УНИВЕРЗИТЕТ У КРАГУЈЕВЦУ
ПРИРОДНО–МАТЕМАТИЧКИ ФАКУЛТЕТ

Линеарна алгебра 1

СКРИПТА

КРАГУЈЕВАЦ
2024

Садржај

Предговор

Скрипта за предмет Линеарна алгебра 1.

Глава 1

Алгебарске структуре

1.1 Бинарне операције, основне структуре и морфизми

Нека је A непразан скуп и f пресликавање скупа $A \times A$ у скуп A. Дакле, нека елементи a и b из A, као уређени пар $(a, b) \in A^2$, одређују пресликавањем f један елемент c из A, тако да је $c = f(a, b)$. Чини се, као да елементи a и b из A одређују трећи елемент c, такође из A. Елементи a и b из A ступају у једну операцију којом се добија елемент c из A.

Дефиниција 1.1. Пресликавање $f : A \times A \to A$ се зове бинарна операција на скупу A.

Надаље ћемо са $*$, или на неки други начин, на пример са $\circ$, $\oplus$, $\odot$, $\square$, $+$, $\ldots$ означавати бинарну операцију у смислу претходне дефиниције. Тада кажемо да је скуп A снабдевен операцијом $*$. Ту чињеницу ћемо симболизовати са $(A, *)$.

Наравно, могуће је у истом скупу дефинисати више операција, на пример, у скупу $\mathbb{R}$ операције $+$ и $\cdot$. Тада бисмо имали означавање $(\mathbb{R}, +, \cdot)$.

За $(A, *)$ кажемо да је алгебарска структура. Та је структура богатија ако операција $*$ обилује већим бројем особина. Било која уведена бинарна операција има извесне особине. Природно је испитивати да ли та операција има бар неке од особина које имају, на пример, нама добро познате операције сабирање и множење у скупу реалних бројева. Међутим, ваља испитати да ли уведена операција има и неке друге особине.

Стога ћемо, пре него што приступимо детаљнијем испитивању неких алгебарских структура, дефинисати основне особине бинарних операција.

Нека је бинарна операција $*$ дефинисана у непразном скупу A.

Дефиниција 1.2. Кажемо да је бинарна операција $*$ асоцијативна ако за свако $a, b, c \in A$ важи

$$a * (b * c) = (a * b) * c.$$

Дакле, ако је операција $*$ асоцијативна, могуће је писати

$$a * (b * c) = (a * b) * c = a * b * c.$$

Дефиниција 1.3. Бинарна операција $*$ је комутативна, ако за свако $a, b \in A$ важи једнакост

$$a * b = b * a.$$

Дефиниција 1.4. Ако у $(A, *)$ постоји елемент e, такав да је за свако $a \in A$

$$a * e = e * a = a,$$

кажемо да је $e \in A$ неутрални или јединични елемент за операцију $*$.

Понекада, за јединични елемент се каже да је јединица.

Теорема 1.1. Ако у $(A, *)$ постоји неутрални елемент, онда је он јединствен.

Доказ. Претпоставимо супротно, тј. да у скупу A постоје два елемента e и f $(e \neq f)$, таква да је за свако $a \in A$

$$a * e = e * a = a$$

и

$$a * f = f * a = a.$$

Како је a произвољан елемент из A, ставимо $a = f$ у првој једнакости и $a = e$ у другој. Тада добијамо

$$f * e = e * f = f$$

и

$$e * f = f * e = e,$$

одакле следује $e = f$, што је у контрадикцији са претпоставком $e \neq f$. □

Дефиниција 1.5. Ако у $(A, *)$ постоји неутрални елемент e и ако за $a \in A$ постоји елемент $a^{-1} \in A$, такав да је

$$a^{-1} * a = a * a^{-1} = e,$$

кажемо да је a^{-1} инверзни елемент за $a \in A$, у односу на операцију $*$.

Наравно, ако, у смислу претходне дефиниције постоји $a^{-1} \in A$, тада је $a \in A$ инверзни елемент за a^{-1}. Важи, дакле, $(a^{-1})^{-1} = a$.

Уместо ознаке a^{-1} за инверзни елемент користимо и ознаку a'.

Теорема 1.2. Нека у $(A, *)$ постоји неутрални елемент e и нека је $*$ асоцијативна операција. Ако за елемент $a \in A$ постоји инверзни елемент $a^{-1} \in A$, тада је он јединствен.

Доказ. Претпоставимо супротно, тј. нека за $a \in A$ постоје два међу собом различита инверзна елемента a_1^{-1} и a_2^{-1}. Тада важи

$$a_1^{-1} = a_1^{-1} * e = a_1^{-1} * (a * a_2^{-1}) = (a_1^{-1} * a) * a_2^{-1} = e * a_2^{-1} = a_2^{-1},$$

што је у супротности са учињеном претпоставком. □

Изучићемо сада неке алгебарске структуре. Нека је $*$ једна бинарна операција дефинисана у непразном скупу G.

Дефиниција 1.6. За алгебарску структуру $(G, *)$ кажемо да је групоид.

Дефиниција 1.7. Ако је операција $*$ асоцијативна, за структуру $(G, *)$ кажемо да је асоцијативни групоид или полугрупа (или семигрупа).

Пример 1.1. Како је операција сабирања у скупу природних бројева $\mathbb{N}$ асоцијативна, структура $(\mathbb{N}, +)$ је асоцијативни групоид.

Дефиниција 1.8. Ако у групоиду $(G, *)$ постоји неутрални елемент, тада кажемо да је групоид $(G, *)$ са јединицом.

Пример 1.2. Структуре $(\mathbb{N}_0, +)$ и $(\mathbb{N}, \cdot)$ су групоиди са јединицом. Неутрални елементи у овим структурама су 0 и 1, респективно.

Дефиниција 1.9. Нека је бинарна операција $*$, дефинисана у скупу G. За групоид $(G, *)$ кажемо да је група ако су испуњени следећи услови:

(Г1) Операција $*$ је асоцијативна;

(Г2) У скупу G постоји неутрални елемент за операцију $*$;

(Г3) За сваки елемент из G постоји у G њему инверзни елемент у односу на операцију $*$.

Дефиниција 1.10. За групу $(G, *)$ кажемо да је комутативна или Абелова, ако операција $*$ има особину комутативности.

Ако скуп G садржи коначан број елемената, на пример n, за групу $(G, *)$ кажемо да је коначног реда n.

Дефиниција 1.11. Нека су $(G_1, *)$ и $(G_2, \circ)$ групе и нека је f пресликавање скупа G_1 у скуп G_2 такво да је, за свако $a, b \in G_1$,

$$f(a * b) = f(a) \circ f(b).$$

За пресликавање f кажемо да је хомоморфизам групе $(G_1, *)$ у групу $(G_2, \circ)$. Ако је f пресликавање „на”, за групу $(G_2, \circ)$ кажемо да је хомоморфна слика групе $(G_1, *)$.

Дефиниција 1.12. Ако су $(G_1, *)$ и $(G_2, \circ)$ групе истога реда и ако је f бијективно пресликавање скупа G_1 на скуп G_2 такво да је, за свако $a, b \in G_1$,

$$f(a * b) = f(a) \circ f(b),$$

кажемо да је пресликавање f изоморфизам групе $(G_1, *)$ на групу $(G_2, \circ)$.

Пример 1.3. Функција $f(x) = \log x$ је један изоморфизам групе $(\mathbb{R}^+, \cdot)$ на групу $(\mathbb{R}, +)$.

Теорема 1.3. Ако је пресликавање f изоморфизам групе $(G_1, *)$ на групу $(G_2, \circ)$, тада је инверзно пресликавање f^{-1} изоморфизам групе $(G_2, \circ)$ на групу $(G_1, *)$.

Доказ. Нека су x и y било који елементи из G_2. Тада су $f^{-1}(x)$ и $f^{-1}(y)$ њима одговарајући елементи из G_1. Како је f изоморфизам групе $(G_1, *)$ на групу $(G_2, \circ)$, важи једнакост

$$f(f^{-1}(x) * f^{-1}(y)) = f(f^{-1}(x)) \circ f(f^{-1}(y)) = x \circ y,$$

одакле непосредно следује

$$f^{-1}(x \circ y) = f^{-1}(f(f^{-1}(x) * f^{-1}(y))) = f^{-1}(x) * f^{-1}(y).$$

Према томе, пресликавање f^{-1} је изоморфизам групе $(G_2, \circ)$ на групу $(G_1, *)$. $\square$

Дакле, ако постоји изоморфизам групе $(G_1, *)$ на групу $(G_2, \circ)$, постоји и изоморфизам групе $(G_2, \circ)$ на групу $(G_1, *)$. Због тога, за такве групе кажемо да су изоморфне, тј. кажемо да је свака од њих изоморфна оној другој, у ознаци $(G_1, *) \cong (G_2, \circ)$.

Дефиниција 1.13. Ако је пресликавање f изоморфизам групе $(G, *)$ на саму себе, за пресликавање f кажемо да је аутоморфизам групе $(G, *)$.

1.2 Алгебарске структуре са две операције

Нека је S непразан скуп и нека су у њему дефинисане две бинарне операције $*$ и $\circ$. Самим тим, $(S,*)$ и $(S,\circ)$ су извесне алгебарске структуре. Међутим, могуће је посматрати нову структуру коју чини скуп S снабдевен обема операцијама.

Пре него што изучимо неке од ових структура, дефинисаћемо особину дистрибутивност једне операције у односу на другу операцију.

Дефиниција 1.14. Кажемо да је бинарна операција $*$ дистрибутивна у односу на бинарну операцију $\circ$ ако за свако $a,b,c\in S$ важе једнакости

$$a*(b\circ c)=(a*b)\circ(a*c),\quad (a\circ b)*c=(a*c)\circ(b*c).$$

Наравно, ако за свако $a,b,c\in S$ важе једнакости

$$a\circ(b*c)=(a\circ b)*(a\circ c),\quad (a*b)\circ c=(a\circ c)*(b\circ c),$$

кажемо да је бинарна операција $\circ$ дистрибутивна у односу на операцију $*$.

Пример 1.4. Множење реалних бројева је дистрибутивна операција у односу на сабирање реалних бројева. Обрнуто, сабирање није дистрибутивна операција у односу на множење реалних бројева.

Дефиниција 1.15. Нека су у скупу S дефинисане две бинарне операције $*$ и $\circ$. Ако су испуњени следећи услови:

(P1) $(S,*)$ је комутативна група;

(P2) Операција $\circ$ је асоцијативна;

(P3) Операција $\circ$ је дистрибутивна у односу на операцију $*$,

кажемо да скуп S чини прстен у односу на операције $*$ и $\circ$, означавајући га са $(S,*,\circ)$.

Пример 1.5. $(\mathbb{Z},+,\cdot)$ је прстен. Заиста, овде је $(Z,+)$ Абелова група, операција $\cdot$ је асоцијативна и, најзад, операција $\cdot$ је дистрибутивна у односу на операцију сабирања $+$.

Управо, због прстена целих бројева $(\mathbb{Z},+,\cdot)$ уобичајено је да се неутрални елемент за операцију $*$ означава са 0, а инверзни елемент елемента a са $-a$.

Теорема 1.4. У прстену $(S,*,\circ)$ важи:

(1) $0\circ a=a\circ 0=0$;

(2) $a\circ(-b)=-(a\circ b)=(-a)\circ b$;

(3) $(-a)\circ(-b)=a\circ b$.

Доказ. (1) Коришћењем претходних особина лако налазимо да је

$$\begin{aligned}0=&(-(a\circ 0))*(a\circ 0)\\=&(-(a\circ 0))*(a\circ(0*0))\\=&(-(a\circ 0))*((a\circ 0)*(a\circ 0))\\=&((-(a\circ 0))*(a\circ 0))*(a\circ 0)\\=&0*(a\circ 0)=a\circ 0.\end{aligned}$$

Слично, $0 \circ a = 0$.

(2) Једноставно налазимо да је

$$\begin{aligned}(-a) \circ b =&0 * ((-a) \circ b)\\ =&((-(a \circ b)) * (a \circ b)) * ((-a) \circ b)\\ =&(-(a \circ b)) * ((a \circ b) * ((-a) \circ b))\\ =&(-(a \circ b)) * ((a * (-a)) \circ b)\\ =&(-(a \circ b)) * (0 \circ b)\\ =&(-(a \circ b)) * 0\\ =&-(a \circ b).\end{aligned}$$

Слично, $a \circ (-b) = -(a \circ b)$.

(3) Важи да је $(-a) \circ (-b) = -(a \circ (-b)) = -(-(a \circ b)) = a \circ b$. $\square$

Дефиниција 1.16. Прстен $(S, *, \circ)$ је комутативан ако је операција $\circ$ комутативна.

Дефиниција 1.17. Прстен $(S, *, \circ)$ је прстен са јединицом ако постоји елемент $1 \in S$ такав да важи $1 \circ x = x \circ 1 = x$.

Елемент $1 \in S$ се зове јединица прстена.

Дефиниција 1.18. Комутативан прстен са јединицом $(S, *, \circ)$ је интегрални домен ако нема делитеље нуле, тј.

$$(\forall a, b \in S)(a \circ b = 0 \Leftrightarrow a = 0 \vee b = 0).$$

Пример 1.6. $(\mathbb{Z}, +, \cdot)$ и $(\mathbb{Q}, +, \cdot)$ су интегрални домени, док $(\mathbb{Z}_4, +_4, \cdot_4)$ је комутативан прстен са јединицом, али није интегрални домен (нпр. $2 \cdot_4 2 = 0$)

Дефиниција 1.19. Нека је $(S, +, \cdot, 0, 1)$ прстен са јединицом. Уколико постоји $n \geq 2$, такво да је $\underbrace{1 + \cdots + 1}_{n} = 0$ онда кажемо да је прстен P коначне карактеристике и најмање такво n зовемо карактеристика прстена S.

Дефиниција 1.20. Нека је $(S, +, \cdot, 0, 1)$ прстен са јединицом. Уколико је $\underbrace{1 + \cdots + 1}_{n} \neq 0$, за све $n \geqslant 2$, онда кажемо да је прстен карактеристике нула (или бесконачне карактеристике).

Карактеристику прстена S ћемо означавати са $\mathrm{char}(S)$.

Дефиниција 1.21. Ако је $(S \setminus \{0\}, \circ)$ група, за прстен $(S, *, \circ)$ кажемо да је тело.

Дефиниција 1.22. Ако је $(F \setminus \{0\}, \circ)$ Абелова група, за прстен $(F, *, \circ)$ кажемо да је поље.

Неутрални елемент у односу на операцију $\circ$ најчешће означавамо са 1, а инверзни елемент елемента a са a^{-1}.

Пример 1.7. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ и $(\mathbb{C}, +, \cdot)$ су поља, док $(\mathbb{Z}, +, \cdot)$ није поље. $(\mathbb{Z}_n, +_n, \cdot_n)$ је поље ако и само ако је n прост број.

Теорема 1.5. Свако поље је интегрални домен.

Доказ. Нека је $(F, +, \cdot)$ поље. Покажимо да у пољу F нема делитеља нуле. За произвољно $a, b \in F$ из $a \cdot b = 0$ и $a \neq 0$ следи да постоји $a^{-1} \in F$ и стога

$$b = 1 \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0.$$

Дакле, из $a \cdot b = 0$ следи $a = 0$ или $b = 0$.

Стога, $(F, +, \cdot)$ је и интегрални домен. □

Теорема 1.6. Ако поље $(F, +, \cdot)$ има коначну карактеристику онда она мора бити прост број.

Доказ. Нека је карактеристика поља $(F, +, \cdot)$ број $p \neq 0$. Ако је $p = m \cdot k$, $1 < m < p$, $1 < k < p$ сложен број тада из

$$0 = \underbrace{1 + \cdots + 1}_{p} = (\underbrace{1 + \cdots + 1}_{m}) \cdot (\underbrace{1 + \cdots + 1}_{k})$$

следи $\underbrace{1 + \cdots + 1}_{m} = 0$ или $\underbrace{1 + \cdots + 1}_{k} = 0$ па је $\mathrm{char}(F) \leqslant m < p$ или $\mathrm{char}(F) \leqslant k < p$, што је супротно претпоставци $\mathrm{char}(F) = p$. Дакле, p је прост број. □

Глава 2

Полиноми

2.1 Прстен полинома

Нека је $(\mathbb{F}, +, \cdot, 0, 1)$ поље, $n \in \mathbb{N} \cup \{0\}$, $a_0, a_1, \ldots, a_n \in \mathbb{F}$. Уместо израза $a \cdot b$ $(a, b \in \mathbb{F})$ писаћемо једноставно ab.

Нека је, даље, операција степеновања уведена на уобичајени начин помоћу

$$x^0 = 1, \qquad x^k = xx^{k-1}, \quad k \in \mathbb{N}.$$

Дефиниција 2.1. Ако $x \in \mathbb{F}$ и $n \in \mathbb{N} \cup \{0\}$, $a_0, a_1, \ldots, a_n \in \mathbb{F}$, формални израз

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

назива се алгебарски полином по x над пољем $\mathbb{F}$. За елементе a_k кажемо да су коефицијенти полинома $p(x)$. Ако је коефицијент $a_n \neq 0$, за полином $p(x)$ кажемо да је степена n и то означавамо са $\mathrm{deg} p(x) = n$. За коефицијент $a_n \neq 0$ кажемо да је водећи или најстарији коефицијент полинома $p(x)$.

Дакле, степен полинома $p(x)$ је највиши степен од x који се појављује у изразу за $p(x)$ са ненула коефицијентима.

Дефиниција 2.2. За полином

$$O(x) = 0 + 0x + \cdots + 0x^{n-1} + 0x^n$$

кажемо да је нула полином и означавамо га просто са 0.

Степен нула полинома $O(x)$ се не дефинише.

Полиноми степена нула се називају константе и то су елементи поља $\mathbb{F}$. Елемент $x \in \mathbb{F}$ може се интерпретирати као полином првог степена дефинисан са $p(x) = x$. За елемент x користи се термин непозната. За полином $p(x)$ уведен у првој дефиницији каже се да је полином по (неодређеној) непознатој x.

Дефиниција 2.3. За полином чији је водећи коефицијент једнак јединици кажемо да је нормиран (моничан).

Дакле, нормирани полином има облик

$$p(x) = a_0 + a_1x + \cdots + a_{(n-1)}x^{n-1} + x^n.$$

Скуп свих полинома над пољем $\mathbb{F}$ означавамо са $\mathbb{F}[x]$. Од интереса је често уочити скуп свих оних полинома чији степен није већи од n. Тај подскуп ћемо означавати са $\mathbb{F}_n[x]$. Произвољни полином из $\mathbb{F}_n[x]$ има облик

$$p(x) = a_0 + a_1x + \cdots + a_nx^n,$$

при чему ако је $\deg p(x) = m < n$ имамо да је $a_{m+1} = \cdots = a_n = 0$.

У скуп $\mathbb{F}[x]$ можемо увести релацију једнакост као и операције: сабирање и множење полинома на следећи начин:

Дефиниција 2.4. Полиноми

$$p(x) = a_0 + a_1x + \cdots + a_nx^n \ \text{ и } \ q(x) = b_0 + b_1x + \cdots + b_mx^m$$

су једнаки ако и само ако је $a_k = b_k$ за свако $k \geqslant 0$, тј. када су њихови коефицијенти једнаки.

Дефиниција 2.5. За два полинома

$$p(x) = a_0 + a_1x + \cdots + a_nx^n \ \text{ и } \ q(x) = b_0 + b_1x + \cdots + b_mx^m$$

збир и производ су редом

$$(p+q)(x) = p(x) + q(x) = c_0 + c_1x + \cdots + c_rx^r$$

и

$$(pq)(x) = p(x)q(x) = d_0 + d_1x + \cdots + d_sx^s$$

где су

$$c_k = a_k + b_k, \quad 0 \leqslant k \leqslant r = \max\{n, m\},$$

и

$$d_k = \sum_{i=0}^{k} a_ib_{k-i}, \quad 0 \leqslant k \leqslant s = n + m.$$

Дакле, ако $p(x) \in \mathbb{F}_n[x]$ и $q(x) \in \mathbb{F}_m[x]$, тада $(p+q)(x) \in \mathbb{F}_r[x]$ и $(pq)(x) \in \mathbb{F}_s[x]$, где су $r = \max\{n, m\}$ и $s = n + m$. Напоменимо да за ненула полиноме $p(x)$ и $q(x)$ важи

$$\deg(pq)(x) = \deg p(x) + \deg q(x).$$

Такође, ако $p(x), q(x) \in \mathbb{F}[x]$ и $p(x) + q(x) \neq 0$, тада је

$$\deg(p+q)(x) \leqslant \max\{\deg p(x), \deg q(x)\}.$$

Као специјалан случај производа полинома имамо производ полинома $p(x)$ скаларом $\alpha \in \mathbb{F}$, који се може третирати као полином нултог степена. Дакле,

$$\alpha p(x) = \alpha(a_0 + a_1x + \cdots + a_nx^n) = (\alpha a_0) + (\alpha a_1)x + \cdots + (\alpha a_n)x^n.$$

Није тешко доказати следећи резултат:

Теорема 2.1. $(\mathbb{F}[x], +, \cdot)$ је интегрални домен (комутативан прстен са јединицом без делилаца нуле).

Доказ. Заиста, имамо да важи следеће.

(P_1) $(F[x],+)$ је Абелова група.

Комутативност и асоцијативност сабирања полинома следе из дефиниције сабирања полинома и особина сабирања у пољу $\mathbb{F}$. Неутрални за сабирање је нула полином, а супротни (инверзни) полином за полином $p(x)=a_0+a_1x+\cdots+a_nx^n$ је полином $-p(x)=-a_0+(-a_1)x+\cdots+(-a_n)x^n$.

(P_2) Асоцијативност множења полинома следи из дефиниције операције $\cdot$, асоцијативности множења у $\mathbb{F}$ и дистрибутивности $\cdot$ према $+$ у $\mathbb{F}$.

(P_3) Дистрибутивност $\cdot$ према $+$ следи из дистрибутивности $+$ и $\cdot$ у пољу $\mathbb{F}$. Неутрални за множење је константни полином 1.

Дакле, $F[x]$ је комутативан прстен са јединицом. Докажимо да $F[x]$ нема делиоце нуле, тј. да производ два ненула полинома не може бити нула полином.

Нека су $p(x),q(x)\in F[x]$, $p(x)\neq 0,\ q(x)\neq 0$. Тада постоји $\deg p(x)=m$, $\deg q(x)=n$, $m,n\in\mathbb{N}\cup\{0\}$, па следи да је $\deg(p(x)q(x))=\deg p(x)+\deg q(x)=n+m$. Дакле, полином $p(x)q(x)$ има степен, па је $p(x)q(x)\neq 0$.

Закључујемо да је $F[x]$ комутативан прстен са јединицом без делилаца нуле, тј. $F[x]$ је интегрални домен. □

Пример 2.1. Имамо да је $(\mathbb{R}[x],+,\cdot)$ прстен реалних полинома, а $(\mathbb{C}[x],+,\cdot)$ прстен комплексних полинома. За такве скупове полинома важи $\mathbb{R}[x]\subset\mathbb{C}[x]$.

Теорема 2.2. Елемент $p(x)\in F[x]$, $p(x)\neq 0$, има инверзни акко је $\deg p(x)=0$, тј. $p(x)$ је ненула константни полином.

Доказ. Нека $p(x)$ има инверзни и нека је то $q(x)\in\mathbb{F}[x]$. Тада је $p(x)q(x)=q(x)p(x)=1$. Претпоставимо да је $\deg p(x)\geqslant 1$. Тада је $0=\deg(1)=\deg(p(x)q(x))=\deg p(x)+\deg q(x)\geqslant 1$, што је контрадикција. Дакле, следи да је $\deg p(x)=0$.

Обратно, нека је $p(x)$ ненула константни полином. То значи $p(x)=a_0,\ a_0\in\mathbb{F},\ a_0\neq 0$. Тада постоји $a_0^{-1}\in\mathbb{F}$ (инверзни од a_0 у односу на операцију $\cdot$ у пољу $\mathbb{F}$). За $q(x)=a_0^{-1}\in\mathbb{F}\subseteq\mathbb{F}[x]$ важи $p(x)q(x)=a_0\cdot a_0^{-1}=1$. Следи да је $q(x)$ инверзни од $p(x)$ у $\mathbb{F}[x]$. □

На крају овог одељка укажимо на важну чињеницу да се полином може третирати и као функција. Наиме, на основу дефиниције полинома може се дефинисати пресликавање $f:\mathbb{F}\to\mathbb{F}$, помоћу

$$f(c)=a_0+a_1c+\cdots+a_nc^n\in\mathbb{F}.$$

Пресликавање f називамо полиномска (полиномна) функција.

2.2 Дељивост полинома

Дефиниција 2.6. Ако важи $p(c)=0$ онда се c назива нула или корен полинома $p(x)$.

Једначина $a_0+a_1x+\cdots+a_nx^n=0$ $(a_n\neq 0)$ се назива алгебарска једначина n-тог степена.

$n=1:\quad a_0+a_1x=0\ (a_1\neq 0)$ - линеарна једначина;

$n=2:\quad a_0+a_1x+a_2x^2=0\ (a_2\neq 0)$ - квадратна једначина.

Пример 2.2. (a) Нула полинома $p(x)=2-3x+x^3$, $p(x)\in\mathbb{R}[x]$ је број -2, јер $p(-2)=2-3(-2)+(-2)^3=0$.

(б) Полином $q(x) = x^2 + 1$, $q(x) \in \mathbb{R}[x]$, нема нуле (у $\mathbb{R}$).

(в) Полином $q(x) = x^2 + 1$, $f \in \mathbb{C}[x]$, има нуле i и $-i$.

ТЕОРЕМА 2.3. За сваки полином $p(x)$ и сваки ненула полином $q(x)$, постоје јединствени полиноми $s(x)$ и $r(x)$ такви да важи једнакост

$$p(x) = s(x)q(x) + r(x),$$

при чему је $r(x)$ нула полином или $\deg r(x) < \deg q(x)$.

Доказ. Претпоставимо да $p(x)$ и $q(x)$ имају степене n и m, респективно, и да су

$$p(x) = a_0 + a_1x + \cdots + a_nx^n \quad \text{и} \quad q(x) = b_0 + b_1x + \cdots + b_mx^m.$$

Ако је $n < m$ или $p(x) = 0$, тада једнакост важи са $s(x) = 0$ и $r(x) = p(x)$.

Претпоставимо зато да је $n \geqslant m$. Посматрајмо полином

$$p_1(x) = p(x) - \frac{a_n}{b_m}x^{n-m}q(x),$$

чији је степен, очигледно, мањи од n. Са n_1 означимо тај степен, а са $a_{n_1}^{(1)}$ најстарији коефицијент полинома $p_1(x)$. Ако је $n_1 \geqslant m$ ставимо даље

$$p_2(x) = p_1(x) - \frac{a_{n_1}^{(1)}}{b_m}x^{n_1-m}q(x),$$

и са n_2 и $a_{n_2}^{(2)}$ означимо степен и најстарији коефицијент овог полинома, респективно. Процес настављамо ако је $n_2 \geqslant m$.

Јасно је да степени полинома $p_1(x), p_2(x), \dots$ опадају и да после коначног броја корака добијамо једнакост

$$p_k(x) = p_{k-1}(x) - \frac{a_{n_{k-1}}^{(k-1)}}{b_m}x^{n_{k-1}-m}q(x),$$

у којој је $p_k(x)$ нула полином или такав да му је степен n_k мањи од m. У том случају процес прекидамо, а $p_k(x)$ се, коришћењем претходних једнакости, може представити у облику $p_k(x) = p(x) - s(x)q(x)$, где смо ставили

$$s(x) = \frac{a_n}{b_m}x^{n-m} + \frac{a_{n_1}^{(1)}}{b_m}x^{n_1-m} + \cdots + \frac{a_{n_{k-1}}^{(k-1)}}{b_m}x^{n_{k-1}-m}.$$

Дакле, овај полином $s(x)$ и $r(x) = p_k(x)$ задовољавају једнакост, при чему је $r(x)$ нула полином или је његов степен мањи од степена полинома $q(x)$.

За доказ јединствености полинома $s(x)$ и $r(x)$, претпоставимо да постоје и полиноми $\widehat{s}(x)$ и $\widehat{r}(x)$, који задовољавају једнакост

$$p(x) = \widehat{s}(x)q(x) + \widehat{r}(x),$$

при чему је $\widehat{r}(x) = 0$ или $\deg\widehat{r}(x) < \deg q(x)$. Тада је

$$(s(x) - \widehat{s}(x))q(x) = \widehat{r}(x) - r(x),$$

при чему је полином на десној страни ове једнакости нула полином или је, пак његов степен мањи од степена полинома $q(x)$. С друге стране, ако је $s(x) - \widehat{s}(x) \neq 0$, тада полином на левој страни у једнакости је не мањег степена од степена полинома $q(x)$. Према томе, једнакост је могућа само ако је

$$\widehat{s}(x) = s(x), \qquad \widehat{r}(x) = r(x),$$

па је тиме доказ завршен. □

Као што је речено у претходном одељку, за полиноме у скупу $\mathbb{F}[x]$ не постоји операција дељење, инверзна операцији множења. Може се, међутим, сагласно особини из претходне теореме, дефинисати дељење полинома полиномом са остатком.

Дефиниција 2.7. За полином $s(x)$ који задовољава једнакост кажемо да је количник при дељењу полинома $p(x)$ полиномом $q(x)$, а за одговарајући полином $r(x)$ да је остатак при том дељењу.

Ако је остатак нула полином, кажемо да је $p(x)$ дељиво са $q(x)$ и полином $q(x)$ зовемо делилац полинома $p(x)$.

Чињеницу да је $q(x)$ делилац полинома $p(x)$ симболизујемо са $q(x) \mid p(x)$.

2.3 Највећи заједнички делилац

Дефиниција 2.8. Полином $d(x)$ је заједнички делилац за полиноме $p(x)$ и $q(x)$ ако $d(x) \mid p(x)$ и $d(x) \mid q(x)$.

Дефиниција 2.9. Полином $d(x)$ је највећи заједнички делилац за полиноме $p(x)$ и $q(x)$, тј. $d(x) = \mathrm{NZD}(p(x), q(x))$, ако је заједнички делилац за ове полиноме и ако је дељив са свим осталим заједничким делиоцима ових полинома.

Приметимо да ако је $d(x) = \mathrm{NZD}(p(x), q(x))$, тада је и полином $\alpha d(x)$, ($\alpha \neq 0$, $\alpha \in \mathbb{F}$) такође највећи заједнички делилац полинома $p(x)$ и $q(x)$.

Теорема 2.4. За свака два полинома $p(x)$ и $q(x)$ постоји највећи заједнички делилац $d(x)$ и он је јединствен до на мултипликативну константу.

Доказ. Претпоставимо да је $\mathrm{deg}p(x) \geqslant \mathrm{deg}q(x)$. Са $s_1(x)$ и $r_1(x)$ означимо редом количник и остатак при дељењу полинома $p(x)$ са $q(x)$. Ако је $r_1(x) = 0$ тада је $q(x)$ највећи заједнички делилац полинома $p(x)$ и $q(x)$. Међутим, ако $r_1(x)$ није нула полином, тада делимо полином $q(x)$ са $r_1(x)$, и одговарајући количник и остатак при дељењу означавамо са $s_2(x)$ и $r_2(x)$, респективно. Ако је $r_2(x) = 0$ тада је $r_1(x)$ највећи заједнички делилац за полиноме $p(x)$ и $q(x)$. Заиста, из

$$p(x) = s_1(x)q(x) + r_1(x),$$

$$q(x) = s_2(x)r_1(x) + r_2(x),$$

следује $p(x) = (s_1(x)s_2(x) + 1)r_1(x)$ и $q(x) = s_2(x)r_1(x)$, тј. $r_1(x) \mid p(x)$ и $r_1(x) \mid q(x)$. Да бисмо доказали да је $r_1(x)$ највећи заједнички делилац за $p(x)$ и $q(x)$ довољно је претпоставити да ови полиноми имају заједнички делилац $d(x)$ и приметити да следује $d(x) \mid r_1(x)$.

Међутим, уколико $r_2(x)$ није нула полином, претходни поступак се наставља, сагласно следећим једнакостима,

$$r_1(x) = s_3(x)r_2(x) + r_3(x),$$

$$r_2(x) = s_4(x)r_3(x) + r_4(x),$$

$$\vdots$$

$$r_{k-1}(x) = s_{k+1}(x)r_k(x) + r_{k+1}(x),$$

све до испуњења услова $r_{k+1}(x) = 0$. Тада је $r_k(x) = \mathrm{NZD}(p(x), q(x))$. Ово закључујемо сличним резоновањем као у случају $k = 1$. □

У доказу ове теореме коришћен је Еуклидов алгоритам, при чему су за одређивање највећег заједничког делиоца (NZD) два полинома битни само остаци $r_\nu(x)$, а не и количници $s_\nu(x)$, $\nu = 1, 2, \ldots$. Имајући на уму јединственост NZD до на мултипликативну константу могуће је у сваком кораку Еуклидовог алгоритма множити остатке $r_\nu(x)$ погодним константама различитим од нуле у циљу добијања једноставнијих израза при дељењу.

Дефиниција 2.10. Ако је највћи заједнички делилац за полиноме $p(x)$ и $q(x)$ константа, за те полиноме кажемо да су узајамно прости.

Пример 2.3. За полиноме у $\mathbb{R}[x]$,

$$p(x) = 2x^4 + 4x^3 + x^2 - 2x - 8, \quad q(x) = x^3 + x^2 + 4,$$

одредићемо NZD.

Добијамо да је

$$d(x) = \mathrm{NZD}(p(x), q(x)) = x + 2.$$

Теорема 2.5. Ако је $d(x) = \mathrm{NZD}(p(x), q(x))$ тада постоје полиноми $u(x)$ и $v(x)$ такви да је

$$d(x) = u(x)p(x) + v(x)q(x).$$

Доказ. На основу претходне теореме имамо редом

$r_1(x) = p(x) - s_1(x)q(x),$

$r_2(x) = -s_2(x)p(x) + (1 + s_1(x)s_2(x))q(x),$

$r_3(x) = (1 + s_2(x)s_3(x))p(x) - (s_1(x) + s_3(x) + s_1(x)s_2(x)s_3(x))q(x),$

итд. Најзад, $d(x) = r_k(x)$ има облик који се тражи. □

2.4 Особине релације дељивости полинома

Присетимо се дефиниције из претходног излагања.

Дефиниција 2.11. За полином $s(x)$ који задовољава једнакост

$$p(x) = s(x)q(x) + r(x),$$

кажемо да је количник при дељењу полинома $p(x)$ полиномом $q(x)$, а за одговарајући полином $r(x)$ да је остатак при том дељењу.

Ако је остатак нула полином, кажемо да је $p(x)$ дељиво са $q(x)$ и полином $q(x)$ зовемо делилац полинома $p(x)$.

Чињеницу да је $q(x)$ делилац полинома $p(x)$ симболизујемо са $q(x) \mid p(x)$.

Односно, имамо да

$$q(x) \mid p(x) \Leftrightarrow (\exists s(x) \in \mathbb{F}[x])p(x) = s(x) \cdot q(x).$$

Неке особине дељивости полинома наводимо у следећој теореми.

ТЕОРЕМА 2.6. За произвољне полиноме $p(x), q(x), t(x) \in \mathbb{F}[x]$ важе тврђења:

(а) $p(x) \mid p(x)$;

(б) $c \mid p(x)$ за свако $c \in \mathbb{F} \setminus \{0\}$;

(в) $p(x) \mid q(x) \Leftrightarrow p(x) \mid c \cdot q(x)$ за свако $c \in \mathbb{F} \setminus \{0\}$;

(г) $p(x) \mid q(x) \Leftrightarrow c \cdot p(x) \mid q(x)$ за свако $c \in \mathbb{F} \setminus \{0\}$;

(д) Ако $q(x) \mid p(x)$ и $p(x) \mid q(x)$, тада је $p(x) = c \cdot q(x)$ за неко $c \in \mathbb{F} \setminus \{0\}$;

(ђ) Ако $t(x) \mid q(x)$ и $q(x) \mid p(x)$, тада $t(x) \mid p(x)$;

(е) Ако $t(x) \mid p(x)$ и $t(x) \mid q(x)$, тада $t(x) \mid u(x) \cdot p(x) + v(x) \cdot q(x)$ за свако $u(x), v(x) \in \mathbb{F}[x]$.

Доказ. (а) Тврђење очигледно важи, јер постоји $1 \in \mathbb{F}[x]$ такав да је $p(x) = 1 \cdot p(x)$.

(б) Како је $p(x) = (\frac{1}{c}p(x)) \cdot c$ и при томе важи да $\frac{1}{c}p(x) \in \mathbb{F}[x]$, закључујемо да $c \mid p(x)$.

(в) Нека $p(x) \mid q(x)$, а то значи да постоји $s(x) \in \mathbb{F}[x]$ такав да је $q(x) = s(x) \cdot p(x)$. Како је $c \cdot q(x) = c \cdot (s(x) \cdot p(x)) = (c \cdot s(x)) \cdot p(x)$, то закључујемо да $p(x) \mid c \cdot q(x)$.

Обратно, нека $p(x) \mid c \cdot q(x)$, а то значи да постоји $s_1(x) \in \mathbb{F}[x]$ такав да је $c \cdot q(x) = s_1(x) \cdot p(x)$. Имамо да је $q(x) = (\frac{1}{c} \cdot s_1(x)) \cdot p(x)$, па закључујемо да $p(x) \mid q(x)$.

(г) Нека $p(x) \mid q(x)$, а то значи да постоји $s(x) \in \mathbb{F}[x]$ такав да је $q(x) = s(x) \cdot p(x)$. Како је $q(x) = (\frac{1}{c}s(x)) \cdot (cp(x))$, то закључујемо да $c \cdot p(x) \mid q(x)$.

Обратно, нека $c \cdot p(x) \mid q(x)$, а то значи да постоји $s_1(x) \in \mathbb{F}[x]$ такав да је $q(x) = s_1(x) \cdot cp(x)$. Имамо да је $q(x) = (cs_1(x)) \cdot p(x)$, па закључујемо да $p(x) \mid q(x)$.

(д) Нека $q(x) \mid p(x)$ и $p(x) \mid q(x)$. Тада постоје $s_1(x), s_2(x) \in \mathbb{F}[x]$ такво да је $q(x) = s_1(x) \cdot p(x)$ и $p(x) = s_2(x) \cdot q(x)$. Дакле, важи да је $s_1(x) \cdot s_2(x) = 1$, односно имамо да је $\mathrm{deg} s_1(x) = \mathrm{deg} s_2(x) = 0$, јер су међусобно инверзни. Дакле, важи да је $s_2(x) = c$, па је $p(x) = cq(x)$.

(ђ) Нека $t(x) \mid q(x)$ и $q(x) \mid p(x)$. Тада постоје $s_1(x), s_2(x) \in \mathbb{F}[x]$ такво да је $q(x) = s_1(x) \cdot t(x)$ и $p(x) = s_2(x) \cdot q(x)$. Дакле, имамо да је $p(x) = s_2(x) \cdot s_1(x) \cdot t(x)$, односно $p(x) = s(x) \cdot t(x)$ где је $s_2(x) \cdot s_1(x) = s(x)$. Коначно закључујемо да $t(x) \mid p(x)$.

(е) Нека $t(x) \mid p(x)$ и $t(x) \mid q(x)$. Тада постоје $s_1(x), s_2(x) \in \mathbb{F}[x]$ такво да је $p(x) = s_1(x) \cdot t(x)$ и $q(x) = s_2(x) \cdot t(x)$. За све $u(x), v(x) \in \mathbb{F}[x]$ важи да је

$$u(x) \cdot p(x) + v(x) \cdot q(x) = u(x) \cdot s_1(x) \cdot t(x) + v(x) \cdot s_2(x) \cdot t(x) = (u(x) \cdot s_1(x) + v(x) \cdot s_2(x)) \cdot t(x).$$

Дакле, важи да $t(x) \mid u(x) \cdot p(x) + v(x) \cdot q(x)$. □

2.5 Безуов став

Нека је $a \in \mathbb{F}$ и $p(x) = a_0 + a_1x + \cdots + a_nx^n$. Тада је

$$p(a) = a_0 + a_1a + \cdots + a_na^n$$

један елемент у пољу $\mathbb{F}$. За $p(a)$ кажемо да је вредност полинома у тачки $x = a$.

За елемент $a \in \mathbb{F}$ кажемо да је нула полинома $p(x) \in \mathbb{F}[x]$ ако је вредност полинома у тој тачки једнака нули, тј. $p(a) = 0$. У том случају, за полином првог степена $x - a$ кажемо да је линеарни фактор.

ТЕОРЕМА 2.7. Ако је a нула полинома $p(x) \in \mathbb{F}[x]$, тада је $p(x)$ дељив линеарним фактором $x - a$.

Доказ. Како је

$$x^k - a^k = (x^{k-1} + x^{k-2}a + \cdots + xa^{k-2} + a^{k-1})(x-a),$$

имамо

$$\begin{aligned} p(x) - p(a) =& a_1(x-a) + a_2(x^2-a^2) + \cdots + a_n(x^n - a^n) \\ =& [a_1 + a_2(x+a) + \cdots + a_n(x^{n-1} + \cdots + a^{n-1})](x-a) \\ =& q(x)(x-a), \end{aligned}$$

где је $q(x)$ полином степена $n-1$. С друге стране, по претпоставци је $p(a) = 0$, па имамо да је $p(x) = q(x)(x-a)$, што значи да је полином $p(x)$ дељив линеарним фактором $x - a$. □

Следеће тврђење је познато као Безуов став:

Теорема 2.8. Остатак при дељењу полинома $p(x)$ са $x - a$ једнак је вредности полинома $p(a)$.

Доказ. Како је $q(x) = x - a$ полином првог степена то постоји јединствени полином $s(x)$ и константа r (полином степена нула) тако да је

$$p(x) = s(x)(x-a) + r.$$

Стављајући $x = a$ добијамо да је $r = p(a)$. □

Коришћењем претходне теореме, сваки полином $p(x) \in \mathbb{F}[x]$ степена n можемо на јединствен начин представити (разложити) по степенима од $x - a$, тј.

$$p(x) = A_0 + A_1(x-a) + A_2(x-a)^2 + \cdots + A_n(x-a)^n,$$

где су A_k, $k = 0, 1, \ldots, n$ елементи поља $\mathbb{F}$.

Заиста, на основу претходне теореме имамо

$$p(x) = A_0 + p_1(x)(x-a),$$

где смо ставили $A_0 = r = p(a)$ и $p_1(x) = s(x)$. Ако је $p_1(x)$ полином нултог степена тражени развој је добијен. У противном случају, делимо полином $p_1(x)$ са $x - a$, добијајући притом да је

$$p_1(x) = A_1 + p_2(x)(x-a),$$

где је $A_1 = p_1(a)$. На овај начин, добијамо да је

$$p(x) = A_0 + A_1(x-a) + p_2(x)(x-a)^2.$$

Настављајући овај поступак добићемо развој

$$p(x) = A_0 + A_1(x-a) + A_2(x-a)^2 + \cdots + A_n(x-a)^n.$$

Последица 1. Ако је $p(x) = a_0 + a_1x + \cdots + a_nx^n$, $a_n \neq 0$, $n \geq 1$ и ако су $c_1, c_2, \ldots, c_n$ различити корени полинома $p(x)$, тада је

$$p(x) = a_n(x-c_1)\ldots(x-c_n) \quad \text{(факторизација полинома).}$$

Доказ. Доказ индукцијом по степену n полинома $p(x)$.

Покажимо да тврђење важи за $n = 1$. Нека је c_1 корен полинома $p(x) = a_0 + a_1x$. Тада $a_0 + a_1c_1 = 0$, па је $a_0 = -a_1c_1$, одакле следи $p(x) = -a_1c_1 + a_1x = a_1(x - c_1)$.

Претпоставимо да је тврђење тачно за све полиноме степена мањег од n, где је $n > 1$.

Пошто је c_1 корен полинома $p(x)$ који је степена n, важи да је $x-c_1 \mid p(x)$, па постоји полином $q \in \mathbb{F}[x]$, тако да $p(x) = q(x)(x - c_1)$. Степен полинома $q(x)$ је $n - 1$, а водећи коефицијент a_n. Тада важи и да је $0 = p(c_j) = (c_j - c_1)q(c_j)$ $(j = 2, \ldots, n)$, а како је $c_j - c_1 \neq 0$, за $j \neq 1$, следи да је $q(c_j) = 0$ за сваки $j = 2, \ldots, n$. Дакле $q(x)$ има $n - 1$ различитих корена $c_2, \ldots, c_n \in \mathbb{F}$. Према индукцијској хипотези следи $q(x) = a_n(x - c_2) \ldots (x - c_n)$. Заменом у $p(x) = q(x)(x - c_1)$ добијамо

$$p(x) = a_n(x - c_1)(x - c_2) \ldots (x - c_n),$$

што је и требало показати. □

ПОСЛЕДИЦА 2. Полином $p(x)$ степена $n \geq 1$ не може имати више од n различитих корена.

Доказ. Претпоставимо супротно, да полином $p(x)$ са водећим коефицијентом $a_n \neq 0$, има $n + 1$ различитих корена $c_1, \ldots, c_n, c$. Тада је, по Последици 1,

$$p(x) = a_n(x - c_1) \ldots (x - c_n),$$

па је

$$0 = p(c) = \underbrace{a_n}_{\neq 0} \underbrace{(c - c_1)}_{\neq 0} \underbrace{(c - c_2)}_{\neq 0} \ldots \underbrace{(c - c_n)}_{\neq 0},$$

што је контрадикција. □

ПОСЛЕДИЦА 3. Ако су $p(x), q(x)$ полиноми степена $\leq n$ и $c_1, c_2, \ldots, c_{n+1}$ различити елементи поља $\mathbb{F}$ такви да $p(c_i) = q(c_i),\ i = 1, 2, \ldots n + 1$, онда је $p(x) = q(x)$.

Доказ. Ставимо да је $h(x) = p(x) - q(x)$ и претпоставимо да је $h(x) \neq 0$. Имамо да је $\mathrm{deg}h(x) \leq \max\{\mathrm{deg}p(x), \mathrm{deg}q(x)\} \leq n$ и $h(c_i) = p(c_i) - q(c_i) = 0$, за свако $i = 1, \ldots, n + 1$.

Дакле, $h(x)$ има $n + 1$ различитих корена у $\mathbb{F}$, што је контрадикција са последицом 2. Дакле, $h(x) = 0$, тј. $p(x) = q(x)$. □

ПОСЛЕДИЦА 4. Ако су $c_1, c_2, \ldots, c_{n+1}$ различити, а $b_1, b_2, \ldots, b_{n+1}$ произвољни елементи поља $\mathbb{F}$, тада постоји тачно један полином $p(x) \in \mathbb{F}[x]$ степена $\leq n$ тако да $p(c_i) = b_i$ за $i = 1, \ldots, n + 1$.

Доказ. Егзистенција полинома $p(x)$. Посматрајмо Лагранжов интерполациони полином, тј. полином облика:

$$\begin{aligned} p(x) = \quad & b_1 \cdot \frac{(x - c_2)(x - c_3) \cdots (x - c_{n+1})}{(c_1 - c_2)(c_1 - c_3) \ldots (c_1 - c_{n+1})} + b_2 \cdot \frac{(x - c_1)(x - c_3) \cdots (x - c_{n+1})}{(c_2 - c_1)(c_2 - c_3) \ldots (c_2 - c_{n+1})} \\ & + \cdots + b_{n+1} \cdot \frac{(x - c_1)(x - c_2) \cdots (x - c_n)}{(c_{n+1} - c_1)(c_{n+1} - c_2) \ldots (c_{n+1} - c_n)}. \end{aligned}$$

Полином $p(x)$ испуњава услове $p(c_i) = b_i,\ i = 1, \ldots, n + 1$ и $\mathrm{deg}p(x) \leq n$.

Јединственост. Ако је $q(x) \in \mathbb{F}[x]$ такав да је $\mathrm{deg}q(x) \leq n$ и $q(c_i) = b_i$ $(i = 1, \ldots, n + 1)$, према претходној последици следи $q(x) = p(x)$. □

Дакле, на основу претходне последице можемо закључити да је линеарни полином $p(x)$ одређен својим вредностима $p(c_0),\ p(c_1)$ у двема различитим тачкама $c_0 \neq c_1$. Квадратни полином је одређен својим вредностима у трима различитим тачкама.

2.6 Хорнерова шема и Виетове формуле

ДЕФИНИЦИЈА 2.12. Ако је $p(x) = a_0 + a_1x + \cdots + a_nx^n$ произвољан полином из $\mathbb{F}[x]$, тада за полином

$$p'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} \in \mathbb{F}[x]$$

кажемо да је (први) извод полинома $p(x)$. За пресликавање $p(x) \mapsto p'(x)$ кажемо да је диференцирање у прстену $\mathbb{F}[x]$.

Виши изводи $p^{(k)}(x)$ дефинишу се рекурзивно; на пример, извод полинома $p'(x)$ назива се други извод полинома $p(x)$, итд. По дефиницији, $p^{(0)}(x) = p(x)$.

Напоменимо да је $\mathrm{deg} p'(x) = \mathrm{deg} p(x) - 1$. Такође, за свако $k > n = \mathrm{deg} p(x)$ имамо да је $p^{(k)}(x)$ нула полином.

Један елементаран, али важан проблем је израчунавање вредности полинома за дато $x = a$. Представимо полином по опадајућим степенима

$$p(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n.$$

Ако бисмо израчунавали вредност полинома $p(a)$, на основу претходног израза, било би потребно $2n - 1$ множења и n сабирања. Међутим, уколико $p(x)$ представимо у облику

$$p(x) = (\cdots((a_0x + a_1)x + a_2)x + \cdots + a_{n-1})x + a_n$$

потребно је само n множења и n сабирања.

Са $b_0, b_1, \ldots, b_{n-1}$ означимо коефицијенте полинома $s(x)$ из Безуовог става и ставимо $b_n = r$. Тада имамо

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n = (b_0x^{n-1} + b_1x^{n-2} + \cdots + b_{n-1})(x - a) + b_n,$$

одакле, упоређивањем коефицијената уз одговарајуће степене на левој и десној страни претходне једнакости, добијамо

$$a_0 = b_0, \quad a_k = b_k - b_{k-1}a \qquad (k = 1, \ldots, n).$$

На основу ових једнакости може се формирати рекурзивни поступак за израчунавање вредности полинома за $x = a$:

$$b_0 = a_0, \quad b_k = a_k + b_{k-1}a \qquad (k = 1, \ldots, n),$$

који после n корака даје вредност полинома, тј. $p(a) = b_n$.

Изложени поступак познат је као Хорнерова шема и може се интерпретирати кроз следећу шему:

a	a_0	a_1	a_2	a_3	$\cdots$	a_{n-1}	a_n
		b_0a	b_1a	b_2a		$b_{n-2}a$	$b_{n-1}a$
	b_0	b_1	b_2	b_3		b_{n-1}	$b_n = p(a)$

Прву врсту, дакле, започињемо са вредношћу $x = a$ за коју израчунавамо вредност полинома, а затим пишемо коефицијенте полинома, почев од најстаријег коефицијента. У трећој врсти пишемо коефицијенте b_k, које израчунавамо сабирањем одговарајућих елемената прве и друге врсте, при чему је $b_0 = a_0$. Елементе друге врсте формирамо множењем вредности a са претходним елементом из треће врсте. Елементи треће врсте су, дакле, коефицијенти полинома $s(x)$ и остатак при дељењу $r = p(a)$.

Пример 2.4. Нека је $p(x) = 4x^4 - 4x^3 + 13x^2 - 16x - 12 \in \mathbb{R}[x]$. Применом Хорнерове шеме одредићемо вредност $p(2)$.

2	4	−4	13	−16	−12
		8	8	42	52
	4	4	21	26	40

Дакле, $p(2) = 40$. Количник при дељењу полинома $p(x)$ са $x - 2$ је полином $s(x) = 4x^3 + 4x^2 + 21x + 26$, а остатак дељења је $r = p(2) = 40$. Наведена шема се може упростити изостављањем друге врсте. На пример, за $a = -\frac{1}{2}$ имамо

$-\frac{1}{2}$	4	−4	13	−16	−12
	4	−6	16	−24	0

одакле закључујемо да је $a = -\frac{1}{2}$ нула полинома $p(x)$.

Применимо сада поступак сукцесивног дељења у циљу добијања разлагања полинома $p(x)$ по степенима од $x - 2$ и израчунавања извода полинома у тачки $x = 2$.

Поступак је приказан у следећој табели:

2	4	−4	13	−16	−12
	4	4	21	26	40
	4	12	45	116	
	4	20	85		
	4	28			
	4				

Према томе,

$$p(x) = 40 + 116(x-2) + 85(x-2)^2 + 28(x-2)^3 + 4(x-2)^4.$$

Посматрајмо полином $p(x)$ са комплексним коефицијентима степена n. Нека су његове нуле редом $x_1, x_2, \ldots, x_n$. Важе тзв. Виетове формуле

$$\begin{aligned}
x_1 + x_2 + \cdots + x_n &= -\frac{a_{n-1}}{a_n} \\
x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n &= \frac{a_{n-2}}{a_n} \\
x_1x_2x_3 + x_1x_2x_4 + \ldots &= -\frac{a_{n-3}}{a_n} \\
&\vdots \\
x_1x_2\ldots x_n &= (-1)^n\frac{a_0}{a_n}.
\end{aligned}$$

За $n = 2$ имамо да је $p(x) = a_2x^2 + a_1x + a_0$, $a_2 \neq 0$, па важе формуле

$$\begin{aligned}
x_1 + x_2 &= -\frac{a_1}{a_2} \\
x_1x_2 &= \frac{a_0}{a_2}.
\end{aligned}$$

За $n = 3$ имамо да је $p(x) = a_3x^3 + a_2x^2 + a_1x + a_0$, $a_3 \neq 0$ па важе формуле

$$\begin{aligned}
x_1 + x_2 + x_3 &= -\frac{a_2}{a_3} \\
x_1x_2 + x_1x_3 + x_2x_3 &= \frac{a_1}{a_3} \\
x_1x_2x_3 &= -\frac{a_0}{a_3}.
\end{aligned}$$

Доказ за $n = 3$. Како је $p(x) = a_3(x-x_1)(x-x_2)(x-x_3) = a_3x^3 - a_3(x_1+x_2+x_3)x^2 + a_3(x_1x_2+x_1x_3+x_2x_3)x - a_3x_1x_2x_3$. Са друге стране имамо да је $p(x) = a_0 + a_1x + a_2x^2 + a_3x^3$. Дакле, важи

$$\begin{aligned}
x_1 + x_2 + x_3 &= -\frac{a_2}{a_3} \\
x_1x_2 + x_1x_3 + x_2x_3 &= \frac{a_1}{a_3} \\
x_1x_2x_3 &= -\frac{a_0}{a_3}.
\end{aligned}$$

2.7 Сводљивост полинома

Један од битних задатака јесте растављање полинома на чиниоце, наравно, уколико је то могуће. Из тог разлога, уводимо појмове сводљив и несводљив полином. Нека је $p(x) \in \mathbb{F}[x]$ и нека је $\deg p(x) = n \geqslant 1$. Тривијални делиоци полинома $p(x)$ су полиноми нултог степена, тј. полиноми c, где је $c \in \mathbb{F} \setminus \{0\}$ и полиноми $cp(x)$. Поставља се питање да ли полином $p(x)$ има и нетривијалних делилаца, тј. делилаца степена k, где је $0 < k < n$?

Дефиниција 2.13. Полином $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$ је сводљив над пољем $\mathbb{F}$ ако постоје полиноми $g(x), h(x) \in \mathbb{F}[x]$, такви да је $p(x) = g(x) \cdot h(x)$, $\deg g(x) < n, \deg h(x) < n$. У супротном, $p(x)$ је несводљив над пољем $\mathbb{F}$.

Другим речима, полином $p(x)$ степена $n \geqslant 1$ је несводљив ако има само тривијалне делиоце, тј. само делиоце степена 0 и степена n.

Из дефиниције непосредно следи:

- Сви полиноми степена 1 су несводљиви.
- Полиноми степена 0 нису ни сводљиви, ни несводљиви.

Теорема 2.9. Полином $p(x) \in \mathbb{F}[x]$ степена 2 или 3 је сводљив над $\mathbb{F}$ ако и само ако $p(x)$ има корен у $\mathbb{F}$.

Доказ. Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\deg p(x) = 2$ или $\deg p(x) = 3$.

Претпоставимо да је полином $p(x)$ сводљив. Тада је $p(x) = g(x) \cdot h(x)$, где је $\deg g(x) = 1$ или $\deg h(x) = 1$. Нека је на пример $g(x) = ax + b, a \neq 0$, па је $c = -a^{-1}b \in \mathbb{F}$ корен полинома $g(x)$. Дакле, имамо да је $p(c) = g(c) \cdot h(c) = 0$.

Обратно, претпоставимо да постоји $c \in \mathbb{F}$ тако да је $p(c) = 0$. Имамо да $(x - c) \mid p(x)$, па је $p(x) = q(c) \cdot (x - c)$, где је $\deg(x - c) < \deg p(x)$ и $\deg q(x) < \deg p(x)$. Дакле, полином $p(x)$ је сводљив. □

Пример 2.5. Приметимо да је полином $x^2 - 2 \in \mathbb{Q}[x]$ несводљив, док полином $x^2 - 2 \in \mathbb{R}[x]$ јесте сводљив, јер је $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. Полином $x^2 + 1 \in \mathbb{R}[x]$ је несводљив, а $x^2 + 1 \in \mathbb{C}[x]$ је сводљив полином, јер је $x^2 + 1 = (x - i)(x + i)$.

Претходно тврђење (смер $\to$) не важи за полиноме степена већег од 3, тј. полином степена већег од 3 може бити сводљив над $\mathbb{F}$ иако нема корен у $\mathbb{F}$, што показује следећи пример.

Пример 2.6. Посматрајмо пример $x^4 + x^2 + 1 = (x^2 + 1)^2 - x^2 = (x^2 - x + 1)(x^2 + x + 1)$ који је сводљив над $\mathbb{R}$, али $x^4 + x^2 + 1$ нема корен у $\mathbb{R}$ (јер $x^2 - x + 1$ и $x^2 + x + 1$ немају корен у $\mathbb{R}$).

Доказујема два помоћна тврђења (леме), која су аналогна одговарајућим тврђењима за просте бројеве:

Лема 2.1. Ако је $p(x) \in \mathbb{F}[x]$ несводљив полином и $q(x) \in \mathbb{F}[x]$ произвољан, тада је или $\mathrm{NZD}(p(x), q(x)) = 1$ или $p(x) \mid q(x)$.

Доказ. Нека је $d(x) = \mathrm{NZD}(p(x), q(x))$ и нека је $p(x)$ несводљив полином. Како $d(x) \mid p(x)$, то је $d(x)$ тривијални делилац. Дакле, имамо да је $d(x)$ константан полином или $d(x) = cp(x)$ за неко $c \in \mathbb{F} \setminus \{0\}$. Тада је $d(x) = 1$ због нормираности или $(cp(x)) \mid q(x)$, односно $\mathrm{NZD}(p(x), q(x)) = 1$ или $p(x) \mid q(x)$. □

Лема 2.2. Ако је $p(x) \in \mathbb{F}[x]$ несводљив, а $g(x), h(x) \in \mathbb{F}[x]$ произвољни, тада

$$p(x) \mid (g(x) \cdot h(x)) \Rightarrow p(x) \mid g(x) \vee p(x) \mid h(x).$$

Доказ. Нека је $p(x)$ несводљив и $p(x) \mid (g(x) \cdot h(x))$. Претпоставимо да $p(x) \nmid g(x)$, па закључујемо да је $\mathrm{NZD}(p(x), g(x)) = 1$ на основу леме 2.1. Из теореме о највећем заједничком делиоцу имамо да је $1 = s_0(x) \cdot p(x) + t_0(x) \cdot g(x)$ за неко $s_0(x), t_0(x) \in \mathbb{F}[x]$. Дакле, имамо да је

$$h(x) = h(x) \cdot 1 = h(x) \cdot (s_0(x) \cdot p(x) + t_0(x) \cdot g(x)) = s_0(x)p(x)h(x) + t_0(x)(h(x)g(x)) =$$

$$s_0(x)p(x)h(x) + t_0(x)(q(x)p(x)) = (s_0(x)h(x) + t_0(x)q(x))p(x).$$

Дакле, $p(x) \mid h(x)$. □

Следећа теореме је позната као теорема дуална основном ставу аритметике.

Теорема 2.10. Сваки полином $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$ се може јединствено, до редоследа фактора, представити у облику $p(x) = ap_1(x)p_2(x) \dots p_r(x)$, где $a \in \mathbb{F} \backslash \{0\}$ и $p_1(x), \dots, p_r(x)$ су несводљиви нормирани полиноми у $\mathbb{F}[x]$ (не обавезно различити).

Доказ. Прво, докажимо егзистенцију таквог представљања полинома $p(x)$. Доказ изводимо трансфинитном индукцијом по степену n полинома $p(x)$.

- Нека је полином $p(x)$ степена $n = 1$, односно нека је $p(x) = ax + b = a\underbrace{(x + a^{-1}b)}_{=p_1}$, где је $p_1 = x + a^{-1}b$ је нормиран и несводљив полином. Дакле, база индукције важи.
- Претпоставимо да тврђење важи за све полиноме степена мањег од n.
- Докажимо да тврђење важи и за полином $p(x)$ степена $n > 1$. Разликлујемо два случаја.
  1. Ако је $p(x)$ несводљив, $p(x) = a_0 + a_1x + \dots + a_nx^n$, $a_n \neq 0$, тада је $p(x) = a_np_1$, где је $p_1 = a_n^{-1}a_0 + a_n^{-1}a_1x + \dots + x^n$ несводљив и нормиран полином.
  2. Ако је $p(x)$сводљив, тј. $p(x) = g(x)h(x)$, где је $\deg g(x) < n, \deg h(x) < n$. Тада, по индуктивној хипотези имамо да важи
     $g(x) = bp_1(x) \dots p_k(x)$, $h(x) = cp_{k+1}(x) \dots p_r(x)$, где су $b \neq 0$ и $c \neq 0$ и сви $p_i(x)$ су нормирани и несводљиви полиноми, па је

     $$p(x) = g(x) \cdot h(x) = \underbrace{(b \cdot c)}_{=a} p_1(x) \dots p_k(x)p_{k+1}(x) \dots p_r(x),$$

     где је $a = bc \neq 0$, што је и требало показати.

Докажимо јединственост таквог представљања полинома $p(x)$. Нека се полином $p(x)$ може представити бар на два начина, тј. $p(x) = ap_1(x) \dots p_r(x)$ и $p(x) = bq_1(x) \dots q_s(x)$, где је $a \neq 0,\ b \neq 0$ и $p_1(x), \dots, p_r(x), q_1(x), \dots, q_s(x)$ су нормирани и несводљиви полиноми.

Индукцијом по r докажимо да је $a = b$, $r = s$ и $\{p_1(x), \dots, p_r(x)\} = \{q_1(x), \dots, q_s(x)\}$.

- Нека је $r = 1$. Тада пратећи следеће импликације налазимо да

$$\begin{aligned} p(x) = ap_1(x) \quad &\Rightarrow \quad p_1(x) = a^{-1}p(x) \ \Rightarrow \ p_1(x) = (a^{-1}b)q_1(x) \dots q_s(x) \\ &\Rightarrow \quad s = 1 \quad (\text{јер је } p_1(x) \text{ несводљив}) \\ &\Rightarrow \quad p_1(x) = (a^{-1}b)q_1(x) \\ &\Rightarrow \quad a^{-1}b = 1 \quad (\text{јер су } p_1(x), q_1(x) \text{ нормирани}) \\ &\Rightarrow \quad a = b, \quad p_1(x) = q_1(x). \end{aligned}$$

- Нека тврђење важи за $r-1$.
- Докажимо да тврђење важи и за r, па имамо да из

$$\begin{array}{rl} & ap_1(x)\dots p_r(x) = bq_1(x)\dots q_s(x) \\ \Rightarrow & \quad p_1(x) \mid (bq_1(x)\dots q_s(x)) \\ \Rightarrow & p_1(x) \mid q_1(x) \vee p_1(x) \mid q_2(x) \vee \dots \vee p_1(x) \mid q_s(x) \quad \text{(из Леме 2.2).} \end{array}$$

Нека важи да $p_1(x) \mid q_1(x)$. Тада из несводљивости и нормираности полинома $p_1(x)$ и $q_1(x)$ следи $p_1(x) = q_1(x)$, па из

$$\begin{array}{rcl} ap_1(x)p_2(x)\dots p_r(x) & = & bp_1(x)q_2(x)\dots q_s(x) \\ \Rightarrow a(\underbrace{p_2(x)\dots p_r(x)}_{r-1}) & = & b(q_2(x)\dots q_s(x)) \text{ (скраћивањем са } p_1(x)) \\ \Rightarrow a=b,\ r=s,\ \{p_2(x),\dots,p_r(x)\} & = & \{q_2(x),\dots,q_s(x)\} \text{ (по индуктивној хипотези)} \\ \Rightarrow \{p_1(x),\dots,p_r(x)\} & = & \{q_1(x),\dots,q_s(x)\}, \end{array}$$

што је и требало показати. □

2.8 Алгебарски затворена поља

Полиноми карактеришу и поља на известан начин. Из тог разлога имамо класификацију поља на основу следеће дефиниције.

Дефиниција 2.14. Поље $\mathbb{F}$ је алгебарски затворено ако сваки полином $p(x) \in \mathbb{F}[x]$, степена $n \geqslant 1$ има бар један корен у $\mathbb{F}$.

Пример 2.7. Поље $\mathbb{R}$ није алгебарски затворено, нпр. полином $p(x) = x^2 + 1 \in \mathbb{R}[x]$ нема корен у $\mathbb{R}$.

За разлику од поља реалних бројева које није алгебарски затворено, поље комплексних бројева јесте о чему сведочи следеће тврђење.

Основни став линеарне алгебре. Поље комплексних бројева је алгебарски затворено.

Сада, можемо описати несводљиве полиноме над алгебарски затвореним пољем.

Теорема 2.11. Следећа тврђења су еквивалентна:

1. Поље $\mathbb{F}$ је алгебарски затворено.
2. Једини несводљиви полиноми у $\mathbb{F}[x]$ су линеарни полиноми.
3. Сваки полином $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$ може се факторисати у производ n линеарних полинома (чинилаца).

Доказ. (1. $\rightarrow$ 2.) Претпоставимо да је поље $\mathbb{F}$ алгебарски затворено. Како су линеарни полиноми несводљиви, покажимо да над алгебарски затвореним пољем $\mathbb{F}$ нема других несводљивих полинома. Нека је $p(x) \in \mathbb{F}[x]$, произвољан полином степена већег од један. Искористимо чињеницу да је поље $\mathbb{F}$ алгебарски затворено и закључити да постоји $c \in \mathbb{F}$ такав да је $p(c) = 0$, односно да важи $(x-c) \mid p(x)$. Дакле, имамо да је $p(x) = (x-c)q(x)$, где је $x-c, q(x) \in \mathbb{F}[x]$ и важи $\deg(x-c) = 1 < \deg p(x)$, одакле можемо закључити да је полином $p(x)$ сводљив.

(2. → 3.) Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\deg p(x) = n \geqslant 1$. Тада на основу теореме која је дуална Основном ставу аритметике налазимо да је $p(x) = a \cdot p_1(x) \cdot \ldots \cdot p_r(x)$, где су сви $p_i(x)$ нормирани и несводљиви полиноми. Из услова теореме закључујемо да су сви $p_i(x)$ линеарни. Како је $\deg p(x) = \deg p_1(x) + \cdots + \deg p_r(x) = \underbrace{1 + \cdots + 1}_{r}$, следи да је $n = r$, па је $p(x)$ производ n линеарних полинома (чинилаца).

(3. → 1.) Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\deg p(x) = n \geqslant 1$. На основу претпоставке теореме имамо да је $p(x) = p_1(x) \cdot \ldots \cdot p_n(x)$ и сви $p_i(x)$ су линеарни. Претпоставимо да је $p_1(x) = ax + b$, $a \neq 0$. Лако налазимо да је $c = -a^{-1}b \in \mathbb{F}$ корен полинома $p_1(x)$, а тиме и полинома $p(x)$, што је и требало показати. □

Последица 1. Полином $p(c) \in \mathbb{C}[x]$ степена $n \geqslant 1$, са водећим коефицијентом a_n, може се на јединствен начин (до редоследа фактора) факторисати у облику

$$p(x) = a_n(x - c_1)(x - c_2) \cdot \ldots \cdot (x - c_n),$$

где су $c_1, \ldots, c_n$ корени (не морају бити различити) полинома $p(x)$.

Пример 2.8. Испитати сводљивост полинома $p(x) = x^7 - x^6 + x^5 - x^4 + x^3 - x^2 + x - 1$ над пољима $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, а затим га представити као производ несводљивих полинома редом, над свим тим пољима. Имамо да је

$$p(x) = x^6(x-1) + x^4(x-1) + x^2(x-1) + (x-1) = (x-1)(x^6 + x^4 + x^2 + 1),$$

где су $x - 1$, $x^6 + x^4 + x^2 + 1 \in \mathbb{Q}[x]$ полиноми нижег степена од $p(x)$, па је $p(x)$ сводљив над пољем $\mathbb{Q}$, а тиме и над пољима $\mathbb{R}$ и $\mathbb{C}$.

Даље, покушајмо да дати полином раставимо на седам линеарних фактора у датим пољима.

- У пољу $\mathbb{Q}$ то није могуће, јер је
  $$p(x) = (x-1)(x^4(x^2+1) + (x^2+1)) = (x-1)(x^2+1)(x^4+1)$$
  факторизација над $\mathbb{Q}$, док полиноми $x^2 + 1$ и $x^4 + 1$ су несводљиви над $\mathbb{Q}$.
- Ни у пољу реалних бројева то није могуће, јер је
  $$p(x) = (x-1)(x^2+1)((x^2+1)^2 - 2x^2) = (x-1)(x^2+1)(x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$$
  факторизација над $\mathbb{R}$, а три квадратана полинома су несводљива.
- У пољу комплексних бројева то јесте могуће и добијамо да је
  $$p(x) = (x-1)(x+i)(x-i)(x+\frac{\sqrt{2}}{2}(1+i))(x+\frac{\sqrt{2}}{2}(1-i))(x-\frac{\sqrt{2}}{2}(1+i))(x-\frac{\sqrt{2}}{2}(1-i))$$
  факторизација над $\mathbb{C}$.

2.9 Вишеструки корени полинома

Ако се у разлагању $p(x) = a_n(x - c_1)(x - c_2) \ldots (x - c_n)$ полинома $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$, елемент $c \in \mathbb{F}$ јавља у низу $c_1, \ldots, c_n$ тачно k пута, где је $1 \leqslant k \leqslant n$, кажемо да је $c \in \mathbb{F}$ корен реда k полинома $p(x)$.

ДЕФИНИЦИЈА 2.15. Елемент $c \in \mathbb{F}$ је корен реда k полинома $p(x) \in \mathbb{F}[x]$ ако $(x-c)^k \mid p(x)$ и $(x-c)^{k+1} \nmid p(x)$, тј.

$$p(x) = (x-c)^k q(x), \qquad q(x) \in \mathbb{F}[x], \qquad q(c) \neq 0.$$

- Ако је $k > 1$, тада је c вишеструк корен,
- ако је $k = 1$, тада је c прост корен.

Полином $p(x) \in \mathbb{C}[x]$ степена $n \geqslant 1$ са водећим коефицијентом a_n може се на јединствен начин (до редоследа фактора) факторисати у облику

$$p(x) = a_n(x-c_1)^{k_1}(x-c_2)^{k_2} \ldots (x-c_r)^{k_r}, \quad a_n \neq 0,$$

где су $c_1, \ldots, c_r$ различити корени полинома $p(x)$ реда $k_1, \ldots, k_r$, респективно, и важи да је $k_1 + k_2 + \cdots + k_r = n$.

ТЕОРЕМА 2.12. Нека је $\mathbb{F}$ поље, $\mathrm{char}\mathbb{F} = 0$ и $c \in \mathbb{F}$ корен реда k полинома $p(x) \in \mathbb{F}[x]$.

- Ако је $k > 1$, тада је c корен реда $k-1$ првог изводног полинома $p'(x)$,
- ако је $k = 1$ тада c није корен полинома $p'(x)$.

Доказ. Нека је $p(x) = (x-c)^k q(x)$, $q(x) \in \mathbb{F}[x]$ и $q(c) \neq 0$. Тада имамо да је

$$p'(x) = k(x-c)^{k-1}q(x) + (x-c)^k q'(x) = (x-c)^{k-1}\underbrace{(kq(x) + (x-c)q'(x))}_{q_1(x)}.$$

Сада, размотримо следеће случајеве.

- Нека је $k > 1$. Како је $p'(x) = (x-c)^{k-1}q_1(x)$ и $q_1(c) = kq(c) \neq 0$ следи да је $c \in \mathbb{F}$ корен реда $k-1$ полинома $p'(x)$.
- Нека је $k = 1$. Из чињенице да је $p'(x) = q_1(x)$ и $q_1(c) = kq(c) \neq 0$ следи да $c \in \mathbb{F}$ није корен полинома $p'(x)$. □

ПОСЛЕДИЦА 1. Све вишеструке нуле полинома $p(x)$ су све нуле полинома $\mathrm{NZD}(p(x), p'(x))$.

Доказ. Посматрајмо следећи еквиваленцијски ланац.

$c \in \mathbb{F}$ је вишеструки корен полинома $p(x)$
$\Leftrightarrow$ c је корен полинома $p(x)$ и $p'(x)$ (на основу претходне теореме)
$\Leftrightarrow$ $(x-c) \mid p(x), \quad (x-c) \mid p'(x)$
$\Leftrightarrow$ $(x-c) \mid \mathrm{NZD}(p(x), p'(x))$
$\Leftrightarrow$ c је корен полинома $\mathrm{NZD}(p(x), p'(x))$.

Дакле, важи тврђење последице. □

ПОСЛЕДИЦА 2. Полином $\dfrac{p(x)}{\mathrm{NZD}(p(x), p'(x))}$ има само просте корене и ти корени су различити корени полинома $p(x)$.

ПРИМЕР 2.9. Одредити вишеструке корене полинома $p(x) = x^7 - 2x^5 - x^4 + x^3 + 2x^2 - 1$. Потребно је одредити $\mathrm{NZD}(p(x), p'(x))$. Најпре, одредимо $p'(x) = 7x^6 - 10x^4 - 4x^3 + 3x^2 + 4x$. Познатим поступком налазимо да је

$$\mathrm{NZD}(p(x), p'(x)) = x^3 - x^2 - x + 1 = x^2(x-1) - (x-1) = (x^2-1)(x-1) = (x-1)^2(x+1),$$

На основу добијеног полинома, можемо закључити следеће.

- 1 и -1 су заједнички корени полинома $p(x)$ и $p'(x)$,
- -1 је прост корен полинома $p'(x)$ и корен реда 2 полинома $p(x)$,
- 1 је корен реда 2 полинома $p'(x)$ и корен реда 3 полинома $p(x)$,

па је

$$p(x) = (x-1)^3(x+1)^2 q(x), \qquad \deg q(x) = 2.$$

Из Хорнерове шеме добијамо

1	1	0	-2	-1	1	2	0	-1
	1	1	-1	-2	-1	1	1	0
	1	2	1	-1	-2	-1	0	
-1	1	3	4	3	1	0		
	1	2	2	1	0			
	1	1	1	0				

па је $q(x) = x^2 + x + 1$, односно $p(x) = (x-1)^3(x+1)^2(x^2+x+1)$.

Заиста, полином $\dfrac{p(x)}{\mathrm{NZD}(p(x), p'(x))} = (x-1)(x+1)(x^2+x+1)$ има само просте корене и то су корени полинома $p(x)$.

Теорема 2.13. Ако је $\mathbb{F}$ поље, $\mathrm{char}\mathbb{F} = 0$, $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$ и $c \in \mathbb{F}$, тада је

$$p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \frac{p''(c)}{2!}(x-c)^2 + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n$$

$$\text{и} \quad a_k = \frac{p^{(k)}(0)}{k!} \ (k = 0, 1, \ldots, n), \ \text{где } p^{(0)} \overset{\text{def}}{=} p(x).$$

Доказ. Нека је $p(x) = b_0 + b_1(x-c) + b_2(x-c)^2 + \cdots + b_n(x-c)^n$. Одредимо коефицијенте $b_0, \ldots, b_n$.

Стављајући да је $x = c$ добијамо да је $b_0 = p(c)$, а то можемо записати у облику $b_0 = \dfrac{p^{(0)}(c)}{0!}$.

Сада, одредимо први изводни полином, тј. налазимо да је

$$p'(x) = b_1 + 2b_2(x-c) + 3b_3(x-c)^2 + \cdots + nb_n(x-c)^{n-1},$$

па стављајући да је $x = c$ добијамо $b_1 = p'(c)$, а то можемо записати у облику $b_1 = \dfrac{p'(c)}{1!}$.

Сада, одредимо други изводни полином, тј. налазимо да је

$$p''(x) = 2 \cdot 1 \cdot b_2 + 3 \cdot 2b_3(x-c) + \cdots + n(n-1)b_n(x-c)^{n-2},$$

па стављајући да је $x = c$ добијамо $p''(c) = 2!b_2$, а то можемо записати у облику $b_2 = \dfrac{p''(c)}{2!}$.

Настављајући поступак, налазимо да је

$$p^{(k)} = k!b_k + (k+1)!b_{k+1}(x-c) + \cdots + n(n-1)\ldots(n-k+1)b_n(x-c)^{n-k},$$

па стављајући да је $x = c$ добијамо $p^{(k)}(c) = k!b_k$, а то можемо записати у облику $b_k = \dfrac{p^{(k)}(c)}{k!}$, за $k = 0, 1, 2, \ldots, n$.

Дакле, важи да је

$$p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \frac{p''(c)}{2!}(x-c)^2 + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n.$$

За $c = 0$ добијамо

$$p(x) = p(0) + \frac{p'(0)}{1!}x + \cdots + \frac{p^{(n)}(0)}{n!}x^n.$$

Упоређивањем коефицијената са $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{F}[x]$ следи

$$a_k = \frac{p^{(k)}(0)}{k!} \quad (k = 0, 1, \ldots, n),$$

што је и требало показати. □

Полином из претходне теореме се назива Тејлоров полином.

ТЕОРЕМА 2.14. Ако је $\mathbb{F}$ поље, $\mathrm{char}\mathbb{F} = 0, p(x) \in \mathbb{F}[x]$ полином степена $n \geqslant 1$ и $c \in \mathbb{F}$, тада је c корен реда k полинома $p(x)$ акко је

$$p(c) = p'(c) = \cdots = p^{(k-1)}(c) = 0 \quad \text{и} \quad p^{(k)}(c) \neq 0.$$

Доказ. Нека је c корен реда k полинома $p(x)$. Тада је c корен реда $k-1$ полинома $p'(x)$ итд. Односно, c је прост корен полинома $p^{(k-1)}(x)$ и c није корен полинома $p^{(k)}(x)$. Дакле, важи да је

$$p(c) = p'(c) = \cdots = p^{(k-1)}(c) = 0 \quad \text{и} \quad p^{(k)}(c) \neq 0.$$

Обратно, нека важи следеће

$$p(c) = p'(c) = \cdots = p^{(k-1)}(c) = 0 \quad \text{и} \quad p^{(k)}(c) \neq 0.$$

Из $p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n$ и $p(c) = \cdots = p^{(k-1)}(c) = 0$ следи да је

$$p(x) = \frac{p^{(k)}(c)}{k!}(x-c)^k + \frac{p^{(k+1)}(c)}{(k+1)!}(x-c)^{k+1} + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n.$$

Дакле, имамо облик

$$p(x) = (x-c)^k \left(\underbrace{\frac{p^{(k)}(c)}{k!} + \frac{p^{(k+1)}(c)}{(k+1)!}(x-c) + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^{n-k}}_{q(x)} \right),$$

при чему је $q(c) = \frac{p^{(k)}(c)}{k!} \neq 0$, па је c корен реда k полинома $p(x)$. □

ПРИМЕР 2.10. За полином $p(x) = 2x^6 - x^5 - 13x^4 + 13x^3 + 19x^2 - 32x + 12$ и $c = 1$ важи следеће

$p(1) = 0,$

$p'(x) = 12x^5 - 5x^4 - 52x^3 + 39x^2 + 38x - 32, \quad p'(1) = 0,$

$p''(x) = 60x^4 - 20x^3 - 156x^2 + 78x + 38, \quad p''(1) = 0,$

$p'''(x) = 240x^3 - 60x^2 - 312x + 78, \quad p'''(1) = -54 \neq 0,$

па је $c = 1$ корен реда 3 полинома $p(x)$. Дакле, важи да је $p(x) = (x-1)^3q(x)$.

Помоћу Хорнерове шеме налазимо $q(x) = 2x^3 + 5x^2 - 4x - 12$, па је

$$p(x) = (x-1)^3(2x^3 + 5x^2 - 4x - 12).$$

2.10 Особине корена реалних полинома

У општем случају, реални полином се не може представити као производ линеарних реалних полинома (јер $\mathbb{R}$ није алгебарски затворено поље). Како је $\mathbb{R}[x] \subseteq \mathbb{C}[x]$, сваки реални полином можемо посматрати и као комплексни полином. Поље $\mathbb{C}$ је алгебарски затворено, па се сваки реални полином степена $n \geqslant 1$ може представити као производ комплексних линеарних полинома.

Теорема 2.15. Ако је комплексан број $c = \alpha + i\beta$ $(\alpha, \beta \in \mathbb{R})$ корен полинома $p(x) \in \mathbb{R}[x]$, тада је и $\overline{c} = \alpha - i\beta$ корен полинома $p(x)$.

Доказ. Нека је $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{R}[x]$ и $p(c) = 0$. Применом особина операције конјуговања ($\overline{z_1z_2} = \overline{z_1} \cdot \overline{z_2}, \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}, \quad z_1, z_2 \in \mathbb{C}$) добијамо следеће

$$\begin{array}{rcl} p(\overline{c}) & = & a_0 + a_1\overline{c} + a_2\overline{c}^2 + \cdots + a_n\overline{c}^n \\ & = & a_0 + a_1\overline{c} + a_2\overline{c^2} + \cdots + a_n\overline{c^n} \\ & = & \overline{a_0} + \overline{a_1}\,\overline{c} + \overline{a_2}\,\overline{c^2} + \cdots + \overline{a_n}\,\overline{c^n} \quad (\overline{a_i} = a_i, \text{ јер } a_i \in \mathbb{R}) \\ & = & \overline{a_0} + \overline{a_1c} + \overline{a_2c^2} + \cdots + \overline{a_nc^n} \\ & = & \overline{a_0 + a_1c + \cdots + a_nc^n} = \overline{p(c)} = \overline{0} = 0.\square \end{array}$$

Напомена. Претходна теорема не важи за комплексне нереалне полиноме, на пример $x^2 - (1+i)x + i \in \mathbb{C}[x]$ има корене 1 и i ($-i$ није корен).

Последица 1. Сваки реални полином непарног степена има бар један корен у $\mathbb{R}$.

Теорема 2.16. Једини несводљиви полиноми у $\mathbb{R}[x]$ су линеарни полиноми и квадратни полиноми са негативном дискриминантом.

Доказ. Линеарни полиноми су свакако несводљиви (јер имају само тривијалне делиоце). Квадратни реални полиноми су несводљиви над $\mathbb{R}$ акко немају корен у $\mathbb{R}$, акко имају негативну дискриминанту. Докажимо да су сви остали реални полиноми сводљиви. Нека је $p(x) \in \mathbb{R}[x]$, $\deg p(x) > 2$. Тада $p(c) \in \mathbb{C}[x]$, $\mathbb{C}$ је алгебарски затворено, па постоји корен $c = \alpha + i\beta$ $(\alpha, \beta \in \mathbb{R})$ полинома $p(x)$.

Ако је $\beta = 0$, онда је $c = \alpha \in \mathbb{R}$, па је $p(x) = (x - \alpha)q,\ q \in \mathbb{R}[x]$. Дакле, $p(x)$ је сводљив над $\mathbb{R}$.

Ако је $\beta \neq 0$ онда $c \notin \mathbb{R}$, па је $\overline{c} = \alpha - i\beta$ је такође корен полинома $p(x)$. За полином

$$g(x) = (x - c)(x - \overline{c}) = (x - \alpha)^2 + \beta^2 = x^2 - 2\alpha x + \alpha^2 + \beta^2 \in \mathbb{R}[x]$$

имамо да је $D = 4\alpha^2 - 4(\alpha^2 + \beta^2) = -4\beta^2 < 0$, па је $g(x)$ несводљив над $\mathbb{R}$.

Докажимо да се полином $p(x)$ увек може раставити на чиниоце који су степена највише два. По теореми о дељењу имамо да је

$$p(x) = g(x)q(x) + r(x), \quad q(x), r(x) \in \mathbb{R}[x], \quad r(x) = 0 \text{ или } \deg r(x) < \deg g(x).$$

- $r(x) = 0 \Rightarrow\ p(x) = g(x)q(x)$, где је $g(x), q(x) \in \mathbb{R}[x]$, $\deg g(x) = 2 < \deg p(x)$ $\Rightarrow p(x)$ је сводљив над $\mathbb{R}$.

- $r(x) \neq 0 \Rightarrow\ \deg r(x) = 0$ или $\deg r(x) = 1$.

$$\begin{array}{ll} \deg r(x) = 0 & \Rightarrow r(x) \in \mathbb{R} \\ & \Rightarrow 0 = p(c) = g(c)q(c) + r = r. \text{ Контрадикција.} \end{array}$$

$$\begin{aligned}\deg r(x)=1 \quad &\Rightarrow r(x)=ax+b,\ a\neq 0,\\ &\Rightarrow 0=p(c)=g(c)q(c)+ac+b\\ &\Rightarrow ac+b=0\\ &\Rightarrow c=-a^{-1}b\in\mathbb{R}.\ \text{Контрадикција.}\square\end{aligned}$$

ПОСЛЕДИЦА 1. Сваки реални полином $p(x)$ степена $n \geqslant 1$, са водећим коефицијентом a_n, може се на јединствен начин (до редоследа фактора) представити у облику

$$p(x)=a_n(x-c_1)^{k_1}\dots(x-c_r)^{k_r}(x^2+p_1x+q_1)^{l_1}\dots(x^2+p_tx+q_t)^{l_t},$$

при чему су $c_1,\dots,c_r\in\mathbb{R}$ различити корени полинома $p(x)$ реда $k_1,\dots,k_r$ (респективно), $p_i,q_i\in\mathbb{R},\quad p_i^2-4q_i<0\ \ (i=1,\dots t)$ и $k_1+\dots+k_r+2(l_1+\dots+l_t)=n$.

Дакле, сваки полином $p(x)\in\mathbb{R}[x]$ степена $n\geqslant 1$ има тачно n корена у $\mathbb{C}$. Како их практично одредити?

- Ако је $n=1$ или $n=2$ познате су формуле за одређивање корена полинома коначном применом операција сабирања, множења, дељења и кореновања на коефицијенте полинома.
- Ако је $n=3$ или $n=4$ знамо за Карданове (Girolamo Cardano, 1501–1576.) и Фераријеве (Lodovico Ferrari, 1522–1565.) формуле, веома компликоване и без практичног значаја.
- Ако је $n\geqslant 5$, Абел (Niels Henrik Abel 1802–1829.) и Галоа (Evariste Galois 1811–1832.) су доказали да, у општем случају, да такве формуле не постоје, тј. да се сви корени полинома степена већег од 4 не могу добити применом коначног низа операција сабирања, одузимања, множења, дељења и кореновања на коефицијенте полинома.

  Само у неким специјалним случајевима постоје поступци за налажење корена полинома степена већег од 4.

За $p(x)\in\mathbb{Z}[x]$ постоји практични поступак за налажење рационалних нула (ако их полином има).

ТЕОРЕМА 2.17. Ако је $\dfrac{p}{q}$ $(p\in\mathbb{Z},\ q\in\mathbb{N}$ и $\mathrm{NZD}(p,q)=1)$ корен полинома $z(x)=a_0+a_1x+\dots+a_nx^n\in\mathbb{Z}[x]\ \ (a_n\neq 0, a_0\neq 0)$, тада $p\mid a_0$ и $q\mid a_n$.

Доказ. Из чињенице да је $z(\frac{p}{q})=0$ следи

$$a_0+a_1\frac{p}{q}+a_2\frac{p^2}{q^2}+\dots+a_{n-1}\frac{p^{n-1}}{q^{n-1}}+a_n\frac{p^n}{q^n}=0/\cdot q^{n-1}/\cdot\frac{q^n}{p},\ p\neq 0,$$

па је

$$\underbrace{a_0q^{n-1}+a_1pq^{n-2}+\dots+a_{n-1}p^{n-1}}_{\in\mathbb{Z}}+a_n\frac{p^n}{q}=0,$$

односно, добијамо да је $\dfrac{a_np^n}{q}\in\mathbb{Z}$. Како је $\mathrm{NZD}(p,q)=1$, то је и $\mathrm{NZD}(p^n,q)=1$, па $q\mid a_n$. Из

$$\frac{a_0q^n}{p}+\underbrace{a_1q^{n-1}+\dots a_{n-1}p^{n-2}q+a_np^{n-1}}_{\in\mathbb{Z}}=0,$$

налазимо да је $\dfrac{a_0q^n}{p}\in\mathbb{Z}$. Како је $\mathrm{NZD}(p,q)=1$, следи да $\mathrm{NZD}(q^n,p)=1$, па $p\mid a_0$. $\square$

ПОСЛЕДИЦА 1. Ако је цели број $c\in\mathbb{Z}$ корен полинома са целим коефицијентима $z(x)=a_0+a_1x+\dots+a_nx^n\in\mathbb{Z}[x]$, $a_0a_n\neq 0$, онда $c\mid a_0$.

ПРИМЕР 2.11. Ако је $z(x) = 2x^4+3x^3-3x^2-5x-6, z(\frac{p}{q}) = 0 \quad (p \in \mathbb{Z}, q \in \mathbb{N}, \mathrm{NZD}(p,q) = 1)$ онда

$$\begin{array}{rcl} p \mid (-6),\ p \in \mathbb{Z} & \Rightarrow & p \in \{\pm 1, \pm 2, \pm 3, \pm 6\} \\ q \mid 2,\ q \in \mathbb{N} & \Rightarrow & q \in \{1, 2\} \end{array} \Rightarrow \frac{p}{q} \in \{\pm 1, \pm 2, \pm 3, \pm 6, \pm\frac{1}{2}, \pm\frac{3}{2}\}.$$

Провером налазимо да је $z(-2) = 0, z(\frac{3}{2}) = 0$, па су $c_1 = -2$ и $c_2 = \frac{3}{2}$ корени. Тада је

$$z(x) = (x+2)\left(x - \frac{3}{2}\right) q(x), q(x) = 2x^2 + 2x + 2,$$

па су преостала два корена корени полинома $q(x)$:

$$c_3 = \frac{-1 + i\sqrt{3}}{2}, \quad c_4 = \frac{-1 - i\sqrt{3}}{2}.$$

ПРИМЕР 2.12. Факторисати полином $z(x) = x^5 - x^4 - 5x^3 + 2x^2 + 4x + 8$

(а) над пољем $\mathbb{R}$,

(б) над пољем $\mathbb{C}$.

Из $p(c) = 0,\ c \in \mathbb{Z} \Rightarrow \ c \mid 8 \ \Rightarrow c \in \{-8, -4, -2, 2, 4, 8\}$ ("кандидати" за целобројне корене).

Провером (Хорнеровом шемом или преко изводног полинома) добијамо да је број 2 двоструки, а број -2 прост корен полинома $z(x)$, па је

$$z(x) = (x-2)^2(x+2)(x^2+x+1).$$

Дакле, имамо да је

(а) $z(x) = (x-2)^2(x+2)(x^2+x+1)$,

(б) $z(x) = (x-2)^2(x+2)(x+\frac{1}{2}(1-i\sqrt{3}))(x+\frac{1}{2}(1+i\sqrt{3}))$.

ТЕОРЕМА 2.18. Ако је $a + b\sqrt{n}$ $(a, b \in \mathbb{Q}$ и $n \in \mathbb{N}$ није потпун квадрат) корен полинома $p(x) \in \mathbb{Q}[x]$, онда је и $a - b\sqrt{n}$ корен полинома $p(x)$.

Доказ. За $\mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} | a, b \in \mathbb{Q}\}$ лако се проверава да је $(\mathbb{Q}(\sqrt{n}), +, \cdot)$ потпоље поља реалних бројева. За бројеве $c = a + b\sqrt{n}$ и $\overline{c} = a - b\sqrt{n}$ кажемо да су конјуговани. Конјуговање има особине (проверити):

- $\overline{c+d} = \overline{c} + \overline{d}$,
- $\overline{c \cdot d} = \overline{c} \cdot \overline{d}$,
- $c = \overline{c} \Leftrightarrow c \in \mathbb{Q}$.

Ако је $c = a + b\sqrt{n}$ корен полинома $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Q}[x]$ онда

$$p(\overline{c}) = \overline{p(c)} = \overline{0} = 0,$$

тј. $\overline{c}$ је такође корен полинома $p(x)$. □

Глава 3

Векторски простори

3.1 Дефиниција векторског простора

Један од најзначајнијих појмова у математици јесу вектори.

Дефиниција 3.1. Нека је:

- $V = \{x, y, z, x_1, y_1, z_1, \dots\}$ непразан скуп,
- $F = \{\alpha, \beta, \gamma, \dots\}$ и $(F, \oplus, \odot, 0, 1)$ поље,
- $+ : V \times V \to V,\ (x, y) \mapsto x + y,\ \cdot : F \times V \to V,\ (\alpha, x) \mapsto \alpha \cdot x$.

Уређена четворка $(V, +, \cdot, F)$ је векторски простор ако за свако $x, y \in V$ и свако $\alpha, \beta \in F$ важи:

(V_1) $(V, +)$ је Абелова група,

(V_2) $\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$,

(V_3) $(\alpha \oplus \beta) \cdot x = \alpha \cdot x + \beta \cdot x$,

(V_4) $\alpha \cdot (\beta \cdot x) = (\alpha \odot \beta) \cdot x$,

(V_5) $1 \cdot x = x$.

У складу са претходном дефиницијом, издвајамо следеће појмове.

- Елементи скупа V се зову вектори.
- Елементи поља F се зову скалари.
- $+$ је сабирање вектора, а $\cdot$ множење вектора скаларом.
- Неутрални у групи $(V, +)$ означавамо са 0_V или само 0 и зовемо нула вектор.
- Инверзни од x у групи $(V, +)$ означавамо са $-x$ и зовемо супротан вектор од x.
- $\cdot$ обично изостављамо (уместо $\alpha \cdot x$ пишемо αx)
- Када год то не изазива забуну уместо ознака $\oplus$ и $\odot$ (операције у пољу F) користићемо $+$ и $\cdot$.

- За нула вектор и нула скалар користићемо исту ознаку 0, кад год је из контекста јасно да ли се ради о вектору или скалару.

Пример 3.1. $(V, +, \cdot, \mathbb{R})$ је реални векторски простор, $(V, +, \cdot, \mathbb{C})$ комплексни векторски простор.

Скуп аксиома (V_1)-(V_5) је независан (ниједна од њих није последица осталих). Из тог разлога уочимо следећи пример.

Пример 3.2. Нека је $(\mathbb{C}, +, \cdot, \mathbb{C})$, $x + y \overset{\text{def}}{=} y, \alpha \cdot x \overset{\text{def}}{=} x(\alpha, x, y \in \mathbb{C})$.

Аксиоме (V_2)-(V_5) важе у посматраној структури. нпр. $(V_2)\, \alpha \cdot (x+y) = x+y = \alpha \cdot x + \alpha \cdot y$, али V_1 не важи, јер $x + y \neq y + x$, за $x \neq y$ (нпр. $1 + 2 = 2, 2 + 1 = 1$). Дакле, можемо закључити да је (V_2)-$(V_5) \not\models (V_1)$.

Теорема 3.1. У векторском простору $(V, +, \cdot, F)$ важи:

(1) $\alpha \cdot 0_V = 0_V, \alpha \in F$,

(2) $0_F \cdot x = 0_V, x \in V$,

(3) $\alpha \cdot x = 0_V \Leftrightarrow \alpha = 0_F \vee x = 0_V, x \in V, \alpha \in F$,

(4) $\alpha(-x) = -(\alpha x) = (-\alpha)x, x \in V, \alpha \in F$

(5) $(\alpha_1 + \cdots + \alpha_n) \cdot x = \alpha_1 \cdot x + \cdots + \alpha_n \cdot x$,
$\alpha \cdot (x_1 + \cdots + x_n) = \alpha \cdot x_1 + \cdots + \alpha \cdot x_n$,
$n \in \mathbb{N}, \quad x, x_1, \ldots, x_n \in V, \quad \alpha, \alpha_1, \ldots \alpha_n \in F$.

Доказ.

(1) Заиста, важи да је

$$\begin{array}{rcl} \alpha \cdot (0_V + 0_V) & = & \alpha \cdot 0_V \\ \alpha \cdot 0_V + \alpha \cdot 0_V & = & \alpha \cdot 0_V \;/ - (\alpha \cdot 0_V) \\ (\alpha \cdot 0_V + \alpha \cdot 0_V) - (\alpha \cdot 0_V) & = & \alpha \cdot 0_V - (\alpha \cdot 0_V) \\ \alpha \cdot 0_V + (\alpha \cdot 0_V - (\alpha \cdot 0_V)) & = & 0_V \\ \alpha \cdot 0_V + 0_V & = & 0_V \\ \alpha \cdot 0_V & = & 0_V. \end{array}.$$

(2) Слично као и претходно.

(3) Докажимо $\alpha \cdot x = 0_V \Leftrightarrow \alpha = 0_F \vee x = 0_V$. Нека је

$$\begin{array}{ll} & \alpha \cdot x = 0_V, \quad \alpha \neq 0_F \\ \rightarrow & (\exists \alpha^{-1} \in F)\, \alpha^{-1} \cdot (\alpha \cdot x) = \alpha^{-1} \cdot 0_V \\ \rightarrow & (\alpha^{-1}\alpha) \cdot x = 0_V \quad \text{(применом (1) и } (V_4)) \\ \rightarrow & 1 \cdot x = 0_V \\ \rightarrow & x = 0_V \quad \text{(из } V_5). \end{array}$$

Обратно, директно следи из (1) и (2).

(4) Имамо да је

$$\begin{aligned}(-\alpha)\cdot x &= (-\alpha)\cdot x + 0_V\\ &= (-\alpha)\cdot x + (\alpha\cdot x + (-(\alpha\cdot x)))\\ &= ((-\alpha)\cdot x + \alpha\cdot x) + (-(\alpha x))\\ &= (-\alpha+\alpha)\cdot x + (-(\alpha x))\\ &= 0_F\cdot x + (-(\alpha\cdot x))\\ &= 0_V + (-(\alpha\cdot x))\\ &= -(\alpha\cdot x).\end{aligned}$$

(5) Једноставно, индукцијом по n.

Пример 3.3. (1) $V =$ "скуп геометријских вектора (оријентисаних дужи) у равни", где је $+$ сабирање вектора, $\cdot$ множење вектора реалним бројем, је векторски простор над пољем реалних бројева.

(2) $(F, +, \cdot, F)$, где су $+$ и $\cdot$ сабирање и множење у пољу F,је векторски простор поља F.

(3) Ако је H потпоље поља F, $+$ и $\cdot$ операције из поља F, онда $F_H = (F, +, \cdot, H)$ је векторски простор потпоља.

(а) $\mathbb{R}_{\mathbb{Q}} = (\mathbb{R}, +, \cdot, \mathbb{Q})$;

(б) $\mathbb{C}_{\mathbb{R}} = (\mathbb{C}, +, \cdot, \mathbb{R})$.

(4) $(F^n, +, \cdot, F)$, где су + и $\cdot$ дефинисани са

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) \overset{\text{def}}{=} (x_1 + y_1, \ldots, x_n + y_n),$$

$$\alpha\cdot(x_1, \ldots, x_n) \overset{\text{def}}{=} (\alpha x_1, \ldots, \alpha x_n),$$

за $(x_1, \ldots x_n), (y_1, \ldots, y_n) \in F^n$, $\alpha \in F$, је векторски простор уређених $n-$торки из поља F.

Посебно, $(\mathbb{R}^n, +, \cdot, \mathbb{R})$, $(\mathbb{C}^n, +, \cdot, \mathbb{C})$ су простори уређених $n-$торки реалних, односно, комплексних бројева.

(5) $(F^{\mathbb{N}}, +, \cdot, F)$, $F^{\mathbb{N}}$-скуп свих низова елемената поља F, $+$ и $\cdot$ су дефинисани са

$$(x_n) + (y_n) \overset{\text{def}}{=} (x_n + y_n),$$

$$\alpha\cdot(x_n) \overset{\text{def}}{=} (\alpha x_n),$$

за $\alpha \in F$, $(x_n) \in F^{\mathbb{N}}$, $(y_n) \in F^{\mathbb{N}}$ је векторски простор низова елемената из F.

$(\mathbb{R}^{\mathbb{N}}, +, \cdot, \mathbb{R})$, $(\mathbb{C}^{\mathbb{N}}, +, \cdot, \mathbb{C})$ су векторски простори низова реалних, односно, комплексних бројева.

(6) $(F^S, +, \cdot, F)$, F^S скуп свих функција које сликају S у F, $+$ и $\cdot$ су дефинисани са

$$f + g : S \to F, (f+g)(x) \overset{\text{def}}{=} f(x) + g(x),\ (x \in S),$$

$$(\alpha f) : S \to F, (\alpha f)(x) \overset{\text{def}}{=} \alpha f(x), (x \in S)$$

за $f, g \in F^S$ и $\alpha \in F$, је векторски простор функција из S у F.

Напомена. Стављајући $S = \mathbb{N}$, као специјални случај примера (6) добијамо пример (5).

(7) $(F_n[x],+,\cdot,F)$, $F_n[x]$ скуп полинома по x степена $\leqslant n$ са коефицијентима из поља F,

$$\begin{aligned}(a_0+\cdots+a_nx^n)+(b_0+\cdots+b_nx^n) &\overset{\text{def}}{=} (a_0+b_0)+\cdots+(a_n+b_n)x^n\\ \alpha(a_0+a_1x+\cdots+a_nx^n) &\overset{\text{def}}{=} (\alpha a_0)+(\alpha a_1)x+\ldots(\alpha a_n)x^n\\ (\text{за } \alpha\in F,\ a_0+\cdots+a_nx^n &\in F_n[x],\ b_0+\cdots+b_nx^n\in F_n[x])\end{aligned}$$

је векторски простор полинома по x степена $\leqslant n$ са коефицијентима из F.

Посебно, $(\mathbb{R}_n[x],+,\cdot,\mathbb{R})$-простор реалних полинома степена највише n. $(\mathbb{C}_n[x],+,\cdot,\mathbb{C})$ простор комплексних полинома степена највише n.

(8) Ако је V скуп полинома фиксираног степена n, $+$ и $\cdot$ дефинисани као у $F_n[x]$), тада V није векторски простор. Нпр. $p(x)=x^n-1\in V, q(x)=-x^n+x\in V, (p+q)(x)=x-1\notin V$.

3.2 Векторски потпростори

Дефиниција 3.2. Нека је $(V,+,\cdot,F)$ векторски простор и U непразан подскуп од V. Уколико је U и сам векторски простор у односу на рестрикције операције $+$ и функције $\cdot$, онда кажемо да је U векторски потпростор простора V и пишемо $U\preceq V$.

Једноставан критеријум за проверу који подскупови датог векторског простора представљају и његове потпросторе даје следећа теорема.

Теорема 3.2. Нека је $(V,+,\cdot,F)$ векторски простор и $\emptyset\neq U\subseteq V$. Тада $U\preceq V$ акко важе услови:

(1) $x\in U\wedge\alpha\in F\Rightarrow\alpha\cdot x\in U$ (тј. U је затворен за множење скаларом);

(2) $x\in U\wedge y\in U\Rightarrow x+y\in U$ (тј. U је затворен за сабирање вектора).

Доказ. Ако $U\preceq V$ онда је $(U,+,\cdot,F)$ векторски простор, па је скуп U затворен за сабирање вектора, као и за множење вектора скаларом.

Обратно, нека је $U\neq\emptyset$ и нека важе особине (1) и (2). Покажимо да је $(U,+,\cdot,F)$ векторски простор.

Особина (V_1) важи на основу следећег.

- Операција $+$ је комутативна и асоцијативна на V, па је таква и на његовом подскупу U.
- Из $U\neq\emptyset$ следи да постоји елемент $x\in U$. Тада
  $-1\in F, x\in U\overset{(1)}{\Rightarrow}(-1)\cdot x\in U\Rightarrow -x\in U$.
- $x\in U, -x\in U\overset{(2)}{\Rightarrow}x+(-x)\in U\Rightarrow 0_V\in U$.

Дакле, показали смо да је $(U,+)$ Абелова група. Аксиоме (V_2)–(V_5) важе, јер важе на целом скупу V. □

Услови (1) и (2) су еквивалентни услову

$(1')$ $x,y\in U\wedge\alpha,\beta\in F\ \Rightarrow\ \alpha\cdot x+\beta\cdot y\in U$.

Теорема 3.3. Нека је $(V,+,\cdot,F)$ векторски простор и $U_1,U_2\preceq V$. Тада је $U_1\cap U_2\preceq V$.

Доказ. Из $0 \in U_1$ и $0 \in U_2$ следи $0 \in U_1 \cap U_2$, па је $U_1 \cap U_2 \neq \emptyset$.

Проверимо услове (1) и (2).

(1)

$$\left.\begin{array}{c} x \in U_1 \cap U_2 \\ \alpha \in F \end{array}\right\} \Rightarrow \left.\begin{array}{cc} x \in U_1, & \alpha \in F \\ x \in U_2, & \alpha \in F \end{array}\right\} \Rightarrow \left.\begin{array}{c} \alpha \cdot x \in U_1 \\ \alpha \cdot x \in U_2 \end{array}\right\} \Rightarrow \alpha \cdot x \in U_1 \cap U_2.$$

(2)

$$x, y \in U_1 \cap U_2 \Rightarrow \left.\begin{array}{c} x, y \in U_1 \\ x, y \in U_2 \end{array}\right\} \Rightarrow \left.\begin{array}{c} x + y \in U_1 \\ x + y \in U_2 \end{array}\right\} \Rightarrow x + y \in U_1 \cap U_2.\square$$

ТЕОРЕМА 3.4. (а) Пресек произвољне фамилије векторских потпростора $\{U_i \mid i \in I\}$ простора $(V, +, \cdot, F)$ је такође потпростор простора V.

(б) Ако је $U_1 \preceq V$ и $U_2 \preceq V$, тада
$U_1 \cup U_2 \preceq V$ акко $U_1 \subseteq U_2$ или $U_2 \subseteq U_1$.

ПРИМЕР 3.4. 1. $\{0\}$ и V су тривијални потпростори простора V.

2. $U_1 = \{(x, 3x) | x \in \mathbb{R}\} \preceq \mathbb{R}^2$ (скуп свих тачака на правој $y = 3x$ је потпростор од $\mathbb{R}^2$). Провера:

   - $U_1 \neq \emptyset$ јер $(0, 0) \in U_1$;
   - (1) $(a, 3a) \in U_1 \land (b, 3b) \in U_1 \Rightarrow (a, 3a) + (b, 3b) = (a + b, 3(a + b)) \in U_1$;
   - (2) $\alpha \in \mathbb{R},\ (a, 3a) \in U_1 \Rightarrow \alpha \cdot (a, 3a) = (\alpha a, 3(\alpha a)) \in U_1$.

   $U_2 = \{(x, 3x + 2) | x \in \mathbb{R}\}$ није потпростор од $\mathbb{R}^2$ (не садржи нула вектор (0,0)).

   $U = \{(x, y) | ax + by + c = 0\} \preceq \mathbb{R}^2$ акко $c = 0$

   тј. тачке неке праве у $\mathbb{R}^2$ чине потпростор акко та права пролази кроз (0,0).

3. $U = \{(x, y, z) | x + y + 2z = 0\} \preceq \mathbb{R}^3$ (скуп тачака у $\mathbb{R}^3$ које припадају равни $x + y + 2z = 0$ је потпростор од $\mathbb{R}^3$).

   $U = \{(x, y, z) | ax + by + cz + d = 0\} \preceq \mathbb{R}^3$ акко $d = 0$

   (раван у $\mathbb{R}^3$ је потпростор акко пролази кроз координатни почетак).

4. Ако $V = \mathbb{R}^{\mathbb{R}}$, тј. V је простор реалних функција тада

   - $U_1 = \{f \in \mathbb{R}^{\mathbb{R}} | (\forall x \in \mathbb{R}) f(-x) = f(x)\} \preceq V$
     (потпростор парних реалних функција). Провера:
     - $0 \in U_1$ јер $0(-x) = 0 = 0(x)$ (нула функција је парна)
     - (1) $\alpha \in \mathbb{R}, f \in U_1 \quad \Rightarrow (\alpha \cdot f)(-x) = \alpha f(-x) = \alpha f(x) = (\alpha \cdot f)(x)$
       $\Rightarrow \alpha \cdot f \in U_1$
     - (2) $f, g \in U_1 \Rightarrow f(-x) = f(x),\ g(-x) = g(x)$
       $\Rightarrow (f + g)(-x) = f(-x) + g(-x) = f(x) + g(x) = (f + g)(x)$
       $\Rightarrow f + g \in U_1$.
   - $U_2 = \{f \in \mathbb{R}^{\mathbb{R}} | (\forall x \in \mathbb{R}) f(-x) = -f(x)\} \preceq V$
     (потпростор непарних реалних функција).
   - $U_3 = \{f \in \mathbb{R}^{\mathbb{R}} | f$ је непрекидна ф-ја на $\mathbb{R}\} \preceq V$.
   - $U_4 = \{f \in \mathbb{R}^{\mathbb{R}} | f$ је диференцијабилна ф-ја на $\mathbb{R}\} \preceq V$.

ПРИМЕР 3.5.
- Да ли је $\mathbb{R}^2 \preceq \mathbb{R}^3$? Не, $\mathbb{R}^2 \not\subseteq \mathbb{R}^3$.
- Да ли је $U = \{(a,b,0)|a,b \in \mathbb{R}\}$ потпростор од $\mathbb{R}^3$? Да.
- Да ли је $U' = \{(a,b,0)|a,b \in \mathbb{Z}\}$ потпростор од $\mathbb{R}^3$? Не, није затворен за множење скаларом, нпр. $(1,1,0) \in U'$, $\sqrt{2} \in \mathbb{R}$, $\sqrt{2} \cdot (1,1,0) = (\sqrt{2}, \sqrt{2}, 0) \notin U'$.

ДЕФИНИЦИЈА 3.3. Ако су U_1 и U_2 потпростори векторског простора V, тада

$$U_1 + U_2 \overset{\text{def}}{=} \{x_1 + x_2 | x_1 \in U_1, x_2 \in U_2\}$$

зовемо збир (сума) потпростора U_1 и U_2.

ТЕОРЕМА 3.5. Ако $U_1 \preceq V$ и $U_2 \preceq V$ онда и $U_1 + U_2 \preceq V$.

Доказ. Заиста,

- $0 = \underbrace{0}_{\in U_1} + \underbrace{0}_{\in U_2} \Rightarrow 0 \in U_1 + U_2 \Rightarrow U_1 + U_2 \neq \emptyset.$
- $x, y \in U_1 + U_2 \Rightarrow (\exists x_1, y_1 \in U_1)(\exists x_2, y_2 \in U_2)\ (x = x_1 + x_2,\ y = y_1 + y_2)$

  (1) $\alpha \cdot x = \alpha(x_1 + x_2) = \underbrace{\alpha x_1}_{\in U_1} + \underbrace{\alpha x_2}_{\in U_2} \in U_1 + U_2$

  $$\begin{array}{lrl} & x + y & = (x_1 + x_2) + (y_1 + y_2) = \\ (2) & & = \underbrace{(x_1 + y_1)}_{\in U_1} + \underbrace{(x_2 + y_2)}_{\in U_2} \in U_1 + U_2. \square \end{array}$$

Напомена. Разлагање $x = y + z$, $y \in U_1$, $z \in U_2$ вектора x, у општем случају, није јединствено, тј. из

$$x = y + z \in U_1 + U_2 \quad \text{и} \quad x = y' + z' \in U_1 + U_2,$$

у општем случају, не следи $y = y'$ и $z = z'$.

Показаћемо да је ово разлагање јединствено, за сваки $x \in V$, акко $U_1 \cap U_2 = \{0\}$.

ДЕФИНИЦИЈА 3.4. Збир $U_1 + U_2$ је директан ако је $U_1 \cap U_2 = \{0\}$. Обележава се са $U_1 \oplus U_2$.

ТЕОРЕМА 3.6. (Спектрална теорема) Нека $U_1 \preceq V$ и $U_2 \preceq V$. Тада $V = U_1 \oplus U_2$ акко се сваки вектор $x \in V$ може на јединствен начин представити у облику $x = y + z$, где $y \in U_1$ и $z \in U_2$, тј.

$$V = U_1 \oplus U_2 \Leftrightarrow (\forall x \in V)(\exists_1 y \in U_1)(\exists_1 z \in U_2)\ x = y + z.$$

Доказ. ($\rightarrow$) Нека је $V = U_1 \oplus U_2$, тј. $V = U_1 + U_2$ и $U_1 \cap U_2 = \{0\}$.

- Егзистенција разлагања: $V \subseteq U_1 + U_2 \ \Rightarrow\ (\forall x \in V)(\exists y \in U_1)(\exists z \in U_2)\ x = y + z$.
- Јединственост: претпоставимо супротно, тј. да постоји вектор x који се на два начина може разложити преко вектора из U_1 и U_2. То значи

$$\begin{array}{rcl} x = y + z & & x = y' + z', \quad y, y' \in U_1, z, z' \in U_2 \\ y + z & = & y' + z' \\ \underbrace{y + (-y')}_{\in U_1} & = & \underbrace{-z + z'}_{\in U_2} \in U_1 \cap U_2 \\ y + (-y') = 0 & & -z + z' = 0 \quad \text{јер } U_1 \cap U_2 = \{0\}. \\ y = y' & & z = z' \end{array}$$

($\leftarrow$) Претпоставимо да сваки вектор $x \in V$ има јединствено разлагање

$$x = y + z, \quad y \in U_1, z \in U_2.$$

- Докажимо најпре $V = U_1 + U_2$.

$$\begin{array}{l} (\forall x \in V)\; x \in U_1 + U_2 \quad \text{(јер сваки вектор има разлагање)} \\ \Rightarrow V \subseteq U_1 + U_2 \\ \Rightarrow V = U_1 + U_2. \end{array}$$

- Покажимо још да је $U_1 \cap U_2 = \{0\}$.

$$\begin{array}{l} x \in U_1 \cap U_2 \\ \Rightarrow x = \underbrace{x}_{\in U_1} + \underbrace{0}_{\in U_2}, \quad x = \underbrace{0}_{\in U_1} + \underbrace{x}_{\in U_2} \\ \Rightarrow \qquad x = 0 \quad \text{(због јединствености разлагања)} \\ \Rightarrow U_1 \cap U_2 = \{0\}.\Box \end{array}$$

Пример 3.6. Докажимо

$$\mathbb{R}^3 = U_1 \oplus U_2, \text{ где је } U_1 = \{(a,a,a) \mid a \in \mathbb{R}\},\ U_2 = \{(a,b,c) \mid a+b+c=0\}.$$

Лако се проверава да $U_1 \preceq \mathbb{R}^3$, $U_2 \preceq \mathbb{R}^3$. За $(x,y,z) \in \mathbb{R}^3$ одредимо $(a,a,a) \in U_1$ и $(a',b',c') \in U_2$ тако да

$$(x,y,z) = (a,a,a) + (a',b',c'),$$

тј.

$$(x,y,z) = (a+a', a+b', a+c').$$

Из

$$\begin{array}{rcl} x &=& a+a' \\ y &=& a+b' \\ z &=& a+c' \\ a'+b'+c' &=& 0 \end{array} \quad \Leftrightarrow \quad \begin{array}{rcl} a &=& \frac{x+y+z}{3} \\ a' &=& \frac{2x-y-z}{3} \\ b' &=& \frac{2y-x-z}{3} \\ c' &=& \frac{2z-x-y}{3} \end{array}$$

следи да вектор (x,y,z) има јединствено разлагање

$$(x,y,z) = \underbrace{\left(\frac{x+y+z}{3}, \frac{x+y+z}{3}, \frac{x+y+z}{3}\right)}_{\in U_1} + \underbrace{\left(\frac{2x-y-z}{3}, \frac{2y-x-z}{3}, \frac{2z-x-y}{3}\right)}_{\in U_2}.$$

Пример 3.7. $\mathbb{R}^\mathbb{R} = U_1 \oplus U_2$, $U_1 = \{f \in \mathbb{R}^\mathbb{R} \mid (\forall x \in \mathbb{R}) f(-x) = f(x)\}$,
$U_2 = \{f \in \mathbb{R}^\mathbb{R} \mid (\forall x \in \mathbb{R}) f(-x) = -f(x)\}$.

- $\mathbb{R}^\mathbb{R} = U_1 + U_2$

  За $f \in \mathbb{R}^\mathbb{R}$ одредимо $g \in U_1$ и $h \in U_2$ тако да је $f = g + h$. Из

$$(\forall x \in \mathbb{R}) \begin{array}{rcl} f(x) &=& g(x)+h(x) \\ f(-x) &=& g(-x)+h(-x) \end{array} \Rightarrow (\forall x \in \mathbb{R}) \begin{array}{rcl} f(x) &=& g(x)+h(x) \\ f(-x) &=& g(x)-h(x) \end{array}$$

  сабирањем и одузимањем последње две једнакости добијамо

$$g(x) = \frac{f(x)+f(-x)}{2}, \quad h(x) = \frac{f(x)-f(-x)}{2},$$

  па произвољна функција $f \in \mathbb{R}^\mathbb{R}$ има разлагање

$$f(x) = \underbrace{\frac{f(x)+f(-x)}{2}}_{\in U_1} + \underbrace{\frac{f(x)-f(-x)}{2}}_{\in U_2}.$$

- $U_1 \cap U_2 = \{0\}$

$$f \in U_1 \cap U_2 \quad \Rightarrow \quad \begin{array}{c} f \in U_1 \\ f \in U_2 \end{array} \quad \Rightarrow \quad \left.\begin{array}{l} (\forall x \in \mathbb{R})\, f(-x) = f(x) \\ (\forall x \in \mathbb{R})\, f(-x) = -f(x) \end{array}\right\} (-)$$
$$\Rightarrow (\forall x \in \mathbb{R})\, 2f(x) = 0 \Rightarrow (\forall x)\, f(x) = 0 \Rightarrow f = 0$$

Дефиниција 3.5. Нека $U_i \preceq V$, $1 \leq i \leq n$.

$$U_1 + \cdots + U_n \stackrel{\text{def}}{=} \big\{x_1 + \cdots + x_n \mid x_i \in U_i, i = 1, 2, \ldots, n\big\}$$

је збир потпростора $U_1, \ldots, U_n$.

Збир је директан, у означи $U_1 \oplus \cdots \oplus U_n$, ако

$$U_i \cap (U_1 + \cdots + U_{i-1}) = \{0\}, \quad i = 2, \ldots, n.$$

3.3 Линеарна пресликавања (хомоморфизми)

Везе између векторских простора успостављамо пресликавањима која „чувају” структуру векторских простора и која се зову линеарна пресликавања.

Дефиниција 3.6. Пресликавање $f : V \to U$ је линеарно пресликавање (хомоморфизам) векторског простора $(V, +_V, \cdot_V, F)$ у векторски простор $(U, +_U, \cdot_U, F)$ ако важи:

1. $f(x +_V y) = f(x) +_U f(y) \quad (x, y \in V)$ - адитивност
2. $f(\alpha \cdot_V x) = \alpha \cdot_U f(x) \quad (x \in V, \alpha \in F)$ - хомогеност.

Услови 1. и 2. су еквивалентни услову

$1'$. $f(\alpha \cdot_V x +_V \beta \cdot_V y) = \alpha \cdot_U f(x) +_U \beta \cdot_U f(y)$ $(x, y \in V, \alpha, \beta \in F)$ - линеарност

Дефиниција 3.7. Линеарно пресликавање $f : V \to V$ векторског простора V у самог себе назива се ендоморфизам или линеарни оператор векторског простора V.

Дефиниција 3.8. Нека је $f : V \to U$ линеарно пресликавање векторских простора.

(1) f је мономорфизам ако је „1-1”;

(2) f је епиморфизам ако је „на”;

(3) f је изоморфизам ако је бијекција.

Дефиниција 3.9. Векторски простори U и V над пољем F су изоморфни, у ознаци$U \cong V$, ако постоји бар један изоморфизам $f : U \to V$.

Лема 3.1. Ако је $f : V \to U$ линеарно пресликавање векторских простора, онда је

1. $f(0_V) = 0_U$,
2. $f(-_V x) = -_U f(x), \quad x \in V$.

Доказ. Заиста, важи да је

1. $f(0_V) = f(0_F \cdot_V x) = 0_F \cdot_U f(x) = 0_U$;
2. $f(-_V x) = f((-1)_F \cdot_V x) = (-1)_F \cdot_U f(x) = -_U(1_F \cdot f(x)) = -_U f(x)$. $\square$

ПРИМЕР 3.8.

1. $f : V \to V,\ f(x) = x$, тј. $f = i_V$ -идентично пресликавање је изоморфизам.
2. $f : V \to V,\ f(x) \overset{\text{def}}{=} 0$, тј. $f = 0$ - нула функција је ендоморфизам простора V, јер је $f(\alpha \cdot x + \beta \cdot y) = 0 = 0 + 0 = \alpha \cdot 0 + \beta \cdot 0 = \alpha \cdot f(x) + \beta \cdot f(y)$.
3. $f : \mathbb{R}^3 \to \mathbb{R}^2,\ f(x, y, z) = (2x + y, x - 2y + z)$ је линеарно пресликавање $\mathbb{R}^3$ у $\mathbb{R}^2$ јер
$$\begin{aligned} &f((x,y,z) + (x',y',z')) = f(x + x', y + y', z + z') = \\ &= (2(x + x') + (y + y'), (x + x') - 2(y + y') + (z + z')) \\ &= ((2x + y) + (2x' + y'), (x - 2y + z) + (x' - 2y' + z')) \\ &= (2x + y, x - 2y + z) + (2x' + y', x' - 2y' + z') \\ &= f(x,y,z) + f(x',y',z') \end{aligned}$$
и
$$\begin{aligned} f(\alpha(x,y,z)) &= f(\alpha x, \alpha y, \alpha z) = (2\alpha x + \alpha y, \alpha x - 2\alpha y + \alpha z) \\ &= (\alpha(2x + y), \alpha(x - 2y + z)) \\ &= \alpha(2x + y, x - 2y + z) \\ &= \alpha f(x,y,z). \end{aligned}$$
4. $D : \mathbb{R}_n[x] \to \mathbb{R}_{n-1}[x],\ D(f) = f'$ је линеарно пресликавање $\mathbb{R}_n[x]$ у $\mathbb{R}_{n-1}[x]$ јер је
$$D(\alpha \cdot f + \beta \cdot g) = (\alpha \cdot f + \beta \cdot g)' = \alpha \cdot f' + \beta \cdot g' = \alpha \cdot D(f) + \beta \cdot D(g).$$
5. $p_i : \mathbb{R}^n \to \mathbb{R},\ p_i(x_1, \ldots, x_n) = x_i$ -i-та пројекција је линеарно пресликавање $\mathbb{R}^n$ у $\mathbb{R}$.
6. $f : \mathbb{R}^2 \to \mathbb{R}^2,\ f(x, y) = (x \cos\alpha - y \sin\alpha, x \sin\alpha + y \cos\alpha), 0 \le \alpha < 2\pi$ (ротација равни $\mathbb{R}^2$ око (0,0) за угао α) је линеарно пресликавање.
7. $f : \mathbb{R}^2 \to \mathbb{R}^2,\ f(x, y) = (x + 1, x + y)$ није линеарно, јер $f(0, 0) = (1, 0) \neq (0, 0)$.

3.4 Линеарна независност вектора

Нека је $(V, +, \cdot, F)$ векторски простор.

ДЕФИНИЦИЈА 3.10. Вектор $x \in V$ је линеарна комбинација вектора $x_1, \ldots, x_n \in V$ ако постоје скалари $\alpha_1, \ldots, \alpha_n \in F$ такви да је
$$x = \alpha_1 \cdot x_1 + \cdots + \alpha_n \cdot x_n.$$

ПРИМЕР 3.9. Вектор $(1, 2, -3) \in \mathbb{R}^3$ је линеарна комбинација вектора $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$ јер је
$$\begin{aligned} (1, 2, -3) &= (1, 0, 0) + (0, 2, 0) + (0, 0, -3) \\ &= 1 \cdot (1, 0, 0) + 2 \cdot (0, 1, 0) - 3 \cdot (0, 0, 1). \end{aligned}$$

ПРИМЕР 3.10. Покажимо да вектор $(1, 2, 3)$ није линеарна комбинација следећих вектора $(1, 1, 1), (1, 1, 0), (1, 1, 2)$.

Потражимо $\alpha, \beta, \gamma \in \mathbb{R}$ такве да је
$$\begin{aligned} & (1,2,3) = \alpha(1,1,1) + \beta(1,1,0) + \gamma(1,1,2) \\ \Leftrightarrow\ & (1,2,3) = (\alpha,\alpha,\alpha) + (\beta,\beta,0) + (\gamma,\gamma,2\gamma) \\ \Leftrightarrow\ & (1,2,3) = (\alpha+\beta+\gamma, \alpha+\beta+\gamma, \alpha+2\gamma) \\ \Leftrightarrow\ & \left\{ \begin{array}{rcl} 1 &=& \alpha+\beta+\gamma \\ 2 &=& \alpha+\beta+\gamma \\ 3 &=& \alpha+2\gamma. \end{array} \right. \end{aligned}$$

Овај систем једначина нема решење (1=2), па $(1, 2, 3)$ није линеарна комбинација вектора $(1, 1, 1), (1, 1, 0), (1, 1, 2)$.

Пример 3.11. Да ли је полином $p = 2 - 3x + x^2 \in \mathbb{Q}[x]$ линеарна комбинација полинома $p_1 = 2 - x, p_2 = x + 2x^2$ и $p_3 = 3 - 2x + 3x^2$?

Испитајмо да ли постоје скалари $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}$ такви да је

$$p = \alpha_1 p_1 + \alpha_2 p_2 + \alpha_3 p_3,$$

тј.

$$2 - 3x + x^2 = \alpha_1(2 - x) + \alpha_2(x + 2x^2) + \alpha_3(3 - 2x + 3x^2),$$

што је еквивалентно систему линеарних једначина

$$\begin{array}{rcl} 2 & = & 2\alpha_1 + 3\alpha_3 \\ -3 & = & -\alpha_1 + \alpha_2 - 2\alpha_3 \\ 1 & = & 2\alpha_2 + 3\alpha_3 \end{array} .$$

Овај систем једначина има јединствено решење

$$\alpha_1 = -\frac{7}{8},\ \alpha_2 = -\frac{11}{8},\ \alpha_3 = \frac{5}{4},$$

па је

$$p = -\frac{7}{8}p_1 - \frac{11}{8}p_2 + \frac{5}{4}p_3.$$

Дакле, p је линеарна комбинација вектора p_1, p_2 и p_3.

Дефиниција 3.11.

1. Скуп вектора $\{x_1, \dots, x_n\}$ је линеарно зависан ако постоје скалари $\alpha_1, \dots, \alpha_n$ од којих је бар један различит од нуле, такви да је $\alpha_1 x_1 + \cdots + \alpha_n x_n = 0$, тј.

$$(\exists \alpha_1, \dots, \alpha_n \in F)\ (\alpha_1 x_1 + \cdots + \alpha_n x_n = 0 \wedge (\alpha_1, \dots, \alpha_n) \neq (0, \dots, 0)).$$

2. Скуп вектора $\{x_1, \dots, x_n\}$ је линеарно независан ако није линеарно зависан, тј.

$$(\forall \alpha_1, \dots, \alpha_n \in F)(\alpha_1 x_1 + \cdots + \alpha_n x_n = 0 \Rightarrow \alpha_1 = \cdots = \alpha_n = 0).$$

Дефиниција 3.12.

- Бесконачан скуп вектора $S \subseteq V$ је линеарно зависан ако је бар један његов коначан подскуп линеарно зависан.
- Бесконачан скуп вектора $S \subseteq V$ је линеарно независан ако је сваки његов коначан подскуп линеарно независан.

Теорема 3.7.

(1) Сваки надскуп линеарно зависног скупа вектора је линеарно зависан.

(2) Сваки подскуп линеарно независног скупа вектора је линеарно независан.

(3) Сваки скуп који садржи нула вектор је линеарно зависан.

Доказ. (1) и (2) следе непосредно из дефиниције.

(3) Скуп $\{0_V\}$ је линеарно зависан, јер постоји скалар $\alpha = 1$ такав да је

$$1 \cdot 0_V = 0_V \quad \text{и} \quad 1 \neq 0_F.$$

На основу (1) следи да је и сваки скуп који садржи 0_V линеарно зависан. □

Последица. Синглтон $\{x\}$ је линеарно зависан акко је $x = 0$.

Пример 3.12. Скуп вектора $\{(1, 0, 0), (1, 1, 0), (1, 1, 1)\}$ простора $\mathbb{R}^3$ је линеарно независан, јер

$$\alpha(1, 0, 0) + \beta(1, 1, 0) + \gamma(1, 1, 1) = 0 \Rightarrow \alpha = \beta = \gamma = 0.$$

Пример 3.13. Скуп вектора $\{f = x^2 + 3x + 1,\ g = 5x^2 + x,\ h = -3x^2 + 5x + 2\}$ простора $\mathbb{R}_2[x]$ је линеарно зависан, јер из

$$\alpha(x^2 + 3x + 1) + \beta(5x^2 + x) + \gamma(-3x^2 + 5x + 2) = 0$$

следи

$$(\alpha + 5\beta - 3\gamma)x^2 + (3\alpha + \beta + 5\gamma)x + (\alpha + 2\gamma) = 0$$

одакле добијамо систем једначина

$$\begin{array}{rcl} \alpha + 5\beta - 3\gamma &=& 0\\ 3\alpha + \beta + 5\gamma &=& 0\\ \alpha \ \ + 2\gamma &=& 0 \end{array}$$

који има и нетривијална решења, рецимо $\alpha = 2, \beta = -1, \gamma = -1$.

Пример 3.14. $\{1, x, x^2, x^3 \dots\}$ је линеарно независан скуп вектора простора $F[x]$.

Заиста, уочимо произвољан коначан подскуп

$$\{x^{m_1}, x^{m_2}, \dots, x^{m_k}\} \quad (m_1 < m_2 < \dots < m_k).$$

Из

$$\alpha_1 x^{m_1} + \alpha_2 x^{m_2} + \dots + \alpha_k x^{m_k} = 0$$

(где је 0 нула полином, тј. $0 = 0 \cdot 1 + 0 \cdot x + \dots + 0 \cdot x^{m_k}$) следи

$$\alpha_1 = \alpha_2 = \dots = \alpha_k = 0,$$

па је скуп вектора $\{x^{m_1}, \dots, x^{m_k}\}$ линеарно независан, а како је то произвољан коначан подскуп скупа $\{1, x, x^2, \dots\}$, следи да је и $\{1, x, x^2, \dots\}$ линеарно независан.

Пример 3.15. Скуп

$$\{f, g\} \text{ где } f, g \in \mathbb{R}^{\mathbb{R}}, \quad f(x) = e^x, \quad g(x) = e^x \sin x,$$

је линеарно независан.

Заиста,

$$\begin{array}{rl} & \alpha f + \beta g = 0, \text{ за } \alpha, \beta \in \mathbb{R}\\ \Rightarrow (\forall x \in \mathbb{R}) & \alpha \cdot f(x) + \beta \cdot g(x) = 0(x) \quad (0 : \mathbb{R} \to \mathbb{R},\ 0(x) = 0),\\ \Rightarrow (\forall x \in \mathbb{R}) & \alpha \cdot e^x + \beta \cdot e^x sinx = 0,\\ \overset{x=0}{\Rightarrow} & \alpha = 0\\ \Rightarrow & (\forall x \in \mathbb{R})\, \beta \cdot e^x sinx = 0\\ \overset{x=\frac{\pi}{2}}{\Rightarrow} & \beta \cdot e^{\frac{\pi}{2}} \cdot 1 = 0\\ \Rightarrow & \beta = 0 \end{array}$$

па је $\{f, g\}$ линеарно независан скуп вектора.

Често се за утврђивање линеарне зависности користи критеријум дат следећом теоремом.

Теорема 3.8. Скуп вектора $\{x_1, \dots, x_n\},\ n > 1$, је линеарно зависан акко се бар један од њих изражава као линеарна комбинација осталих.

Доказ. ($\rightarrow$) Нека је $\{x_1, \dots, x_n\}$ скуп линеарно зависних вектора. Тада постоје скалари $\alpha_1, \dots, \alpha_n$ од којих је бар један различит од нуле, такви да је

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = 0.$$

Нека је $\alpha_i \neq 0$. Тада постоји $\alpha_i^{-1} \in F$, па множењем претходне једнакости са α_i^{-1} добијамо

$$\alpha_i{}^{-1}\alpha_1 x_1 + \cdots + \alpha_i^{-1}\alpha_{i-1}x_{i-1} + \underbrace{\alpha_i\alpha_i^{-1}}_{=1} x_i + \alpha_i^{-1}\alpha_{i+1}x_{i+1} + \cdots + \alpha_i^{-1}\alpha_n \cdot x_n = 0,$$

одакле је

$$x_i = -(\alpha_1\alpha_i{}^{-1})x_1 - \cdots - (\alpha_{i-1}\alpha_i^{-1})x_{i-1} - (\alpha_{i+1}\alpha_i^{-1})x_{i+1} - \cdots - (\alpha_n\alpha_i{}^{-1}) \cdot x_n,$$

тј. x_i је линеарна комбинација осталих вектора.

($\leftarrow$) Нека је x_i линеарна комбинација преосталих вектора скупа $\{x_1, \dots, x_n\}$.

Тада постоје скалари $\beta_1, \dots, \beta_{i-1}, \beta_{i+1}, \dots, \beta_n$ такви да је

$$x_i = \beta_1 x_1 + \dots \beta_{i-1}x_{i-1} + \beta_{i+1}x_{i+1} + \cdots + \beta_n x_n,$$

па је

$$\left.\begin{array}{l} \beta_1 x_1 + \cdots + \beta_{i-1}x_{i-1} + \underbrace{(-1)}_{\neq 0} \cdot x_i + \beta_{i+1}x_{i+1} + \cdots + \beta_n x_n = 0 \quad \text{и} \\ (\beta_1, \dots, \beta_{i-1}, -1, \beta_{i+1}, \dots, \beta_n) \neq (0, \dots, 0) \end{array}\right. ,$$

што значи да је $\{x_1, \dots, x_n\}$ линеарно зависан скуп вектора. □

Напомена. Ако је скуп вектора линеарно зависан, не следи да се сваки елемент тог скупа може изразити као линеарна комбинација осталих вектора.

Пример 3.16. Скуп вектора $\{1 - x, x, x^2, 1\}$ простора полинома $\mathbb{R}_2[x]$ је линеарно зависан, али се вектор x^2 не може изразити као линеарна комбинација осталих вектора овог скупа.

3.5 Линеарни омотач скупа вектора

Нека је $(V, +, \cdot, F)$ векторски простор над пољем F.

Дефиниција 3.13. Нека је $\emptyset \neq S \subseteq V$. Скуп свих коначних линеарних комбинација вектора скупа S се зове линеарни омотач (покривач) или линеал над скупом S и означава са $\mathcal{L}(S)$, тј.

$$\mathcal{L}(S) \overset{\text{def}}{=} \big\{\alpha_1 \cdot x_1 + \cdots + \alpha_n \cdot x_n \mid n \in \mathbb{N}, x_1, \dots, x_n \in S, \alpha_1, \dots, \alpha_n \in F\big\}.$$

Теорема 3.9. Ако је $\emptyset \neq S \subseteq V$, тада је $\mathcal{L}(S)$ најмањи потпростор векторског простора V који садржи скуп S.

Доказ. Доказ изводимо по деловима.

- $x \in S \Rightarrow x = 1 \cdot x \in \mathcal{L}(S)$, па је $S \subseteq \mathcal{L}(S)$.
- Докажимо да је $\mathcal{L}(S) \preceq V$.

$$\begin{array}{ll} & x, y \in \mathcal{L}(S),\ \lambda, \mu \in F \\ \Rightarrow & \begin{array}{l} x = \alpha_1 x_1 + \cdots + \alpha_n x_n,\ x_i \in S, \alpha_i \in F,\ i = 1, \dots, n \\ y = \beta_1 y_1 + \cdots + \beta_m y_m,\ y_j \in S, \beta_j \in F,\ j = 1, \dots, m \end{array} \\ \Rightarrow & \lambda x + \mu y = \lambda(\alpha_1 x_1 + \cdots + \alpha_n x_n) + \mu(\beta_1 y_1 + \cdots + \beta_m y_m) = \\ & \qquad = (\lambda\alpha_1)x_1 + \cdots + (\lambda\alpha_n)x_n + (\mu\beta_1)y_1 + \cdots + (\mu\beta_m)y_m \in \mathcal{L}(S). \end{array}$$

- Покажимо да је $\mathcal{L}(S)$ најмањи од свих потпростора који садрже S.

  Нека је $U \preceq V$ такав да $S \subseteq U$. Тада

  $$\begin{aligned} & x \in \mathcal{L}(S) \\ \Rightarrow \quad & x = \alpha_1 x_1 + \cdots + \alpha_n x_n,\ x_i \in S, \alpha_i \in F, i = 1, \ldots, n \\ \Rightarrow \quad & x \in U (\text{јер је } U \preceq V, \text{ па је затворен за линеарне комбинације}). \end{aligned}$$

  Дакле, $\mathcal{L}(S) \subseteq U$. □

Пример 3.17. (1) Ако је $V = \mathbb{R}^2,\ S = \{(1,2)\}$, тада $\mathcal{L}(S) = \{\alpha(1,2) \mid \alpha \in \mathbb{R}\} = \{(\alpha, 2\alpha) \mid \alpha \in \mathbb{R}\}$ је права у $\mathbb{R}^2$ кроз тачке (1,2) и (0,0).

(2) Ако је $V = \mathbb{R}^3,\ S = \{(1,2,3)\}$ тада $\mathcal{L}(S) = \{(x, 2x, 3x) \mid x \in \mathbb{R}\}$ је права у простору $\mathbb{R}^3$ одређена тачкама $(0,0,0)$ и $(1,2,3)$.

(3) Ако је $V = \mathbb{R}^3$ и $S = \{(1,0,0), (0,1,0)\}$ тада је $\mathcal{L}(S)$ раван xOy.

Теорема 3.10. (1) $\mathcal{L}(S) = S$ акко $S \preceq V$;

(2) $\mathcal{L}(\mathcal{L}(S)) = \mathcal{L}(S)$, тј. $\mathcal{L}^2 = \mathcal{L}$ (идемпотентност);

(3) $S \subseteq T \Rightarrow \mathcal{L}(S) \subseteq \mathcal{L}(T)$;

(4) $\mathcal{L}(S \cup T) = \mathcal{L}(S) + \mathcal{L}(T)$;

(5) $S \subseteq T \subseteq \mathcal{L}(S) \Rightarrow\ \mathcal{L}(S) = \mathcal{L}(T)$;

(6) $x \in \mathcal{L}(S) \Rightarrow\ \mathcal{L}(S \cup \{x\}) = \mathcal{L}(S)$.

Доказ.

(1) Следи непосредно из Теореме 3.9.

(2) $\mathcal{L}(S) \preceq V$ из Теореме 3.9. $\Rightarrow \mathcal{L}(\mathcal{L}(S)) = \mathcal{L}(S)$ из (1).

(3) Следи непосредно из дефиниције линеарног омотача скупа вектора.

(4) $\mathcal{L}(S \cup T) = \mathcal{L}(S) + \mathcal{L}(T)$?

$$\begin{aligned} x \in\ & \mathcal{L}(S \cup T) \Leftrightarrow x = \alpha_1 x_1 + \cdots + \alpha_n x_n, \quad x_i \in S \cup T, \alpha_i \in F \\ & \Leftrightarrow x = \underbrace{\beta_1 y_1 + \cdots + \beta_k y_k}_{=y} + \underbrace{\gamma_1 z_1 + \cdots + \gamma_l z_l}_{=z}, y_i \in S, z_i \in T,\ k + l = n \\ & \Leftrightarrow x = y + z, \quad y \in \mathcal{L}(S), z \in \mathcal{L}(T) \\ & \Leftrightarrow x \in \mathcal{L}(S) + \mathcal{L}(T). \end{aligned}$$

(5) $S \subseteq T \subseteq \mathcal{L}(S)\ \Rightarrow\ \mathcal{L}(S) = \mathcal{L}(T)$?

$$\left.\begin{array}{r} S \subseteq T \overset{(3)}{\Rightarrow} \mathcal{L}(S) \subseteq \mathcal{L}(T) \\ T \subseteq \mathcal{L}(S) \overset{(3)}{\Rightarrow} \mathcal{L}(T) \subseteq \mathcal{L}(\mathcal{L}(S)) \overset{(2)}{=} \mathcal{L}(S) \end{array}\right\} \Rightarrow \mathcal{L}(S) = \mathcal{L}(T).$$

(6) $x \in \mathcal{L}(S) \Rightarrow\ \mathcal{L}(S \cup \{x\}) = \mathcal{L}(S)$?

$$\begin{aligned} x \in \mathcal{L}(S) \quad & \Rightarrow \quad S \subseteq S \cup \{x\} \subseteq \mathcal{L}(S) \\ & \Rightarrow \quad \mathcal{L}(S) = \mathcal{L}(S \cup \{x\}) \quad (\text{из } (5)). \end{aligned}$$

□

Дефиниција 3.14. Ако је $\mathcal{L}(S) = V$ кажемо да скуп S генерише простор V, а скуп S се зове генераторни скуп (генератриса) простора V.

Пример 3.18. (1) $\mathbb{R}^3 = \mathcal{L}(\{(1,0,0),(0,1,0),(0,0,1)\})$, јер за произвољан вектор $(x,y,z) \in \mathbb{R}^3$ важи $(x,y,z) = x\cdot(1,0,0) + y\cdot(0,1,0) + z\cdot(0,0,1)$.

(2) $\mathbb{R}_3[x] = \mathcal{L}\{1, x, x^2, x^3\}$, јер за свако $f \in \mathbb{R}_3[x]$ важи

$f = a_0\cdot 1 + a_1\cdot x + a_2\cdot x^2 + a_3\cdot x^3$ $(a_0, a_1, a_2, a_3 \in \mathbb{R})$.

Приметимо да и сваки надскуп скупа $\{1, x, x^2, x^3\}$ генерише простор $\mathbb{R}_3[x]$, као и да ниједан његов прави подскуп не генерише простор $\mathbb{R}_3[x]$.

(3) $\mathbb{R}[x] = \mathcal{L}\{1, x, x^2, \ldots\}$.

Пример 3.19. Да ли скуп полинома $\{f = x^2 + x,\ g = x^2 - 1,\ h = x + 1\}$ генерише простор $\mathbb{R}_2[x]$?

Испитајмо да ли за произвољан полином $p = ax^2 + bx + c \in \mathbb{R}_2[x]$ постоје скалари $\alpha, \beta, \gamma \in \mathbb{R}$ такви да је

$$\begin{array}{cl} & p = \alpha f + \beta g + \gamma h \\ \Leftrightarrow & ax^2 + bx + c = \alpha(x^2 + x) + \beta(x^2 - 1) + \gamma(x + 1) \end{array}$$

$$\Leftrightarrow \begin{array}{rcl} \alpha+\beta &=& a \\ \alpha+\gamma &=& b \\ -\beta+\gamma &=& c \end{array} \Leftrightarrow \begin{array}{rcl} \alpha+\beta &=& a \\ -\beta+\gamma &=& b-a \\ -\beta+\gamma &=& c \end{array} \Leftrightarrow \begin{array}{rcl} \alpha+\beta &=& a \\ -\beta+\gamma &=& b-a \\ 0 &=& c-b+a. \end{array}$$

Добијени систем једначина је сагласан акко $c - b + a = 0$, па скуп $\{f, g, h\}$ не генерише цео простор $\mathbb{R}_2[x]$, тј. $\mathcal{L}\{f, g, h\} \subsetneqq \mathbb{R}_2[x]$. Такође

$$\begin{array}{rcl} \mathcal{L}\{f,g,h\} &=& \{ax^2 + bx + c \in \mathbb{R}_2[x] \mid c - b + a = 0\} \\ &=& \{ax^2 + bx + c \in \mathbb{R}_2[x] \mid c = b - a\} \\ &=& \{ax^2 + bx + (b - a) \mid a, b \in \mathbb{R}\} \\ &=& \{a(x^2 - 1) + b(x + 1) \mid a, b \in \mathbb{R}\} = \mathcal{L}\{g, h\}. \end{array}$$

До истог закључка се могло доћи и на следећи начин:

$f = 1\cdot g + 1\cdot h \in \mathcal{L}\{g, h\} \ \Rightarrow \mathcal{L}\{f, g, h\} = \mathcal{L}\{g, h\}$ (особина (6)).

3.6 База векторског простора

Нека је $(V, +, \cdot, F)$ векторски простор и $\emptyset \neq B \subseteq V$.

Дефиниција 3.15. Скуп вектора B је база простора V ако је линеарно независан и генерише простор V, тј.

(B_1) $\mathcal{L}(B) = V$;

(B_2) B је линеарно независан скуп вектора.

Пример 3.20. 1. $(F, +, \cdot, F)$, једна база је $B = \{1\}$.

(B_1) $F = \mathcal{L}\{1\}$ јер $(\forall x \in F)$ $\underbrace{x}_{\text{вектор}} = \underbrace{x}_{\text{скалар}} \cdot \underbrace{1}_{\text{вектор}}$;

(B_2) $\{1\}$ је линеарно независан, јер $\alpha\cdot 1 = 0 \Rightarrow \alpha = 0$.

2. $(\mathbb{C}, +, \cdot, \mathbb{R})$, једна база је $B = \{1, i\}$.

(B_1) $(\forall x \in \mathbb{C})(\exists \alpha, \beta \in \mathbb{R})\ x = \alpha\cdot 1 + \beta\cdot i \Rightarrow \mathbb{C} = \mathcal{L}\{1, i\}$;

(B_2) $\{1, i\}$ је линеарно независан, јер $\alpha\cdot 1 + \beta\cdot i = 0 \Rightarrow \alpha = \beta = 0$.

3. $(F^n, +, \cdot, F)$, база $B = \{e_1 = (1, 0, \dots, 0), e_2 = (0, 1, 0, \dots, 0), \dots, e_n = (0, \dots, 0, 1)\}$ се зове стандардна база простора F^n.

   (B_1) $(x_1, x_2, \dots, x_n) = x_1 \cdot (1, 0, \dots, 0) + \cdots + x_n \cdot (0, \dots, 0, 1)$,
   сваки $(x_1, \dots, x_n) \in F^n$ је линеарна комбинација вектора из B.

   $$(B_2)\quad \begin{array}{ll} & \alpha_1 \cdot (1, 0, \dots, 0) + \cdots + \alpha_n \cdot (0, \dots, 0, 1) = (0, \dots, 0) \\ \Rightarrow & (\alpha_1, 0, \dots, 0) + \cdots + (0, \dots, 0, \alpha_n) = (0, \dots, 0) \\ \Rightarrow & (\alpha_1, \alpha_2, \dots, \alpha_n) = (0, \dots, 0) \\ \Rightarrow & B \text{ је линеарно независан скуп.} \end{array}$$

4. $(F^{\mathbb{N}}, +, \cdot, F)$, једна база је $B = \{(1, 0, 0, \dots), (0, 1, 0, \dots), \dots\}$.

5. $(F_n[x], +, \cdot, F)$, база $B = \{1, x, x^2, \dots, x^n\}$ се зове стандардна база простора $F_n[x]$.

6. $(F^S, +, \cdot, F)$, једна база је $B = \{\chi_s \mid s \in S\}$, где

   $$\chi_s : S \to F,\ \chi_s(t) \overset{\text{def}}{=} \begin{cases} 1, & t = s \\ 0, & t \neq s \end{cases}.$$

Теорема 3.11. Непразан скуп $B \subseteq V$ је база векторског простора V акко је скуп B минимални скуп који генерише V.

Доказ. $(\to)$ Нека за B важе аксиоме (B_1) и (B_2).

- Из (B_1) следи да B генерише V.
- Покажимо да је B минимални скуп са том особином, тј. да ниједан његов прави подскуп не генерише V.

  Претпоставимо супротно, тј. нека је $\emptyset \neq B' \subsetneqq B$ такав да је $\mathcal{L}(B') = V$.

  $(\exists x) x \in B \setminus B'$ (јер $B' \subsetneqq B$)
  $\Rightarrow x \in \mathcal{L}(B')$ (јер B' генерише цео простор V)
  $\Rightarrow B' \cup \{x\}$ је линеарно зависан
  $\Rightarrow B$ је линеарно зависан(као надскуп линеарно зависног скупа $B' \cup \{x\}$)
  Контрадикција са (B_2).

$(\leftarrow)$ Нека је B минималан скуп вектора који генерише простор V.

(B_1) $\mathcal{L}(B) = V$ (по претпоставци);

(B_2) Докажимо да је B линеарно независан скуп вектора.

Претпоставимо супротно, тј. да је B линеарно зависан скуп. Тада постоји $x \in B$ који је линеарна комбинација осталих вектора из B, тј.

$$x \in \mathcal{L}(B'), \quad \text{где је } B' = B \setminus \{x\}.$$

Тада важи

$$\mathcal{L}(B') \overset{(6)}{=} \mathcal{L}(B' \cup \{x\}) = \mathcal{L}(B) = V$$

што је супротно претпоставци да је B минимални скуп који генерише V. Дакле, B је линеарно независан скуп вектора. □

Теорема 3.12. Непразан скуп $B \subseteq V$ је база векторског простора V акко је максималан линеарно независан скуп.

Доказ. Из (B_2) следи да је B линеарно независан. Покажимо да је B максималан такав скуп, тј. да је сваки његов прави надскуп линеарно зависан.

Нека је $B \subsetneqq B'$. Тада

$$\begin{array}{ll} & (\exists x) x \in B' \setminus B \\ \Rightarrow & x \in \mathcal{L}(B) \quad (\text{ јер } \mathcal{L}(B) = V) \\ \Rightarrow & B \cup \{x\} \text{ је линеарно зависан} \\ \Rightarrow & B' \text{ је линеарно зависан} \quad (\text{из } B \cup \{x\} \subseteq B') \end{array}$$

Дакле, B је максималан линеарно независан скуп вектора.

$(\leftarrow)$ Нека је B максималан линеарно независан скуп.

(B_2) Важи по претпоставци.

(B_1) Докажимо да B генерише цео простор V. Претпоставимо супротно, тј.

$$\begin{array}{ll} & \mathcal{L}(B) \subsetneqq V \\ \Rightarrow & (\exists x) x \in V \setminus \mathcal{L}(B) \\ \Rightarrow & B' = B \cup \{x\} \text{ је линеарно независан} \end{array}$$

Контрадикција са претпоставком да је B максималан линеарно независан скуп.

Дакле, $\mathcal{L}(B) = V$. □

Теорема 3.13. (Карактеризација базе.) Скуп $B = \{x_1, \dots, x_n\}$ је база простора V акко сваки $x \in V$ има јединствену репрезентацију $x = \alpha_1 x_1 + \cdots + \alpha_n x_n$, где $\alpha_1, \dots, \alpha_n \in F$, тј.

$$(\forall x \in V)(\exists_1 (\alpha_1, \dots, \alpha_n) \in F^n)\ x = \alpha_1 x_1 + \cdots + \alpha_n x_n. \qquad (*)$$

Доказ. $(\rightarrow)$ Егзистенција репрезентације: из (B_1) следи

$$\mathcal{L}(B) = V \Rightarrow (\forall x \in V)(\exists (\alpha_1, \dots, \alpha_n) \in F^n)\ x = \alpha_1 x_1 + \cdots + \alpha_n x_n.$$

Јединственост:

$$\begin{array}{rl} x = \alpha_1 x_1 + & \cdots + \alpha_n x_n,\ x = \beta_1 x_1 + \cdots + \beta_n x_n \quad (\alpha_i, \beta_i \in F) \\ \Rightarrow & \alpha_1 x_1 + \cdots + \alpha_n x_n = \beta_1 x_1 + \cdots + \beta_n x_n \\ \Rightarrow & (\alpha_1 - \beta_1) x_1 + \cdots + (\alpha_n - \beta_n) x_n = 0 \\ \Rightarrow & \alpha_1 - \beta_1 = 0, \dots, \alpha_n - \beta_n = 0 \text{ (следи из } (B_2)) \\ \Rightarrow & \alpha_1 = \beta_1, \dots, \alpha_n = \beta_n \\ \Rightarrow & (\alpha_1, \dots, \alpha_n) = (\beta_1, \dots, \beta_n). \end{array}$$

$(\leftarrow)$

(B_1) Из егзистенције репрезентације $(*)$ следи $V \subseteq \mathcal{L}(B)$. Обрнута инклузија свакако важи, па је $\mathcal{L}(B) = V$.

(B_2) Нека је

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = 0, \quad \alpha_1, \dots, \alpha_n \in F.$$

Свакако је

$$0_F \cdot x_1 + \cdots + 0_F \cdot x_n = 0.$$

Из јединствености репрезентације нула вектора преко вектора из B следи

$$\alpha_1 = 0, \dots, \alpha_n = 0.$$

Дакле, B је линеарно независан скуп вектора. □

ДЕФИНИЦИЈА 3.16. Скаларе $\alpha_1, \dots, \alpha_n$ из репрезентације $x = \alpha_1 x_1 + \dots + \alpha_n x_n$ зовемо координатама вектора x у бази $B = \{x_1, \dots, x_n\}$.

ПРИМЕР 3.21. Како је $(1,2,3) = 1 \cdot (1,0,0) + 2 \cdot (0,1,0) + 3 \cdot (0,0,1)$, то вектор $(1,2,3)$ у стандардној бази $e = \{(1,0,0),(0,1,0),(0,0,1)\}$ има координате $(1,2,3)$.

Координате вектора $(1,2,3)$ у бази $B = \{(1,0,0),(1,1,0),(1,1,1)\}$ су $(-1,-1,3)$ јер је $(1,2,3) = -1 \cdot (1,0,0) - 1 \cdot (1,1,0) + 3 \cdot (1,1,1)$.

ТЕОРЕМА 3.14. Нека је $B = \{x_1, \dots, x_n\}$ база простора V. Пресликавање

$$k_B : V \to F^n, \quad k_B(x) \overset{\text{деф}}{=} (\alpha_1, \dots, \alpha_n), \quad \text{за } x = \alpha_1 x_1 + \dots + \alpha_n x_n,$$

је изоморфизам простора V на простор F^n.

Доказ.

- k_B је добро дефинисано и "1-1": Према Теореми 3.13. произвољни вектори $x, y \in V$ имају јединствене репрезентације $x = \alpha_1 x_1 + \dots + \alpha_n x_n$, $\quad y = \beta_1 x_1 + \dots + \beta_n x_n$. Тада $x = y \Leftrightarrow (\alpha_1, \dots, \alpha_n) = (\beta_1, \dots, \beta_n) \Leftrightarrow k_B(x) = k_B(y)$.
- k_B је "на" јер $(\forall(\alpha_1, \dots, \alpha_n) \in F^n)(\exists x = \alpha_1 x_1 + \dots + \alpha_n x_n \in V) k_B(x) = (\alpha_1, \dots, \alpha_n)$.
- k_B је линеарно:

$$\begin{aligned}(1)\ k_B(x+\ \ y) &= k_B((\alpha_1 x_1 + \dots + \alpha_n x_n) + (\beta_1 x_1 + \dots + \beta_n x_n)) \\ &= k_B((\alpha_1 + \beta_1)x_1 + \dots + (\alpha_n + \beta_n)x_n) = (\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n) \\ &= (\alpha_1, \dots, \alpha_n) + (\beta_1, \dots, \beta_n) = k_B(x) + k_B(y)\end{aligned}$$

$$\begin{aligned}(2)\quad k_B(\alpha x) &= k_B(\alpha(\alpha_1 x_1 + \dots + \alpha_n x_n) = k_B((\alpha\alpha_1)x_1 + \dots + (\alpha\alpha_n)x_n) \\ &= (\alpha\alpha_1, \dots, \alpha\alpha_n) = \alpha(\alpha_1, \dots, \alpha_n) = \alpha k_B(x)\ \Box\end{aligned}$$

Упоредимо број линеарно независних вектора са бројем генераторних вектора неког простора V.

ТЕОРЕМА 3.15. Ако је $S = \{x_1, \dots, x_n\}$ линеарно независан скуп вектора и $G = \{y_1, \dots, y_m\}$ генераторни скуп вектора векторског простора V, онда је $n \leq m$.

Доказ.

$$\begin{gathered} x_1 \in V,\ \mathcal{L}(G) = V \Rightarrow G_1 = \{x_1, y_1, \dots, y_m\} \text{ је линеарно зависан} \\ \Rightarrow (\exists \beta, \alpha_1, \dots, \alpha_m \in F)(\beta x_1 + \alpha_1 y_1 + \dots + \alpha_m y_m = 0 \land (\beta, \alpha_1, \dots, \alpha_m) \neq (0, \dots, 0)) \end{gathered}$$

- $\alpha_1 = \dots = \alpha_m = 0 \Rightarrow \beta x_1 = 0 \Rightarrow \beta = 0 (x_1 \neq 0$, јер је S линеарно независан), па је G_1 линеарно независан. Контрадикција.
- Бар један од скалара $\alpha_1, \dots, \alpha_m$ је различит од нуле. Уочимо y_s, $s \in \{1, \dots, m\}$ такав да је y_s линеарна комбинација претходних у низу.

Тада је

$$\mathcal{L}(G_1 \setminus \{y_s\}) = \mathcal{L}(G_1) = V.$$

Избацимо y_s из G_1 и поновимо поступак.

$$G_2 = \{x_1, x_2, y_1, \dots, \widehat{y_s}, \dots, y_m\}$$

(где $\widehat{y_s}$ означава да је елемент y_s избачен) је линеарно зависан. Уочимо y_t који је линеарна комбинација претходних и избацимо га.

Тада $G_2 \setminus \{y_t\}$ генерише V, па је

$$G_3 = \{x_1, x_2, x_3, y_1, \dots, \widehat{y_s}, \dots, \widehat{y_t}, \dots, y_m\}$$

линеарно зависан.

$$\vdots$$

У $n-$том кораку добијамо

$$G_n = \{x_1, x_2, \dots, x_n, \quad \underbrace{y_k, \dots}_{\text{бар једно } y_k} \quad \}$$

који је линеарно зависан (по конструкцији), па садржи бар један y_k (ако не садржи ниједно y_k онда $G_n = S$, па би био линеарно независан). Како смо у сваком од претходних $n-1$ кораку убацили по један x_i и избацили по један елемент скупа G, следи да је $n \leq m$. □

Последица. Ако векторски простор V има коначну базу, онда свака његова база има исти број вектора.

Доказ. Нека простор V има коначну базу и нека су

$B_1 = \{x_1, \dots, x_n\}$ и $B_2 = \{y_1, \dots, y_m\}$ две базе простора V. Тада, према Теореми 3.15.

$$\left.\begin{array}{l}\left.\begin{array}{ll} B_1 & \text{је линеарно независан} \\ B_2 & \text{генерише } V \end{array}\right\} \Rightarrow \quad n \leq m \\ \left.\begin{array}{ll} B_2 & \text{је линеарно независан} \\ B_1 & \text{генерише } V \end{array}\right\} \Rightarrow \quad m \leq n \end{array}\right\} \Rightarrow n = m.$$

Теорема 3.16. Сваки векторски простор $V \neq \{0\}$ има базу.

3.7 Димензија векторског простора

Дефиниција 3.17. Димензија векторског простора V се обележава са $\dim V$ и дефинише на следећи начин:

(1) Ако је $V = \{0\}$, онда $\dim V = 0$.

(2) Ако простор V има базу од n елемената, онда $\dim V = n$.

(3) Ако простор нема коначну базу, онда $\dim V = \infty$.

Ако је $\dim V \in \mathbb{N} \cup \{0\}$ онда је V коначнодимензионалан векторски простор.

Пример 3.22. 1. $(F, +, \cdot, F)$ има базу $B = \{1\}$, па је $\dim F$=1.

2. $\mathbb{C}_{\mathbb{R}} = (\mathbb{C}, +, \cdot, \mathbb{R})$ има базу $B = \{1, i\}$, па је $\dim \mathbb{C}_{\mathbb{R}} = 2$.

3. $(F^n, +, \cdot, F)$ има базу $B = \{(1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, \dots, 0, 1)\}$, па је $\dim F^n = n$.

4. $(F_n[x], +, \cdot, F)$ има базу $B = \{1, x, \dots, x^n\}$, па је $\dim F_n[x] = n + 1$.

5. $(F[x], +, \cdot, F)$ нема коначну базу, па је $\dim F[x] = \infty$.

6. $(F^{\mathbb{N}}, +, \cdot, F)$ нема коначну базу, па је $\mathrm{dim} F^{\mathbb{N}} = \infty$.

Пример 3.23. Дати су скупови вектора

$T_1 = \{(1,2,3),(2,4,5)\}$,
$T_2 = \{(1,0,0),(0,1,0),(0,1,1),(1,2,3)\}$,
$T_3 = \{(1,1,1),(2,0,2),(0,1,0)\}$,
$T_4 = \{(2,0,0),(2,2,0),(2,2,2)\}$ простора $\mathbb{R}^3$.

Који од датих скупова су

(i) линеарно независни,
(ii) генераторни за $\mathbb{R}^3$,
(iii) база за $\mathbb{R}^3$?

Пример 3.24. За сваки од датих потпростора простора $\mathbb{R}^3$ одредити по једну базу и димензију:

- $U_1 = \{(x,y,z) \in \mathbb{R}^3 \mid x = y = z\}$.
- $U_2 = \{(x,y,z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 0\}$.
- $U_3 = \{(x,y,z) \in \mathbb{R}^3 \mid x^2 + z^2 = 0\}$.
- $U_4 = \{(x,y,z) \in \mathbb{R}^3 \mid x = y + z\}$.

Теорема 3.17. Сваки линеарно независан скуп вектора коначно димензионог простора V је или база или се може проширити до базе тог простора.

Доказ. Нека је $\mathrm{dim} V = n$ и нека је $S = \{x_1, \ldots, x_m\}$ линеарно независан скуп.

Тада, по Теореми 3.15. $m \leq n$.

- $m = n$ следи да је S база за V (по Теореми 3.12.)
- $m < n \Rightarrow \mathcal{L}(S) \neq V \Rightarrow \exists x_{m+1} \in V \setminus \mathcal{L}(S)$
  $\Rightarrow S_1 = \{x_1, \ldots, x_m, x_{m+1}\}$ је линеарно независан.
  - $m + 1 = n \ \Rightarrow S_1$ је база за V
  - $m + 1 \neq n$ настављамо поступак

  $\vdots$

  $S_k = \{x_1, \ldots, x_m, x_{m+1}, \ldots, x_{m+k}\}$, при чему $m + k = n$, је линеарно независан

$\Rightarrow \mathcal{L}(S_k) = V$ (у супротном би постојало $n+1$ линеарно независних вектора, контрадикција са $\mathrm{dim} V = n$) $\Rightarrow S_k$ је база за V. □

Пример 3.25. Уколико је могуће, проширити до базе следеће скупове вектора:

(i) $\{1, x+2\}$ у простору $\mathbb{R}_2[x]$
(ii) $\{(1,1),(2,2)\}$ у простору $\mathbb{R}^2$.

Теорема 3.18. Нека је $(V, +, \cdot, F)$ коначнодимензиони векторски простор и нека су U, U_1, U_2 његови потпростори. Тада

(1) $\dim U \leq \dim V$,

(2) $\dim U = \dim V \;\Rightarrow\; U = V$,

(3) $\dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2)$ - Грасманова формула.

Посебно, ако $V = U_1 \oplus U_2$, онда $\dim V = \dim U_1 + \dim U_2$.

Доказ.

(1) Потростор U има коначну базу, иначе би у U, а тиме и у V, постојао бесконачан линеарно независан скуп вектора, што би противречило претпоставци да је V коначнодимензионалан.

Нека је $B_U = \{x_1, \ldots, x_n\}$ база простора U.

$\Rightarrow B_U$ је линеарно независан скуп вектора

$\Rightarrow B_U$ се може проширити до базе простора V

$\Rightarrow\; \dim U \leq \dim V$.

(2) Нека је

$$U \preceq V, \quad \dim U = \dim V = n \quad i \quad B_U = \{x_1, \ldots, x_n\} \text{ база од } U$$

$\Rightarrow B_U$ је линеарно независан скуп вектора у простору V димензије n

$\Rightarrow \mathcal{L}(B_U) = V$

$(\mathcal{L}(B_U) \neq V \Rightarrow$ постоји $x \in V \setminus \mathcal{L}(B_U)$

$\Rightarrow \{x_1, \ldots, x_n, x\}$ је линеарно независан скуп, контрадикција са $\dim V = n)$

$\Rightarrow U = \mathcal{L}(B_U) = V$.

(3) $$\begin{matrix} U_1, U_2 \preceq V \Rightarrow U_1 \cap U_2 \preceq V \\ V \text{ коначне димензије} \end{matrix} \Rightarrow U_1 \cap U_2 \text{ коначне димензије.}$$

Нека је $\dim(U_1 \cap U_2) = m > 0$ и $B' = \{x_1, \ldots, x_m\}$ једна база од $U_1 \cap U_2$.

$\Rightarrow B'$ је линеарно независан скуп у U_1

$\Rightarrow B'$ је или база или се може проширити до базе простора U_1.

- B' је база за $U_1 \Rightarrow \dim U_1 = \dim(U_1 \cap U_2) \overset{(2)}{\Rightarrow} U_1 = U_1 \cap U_2 \Rightarrow\; U_1 \subseteq U_2, U_1 + U_2 = U_2$

  $\Rightarrow \dim(U_1 + U_2) = \dim U_2 = \dim U_1 + \dim U_2 - \dim U_1 = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2)$,
- B' се може се проширити до базе $\{x_1, \ldots, x_m, y_1, \ldots, y_k\}$ од U_1.

  B' се може проширити до базе $\{x_1, \ldots, x_m, z_1, \ldots, z_l\}$ простора U_2.

Докажимо да је $B = \{x_1, \ldots, x_m, y_1, \ldots, y_k, z_1, \ldots, z_l\}$ база простора $U_1 + U_2$.

(B_1) $\mathcal{L}(B) = U_1 + U_2$?

Ако $x = y + z \in U_1 + U_2$, онда $y \in U_1$ и $z \in U_2$ су облика

$$\begin{aligned} y &= \alpha_1 x_1 + \ldots \alpha_m x_m + \beta_1 y_1 + \cdots + \beta_k y_k, \quad (\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_k \in F) \\ z &= \gamma_1 x_1 + \cdots + \gamma_m x_m + \delta_1 z_1 + \cdots + \delta_l z_l, \quad (\gamma_1, \ldots, \gamma_m, \delta_1, \ldots, \delta_l \in F) \end{aligned}$$

$$\begin{aligned} \Rightarrow x = (\alpha_1 + \gamma_1) x_1 + \cdots + \; & (\alpha_m + \gamma_m) x_m + \\ & + \beta_1 y_1 + \cdots + \beta_k y_k + \delta_1 z_1 + \cdots + \delta_l z_l \in \mathcal{L}(B) \end{aligned}$$

$\Rightarrow U_1 + U_2 = \mathcal{L}(B)$

(B_2) B је линеарно независан скуп вектора?

Нека је

$$\alpha_1 x_1 + \cdots + \alpha_m x_m + \beta_1 y_1 + \cdots + \beta_k y_k + \underbrace{\gamma_1 z_1 + \cdots + \gamma_l z_l}_{=z} = 0.$$

$$\left.\begin{array}{l} z = \gamma_1 z_1 + \cdots + \gamma_l z_l \in U_2 \\ z = (-\alpha_1)x_1 + \cdots + (-\alpha_m)x_m + (-\beta_1)y_1 + \cdots + (-\beta_k)y_k \in U_1 \end{array}\right. \Rightarrow z \in U_1 \cap U_2$$

$$\Rightarrow z = \lambda_1 x_1 + \cdots + \lambda_m x_m \quad (\lambda_i \in F)$$

$\lambda_1 x_1 + \cdots + \lambda_m x_m = \gamma_1 z_1 + \cdots + \gamma_l z_l$

$\lambda_1 x_1 + \cdots + \lambda_m x_m + (-\gamma_1)z_1 + \cdots + (-\gamma_l)z_l = 0$

$\lambda_1 = \cdots = \lambda_m = \gamma_1 = \cdots = \gamma_l = 0$(јер је $\{x_1, \ldots, x_m, z_1, \ldots, z_l\}$ база за U_2)

$\alpha_1 x_1 + \cdots + \alpha_m x_m + \beta_1 y_1 + \cdots + \beta_k y_k = 0$

$\alpha_1 = \cdots = \alpha_m = \beta_1 = \cdots = \beta_k = 0$(јер је $\{x_1, \ldots, x_m, y_1, \ldots, y_k\}$ база за U_1)

$\Rightarrow B$ је линеарно независан скуп вектора.

B је база простора $U_1 + U_2$, па је

$\dim(U_1 + U_2) = m + k + l = (m + k) + (m + l) - m = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2)$.

$V = U_1 \oplus U_2 \Rightarrow U_1 \cap U_2 = \emptyset \Rightarrow \dim(U_1 \cap U_2) = 0 \Rightarrow \dim(U_1 \oplus U_2) = \dim U_1 + \dim U_2$.

Пример 3.26. Одредити све потпросторе простора $\mathbb{R}^2$. Одредити $U = \mathcal{L}\{(1, 1), (1, 3)\}$.

Пример 3.27. Нека су U_1 и U_2 потпростори од V, $\dim U_1 = 3$, $\dim U_2 = 4$ и $\dim V = 6$. Одредити могуће димензије за $U_1 \cap U_2$.

3.8 Основни став линеарне алгебре

Дефиниција 3.18. Пресликавање $f : V \to U$ је линеарно пресликавање (хомоморфизам) векторског простора $(V, +_V, \cdot_V, F)$ у векторски простор $(U, +_U, \cdot_U, F)$ ако важи:

1. $f(x +_V y) = f(x) +_U f(y) \quad (x, y \in V)$ - адитивност
2. $f(\alpha \cdot_V x) = \alpha \cdot_U f(x) \quad (x \in V, \alpha \in F)$ - хомогеност.

Услови 1. и 2. су еквивалентни услову

$1'$. $f(\alpha \cdot_V x +_V \beta \cdot_V y) = \alpha \cdot_U f(x) +_U \beta \cdot_U f(y) \quad (x, y \in V, \alpha, \beta \in F)$ - линеарност

Докажимо да је свако линеарно пресликавање коначнодимензионог векторског простора потпуно одређено сликама базних вектора.

Теорема 3.19. (Основни став линеарне алгебре) Ако је $B = \{x_1, \ldots, x_n\}$ база векторског простора V_1 и $y_1, \ldots, y_n$ произвољни вектори простора V_2, тада постоји тачно једно линеарно пресликавање $f : V_1 \to V_2$ тако да је $f(x_1) = y_1, \ldots, f(x_n) = y_n$.

Доказ. **Егзистенција**:

$(\forall x \in V_1)(\exists_1(\alpha_1, \ldots, \alpha_n) \in F^n)\ x = \alpha_1 x_1 + \cdots + \alpha_n x_n$ (јер је B база за V_1).

Дефинишимо $f(x) \overset{\text{def}}{=} \alpha_1 \cdot y_1 + \cdots + \alpha_n \cdot y_n$.

- f је добро дефинисано, јер је $(\alpha_1, \ldots, \alpha_n)$ једнозначно одређено.

- Проверимо да је f линеарно.

$$\begin{aligned}&x = \alpha_1 x_1 + \cdots + \alpha_n x_n, y = \beta_1 x_1 + \cdots + \beta_n x_n, \lambda, \mu \in F\\ &\Rightarrow \lambda x + \mu y = \lambda(\alpha_1 x_1 + \cdots + \alpha_n x_n) + \mu(\beta_1 x_1 + \cdots + \beta_n x_n)\\ &\qquad = (\lambda\alpha_1 + \mu\beta_1)x_1 + \cdots + (\lambda\alpha_n + \mu\beta_n)x_n\end{aligned}$$

$$\begin{aligned}\Rightarrow f(\lambda x + \mu y) &= (\lambda\alpha_1 + \mu\beta_1)y_1 + \cdots + (\lambda\alpha_n + \mu\beta_n)y_n,\\ &= \lambda(\alpha_1 y_1 + \cdots + \alpha_n y_n) + \mu(\beta_1 y_1 + \cdots + \beta_n y_n)\\ &= \lambda f(x) + \mu f(y).\end{aligned}$$

- Проверимо да важи $f(x_i) = y_i$, за свако $i = 1, \ldots, n$.

$$\begin{aligned}f(x_i) &= f(0 \cdot x_1 + \cdots + 1 \cdot x_i + \cdots + 0 \cdot x_n)\\ &= 0 \cdot y_1 + \cdots + 1 \cdot y_i + \cdots + 0 \cdot y_n\\ &= y_i \quad (i = 1, 2, \ldots, n).\end{aligned}$$

Следи да је f тражено пресликавање.

Јединственост:

Нека је $g : V_1 \to V_2$ линеарно пресликавање такво да је $g(x_i) = y_i, \quad i = 1, \ldots, n.$

Тада, за произвољно $x = \alpha_1 x_1 + \cdots + \alpha_n x_n \in V_1$ важи

$$\begin{aligned}g(x) &= g(\alpha_1 x_1 + \cdots + \alpha_n x_n)\\ &= \alpha_1 g(x_1) + \cdots + \alpha_n g(x_n)\\ &= \alpha_1 y_1 + \cdots + \alpha_n y_n = f(x),\end{aligned}$$

$$\Rightarrow\ g = f.\ \square$$

Пример 3.28. Одредити линеарно пресликавање $f : R^2 \to R^3$ такво да важи $f(1,0) = (2,-1,0)$, $f(1,1) = (3,-1,-2)$.

$$\begin{aligned}&B = \{(1,0),(1,1)\} \text{ је база простора } R^2\\ &\Leftrightarrow\ (\forall (x,y) \in R^2)(\exists_1 (\alpha,\beta) \in R^2)\ (x,y) = \alpha(1,0) + \beta(1,1)\\ &\Leftrightarrow (x,y) = (\alpha + \beta, \beta)\\ &\Leftrightarrow x = \alpha + \beta,\ y = \beta \quad (\text{систем једначина по } \alpha \text{ и } \beta)\\ &\Leftrightarrow \beta = y, \alpha = x - y\\ &\Leftrightarrow (x,y) = (x-y)\cdot(1,0) + y \cdot (1,1)\\ &\Rightarrow f(x,y) = f((x-y)\cdot(1,0) + y\cdot(1,1))\\ &\qquad = (x-y)\cdot f(1,0) + y \cdot f(1,1)\\ &\qquad = (x-y)\cdot(2,-1,0) + y\cdot(3,-1,-2)\\ &\qquad = (2x-2y, -x+y, 0) + (3y, -y, -2y)\\ &\qquad = (2x+y, -x, -2y).\end{aligned}$$

Теорема 3.20. Нека је $f : V_1 \to V_2$ линеарно пресликавање. Тада:

(1) Ако је $\{x_1, \ldots, x_n\} \subseteq V_1$ линеарно зависан скуп вектора, онда је и $\{f(x_1), \ldots, f(x_n)\}$ линеарно зависан (у V_2).

(2) f је мономорфизам акко сваки линеарно независни скуп вектора у V_1 слика у линеарно независни скуп вектора у V_2.

(3) f је епиморфизам акко сваки генераторни скуп вектора простора V_1 слика у генераторни скуп вектора простора V_2.

(4) f је изоморфизам акко f чува базу.

Доказ.

(1)
$$\begin{array}{l}
\{x_1,\dots,x_n\} \text{ je линеарно зависан у } V_1 \\
\Rightarrow (\exists i \in \{1,\dots,n\})\; x_i \in \mathcal{L}\{x_1,\dots,x_{i-1},x_{i+1},\dots,x_n\} \\
\Rightarrow x_i = \alpha_1 x_1 + \cdots + \alpha_{i-1}x_{i-1} + \alpha_{i+1}x_{i+1} + \cdots + \alpha_n x_n,\ \alpha_i \in F \\
\Rightarrow f(x_i) = \alpha_1 f(x_1) + \cdots + \alpha_{i-1}f(x_{i-1}) + \alpha_{i+1}f(x_{i+1}) + \cdots + \alpha_n f(x_n)) \\
\Rightarrow\ f(x_i) \in \mathcal{L}\{f(x_1),\dots,f(x_{i-1}),f(x_{i+1}),\dots,f(x_n)\} \\
\Rightarrow \{f(x_1),\dots,f(x_n)\} \text{ je линеарно зависан скуп у } V_2
\end{array}$$

(2) ($\rightarrow$) Нека je f линеарно 1-1 пресликавање и $\{x_1,\dots,x_n\}$ линеарно независан скуп вектора у V_1. Покажимо да je и $\{f(x_1),\dots,f(x_n)\}$ линеарно независан.

$$\begin{array}{l}
\alpha_1 \cdot f(x_1) + \cdots + \alpha_n \cdot f(x_n) = 0,\ \alpha_1,\dots,\alpha_n \in F \\
\Rightarrow f(\alpha_1 \cdot x_1 + \cdots + \alpha_n \cdot x_n) = 0 = f(0) \quad \text{(jep je } f \text{ линеарно)} \\
\Rightarrow \alpha_1 \cdot x_1 + \cdots + \alpha_n \cdot x_n = 0 \quad \text{(jep je } f \text{ 1-1)} \\
\Rightarrow \alpha_1 = \cdots = \alpha_n = 0 \quad \text{(jep je } \{x_1,\dots,x_n\} \text{ лин. независан).}
\end{array}$$

($\leftarrow$) Нека линеарно пресликавање f сваки линеарно независни скуп вектора слика у линеарно независан скуп вектора. Докажимо да je f 1-1.

$$\begin{array}{lll}
x_1 \neq x_2 & \Rightarrow & \{x_1 - x_2\} \text{ je лин. независан (jep } x_1 - x_2 \neq 0) \\
 & \Rightarrow & \{f(x_1 - x_2)\} \text{ je лин. независан (следи из претпоставке)} \\
 & \Rightarrow & f(x_1 - x_2) \neq 0 \\
 & \Rightarrow & f(x_1) - f(x_2) \neq 0 \\
 & \Rightarrow & f(x_1) \neq f(x_2).
\end{array}$$

(3) ($\rightarrow$) Нека je f епиморфизам и $V_1 = \mathcal{L}\{x_1,\dots,x_n\}$. Покажимо да $\{f(x_1),\dots,f(x_n)\}$ генерише простор V_2.

$$\begin{array}{ll}
f \text{ je "на"} & \Rightarrow (\forall y \in V_2)(\exists x \in V_1)\; y = f(x) \\
 & \Rightarrow y = f(x) = f(\alpha_1 x_1 + \cdots + \alpha_n x_n) \\
 & \qquad = \alpha_1 f(x_1) + \cdots + \alpha_n f(x_n) \\
 & \Rightarrow y \in \mathcal{L}\{f(x_1),\dots,f(x_n)\} \\
 & \Rightarrow V_2 \subseteq \mathcal{L}\{f(x_1),\dots,f(x_n)\}
\end{array}$$

Свакако je $\mathcal{L}\{f(x_1),\dots,f(x_n)\} \subseteq V_2$, па важи $V_2 = \mathcal{L}\{f(x_1),\dots,f(x_n)\}$.

($\leftarrow$) Нека линеарно пресликавања $f : V_1 \rightarrow V_2$ сваки скуп генератора простора V_1 слика у скуп генератора простора V_2 и нека $\{x_1,\dots,x_n\}$ генерише простор V_1. Тада

$$\begin{array}{l}
V_1 = \mathcal{L}\{x_1,\dots,x_n\} \\
\Rightarrow V_2 = \mathcal{L}\{f(x_1),\dots,f(x_n)\} \text{ (по претпоставци)} \\
\Rightarrow (\forall y \in V_2)(\exists \beta_1,\dots,\beta_n \in F)\; y = \beta_1 f(x_1) + \cdots + \beta_n f(x_n) \\
\qquad\qquad\qquad\qquad\qquad\qquad = f(\underbrace{\beta_1 x_1 + \cdots + \beta_n x_n}_{=x \in V_1}) \\
\Rightarrow (\forall y \in V_2)(\exists x \overset{\text{def}}{=} \beta_1 x_1 + \cdots + \beta_n x_n \in V_1)\; y = f(x) \\
\Rightarrow f \text{ je "на".}
\end{array}$$

(4) следи из (2) и (3). □

Теорема 3.21. Ако су V_1 и V_2 коначно димензиони векторски простори над истим пољем F, тада

$$V_1 \cong V_2 \Longleftrightarrow dimV_1 = dimV_2.$$

Доказ. ($\to$)

$f : V_1 \cong V_2$ и $\{x_1, \dots, x_n\}$ база за V_1
$\Rightarrow \{f(x_1), \dots, f(x_n)\}$ је база за V_2 (Теорема 3.20.(4))
$\Rightarrow dimV_2 = n = dimV_1$.

($\leftarrow$) Нека је $dimV_1 = dimV_2 = n$,
$B_1 = \{x_1, \dots, x_n\}$, $B_2 = \{y_1, \dots, y_n\}$ базе, редом, за V_1 и V_2
$\Rightarrow$ постоји јединствено линеарно пресликавање $f : V_1 \to V_2$, тако да је
$f(x_i) = y_i$, $i = 1, \dots, n$ (из Основног става линеарне алгебре)
$\Rightarrow$ *f* је изоморфизам (Теорема 3.20. (4))
$\Rightarrow V_1 \cong V_2$. □

3.9 Слика и језгро линеарног пресликавања

ДЕФИНИЦИЈА 3.19. Нека је $f : V_1 \to V_2$ линеарно пресликавање. Тада

- $kerf \overset{\text{def}}{=} \{x \in V_1 | f(x) = 0\}$ се зове језгро хомоморфизма f
- $Imf \overset{\text{def}}{=} \{f(x) | x \in V_1\}$ се зове слика хомоморфизма f.

Неке особине језгра и слике линеарног пресликавања су дате следећом теоремом.

ТЕОРЕМА 3.22. Нека је $f : V_1 \to V_2$ линеарно пресликавање. Тада

(1) $Imf \preceq V_2$.

(2) *f* је "на" акко $Imf = V_2$.

(3) $kerf \preceq V_1$.

(4) *f* је 1-1 акко $kerf = \{0\}$.

(5) $f : V_1 \cong V_2$ акко $kerf = \{0\}$ и $Imf = V_2$.

(6) Ако је V_1 коначно димензиони векторски простор, тада су $kerf$ и Imf коначне димензије и важи $dimV_1 = dim(kerf) + dim(Imf)$.

Доказ.

(1)
- $0 = f(0) \Rightarrow 0 \in Imf \Rightarrow \emptyset \neq Imf \subseteq V_2$
- $y_1, y_2 \in Imf, \alpha, \beta \in F \Rightarrow \ (\exists x_1, x_2 \in V_1)\ y_1 = f(x_1),\ y_2 = f(x_2)$
  $\Rightarrow \alpha y_1 + \beta y_2 = \alpha f(x_1) + \beta f(x_2) = f(\alpha x_1 + \beta x_2) \in Imf$

(2) следи из дефиниције "на" функције и Imf

(3)
- $f(0) = 0 \Rightarrow 0 \in kerf \Rightarrow \emptyset \neq kerf \subseteq V_1$
- $$\begin{aligned} x_1, x_2 \in kerf, \alpha, \beta \in F \quad &\Rightarrow f(\alpha x_1 + \beta x_2) = \alpha f(x_1) + \beta f(x_2) \\ &= \alpha \cdot 0 + \beta \cdot 0 = 0 \\ &\Rightarrow \alpha x_1 + \beta x_2 \in kerf \end{aligned}$$

(4) ($\to$) Нека је f "1-1". Тада

$$x \in kerf \Rightarrow f(x) = 0 = f(0) \Rightarrow x = 0$$
$$\Rightarrow kerf = \{0\}.$$

($\leftarrow$) Нека је $kerf = \{0\}$. Тада

$$\begin{aligned} f(x) = f(y) \quad &\Rightarrow f(x) - f(y) = 0 \\ &\Rightarrow f(x-y) = 0 \\ &\Rightarrow x - y \in kerf \qquad \Rightarrow f \text{ је "1-1"} \\ &\Rightarrow x - y = 0 \\ &\Rightarrow x = y \end{aligned}$$

(5) следи из (2) и (4).

(6) V_1 коначне димензије, $kerf \preceq V_1 \Rightarrow kerf$ је коначне димензије и $0 \leq dim(kerf) \leq dimV_1$. Могући су следећи случајеви:

- $dim(kerf) = 0 \Rightarrow kerf = \{0\} \Rightarrow f : V_1 \to Imf$ је изоморфизам $\Rightarrow dim(Imf) = dimV_1 \Rightarrow dimV_1 = dim(kerf) + dim(Imf)$.
- $dim(kerf) = dimV_1 \Rightarrow kerf = V_1 \Rightarrow Imf = \{0\} \Rightarrow dim(Imf) = 0 \Rightarrow dimV_1 = dim(kerf) + dim(Imf)$.
- $0 < dim(kerf) < dimV_1$ и $\{x_1, \ldots, x_k\}$ нека је база за $kerf$.

  Проширимо је до базе $\{x_1, \ldots, x_k, x_{k+1}, \ldots, x_n\}$ простора V_1.

  Покажимо да је $B = \{f(x_{k+1}), \ldots, f(x_n)\}$ база простора Imf.

$$(B_1) \quad \begin{aligned} y \in Imf \quad &\Rightarrow \quad (\exists x \in V_1) y = f(x) \\ &\Rightarrow \quad y = f(\alpha_1 x_1 + \cdots + \alpha_k x_k + \alpha_{k+1} x_{k+1} + \cdots + \alpha_n x_n) \\ &\quad\quad = \alpha_1 f(x_1) + \cdots + \alpha_k f(x_k) + \alpha_{k+1} f(x_{k+1}) + \cdots + \alpha_n f(x_n) \\ &\quad\quad = \alpha_1 \cdot 0 + \cdots + \alpha_k \cdot 0 + \alpha_{k+1} f(x_{k+1}) + \cdots + \alpha_n f(x_n) \\ &\quad\quad = \alpha_{k+1} f(x_{k+1}) + \cdots + \alpha_n f(x_n) \\ &\Rightarrow \quad y \in \mathcal{L}(B) \end{aligned} \quad \Rightarrow$$

$$Imf = \mathcal{L}(B).$$

(B_2) линеарна независност

$$\begin{aligned} &\lambda_{k+1} f(x_{k+1}) + \cdots + \lambda_n f(x_n) = 0,\ \lambda_{k+1}, \ldots, \lambda_n \in F \\ &\Rightarrow f(\lambda_{k+1} x_{k+1} + \cdots + \lambda_n x_n) = 0 \\ &\Rightarrow \lambda_{k+1} x_{k+1} + \cdots + \lambda_n x_n \in kerf \\ &\Rightarrow \lambda_{k+1} x_{k+1} + \cdots + \lambda_n x_n = \alpha_1 x_1 + \cdots + \alpha_k x_k,\ \alpha_1, \ldots, \alpha_k \in F \\ &\Rightarrow (-\alpha_1) x_1 + \cdots + (-\alpha_k) x_k + \lambda_{k+1} x_{k+1} + \cdots + \lambda_n x_n = 0 \\ &\Rightarrow -\alpha_1 = \cdots = -\alpha_k = \lambda_{k+1} = \cdots = \lambda_n = 0 \text{ (јер } \{x_1, \ldots, x_n\} \text{ база за } V_1) \end{aligned}$$

$\Rightarrow B = \{f(x_{k+1}), \ldots, f(x_n)\}$ је линеарно независан скуп вектора.

B је база за $imf \Rightarrow dim(Imf) = |B| = n - k = dimV_1 - dim(kerf)$

$\Rightarrow dimV_1 = dim(kerf) + dim(Imf)$ □

Дефиниција 3.20. Ако је $f : V_1 \to V_2$ линеарно пресликавање, онда

- $r(f) \overset{\text{def}}{=} dim(Imf)$ се зове ранг хомоморфизма f
- $d(f) \overset{\text{def}}{=} dim(kerf)$ се зове дефект хомоморфизма f.

ПРИМЕР 3.29. За дата линеарна пресликавања одредити $Kerf$ и Imf:

(i) $p_i : \mathbb{R}^n \to \mathbb{R}$, $p_i(x_1, \ldots, x_n) = x_i$

(ii) $D : \mathbb{R}_n[x] \to \mathbb{R}_n[x]$, $D(p) = p'$

(iii) $f : \mathbb{R}^3 \to \mathbb{R}^3$, $f(x, y, z) = (x + y, 0, y - z)$

(iv) $f : \mathbb{R}^4 \to \mathbb{R}^3$, $f(x, y, z, u) = (x + y, y - z, x + u)$

За свако од датих пресликавања одредити да ли је ињективно и да ли је сирјективно.

Глава 4

Матрице и детерминанте

4.1 Дефиниција матрице

Нека је $(F, +, \cdot, 0, 1)$ поље, $n, m \in \mathbb{N}$.

Дефиниција 4.1. Матрица типа $m \times n$ над пољем F је свако пресликавање

$$A : \{1, 2, \dots, m\} \times \{1, 2, \dots, n\} \to F.$$

Ако је $A(i, j) = a_{ij} \in F$, матрицу A записујемо у облику

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \text{ или краће, } A = [a_{ij}]_{m \times n}.$$

Скалари a_{ij} се зову елементи матрице,

$v_i = [a_{i1}\ a_{i2}\ \dots\ a_{in}]$ је i-та врста $(i \in \{1, \dots, m\})$,

$$k_j = \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix} \text{ је } j\text{–та колона} \quad (j \in \{1, \dots, n\}) \text{ матрице } A.$$

Први индекс означава број врсте, а други индекс број колоне у којој се елемент налази. Матрица типа $m \times n$ има m врста и n колона.

$M_{m \times n}(F)$ - скуп свих матрица типа $m \times n$ над пољем F. Ако је $m = n$ (број врста једнак броју колона) кажемо да је A квадратна матрица реда n. $M_n(F)$ - скуп свих квадратних матрица реда n над пољем F.

Пример 4.1. Матрице $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix}$, $B = \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix}$ $C = [1\ 3\ -2\ 5]$ су типа, редом, 3×2 (3 врсте, 2 колоне), 3×1 (матрица колона) и 1×4 (матрица врста) $a_{12} = 2,\ a_{21} = 3,\ a_{32} = 6,\ b_{11} = 1,\ b_{31} = 4,\ c_{12} = 3,\ c_{13} = -2$, $D = \begin{bmatrix} 1 & 2 & 0 \\ 3 & 4 & -1 \\ 5 & 6 & 7 \end{bmatrix}$ квадратна матрица реда 3.

ДЕФИНИЦИЈА 4.2. Нека су $A = [a_{ij}],\ B = [b_{ij}] \in M_{m\times n}(F)$. Тада

$$A = B \overset{\text{def}}{\Leftrightarrow} (\forall i \in \{1,\dots,m\})(\forall j \in \{1,\dots,n\})\ a_{ij} = b_{ij}.$$

ПРИМЕР 4.2.

$$\begin{bmatrix} x & y \\ z & u \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \quad \Leftrightarrow \quad \begin{cases} x & = & 1 \\ y & = & 2 \\ z & = & 3 \\ u & = & 4. \end{cases}$$

На скупу $M_{m\times n}(F)$ дефинишемо бинарну операцију сабирање матрица на следећи начин:

ДЕФИНИЦИЈА 4.3. Ако су $A = [a_{ij}],\ B = [b_{ij}] \in M_{m\times n}(F)$, тада

$$A + B \overset{\text{def}}{=} [a_{ij} + b_{ij}]_{m\times n}, \quad \text{тј.}$$

$$\begin{bmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{bmatrix} + \begin{bmatrix} b_{11} & \dots & b_{1n} \\ b_{21} & \dots & b_{2n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \dots & b_{mn} \end{bmatrix} = \begin{bmatrix} a_{11}+b_{11} & \dots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & \dots & a_{2n}+b_{2n} \\ \vdots & \ddots & \vdots \\ a_{m1}+b_{m1} & \dots & a_{mn}+b_{mn} \end{bmatrix}.$$

ПРИМЕР 4.3. $\begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix} + \begin{bmatrix} 0 & -2 \\ 1 & 5 \\ 3 & -3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 4 & 9 \\ 8 & 3 \end{bmatrix}.$

ДЕФИНИЦИЈА 4.4.

- Матрица $0 \overset{\text{def}}{=} [0]_{m\times n}$ (тј. сви елементи су једнаки 0) се зове нула матрица.
- Матрица $-A \overset{\text{def}}{=} [-a_{ij}]_{m\times n}$ се зове супротна матрица матрице $A = [a_{ij}]_{m\times n}$.

ТЕОРЕМА 4.1. $(M_{m\times n}(F), +)$ је Абелова група.

Доказ. Лако се проверавају аксиоме Абелове групе:

(0) $A, B \in M_{m\times n}(F) \Rightarrow A + B \in M_{m\times n}(F)$;

(1) $(A + B) + C = A + (B + C), \quad A, B, C \in M_{m\times n}(F)$;

(2) $A + B = B + A$

$A + B = [a_{ij}]_{m\times n} + [b_{ij}]_{m\times n} = [a_{ij} + b_{ij}]_{m\times n} = [b_{ij} + a_{ij}]_{m\times n} = [b_{ij}]_{m\times n} + [a_{ij}]_{m\times n} = B + A$;

(3) $A + 0 = A$ (нула матрица је неутрални за сабирање матрица);

(4) $A + (-A) = 0$. □

Дефинишемо и множење матрице скаларом.

ДЕФИНИЦИЈА 4.5. Нека $A = [a_{ij}] \in M_{m\times n}(F)$ и $\lambda \in F$. Тада

$$\lambda \cdot A \overset{\text{def}}{=} [\lambda a_{ij}]_{m\times n}, \quad tj.$$

$$\lambda \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} = \begin{bmatrix} \lambda a_{11} & \lambda a_{12} & \dots & \lambda a_{1n} \\ \lambda a_{21} & \lambda a_{22} & \dots & \lambda a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda a_{m1} & \lambda a_{m2} & \dots & \lambda a_{mn} \end{bmatrix}.$$

ПРИМЕР 4.4. $3 \cdot \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} = \begin{bmatrix} 3 & 6 & 9 \\ 12 & 15 & 18 \end{bmatrix}$.

Особине множења матрице скаларом дате су следећом теоремом.

ТЕОРЕМА 4.2. Ако $A, B \in M_{m\times n}(F)$ и $\lambda, \mu \in F$ онда

(1) $\lambda(A+B) = \lambda \cdot A + \lambda \cdot B$;

(2) $(\lambda+\mu)\cdot A = \lambda \cdot A + \mu \cdot A$;

(3) $\lambda \cdot (\mu \cdot A) = (\lambda\mu)\cdot A$;

(4) $1 \cdot A = A$.

Доказ. (1)

$$\begin{array}{rcl} \lambda(A+B) & = & \lambda([a_{ij}]+[b_{ij}]) \\ & = & \lambda[a_{ij}+b_{ij}] \quad \text{(по деф. сабирања матрица)} \\ & = & [\lambda(a_{ij}+b_{ij})] \quad \text{(по деф. множења скаларом)} \\ & = & [\lambda a_{ij}+\lambda b_{ij}] \quad \text{(дистрибутивност + и } \cdot \text{ у пољу)} \\ & = & [\lambda a_{ij}]+[\lambda b_{ij}] \quad \text{(по деф. сабирања матрица)} \\ & = & \lambda[a_{ij}]+\lambda[b_{ij}] \quad \text{(по деф. множења скаларом)} \\ & = & \lambda A + \lambda B. \end{array}$$

Слично се проверавају остале особине. □

ПОСЛЕДИЦА. $(M_{m\times n}(F), +, \cdot, F)$ је векторски простор димензије mn.

Доказ.

- Из Теореме 4.1. и Теореме 4.2. непосредно следи да је $M_{m\times n}(F)$ векторски простор.
- Нека је

$$E_{ij} = \begin{bmatrix} 0 & 0 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & 0 \end{bmatrix}, \text{ 1 је у } i\text{-тој врсти и } j\text{-тој колони.}$$

$B = \{E_{ij} | i = 1, \dots, m,\ j = 1, \dots, n\}$ је једна база простора $M_{m\times n}(F)$ јер:

(B_1) за свако $A \in M_{m\times n}(F)$ важи $A = [a_{ij}]_{m\times n} = a_{11}E_{11} + a_{12}E_{12} + \cdots + a_{mn}E_{mn} \in \mathcal{L}(B)$,

(B_2) B је линеарно независан скуп вектора (очигледно).

$\Rightarrow \quad dim(M_{m\times n}(F)) = m \cdot n$. □

ПРИМЕР 4.5.

$$\left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\}$$

је једна база простора $M_{2\times 3}(\mathbb{R})$,

$$\Rightarrow \quad dim(M_{2\times 3}(\mathbb{R})) = 6.$$

4.2 Множење матрица. Транспонована матрица

Дефиниција 4.6. Ако $A = [a_{ij}]_{m\times n}$, $B = [b_{ij}]_{n\times p}$, тада

$$A \cdot B = [c_{ij}]_{m\times p}, \quad \text{где је} \quad c_{ij} \overset{\text{def}}{=} \sum_{k=1}^{n} a_{ik}b_{kj} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj},\ tj.$$

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \cdot \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1p} \\ b_{21} & b_{22} & \dots & b_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{np} \end{bmatrix} \overset{\text{def}}{=}$$

$$\begin{bmatrix} \sum_{k=1}^{n} a_{1k}b_{k1} & \sum_{k=1}^{n} a_{1k}b_{k2} & \dots & \sum_{k=1}^{n} a_{1k}b_{kp} \\ \sum_{k=1}^{n} a_{2k}b_{k1} & \sum_{k=1}^{n} a_{2k}b_{k2} & \dots & \sum_{k=1}^{n} a_{2k}b_{kp} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{k=1}^{n} a_{mk}b_{k1} & \sum_{k=1}^{n} a_{mk}b_{k2} & \dots & \sum_{k=1}^{n} a_{mk}b_{kp} \end{bmatrix}.$$

Пример 4.6.

$$\begin{bmatrix} 0 & 1 & 2 \\ 3 & 0 & -1 \end{bmatrix}_{2\times 3} \cdot \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix}_{3\times 2} = \begin{bmatrix} 0\cdot 1+1\cdot 3+2\cdot 5 & 0\cdot 2+1\cdot 4+2\cdot 6 \\ 3\cdot 1+0\cdot 3-1\cdot 5 & 3\cdot 2+0\cdot 4-1\cdot 6 \end{bmatrix}_{2\times 2} = \begin{bmatrix} 13 & 16 \\ -2 & 0 \end{bmatrix}.$$

$$\begin{bmatrix} 0 & 1 \\ 3 & 0 \end{bmatrix}_{2\times 2} \cdot \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix}_{3\times 2} \text{ није дефинисано, } \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix}_{3\times 2} \cdot \begin{bmatrix} 0 & 1 \\ 3 & 0 \end{bmatrix}_{2\times 2} = \begin{bmatrix} 6 & 1 \\ 12 & 3 \\ 18 & 5 \end{bmatrix}.$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

Ако је $A = [a_{ij}]_{m\times n}$, $B = [b_{ij}]_{n\times p}$, онда

- за $m \neq p$ производ BA није дефинисан
- за $m = p$ производ BA је дефинисан,
  - за $m \neq n$ матрице AB и BA нису истог типа,
  - за $m = n = p$ матрице AB и BA су истотипне, али не морају бити једнаке.

$AB \neq BA$ у општем случају, па операција $\cdot$ није комутативна.

Дефиниција 4.7. Квадратне матрице A и B истог реда су комутативне ако је $AB = BA$.

Пример 4.7. Матрице $A = \begin{bmatrix} 2 & -1 \\ 0 & 2 \end{bmatrix}$ и $B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ су комутативне, јер

$$AB = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} = BA.$$

Дефиниција 4.8. Квадратна матрица $I_n = [\delta_{ij}] \in M_n(F)$, где $\delta_{ij} \overset{\text{def}}{=} \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$, $tj.$

$$I_n = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

се зове јединична матрица реда n.

ТЕОРЕМА 4.3. Важе следеће једнакости (под условом да сви наведени производи постоје):

(1) $A \cdot (B \cdot C) = (A \cdot B) \cdot C$ - асоцијативност множења матрица,

(2) $A \cdot I_n = A = I_m \cdot A, \quad A \in M_{m \times n}(F)$,

(3) $(A + B) \cdot C = A \cdot C + B \cdot C, A \cdot (B + C) = A \cdot B + A \cdot C$,

(4) $\lambda \cdot (AB) = (\lambda A) \cdot B = A \cdot (\lambda B)$.

Доказ.

(1) Нека $A = [a_{ij}]_{m \times n}$, $B = [b_{ij}]_{n \times p}$, $C = [c_{ij}]_{p \times q}$, $BC = [d_{ij}]_{n \times q}$, $AB = [f_{ij}]_{m \times p}$, $A(BC) = [e_{ij}]_{m \times q}$, $(AB)C = [g_{ij}]_{m \times q}$. Тада

$$\begin{array}{rcl} e_{ij} & = & \sum_{k=1}^n a_{ik} d_{kj} = \sum_{k=1}^n a_{ik} (\sum_{l=1}^p b_{kl} c_{lj}) = \\ & = & \sum_{l=1}^p (\sum_{k=1}^n a_{ik} b_{kl}) c_{lj} = \sum_{l=1}^p f_{il} c_{lj} = g_{ij} \end{array} \quad (i = 1, \ldots m, \ j = 1, \ldots, q)$$

(2) Нека је $A = [a_{ij}]_{m \times n}$, $I_n = [\delta_{ij}]$ и $A \cdot I_n = [b_{ij}]_{m \times n}$. Тада $b_{ij} = \sum_{k=1}^n a_{ik} \delta_{kj} = a_{i1} \underbrace{\delta_{1j}}_{=0} + \cdots + a_{ij} \underbrace{\delta_{jj}}_{=1} + \cdots + a_{in} \underbrace{\delta_{nj}}_{=0} = a_{ij}$

$$\Rightarrow A \cdot I_n = A.$$

(3) и (4) се слично доказују. □

Из Теореме 4.1. и Теореме 4.3. добија се следећа последица.

ПОСЛЕДИЦА. Структура $(M_n(F), +, \cdot)$, где је $+$ сабирање матрица, а $\cdot$ множење матрица, је некомутативан прстен са јединицом I_n.

НАПОМЕНА. Прстен $M_n(F)$ има делиоце нуле, јер постоје ненула матрице чији је производ нула матрица.

ПРИМЕР 4.8. За $n = 2$:

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

У семигрупи $(M_n(F), \cdot)$ индуктивно дефинишемо степен квадратне матрице A:

$$A^0 = I_n, \quad A^1 = A, \quad \ldots, \quad A^{m+1} = A^m \cdot A, \ (m \in \mathbb{N}).$$

ДЕФИНИЦИЈА 4.9. Ако је $A = [a_{ij}]_{m \times n}$ онда се матрица

$$A^T \overset{\text{def}}{=} [a_{ji}]_{n \times m}$$

се зове транспонована матрица матрице A.

Другим речима, A^T се добија из A, пишући, редом, врсте од A као колоне од A^T.

ПРИМЕР 4.9.

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix}^\top = \begin{bmatrix} 1 & 3 & 5 \\ & 4 & 6 \end{bmatrix}.$$

Особине транспоновања су дате у следећој теореми.

ТЕОРЕМА 4.4. (1) $(A+B)^\top = A^\top + B^\top$,

(2) $(\lambda \cdot A)^\top = \lambda \cdot A^\top$,

(3) $(A \cdot B)^\top = B^\top \cdot A^\top$,

(4) $(A^\top)^\top = A$.

Доказ.

- (1), (2) и (4) се једноставно доказују.
- (3) Нека је
  $A = [a_{ij}]_{m\times n}, \quad B = [b_{ij}]_{n\times p}, \quad A^T = [e_{ij}]_{n\times m}, \quad B^T = [f_{ij}]_{p\times n}$
  $AB = [c_{ij}]_{m\times p}, \quad (A\cdot B)^\top = [d_{ij}]_{p\times m}$ и $B^T \cdot A^T = [g_{ij}]_{p\times m}$.
  Тада
  $$d_{ij} = c_{ji} = \sum_{k=1}^{n} a_{jk}b_{ki} = \sum_{k=1}^{n} e_{kj}f_{ik} = \sum_{k=1}^{n} f_{ik}e_{kj} = g_{ij}, \ (i=1,\dots,p, \ j=1,\dots,m)$$
  $\Rightarrow (AB)^T = B^T A^T$. □

ДЕФИНИЦИЈА 4.10. Квадратна матрица $A \in M_n(F)$ је

- симетрична ако је $A^T = A$,
- кососиметрична ако је $A^T = -A$.

ПРИМЕР 4.10. $\begin{bmatrix} 1 & -2 & 3 \\ -2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix}$ је симетрична, јер $\begin{bmatrix} 1 & -2 & 3 \\ -2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix}^T = \begin{bmatrix} 1 & -2 & 3 \\ -2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix}$.

$\begin{bmatrix} 0 & 2 & 3 \\ -2 & 0 & -5 \\ -3 & 5 & 0 \end{bmatrix}$ је кососиметрична, јер

$$\begin{bmatrix} 0 & 2 & 3 \\ -2 & 0 & -5 \\ -3 & 5 & 0 \end{bmatrix}^T = \begin{bmatrix} 0 & -2 & -3 \\ 2 & 0 & 5 \\ 3 & -5 & 0 \end{bmatrix} = -\begin{bmatrix} 0 & 2 & 3 \\ -2 & 0 & -5 \\ -3 & 5 & 0 \end{bmatrix}.$$

ДЕФИНИЦИЈА 4.11. Траг квадратне матрице $A = [a_{ij}] \in M_n(F)$, у ознаци $tr(A)$, је збир свих елемената на главној дијагонали матрице A, тј.

$$tr(A) \overset{\text{def}}{=} a_{11} + a_{22} + \cdots + a_{nn}.$$

ПРИМЕР 4.11. Ако $A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix}$, онда $tr(A) = 1 + 4 + 6 = 11$.

ТЕОРЕМА 4.5. За матрице A, B и $\lambda \in F$ важи:

(1) $tr(A+B) = tr(A) + tr(B)$,

(2) $tr(\lambda A) = \lambda tr(A)$,

(3) $tr(A^T) = tr(A)$,

(4) $tr(A \cdot B) = tr(B \cdot A)$.

Доказ. (4) Нека је $A = [a_{ij}]_{m\times n}$, $B = [b_{ij}]_{n\times m}$, $AB = [c_{ij}]_{m\times m}$, $BA = [d_{ij}]_{n\times n}$. Тада

$$tr(AB) = \sum_{i=1}^{m} c_{ii} = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}b_{ji} = \sum_{j=1}^{m}\sum_{i=1}^{n} b_{ij}a_{ji} = \sum_{i=1}^{n}\sum_{j=1}^{m} b_{ij}a_{ji} = \sum_{i=1}^{n} d_{ii} = tr(BA). \ \square$$

4.3 Регуларне матрице

Дефиниција 4.12.
- Квадратна матрица $A \in M_n(F)$ је регуларна ако постоји квадратна матрица $B \in M_n(F)$ таква да важи

  $$A \cdot B = I_n \quad \text{и} \quad B \cdot A = I_n.$$

  Тада се матрица B зове инверзна матрица матрице A и обележава са A^{-1}.
- Матрица $A \in M_n(F)$ је сингуларна ако није регуларна.

Инверзна матрица регуларне матрице A је јединствена, јер из претпоставке да матрица A има инверзне матрице B и C следи

$$AB = BA = I_n,\ AC = CA = I_n \ \Rightarrow\ B = I_nB = CAB = CI_n = C.$$

Теорема 4.6. Ако су A и B регуларне матрице онда су и матрице $A \cdot B$ и A^T регуларне и важи:

(1) $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$,

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

Доказ. A и B су регуларне $\Rightarrow$ постоје $A^{-1}, B^{-1} \in M_n(F)$ $\Rightarrow$ постоје $B^{-1}A^{-1}, (A^{-1})^T$.

(1) $(AB)(B^{-1}A^{-1}) = ABB^{-1}A^{-1} = AI_nA^{-1} = AA^{-1} = I_n$,
$(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}I_nB = I_n$.

(2) $A^T(A^{-1})^T = (A^{-1}A)^T = I_n^T = I_n,\ (A^{-1})^TA^T = (AA^{-1})^T = I_n^T = I_n$. □

Теорема 4.7. Ако су сви елементи неке врсте (колоне) матрице A једнаки нули, онда је та матрица сингуларна.

Доказ. $A \in M_n(F)$ има нула врсту (колону) $\Rightarrow$ AB (BA) има нула врсту (колону), за свако $B \in M_n(F)$ $\Rightarrow$ $AB \neq I_n$ ($BA \neq I_n$) $\Rightarrow$ A је сингуларна. □

Дефиниција 4.13. Нека је $A \in M_{m\times n}(F)$. Елементарне операције врста или v-операције су:

- v_{ij} - размена i-те и j-те врсте матрице A,
- v_i^λ, $\lambda \neq 0$ - множење елемената i-те врсте бројем $\lambda \neq 0$,
- v_{ij}^λ - множење елемената j-те врсте бројем λ и додавање елементима i-те врсте.

Аналогно се дефинишу елементарне операције на колонама (k-операције):
$k_{ij}, \quad k_i^\lambda, \lambda \neq 0, \quad k_{ij}^\lambda$.

Дефиниција 4.14.

- Матрица A је v-еквивалентна матрици B истог типа, у ознаци $A \sim_v B$, ако се B добија из A коначном применом v-операција.
- Матрица A је k-еквивалентна матрици B истог типа, у ознаци $A \sim_k B$, ако се B добија из A коначном применом k-операција.
- Матрица A је еквивалентна матрици B истог типа, у ознаци $A \sim B$, ако се B добија из A коначном применом v или k-операција.

Очигледно, релације $\sim_v, \quad \sim_k, \quad \sim$ су релације еквиваленције на скупу $M_{m\times n}(F)$.

Дефиниција 4.15.

- Матрица A је степенаста по врстама (v-степенаста) ако број нула које претходе првом ненула елементу врсте расте од врсте до врсте.

  Први ненула елемент врсте ћемо звати истакнути елемент те врсте.
- v-степенаста матрица A је редукована ако су сви њени истакнути елементи једнаки 1, а сви остали елементи у њиховим колонама су једнаки 0.

Пример 4.12. $\begin{bmatrix} 0 & 2 & 3 & 4 \\ 0 & 0 & 5 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ је v-степенаста, али није редукована v-степенаста матрица, истакнути елементи су 2 и 5.

$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 3 & 5 & 4 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ није v-степенаста, $\begin{bmatrix} 0 & 1 & 2 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 1 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$ је редукована v-степенаста матрица.

Теорема 4.8. (а) Свака не-нула матрица $A \in M_{m\times n}(F)$ је v-еквивалентна некој v-степенастој матрици истог типа.

(б) Свака не-нула матрица $A \in M_{m\times n}(F)$ је v-еквивалентна некој редукованој v-степенастој матрици истог типа.

(в) Свака не-нула матрица $A \in M_{m\times n}(F)$ је еквивалентна матрици

$$\begin{bmatrix} 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 \end{bmatrix}$$

(r јединица на дијагонали, остало нуле, $r \leq m, n$) коју краће записујемо у облику блок матрице $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$.

Доказ.

(а) Алгоритам за довођење матрице на v-степенасту матрицу применом елементарних v-операција:

1) Налазимо прву ненула колону (постоји јер $A \neq 0$).
2) У тој колони налазимо не-нула елемент.
3) Ако је нађени елемент у i-тој врсти заменимо i-ту и прву врсту, тј. $v_{1i}(A)$.
4) Помножимо прву врсту инверзом нађеног ненула елемента (тако добијамо да је истакнути елемент прве врсте једнак 1).
5) Прву врсту множимо погодним скаларима и додајемо преосталим врстама, тако да се испод добијене јединице добију све нуле.
6) Посматрамо подматрицу добијену избацивањем прве врсте, свих почетних нула-колона (ако их има) и прве не-нула колоне. Прелазимо на корак 1) и понављамо поступак на добијеној подматрици. Уколико оваква подматрица не постоји - крај поступка.

(б) Поступком описаним под (а) добијамо v-степенасту матрицу чији су сви истакнути елементи једнаки 1.

Множењем сваке ненула врсте погодно изабраним скаларима и додавањем претходним врстама постиже се да у свакој не-нула колони, осим једне јединице сви остали елементи буду једнаки 0.

(в) Поступцима под (а) и (б) добија се v-еквивалентна редукована v-степенаста матрица.

Нека се истакнута јединица прве врсте налази у l колони. Заменимо прву и l-ту колону.

Множењем прве колоне погодно изабраним скаларима и додавањем преосталим колонама постиже се да сви елементи прве врсте, осим првог, буду једнаки нули.

Посматрамо матрицу D добијену избацивањем прве врсте и прве колоне.

- Ако је D нула матрица, теорема је доказана
- ако D није нула матрица, понављамо поступак на матрици D, и даље, све док не добијемо 0 матрицу или стигнемо до последње врсте. □

Пример 4.13. Одредимо v-степенасту матрицу B и редуковану v-степенасту матрицу C које су v-еквивалентне матрици $A = \begin{bmatrix} 1 & -2 & -2 & 3 \\ -3 & 2 & 9 & -7 \\ 2 & 5 & -9 & 3 \end{bmatrix}$.

$$\begin{bmatrix} 1 & -2 & -2 & 3 \\ -3 & 2 & 9 & -7 \\ 2 & 5 & -9 & 3 \end{bmatrix} \sim_v \begin{bmatrix} 1 & -2 & -2 & 3 \\ 0 & -4 & 3 & 2 \\ 0 & 9 & -5 & -3 \end{bmatrix} \sim_v \begin{bmatrix} 1 & -2 & -2 & 3 \\ 0 & -4 & 3 & 2 \\ 0 & 0 & 7 & 6 \end{bmatrix} = B$$

(применом најпре v_{21}^{3}, v_{31}^{-2}, а затим v_{3}^{4}, v_{32}^{9}).

$$B \sim_v \begin{bmatrix} 1 & -2 & -2 & 3 \\ 0 & 1 & -\frac{3}{4} & -\frac{1}{2} \\ 0 & 0 & 1 & \frac{6}{7} \end{bmatrix} \sim_v \begin{bmatrix} 1 & 0 & -\frac{7}{2} & 2 \\ 0 & 1 & -\frac{3}{4} & -\frac{1}{2} \\ 0 & 0 & 1 & \frac{6}{7} \end{bmatrix} \sim_v \begin{bmatrix} 1 & 0 & 0 & 5 \\ 0 & 1 & 0 & \frac{1}{7} \\ 0 & 0 & 1 & \frac{6}{7} \end{bmatrix} = C$$

(применом најпре $v_{2}^{-\frac{1}{4}}$, $v_{3}^{\frac{1}{7}}$, затим v_{12}^{2} па $v_{13}^{\frac{7}{2}}$, $v_{23}^{\frac{3}{4}}$).

Дефиниција 4.16. Ако је $A \in M_{m\times n}(F)$ и $A \sim \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$ $(r \leq m, n)$ онда се блок матрица $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$ зове нормална форма матрице A.

ПРИМЕР 4.14. Одредити нормалну форму матрице $A = \begin{bmatrix} 0 & 2 & 3 & 4 \\ 2 & 3 & 5 & 4 \\ 4 & 8 & 13 & 12 \end{bmatrix}$

$$
\begin{aligned}
A = & \begin{bmatrix} 0 & 2 & 3 & 4 \\ 2 & 3 & 5 & 4 \\ 4 & 8 & 13 & 12 \end{bmatrix} \overset{\mathrm{v}_{12}}{\sim} \begin{bmatrix} 2 & 3 & 5 & 4 \\ 0 & 2 & 3 & 4 \\ 4 & 8 & 13 & 12 \end{bmatrix} \overset{\mathrm{k}_1^{\frac{1}{2}}}{\sim} \begin{bmatrix} 1 & 3 & 5 & 4 \\ 0 & 2 & 3 & 4 \\ 2 & 8 & 13 & 12 \end{bmatrix} \\
& \overset{\mathrm{v}_{31}^{-2}}{\sim} \begin{bmatrix} 1 & 3 & 5 & 4 \\ 0 & 2 & 3 & 4 \\ 0 & 2 & 3 & 4 \end{bmatrix} \overset{\mathrm{k}_{21}^{-3},\mathrm{k}_{31}^{-5},\mathrm{k}_{41}^{-4}}{\sim} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 3 & 4 \\ 0 & 2 & 3 & 4 \end{bmatrix} \overset{\mathrm{k}_2^{\frac{1}{2}}}{\sim} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 3 & 4 \\ 0 & 1 & 3 & 4 \end{bmatrix}. \\
& \overset{\mathrm{v}_{32}^{-1}}{\sim} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 3 & 4 \\ 0 & 0 & 0 & 0 \end{bmatrix} \overset{\mathrm{k}_{32}^{-3},\,\mathrm{k}_{42}^{-4}}{\sim} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} I_2 & 0 \\ 0 & 0 \end{bmatrix}
\end{aligned}
$$

Применом елементарних v-операција на јединичну матрицу добијамо елементарне v-матрице.

Применом елементарних k-операција на јединичну матрицу добијамо елементарне k-матрице.

ДЕФИНИЦИЈА 4.17. Елементарне v-матрице су

$$
\begin{aligned}
P_{ij} &\overset{def}{=} v_{ij}(I_n), \\
P_i^{\lambda} &\overset{def}{=} v_i^{\lambda}(I_n),\ \lambda \neq 0 \\
P_{ij}^{\lambda} &\overset{def}{=} v_{ij}^{\lambda}(I_n),
\end{aligned}
$$

Елементарне k-матрице су

$$
\begin{aligned}
Q_{ij} &\overset{def}{=} k_{ij}(I_n), \\
Q_i^{\lambda} &\overset{def}{=} k_i^{\lambda}(I_n),\ \lambda \neq 0 \\
Q_{ij}^{\lambda} &\overset{def}{=} k_{ij}^{\lambda}(I_n).
\end{aligned}
$$

ПРИМЕР 4.15. $n = 3$: $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, $P_{12} = v_{12}(I_3) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = k_{12}(I_3) = Q_{12}$,

$$P_3^5 = v_3^5(I_3) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{bmatrix} = k_3^5(I_3) = Q_3^5,$$

$$P_{31}^2 = v_{31}^2(I_3) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{bmatrix} = k_{13}^2(I_3) = Q_{13}^2.$$

Лако се може приметити да важи:

$$P_{ij} = Q_{ij}, \qquad P_i^{\lambda} = Q_i^{\lambda},\ \lambda \neq 0, \qquad P_{ij}^{\lambda} = Q_{ji}^{\lambda}.$$

Применом $v(k)$-операције на неку матрицу постиже се исти ефекат као множењем те матрице са леве (десне) стране елементарном $v(k)$ матрицом одговарајућег типа.

ТЕОРЕМА 4.9. Ако је $A \in M_n(F)$ тада:

(1) $v_{ij}(A) = P_{ij} \cdot A, \qquad v_i^{\lambda}(A) = P_i^{\lambda} \cdot A,\ \lambda \neq 0, \qquad v_{ij}^{\lambda}(A) = P_{ij}^{\lambda} \cdot A,$

(2) $k_{ij}(A) = A \cdot Q_{ij}, \qquad k_i^\lambda(A) = A \cdot Q_i^\lambda,\ \lambda \neq 0, \qquad k_{ij}^\lambda(A) = A \cdot Q_{ij}^\lambda.$

Доказ. $P_i^\lambda \cdot A =$

$$= \begin{bmatrix} 1 & 0 & \dots & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & 1 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda a_{i1} & \lambda a_{i2} & \dots & \lambda a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$$

$= v_i^\lambda(A)$. Слично се доказују остали делови тврђења. □

ПОСЛЕДИЦА.

(а) $A \sim_v B$ акко $B = P_r \cdot \dots \cdot P_1 \cdot A$, где су P_i елементарне v-матрице.

(б) $A \sim_k B$ акко $B = A \cdot Q_1 \cdot \dots \cdot Q_s$, где су Q_i елементарне k-матрице.

(в) $A \sim B$ акко $B = P_r \cdot \dots \cdot P_1 \cdot A \cdot Q_1 \cdot \dots \cdot Q_s$, где су P_i елементарне v-матрице, а Q_j елементарне k-матрице.

ТЕОРЕМА 4.10. Елементарне матрице су регуларне.

Доказ. $P_{ij} \cdot P_{ij} = v_{ij}(P_{ij}) = v_{ij}(v_{ij}(I_n)) = I_n \ \Rightarrow\ P_{ij}^{-1} = P_{ij}$.

Слично, $(P_i^\lambda)^{-1} = P_i^{\lambda^{-1}},\ \lambda \neq 0, \qquad (P_{ij}^\lambda)^{-1} = P_{ij}^{-\lambda}$. □

ТЕОРЕМА 4.11. Матрица $A \in M_n(F)$ је регуларна акко $A \sim_v I_n$.

Доказ.

($\rightarrow$) Нека је $A \in M_n(F)$ регуларна матрица

$\Rightarrow A \neq 0$

$\Rightarrow A \sim_v B$ где је $B \in M_n(F)$ редукована v-степенаста матрица (Теорема 8(б))

$\Rightarrow B = P_r \dots P_1 A$, где су $P_1, \dots, P_r$ елементарне v-матрице (Последица (а))

$\Rightarrow B$ је регуларна матрица (као производ регуларних матрица)

$\Rightarrow B$ нема нула врсту (иначе би била сингуларна)

$\Rightarrow B$ има n јединица као истакнуте елементе

$\Rightarrow B = I_n$ (B је редукована, па изнад (наравно и испод) сваке јединице су све нуле)

$\Rightarrow A \sim_v I_n$.

($\leftarrow$) $A \sim_v I_n \quad \Rightarrow I_n \sim_v A$ (јер је $\sim_v$ симетрична)

$\Rightarrow$ постоје елементарне v-матрице $P_1, \dots, P_k$ такве да је $A = P_k \dots P_1 I_n$

$\Rightarrow A$ је регуларна (као производ регуларних матрица). □

ПРИМЕР 4.16.

$$A = \begin{bmatrix} 2 & 3 & -9 \\ 1 & 0 & 0 \\ 0 & -2 & 7 \end{bmatrix} \overset{\mathrm{v}_{12}}{\sim}_v \begin{bmatrix} 1 & 0 & 0 \\ 2 & 3 & -9 \\ 0 & -2 & 7 \end{bmatrix} \overset{\mathrm{v}_{21}^{-2}}{\sim}_v \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & -9 \\ 0 & -2 & 7 \end{bmatrix}$$

$$\overset{\mathrm{v}_2^{\frac{1}{3}}}{\sim}_v \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -3 \\ 0 & -2 & 7 \end{bmatrix} \overset{\mathrm{v}_{32}^{2}}{\sim}_v \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{bmatrix} \overset{\mathrm{v}_{23}^{3}}{\sim}_v \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I_3$$

$$\begin{aligned} &\Rightarrow I_3 = P_{23}^3 P_{32}^2 P_2^{\frac{1}{3}} P_{21}^{-2} P_{12} A \\ &\Rightarrow \ A \sim_v I_3 \\ &\Rightarrow A \text{ је регуларна} \quad \text{и} \quad A = P_{12} P_{21}^2 P_2^3 P_{32}^{-2} P_{23}^{-3} \end{aligned}$$

Један од поступака за налажење инверзне матрице регуларне матрице $A \in M_n(F)$: из $A \sim_v I_n \Rightarrow I_n = P_r \dots P_1 A \ / \cdot A^{-1} \Rightarrow A^{-1} = P_r \dots P_1 I_n$ следи да A^{-1} добијамо применом на I_n истих елементарних v-операција чијом применом на A добијамо I_n, тј.

$$[A|I_n] \sim_v \left[I_n|A^{-1}\right].$$

ПРИМЕР 4.17.

$$[A|I_3] = \left[\begin{array}{ccc|ccc} 2 & 3 & -9 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & -2 & 7 & 0 & 0 & 1 \end{array}\right] \sim_v \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 \\ 2 & 3 & -9 & 1 & 0 & 0 \\ 0 & -2 & 7 & 0 & 0 & 1 \end{array}\right]$$

$$\sim_v \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 3 & -9 & 1 & -2 & 0 \\ 0 & -2 & 7 & 0 & 0 & 1 \end{array}\right] \sim_v \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & -3 & \frac{1}{3} & -\frac{2}{3} & 0 \\ 0 & -2 & 7 & 0 & 0 & 1 \end{array}\right]$$

$$\sim_v \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & -3 & \frac{1}{3} & -\frac{2}{3} & 0 \\ 0 & 0 & 1 & \frac{2}{3} & -\frac{4}{3} & 1 \end{array}\right] \sim_v \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & \frac{7}{3} & -\frac{14}{3} & 3 \\ 0 & 0 & 1 & \frac{2}{3} & -\frac{4}{3} & 1 \end{array}\right] = \left[I_3|A^{-1}\right]$$

$$\Rightarrow \quad A^{-1} = \begin{bmatrix} 0 & 1 & 0 \\ \frac{7}{3} & -\frac{14}{3} & 3 \\ \frac{2}{3} & -\frac{4}{3} & 1 \end{bmatrix}.$$

ТЕОРЕМА 4.12. Матрица $A \in M_n(F)$ је сингуларна акко је v-еквивалентна матрици B која има бар једну нула врсту.

Доказ.

($\rightarrow$) Нека је $A \in M_n(F)$ сингуларна.

$A \sim_v B$, где је B редукована v-степенаста матрица (Теорема 4.8.(б)).

Ако B нема нула врсту онда $B = I_n$, тј. $A \sim_v I_n$, па је A регуларна (Теорема 4.10.). Контрадикција.

($\leftarrow$) Ако $A \sim_v B$ и B има нула врсту, тада B је сингуларна (Теорема 4.7.) и $B = P_r \dots P_1 A$ (Последица), па је и A сингуларна (у супротном B би била регуларна као производ регуларних матрица). □

ПРИМЕР 4.18.

$$A = \begin{bmatrix} 1 & 2 & -3 \\ 3 & -1 & 5 \\ 5 & 3 & -1 \end{bmatrix} \sim_v \begin{bmatrix} 1 & 2 & -3 \\ 0 & -7 & 14 \\ 0 & -7 & 14 \end{bmatrix} \sim_v \begin{bmatrix} 1 & 2 & -3 \\ 0 & -1 & 2 \\ 0 & 0 & 0 \end{bmatrix}$$

$\Rightarrow \quad A$ је сингуларна матрица.

4.4 Пермутације скупа

Нека је X непразан скуп.

ДЕФИНИЦИЈА 4.18.

- Свака бијекција скупа X се зове пермутација скупа X.
- $S_n \overset{\text{def}}{=} \big\{\sigma \mid \sigma : \{1,2,\ldots,n\} \to \{1,\ldots,n\}$ и σ је бијекција$\big\}$ - скуп свих пермутација скупа $X = \{1,2,\ldots,n\}$

ТЕОРЕМА 4.13. $(S_n, \circ)$ је група (где је операција $\circ$ композиција функција).

ДЕФИНИЦИЈА 4.19. Група $(S_n, \circ)$ се зове симетрична група степена n.

Пермутацију $\sigma \in S_n$ записујемо у облику
$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$, или краће $\sigma = \sigma(1)\sigma(2)\ldots\sigma(n)$.

ДЕФИНИЦИЈА 4.20.

- Пар $(\sigma(i), \sigma(j))$ представља инверзију пермутације σ ако важи
$$i < j, \quad \sigma(i) > \sigma(j),$$
тј. инверзију чине свака два елемента пермутације који нису у свом природном поретку из скупа $\mathbb{N}$.
- Са $inv(\sigma)$ означаваћемо скуп свих инверзија пермутације σ.
- Пермутација је парна ако садржи паран број инверзија.
- Ако је број инверзија непаран, пермутација је непарна.

Може се показати да је композиција пермутација исте парности парна пермутација, а композиција пермутација различите парности непарна пермутација.

ДЕФИНИЦИЈА 4.21. Пресликавање $sgn : S_n \to \{-1, 1\}$ дефинисано са

$$sgn(\sigma) \overset{\text{def}}{=} \begin{cases} 1, & \sigma \text{ је парна пермутација} \\ -1, & \sigma \text{ је непарна пермутација} \end{cases} \quad \text{тј. } sgn(\sigma) = (-1)^{|inv(\sigma)|}$$

ћемо звати знак пермутације.

ПРИМЕР 4.19. Посматрајмо пермутације скупа $X = \{1,2,3,4,5\}$.

- За $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}$ важи
$$inv(\sigma) = \big\{(4,3),(4,1),(4,2),(3,1),(3,2),(5,1),(5,2)\big\},$$
па је σ непарна пермутација, тј. $sgn(\sigma) = -1$.
- За $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$ важи
$$inv(\tau) = \big\{(4,3),(4,1),(4,2),(3,1),(3,2),(5,2)\big\},$$
па је τ парна пермутација, тј. $sgn(\tau) = 1$.

- За $\mathbf{1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ важи $inv(\mathbf{1}) = \emptyset$, па је $\mathbf{1}$ парна пермутација.

Дефиниција 4.22. Нека су $i, j \in \{1, 2, \ldots, n\}$. Пермутација $\tau \in S_n$ облика

$$\tau = \begin{pmatrix} 1 & 2 & \ldots & i & \ldots & j & \ldots & n \\ 1 & 2 & \ldots & j & \ldots & i & \ldots & n \end{pmatrix}$$

зове се транспозиција.

Свака пермутација је композиција коначног броја транспозиција.

Особине знака пермутације су дате следећом теоремом:

Теорема 4.14. За $\sigma, \tau \in S_n$ важи

(1) $sgn(\sigma \circ \tau) = sgn(\sigma) \cdot sgn(\tau)$,

(2) $sgn(\sigma^{-1}) = sgn(\sigma)$,

(3) Ако је τ транспозиција, онда је $sgn(\tau) = -1$.

Доказ.

(1)
- σ и τ исте парности $\Rightarrow$ $\sigma \circ \tau$ је парна пермутација $\Rightarrow$
  $sgn(\sigma \circ \tau) = 1 = 1 \cdot 1 = sgn(\sigma) \cdot sgn(\tau)$ (σ и τ парне) или
  $sgn(\sigma \circ \tau) = 1 = (-1) \cdot (-1) = sgn(\sigma) \cdot sgn(\tau)$ (σ и τ непарне)
- σ и τ различите парности $\Rightarrow$ $\sigma \circ \tau$ је непарна пермутација $\Rightarrow$
  $sgn(\sigma \circ \tau) = -1 = 1 \cdot (-1) = sgn(\sigma) \cdot sgn(\tau)$

(2)
$$\begin{aligned} \sigma \circ \sigma^{-1} = \mathbf{1}, sgn(\mathbf{1}) = 1 \quad &\Rightarrow \quad sgn(\sigma) \cdot sgn(\sigma^{-1}) = 1 \\ &\Rightarrow \quad sgn(\sigma^{-1}) = sgn(\sigma). \end{aligned}$$

(3) за $\tau = \begin{pmatrix} 1 & 2 & \ldots & i & i+1 & \ldots & j-1 & j & \ldots & n \\ 1 & 2 & \ldots & j & i+1 & \ldots & j-1 & i & \ldots & n \end{pmatrix}$ важи

$$\begin{aligned} inv(\tau) = \{ \quad & (j, i+1), (j, i+2), \ldots, (j, \underbrace{i + (j - i - 1)}_{=j-1}), (j, i), \\ & (i+1, i), (i+2, i), \ldots, (\underbrace{i + (j - i - 1}_{j-1}, i)\} \end{aligned}$$

$\Rightarrow$ $|inv(\tau)| = 2(j - i - 1) + 1$,

$\Rightarrow$ τ је непарна пермутација. □

4.5 Детерминанте (дефиниција и основна својства)

Дефиниција 4.23. Нека је $A = [a_{ij}] \in M_n(F)$. Детерминанту матрице A дефинишемо на следећи начин

$$detA = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} \overset{def}{=} \sum_{\sigma \in S_n} sgn(\sigma) \cdot a_{1\sigma(1)} \cdot a_{2\sigma(2)} \ldots a_{n\sigma(n)}.$$

Из дефиниције непосредно добијамо:

За $n = 1$ тривијално важи $|a_{11}| = a_{11}$.

За $n = 2$ важи $S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$, па је

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

За $n = 3$:

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33},$$

што се може записати и у облику

$$\begin{aligned} \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} &= a_{11}(a_{22}a_{33} - a_{32}a_{23}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) + \\ &\qquad + a_{13}(a_{21}a_{32} - a_{22}a_{31}) = \\ &= a_{11}\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12}\begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13}\begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix} \end{aligned}$$

Излажемо особине детерминанти које ће нам олакшати њихово израчунавање.

Теорема 4.15. $det(A^T) = detA$.

Доказ. Нека је $A = [a_{ij}] \in M_n(F)$, $A^T = [b_{ij}]$, где је $b_{ij} = a_{ji}$. Тада

$$\begin{aligned} det(A^T) &= \textstyle\sum_{\sigma\in S_n} sgn(\sigma)\cdot b_{1\sigma(1)}\cdot b_{2\sigma(2)}\cdots b_{n\sigma(n)} \\ &= \textstyle\sum_{\sigma\in S_n} sgn(\sigma)\cdots a_{\sigma(1)1}\cdot a_{\sigma(2)2}\cdots a_{\underbrace{\sigma(k)}_{=1}k}\cdots a_{\sigma(n)n} \\ &= \textstyle\sum_{\sigma\in S_n} sgn(\sigma)\cdot a_{1\sigma^{-1}(1)}\cdot a_{2\sigma^{-1}(2)}\cdots a_{n\sigma^{-1}(n)} \; (\sigma(k) = 1 \Leftrightarrow k = \sigma^{-1}(1) \\ &= \textstyle\sum_{\sigma\in S_n} sgn(\sigma^{-1})\cdot a_{1\sigma^{-1}(1)}\cdot a_{2\sigma^{-1}(2)}\dots a_{n\sigma^{-1}(n)} \\ &= \textstyle\sum_{\sigma^{-1}\in S_n} sgn(\sigma^{-1})\cdot a_{1\sigma^{-1}(1)}\cdot a_{2\sigma^{-1}(2)}\cdots a_{n\sigma^{-1}(n)} \\ &\qquad \text{(јер је пресликавање } \sigma\mapsto\sigma^{-1} \text{ бијекција скупа } S_n) \\ &= detA\square \end{aligned}$$

Теорема 4.16. Ако се матрица B добија из A пермутацијом τ врста (колона) матрице A, онда је

$$detB = sgn(\tau)detA.$$

Доказ. Нека се $B = [b_{ij}]$ добија пермутацијом τ колона матрице $A = [a_{ij}]$, тј. $b_{ij} = a_{i\tau(j)}$. Тада је

$$\begin{aligned} detB &= \sum_{\sigma\in S_n} sgn(\sigma)\cdot b_{1\sigma(1)}\cdot b_{2\sigma(2)}\dots b_{n\sigma(n)} \\ &= \sum_{\sigma\in S_n} sgn(\sigma)\cdot a_{1\tau(\sigma(1))}\cdot a_{2\tau(\sigma(2))}\dots a_{n\tau(\sigma(n))} \end{aligned}$$

Означимо $\rho = \tau\circ\sigma$. Тада из $sgn(\rho) = sgn(\tau)\cdot sgn(\sigma)$ и $sgn(\tau) \in \{1,-1\}$ следи

$$sgn(\sigma) = sgn(\rho)\cdot sgn(\tau).$$

Пресликавање $\sigma \mapsto \tau\circ\sigma$ је бијекција скупа S_n, па када σ пролази скуп S_n, онда и ρ пролази цели скуп S_n. Имајући све ово у виду, имамо даље

$$detB = \sum_{\rho\in S_n} sgn(\rho)\cdot sgn(\tau)a_{1\rho(1)}\cdot a_{2\rho(2)}\dots a_{n\rho(n)} = sgn(\tau)detA.\Box$$

ПОСЛЕДИЦА 1.

$$B = v_{ij}(A) \quad\Rightarrow\quad detB = -detA,$$

тј. ако две врсте (колоне) матрице замене места њена детерминанта мења знак.

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = - \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

Доказ. Како се B добија из A транспозицијом τ врста, а транспозиција је непарна пермутација тј. $sgn(\tau) = -1$, применом претходне теореме добијамо

$$detB = sgn(\tau)detA = -detA.\Box$$

ПОСЛЕДИЦА 2. Ако су две врсте (колоне) матрице A једнаке, онда је њена детерминанта једнака 0 (уз услов да $char(F) \neq 2$).

Доказ.

$$\begin{aligned} &v_{ij}(A) = A \quad \text{(јер су } i - \text{та и } j - \text{та врста матрице } A \text{ једнаке)} \\ \Rightarrow\quad & detA = -detA \quad \text{(из претходне теореме)} \\ \Rightarrow\quad & (1+1)detA = 0 \\ \Rightarrow\quad & detA = 0 \quad (1+1 \neq 0 \text{ јер } char(F) \neq 2).\Box \end{aligned}$$

ТЕОРЕМА 4.17.

$$B = v_i^{\lambda}(A) \quad\Rightarrow\quad detB = \lambda detA,$$

тј. детерминанта се множи скаларом тако што се сви елементи једне врсте (колоне) помноже тим скаларом.

$$\lambda \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda a_{i1} & \lambda a_{i2} & \dots & \lambda a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

Доказ.

$$detB = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \ddots & \dots \\ \lambda a_{i1} & \lambda a_{i2} & \dots & \lambda a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \sum_{\sigma\in S_n} sgn(\sigma)a_{1\sigma(1)}\dots(\lambda a_{i\sigma(i)})\dots a_{n\sigma(n)} =$$

$$= \lambda\sum_{\sigma\in S_n} sgn(\sigma)a_{1\sigma(1)}\dots a_{i\sigma(i)})\dots a_{n\sigma(n)} = \lambda detA.\square$$

ПОСЛЕДИЦА 1. Ако су две врсте (колоне) матрице A пропорционалне, тада је $detA = 0$.

Доказ. $$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda a_{i1} & \lambda a_{i2} & \dots & \lambda a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \lambda \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \lambda\cdot 0 = 0.\square$$

ПОСЛЕДИЦА 2. За сваку матрицу $A \in M_n(F)$ и скалар $\lambda \in F$ важи

$$det(\lambda A) = \lambda^n detA.$$

Доказ.

$$\begin{aligned} det(\lambda A) &= \begin{vmatrix} \lambda a_{11} & \lambda a_{12} & \dots & \lambda a_{1n} \\ \lambda a_{21} & \lambda a_{22} & \dots & \lambda a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda a_{n1} & \lambda a_{n2} & \dots & \lambda a_{nn} \end{vmatrix} = \lambda \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \lambda a_{21} & \lambda a_{22} & \dots & \lambda a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda a_{n1} & \lambda a_{n2} & \dots & \lambda a_{nn} \end{vmatrix} \\ &= \underbrace{\lambda\dots\lambda}_{n} \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \lambda^n detA\square \end{aligned}$$

ТЕОРЕМА 4.18.

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \ddots & \dots \\ b_{i1}+c_{i1} & b_{i2}+c_{i2} & \dots & b_{in}+c_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \ddots & \dots \\ b_{i1} & \dots & b_{in} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \ddots & \dots \\ c_{i1} & \dots & c_{in} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}.$$

Доказ. Означимо детерминанту на левој страни са L, а збир детерминанти на десној страни са D. Тада

$$\begin{aligned} L &= \sum_{\sigma\in S_n} sgn(\sigma)\cdot a_{1\sigma(1)}\cdot a_{2\sigma(2)}\dots\big(b_{i\sigma(i)}+c_{i\sigma(i)}\big)\dots a_{n\sigma(n)} \\ &= \sum_{\sigma\in S_n} sgn(\sigma)\cdot a_{1\sigma(1)}\cdot a_{2\sigma(2)}\dots b_{i\sigma(i)}\dots a_{n\sigma(n)} + \\ &\qquad + \sum_{\sigma\in S_n} sgn(\sigma)\cdot a_{1\sigma(1)}\cdot a_{2\sigma(2)}\dots c_{i\sigma(i)}\dots a_{n\sigma(n)} \\ &= D.\square \end{aligned}$$

ПОСЛЕДИЦА 1.

$$det(A+B)\neq detA+detB \quad \text{(у општем случају)}$$

тј. $det: M_n(F)\to F$ није линеарна функционела.

ПОСЛЕДИЦА 2. $B=v_{ij}^{\lambda}(A) \quad\Rightarrow\quad detA=detB$, тј. ако све елементе неке врсте (колоне) матрице A помножимо скаларом и додамо одговарајућим елементима неке друге врсте (колоне) матрице A, детерминанта матрице A се неће променити.

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \ddots & \dots \\ a_{i1}+\lambda a_{j1} & a_{i2}+\lambda a_{j2} & \dots & a_{in}+\lambda a_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \ddots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

Доказ.

$$detB = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \ddots & \dots \\ a_{i1}+\lambda a_{j1} & a_{i2}+\lambda a_{j2} & \dots & a_{in}+\lambda a_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

$$= \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \ddots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \ddots & \dots \\ \lambda a_{j1} & \lambda a_{j2} & \dots & \lambda a_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = detA+\lambda\cdot 0 = detA.\square$$

ТЕОРЕМА 4.19. За матрице $A,B\in M_n(F)$ важи $det(AB)=detA\cdot detB$.

Доказ. Нека $A = [a_{ij}],\ B = [b_{ij}]$ и $AB = [c_{ij}]$, где је $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$. Тада

$$\begin{aligned}
det(AB) &= \begin{vmatrix} \sum_{k_1=1}^{n} a_{1k_1}b_{k_11} & \sum_{k_1=1}^{n} a_{1k_1}b_{k_12} & \dots & \sum_{k_1=1}^{n} a_{1k_1}b_{k_1n} \\ \sum_{k_2=1}^{n} a_{2k_2}b_{k_21} & \sum_{k_2=1}^{n} a_{2k_2}b_{k_22} & \dots & \sum_{k_2=1}^{n} a_{2k_2}b_{k_2n} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{k_n=1}^{n} a_{nk_n}b_{k_n1} & \sum_{k_n=1}^{n} a_{nk_n}b_{k_n2} & \dots & \sum_{k_n=1}^{n} a_{nk_n}b_{k_nn} \end{vmatrix} \\
&= \sum_{k_1=1}^{n} \begin{vmatrix} a_{1k_1}b_{k_11} & a_{1k_1}b_{k_12} & \dots & a_{1k_1}b_{k_1n} \\ \sum_{k_2=1}^{n} a_{2k_2}b_{k_21} & \sum_{k_2=1}^{n} a_{2k_2}b_{k_22} & \dots & \sum_{k_2=1}^{n} a_{2k_2}b_{k_2n} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{k_n=1}^{n} a_{nk_n}b_{k_n1} & \sum_{k_n=1}^{n} a_{nk_n}b_{k_n2} & \dots & \sum_{k_n=1}^{n} a_{nk_n}b_{k_nn} \end{vmatrix} \\
&= \sum_{k_1=1}^{n}\sum_{k_2=1}^{n}\cdots\sum_{k_n=1}^{n} \begin{vmatrix} a_{1k_1}b_{k_11} & a_{1k_1}b_{k_12} & \dots & a_{1k_1}b_{k_1n} \\ a_{2k_2}b_{k_21} & a_{2k_2}b_{k_22} & \dots & a_{2k_2}b_{k_2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{nk_n}b_{k_n1} & a_{nk_n}b_{k_n2} & \dots & a_{nk_n}b_{k_nn} \end{vmatrix}
\end{aligned}$$

$$= \sum_{k_1=1}^{n}\sum_{k_2=1}^{n}\cdots\sum_{k_n=1}^{n} a_{1k_1}a_{2k_2}\dots a_{nk_n} \begin{vmatrix} b_{k_11} & b_{k_12} & \dots & b_{k_1n} \\ b_{k_21} & b_{k_22} & \dots & b_{k_2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{k_n1} & b_{k_n2} & \dots & b_{k_nn} \end{vmatrix}$$

- у суми има n^n сабирака, али су неки од њих једнаки нули
- ако у n-торци $(k_1, \dots, k_n)$ има једнаких елемената, онда у $\begin{vmatrix} b_{k_11} & b_{k_12} & \dots & b_{k_1n} \\ b_{k_21} & b_{k_22} & \dots & b_{k_2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{k_n1} & b_{k_n2} & \dots & b_{k_nn} \end{vmatrix}$ има једнаких врста, па је ова детерминанта =0
- различити од 0 могу бити само они сабирци који се добијају у случају када $(k_1, \dots, k_n)$ представља пермутацију скупа $\{1, 2, \dots, n\}$
- сумирање се, заправо, врши по свим пермутацијама из скупа S_n

$$\begin{aligned}
det(AB) &= \sum_{\sigma\in S_n} a_{1\sigma(1)}\dots a_{n\sigma(n)} \cdot \begin{vmatrix} b_{\sigma(1)1} & b_{\sigma(1)2} & \dots & b_{\sigma(1)n} \\ b_{\sigma(2)1} & b_{\sigma(2)2} & \dots & b_{\sigma(2)n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{\sigma(n)1} & b_{\sigma(n)2} & \dots & b_{\sigma(n)n} \end{vmatrix} \\
&= \sum_{\sigma\in S_n} a_{1\sigma(1)}\dots a_{n\sigma(n)} \cdot sgn(\sigma) \begin{vmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{vmatrix} \\
&= \begin{vmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{vmatrix} \sum_{\sigma\in S_n} sgn(\sigma) a_{1\sigma(1)}\dots a_{n\sigma(n)} \\
&= detA \cdot detB.\square
\end{aligned}$$

Последица. Ако је матрица A регуларна, онда

$$det(A^{-1}) = \frac{1}{detA}.$$

Доказ.

A је регуларна
$\Rightarrow\ A \cdot A^{-1} = I_n$
$\Rightarrow\ detA \cdot det(A^{-1}) = detI_n = 1$ (Теорема 4.19.)
$\Rightarrow\ det(A^{-1}) = \frac{1}{detA}.\square$

4.6 Минори и кофактори

- Вредност детерминанти другог и трећег реда се лако одређује по дефиницији.
- То није случај са детерминантама вишег реда, потребно је израчунати $n!$ производа.
- Зато излажемо поступак којим се израчунавање детерминанте матрице реда n своди на израчунавање n детерминанати матрица реда $n-1$.

Дефиниција 4.24. Нека је $A = [a_{ij}] \in M_n(F)$.

- Са M_{ij} означимо матрицу реда $n-1$ добијену из A изостављањем i-те врсте и j-те колоне,
- $detM_{ij}$ ћемо звати минор елемента a_{ij},
- $A_{ij} = (-1)^{i+j} detM_{ij}$ кофактор елемента a_{ij}, тј.

$$A_{ij} = (-1)^{i+j} \begin{vmatrix} a_{11} & \dots & a_{1j} & \dots & a_{1n} \\ \vdots & \ddots & | & \ddots & \vdots \\ a_{i1}- & -- & a_{ij} & -- & a_{in}- \\ \vdots & \ddots & | & \ddots & \vdots \\ a_{n1} & \dots & a_{nj} & \dots & a_{nn} \end{vmatrix}$$

Придруживање знака $(-1)^{i+j}$ минору M_{ij} можемо приказати

$$\begin{bmatrix} + & - & + & - & \dots \\ - & + & - & + & \dots \\ + & - & + & - & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

Пример 4.20. $A = \begin{bmatrix} 1 & 2 & 3 \\ -2 & 4 & 5 \\ 0 & 6 & 7 \end{bmatrix}$

$$M_{23} = \begin{bmatrix} 1 & 2 \\ 0 & 6 \end{bmatrix}, \quad A_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 2 \\ 0 & 6 \end{vmatrix} = -(1 \cdot 6 - 0 \cdot 2) = -6$$

Теорема 4.20. Ако је $A = [a_{ij}] \in M_n(F)$, тада

(1) $detA = a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in}$ $(i = 1, \ldots, n)$ (развој детерминанте по i-тој врсти)

(2) $detA = a_{1j}A_{1j} + a_{2j}A_{2j} + \cdots + a_{nj}A_{nj} \quad (j = 1, \ldots, n)$ (развој детерминанте по j-тој колони).

Доказ. (1) Груписањем чланова детерминанте матрице A који садрже, редом, $a_{i1}, \ldots, a_{in}$, детерминанту матрице A можемо записати у облику

$$detA = a_{i1}B_{i1} + \cdots + a_{in}B_{in}.$$

Стављајући $a_{ij} = 1$ и $a_{ik} = 0,\ k \neq j$, добијамо $B_{ij} = \begin{vmatrix} a_{11} & \ldots & a_{1j} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \ldots & 1 & \ldots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nj} & \ldots & a_{nn} \end{vmatrix}$

Покажимо $B_{ij} = A_{ij}$.

- за $i = j = n$ важи

$$B_{nn} = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1,1} & a_{n-1,2} & \ldots & a_{n-1,n} \\ 0 & 0 & \ldots & 1 \end{vmatrix} = \sum_{\sigma \in S_n, \sigma(n)=n} sgn(\sigma) a_{1\sigma(1)} \ldots a_{n-1\sigma(n-1)} \cdot 1$$

$$= detM_{nn} = (-1)^{n+n} detM_{nn} = A_{nn}$$

- i и j произвољни
  - i-ту врсту разменимо редом са свим наредним врстама,
  - j-ту колону заменимо са свим наредним колонама
  - $detM_{ij}$ се не мења (њене врсте и колоне остају у истом међ. положају)

$$\begin{aligned} B_{ij} &= (-1)^{n-i}(-1)^{n-j} \begin{vmatrix} a_{11} & \ldots & a_{1j-1} & a_{1j+1} & \ldots & a_{1}n & a_{1j} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{i-1,1} & \ldots & a_{i-1,j-1} & a_{i-1,j+1} & \ldots & a_{i-1,n} & a_{i-1,j} \\ a_{i+1,1} & \ldots & a_{i+1,j-1} & a_{i+1,j+1} & \ldots & a_{i+1,n} & a_{i+1,j} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n1} & \ldots & a_{nj-1} & a_{n,j+1} & \ldots & a_{nn} & a_{nj} \\ 0 & \ldots & 0 & 0 & \ldots & 0 & 1 \end{vmatrix} \\ &= (-1)^{i+j} detM_{ij} = A_{ij}.\Box \end{aligned}$$

ТЕОРЕМА 4.21. Ако је $A = [a_{ij}] \in M_n(F)$ тада

(1) $a_{i1}A_{j1} + a_{i2}A_{j2} + \cdots + a_{in}A_{jn} = 0$, за $i \neq j$

(2) $a_{1i}A_{1j} + a_{2i}A_{2j} + \cdots + a_{ni}A_{nj} = 0$, за $i \neq j$.

Доказ.

- Посматрајмо матрицу B добијену из матрице A тако што је j-та врста замењена i-том, при чему $i \neq j$.
- Матрица B има две исте врсте, па је $detB = 0$.

- Развијањем $detB$ по j-тој врсти (Теорема 6.) добијамо $0 = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} =$ $a_{i1}A_{j1} + \dots + a_{in}A_{jn}$. □

НАПОМЕНА. Обједињујући претходне две теореме добијамо

- $$a_{i1}A_{j1} + a_{i2}A_{j2} + \dots + a_{in}A_{jn} = \begin{cases} detA, & i = j \\ 0, & i \neq j \end{cases},$$
- $$a_{1i}A_{1j} + a_{2i}A_{2j} + \dots + a_{ni}A_{nj} = \begin{cases} detA, & i = j \\ 0, & i \neq j \end{cases}.$$

По којој врсти (колони) развити детерминанту?

- најмање рачунања изискује развој детерминанте по оној врсти или колони која има највећи број нула
- најоптималније је развити детерминанту по врсти или колони која има само један ненула елемент (израчунавање детерминанте реда n се своди на израчунавање само једне детерминанте реда $n-1$)
- таква врста (колона) се увек може добити (применом Последице Теореме 4.)

ПРИМЕР 4.21. Доказати да је детерминанта горње троугаоне матрице једнака производу елемената на главној дијагонали.

$$\begin{aligned} \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{nn} \end{vmatrix} &= a_{11} \begin{vmatrix} a_{22} & a_{23} & \dots & a_{2n} \\ 0 & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{nn} \end{vmatrix} \\ &= a_{11}a_{22} \begin{vmatrix} a_{33} & a_{34} & \dots & a_{3n} \\ 0 & a_{44} & \dots & a_{4n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{nn} \end{vmatrix} \\ &= \dots = a_{11}a_{22} \dots a_{nn} \end{aligned}$$

4.7 Инверзна матрица

ДЕФИНИЦИЈА 4.25. Нека је $A = [a_{ij}] \in M_n(F)$ и $A_{ij} = (-1)^{i+j} detM_{ij}$ кофактор елемента a_{ij}. Тада се матрица $adjA \overset{\text{def}}{=} [A_{ij}]^T$ зове адјунгована матрица матрице A.

ТЕОРЕМА 4.22. За $A \in M_n(F)$ важи
$$A \cdot adjA = adjA \cdot A = detA \cdot I_n.$$

Доказ.

$$
\begin{aligned}
A\cdot adjA &= \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{bmatrix} \\
&= \begin{bmatrix} \sum_{k=1}^{n} a_{1k}A_{1k} & \sum_{k=1}^{n} a_{1k}A_{2k} & \dots & \sum_{k=1}^{n} a_{1k}A_{nk} \\ \sum_{k=1}^{n} a_{2k}A_{1k} & \sum_{k=1}^{n} a_{2k}A_{2k} & \dots & \sum_{k=1}^{n} a_{2k}A_{nk} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{k=1}^{n} a_{nk}A_{1k} & \sum_{k=1}^{n} a_{nk}A_{2k} & \dots & \sum_{k=1}^{n} a_{nk}A_{nk} \end{bmatrix}
\end{aligned}
$$

$$
= \begin{bmatrix} detA & & \dots & 0 \\ 0 & detA & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & detA \end{bmatrix} = detA \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} = detA\cdot I_n.
$$

Слично се доказује и друга једнакост. □

Последица. Квадратна матрица $A \in M_n(F)$ је регуларна акко $detA \neq 0$.

У том случају важи

$$A^{-1} = \frac{1}{detA}\cdot adjA.$$

Доказ. $(\rightarrow)$ Нека је A регуларна

$\Rightarrow$ постоји A^{-1} и важи $A\cdot A^{-1} = I_n$

$\Rightarrow detA\cdot det(A^{-1}) = det(A\cdot A^{-1}) = detI_n = 1$

$\Rightarrow detA \neq 0$.

$(\leftarrow)$ Нека је $detA \neq 0$. Тада, применом особина множења матрица скаларом и претходне теореме добијамо

$$
\begin{array}{c}
A\cdot\left(\frac{1}{detA}adjA\right) = \frac{1}{detA}(A\cdot adjA) = \frac{1}{detA}\cdot detA\cdot I_n = I_n \\
\left(\frac{1}{detA}adjA\right)\cdot A = \frac{1}{detA}(adjA\cdot A) = I_n
\end{array},
$$

$$\Rightarrow \quad A \text{ је регуларна}, \quad A^{-1} = \frac{1}{detA}adjA.\square$$

Пример 4.22. $A = \begin{bmatrix} 2 & 3 & -9 \\ 1 & 0 & 0 \\ 0 & -2 & 7 \end{bmatrix} \Rightarrow detA = \begin{vmatrix} 2 & 3 & -9 \\ 1 & 0 & 0 \\ 0 & -2 & 7 \end{vmatrix} = -1\cdot \begin{vmatrix} 3 & -9 \\ -2 & 7 \end{vmatrix} = -3 \neq 0 \Rightarrow \quad A$ је регуларна.

$$
adjA{=}[A_{ij}]^T{=}\begin{bmatrix} \begin{vmatrix} 0 & 0 \\ -2 & 7 \end{vmatrix} & -\begin{vmatrix} 1 & 0 \\ 0 & 7 \end{vmatrix} & \begin{vmatrix} 1 & 0 \\ 0 & -2 \end{vmatrix} \\ -\begin{vmatrix} 3 & -9 \\ -2 & 7 \end{vmatrix} & \begin{vmatrix} 2 & -9 \\ 0 & 7 \end{vmatrix} & -\begin{vmatrix} 2 & 3 \\ 0 & -2 \end{vmatrix} \\ \begin{vmatrix} 3 & -9 \\ 0 & 0 \end{vmatrix} & -\begin{vmatrix} 2 & -9 \\ 1 & 0 \end{vmatrix} & \begin{vmatrix} 2 & 3 \\ 1 & 0 \end{vmatrix} \end{bmatrix}^T = \begin{bmatrix} 0 & -3 & 0 \\ -7 & 14 & -9 \\ -2 & 4 & -3 \end{bmatrix}
$$

$$
\Rightarrow \quad A^{-1} = \frac{1}{detA}adjA = -\frac{1}{3}\begin{bmatrix} 0 & -3 & 0 \\ -7 & 14 & -9 \\ -2 & 4 & -3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ \frac{7}{3} & -\frac{14}{3} & 3 \\ \frac{2}{3} & -\frac{4}{3} & 1 \end{bmatrix}.
$$

4.8 Ранг матрице

Нека је:

- $A = [a_{ij}] \in M_{m\times n}(F)$,
- $v_i^A = [a_{i1}\ a_{i2}\ \dots\ a_{in}]$ - i-та врста матрице $A \quad (i = 1, 2, \dots, m)$
- $V(A) = \mathcal{L}\{v_1^A, v_2^A, \dots, v_m^A\}$ - векторски простор врста матрице A
- $k_j^A = \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix} = [a_{1j}\ a_{2j} \dots a_{mj}]^T$ - j-та колона матрице $A \quad (j = 1, \dots, n)$
- $K(A) = \mathcal{L}\{k_1^A, \dots, k_n^A\}$ - векторски простор колона матрице A.

Очигледно важи

$$V(A) \preceq M_{1\times n}(F) \cong F^n, \quad K(A) \preceq M_{m\times 1}(F) \cong F^m.$$

Теорема 4.23. Ако $A \sim_v B$, тада $V(A) = V(B)$
(тј. v-еквивалентне матрице имају исти простор врста).

Доказ.

$A \sim_v B \;\Rightarrow$ свака врста матрице B је добијена из врста матрице A применом $v-$ операција
$\Rightarrow$ свака врста матрице B је линеарна комбинација врста матрице A
$\Rightarrow (\forall i \in \{1, \dots, m\})\ v_i^B \in \mathcal{L}\{v_1^A, v_2^A, \dots, v_m^A\}$
$\Rightarrow (\forall i \in \{1, \dots, m\})\ v_i^B \in V(A)$
$\Rightarrow \mathcal{L}\{v_1^B, v_2^B, \dots, v_m^B\} \subseteq V(A)$
$\Rightarrow V(B) \subseteq V(A)$

$V(A) \subseteq V(B)$ (због симетричности релације $\sim_v$)
$\Rightarrow \quad V(A) = V(B)$.

Како одредити једну базу и димензију простора $V(A)$, за $A \in M_{m\times n}(F)$?

$A \neq 0 \;\Rightarrow A \sim_v B$, где је B $v-$ степенаста матрица
$\Rightarrow V(A) = V(B), \quad V(B)$ генеришу ненула врсте матрице B (јер су линеарно независне)
$\Rightarrow dimV(A) = dimV(B) =$ број ненула врста матрице B.□

Пример 4.23. Одредити једну базу и димензију простора
$U = \mathcal{L}\{(1, 2, 3, -4, 5), (-2, 0, 3, 1, 4), (-1, 2, 6, -3, -1), (0, 4, 9, -7, -6)\} \subseteq \mathbb{R}^5$.

$$dimU = dim(V(A)), \quad \text{где је } A = \begin{bmatrix} 1 & 2 & 3 & -4 & -5 \\ -2 & 0 & 3 & 1 & 4 \\ -1 & 2 & 6 & -3 & -1 \\ 0 & 4 & 9 & -7 & -6 \end{bmatrix}.$$

Матрицу A елементарним v-операцијама сводимо на v-степенасту матрицу чије ненула врсте чине базу простора $V(A)$:

$$A \underset{v}{\overset{v_{21}^2, v_{31}^1}{\sim}} \begin{bmatrix} 1 & 2 & 3 & -4 & -5 \\ 0 & 4 & 9 & -7 & -6 \\ 0 & 4 & 9 & -7 & -6 \\ 0 & 4 & 9 & -7 & -6 \end{bmatrix} \underset{v}{\overset{v_{32}^{-1}, v_{42}^{-1}}{\sim}} \begin{bmatrix} 1 & 2 & 3 & -4 & -5 \\ 0 & 4 & 9 & -7 & -6 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\Rightarrow V(A) = \mathcal{L}\big\{[1\,2\,3\,-4\,-5], [0\,4\,9\,-7\,-6]\big\}$$

$$\Rightarrow U = \mathcal{L}\big\{(1,2,3,-4,-5), (0,4,9,-7,-6)\big\}, \quad dimU = 2.$$

ТЕОРЕМА 4.24. За свако $A \in M_{m\times n}(F)$ важи

$$dimV(A) = dimK(A).$$

Доказ. Тврђење је очигледно тачно за $A = 0$.

Нека је: $A \neq 0, \quad dimV(A) = r \leq m, \quad \{B_1, \ldots, B_r\}$ једна база простора $V(A)$, где

$$B_i = [b_{i1}\, b_{i2}\, \ldots\, b_{in}] \ \ (i = 1, \ldots, r)$$

Тада је свака врста матрице A линеарна комбинација $B_1, \ldots, B_r$, тј.

$$\begin{array}{rcl} v_1^A & = & c_{11}B_1 + c_{12}B_2 + \cdots + c_{1r}B_r \\ \cdots & & \qquad\qquad\qquad\qquad , \ c_{ij} \in F, \quad tj. \\ v_m^A & = & c_{m1}B_1 + c_{m2}B_2 + \cdots + c_{mr}B_r \end{array}$$

$$\begin{array}{l} [a_{11} \ldots a_{1n}] = c_{11}[b_{11} \ldots b_{1n}] + c_{12}[b_{21} \ldots b_{2n}] + \cdots + c_{1r}[b_{r1} \ldots b_{rn}] \\ \quad \ldots \\ [a_{m1} \ldots a_{mn}] = c_{m1}[b_{11} \ldots b_{1n}] + c_{m2}[b_{21} \ldots b_{2n}] + \cdots + c_{mr}[b_{r1} \ldots b_{rn}] \end{array}$$

$$\Rightarrow \begin{array}{rcl} a_{1j} & = & c_{11}b_{1j} + c_{12}b_{2j} + \cdots + c_{1r}b_{rj} \\ & \ldots & \\ a_{mj} & = & c_{m1}b_{1j} + c_{m2}b_{2j} + \cdots + c_{mr}b_{rj}, \end{array} \quad \text{за свако } j \in \{1, \ldots, n\}$$

$$\Rightarrow \begin{array}{rcl} a_{1j} & = & c_{11}b_{1j} + c_{12}b_{2j} + \cdots + c_{1r}b_{rj} \\ & \ldots & \\ a_{mj} & = & c_{m1}b_{1j} + c_{m2}b_{2j} + \cdots + c_{mr}b_{rj}, \end{array} \quad \text{за свако } j \in \{1, \ldots, n\}$$

$$\Rightarrow k_j^A = \begin{bmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{bmatrix} = b_{1j} \underbrace{\begin{bmatrix} c_{11} \\ \vdots \\ c_{m1} \end{bmatrix}}_{=C_1} + b_{2j} \underbrace{\begin{bmatrix} c_{12} \\ \vdots \\ c_{m2} \end{bmatrix}}_{=C_2} + \cdots + b_{rj} \underbrace{\begin{bmatrix} c_{1r} \\ \vdots \\ c_{mr} \end{bmatrix}}_{=C_r} \quad (j = 1, \ldots, n)$$

$$\begin{array}{l} \Rightarrow (\forall j \in \{1, \ldots, n\})\ k_j^A \in \mathcal{L}\{C_1, \ldots, C_r\} \\ \Rightarrow \mathcal{L}\{k_1^A, \ldots, k_n^A\} \subseteq \mathcal{L}\{C_1, \ldots, C_r\} \\ \Rightarrow K(A) \subseteq \mathcal{L}\{C_1, \ldots, C_r\} \\ \Rightarrow dimK(A) \leq r \\ \Rightarrow dimK(A) \leq dimV(A) \end{array}$$

Слично, посматрањем A^T, добијамо и $dimV(A) \leq dimK(A)$. □

ДЕФИНИЦИЈА 4.26. (1) ранг0=0 (ранг нула матрице једнак је нула).

(2) Ако је $A \neq 0$ онда је $rang(A) \overset{\text{def}}{=} dimV(A) = dimK(A)$.

Из дефиниције следи да

$$rang : M_{m\times n}(F) \to \{0, 1, \ldots, min\{m, n\}\}.$$

ТЕОРЕМА 4.25. За $A, B \in M_{m\times n}(F)$ важи

$$A \sim B \quad \text{акко} \quad rangA = rangB.$$

Доказ.

$(\rightarrow)$

$A \sim B \;\Rightarrow$ матрица B се добија из A елементарним в и/или к операцијама

$\Rightarrow$ матрица B се добија из A множењем неким елементарним в-матрицама са леве и/или неким елементарним к-матрицама са десне стране

$\Rightarrow B = \underbrace{P_r \dots P_1}_{=P} A \underbrace{Q_1 \dots Q_s}_{=Q}$, где су све P_i елементарне в-матрице,

а све Q_j су елементарне к-матрице

$\Rightarrow B = PAQ$ где су P и Q регуларне матрице.

$B \sim_v AQ \;\Rightarrow\; rangB = rang(AQ)$, на основу Теореме 1.

$A \sim_k AQ \;\Rightarrow\; rang(AQ) = rangA.$

$\Rightarrow rangA = rangB.$

$(\leftarrow)$ Нека је $A \sim \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}, \quad B \sim \begin{bmatrix} I_s & 0 \\ 0 & 0 \end{bmatrix}$ (нормална форма матрица A и B).

$\Rightarrow rangA = rangI_r = r, \quad rangB = s.$

$rangA = rangB \;\Rightarrow\; r = s \;\Rightarrow\; I_r = I_s \Rightarrow A \sim B.$ □

ПРИМЕР 4.24. Одредити ранг матрице $A = \begin{bmatrix} 1 & 2 & -1 & a \\ 2 & 5 & a & -1 \\ 1 & 1 & -6 & 10 \end{bmatrix}$ у зависности од параметра $a \in \mathbb{R}$.

$$A \overset{v_{21}^{-2}, v_{31}^{-1}}{\sim_v} \begin{bmatrix} 1 & 2 & -1 & a \\ 0 & 1 & a+2 & -1-2a \\ 0 & -1 & -5 & 10-a \end{bmatrix} \overset{v_{32}^{1}}{\sim_v} \begin{bmatrix} 1 & 2 & -1 & a \\ 0 & 1 & a+2 & -1-2a \\ 0 & 0 & a-3 & 9-3a \end{bmatrix},$$

па је

(1) $rangA = 2,$ за $a = 3$
(2) $rangA = 3,$ за $a \neq 3$.

ТЕОРЕМА 4.26. За $A \in M_n(F)$ важи

$$rangA = n \quad \text{акко} \quad A \sim_v I_n.$$

Доказ.

$(\rightarrow)$ $rangA = n \;\Rightarrow A \neq 0$

$\Rightarrow A \sim_v B,\; B$ је редукована в-степенаста

$\Rightarrow rangB = rangA = n$ (по Теореми 1.)

$\Rightarrow B$ нема нула врсту

$\Rightarrow B = I_n$

$(\leftarrow)$ $A \sim_v I_n \Rightarrow V(A) = V(I_n)$ (Теорема 1.) $\Rightarrow rangA = rangI_n = n.$ □

ПОСЛЕДИЦА.

(1) $A \in M_n(F)$ је регуларна акко $rangA = n.$

(2) $A \in M_n(F)$ је сингуларна акко $rangA < n.$

Доказ. (1) A је регуларна акко $A \sim_v I_n$ акко $rangA = n.$

(2) A је сингуларна акко $A \sim_v B$, B има нула врсту акко $rangA = rangB < n.$ □

Глава 5

Системи линеарних једначина

5.1 Системи линеарних једначина, основни појмови

Нека је F поље и m, n природни бројеви.

Дефиниција 5.1. Конјункција једначина

$$(S)\quad \begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = & b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n & = & b_2 \\ & \vdots & \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & = & b_m \end{array}\quad ,\ a_{ij},\ b_i \in F\ (i = 1, \ldots, m,\ j = 1, \ldots, n)$$

се назива систем од m линеарних једначина са n непознатих над пољем F. Скалари a_{ij} се зову коефицијенти, b_i слободни чланови система (S), а $x_1, \ldots, x_n$ су непознате.

- Систем (S) је:
  - квадратни ако $m = n$ (број једначина једнак броју непознатих)
  - правоугаони ако је $m \neq n$.
- Систем (S) је:
  - хомоген ако $(b_1, \ldots, b_m) = (0, \ldots, 0)$ (сви слободни чланови су =0),
  - нехомоген ако $(b_1, \ldots, b_m) \neq (0, \ldots, 0)$ (бар један слободни члан је $\neq 0$).

Дефиниција 5.2.

- Уређена n-торка $(\xi_1, \ldots, \xi_n) \in F^n$ је решење система (S) ако $(\forall i = 1, \ldots, m) \quad a_{i1}\xi_1 + a_{i2}\xi_2 + \cdots + a_{in}\xi_n = b_i.$
- Решити систем (S) значи одредити скуп $\mathcal{R}_S \subseteq F^n$ свих његових решења.
- Систем (S) је:
  - несагласан (противречан, немогућ) ако је $\mathcal{R}_S = \emptyset$,
  - сагласан (непротивречан, конзистентан) ако је $\mathcal{R}_S \neq \emptyset$
    - $card\mathcal{R}_S = 1$- систем је одређен (има јединствено решење)
    - $card\mathcal{R}_S > 1$ - систем је неодређен.

- Хомоген систем

$$(H)\quad \begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &=& 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &=& 0 \\ &\vdots& \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &=& 0 \end{array}$$

  је увек сагласан, јер има бар једно решење $(0, \dots, 0)$ (n-торка нула).

  - решење $(0, \dots, 0)$ се зове тривијално решење хомогеног система
  - остала решења, ако постоје, називају се нетривијална.

Пример 5.1. Посматрајмо систем $ax = b$ од једне једначине, са једном непознатом, над произвољним пољем F.

- $a = 0,\ b \neq 0 \quad \Rightarrow \quad \mathcal{R}_S = \emptyset$ - систем није сагласан
- $a = 0,\ b = 0 \quad \Rightarrow \quad \mathcal{R}_S = F$ - систем је неодређен, сваки елемент поља је решење
- $a \neq 0 \quad \Rightarrow \quad \mathcal{R}_S = \{a^{-1}b\}$ - систем има јединствено решење

Теорема 5.1. Ако су $\xi = (\xi_1, \dots, \xi_n)$ и $\eta = (\eta_1, \dots, \eta_n)$ два различита решења система (S) и $\lambda \in F, \lambda \neq 0, \lambda \neq 1,$ тада је и $\lambda\xi + (1-\lambda)\eta = (\lambda\xi_1 + (1-\lambda)\eta_1, \dots, \lambda\xi_n + (1-\lambda)\eta_n)$ решење система (S) различито од претходних.

Доказ.

$$\begin{array}{ll} (\forall i = 1, \dots m) & a_{i1}(\lambda\xi_1 + (1-\lambda)\eta_1) + \cdots + a_{in}(\lambda\xi_n + (1-\lambda)\eta_n) = \\ & = \lambda(a_{i1}\xi_1 + \cdots + a_{in}\xi_n) + (1-\lambda)(a_{i1}\eta_1 + \cdots + a_{in}\eta_n) = \\ & = \lambda b_i + (1-\lambda)b_i = b_i \end{array}$$

$\Rightarrow \quad \lambda\xi + (1-\lambda)\eta$ је решење система (S).

Како је $\lambda \neq 0$ и $\lambda \neq 1$ ово решење је различито од ξ и η.

У супротном,

$$\begin{array}{rl} \lambda\xi + (1-\lambda)\eta = \xi & \Rightarrow (\lambda - 1)\xi - (\lambda - 1)\eta = 0 \\ & \Rightarrow \underbrace{(\lambda - 1)}_{\neq 0}\underbrace{(\xi - \eta)}_{\neq 0} = 0, \end{array} \qquad \text{контрадикција. } \square$$

Ако систем линеарних једначина над бесконачним пољем има два различита решења, онда их има и бесконачно много.

Теорема 5.2. Ако је $\xi = (\xi_1, \dots, \xi_n)$ решење сагласног система (S) и (H) одговарајући хомоген систем, тј.

$$(H)\quad \begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &=& 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &=& 0 \\ &\vdots& \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &=& 0 \end{array}, \quad \text{тада је} \quad \mathcal{R}_S = \mathcal{R}_H + \xi.$$

Доказ.

- Докажимо најпре $\mathcal{R}_S \subseteq \mathcal{R}_H + \xi$.

  Нека је $\eta = (\eta_1, \dots, \eta_n) \in \mathcal{R}_S$. Тада, за $\eta - \xi = (\eta_1 - \xi_1, \dots, \eta_n - \xi_n)$ и свако $i = 1, \dots, m$ важи

  $$a_{i1}(\eta_1 - \xi_1) + \dots + a_{in}(\eta_n - \xi_n) = (a_{i1}\eta_1 + \dots + a_{in}\eta_n) - (a_{i1}\xi_1 + \dots + a_{in}\xi_n) = b_i - b_i = 0$$

  тј. $\eta - \xi \in \mathcal{R}_H$, па $\eta = \underbrace{(\eta - \xi)}_{\in \mathcal{R}_H} + \xi \ \in \mathcal{R}_H + \xi$.

- Докажимо сада $\mathcal{R}_S \supseteq \mathcal{R}_H + \xi$.

  За $\eta \in \mathcal{R}_H$ лако се проверава да је $\eta + \xi$ решење система (S), тј. $\eta + \xi \in \mathcal{R}_S$. □

5.2 Елементарне трансформације система једначина. Гаусов поступак решавања

ДЕФИНИЦИЈА 5.3. Системи линеарних једначина (S) и (S') над истим пољем и са истим бројем непознатих, су еквивалентни (ознака $(S) \sim (S')$) ако имају исти скуп решења, тј. $\mathcal{R}_S = \mathcal{R}_{S'}$.

Очигледно, релација $\sim$ (еквивалентности два система једначина) је релација еквиваленције.

ДЕФИНИЦИЈА 5.4. Под елементарним операцијама система линеарних једначина подразумевамо:

- J_{ij} - размена $i-$те и j-те једначине,
- $J_i^\lambda, \lambda \neq 0$ - множење i-те једначине скаларом $\lambda \neq 0$,
- J_{ij}^λ -додавање i-тој једначини j-те једначине која је помножена скаларом λ,
- изостављање једначине облика $0x_1 + \dots + 0x_n = 0$.

Елементарне операције су инвертибилне:

$$J_{ij}^{-1} = J_{ij}, \quad (J_i^\lambda)^{-1} = J_i^{\frac{1}{\lambda}},\ \lambda \neq 0, \quad (J_{ij}^\lambda)^{-1} = J_{ij}^{-\lambda}.$$

ЛЕМА 5.1. Систем (S') добијен од система (S) применом коначног низа елементарних операција је еквивалентан систему (S).

Доказ. Довољно је доказати за случај када је (S') добијен из (S) применом једне елементарне операције.

- Ако је (S') добијен применом J_{ij} или J_i^λ тврђење је очигледно.
- Нека је (S') добијен из (S) применом J_{ij}^λ. Тада, системи (S) и (S') се разликују само у i-тој једначини, која у систему (S') гласи

  $$(a_{i1} + \lambda a_{j1})x_1 + (a_{i2} + \lambda a_{j2})x_2 + \dots + (a_{in} + \lambda a_{jn})x_n = b_i + \lambda b_j.$$

  (1) Нека је (S) сагласан и $\xi = (\xi_1, \dots, \xi_n) \in \mathcal{R}_S$. Тада

  $$\begin{aligned} &(a_{i1} + \lambda a_{j1})\xi_1 + \dots + (a_{in} + \lambda a_{jn})\xi_n = \\ &(a_{i1}\xi_1 + \dots + a_{in}\xi_n) + \lambda(a_{j1}\xi_1 + \dots + a_{jn}\xi_n) = b_i + \lambda b_j \\ &\Rightarrow \quad (\xi_1, \dots, \xi_n) \in \mathcal{R}_{S'} \\ &\Rightarrow \quad \mathcal{R}_S \subseteq \mathcal{R}_{S'}. \end{aligned}$$

(2) Ако је (S') сагласан онда је и (S) сагласан и важи $\mathcal{R}_{S'} \subseteq \mathcal{R}_S$
(следи из (1) имајући у виду да систем (S) добијамо из (S') применом инверзне елементарне операције $J_{ij}^{-\lambda}$).

(3) Ако један од система (S) или (S') није сагласан, контрапозицијом већ доказаног закључујемо да и други систем није сагласан. □

ДЕФИНИЦИЈА 5.5. Систем линеарних једначина облика

$$(ST) \qquad \begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = & b_1 \\ a_{22}x_2 + \cdots + a_{2n}x_n & = & b_2 \\ & \vdots & \\ a_{kk}x_k + \cdots + a_{kn}x_n & = & b_k \qquad a_{11}a_{22}\ldots a_{kk} \neq 0, \\ 0 & = & b_{k+1} \\ & \vdots & \\ 0 & = & b_m, \end{array}$$

се зове степенаст систем. Непознате $x_1, x_2, \ldots, x_k$ се зову главне непознате, а остале, ако постоје, су слободне непознате.

Решавање степенастог система линеарних једначина:

- Ако је $(b_{k+1}, \ldots, b_m) \neq (0, \ldots, 0)$ онда систем није сагласан, тј. $\mathcal{R}_S = \emptyset$.
- Ако је $(b_{k+1}, \ldots, b_m) = (0, \ldots, 0)$ онда је систем сагласан и разликујемо два случаја:
- ако је $k = n$ систем има јединствено решење (све непознате су главне)

  решавамо систем од последње према првој једначини:
  - $x_n = b_n/a_{nn}$.
  - Заменимо добијено x_n у претпоследњој једначини и из ње одредимо јединствено x_{n-1}.
  - Настављајући поступак одредимо и преостале непознате.
- Ако је $k < n$ тада постоје слободне непознате $\{x_{k+1}, \ldots, x_n\}$ које "пребацимо" на десну страну тако да добијамо:

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1k}x_k & = & b_1 - a_{1k+1}x_{k+1} - \cdots - a_{1n}x_n \\ a_{22}x_2 + \ldots a_{2k}x_k & = & b_2 - a_{2k+1}x_{k+1} - \cdots - a_{2n}x_n \\ & \vdots & \\ a_{kk}x_k & = & b_k - a_{kk+1}x_{k+1} - \cdots - a_{kn}x_n \end{array}$$

затим систем решимо по главним непознатим $x_1, \ldots, x_k$. Дакле, систем има бесконачно много решења, тј. неодређен је.

ТЕОРЕМА 5.3. (Гаус) Сваки систем линеарних једначина еквивалентан је неком степенастом систему.

Доказ. Не умањујући општост можемо претпоставити да је $a_{11} \neq 0$ (ако није, како је бар један коефицијент уз x_1 različitit од нуле, рецимо $a_{i1} \neq 0$, заменом прве и i-те врсте постижемо да је коефицијент уз x_1 у првој једначини различит од нуле). Примењујући $J_{21}^{-\frac{a_{21}}{a_{11}}}, \dots, J_{m1}^{-\frac{a_{m1}}{a_{11}}}$ добијамо следећи систем еквивалентан систему (S):

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &=& b_1 \\ a'_{22}x_2 + \cdots + a'_{2n}x_n &=& b'_2 \\ &\vdots& \\ a'_{m2}x_2 + \cdots + a'_{mn}x_n &=& b'_m \end{array} \text{, где } \begin{array}{rcl} a'_{ij} &=& a_{ij} - a_{1j}\frac{a_{i1}}{a_{11}} \\ b'_i &=& b_i - b_1\frac{a_{i1}}{a_{11}} \end{array}.$$

Сада, занемарујући прву једначину, поновимо поступак на систем који чине преостале једначине. Настављајући поступак добијамо степенаст систем. □

Пример 5.2.

$$(S)\quad \begin{array}{rcl} x_1 + 2x_2 + 3x_3 + 4x_4 &=& 5 \\ 2x_1 + 2x_2 - x_3 + 2x_4 &=& 6 \\ 3x_1 + 2x_2 - 5x_3 &=& \lambda \end{array} \overset{J_{21}^{-2}, J_{31}^{-3}}{\Longleftrightarrow} \begin{array}{rcl} x_1 + 2x_2 + 3x_3 + 4x_4 &=& 5 \\ -2x_2 - 7x_3 - 6x_4 &=& -4 \\ -4x_2 - 14x_3 - 12x_4 &=& \lambda - 15 \end{array}$$

$$\overset{J_{2}^{-1}, J_{32}^{-2}}{\Longleftrightarrow} \begin{array}{rcl} x_1 + 2x_2 + 3x_3 + 4x_4 &=& 5 \\ 2x_2 + 7x_3 + 6x_4 &=& 4 \\ 0 &=& \lambda - 7 \end{array}$$

- $\lambda \neq 7 \Rightarrow \mathcal{R}_S = \emptyset$
- $\lambda = 7$:

$$(S) \Leftrightarrow \begin{array}{rcl} x_1 + 2x_2 &=& -3x_3 - 4x_4 + 5 \\ 2x_2 &=& -7x_3 - 6x_4 + 4 \end{array} \Leftrightarrow \begin{array}{rcl} x_1 &=& 1 + 4x_3 + 2x_4 \\ x_2 &=& 2 - \frac{7}{2}x_3 - 3x_4 \end{array}$$

$$\mathcal{R}_S = \{(1 + 4\alpha + 2\beta, 2 - \frac{7}{2}\alpha - 3\beta, \alpha, \beta) | \alpha, \beta \in \mathbb{R}\}.$$

Последица. Сваки хомоген систем у коме је број једначина мањи од броја непознатих $(m < n)$ има и нетривијална решења.

Доказ. Свођењем хомогеног система у коме је $m < n$ на степенаст облик добија се да су све контролне једначине облика $0 = 0$ и $k < n,$ па је систем неодређен, тј. има и нетривијалних решења. □

Пример 5.3.

$$(H)\quad \begin{array}{rcl} x_1 + 2x_2 + 3x_3 + 4x_4 &=& 0 \\ 2x_1 + 2x_2 - x_3 + 2x_4 &=& 0 \\ 3x_1 + 2x_2 - 5x_3 + \lambda x_4 &=& 0 \end{array} \Leftrightarrow \begin{array}{rcl} x_1 + 2x_2 + 3x_3 + 4x_4 &=& 0 \\ 2x_2 + 7x_3 + 6x_4 &=& 0 \\ -4x_2 - 14x_3 + (\lambda + 2)x_4 &=& 0 \end{array}$$

$$\Leftrightarrow \begin{array}{rcl} x_1 + 2x_2 + 3x_3 + 4x_4 &=& 0 \\ 2x_2 + 7x_3 + 6x_4 &=& 0 \\ \lambda x_4 &=& 0 \end{array}$$

(1) За $\lambda \neq 0$: $$(H) \Leftrightarrow \begin{array}{rcl} x_1 + 2x_24 &=& -3x_3 \\ 2x_2 &=& -7x_3 \\ x_4 &=& 0 \end{array} \Leftrightarrow \begin{array}{rcl} x_1 &=& 4x_3 \\ x_2 &=& \frac{-7}{2}x_3 \\ x_4 &=& 0 \end{array},$$

$$\mathcal{R}_H = \{(4\alpha, -\frac{7}{2}\alpha, \alpha, 0) | \alpha \in \mathbb{R}\}.$$

(2) За $\lambda = 0$: $$(H) \Leftrightarrow \begin{array}{rcl} x_1 + 2x_2 &=& -3x_3 - 4x_4 \\ 2x_2 &=& -7x_3 - 6x_4 \end{array} \Leftrightarrow \begin{array}{rcl} x_1 &=& 4x_3 + 2x_4 \\ x_2 &=& -\frac{7}{2}x_3 - 3x_4 \end{array}$$

$$\mathcal{R}_H = \{(4\alpha + 2\beta, -\frac{7}{2}\alpha - 3\beta, \alpha, \beta) | \alpha, \beta \in \mathbb{R}\}.$$

5.3 Кронекер-Капелијева теорема

Систем линеарних једначина

$$(S)\qquad \begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

је еквивалентан матричној једначини

$$A \cdot X = B,$$

где је

$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$, $X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$, $B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$, па се решавање система (S) своди на решавање матричне једначине $AX = B$.

Ако је $m = n$ и A регуларна матрица, онда постоји A^{-1}, па је $A^{-1} \cdot \backslash AX = B \Leftrightarrow A^{-1}AX = A^{-1}B \Leftrightarrow I_nX = A^{-1}B \Leftrightarrow X = A^{-1}B$,

тј. матрица $A^{-1}B$ је јединствено решење матричне једначине $AX = B$.

Пример 5.4. Систем једначина

$$\begin{aligned} x_1 + 2x_2 - 3x_3 &= 8 \\ x_1 \ \ + 2x_3 &= -1 \\ -2x_2 + x_3 &= -5 \end{aligned}$$

је еквивалентан матричној једначини $AX = B$, где је

$$A = \begin{bmatrix} 1 & 2 & -3 \\ 1 & 0 & 2 \\ 0 & -2 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}, \quad B = \begin{bmatrix} 8 \\ -1 \\ -5 \end{bmatrix}$$

$detA = 8 \neq 0 \Rightarrow A$ је регуларна $\Rightarrow \quad A^{-1} = \frac{1}{8}\begin{bmatrix} 4 & 4 & 4 \\ -1 & 1 & -5 \\ -2 & 2 & -2 \end{bmatrix} \Rightarrow X = A^{-1}B =$

$$\frac{1}{8}\begin{bmatrix} 4 & 4 & 4 \\ -1 & 1 & -5 \\ -2 & 2 & -2 \end{bmatrix}\begin{bmatrix} 8 \\ -1 \\ -5 \end{bmatrix} = \frac{1}{8}\begin{bmatrix} 8 \\ 16 \\ -8 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ -1 \end{bmatrix}$$

$$\Rightarrow \qquad \mathcal{R}_S = \{(1, 2, -1)\}.$$

Систем (S) је потпуно одређен матрицама A и B, тј. матрицом

$$[A|B] = \left[\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{array}\right]$$

коју називамо проширена матрица система.

Тада, Гаусов метод елиминације непознатих матрично описујемо сводећи проширену матрицу $[A|B]$ система (S) на v-еквивалентну матрицу степенасту по врстама.

Ако пак матрицу $[A|B]$ сведемо на редуковану v-степенасту матрицу, добијамо матрични опис једне модификације Гаусс-ове методе, тзв. Гаусс-Јордан-ове методе редукције. На овај начин се добија v-степенаст систем који је већ решен, наравно уколико је сагласан.

ПРИМЕР 5.5. Решити над пољем $\mathbb{R}$ систем једначина

$$(S)\quad \begin{array}{rcl} x_1 + 2x_2 + 3x_3 + 4x_4 & = & 5 \\ 2x_1 + 2x_2 - x_3 + 2x_4 & = & 6 \\ 3x_1 + 2x_2 - 5x_3 & = & \lambda \end{array}, \quad \lambda \in \mathbb{R}.$$

$$[A|B] = \left[\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & -1 & 2 & 6 \\ 3 & 2 & -5 & 0 & \lambda \end{array}\right] \overset{v_{21}^{-2}, v_{31}^{-3}}{\sim}_v \left[\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 5 \\ 0 & -2 & -7 & -6 & -4 \\ 0 & -4 & -14 & -12 & \lambda - 15 \end{array}\right]$$

$$\overset{v_{32}^{-2}, v_{2}^{-1}}{\sim}_v \left[\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 5 \\ 0 & 2 & 7 & 6 & 4 \\ 0 & 0 & 0 & 0 & \lambda - 7 \end{array}\right],$$

па је систем (S) еквивалентан степенастом систему

$$\begin{array}{rcl} x_1 + 2x_2 + 3x_3 + 4x_4 & = & 5 \\ 2x_2 + 7x_3 + 6x_4 & = & 4 \\ 0 & = & \lambda - 7 \end{array}.$$

Матрицу $[A|B]$ можемо свести и на еквивалентну редуковану v-степенасту матрицу:

$$[A|B] \overset{v_{12}^{-1}, v_{2}^{\frac{1}{2}}}{\sim}_v \left[\begin{array}{cccc|c} 1 & 0 & -4 & -2 & 1 \\ 0 & 1 & \frac{7}{2} & 3 & 2 \\ 0 & 0 & 0 & 0 & \lambda - 7 \end{array}\right] \text{ – редукована в-степенаста матрица}$$

Ово је проширена матрица система

$$\begin{array}{ccccc} x_1 & & -4x_3 & -2x_4 & = & 1 \\ & x_2 & +\frac{7}{2}x_3 & +3x_4 & = & 2 \\ & & & 0 & = & \lambda - 7 \end{array}.$$

Систем је сагласан за $\lambda = 7$ и решење је

$$\begin{array}{rcl} x_1 & = & 1 + 4x_3 + 2x_4 \\ x_2 & = & 2 - \frac{7}{2}x_3 - 3x_4 \\ & & x_3, x_4 \in \mathbb{R} \text{ (слободне непознате)} \end{array}$$

тј.

$$\mathcal{R}_S = \{(1 + 4\alpha + 2\beta, 2 - \frac{7}{2}\alpha - 3\beta, \alpha, \beta) | \alpha, \beta \in \mathbb{R}\}$$

Нека је

$$(S)\quad \begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = & b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n & = & b_2 \\ & \vdots & \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & = & b_m \end{array}$$

$$k_1^A = \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{bmatrix}, \quad k_2^A = \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{bmatrix}, \ldots, \; k_n^A = \begin{bmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{bmatrix}$$ колоне матрице система $A = [a_{ij}]$, тада

$$(S) \quad \Leftrightarrow \quad x_1 k_1^A + \cdots + x_n k_n^A = B,$$

тј. (S) је сагласан акко B је линеарна комбинација колона матрице A.

ТЕОРЕМА 5.4. Теорема (Cronecker-Capelli) Систем једначина $A\cdot X = B$ је сагласан акко је $rangA = rang[A|B]$.

Доказ.

$$\begin{array}{lcl}
(S) \text{ је сагласан} & \Leftrightarrow & \mathcal{R}_S \neq \emptyset \\
 & \Leftrightarrow & (\exists(\xi_1,\dots,\xi_n)\in F^n)\quad \xi_1\cdot k_1^A+\cdots+\xi_n\cdot k_n^A = B \\
 & \Leftrightarrow & \mathcal{L}\{k_1^A,\dots,k_n^A\} = \mathcal{L}\{k_1^A,\dots,k_n^A,B\} \\
 & \Leftrightarrow & dim\mathcal{L}\{k_1^A,\dots,k_n^A\} = dim\mathcal{L}\{k_1^A,\dots,k_n^A,B\} \\
 & & ((\leftarrow) \text{ следи из } \mathcal{L}\{k_1^A,\dots,k_n^A\} \preceq \mathcal{L}\{k_1^A,\dots,k_n^A,B\}) \\
 & \Leftrightarrow & rangA = rang[A|B]\square
\end{array}$$

Нека је

$$(H)\qquad \begin{array}{rcl}
a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n & = & 0 \\
a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n & = & 0 \\
 & \vdots & \\
a_{m1}x_1+a_{m2}x_2+\cdots+a_{mn}x_n & = & 0
\end{array}\quad ,\quad A = [a_{ij}]_{m\times n}.$$

ТЕОРЕМА 5.5. Хомоген систем једначина (H) са n непознатих има нетривијална решења акко $rangA < n$.

Доказ.

$$\begin{array}{l}
(H) \text{ има нетривијална решења} \\
\Leftrightarrow (\exists(\xi_1,\dots,\xi_n)\in F^n)\ (\xi_1\cdot k_1^A+\cdots+\xi_n\cdot k_n^A = 0 \wedge (\xi_1,\dots,\xi_n)\neq(0,\dots,0)) \\
\Leftrightarrow \{k_1^A,\dots,k_n^A\} \text{ је линеарно зависан скуп вектора} \\
\Leftrightarrow dim\mathcal{L}\{k_1^A,\dots,k_n^A\} < n \\
\Leftrightarrow rangA < n\square
\end{array}$$

ТЕОРЕМА 5.6. Скуп решења хомогеног система линеарних једначина $\mathcal{R}_H$ је потпростор векторског простора F^n и $dim\mathcal{R}_H = n - rangA$, где је A матрица система (H).

Доказ.

- Докажимо најпре да је $\mathcal{R}_H \preceq F^n$.
  - $\mathcal{R}_H \neq \emptyset$ (јер (H) има тривијално решење (0,. . . ,0))
  -

    $$\begin{array}{l}
    (\xi_1,\dots,\xi_n),(\eta_1,\dots,\eta_n)\in\mathcal{R}_H,\ \lambda,\mu\in F \\
    \Rightarrow \lambda(\xi_1,\dots,\xi_n)+\mu(\eta_1,\dots,\eta_n) = (\lambda\xi_1+\mu\eta_1,\dots,\lambda\xi_n+\mu\eta_n) \\
    \Rightarrow (\forall i=\overline{1,n})\ a_{i1}(\lambda\xi_1+\mu\eta_1)+\cdots+a_{in}(\lambda\xi_n+\mu\eta_n) = \\
    \qquad\qquad = \lambda\underbrace{(a_{i1}\xi_1+\cdots+a_{in}\xi_n)}_{=0}+\mu\underbrace{(a_{i1}\eta_1+\cdots+a_{in}\eta_n)}_{=0} = 0 \\
    \Rightarrow \lambda(\xi_1,\dots,\xi_n)+\mu(\eta_1,\dots,\eta_n)\in\mathcal{R}_H
    \end{array}$$

- Докажимо да је $dim\mathcal{R}_H = n - rangA$, где је A матрица система (H).

  Нека је $f_A : M_{n\times 1}(F)\to M_{m\times 1}(F),\quad f_A(X) \overset{\text{def}}{=} A\cdot X$, за $X\in M_{n\times 1}(F)$.

Тада

$$\begin{aligned} kerf_A &= \big\{X \in M_{n\times 1}(F)\big|f_A(X) = 0\big\} = \big\{X \in M_{n\times 1}(F)\big|AX = 0\big\} \cong \mathcal{R}_H \\ Imf_A &= \mathcal{L}\left\{f_A\left(\begin{bmatrix}1\\ \vdots\\ 0\end{bmatrix}\right), \dots, f_A\left(\begin{bmatrix}0\\ \vdots\\ 1\end{bmatrix}\right)\right\} = \mathcal{L}\{k_1^A, \dots, k_n^A\}\end{aligned}$$

$$n = dimM_{n\times 1}(F) = dim(kerf_A) + dim(Imf_A) = dim\mathcal{R}_H + rangA$$
$$\Rightarrow dim\mathcal{R}_H = n - rangA\square$$

Последица.

(1) Ако $m < n$ онда хомогени систем (H) има нетривијална решења.

(2) Квадратни хомоген систем (H) има нетривијална решења акко $detA = 0$.

Доказ.

(1) $m < n \ \Rightarrow\ rangA \leq min\{m, n\} < n \ \Rightarrow dim\mathcal{R}_H = n - rangA > 0$, па систем има нетривијална решења.

(2) Ако је $m = n$ онда систем има нетривијална решења акко $dim\mathcal{R}_H > 0$ акко $rangA < n$ акко $detA = 0$. $\square$

5.4 Крамерове формуле

Нека је дат квадратни систем линеарних једначина

$$(KS) \qquad \begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &= b_n, \end{aligned} \quad .$$

Нека је $A = [a_{ij}] \in M_n(F)$ матрица система, $D = detA$ њена детерминанта и за свако $i \in \{1, \dots, n\}$ нека је D_{x_i} детерминанта добијена из D заменом $i-$те колоне колоном слободних чланова, тј.

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

$$D_{x_1} = \begin{vmatrix} b_1 & a_{12} & \dots & a_{1n} \\ b_2 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_n & a_{n2} & \dots & a_{nn} \end{vmatrix}, \dots, D_{x_n} = \begin{vmatrix} a_{11} & a_{12} & \dots & b_1 \\ a_{21} & a_{22} & \dots & b_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & b_n \end{vmatrix}.$$

Теорема 5.7. Теорема (Cramer) Квадратни систем линеарних једначина (KS) има јединствено решење акко $D \neq 0$ и тада важи

$$(x_1, \dots, x_n) = (D_{x_1}/D, \dots, D_{x_n}/D).$$

Доказ. Свакако важи

$$(KS) \Leftrightarrow AX = B,$$

где је $B = [b_i] \in M_{n\times 1}(F)$ матрица слободних чланова, а $X = [x_i] \in M_{n\times 1}(F)$ матрица непознатих.

($\rightarrow$) Нека је $\xi = (\xi_1, \dots, \xi_n)$ решење (јединствено) система (KS). Тада је систем (KS) сагласан и важи

$$\mathcal{R}_{KS} = \mathcal{R}_H + \xi \Rightarrow \mathcal{R}_H = \{(0, \dots 0)\} \Rightarrow dim\mathcal{R}_H = 0 \Rightarrow rangA = n \Rightarrow D \neq 0.$$

($\leftarrow$) Нека је $D \neq 0$. Тада постоји A^{-1} и важи

$$\begin{aligned} X &= A^{-1}\cdot B = \tfrac{1}{D}adjA\cdot B = \tfrac{1}{D}\begin{bmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & A_{22} & \dots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \dots & A_{nn}\end{bmatrix}^T \cdot \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n\end{bmatrix} \\ &= \tfrac{1}{D}\begin{bmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1n} & A_{2n} & \dots & A_{nn}\end{bmatrix} \cdot \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n\end{bmatrix} \\ &= \tfrac{1}{D}\begin{bmatrix} b_1A_{11} + b_2A_{21} + \dots + b_nA_{n1} \\ \vdots \\ b_1A_{1n} + b_2A_{2n} + \dots + b_nA_{nn}\end{bmatrix} = \tfrac{1}{D}\begin{bmatrix} D_{x_1} \\ \vdots \\ D_{x_n}\end{bmatrix} = \begin{bmatrix} \frac{D_{x_1}}{D} \\ \vdots \\ \frac{D_{x_n}}{D}\end{bmatrix} \end{aligned}$$

$$\Rightarrow \quad x_1 = \tfrac{D_{x_1}}{D}, x_2 = \tfrac{D_{x_2}}{D}, \dots, x_n = \tfrac{D_{x_n}}{D}. \ \square$$

За нехомоген систем (KS):

- $D \neq 0 \Rightarrow \mathcal{R}_{KS} = \{(D_{x_1}/D, \dots, D_{x_n}/D)\}$ (јединствено решење);
- $D = 0, (\exists i \in \{1, \dots, n\})\ D_{x_i} \neq 0 \Rightarrow \mathcal{R}_{KS} = \emptyset$ (систем није сагласан);

  (Ако $(\xi_1, \dots, \xi_n) \in \mathcal{R}_{KS}$, $D = 0$ онда, применом особина детерминанти добијамо

$$\begin{aligned} D_{x_i} &= \begin{vmatrix} a_{11} & \dots & b_1 & \dots & a_{1n} \\ a_{21} & \dots & b_2 & \dots & a_{2n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \dots & b_n & \dots & a_{nn}\end{vmatrix} = \begin{vmatrix} a_{11} & \dots & \sum_{j=1}^n a_{1j}\xi_j & \dots & a_{1n} \\ a_{21} & \dots & \sum_{j=1}^n a_{2j}\xi_j & \dots & a_{2n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \dots & \sum_{j=1}^n a_{nj}\xi_j & \dots & a_{nn}\end{vmatrix} = \\ &= \sum_{j=1}^n \begin{vmatrix} a_{11} & \dots & a_{1j}\xi_j & \dots & a_{1n} \\ a_{21} & \dots & a_{2j}\xi_j & \dots & a_{2n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nj}\xi_j & \dots & a_{nn}\end{vmatrix} = \sum_{j=1}^n \xi_j \begin{vmatrix} a_{11} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & \dots & a_{2j} & \dots & a_{2n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nj} & \dots & a_{nn}\end{vmatrix} \\ &= \xi_1\cdot 0 + \xi_2\cdot 0 + \dots + \xi_i\cdot D + \dots \xi_n\cdot 0 = \xi_i\cdot 0 = 0 \end{aligned}$$

  (за $j \neq i$ детерминанта у горњој суми има две једнаке колоне, па је =0, само за $j = i$ добија се управо D).

  Дакле, $D_{x_i} = 0$, за свако $i = 1, \dots, n$, супротно претпоставци.

- $D = D_{x_1} = \dots = D_{x_n} = 0 \Rightarrow$ систем или нема решења или има бесконачно много решења (Крамерова теорема не даје одговор).

За хомоген квадратни систем

$$(KH)\quad \begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= 0 \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &= 0 \end{aligned}$$

важи $D_{x_1} = \cdots = D_{x_n} = 0$, па је:

- $D \neq 0 \Rightarrow \mathcal{R}_{KS} = \{(0, \ldots, 0)\}$ (само тривијално решење),
- $D = 0 \Rightarrow$ систем (KH) има и нетривијална решења.

НАПОМЕНА. Због гломазног рачуна, Крамерова теорема има већи теоријски, него практични значај. У пракси се обично, за $n \geq 4$, примењују друге методе.

ПРИМЕР 5.6. Решити над пољем $\mathbb{R}$ систем једначина

$$\begin{array}{rcl} ax + y + z &=& 1 \\ x + ay + z &=& 1 \\ x + y + az &=& 1 \end{array}, \; a \in \mathbb{R}.$$

$$D = \begin{vmatrix} a & 1 & 1 \\ 1 & a & 1 \\ 1 & 1 & a \end{vmatrix} = (a-1)^2(a+2),\; D_x = \begin{vmatrix} 1 & 1 & 1 \\ 1 & a & 1 \\ 1 & 1 & a \end{vmatrix} = (a-1)^2,$$

$$D_y = \begin{vmatrix} a & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & a \end{vmatrix} = (a-1)^2,\; D_z = \begin{vmatrix} a & 1 & 1 \\ 1 & a & 1 \\ 1 & 1 & 1 \end{vmatrix} = (a-1)^2$$

- $a \neq 1, a \neq -2 \Rightarrow D \neq 0 \Rightarrow$ систем има јединствено решење
  $\mathcal{R}_S = \{(\frac{D_x}{D}, \frac{D_y}{D}, \frac{D_z}{D})\} = \{(\frac{1}{a+2}, \frac{1}{a+2}, \frac{1}{a+2})\}$
- $a = 1 \Rightarrow D = D_x = D_y = D_z = 0 \Rightarrow \quad x + y + z = 1$
  $\Rightarrow \mathcal{R}_S = \{(1 - y - z, y, z) | y, z \in \mathbb{R}\}$ - бесконачно много решења
- $a = -2 \Rightarrow D = 0,\; D_x = 9 \Rightarrow\; \mathcal{R}_S = \emptyset$ - систем није сагласан

ПРИМЕР 5.7. Решити над пољем $\mathbb{R}$ систем једначина

$$\begin{array}{rcl} ax + y + z &=& 1 \\ x + ay + z &=& 0 \\ x + y + az &=& 2 \end{array}, \; a \in \mathbb{R}.$$

$$D = (a-1)^2(a+2), \quad D_x = (a-1)^2, \quad D_y = 3(1-a), \quad D_z = (2a+1)(a-1)$$

- $a \neq 1, a \neq -2 :\; D \neq 0 \Rightarrow$ систем има јединствено решење $\mathcal{R}_S = \{(\frac{D_x}{D}, \frac{D_y}{D}, \frac{D_z}{D})\} = \{(\frac{1}{a+2}, \frac{3}{(a+2)(1-a)}, \frac{2a+1}{(a+2)(a-1)})\}$
- $a = -2 :\; D = 0,\; D_x = 9 \neq 0 \Rightarrow$ систем није сагласан
- $a = 1 : D = D_x = D_y = D_z = 0,$ али ипак систем није сагласан!