BUDAPESTI MŰSZAKI
MATEMATIKA
ÉS GAZDASÁGTUDOMÁNYI
INTÉZET
EGYETEM

Alkalmazott algebra

BMETE90MX57 (FELSŐBB MATEMATIKA INFORMATIKUSOKNAK)

Algebrai struktúrák, vektorterek

SKALÁROK, VEKTOROK, MÁTRIXOK

Wettl Ferenc

ALGEBRA TANSZÉK

Ismeretek, képességek, célok

- Test, gyűrű, vektortér felismerése
- Számolás véges testekkel
- Mátrixszorzás, lineáris leképezés
- Vektorterek izomorfizmusa

Bevezetés

Rövidítések, jelölések

- **Rövidítések:** **D**efiníció, **J**elölés, **Á**llítás, **T**étel, **B**izonyítás, **L**emma, **P**élda, **F**eladat, **M**egoldás, **m**egjegyzés
  L! Legyen, **Amh** Azt mondjuk hogy, **Tfh** Tegyük fel hogy
- **Számhalmazok:** $\mathbb{R}$ valós, $\mathbb{N}$ természetes, $\mathbb{N}^+$ pozitív egész, $\mathbb{Q}$ racionális, $\mathbb{Z}$ egész, $\mathbb{C}$ komplex, $\mathbb{F}_q = \mathrm{GF}(q)$ a q elemű véges test

D L! H halmaz, H^n = a H elemeiből képzett rendezett elem-n-esek halmaza, azaz $H^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in H, i = 1, 2, \ldots, n\}$.

D *R reláció a H halmazon*: a H rendezett párjai egy részhalmaza, azaz $R \subseteq H^2$.

J ha $(a, b) \in R$, akkor $a\ R\ b$

P $H = \{1, 2, 3\}$, $'<' = \{(1, 2), (1, 3), (2, 3)\} \subset H^2$,
azaz $1 < 2$, $1 < 3$, $2 < 3$.

Ekvivalenciareláció

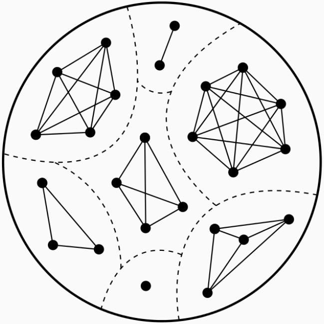
D A H halmazon értelmezett R reláció ekvivalenciareláció, ha $\forall a, b, c \in H$ elemre
(1) $a\ R\ a$ (reflexív),
(2) ha $a\ R\ b$, akkor $b\ R\ a$ (szimmetrikus),
(3) ha $a\ R\ b$, $b\ R\ c$, akkor $a\ R\ c$ (tranzitív).

F Melyik ekvivalenciareláció az alábbiak közül? egyenlőség, $<$, párhuzamosság, $\leqslant$, évfolyamtárs, ismerős, felmenő.

M egyenlőség, párhuzamosság, (évfolyamtárs,) a többi nem.

Ekvivalenciareláció és osztályozás

T Minden H-n értelmezett R ekvivalenciareláció megad H-n egy osztályozást, azaz H-t diszjunkt részhalmazok – ún. ekvivalenciaosztályoknak – uniójára bontja.



(ábra a wikipédiából)

Algebrai struktúrák

Algebrai struktúrák

Számok: test és gyűrű

Test – számolunk, mint a valós számokkal

D Egy legalább kételemű $\mathbb{F}$ halmazt (jelölje e két elemet 0 és 1) testnek nevezünk, ha értelmezve van $\mathbb{F}$ elempárjain egy összeadás és egy szorzás nevű bináris művelet, melyekre bármely $a, b, c \in \mathbb{F}$ elemekre és bármely $d \in \mathbb{F} \setminus 0$ elemre

$a + b = b + a$	$ab = ba$	kommutativitás
$a + (b + c) = (a + b) + c$	$a(bc) = (ab)c$	asszociativitás
$0 + a = a$	$1a = a$	semleges elemek
$\exists x \in \mathbb{F} : a + x = 0$	$\exists y \in \mathbb{F} : dy = 1$	additív/multipl. inverz
$(a + b)c = ac + bc$		disztributivitás

P $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$

P Véges testek: $\mathbb{Z}_p$ (prím modulusú maradékosztályok teste, más jelölések: $\mathbb{F}_p$, $\mathrm{GF}(p)$), $\mathrm{GF}(q)$, ahol q prímhatvány.

Gyűrű – számolunk, mint az egészekkel

D Ha a testnél definiált szorzás csak asszociatív, gyűrűről, ha kommutatív is, kommutatív gyűrűről, ha az asszociativitás mellett van egységeleme is, egységelemes gyűrűről beszélünk.

P Minden test gyűrű.

P $\mathbb{Z}$ egységelemes kommutatív gyűrű, $\mathbb{N}$ nem gyűrű.

P A páros számok kommutatív gyűrűt alkotnak, de ez nem egységelemes.

P A modulo m maradékosztályok $\mathbb{Z}_m$ struktúrája egységelemes kommutatív gyűrű, és pontosan akkor test, ha m prím.

P Az $\mathbb{F}$ test fölötti együtthatós polinomok egységelemes kommutatív gyűrűt alkotnak, jelölés: $\mathbb{F}[x]$.

Maradékosztály-test

$\mathbb{Z}_2 = \mathbb{F}_2 = \mathrm{GF}(2)$:

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

$\mathbb{Z}_3 = \mathbb{F}_3 = \mathrm{GF}(3)$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_5 = \mathbb{F}_5 = \mathrm{GF}(5)$:

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

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Maradékosztály-gyűrű

$\mathbb{Z}_6$ gyűrű:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

m Véges testeket és gyűrűket széles körben alkalmazza a kódelmélet és a kriptográfia, a matematikán belül a kombinatorikában, a racionális test fölötti polinomok faktorizációjában, vagy épp a nagy Fermat-tétel bizonyításában.

Prímhatványrendű testek

m $\mathrm{GF}(4)$: választunk egy $\mathbb{F}_2$ fölötti másodfokú irreducibilis (felbonthatatlan) polinomot, pl. x^2+x+1.
Ha egy másod vagy harmadfokú polinom felbontható, akkor van elsőfokú tényezője, így van gyöke, de ennek nincs, mert 0-ban és 1-ben sem 0 az értéke.

- A $\mathrm{GF}(4)$ elemei $0, 1, x, x+1$ (a legföljebb elsőfokú polinomok), és a számolás köztük modulo x^2+x+1 történik:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

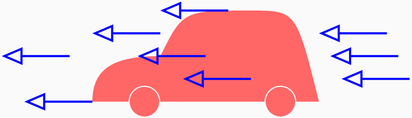
$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

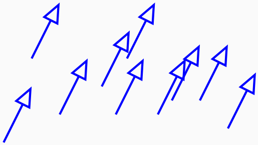
m $\mathrm{GF}(2^n)$ konstrukciója hasonlóan megy egy $\mathrm{GF}(2)$ fölötti n-edfokú, irreducibilis polinommal.

Algebrai struktúrák

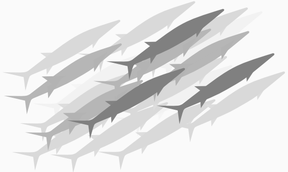
Vektortér

Szabad vektor





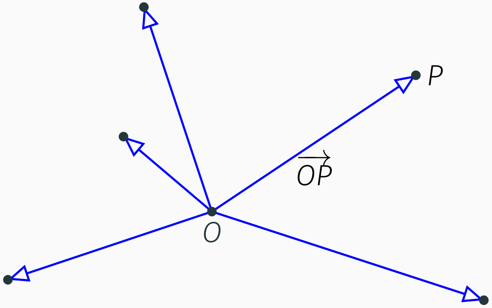
- Ha az irányított szakasz a hal, a vektor a halraj.



D *R*: két irányított szakasz ekvivalens, ha egyik a másikba „tolható". Ekkor a vektorok az ekvivalenciaosztályok.

Origó

- A közös kezdőpont



- A pontok és a vektorok közt kölcsönösen egyértelmű megfeleltetés: egy P pontnak az $\overrightarrow{OP}$ vektor felel meg, az origónak a nullvektor.
- Tehát az $(x_1, x_2, \ldots, x_n)$ egy pontot és egy vektort is jelölhet.

D

Vektortér

A $\mathcal{V}$ halmazt $\mathbb{F}$ fölötti vektortérnek nevezzük (jel.: $\mathcal{V}_{\mathbb{F}}$), ha tartalmaz egy $\mathbf{0}$-val jelölt elemet, és értelmezve van rajta egy összeadás és egy skalárral szorzás művelet, melyekre tetszőleges $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{V}$ és $c, d \in \mathbb{F}$ esetén

(A1)	$\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$	az összeadás kommutatív
(A2)	$(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$	az összeadás asszociatív
(A3)	$\mathbf{u} + \mathbf{0} = \mathbf{u}$	az összeadás nulleleme
(M1)	$(cd)\mathbf{u} = c(d\mathbf{u})$	a két szorzás kompatibilis
(M2)	$1\mathbf{u} = \mathbf{u}$	a test egységelemével
(M3)	$0\mathbf{u} = \mathbf{0}$	a test nullelemével
(D1)	$c(\mathbf{u} + \mathbf{v}) = c\mathbf{u} + c\mathbf{v}$	disztributív
(D2)	$(c + d)\mathbf{u} = c\mathbf{u} + d\mathbf{u}$	disztributív.

Vektortér tulajdonságai

m Összeadáson egy $\mathcal{V} \times \mathcal{V} \to \mathcal{V}; (\mathbf{u}, \mathbf{v}) \mapsto \mathbf{u} + \mathbf{v}$, míg skalárral való szorzáson egy $\mathbb{F} \times \mathcal{V} \to \mathcal{V}; (c, \mathbf{u}) \mapsto c\mathbf{u}$ leképezést értünk.

m (A2) $\rightsquigarrow$ többtagú összeget nem kell zárójelezni $\rightsquigarrow$ az $\mathbf{u} + \mathbf{v} + \mathbf{w}$ jelölés egyértelmű.

Á (M3) kicserélhető a következő tulajsonsággal

$$\text{(A4)} \quad \forall \mathbf{u} \in \mathcal{V}\ \exists \mathbf{v} \in \mathcal{V}\colon\ \mathbf{u} + \mathbf{v} = \mathbf{0} \quad \text{additív inverz létezése (J: } -\mathbf{u}\text{)}$$

B (M3) $\Rightarrow$ (A4): tetszőleges $\mathbf{u}$-ra $\mathbf{0} = 0\mathbf{u} = (1 - 1)\mathbf{u} = \mathbf{u} + \mathbf{v}$, ahol $\mathbf{v} = (-1)\mathbf{u}$.

(A4) $\Rightarrow$ (M3): $0\mathbf{u} = (0 + 0)\mathbf{u} = 0\mathbf{u} + 0\mathbf{u} \rightsquigarrow$

$\mathbf{0} = 0\mathbf{u} + \mathbf{v} = (0\mathbf{u} + 0\mathbf{u}) + \mathbf{v} = 0\mathbf{u} + (0\mathbf{u} + \mathbf{v}) = 0\mathbf{u} + \mathbf{0} = 0\mathbf{u}$.

m A vektortér definíciójára (A1)–(A4), (M1)–(M2), (D1)–(D2) is használható (ált. így szokták).

Példák vektorterekre

Á $\mathcal{V} = \{\mathbf{0}\}$ bármely test fölött vektortér. Ezt nevezzük zérustérnek.

P $\mathbb{F}^n$ vektortér $\mathbb{F}$ fölött a szokásos vektorműveletekkel.
Speciálisan $\mathbb{F}^1$ (azaz maga $\mathbb{F}$) is $\mathbb{F}$ fölötti vektortér.

P az $\mathbb{F}$ fölötti $m \times n$-es mátrixok $\mathbb{F}^{m\times n}$ tere,
a polinomok $\mathbb{F}[x]$ tere, $\mathbb{F}[x]_n = \{f \in \mathbb{F}[x] \mid \deg f \leqslant n\}$,
$\mathbb{F}[[x]] = \{\sum_{n=0}^{\infty} a_n x^n\}$ a formális hatványsorok

P $\mathcal{C}^0_{\mathbb{R}}$, és $\mathcal{C}^1_{\mathbb{R}}$ az $\mathbb{R}$-en folytonos, illetve folytonosan diffható fv-ek

P $\mathbb{R}^{\mathbb{N}}$, a végtelen valós sorozatok

P $\mathbb{R}^\infty$: azon $\mathbb{R}^{\mathbb{N}}$-beliek, ahol véges sok elemet kivéve $\forall$ elem 0

T Függvényterek L! $X \neq \emptyset$ tetszőleges halmaz, $\mathbb{F}$ test, $\mathcal{V}$ egy $\mathbb{F}$ fölötti vektortér, $\mathbb{F}^X := \{X \to \mathbb{F}\ \text{ függvények}\}$,
$\mathcal{V}^X := \{X \to \mathcal{V}\ \text{ függvények}\}$. $\mathbb{F}^X$ és $\mathcal{V}^X$ vektortér $\mathbb{F}$ fölött a szokásos műveletekkel: $(f+g)(x) = f(x) + g(x)$, $(cf)(x) = cf(x)$ minden $x \in X$-re, ahol a zérusfüggvény a nullelem.

Altér

D $\mathcal{U} \subseteq \mathcal{V}$ altere $\mathcal{V}$-nek, ha nem üres és zárt a vektorösszeadás és skalárral szorzásra nézve. Jelölés: $\mathcal{U} \leqslant \mathcal{V}$.

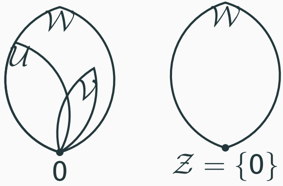
Á Minden altérnek eleme a nullvektor és ha $\mathbf{v} \in \mathcal{V}$, akkor $-\mathbf{v} \in \mathcal{V}$.

P A zérustér és $\mathcal{V}$ is alterek: $\{\mathbf{0}\} \leqslant \mathcal{V}$, $\mathcal{V} \leqslant \mathcal{V}$.

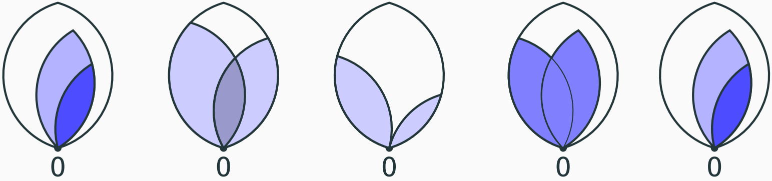
P $\mathbb{R}^3$ alterei: zérustér, origón átmenő egyenes/sík vektorai, $\mathbb{R}^3$

Á $\mathbb{F}[x]_n \leqslant \mathbb{F}[x] \leqslant \mathbb{F}[[x]]$, $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \leqslant \mathbb{R}_{\mathbb{Q}}$, $\mathcal{C}^1_{\mathbb{R}} \leqslant \mathcal{C}^0_{\mathbb{R}}$)

Levéldiagram



- Altér altere altér, azaz ha $\mathcal{U} \leqslant \mathcal{V}$, és $\mathcal{W} \leqslant \mathcal{U}$, akkor $\mathcal{W} \leqslant \mathcal{V}$.
- Alterek metszete altér: $\mathcal{U} \cap \mathcal{V} = \mathcal{W}$.
- Két altér uniója pontosan akkor altér, ha egyikük altere a másiknak.



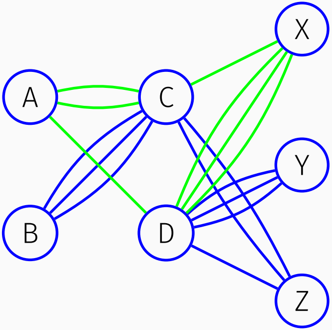
Mátrixok, lineáris leképezések

Táblázatok szorzata

P Az alábbi két táblázat azt mutatja, hogy az A és B városokból hány különböző autópálya vezet közvetlenül a C és D városokba, illetve a C és D városokból az X, Y és Z városokba.

	C	D
A	2	1
B	3	0

	X	Y	Z
C	1	0	2
D	3	3	1



	X	Y	Z
C	1	0	2
D	3	3	1

	C	D
A	2	1
B	3	0

	X	Y	Z
A	5	3	5
B	3	0	6

Mátrixszorzás

$$
\begin{array}{cc}
 & \begin{bmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{tj} \end{bmatrix} \\
\begin{bmatrix} \\ a_{i1} & a_{i2} & \dots & a_{it} \\ \\ \end{bmatrix} & \begin{bmatrix} \\ c_{ij} \\ \\ \end{bmatrix}
\end{array}
$$

A $m \times s$ **B** $t \times n$

feltéve, hogy $s = t$

C $=$ **AB** típusa $m \times n$

$$c_{ij} = \sum_{k=1}^{t} a_{ik} b_{kj} = \mathbf{a}_{i*} \cdot \mathbf{b}_{*j}$$

Lineáris helyettesítések kompozíciója

P Írjuk fel a következő két lineáris helyettesítés egymás után való elvégzésével, azaz kompozíciójával kapott lineáris helyettesítés egyenleteit!

$$\begin{aligned} a &= 2c + d \qquad & c &= x + 2z \\ b &= 3c & d &= 3x + 3y + z \end{aligned}$$

M A következőt kapjuk:

	x	y	z
c	1	0	2
d	3	3	1

$$\begin{aligned} a &= 5x + 3y + 5z \\ b &= 3x + 6z \end{aligned}$$

táblázatosítva:

	c	d
a	2	1
b	3	0

	x	y	z
a	5	3	5
b	3	0	6

Mátrix és vektor szorzata

m Az föntiek így is írhatók:

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 3 & 0 \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix}, \quad \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 \\ 3 & 3 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \quad \rightsquigarrow$$

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 3 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 2 \\ 3 & 3 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 5 & 3 & 5 \\ 3 & 0 & 6 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

Á L! $\mathbf{A} \in \mathbb{F}^{m\times n}$, ekkor az $A : \mathbb{F}^n \to \mathbb{F}^m; \mathbf{x} \mapsto \mathbf{Ax}$ mátrixleképezés a következő két tulajdonsággal rendelkezik:

- $\forall \mathbf{x} \in \mathbb{F}^n,\ c \in \mathbb{F} : A(c\mathbf{x}) = cA(\mathbf{x})$ (homogén)
- $\forall \mathbf{x}, \mathbf{y} \in \mathbb{F}^n : A(\mathbf{x} + \mathbf{y}) = A(\mathbf{x}) + A(\mathbf{y})$ (additív)

Lineáris leképezések

Lineáris leképezés

D Legyen $\mathcal{V}$ és $\mathcal{W}$ két $\mathbb{F}$ test fölötti vektortér. Azt mondjuk, hogy egy $A : \mathcal{V} \to \mathcal{W}$ leképezés lineáris, ha homogén és additív, azaz ha tetszőleges $\mathbf{x}, \mathbf{y} \in \mathcal{V}$ elemre és $c \in \mathbb{F}$ skalárra

$$A(c\mathbf{x}) = cA\mathbf{x} \qquad (A \text{ homogén,})$$

$$A(\mathbf{x} + \mathbf{y}) = A\mathbf{x} + A\mathbf{y} \qquad (A \text{ additív.})$$

A $\mathcal{V} \to \mathcal{V}$ lineáris leképezést lineáris transzformációnak is nevezzük.

P A síkbeli vektorok egy O pont körüli forgatása, egy egyenesre való tükrözése és merőleges vetítése lineáris leképezés.

P A $D : f \mapsto f'$ és az $I : f \mapsto \int_a^b f$ leképezések lineáris leképezések.

P Tetszőleges $\mathbf{A} \in \mathbb{F}^{m \times n}$ mátrixra az $A : \mathbb{F}^n \to \mathbb{F}^m; \mathbf{x} \mapsto \mathbf{A}\mathbf{x}$ mátrixleképezés lineáris leképezés.

További példák

D Négyzetes mátrix nyomán főátlójában lévő elemeinek összegét értjük. jelölés: $\mathrm{trace}(\mathbf{A})$.

Á A nyom $\mathbb{F}^{n\times n} \to \mathbb{F}$ lineáris leképezés, mert

1. $\mathrm{trace}(c\mathbf{A}) = c \,\mathrm{trace}\,\mathbf{A}$
2. $\mathrm{trace}(\mathbf{A}+\mathbf{B}) = \mathrm{trace}\,\mathbf{A} + \mathrm{trace}\,\mathbf{B}$

Á A determináns minden sorában (a többi sor rögzítése mellett) lineáris leképezés, mert minden sorában homogén és additív. Egy $n \times n$-es determináns, mint sorvektorainak n-változós függvénye, minden változójában lineáris, az ilyen függvényt nevezzük multilineárisnak.

Lineáris leképezés ekvivalens definíciói

Á Egy tetszőleges $A : \mathcal{V}_{\mathbb{F}} \to \mathcal{W}_{\mathbb{F}}$ leképezésre az alábbi állítások ekvivalensek:

1. A lineáris, azaz homogén és additív.
2. Tetszőleges $\mathbf{x}, \mathbf{y} \in \mathcal{V}_{\mathbb{F}}$ és $c, d \in \mathbb{F}$ esetén
$$A(c\mathbf{x} + d\mathbf{y}) = cA(\mathbf{x}) + dA(\mathbf{y})$$
3. Tetszőleges $\mathbf{x}, \mathbf{y} \in \mathcal{V}_{\mathbb{F}}$ és $c \in \mathbb{F}$ esetén
$$A(c\mathbf{x} + \mathbf{y}) = cA(\mathbf{x}) + A(\mathbf{y})$$
4. „Megőrzi" a lineáris kombinációt, azaz tetszőleges $\mathbf{x}_1, \ldots, \mathbf{x}_k \in \mathcal{V}_{\mathbb{F}}$ vektorokra és $c_1, c_2, \ldots, c_k \in \mathbb{F}$ skalárra
$$A(c_1\mathbf{x}_1 + \cdots + c_k\mathbf{x}_k) = c_1A\mathbf{x}_1 + \cdots + c_kA\mathbf{x}_k.$$

A lineáris $\mathbb{F}^n \to \mathbb{F}^m$ leképezések mátrixleképezések

T Egy $\mathcal{A} : \mathbb{F}^n \to \mathbb{F}^m$ függvény pontosan akkor lineáris leképezés, ha létezik egy olyan $m \times n$-es $\mathbf{A}$ mátrix, hogy az $\mathcal{A}$ = az $\mathbf{x} \mapsto \mathbf{Ax}$ mátrixleképezéssel. Ekkor $\boxed{\mathbf{A} = [\mathcal{A}\mathbf{e}_1|\mathcal{A}\mathbf{e}_2|\dots|\mathcal{A}\mathbf{e}_n],}$ ahol $\mathbf{e}_i$ az i-edik standard egységvektor ($i = 1, 2, \dots, n$).

B ($\mathcal{A}$ mátrixleképezés $\Rightarrow$ $\mathcal{A}$ lineáris) $\mathcal{A} : \mathbf{x} \mapsto \mathbf{Ax} \rightsquigarrow$

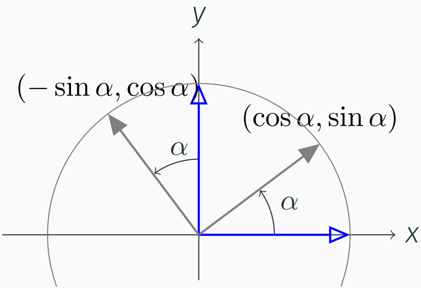
$$\mathcal{A}(c\mathbf{x} + \mathbf{y}) = \mathbf{A}(c\mathbf{x} + \mathbf{y}) = c\mathbf{Ax} + \mathbf{Ay} = c\mathcal{A}(\mathbf{x}) + \mathcal{A}(\mathbf{y})$$

($\mathcal{A}$ mátrixleképezés $\Leftarrow$ $\mathcal{A}$ lineáris)

$$\begin{aligned}
\mathcal{A}\mathbf{x} &= \mathcal{A}(x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + \dots + x_n\mathbf{e}_n) \\
&= x_1\mathcal{A}\mathbf{e}_1 + x_2\mathcal{A}\mathbf{e}_2 + \dots + x_n\mathcal{A}\mathbf{e}_n \\
&= \begin{bmatrix} \mathcal{A}\mathbf{e}_1 & \mathcal{A}\mathbf{e}_2 & \dots & \mathcal{A}\mathbf{e}_n \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \\
&= \mathbf{Ax}
\end{aligned}$$

Forgatás

Á Forgatás 2D-ben: $\begin{bmatrix} A\mathbf{i} & A\mathbf{j} \end{bmatrix} = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$



Á Forgatás tengely körül 3D-ben:

$$\begin{bmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{bmatrix}, \quad \begin{bmatrix} \cos\alpha & 0 & \sin\alpha \\ 0 & 1 & 0 \\ -\sin\alpha & 0 & \cos\alpha \end{bmatrix}.$$

Kvaterniók*

Sir William Rowan Hamilton 1843 október 16. Kvaterniók: $a+bi+cj+dk$ alakú számok, ahol $a, b, c, d \in \mathbb{R}$, i, j, k olyan „imaginárius” számok, melyekre $i^2 = j^2 = k^2 = ijk = -1$, $ij = k$, $ji = -k$, $jk = i$,..., összeadás „koordinátánként”, szorzás az előző szabályok szerint: az $\mathbf{u} = u_1 i + u_2 j + u_3 k$, $\mathbf{v} = v_1 i + v_2 j + v_3 k$ jelöléssel $(a+\mathbf{u})(b+\mathbf{v}) = ab - \mathbf{u}\cdot\mathbf{v} + a\mathbf{v} + b\mathbf{u} + \mathbf{u}\times\mathbf{v}$.

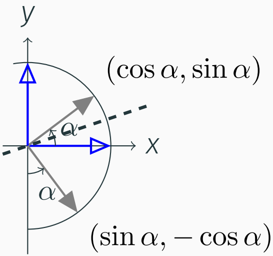
Here as he walked by on the 16th of October 1843 Sir William Rowan Hamilton in a flash of genius discovered the fundamental formula for quaternion multiplication $i^2 = j^2 = k^2 = ijk = -1$ & cut it on a stone of this bridge.

T Forgatás kvaterniókkal: $\mathbf{q} = \cos\frac{\alpha}{2} + (e_1 i + e_2 j + e_3 k)\sin\frac{\alpha}{2}$ a forgatást jellemző kvaternió, a (v_1, v_2, v_3)-hoz tartozó kvaternió $\mathbf{v} = v_1 i + v_2 j + v_3 k$. Az elforgatott: $\mathbf{qvq}^{-1}$, ahol $\mathbf{q}^{-1} = \cos\frac{\alpha}{2} - (e_1 i + e_2 j + e_3 k)\sin\frac{\alpha}{2}$

Tükrözés

T A sík vektorait az x-tengellyel $\alpha/2$ szöget bezáró egyenesre tükröző lineáris leképezés mátrixa

$$\begin{bmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{bmatrix}.$$

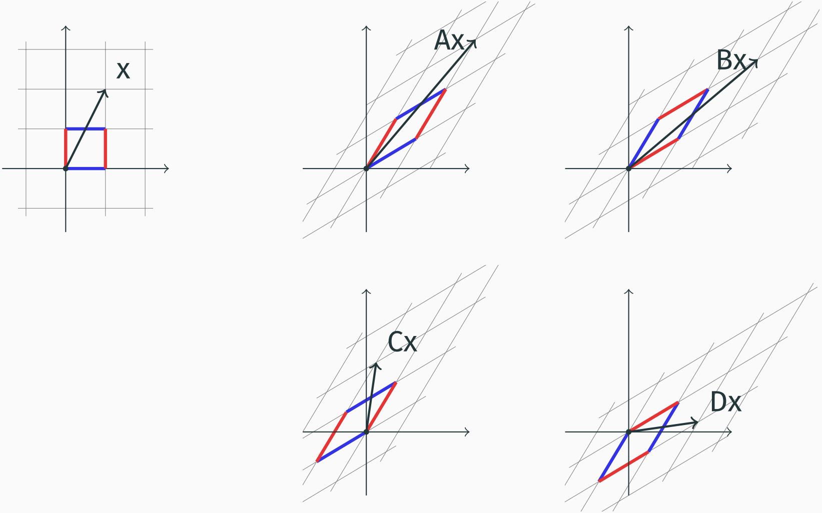


Mátrixleképezés és lineáris leképezés különbségei

- Lineáris leképezésekről olyan esetben is beszélhetünk, amikor a leképezésnek nincs mátrixa (pl. végtelen dimenziós vektorterek esetén).
- Különbség van a lineáris leképezés és a mátrixleképezés közt $\mathbb{F}^n \to \mathbb{F}^m$ függvények esetén is:
- A lineáris leképezés független a bázistól, az csak maga a függvény, mely megadja, hogy melyik vektornak melyik vektor a képe.
- A mátrixleképezés mindig valamely bázisra vonatkozik. Egy lineáris leképezéshez minden bázisban tartozik egy mátrixleképezés, melynek mátrixa függ a bázistól.
- A lineáris $\mathbb{F} \to \mathbb{F}$ leképezések azonosak az $x \mapsto cx$ függvényekkel, ahol $c \in \mathbb{F}$ konstans (NEM az $x \mapsto cx + b$ függvények!!!).

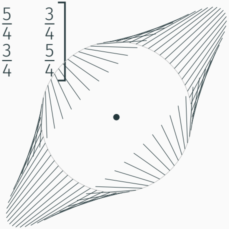
A mátrixleképezés szemléltetése négyzetráccsal

$$A = \begin{bmatrix} \frac{5}{4} & \frac{3}{4} \\ \frac{3}{4} & \frac{5}{4} \end{bmatrix}, B = \begin{bmatrix} \frac{3}{4} & \frac{5}{4} \\ \frac{5}{4} & \frac{3}{4} \end{bmatrix}, C = \begin{bmatrix} -\frac{5}{4} & \frac{3}{4} \\ -\frac{3}{4} & \frac{5}{4} \end{bmatrix}, D = \begin{bmatrix} -\frac{3}{4} & \frac{5}{4} \\ -\frac{5}{4} & \frac{3}{4} \end{bmatrix}$$

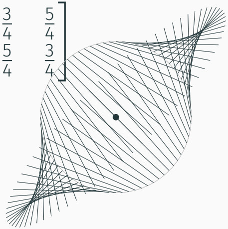


A mátrixleképezés szemléltetése egységkör-ábrával

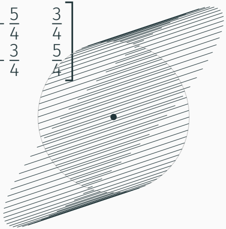
$$A = \begin{bmatrix} \frac{5}{4} & \frac{3}{4} \\ \frac{3}{4} & \frac{5}{4} \end{bmatrix}$$



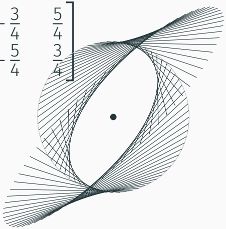
$$B = \begin{bmatrix} \frac{3}{4} & \frac{5}{4} \\ \frac{5}{4} & \frac{3}{4} \end{bmatrix}$$



$$C = \begin{bmatrix} -\frac{5}{4} & \frac{3}{4} \\ -\frac{3}{4} & \frac{5}{4} \end{bmatrix}$$



$$D = \begin{bmatrix} -\frac{3}{4} & \frac{5}{4} \\ -\frac{5}{4} & \frac{3}{4} \end{bmatrix}$$



Képtér, magtér, altér képe

D L! $A : \mathcal{V} \to \mathcal{W}$ lineáris leképezés. Az A értékkészlete altér $\mathcal{W}$-ben, amit az A képterének nevezünk, jele $\mathrm{Im}(A)$. $\mathrm{Im}(A) \leqslant \mathcal{W}$.

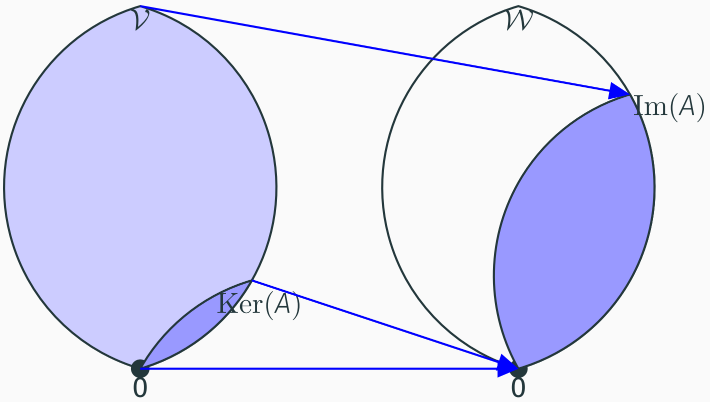
D Azok az $\mathbf{x} \in \mathcal{V}$ vektorok, melyekre $A\mathbf{x} = \mathbf{0}$ alteret alkotnak, amit az A magterének (kernel) nevezünk, jele $\mathrm{Ker}(A)$. $\mathrm{Ker}(A) \leqslant \mathcal{V}$.

D Egy altér eltoltjait affin altereknek nevezzük.

Tehát ha $\mathcal{V} \leqslant \mathcal{W}$ és $\mathbf{u} \in \mathcal{W}$, akkor $\mathcal{V} + \mathbf{u} = \{\mathbf{v} + \mathbf{u} \mid \mathbf{v} \in \mathcal{V}\}$ affin altér. ($\mathbf{u} \in \mathcal{V}$ esetén $\mathcal{V} + \mathbf{u} = \mathcal{V}$, tehát az altér is affin altér, de ha egy affin altérnek nem eleme a nullvektor, akkor az nem altér.)

Á Lineáris leképezés alteret altérbe, affin alteret affin altérbe visz.

A lineáris leképezés szemléltetése levéldiagrammal



Lineáris leképezések

Izomorfizmus

Az izomorfizmus fogalma

- Két algebrai struktúra izomorf, ha elemeik közt van egy műveletttartó bijekció.
- Például az egyműveletes $\langle \mathbb{Z}_6, + \rangle$ izomorf $\langle \mathbb{Z}_2 \times \mathbb{Z}_3, + \rangle$ struktúrával, ahol a bijekció $(0,0) \leftrightarrow 0$, $(1,1) \leftrightarrow 1$, $(0,2) \leftrightarrow 2$, $(1,0) \leftrightarrow 3$, $(0,1) \leftrightarrow 4$, $(1,2) \leftrightarrow 5$, azaz általában $(a, b) \leftrightarrow (3a + 4b) \bmod 6$.

D Két vektortér izomorf, ha létezik köztük egy bijektív lineáris leképezés. E leképezés neve izomorfizmus.

J $\mathcal{V} \simeq \mathcal{W}$

Az izomorfizmus tulajdonságai

T Két izomorfizmus kompozíciója és egy izomorfizmus inverze is izomorfizmus.

T **Véges dimenziós terek jellemzése**

Ha az $\mathbb{F}$ test fölötti $\mathcal{V}$ vektortérnek van n-elemű bázisa, akkor $\mathcal{V} \simeq \mathbb{F}^n$.

P $\mathcal{P}_1 = \{ax + b \mid a, b \in \mathbb{R}\}$ a legföljebb elsőfokú polinomok tere, akkor $\mathcal{P}_1 \simeq \mathbb{R}^2$.

P Komplex számsík: $\mathbb{R}^2 \simeq \mathbb{C}_{\mathbb{R}} \quad (\mathbb{C}_{\mathbb{R}} = \{a + b\mathrm{i} \mid a, b \in \mathbb{R})$