јесте изоморфизам, ако и само ако уређена n-торка вектора $(f(a_1), f(a_2), \dots, f(a_n))$ јесте база простора V_2.

Доказ: ($\Rightarrow$) Нека је f изоморфизам.

1. Доказати независност n-торке $(f(a_1), f(a_2), \dots, f(a_n))$.

Из $\alpha_1 f(a_1) + \alpha_2 f(a_2) + \dots + \alpha_n f(a_n) = 0$, због линеарности следи да је $f(\alpha_1 a_1 + \alpha_n a_n + \dots \alpha_n a_n) = 0$, а због инјективности и због $f(0) = 0$ следи да је $\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n = 0$. Због независности n-торке $(a_1, a_2, \dots, a_n)$ сада је $\alpha_1 = \alpha_2 = \dots = \alpha_n = 0$ тј. $(f(a_1), f(a_2), \dots, f(a_n))$ је независна n-торка простора V_2.

2. Доказати сада да је $(f(a_1), f(a_2), \dots, f(a_n))$ и генераторна.

Узети произвољан вектор y из V_2. Тада због сурјективности функције f постоји $x \in V_1$ такав да је $y = f(x)$. Како је $(a_1, a_2, \dots, a_n)$ база простора V_1, онда постоје скалари $\alpha_1, \alpha_2, \dots, \alpha_n \in F$ такви да је $x = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n$. Због линеарности функције f следи $y = f(x) = \alpha_1 f(a_1) + \alpha_2 f(a_2) + \dots + \alpha_n f(a_n)$, што значи да је сваки елемент y простора V_2 линеарна комбинација вектора n-торке $(f(a_1), f(a_2), \dots, f(a_n))$

($\Leftarrow$) Нека је $(f(a_1), f(a_2), \dots, f(a_n))$ база простора V_2.

3. Доказати инјективност функције f.

Из $f(x) = f(y)$ односно $f(\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n) = f(\beta_1 a_1 + \beta_2 a_2 + \dots + \beta_n a_n)$ због линеарности следи да је $(\alpha_1 - \beta_1) f(a_1) + (\alpha_2 - \beta_2) f(a_2) + \dots + (\alpha_n - \beta_n) f(a_n) = 0$ а због независности n-торке $(f(a_1), f(a_2), \dots, f(a_n))$ следи да је

$\alpha_1 - \beta_1 = 0 \wedge \alpha_2 - \beta_n = 0 \wedge \dots \wedge \alpha_n - \beta_n = 0 \Leftrightarrow \alpha_1 = \beta_1 \wedge \alpha_2 = \beta_2 \wedge \dots \wedge \alpha_n = \beta_n$

односно $x = y$ што значи да је f инјективна.

4. Доказати сада сурјективност функције f.

Како је n-торка вектора $(f(a_1), f(a_2), \dots, f(a_n))$ и генератори то за сваки $y \in V_2$ постоје скалари $\lambda_1, \lambda_2, \dots, \lambda_n \in F$ такви да је $y = \lambda_1 f(a_1) + \lambda_2 f(a_2) + \dots + \lambda_n f(a_n)$. Нека је $x = \lambda_1 a_1 + \lambda_2 a_2 + \dots + \lambda_n a_n$. Тада због линеарности $f(x) = f(\lambda_1 a_1 + \lambda_2 a_2 + \dots + \lambda_n a_n) =$
$= \lambda_1 f(a_1) + \lambda_2 f(a_2) + \dots + \lambda_n f(a_n) = y$ тј. $f(x) = y$, односно f је сурјективна јер је доказано да за свако $y \in V_2$ постоји $x \in V_1$ тако да је $f(x) = y$. $\square$

Матрице и линеарне трансформације

16.33 Свака линеарна трансформација f из скупа свих линеарних трансформаца $L_{22} = \{f : \mathbb{R}^2 \to \mathbb{R}^2 \mid f \text{ је линеарна трансформација}\}$ има облик $f(x_1, x_2) = (ax_1 + bx_2, cx_1 + dx_2)$, где су a, b, c и d неки реални бројеви, који су једнозначно одређени за дату линеарну трансформацију.

...

Доказ:

Нека је f нека произвољна линеарна трансформација из L_{22} и нека се вектори $(1,0)$ и $(0,1)$ пресликавају са f редом у векторе (a,c) и (b,d) односно $f(1,0) = (a,c)$ и $f(0,1) = (b,d)$, чиме је због теореме 15.13. (основни став линеарне алгебре) линеарна трансформација f једнозначно одређена. Сада због линеарности функције f следи

$$f(x_1, x_2) = f(x_1(1,0) + x_2(0,1)) = x_1 f(1,0) + x_2 (0,1) = x_1(a,c) + x_2(b,d) =$$
$$= (ax_1 + bx_2, cx_1 + dx_2).$$

$\square$

Ранг матрице и инверзна матрица

17.12 Еквивалентним односно елементарним трансформацијама ранг матрице се не мења.

Доказ: Како се заменом места врстама у квадратној матрици мења знак њен њене детерминанте, а апсолутна вредност се не мења, и како множењем једне врсте матрице X са λ, детерминанте те нове матрице је $\lambda \det(X)$, следи да примена првих двеју еквивалентних трансформација не мења ранг матрице. Покажимо да и трећа не мења ранг.

Ако се некој квадратној подматрици X нека врста дода некој другој врсти, $\det X$ тај минор се не мења због теореме 10.16 (Гаусов алгоритам).

Нека је ранг матрице M_{mn} једнак r. Уочимо сада неку подматрицу C_{rr} матрице M_{mn} такву да је $\det C_{rr} \neq 0$ (која постоји јер је $\operatorname{rang} M_{mn} = r$) и неку врсту која не пролази кроз C_{rr}. Означимо са $b_1, b_2, \dots, b_r$ оне елементе те врсте који припадају колонама које пролазе кроз уочени минор. Нека је A_{rr} подматрица добијена од подматрице C_{rr} тако што је i-та врста подматрице C_{rr} замењена са $b_1, b_2, \dots, b_r$ и нека је B_{rr} подматрица добијена од подматрице C_{rr} тако што је i-тој врсти додата врста $b_1, b_2, \dots, b_r$. Сада на основу теореме 10.18 (особина детерминанти) следи да је $\det C_{rr} + \det A_{rr} = \det B_{rr}$. Како је $\det C_{rr} \neq 0$, то из претходне једнакости следи да је бар један од минора $\det B_{rr}$ и $\det A_{rr}$ различит од нуле, а како су они оба реда r, следи да се ранг матрице M_{mn} неће смањити. Ранг се неће ни повећати, јер кад су $\det C_{r+1,r+1} = 0$ и $\det A_{r+1,r+1} = 0$, то је и $\det B_{r+1,r+1} = \det C_{r+1,r+1} + \det A_{r+1,r+1} = 0 + 0 = 0$.

$\square$

17.15 Ако је r ранг матрице $B_{mn}=[b_{ij}]_{mn}$, тада се, еквивалентним трансформацијама, од те матрице може добити матрица ★

$$★\quad \begin{bmatrix} 1 & a_{12} & a_{13} & a_{14} & \cdots & a_{1r+1} & \cdots & a_{1n} \\ 0 & 1 & a_{23} & a_{24} & \cdots & a_{2r+1} & \cdots & a_{2n} \\ 0 & 0 & 1 & a_{34} & \cdots & a_{3r+1} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & 1 & a_{rr+1} & \cdots & a_{rn} \\ 0 & 0 & 0 & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & \cdots & 0 \end{bmatrix}$$

у којој не постоје елементи испод главне дијагонале и r-те врсте различити од нуле, а првих r елемената на главној дијагонали су јединице. Очевидно је да матрица облика ★ има ранг r.

Матрице облика ★ назваће се степенасте матрице, а матрице које се од матрица облика ★ разликују само у томе што су уместо јединица бројеви различити од нуле, биће такође степенасте матрице.

Доказ: Строги доказ ове теореме даје се индукцијом по броју врста m матрице $[b_{ij}]_{mn}$, за свако n. За $r=\operatorname{rang} B_{mn}=0$ тврђење је очевидно тачно. Нека је сада $r=\operatorname{rang} B_{mn}\neq 0$ односно $B_{mn}\neq 0$. За $m=1$ тврђење је тачно јер тада матрица има само једну врсту у којој је бар један елемент различит од нуле због $B_{mn}\neq 0$. Како сада матрица има само једну врсту заменићемо места колонама тако да на првом месту буде елемент различит од нуле, а потом целу тд врсту поделити са елементом који се налази на првом месту.

Претпоставимо сада да је тврђење тачно за m и докажимо да важи и за $m+1$. Уочити матрицу $B_{m+1,n}$ од $m+1$ врста. Ова матрица се еквивалентним трансформацијама једноставно своди на матрицу у којој је први елемент прве врсте јединица, а сви остали елементи прве колоне једнаки нули, што је могуће јер је $B_{m1} \neq 0$ (Гаусовим алгоритмом). Ако је матрица $B_{m+1,n}$ имала само једну колону доказ је готов. Ако је имала две или више колоне, тада се брисањем прве врсте и прве колоне добија матрица од m врста која је или нула матрица или се на њу може применити индуктивна претпоставка. После овога, у оба случаја очевидно је добијена матрица траженог облика, па је доказ индукцијом завршен.

$\square$

17.19 За сваку квадратну матрицу B_{nn} важи да је њена детерминанта различита од нуле ако и само ако су њени вектори колоне (врсте) линеарно независна, тј:

$$\det B_{nn} \neq 0 \iff (b_1, b_2, \dots, b_n) \text{ је независна,}$$

где је $b_i = (b_{1i}, b_{2i}, \dots, b_{ni})$ i-ти вектор колоне матрице $B_{nn} = [b_{ij}]_{nn}$ за свако $i = 1, 2, \dots, n$.

Доказ:

($\Rightarrow$) Ако је $\det B_{nn} \neq 0$, тада је n-торка вектора $(b_1, b_2, \dots, b_n)$ независна. Доказ се изводи контрадикцијом, односно претпоставком да је n-торка вектора $(b_1, b_2, \dots, b_n)$ зависна. Тада се бар једна колона b_k од колона те n-торке може написати као линеарна комбинација преосталих колона и нека су скалари у тој линеарној комбинацији редом $\lambda_1, \lambda_2, \lambda_3, \dots, \lambda_{n-1}$. Ако се свака од преосталих колона помножи са $-\lambda_1, -\lambda_2, \dots, -\lambda_{n-1}$ и дода колони b_k, добиће се у колони b_k све нуле, то јесте да је $\det B_{nn} = 0$, што је контрадикција услову.

($\Leftarrow$) Нека је n-торка вектора $(b_1, b_2, \dots, b_n)$ независна. Тада је $\det B_{nn} \neq 0$. Доказ иде контрадикцијом то јесте претпоставка да је $\det B_{nn} = 0$, што значи да је $\operatorname{rang} B_{nn} < n$, односно $\dim L(b_1, b_2, \dots, b_n) < n$ због теореме 17.16. Како n-торка вектора $(b_1, b_2, \dots, b_n)$ генерише простор димензије мање од n, по теореми 14.38 n-торка $(b_1, b_2, \dots, b_n)$ линеарно је зависна, што је контрадикција услову.

$\square$

17.24 Нека је $(a_1, \dots, a_n)$ произвољна n-торка вектора из векторског простора $V=(V, R, +, \cdot)$ која генерише потпростор $W=(W, R, +, \cdot)$. Ако је $\dim W < m$ тада уређена m-торка вектора $M=(\lambda_{11} a_1 + \dots + \lambda_{1n} a_n, \dots, \lambda_{m1} a_1 + \dots + \lambda_{mn} a_n)$ је увек зависна.

Доказ: Како број m вектора у m-торци M је већи од димензије простора којем припадају сви вектори те m-торке M, то онда по теореми да је број независних мањи или једнак од генераторних следи тврђење.

17.25 Нека је $(a_1, \dots, a_n)$ зависна n-торка вектора из векторског простора $V=(V, R, +, \cdot)$. Тада m-торка вектора $M=(\lambda_{11} a_1 + \dots + \lambda_{1n} a_n, \dots, \lambda_{m1} a_1 + \dots + \lambda_{mn} a_n)$ за $m \geq n$ је увек зависна.

Доказ: n-торка $(a_1, \dots, a_n)$ генерише потпростор $W=L(a_1, a_2, \dots, a_n)$, а како је n-торка зависна онда је $\dim W < n \leq m$. Вектори m-торке M припадају простору W, а пошто је њихов број већи од димензије простора, они не могу бити независни, па су они зависни.