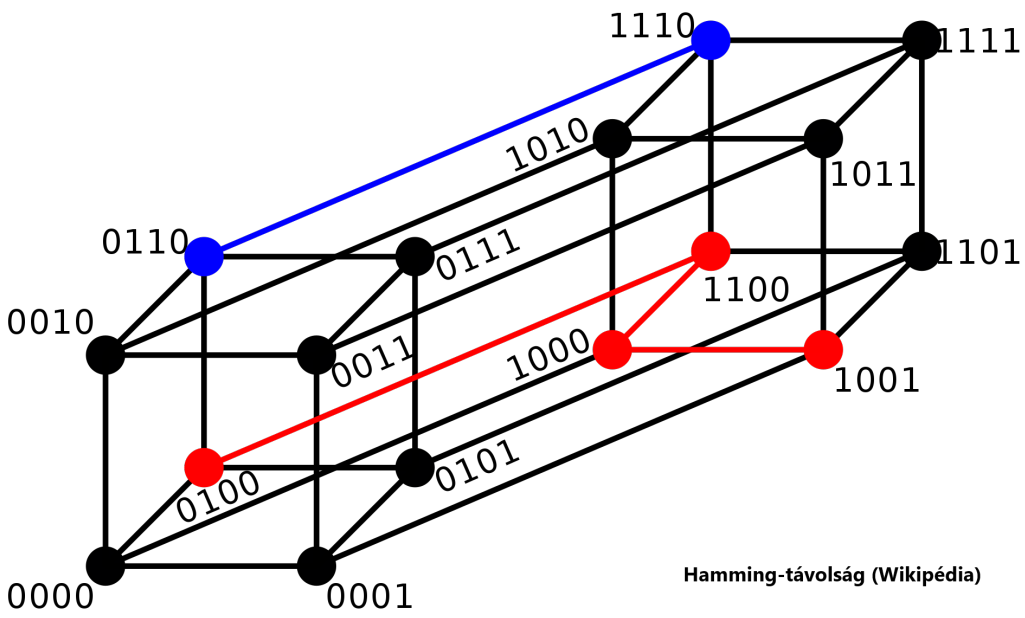
Diszkrét Matematika III.

(Informatikusoknak)

Maróti Miklós & **Kátai-Urbán Kamilla**



2024

Az előadásvázlat a Diszkrét matematika III. (informatikusoknak) tárgyhoz készült. A megfelelő témakörökhöz a 2020-ban tartott online előadások videóit illesztettük be. Az előadáson szereplő fogalmak gyakorlására szolgálnak az itt található feladatsorok.

Tartalomjegyzék

1. Permutációk 3
2. Rang, altér 9
3. Lineáris leképezések 14
4. Polinomok 18
5. Testek 24
6. Hibajavító kódolás 28
7. Videók jegyzéke 35

1. Permutációk

Videó: **Permutációk megadása**

1.1. Definíció. Az A halmaz permutációin a $\pi : A \to A$ bijektív leképezéseket értjünk. Tetszőleges n pozitív egészre az $\{1, \dots, n\}$ halmaz összes permutációinak halmazát S_n-nel jelöljük.

1.2. Jelölés. A $\pi \in S_n$ permutációt megadhatjuk kétsoros írásmóddal

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1\pi & 2\pi & \cdots & n\pi \end{pmatrix},$$

vagy elempárok halmazaként:

$$\pi = \{(1, 1\pi),\ (2, 2\pi),\ \dots,\ (n, n\pi)\}.$$

1.3. Példa. Ha $\alpha \in S_3$ az a permutáció, amelyre $1\alpha = 2$, $2\alpha = 1$ és $3\alpha = 3$, akkor

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \{(1, 2),\ (2, 1),\ (3, 3)\}.$$

1.4. Példa. Nem minden leképezés permutáció, például a

$$\varphi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 3 \end{pmatrix} = \{(1, 3),\ (2, 1),\ (3, 3)\}$$

leképezés se nem injektív (mert az 1 és 3 elemeknek ugyanaz a képe) se nem szürjektív (mert az érkezési halmaz 2 elmének nincsen őse).

1.5. Tétel. $|S_n| = n!$

1.6. Példa.

$$S_1 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\},$$
$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\},$$
$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

Videó: **Permutációk szorzása**

1.7. Példa. Számoljuk ki az

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ és } \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

permutációk szorzatát. Tudjuk, hogy minden x elemre $x(\alpha\beta) = (x\alpha)\beta$ (ez a leképezés szorzás definíciója). Tehát

$$\begin{aligned} 1(\alpha\beta) &= (1\alpha)\beta = 2\beta = 3, \\ 2(\alpha\beta) &= (2\alpha)\beta = 1\beta = 2, \\ 3(\alpha\beta) &= (3\alpha)\beta = 3\beta = 1, \end{aligned}$$

azaz

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Most kiszámoljuk a $\beta\alpha$ szorzatot is (a zárójelek elhagyásával):

$$\begin{aligned} 1\beta\alpha &= 2\alpha = 1, \\ 2\beta\alpha &= 3\alpha = 3, \\ 3\beta\alpha &= 1\alpha = 2, \end{aligned}$$

azaz

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Vegyük észre, hogy $\alpha\beta \neq \beta\alpha$, azaz a permutációk szorzása nem kommutatív. Végezetül kiszámoljuk β inverzét. Mivel

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \{(1,2),\ (2,3),\ (3,1)\}$$

ezért

$$\beta^{-1} = \{(2,1),\ (3,2),\ (1,3)\} = \{(1,3),\ (2,1),\ (3,2)\} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Természetesen β és β^{-1} szorzata az identikus leképezés:

$$\beta\beta^{-1} = \beta^{-1}\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

1.8. Tétel. $(S_n; \circ)$ csoport.

1.9. Definíció. A $\pi \in S_n$ permutáció az $x \in \{1, \dots, n\}$ elemet mozgatja, ha $x\pi \neq x$. A $\pi \in S_n$ által mozgatott elemek halmazát M_π-vel jelöljük, azaz

$$M_\pi = \{\, x \in \{1, \dots, n\} : x\pi \neq x \,\}.$$

1.10. Példa. Az

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

permutáció által mozgatott elemek halmaza $M_\alpha = \{1, 2\}$.

1.11. Kérdések. Hány olyan $\pi \in S_9$ permutáció van, amelyre

1. $M_\pi = \{2, 3, 5\}$,
2. $|M_\pi| = 1$,
3. $|M_\pi| = 2$,
4. $|M_\pi| = 3$?

1.12. Definíció. A $\pi, \sigma \in S_n$ permutációkat idegennek nevezzük, ha $M_\pi \cap M_\sigma = \emptyset$.

1.13. Kérdések.

1. Az S_n halmazon az „idegenség” reláció reflexív, szimmetrikus, illetve tranzitív-e?
2. Hány olyan permutációja van S_4-nek, amely az $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{smallmatrix}\right)$ permutációval idegen?
3. Van-e olyan permutáció, amely idegen az inverzével?

1.14. Tétel. Ha a $\pi, \sigma \in S_n$ permutációk idegenek, akkor

1. $\pi\sigma = \sigma\pi$, és
2. $(\pi\sigma)^k = \pi^k\sigma^k$ minden k egészre.

Videó: **Ciklus definíciója**

1.15. Definíció. Legyen $n \geqslant k \geqslant 2$, és az $a_1, \dots, a_k \in \{1, \dots, n\}$ elemek páronként különbözőek. Ekkor azt a $\pi \in S_n$ permutációt, amelyre

$$\begin{aligned} a_1\pi &= a_2, \\ a_2\pi &= a_3, \\ &\vdots \\ a_{k-1}\pi &= a_k, \\ a_k\pi &= a_1, \end{aligned}$$

és $x\pi = x$ minden $x \in \{1, \dots, n\} \setminus \{a_1, \dots, a_k\}$ elemre, ciklusnak nevezzük és röviden így jelöljük:

$$\pi = (a_1\ a_2\ \cdots\ a_k).$$

A k számot a ciklus hosszának nevezzük. A 2 hosszúságú ciklusokat transzpozícióknak hívjuk.

1.16. Példa. Az

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

permutáció ciklus, mivel a $k = 2$, $a_1 = 1$ és $a_2 = 2$ választással éppen ezt a permutációt kapjuk, azaz $\alpha = (1\ 2)$. Mivel α hossza éppen 2, ezért α transzpozíció is. A

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

permutáció szintén ciklus, és $\beta = (1\ 2\ 3)$.

1.17. Kérdések.

1. Mi az $(a_1\ a_2\ \cdots\ a_k)$ ciklus által mozgatott elemek halmaza?
2. Igaz-e, hogy ha $\pi, \sigma, \tau \in S_7$ páronként idegen permutációk, akkor $(\pi\sigma\tau)^5 = \pi^5\sigma^5\tau^5$?

1.18. Megjegyzés. Vegyük észre, hogy egy permutáció ciklusos alakban való megadása nem egyértelmű! Egyrészt ugyanazt a permutációt többféleképpen is felírhatjuk ciklusként:

$$(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2).$$

A másik probléma pedig az, hogy az $(1\ 2\ 3)$ permutációról nem tudjuk eldönteni, hogy az S_3 vagy esetleg az S_4 csoport eleme-e. Természetesen ha S_3-beli permutációkról beszélünk, akkor

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

viszont S_4-ben már

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

és ez a két permutáció nem ugyanaz. Ugyan ez a probléma az identikus permutáció „id” jelölésével is, arról sem lehet eldönteni, hogy melyik permutációcsoportban használjuk.

1.19. Példa.

$$\begin{aligned} S_1 &= \{\mathrm{id}\}, \\ S_2 &= \{\mathrm{id}, (1\ 2)\}, \\ S_3 &= \{\mathrm{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (3\ 2\ 1)\}. \end{aligned}$$

1.20. Kérdések.

1. Hány transzpozíció van S_4-ben?
2. Hány 3-hosszúságú ciklus van S_4-ben?
3. Hány 4-hosszúságú ciklus van S_4-ben?
4. Hány 1-hosszúságú ciklus van S_4-ben?
5. Hány ciklus van S_4-ben?
6. Hány olyan permutáció van S_4-ben amely nem ciklus?
7. Hány n-hosszúságú ciklus van S_n-ben?

1.21. Példa. Természetesen nem minden permutáció ciklus, vegyük például a

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

permutációt. Tegyük fel, hogy π ciklus, és tekintsük azt az esetet, amikor $a_1 = 1$. Ekkor $a_1\pi = 2$, azaz $a_2 = 2$, továbbá $a_2\pi = 3$, azaz $a_3 = 3$. A következő lépésben azt kapjuk, hogy $a_3\pi = 1$ ami éppen egyenlő a_1-gyel, azaz $k = 3$ és az $(1\ 2\ 3)$ ciklust kaptuk. Viszont π több elemet mozgat mint 3, tehát π nem egyenlő $(1\ 2\ 3)$-mal, azaz $a_1 \neq 1$. Minden más esetben hasonló ellentmondásra jutunk.

Persze π előáll ciklusok szorzataként:

$$\pi = (1\ 2\ 3)(4\ 5).$$

Videó: **Ciklusokra való felbontás**

1.22. Tétel. Minden S_n-beli permutáció előáll páronként idegen ciklusok szorzataként, és ez az előállítás a tényezők sorrendjétől eltekintve egyértelműen meghatározott. (Az identikus permutációt ciklusok üres szorzatának tekintjük.)

1.23. Példa. Adjuk meg a $\pi = (5\ 2\ 3\ 4)(1\ 3\ 5)(4\ 3\ 7)$ permutációt páronként idegen ciklusok szorzataként. Tekintsük azokat az elemeket, melyeket a szorzat valamely tagja mozgat: $\{1, 2, 3, 4, 5, 7\}$. Vegyünk ki ezek közül egyet, mondjuk az 1-et, és számoljuk ki, hogy ezt a π permutáció milyen elemekbe viszi át:

$$1\pi = 1(5\ 2\ 3\ 4)(1\ 3\ 5)(4\ 3\ 7) = 1(1\ 3\ 5)(4\ 3\ 7) = 3(4\ 3\ 7) = 7.$$

Folytassuk a kapott elemekkel, azaz

$$\begin{aligned} 7\pi &= 7(5\ 2\ 3\ 4)(1\ 3\ 5)(4\ 3\ 7) = 7(1\ 3\ 5)(4\ 3\ 7) = 7(4\ 3\ 7) = 4, \\ 4\pi &= 4(5\ 2\ 3\ 4)(1\ 3\ 5)(4\ 3\ 7) = 5(1\ 3\ 5)(4\ 3\ 7) = 1(4\ 3\ 7) = 1. \end{aligned}$$

Visszaértünk ahhoz az elemhez, amiből kiindultunk, tehát megvan az első ciklusunk: $(1\ 7\ 4)$. A maradék elemekből vegyük a következőt, mondjuk a 2-t, és számoljuk ki hogy ezt π milyen elemekbe viszi át:

$$\begin{aligned} 2\pi &= 2(5\ 2\ 3\ 4)(1\ 3\ 5)(4\ 3\ 7) = 3(1\ 3\ 5)(4\ 3\ 7) = 5(4\ 3\ 7) = 5, \\ 5\pi &= 5(5\ 2\ 3\ 4)(1\ 3\ 5)(4\ 3\ 7) = 2(1\ 3\ 5)(4\ 3\ 7) = 2(4\ 3\ 7) = 2, \end{aligned}$$

azaz a második ciklus a $(2\ 5)$ transzpozíció. Kimaradt még a 3, amelyre elvégezve a számolást azt kapjuk, hogy

$$3\pi = 3(5\ 2\ 3\ 4)(1\ 3\ 5)(4\ 3\ 7) = 4(1\ 3\ 5)(4\ 3\ 7) = 4(4\ 3\ 7) = 3,$$

azaz π a 3-at nem mozgatja, tehát ezt az elemet figyelmen kívül hagyhatjuk. Tehát π páronként idegen ciklusok szorzatára bontott alakja $\pi = (1\ 7\ 4)(2\ 5)$. Ezt a számolást nem írjuk le általában, hanem fejben végezzük el!

1.24. Kérdések. Hány olyan permutáció van G-ben, amelynek páronként idegen ciklusok szorzatára bontott alakja P alakú:

1. $G = S_4$, $P = (\cdot\ \cdot)(\cdot\ \cdot)$,
2. $G = S_5$, $P = (\cdot\ \cdot)(\cdot\ \cdot)$,
3. $G = S_5$, $P = (\cdot\ \cdot)(\cdot\ \cdot\ \cdot)$?

1.25. Tétel. Tetszőleges $\pi = (a_1\ a_2\ \cdots\ a_k) \in S_n$ ciklusra

1. $\pi^{-1} = (a_k\ a_{k-1}\ \cdots\ a_1)$,
2. $\pi^k = \mathrm{id}$,
3. Ha $i \equiv j \pmod{k}$, akkor $\pi^i = \pi^j$.

Videó: Ciklusokkal való számolás

1.26. Példa. Kiszámoljuk az $((1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9))^{-22}$ permutációt páronként idegen ciklusok szorzataként. Mivel az $(1\ 2\ 3\ 4)$, $(5\ 6\ 7)$ és $(8\ 9)$ ciklusok páronként idegenek, ezért

$$((1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9))^{-22} = (1\ 2\ 3\ 4)^{-22}(5\ 6\ 7)^{-22}(8\ 9)^{-22}.$$

Az $(1\ 2\ 3\ 4)$ ciklus hossza 4 és a -22-edik hatványát keressük. Mivel $-22 \equiv 2 \pmod{4}$, ezért

$$(1\ 2\ 3\ 4)^{-22} = (1\ 2\ 3\ 4)^2 = (1\ 3)(2\ 4).$$

Hasonlóan $-22 \equiv -1 \pmod{3}$, illetve $-22 \equiv 0 \pmod{2}$, azaz

$$\begin{aligned} (5\ 6\ 7)^{-22} &= (5\ 6\ 7)^{-1} = (7\ 6\ 5), \text{ és} \\ (8\ 9)^{-22} &= (8\ 9)^0 = \mathrm{id}. \end{aligned}$$

Tehát

$$((1\ 2\ 3\ 4)(5\ 6\ 7))^{-22} = (1\ 3)(2\ 4)(7\ 6\ 5).$$

1.27. Példa. Oldjuk meg az

$$(1\ 3\ 2)(2\ 5)\pi(4\ 5\ 7) = (2\ 6)$$

egyenletet. Az egyenlet mindkét oldalát ugyanazzal a permutációval ugyanarról az oldalról beszorozhatjuk. Először balról szorzunk $(1\ 3\ 2)$ inverzével:

$$(1\ 3\ 2)^{-1}(1\ 3\ 2)(2\ 5)\pi(4\ 5\ 7) = (1\ 3\ 2)^{-1}(2\ 6),$$

azaz

$$(2\ 5)\pi(4\ 5\ 7) = (2\ 3\ 1)(2\ 6).$$

Ezt folytatva azt kapjuk, hogy

$$\pi = (5\ 2)(2\ 3\ 1)(2\ 6)(7\ 5\ 4),$$

amit a szokásos módon páronként idegen ciklusok szorzatára bontunk: $\pi = (5\ 3\ 1\ 6\ 2\ 4\ 7)$.

Videó: **Permutációk paritása**

1.28. Tétel. Tetszőleges ciklus felírható transzpozíciók szorzataként, mégpedig

$$(a_1\ a_2\ a_3\ \cdots\ a_k) = (a_1\ a_2)(a_1\ a_3)\cdots(a_1\ a_k).$$

Következésképpen, minden permutáció transzpozíciók szorzatára bontható (de ez általában nem egyértelmű).

1.29. Példa. $(1\ 2\ 3\ 4)(5\ 6) = (1\ 2)(1\ 3)(1\ 4)(5\ 6)$, de mivel $(1\ 2\ 3\ 4) = (2\ 3\ 4\ 1)$, ezért $(1\ 2\ 3\ 4)(5\ 6) = (2\ 3)(2\ 4)(2\ 1)(5\ 6)$, vagy $(1\ 2\ 3\ 4)(5\ 6) = (2\ 3)(5\ 6)(2\ 4)(2\ 1)$, mert idegen transzpozíciók felcserélhetők.

1.30. Tétel. Minden permutáció vagy csak páros vagy csak páratlan sok transzpozíció szorzataként írható fel.

1.31. Definíció. A $\pi \in S_n$ permutációt párosnak nevezzük, ha felbontható páros sok transzpozíció szorzatára. A nempáros permutációkat páratlannak nevezzük. Továbbá definiáljuk:

$$\operatorname{sgn}(()\,\pi) = \begin{cases} +1, & \text{ha } \pi \text{ páros,} \\ -1, & \text{ha } \pi \text{ páratlan.} \end{cases}$$

1.32. Kérdések. Az alábbi állítások közül melyek igazak és melyek hamisak?

1. Az identitás páros.
2. Minden transzpozíció páratlan.
3. Minden páros hosszú ciklus páros.
4. Minden páratlan hosszú ciklus páros.
5. Páros permutációk szorzata páros.
6. Páratlan permutációk szorzata páros.
7. Páros és páratlan permutáció szorzata páratlan.
8. Páratlan permutációk inverze páratlan.

1.33. Példa. Megmutatjuk, hogy a 4×4-es tologatós játékban a baloldali kezdőállásból nem lehet előállítani a jobboldalit:

$A =$

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

$B =$

2	1	3	4
5	6	7	8
9	10	11	12
13	14	15	

A játék minden állásához hozzárendeljük az S_{16} csoport egyik elemét, mégpedig úgy, hogy az üres mező helyébe a 16-os számot képzeljük, és a kapott

$T =$

a_1	a_2	a_3	a_4
a_5	a_6	a_7	a_8
a_9	a_{10}	a_{11}	a_{12}
a_{13}	a_{14}	a_{15}	a_{16}

táblázatot felhasználva képezzük a

$$\pi_T = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} & a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} \end{pmatrix}$$

permutációt. Vegyük észre, hogy ha egy állapotban eltolunk egy négyzetet, akkor lényegében felcseréltük a 16-os számot valamely másik számmal. Tehát egy transzpozíciót hajtottunk végre, azaz az állapothoz rendelt permutáció paritása megváltozik. Mivel mind az A, mind a B állapotban az üres mező a jobb alsó sarokban van, ezért biztos, hogy páros sok lépest kell megtennünk A-ból B-be (ugyanannyiszor kell a 16-os számnak felfelé és lefelé, illetve balra és jobbra mozognia). Páros sok lépes során a hozzárendelt permutáció paritása nem változik. De az A kezdőállapotra $\pi_A = \mathrm{id}$ ami páros, míg a jobboldali állapotra $\pi_B = (1\ 2)$ ami páratlan. Tehát nem lehet az A állapotból a B állapotba jutni.

1.34. Definíció. Az S_n csoportot az n-edrendű szimmetrikus csoportnak nevezzük. A páros permutációk $A_n = \{\pi \in S_n : \pi \text{ páros}\}$ halmaza szintén csoportot alkot, amelynek neve az n-edrendű alternáló csoport.

1.35. Kérdések.

1. Hány páratlan permutáció van S_3-ban?
2. Hány páros permutáció van S_3-ban?
3. Hány páratlan permutáció van S_1-ben?
4. Hány páros permutáció van S_1-ben?

1.36. Tétel. Tetszőleges $n \geqslant 2$ egészre $|A_n| = \frac{n!}{2}$.

2. Rang, altér

Videó: **Determináns permutációkkal**

2.1. Tétel. Legyen T test, és $A = (a_{i,j}) \in T^{n\times n}$ tetszőleges négyzetes mátrix. Ekkor

$$|A| = \sum_{\sigma\in S_n} \operatorname{sgn}(()\,\sigma)\cdot a_{1,1\sigma}\cdot a_{2,2\sigma}\cdots a_{n,n\sigma}.$$

2.2. Példa. $n = 2$ esetén:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \operatorname{sgn}(()\,\mathrm{id})\cdot a_{11}a_{22} + \operatorname{sgn}(()(1\ 2))\cdot a_{12}a_{21} = a_{11}a_{22} - a_{12}a_{21}.$$

$n = 3$ esetén:

$$\begin{aligned}\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} &= \operatorname{sgn}(()\,\mathrm{id})\cdot a_{11}a_{22}a_{33} + \operatorname{sgn}(()(1\ 2))\cdot a_{12}a_{21}a_{33} + \operatorname{sgn}(()(1\ 3))\cdot a_{13}a_{22}a_{31} \\ &\quad + \operatorname{sgn}(()(2\ 3))\cdot a_{11}a_{23}a_{32} + \operatorname{sgn}(()(1\ 2\ 3))\cdot a_{12}a_{23}a_{31} + \operatorname{sgn}(()(1\ 3\ 2))\cdot a_{13}a_{21}a_{32} \\ &= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32},\end{aligned}$$

ami éppen a Sarrus-szabály.

2.3. Kérdések. Az alábbi állítások közül melyek igazak és melyek hamisak tetszőleges T testre?

1. $|A| \geqslant 0$ tetszőleges $A \in T^{n\times n}$ mátrixra.
2. Tetszőleges $A \in T^{n\times n}$ mátrixra $|A| \in T$.
3. Ha $A \in T^{n\times k}$ és $B \in T^{k\times m}$, akkor $AB \in \mathbb{C}^{n\times m}$.
4. Ha $A \in T^{n\times n}$ és $B \in T^{n\times n}$, akkor $|AB| = |A|\cdot|B|$.
5. Ha $A \in T^{n\times n}$ és $B \in T^{n\times n}$, akkor $|A + B| = |A| + |B|$.
6. Ha $A \in T^{n\times n}$ és $\lambda \in T$, akkor $|\lambda A| = \lambda^n|A|$.
7. Ha az $A \in T^{n\times n}$ mátrix valamely oszlopában csupa nulla elem van, akkor $|A| = 0$.
8. Ha $A \in T^{n\times n}$ trianguláris, akkor $|A|$ a főátlón elhelyezkedő elemek szorzata.
9. Az $A \in T^{n\times n}$ mátrix akkor és csak akkor invertálható, ha $|A| \neq 0$.

2.4. Definíció. A következő speciális alakú $n \times n$-es determinánst Vandermonde-determinánsnak nevezzük:

$$V(x_1,\dots,x_n) = \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix}.$$

Értéke az alábbi képlet szerint számolható:

$$V(x_1,\dots,x_n) = \prod_{j<i}(x_i - x_j).$$

Videó: **Vektorrendszer rangja**

2.5. Definíció. A T test feletti V vektortér $v_1,\dots,v_k$ vektorrendszere lineárisan független, ha pontosan akkor teljesül, hogy $\lambda_1 v_1 + \dots + \lambda_k v_k = \underline{0}$, ha $\lambda_1 = \dots = \lambda_k = 0$, azaz csak a triviális lineáris kombináció állítja elő a $\underline{0}$-t. Különben a vektorrendszer lineárisan függő.

2.6. Definíció. A T test feletti V vektortér $v_1,\dots,v_k$ vektorrendszer lineárisan független részrendszereinek maximális elemszámát a vektorrendszer rangjának nevezzük, és $r(v_1,\dots,v_k)$-val jelöljük.

Videó: **Mátrixok rangja**

2.7. Definíció. Az $A \in T^{m\times n}$-es mátrix sorrangja az A sorai által alkotott vektorrendszer rangja, oszloprangja az A oszlopai által alkotott vektorrendszer rangja.

2.8. Definíció. Legyen $A \in T^{m\times n}$ tetszőleges T test feletti mátrix és $r \leqslant m, n$ egészek. Az A mátrix r-edrendű aldeterminánsainak az A mátrix tetszőleges r sorát és r oszlopát kijelölve, majd a kijelölt sorok és oszlopok találkozásában lévő elemekből alkotott $r \times r$-es mátrixok determinánsait nevezzük. Az A mátrix determinánsrangja a nemelfajuló (nem nulla) aldeterminánsainak a maximális rendje.

2.9. Példa. Számoljuk ki az

$$A = \begin{pmatrix} 1 & 2 & 4 & 8 & 0 \\ 0 & 1 & 2 & 3 & 0 \\ 1 & 3 & 9 & 27 & 0 \\ 0 & 2 & 4 & 6 & 0 \\ 1 & -1 & 1 & -1 & 0 \\ 1 & 5 & 25 & 125 & 0 \end{pmatrix}$$

mátrix determinánsrangját. A rang maximum 4 lehet, mert ha az utolsó, csupa nulla oszlop benne van egy aldeterminánsban, akkor annak értéke 0. Viszont azokat a sorokat kiválasztva, amelyek 1-gyel kezdődnek az

$$\begin{vmatrix} 1 & 2 & 4 & 8 \\ 1 & 3 & 9 & 27 \\ 1 & -1 & 1 & -1 \\ 1 & 5 & 25 & 125 \end{vmatrix}$$

aldeterminánst kapjuk, amely éppen egy Vandermonde-determináns, ezért értéke

$$(3-2)(-1-2)(5-2)(-1-3)(5-3)(5-(-1)) \neq 0,$$

tehát az A mátrix determinánsrangja 4.

2.10. Tétel (Rangszámtétel)**.** Tetszőleges mátrix sor-, oszlop- és determinánsrangjai megegyeznek.

2.11. Definíció. A rangszámtétel szerint tetszőleges A mátrix sor-, oszlop-, és determinánsrangja megegyezik. Ezt a számot nevezzük az A mátrix rangjának, és $r(A)$-val jelöljük.

2.12. Következmény. Tetszőleges $A \in T^{n\times n}$ mátrixra a következő állítások ekvivalensek:
1. $|A| \neq 0$,
2. A oszlopvektorainak rendszere lineárisan független,
3. A sorvektorainak rendszere lineárisan független,
4. $r(A) = n$.

2.13. Tétel (Kronecker-Capelli-tétel)**.** Tetszőleges T test, $A \in T^{m\times n}$ és $b \in T^m$ esetén az $Ax = b$ lineáris egyenletrendszer akkor és csak akkor oldható meg, ha $r(A) = r(A|b)$.

Videó: **Alterek és bázis**

2.14. Definíció. A $v_1, \ldots, v_k$ vektorok által generált altér elemei a $v_1, \ldots, v_k$ vektorok lineáris kombinációjaként előálló vektorok. Jele: $[v_1, \ldots, v_k]$.

2.15. Definíció. Egy T test feletti V vektortérben a $v_1, \ldots, v_k$ vektorrendszer az U altér bázisa, ha a vektorrendszer lineárisan független és generátorrendszer ($U = [v_1, \ldots, v_k]$). A bázis elemszáma a dimenzió. Jele: $\dim(U)$.

2.16. Tétel. Egy T test feletti V vektortér bármely $v_1, \ldots, v_k$ vektorrendszere esetén

$$r(v_1, \ldots, v_k) = \dim[v_1, \ldots, v_k].$$

2.17. Definíció. Két vektorrendszert ekvivalensnek nevezzük, ha ugyanazt az alteret generálják.

2.18. Definíció. A vektorrendszerek elemi átalakításai a következők:
1. tetszőleges v_i vektor nemnulla $\lambda \in T$ skalárral való szorzása

$$v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_k \quad \sim \quad v_1, \ldots, v_{i-1}, \lambda v_i, v_{i+1}, \ldots, v_k$$

2. tetszőleges v_i vektor tetszőleges $\lambda \in T$ skalárszorosának egy másik v_j $(j \neq i)$ vektorhoz való hozzáadása

$$v_1, \dots, v_{j-1}, v_j, v_{j+1}, \dots, v_k \quad \sim \quad v_1, \dots, v_{j-1}, \lambda v_i + v_j, v_{j+1}, \dots, v_k$$

3. nulla vektor elhagyása (hozzávétele)

$$v_1, \dots, v_{i-1}, \underline{0}, v_{i+1}, \dots, v_k \quad \sim \quad v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_k.$$

2.19. Tétel. Két vektorrendszer akkor és csak akkor ekvivalens, ha elemi átalakítások sorozatával egymásba alakítható. Tehát tetszőleges generátorrendszer elemi átalakítások sorozatával bázissá alakítható.

2.20. Kérdések. Az alábbi állítások közül melyek igazak és melyek hamisak véges dimenziós vektorterekben?
1. Ekvivalens vektorrendszerek elemszáma megegyezik.
2. Elemi átalakítások megfordítottja is elemi átalakítás.
3. Bármely két lineárisan független vektorrendszer elemi átalakítások sorozatával egymásba alakíthatók.
4. Bármely két generátorrendszer elemi átalakítások sorozatával egymásba vihetők.
5. Két azonos vektor közül az egyiknek az elhagyása elemi átalakítások sorozatával megvalósítható.

Videó: **Alterek megadása**

2.21. Példa. Az $\mathbb{R}^4$ vektortérben megadjuk az $(1,1,2,-1)$, $(-2,1,0,1)$ és $(-3,3,2,1)$ vektorok által generált U altér bázisát. Ehhez a generáló vektorokat egy mátrix soraiba beírjuk, majd a mátrixon sorokon végzett elemi átalakításokkal elvégezzük a Gauss-eliminációt. Az elemi átalakítások nem változtatják meg a generált alteret, továbbá könnyen látható, hogy a Gauss-elimináció során kapott nemzéró vektorok lineárisan függetlenek. Így az eljárás végén egy bázist kapunk.

$$\begin{pmatrix} \boxed{1} & 1 & 2 & -1 \\ -2 & 1 & 0 & 1 \\ -3 & 3 & 2 & 1 \end{pmatrix} \sim \begin{pmatrix} \boxed{1} & 1 & 2 & -1 \\ 0 & \boxed{3} & 4 & -1 \\ 0 & 6 & 8 & -2 \end{pmatrix} \sim \begin{pmatrix} \boxed{1} & 1 & 2 & -1 \\ 0 & \boxed{1} & \frac{4}{3} & -\frac{1}{3} \\ 0 & 6 & 8 & -2 \end{pmatrix} \sim \begin{pmatrix} \boxed{1} & 0 & \frac{2}{3} & -\frac{2}{3} \\ 0 & \boxed{1} & \frac{4}{3} & -\frac{1}{3} \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Azaz U kétdimenziós és az $(1, 0, \frac{2}{3}, -\frac{2}{3})$, $(0, 1, \frac{4}{3}, -\frac{1}{3})$ vektorrendszer bázis.

2.22. Megjegyzés. Az előző példában szereplő $(1,1,2,-1)$, $(-2,1,0,1)$, $(-3,3,2,1)$ vektorrendszer rangját is meghatároztuk, ugyanis a 2.16. tétel szerint:

$$r((1,1,2,-1),(-2,1,0,1),(-3,3,2,1)) = \dim(U) = 2.$$

Mivel a vektorrendszer 3 elemű, így a rang definíciója alapján azt is megkaptuk, hogy a vektorrendszer lineárisan függő.

2.23. Példa. Az 2.21. példában szereplő U alteret megadjuk egyenletek segítségével is. Tudjuk, hogy az altér minden eleme a báziselemek lineáris kombinációjaként előáll, azaz

$$\begin{aligned} U &= \left\{ x \cdot (1, 0, \frac{2}{3}, -\frac{2}{3}) + y \cdot (0, 1, \frac{4}{3}, -\frac{1}{3}) : x, y \in \mathbb{R} \right\} \\ &= \left\{ (x, y, \frac{2}{3}x + \frac{4}{3}y, -\frac{2}{3}x - \frac{1}{3}y) : x, y \in \mathbb{R} \right\} \\ &= \left\{ (x_1, x_2, x_3, x_4) : x_3 = \frac{2}{3}x_1 + \frac{4}{3}x_2,\ x_4 = -\frac{2}{3}x_1 - \frac{1}{3}x_2 \right\} \\ &= \left\{ (x_1, x_2, x_3, x_4) : \frac{2}{3}x_1 + \frac{4}{3}x_2 - x_3 = 0,\ x_4 + \frac{2}{3}x_1 + \frac{1}{3}x_2 = 0 \right\}. \end{aligned}$$

Az utolsó halmazt nevezzük az altér egyenletekkel való megadásának.

2.24. Példa. Az előző példában láttuk, hogy hogyan lehet egy generáló vektorokkal megadott alteret egyenletekkel leírni. Most ennek a fordítottját fogjuk elvégezni. Tekintsük a $\mathbb{R}^4$ vektortérben a

$$V = \{ (x_1, x_2, x_3, x_4) : 22x_1 - x_2 + 3x_3 = 0,\ 8x_1 + x_3 + x_4 = 0,\ 4x_1 + 2x_2 + 6x_4 = 0 \}$$

alteret. Az egyenletek közül valamelyiket kiválasztva (mondjuk az elsőt) kifejezzük az egyik változót (mondjuk az x_2-t) a többi segítségével, azaz

$$x_2 = 22x_1 + 3x_3.$$

Azt kaptuk, hogy x_2 kötött változó (azaz a többi ismeretében kiszámítható). Ezt a változót visszahelyettesítve a többi egyenltebe kapjuk, hogy

$$8x_1 + x_3 + x_4 = 0,\ 4x_1 + 2(22x_1 + 3x_3) + 6x_4 = 0,$$

azaz

$$8x_1 + x_3 + x_4 = 0,\ 48x_1 + 6x_3 + 6x_4 = 0.$$

Megint kiválasztunk egy egyenletet (mondjuk az elsőt), és kifejezünk egy változót (mondjuk x_3-at) és kapjuk, hogy

$$x_3 = -8x_1 - x_4$$

szintén kötött változó. Ezt visszahelyettesítve a maradék egyenletbe

$$48x_1 + 6(-8x_1 - x_4) + 6x_4 = 0,$$

amit egyszerűsítve azt kapjuk, hogy $0 = 0$, ami mindig teljesül. Az egyenletek elfogytak, az x_2 és x_3 változók kötöttek, a többi változó (azaz az x_1 és x_4) szabadon választható. A szabadon választható változók száma adja a dimenziót, azaz $\dim(V) = 2$. A homogén lineáris egyenletrendszert megoldhatjuk Gauss-eliminációval is. A szabadon választható változókba behelyettesítjük a 0 és 1 értékeket úgy, hogy mindig egy szabadon választható változó kapjon 1 értéket. Így

$$\begin{array}{llll} x_1 = 1, & x_4 = 0, & x_3 = -8 \cdot 1 - 0 = -8, & x_2 = 22 \cdot 1 + 3 \cdot (-8) = -2, \\ x_1 = 0, & x_4 = 1, & x_3 = -8 \cdot 0 - 1 = -1, & x_2 = 22 \cdot 0 + 3 \cdot (-1) = -3. \end{array}$$

A kapott vektorok $(1, -2, -8, 0)$ és $(0, -3, -1, 1)$ alkotják az altér bázisát.

2.25. Megjegyzés. Ha homogén lineáris egyenletrendszerrel megadott altér esetén keressük a generátorrendszert, akkor az egyenletrendszer megoldására használható a Gauss-elimináció is.

Videó: **Alterek metszete és összege**

2.26. Tétel (Alterek dimenziótétele)**.** Ha U és V véges dimenziós altér valamely vektortérben, akkor $U \cap V$ és $U + V$ is véges dimenziós, és

$$\dim(U \cap V) + \dim(U + V) = \dim(U) + \dim(V).$$

2.27. Példa. A 2.21. és 2.24. feladatokban megadott U és V alterekre kiszámoljuk $U \cap V$ dimenzióját és megadjuk egyenletek segítségével. Mind az U, mind a V altereket már megadtuk egyenletek segítségével. Az $U \cap V$ altérben azon vektorok vannak amelyek mind két egyenletrendszerben előforduló egyenletet teljesítik, azaz

$$U \cap V = \{(x_1, x_2, x_3, x_4) : \frac{2}{3}x_1 + \frac{4}{3}x_2 - x_3 = 0,\ x_4 + \frac{2}{3}x_1 + \frac{1}{3}x_2 = 0,$$
$$22x_1 - x_2 + 3x_3 = 0,\ 8x_1 + x_3 + x_4 = 0, 4x_1 + 2x_2 + 6x_4 = 0\}.$$

Itt a 2.24. példához hasonlóan az egyenletek visszafejtésével meghatározzuk a kötött és szabad változókat. Már tudjuk, hogy

$$x_2 = 22x_1 + 3x_3 \text{ és } x_3 = -8x_1 - x_4$$

kötött változók, így ezt már nem kell még egyszer kiszámolnunk. Ezt visszahelyettesítve az első két egyenletbe kapjuk, hogy

$$\frac{2}{3}x_1 + \frac{4}{3}x_2 - x_3 = \frac{2}{3}x_1 + \frac{4}{3}(22x_1 + 3(-8x_1 - x_4)) - (-8x_1 - x_4)$$
$$= (\frac{2}{3} + \frac{88}{3} - 32 + 8)x_1 + (-4 + 1)x_4 = 6x_1 - 3x_4 = 0,$$

és

$$x_4 + \frac{2}{3}x_1 + \frac{1}{3}x_2 = x_4 + \frac{2}{3}x_1 + \frac{1}{3}(22x_1 + 3(-8x_1 - x_4))$$
$$= (\frac{2}{3} + \frac{22}{3} - 8)x_1 + (1 - 1)x_4 = 0 \cdot x_1 + 0 \cdot x_4 = 0.$$

A második egyenletnél azt kaptuk, hogy $0 = 0$ ami mindig teljesül. Az elsőből pedig azt kapjuk hogy $x_4 = 2x_1$. Tehat az x_2, x_3, x_4 változók kötöttek, az x_1 szabadon választható, az $U \cap V$ altér egy dimenziós, melynek bázisa az

$$x_1 = 1, x_4 = 2, x_3 = -8 \cdot 1 - 2 = -10, x_2 = 22 \cdot 1 + 3 \cdot (-10) = -8,$$

számolás alapján $(1, -8 - 10, 2)$.

2.28. Példa. A 2.21. és 2.24. feladatokban megadott U és V alterekre megadjuk $U + V$ egy generátorrendszerét és dimenzióját. Mind a két altérnek tudjuk a generátorrendszerét, így az $U + V$ alteret ezen generátor vektorok összessége fogja generálni, azaz

$$U + V = [(1, 1, 2, -1),\ (-2, 1, 0, 1),\ (-3, 3, 2, 1),\ (1, -2, -8, 0),\ (0, -3, -1, 1)].$$

Ezt a 2.21. példához hasonlóan Gauss-elimináció segítségével bázissá alakíthatjuk, de ezt most itt nem tesszük meg. A dimenziót viszont az alterek dimenziótételéből egyből megkaphatjuk:

$$\dim(U + V) = \dim(U) + \dim(V) - \dim(U \cap V) = 2 + 2 - 1 = 3.$$

Videó: **Alterek egyértelmű megadása**

3. Lineáris leképezések

Videó: **Definíció, magtér és képtér**

3.1. Definíció. Legyen U és V ugyanazon T test feletti vektortér. A $\varphi : U \to V$ leképezést lineáris leképezésnek nevezzük (vagy vektortér homomorfizmusnak), ha bármely $u, v \in U$ és $\lambda \in T$ esetén

$$(u+v)\varphi = u\varphi + v\varphi \quad \text{és} \quad (\lambda u)\varphi = \lambda(u\varphi).$$

Az U-ból V-be menő lineáris leképezések halmazát $\hom(U, V)$ jelöli. Az U-ból U-ba menő lineáris leképezéseket lineáris transzformációknak nevezzük. A bijektív lineáris leképezések a vektortér izomorfizmusok, továbbá a bijektív lineáris transzformációk a vektortér automorfizmusok.

3.2. Definíció. Legyen $\varphi \in \hom(U, V)$ lineáris leképezés. A

$$\begin{aligned} \operatorname{Ker}\varphi &= \{u \in U : u\varphi = 0\}, \\ \operatorname{Im}\varphi &= \{u\varphi : u \in U\} \end{aligned}$$

halmazokat rendre a φ lineáris leképezés magjának, illetve képterének nevezzük.

3.3. Tétel. Legyen U és V ugyanazon T test feletti vektortér. Tetszőleges $\varphi \in \hom(U, V)$ lineáris leképezésre érvényesek a következők:

1. $0\varphi = 0$,
2. $\operatorname{Ker}\varphi$ altér U-ban,
3. $\operatorname{Im}\varphi$ altér V-ben,
4. φ akkor és csak akkor injektív, ha $\operatorname{Ker}\varphi = \{0\}$,
5. Ha $u_1, \dots, u_k$ generátorrendszer U-ban, akkor $u_1\varphi, \dots, u_k\varphi$ generátorrendszer az $\operatorname{Im}\varphi$ képtérben.
6. Ha $u_1\varphi, \dots, u_k\varphi$ lineárisan független vektorrendszer V-ben, akkor $u_1, \dots, u_k$ lineárisan független U-ban.

3.4. Tétel (Lineáris leképezések dimenziótétele)**.** Legyen U és V ugyanazon T test feletti vektortér, és $\varphi \in \hom(U, V)$. Ha U végesdimenziós, akkor

$$\dim(U) = \dim(\operatorname{Ker}\varphi) + \dim(\operatorname{Im}\varphi).$$

3.5. Következmény. Végesdimenziós vektortér lineáris transzformációja akkor és csak akkor injektív, ha szürjektív.

3.6. Következmény. Legyen T test, $m, n \geqslant 1$ és $A \in T^{m\times n}$. Az $Ax = 0$ homogén lineáris egyenletrendszer megoldásalterének dimenziója (azaz a szabad változók száma) $n - r(A)$.

3.7. Tétel. Ha V a T test feletti n-dimenziós vektortér, akkor V izomorf a T^n vektortérrel. Tehát bármely két T-feletti n-dimenziós vektortér izomorf egymással.

3.8. Definíció. Legyenek U és V ugyanazon T test feletti vektorterek. A $\varphi, \psi \in \hom(U, V)$ lineáris leképezések összegén, illetve a φ leképezés $c \in T$ skalárral való szorzatán azt a $\varphi + \psi : U \to V$, illetve $c\varphi : U \to V$ leképezéseket értjük, amelyekre

$$u(\varphi + \psi) = u\varphi + u\psi, \qquad u(c\varphi) = c(u\varphi) \qquad \text{minden } u \in U \text{ esetén.}$$

3.9. Tétel. Tetszőleges U és V ugyanazon T test feletti vektorterek esetén $\hom(U, V)$ a fent definiált műveletekkel vektorteret alkot T felett.

3.10. Tétel. Tetszőleges U, V és W ugyanazon T test feletti vektorterekre érvényesek a következők:

1. Ha $\varphi \in \hom(U, V)$ és $\psi \in \hom(V, W)$, akkor $\varphi\psi \in \hom(U, W)$.
2. Ha $\varphi \in \hom(U, V)$ bijektív, akkor $\varphi^{-1} \in \hom(V, U)$.
3. Ha $\varphi \in \hom(U, V)$, $\psi \in \hom(V, W)$ és $c \in T$, akkor $c(\varphi\psi) = (c\varphi)\psi = \varphi(c\psi)$.
4. Ha $\varphi, \psi \in \hom(U, V)$ és $\tau \in \hom(V, W)$, akkor $(\varphi + \psi)\tau = \varphi\tau + \psi\tau$.
5. Ha $\varphi \in \hom(U, V)$ és $\psi, \tau \in \hom(V, W)$, akkor $\varphi(\psi + \tau) = \varphi\psi + \varphi\tau$.

3.11. Tétel. Legyen U végesdimenziós, V pedig tetszőleges ugyanazon T test feletti vektortér, $e_1, \dots, e_n \in U$ bázis és $v_1, \dots, v_n \in V$ tetszőleges vektorrendszer. Ekkor létezik egy egyértelműen meghatározott $\varphi \in \hom(U, V)$ lineáris leképezés, amelyre

$$e_1\varphi = v_1, e_2\varphi = v_2, \dots, e_n\varphi = v_n.$$

Videó: **Leképezések mátrixa**

3.12. Definíció. Legyenek U és V végesdimenziós vektorterek a T test felett az $\mathcal{E} : e_1, \dots, e_m \in U$ és $\mathcal{F} : f_1, \dots, f_n \in V$ bázisokkal. Tetszőleges $\varphi \in \hom(U, V)$ lineáris leképezésre léteznek olyan egyértelműen meghatározott $a_{i,j} \in T$ skalárok, hogy

$$e_i\varphi = \sum_{j=1}^{n} a_{i,j} f_j \qquad \text{minden } i = 1, \dots, m \text{ esetén.}$$

Az $(a_{i,j})_{m\times n}$ mátrixot a φ lineáris leképezés $\mathcal{E}$ és $\mathcal{F}$ bázisokban megadott mátrixának nevezzük.

3.13. Példa. Megadjuk a $\varphi : \mathbb{R}^3 \to \mathbb{R}^2$, $(x, y, z)\varphi = (x + 2y, y + z)$ lineáris leképezés mátrixát az $\mathcal{E} : (1, 0, 0), (1, 0, -1), (1, 1, 1)$, valamint az $\mathcal{F} : (1, 0), (1, -1)$ bázisok esetén. Keressük azt az $A = (a_{ij})_{3\times 2}$ mátrixot, amelyre teljesül:

$$\begin{aligned}
(1,0,0)\varphi &= (1,0) = a_{11}(1,0) + a_{12}(1,-1)\\
(1,0,-1)\varphi &= (1,-1) = a_{21}(1,0) + a_{22}(1,-1)\\
(1,1,1)\varphi &= (3,2) = a_{31}(1,0) + a_{32}(1,-1).
\end{aligned}$$

Az első egyenletből az $a_{11} + a_{12} = 1$, valamint a $-a_{12} = 0$ összefüggéseket kapjuk, melynek megoldása: $a_{11} = 1$, $a_{12} = 0$. Hasonlóan a másodikból megkapható, hogy $a_{21} = 0$ és $a_{22} = 1$, a harmadikból pedig $a_{31} = 5$, $a_{32} = -2$ adódik. Tehát a φ lineáris leképezés mátrixa az $\mathcal{E}$ és $\mathcal{F}$ bázisokban:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 5 & -2 \end{pmatrix}.$$

3.14. Tétel. Legyenek U és V végesdimenziós vektorterek a T test felett az $\mathcal{E} : e_1, \dots, e_m \in U$ és $\mathcal{F} : f_1, \dots, f_n \in V$ bázisokkal, továbbá legyen $A \in T^{m\times n}$ a $\varphi \in \hom(U, V)$ lineáris leképezés $\mathcal{E}$ és $\mathcal{F}$ bázisokban megadott mátrixa. Ha az $u \in U$ vektor koordinátasora az $\mathcal{E}$ bázisban $x = (x_1, \dots, x_m)$, akkor az $u\varphi \in V$ vektor koordinátasora az $\mathcal{F}$ bázisban xA.

3.15. Tétel. Legyenek $\mathcal{E}$, $\mathcal{F}$ és $\mathcal{G}$ rendre az U, V és W ugyanazon T test feletti végesdimenziós vektorterek bázisai. Legyen A és B rendre a $\varphi, \psi \in \hom(U, V)$ lineáris leképezések mátrixai az $\mathcal{E}$ és $\mathcal{F}$ bázisokban, illetve C a $\tau \in \hom(V, W)$ lineáris leképezés mátrixa az $\mathcal{F}$ és $\mathcal{G}$ bázisokban, és legyen $c \in T$. Ekkor

1. $A + B$ a $\varphi + \psi$ lineáris leképzés mátrixa az $\mathcal{E}$ és $\mathcal{F}$ bázisokban,
2. cA a $c\varphi$ lineáris leképezés mátrixa az $\mathcal{E}$ és $\mathcal{F}$ bázisokban,
3. AC a $\varphi\tau$ lineáris leképezés mátrixa az $\mathcal{E}$ és $\mathcal{G}$ bázisokban.

3.16. Következmény. Ha U m-dimenziós és V n-dimenziós vektortér a T test felett, akkor a lineáris leképezések $\hom(U, V)$ vektortere izomorf az $m \times n$-es mátrixok $T^{m\times n}$ vektorterével, és így mn dimenziós.

Videó: **Bázisáttérés**

3.17. Definíció. Legyen $\mathcal{E} : e_1, \dots, e_m$ és $\mathcal{E}' : e'_1, \dots, e'_m$ a T test feletti U vektortér két bázisa. Az $\mathrm{id} \in \hom(U, U)$ identikus lineáris leképezés $\mathcal{E}$ és $\mathcal{E}'$ bázisokban megadott mátrixát az $\mathcal{E}$ bázisról az $\mathcal{E}'$ bázisra való áttérés mátrixának hívjuk.

3.18. Példa. Tekintsük az $\mathbb{R}^3$ vektortér $\mathcal{E} : (1, 0, 0), (1, 0, -1), (1, 1, 1)$ és $\mathcal{E}' : (0, 0, 1), (1, 1, 1), (0, -1, -2)$ bázisait. Megadjuk az $\mathcal{E}$ bázisról az $\mathcal{E}'$ bázisra való áttérés mátrixát, ami az előző definíció szerint az identikus leképezés mátrixával egyezik meg. Keressük azt a $P = (p_{ij})_{3\times 3}$ mátrixot, amelyre teljesül, hogy

$$\begin{aligned}
(1,0,0)\mathrm{id} &= (1,0,0) = p_{11}(0,0,1) + p_{12}(1,1,1) + p_{13}(0,-1-2)\\
(1,0,-1)\mathrm{id} &= (1,0,-1) = p_{21}(0,0,1) + p_{22}(1,1,1) + p_{23}(0,-1-2)\\
(1,1,1)\mathrm{id} &= (1,1,1) = p_{31}(0,0,1) + p_{32}(1,1,1) + p_{33}(0,-1-2).
\end{aligned}$$

Az első egyenletből a $p_{12} = 1$, $p_{12} - p_{13} = 0$ és a $p_{11} + p_{12} - 2p_{13} = 0$ összefüggéseket kapjuk, melynek megoldása: $p_{11} = p_{12} = p_{13} = 1$. A második egyenletből hasonlóan számítható, hogy $p_{21} = 0$, $p_{22} = p_{23} = 1$, a harmadikból pedig $p_{31} = p_{33} = 0$ és $p_{32} = 1$ adódik. Tehát az $\mathcal{E}$ bázisról az $\mathcal{E}'$ bázisra való áttérés mátrixa:

$$P = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

3.19. Tétel. Legyen a T test feletti U vektortér két bázisa $\mathcal{E}$ és $\mathcal{E}'$, továbbá legyen P az áttérés mátrixa az $\mathcal{E}$ bázisról az $\mathcal{E}'$ bázisra. Ekkor P nemelfajuló mátrix, továbbá az $\mathcal{E}'$ bázisról az $\mathcal{E}$ bázisra való áttérés mátrixa P^{-1}.

3.20. Tétel. Legyenek U és V ugyanazon T test feletti vektorterek, $\mathcal{E}$ és $\mathcal{E}'$ az U, $\mathcal{F}$ és $\mathcal{F}'$ pedig a V vektortér bázisa. Jelölje P, illetve S az áttérés mátrixát $\mathcal{E}$-ről $\mathcal{E}'$-re, illetve $\mathcal{F}$-ről $\mathcal{F}'$-re. Legyen $\varphi \in \hom(U, V)$ lineáris leképezés, és legyen φ mátrixa az $\mathcal{E}$ és $\mathcal{F}$ bázisokban A. Ekkor φ mátrixa az $\mathcal{E}'$ és $\mathcal{F}'$ bázisokban $P^{-1}AS$.

3.21. Példa. Tekintsük a $\varphi : \mathbb{R}^3 \to \mathbb{R}^2$, $(x, y, z)\varphi = (x + 2y, y + z)$ lineáris leképezést, és az $\mathbb{R}^3$ vektortér $\mathcal{E}' : (0, 0, 1), (1, 1, 1), (0, -1, -2)$, illetve az $\mathbb{R}^2$ vektortér $\mathcal{F}' : (0, -1), (1, 2)$ bázisát. Az 3.20. tétel segítségével megadjuk a φ mátrixát az $\mathcal{E}'$ és $\mathcal{F}'$ bázisokban úgy, hogy felhasználjuk, hogy a 3.13. példában megadtuk a φ leképezés A mátrixát az $\mathcal{E}$ és $\mathcal{F}$ bázisokban, a 3.18. példában pedig az $\mathcal{E}$ bázisról az $\mathcal{E}'$ bázisra való áttérés P mátrixát. Ahhoz, hogy a 3.13. példában szereplő A mátrixot felhasználhassuk a 3.20. tétel szerint ki kell még számolnunk az $\mathcal{F} : (1, 0), (1, -1)$ bázisról az $\mathcal{F}'$ bázisra való áttérés $S = (s_{ij})_{2\times 2}$ mátrixát, amelyre teljesül, hogy:

$$(1, 0)\mathrm{id} = (1, 0) = s_{11}(0, -1) + s_{12}(1, 2)$$
$$(1, -1)\mathrm{id} = (1, -1) = s_{21}(0, -1) + s_{22}(1, 2).$$

Amiből megkapjuk, hogy $s_{11} = 1$, $s_{12} = 1$, $s_{21} = 3$ és $s_{22} = 1$. Meg kell még határoznunk P^{-1}-et:

$$P^{-1} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix}.$$

Tehát a φ lineáris leképezés A' mátrixát a 3.20. tétel alapján következőképpen kapjuk:

$$A' = P^{-1}AS = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 5 & -2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 4 & 3 \\ -1 & -2 \end{pmatrix}.$$

3.22. Definíció. Legyen T test és n pozitív egész. Az $A, B \in T^{n\times n}$ mátrixok hasonlók, ha létezik olyan nemelfajuló $P \in T^{n\times n}$ mátrix, hogy $A = P^{-1}BP$.

3.23. Következmény. Ugyanazon lineáris transzformáció két különböző bázisban felírt mátrixa hasonló.

3.24. Definíció. A φ lineáris leképezés rangján a képterének dimenzióját értjük, azaz $r(\varphi) = \dim(\operatorname{Im} \varphi)$.

3.25. Tétel. Véges dimenziós vektorterek közötti lineáris leképezés rangja megegyezik valamely (bármely) bázisbeli mátrixának rangjával.

3.26. Következmény. Legyen φ lineáris transzformáció valamely végesdimenziós vektortérben. Ekkor φ akkor és csak akkor bijektív, ha valamely (bármely) bázisbeli mátrixa nemelfajuló.

3.27. Tétel. Legyen U m-dimenziós és V n-dimenziós vektorterek ugyanazon T test fölött, és $\varphi \in \hom(U, V)$. Ekkor φ mátrixa az U és V egy-egy alkalmas bázisában

$$\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} \in T^{m\times n},$$

ahol r a φ rangja, E_r az $r \times r$ méretű egységmátrix, és a zérók a megfelelő méretű zérómátrixok.

3.28. Következmény. Legyen T tetszőleges test. Ekkor minden $A \in T^{m\times n}$ mátrixhoz létezik olyan nemelfajuló $P \in T^{m\times m}$ és $Q \in T^{n\times n}$ mátrixok, hogy

$$PAQ = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix},$$

ahol r az A mátrix rangja, és a jobboldalon álló mátrix ugyanaz, mint az előző tételben.

Videó: **Sajátvektor és sajátérték**

3.29. Definíció. Legyen T test, V vektortér T felett, és $\varphi \in \hom(V, V)$. A $\lambda \in T$ skalár a φ lineáris transzformáció sajátértéke, ha létezik olyan nemnulla $v \in V$ vektor, hogy $v\varphi = \lambda v$. A

$$\{v \in V : v\varphi = \lambda v\}$$

alteret a $\lambda \in T$ skalárhoz tartozó sajátaltérnek nevezzük. A nemnulla $v \in V$ vektor a φ lineáris transzformáció sajátvektora, ha valamely sajátaltérben benne van, azaz létezik olyan $\lambda \in T$, hogy $v\varphi = \lambda v$.

3.30. Definíció. Legyen T test, n pozitív egész. Az $A \in T^{n\times n}$ mátrix sajátértéke, sajátaltere és sajátvektora rendre a $\varphi : T^n \to T^n$, $x \mapsto xA$ lineáris transzformáció sajátértéke, sajátaltere, illetve sajátvektora. Azaz $\lambda \in T$ és $x \in T^n$ akkor és csak akkor sajátérték, sajátvektor pár, ha $xA = \lambda x$.

3.31. Tétel. Legyen V n-dimenziós vektortér a T test felett, $e_1, \dots, e_n$ bázis V-ben, $\varphi \in \hom(V, V)$ és $A \in T^{n\times n}$ a φ lineáris transzformáció mátrixa az $e_1, \dots, e_n$ bázisban. Ekkor $\lambda \in T$ és $v \in V$ akkor és csak akkor sajátérték, sajátvektor párja φ-nek, ha λ és v koordinátasora sajátérték, sajátvektor párja A-nak.

3.32. Tétel. Legyen U tetszőleges vektortér a T test felett, $\lambda_1, \dots, \lambda_k \in T$ páronként különböző sajátértékei a $\varphi \in \hom(U, U)$ lineáris transzformációnak, és $U_1, \dots, U_k$ pedig ezen sajátértékekhez tartozó sajátalterek. Ha $U_1 + \cdots + U_k = U$, akkor φ egyértelműen meghatározott.

3.33. Definíció. Az $A \in T^{n\times n}$ mátrix karakterisztikus polinomja az

$$f_A(x) = |A - xE|$$

determinánssal megadott T-feletti polinom. Az $f_A(x)$ polinom T-be eső gyökeit az A mátrix karakterisztikus gyökeinek nevezzük.

3.34. Tétel. Legyen T test. A $\lambda \in T$ skalár akkor és csak akkor sajátértéke az $A \in T^{n\times n}$ mátrixnak, ha λ karakterisztikus gyöke A-nak.

3.35. Tétel. Hasonló mátrixok karakterisztikus polinomja megegyezik.

3.36. Definíció. Véges dimenziós vektortér lineáris transzformációjának karakterisztikus polinomja a lineáris transzformáció valamely (bármely) bázisban felírt mátrixának karakterisztikus polinomja.

4. Polinomok

Videó: **Alapvető definíciók**

4.1. Példa. A következő algebrai struktúrák gyűrűk:
1. $(\mathbb{R};+,\cdot)$, $(\mathbb{Q};+,\cdot)$, $(\mathbb{C};+,\cdot)$, és általában minden test,
2. $(\mathbb{Z};+,\cdot)$, $(\mathbb{P};+,\cdot)$ ahol $\mathbb{P}=\{2a : a\in\mathbb{Z}\}$,
3. $(\mathbb{Z}_n;+,\cdot)$ (modulo n maradékosztályok),
4. $(P(U);\triangle,\cap)$ tetszőleges U halmazra.
5. $(T^{n\times n};+,\cdot)$ tetszőleges T testre,
6. $(R^{n\times n};+,\cdot)$ tetszőleges kommutatív R gyűrűre,
7. test feletti egyváltozós polinomok.

4.2. Tétel. Tetszőleges kommutatív, egységelemes R gyűrűben teljesülnek a következő tulajdonságok:
1. $0\cdot a = a\cdot 0 = 0$ ahol 0 az R gyűrű zéruseleme,
2. $(-a)b = a(-b) = -(ab)$,
3. $(a_1+\cdots+a_m)(b_1+\cdots+b_n) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_ib_j$ (általános disztributivitás),
4. $(a+b)^n = \sum_{i=0}^{n}\binom{n}{i}\cdot a^ib^{n-i}$ (binomiális tétel).

4.3. Definíció. A T test fölötti egyhatározatlanú polinomok az

$$a_0+a_1x+\cdots+a_nx^n \quad (a_i\in T)$$

formális kifejezések, amelyek halmazát $T[x]$-el jelöljük. Ha $a_{i+1}=a_{i+2}=\cdots=a_n=0$, akkor az $a_0+a_1x+\cdots+a_nx^n$ és $a_0+a_1x+\cdots+a_ix^i$ polinomokat egyenlőknek tekintjük (tehát a kezdő zéró együtthatós tagokat figyelmen kívül hagyjuk). Az $a\in T$ elemeket konstans polinomoknak hívjuk.

4.4. Definíció. Legyen T test. Az $f=a_0+a_1x+\cdots+a_nx^n\in T[x]$ polinom polinomfüggvényén az

$$f(c)=\sum_{i=0}^{n} a_ic^i \qquad (c\in T)$$

képlet szerint definiált $f(x): T\to T$ leképezést értjük.

4.5. Példa. A $\mathbb{Z}_2$ test feletti $f=0$ és $g=x+x^2$ polinomokra $f\neq g$ de $f(x)=g(x)$. De tetszőleges $f,g\in\mathbb{R}[x]$ polinomokra $f=g$ akkor és csak akkor, ha $f(x)=g(x)$.

4.6. Definíció. Legyen T tetszőleges test és

$$f=a_0+a_1x+\cdots+a_nx^n\in T[x], \qquad g=b_0+b_1x+\cdots+b_mx^m\in T[x].$$

Az f és g polinomok összegén az

$$f+g=\sum_{i=0}^{\max(n,m)}(a_i+b_i)x^i,$$

polinomot értjük, ahol $a_i=0$, illetve $b_i=0$ értendő, ha $i>n$, illetve $i>m$. Az f és g szorzatán az

$$fg=\sum_{i=0}^{n+m}\left(\sum_{j=0}^{i}a_jb_{i-j}\right)x^i.$$

polinomot értjük.

4.7. Tétel. Tetszőlges T test esetén $T[x]$ kommutatív egységelemes gyűrűt alkot az előbb definiált műveletekkel, amit a T test feletti egyhatározatlanú polinomgyűrűnek hívunk.

4.8. Definíció. Ha az $f=a_0+a_1x+\cdots+a_nx^n\in T[x]$ polinomban $a_n\neq 0$, akkor az n számot az f polinom fokszámának és az a_n elemet az f polinom főegyütthatójának hívjuk. Az f polinomot főpolinomnak nevezzük, ha f főegyütthatója $1\in T$. Tehát a 0 polinomnak nincsen fokszáma (se főegyütthatója), de kényelmes lesz bevezetni a következő jelölést:

$$\deg f=\begin{cases} f \text{ fokszáma}, & \text{ha } f\neq 0,\\ -1, & \text{ha } f=0.\end{cases}$$

4.9. Tétel. Legyen T tetszőleges test és $f, g \in T[x]$ nemzéró polinomok. Ekkor

$$\deg(f+g) \leqslant \max(\deg f, \deg g) \quad \text{és} \quad \deg(fg) = \deg f + \deg g.$$

4.10. Definíció. Az R gyűrűt zérusosztómentesnek nevezzük, ha bármely két 0-tól különböző elem szorzata 0-tól különböző.

4.11. Következmény. Tetszőleges T test esetén $T[x]$ zérusosztómentes.

4.12. Tétel. Tetszőleges zérusosztómentes R gyűrűben teljesülnek a következő ún. kancellatív tulajdonságok:
1. ha $ac = bc$ és $c \neq 0$, akkor $a = b$,
2. ha $ab = ac$ és $a \neq 0$, akkor $b = c$.

Videó: **Oszthatóság**

4.13. Definíció. Legyen T tetszőleges test és $f, g \in T[x]$. Azt mondjuk, hogy f osztója g-nek, vagy g többszöröse f-nek, és azt írjuk, hogy $f \mid g$, ha van olyan $h \in T[x]$ polinom, amelyre $fh = g$.

4.14. Tétel. Tetszőleges T test feletti $T[x]$ polinomgyűrűben teljesülnek a következő oszthatósági tulajdonságok:
1. $f \mid f$,
2. ha $f \mid g$ és $g \mid h$, akkor $f \mid h$,
3. ha $f \mid g$ és $g \mid f$, akkor $f = cg$ valamely $c \in T \setminus \{0\}$ elemre,
4. $1 \mid f$ és $f \mid 0$,
5. $0 \mid f$ akkor és csak akkor, ha $f = 0$,
6. $f \mid 1$ akkor és csak akkor, ha $f \in T \setminus \{0\}$,
7. ha $f \mid g$ és $f \mid h$, akkor $f \mid g + h$ és $f \mid g - h$,
8. ha $f \mid g$ és $h \mid p$, akkor $fh \mid gp$,
9. ha $fh \mid gh$ és $h \neq 0$, akkor $f \mid g$.
10. ha $f \mid g$ és $g \neq 0$, akkor $\deg f \leqslant \deg g$.

4.15. Definíció. Az f és g polinomok asszociáltak, ha $f|g$ és $g|f$, amelyet az $\sim$ relációval jelölünk.

4.16. Példa. $\mathbb{Z}_3[x]$-ben $\overline{2}x^3 + x + \overline{2} \sim x^3 + \overline{2}x + \overline{1}$, valamint $\mathbb{R}[x]$-ben $6x^2 + 2x + 1 \sim x^2 + \frac{1}{3}x + \frac{1}{6}$.

4.17. Következmény. Az asszociáltság ekvivalenciareláció a polinomok halmazán. A 0 polinomhoz semelyik másik polinom sem asszociált. A $\{0\}$ osztályt kivéve minden asszociáltsági osztályban pontosan egy főpolinom van.

Videó: **Legnagyobb közös osztó**

4.18. Definíció. A h polinom az f, g polinomok legnagyobb közös osztója, ha
1. $h \mid f$ és $h \mid g$ (azaz közös osztó), és
2. ha $p \mid f$ és $p \mid g$, akkor $p \mid h$ (azaz minden közös osztónak a többszöröse).

Hasonlóan, a h polinom az f, g polinomok legkisebb közös többszöröse, ha
1. $f \mid h$ és $g \mid h$ (azaz közös többszörös), és
2. ha $f \mid p$ és $g \mid p$, akkor $h \mid p$ (azaz minden közös többszörösnek az osztója).

4.19. Tétel. A legnagyobb közös osztó (és a legkisebb közös többszörös) asszociáltság erejéig egyértelműen meghatározott. Tehát, ha h az f és g polinomok legnagyobb közös osztója, akkor h minden asszociáltja is legnagyobb közös osztó és rajtuk kívül nincs más legnagyobb közös osztó.

4.20. Definíció. Az f és g polinomok legnagyobb közös osztóját $\mathrm{lnko}(()f, g)$-vel jelöljük, és általában nem azt írjuk, hogy $h = \mathrm{lnko}(()f, g)$, hanem azt, hogy $h \sim \mathrm{lnko}(()f, g)$. Hasonlóan a legkisebb közös többszöröst $\mathrm{lkkt}(()f, g)$-vel jelöljük.

4.21. Definíció. Az f és g polinomok relatív prímek, ha $\mathrm{lnko}(()f, g) \sim 1$.

4.22. Tétel. Legyen T test, $f, g \in T[x]$ és $g \neq 0$. Ekkor léteznek olyan egyértelműen meghatározott $q, r \in T[x]$ polinomok, amelyekre $f = qg + r$ és $\deg r < \deg g$. Ezt a műveletet maradékos osztásnak nevezzük, ahol f az osztandó, g az osztó, q a hányados és r a maradék.

4.23. Tétel (Euklideszi algoritmus)**.** Bármely két $f, g \in T[x]$ polinomnak van legnagyobb közös osztója, amely a következő maradékos osztások elvégzésével megkapható:

$$\begin{aligned} f &= q_1 g + r_2 & (\deg r_2 < \deg g)\\ g &= q_2 r_2 + r_3 & (\deg r_3 < \deg r_2)\\ r_2 &= q_3 r_3 + r_4 & (\deg r_4 < \deg r_3)\\ &\vdots & \vdots\\ r_{i-1} &= q_i r_i + r_{i+1} & (\deg r_{i+1} < \deg r_i) \end{aligned}$$

Az eljárás véges számú lépés után véget ér, azaz létezik olyan $n \in \mathbb{N}$, hogy $r_{n+1} = 0$. A legnagyobb közös osztó az utolsó nemnulla maradék, azaz $\operatorname{lnko}(()f, g) \sim r_n$. Az eljárás során kapott egyenleteket visszafejtve olyan u és v polinomokat kapunk, hogy $\operatorname{lnko}(()f, g) = fu + gv$.

4.24. Példa. Euklideszi algoritmus segítségével meghatározzuk $\operatorname{lnko}(()f, g)$-t, ahol $f, g \in \mathbb{Z}_5[x]$, $f = \overline{2}x^4 + \overline{3}x^3 + \overline{3}x^2 + \overline{2}x$, $g = x^3 + \overline{3}x + \overline{1}$. A maradékos osztások elvégzésével kapjuk:

$$\begin{aligned} \overline{2}x^4 + \overline{3}x^3 + \overline{3}x^2 + \overline{2}x &= (\overline{2}x + \overline{3})(x^3 + \overline{3}x + \overline{1}) + \overline{2}x^2 + x + \overline{2}\\ x^3 + \overline{3}x + \overline{1} &= (\overline{3}x + \overline{1})(\overline{2}x^2 + x + \overline{2}) + x + \overline{4}\\ \overline{2}x^2 + x + \overline{2} &= (\overline{2}x + \overline{3})(x + \overline{4}) + \overline{0}. \end{aligned}$$

Így a legnagyobb közös osztó: $\operatorname{lnko}(()f, g) \sim x + \overline{4}$.

4.25. Tétel. Bármely $f, g, h \in T[x]$ polinomra teljesülnek az alábbiak.

1. $\operatorname{lnko}(()\operatorname{lnko}(()f, g), h) \sim \operatorname{lnko}(()f, \operatorname{lnko}(()g, h))$,
2. $\operatorname{lnko}(()f, g) \sim \operatorname{lnko}(()g, f)$,
3. $\operatorname{lnko}(()f, g) \sim f \iff f \mid g$,
4. $\operatorname{lnko}(()f, f) \sim f$,
5. $\operatorname{lnko}(()0, f) \sim f$,
6. $\operatorname{lnko}(()1, f) \sim 1$,
7. $\operatorname{lnko}(()f, g) \sim 0 \iff f = g = 0$,
8. $\operatorname{lnko}(()f, g) \sim \operatorname{lnko}(()f + gh, g)$,
9. $\operatorname{lnko}(()f, g) \cdot h \sim \operatorname{lnko}(()fh, gh)$,
10. $\operatorname{lnko}(()f, g) \neq 0 \implies \operatorname{lnko}(()f/\operatorname{lnko}(()f, g), g/\operatorname{lnko}(()f, g)) \sim 1$
11. $\operatorname{lnko}(()f, g) \sim 1 \implies \operatorname{lnko}(()f, gh) \sim \operatorname{lnko}(()f, h)$.

4.26. Következmény. Bármely $f, g, h \in T[x]$ polinomra teljesülnek az alábbiak.

1. ha $\operatorname{lnko}(()f, g) \sim 1$, $f \mid h$ és $g \mid h$, akkor $fg \mid h$;
2. ha $\operatorname{lnko}(()f, g) \sim 1$ és $f \mid gh$, akkor $f \mid h$;
3. ha $\operatorname{lnko}(()f, g) \neq 0$ és $f \mid gh$, akkor $f/\operatorname{lnko}(()f, g) \mid h$.

4.27. Tétel. Tetszőleges $f, g \in T[x]$ polinomokra

$$\operatorname{lnko}(()f, g) \cdot \operatorname{lkkt}(()f, g) \sim fg.$$

4.28. Tétel. Tetszőleges adott $f, g, h \in T[x]$ polinomok esetén az $fu + gv = h$ diofantoszi egyenlet akkor és csak akkor oldható meg az $u, v \in T[x]$ polinomokra nézve, ha $\operatorname{lnko}(()f, g) \mid h$. Ha u_0, v_0 egy megoldás, akkor az általános megoldás

$$u = u_0 + \frac{g}{\operatorname{lnko}(()f, g)} \cdot t, \qquad v = v_0 - \frac{f}{\operatorname{lnko}(()f, g)} \cdot t,$$

ahol $t \in T[x]$ tetszőlegesen választható.

4.29. Példa. Megoldjuk az $fu + gv = h$ diofantoszi egyenletet, ahol $f, g, h \in \mathbb{Z}_5[x]$, $f = \overline{2}x^4 + \overline{3}x^3 + \overline{3}x^2 + \overline{2}x$, $g = x^3 + \overline{3}x + \overline{1}$ és $h = \overline{2}x^2 + \overline{4}x + \overline{4}$. A 4.24. példában megadtuk, hogy $\operatorname{lnko}(()f, g) \sim x + \overline{4}$. A diofantoszi egyenlet megoldható, ugyanis $h = \overline{2}x^2 + \overline{4}x + \overline{4} = (\overline{2}x + 1)(x + \overline{4})$, így az előző tételben megadott feltétel teljesül. A 4.24. példában szereplő euklideszi algoritmus lépéseinél kifejezzük a maradékot:

$$\begin{aligned} \overline{2}x^2 + x + \overline{2} &= \overline{2}x^4 + \overline{3}x^3 + \overline{3}x^2 + \overline{2}x - (\overline{2}x + \overline{3})(x^3 + \overline{3}x + \overline{1})\\ x + \overline{4} &= x^3 + \overline{3}x + \overline{1} - (\overline{3}x + \overline{1})(\overline{2}x^2 + x + \overline{2}). \end{aligned}$$

Az utolsó egyenlőségtől indulva behelyettesítjük az előző sorban szereplő különbséget, és a zárójeleket felbontjuk úgy, hogy f és g polinomok többszöröseinek összege szerepeljen:

$$\begin{aligned} x+\overline{4} &= x^3+\overline{3}x+\overline{1}-(\overline{3}x+\overline{1})(\overline{2}x^2+x+\overline{2}) = \\ &= x^3+\overline{3}x+\overline{1}-(\overline{3}x+\overline{1})[\overline{2}x^4+\overline{3}x^3+\overline{3}x^2+\overline{2}x-(\overline{2}x+\overline{3})(x^3+\overline{3}x+\overline{1})] = \\ &= (\overline{2}x^4+\overline{3}x^3+\overline{3}x^2)(\overline{2}x+\overline{4})+(x^3+\overline{3}x+\overline{1})(x^2+x+\overline{4}) \end{aligned}$$

A cél az, hogy az $fu+gv=h$ diofantoszi egyenletet megoldjuk, ahogy korábban már láttuk a h többszöröse a legnagyobb közös osztónak ($h=\overline{2}x^2+\overline{4}x+\overline{4}=(\overline{2}x+1)(x+\overline{4})$), így $\overline{2}x+1$-gyel szorozva az előző egyenlőséget megkapjuk a diofantoszi egyenlet egy megoldását:

$$\overline{2}x^2+\overline{4}x+\overline{4}=(\overline{2}x^4+\overline{3}x^3+\overline{3}x^2)(\overline{4}x^2+\overline{4})+(x^3+\overline{3}x+\overline{1})(\overline{2}x^3+\overline{3}x^2+\overline{4}x+\overline{4}).$$

Így az általános megoldás:

$$u=\overline{4}x^2+\overline{4}+\frac{x^3+\overline{3}x+\overline{1}}{x+\overline{4}}\cdot t, \qquad v=\overline{2}x^3+\overline{3}x^2+\overline{4}x+\overline{4}-\frac{\overline{2}x^4+\overline{3}x^3+\overline{3}x^2}{x+\overline{4}}\cdot t,$$

ahol $t\in\mathbb{Z}_5[x]$ tetszőlegesen választható.

Videó: **Polinomok gyökei, Horner-elrendezés**

4.30. Definíció. Az $a\in T$ elem gyöke (más szóval zérushelye) az $f\in T[x]$ polinomnak, ha $f(a)=0$.

4.31. Tétel (Bézout tétele)**.** Bármely $f\in T[x]$ és $a\in T$ esetén

$$f(a)=0 \iff x-a \mid f.$$

4.32. Tétel (Horner-módszer)**.** Legyen $f=a_nx^n+\cdots+a_1x+a_0\in T[x]$ egy n-edfokú polinom és $c\in T$. A Horner-módszerrel elkészített táblázat:

	a_n	a_{n-1}	$\cdots$	a_1	a_0
c	b_n	b_{n-1}	$\cdots$	b_1	b_0

ahol

$$\begin{aligned} b_n &= a_n, \\ b_i &= b_{i+1}\cdot c+a_i \qquad (i=n-1,\dots,0). \end{aligned}$$

Ekkor b_0 nem más, mint az f-nek az $x-c$ polinommal való osztásakor keletkező maradék, $b_nx^{n-1}+\cdots+b_2x+b_1$ pedig ugyanezen osztás hányadosa:

$$f=(x-c)\cdot(b_nx^{n-1}+\cdots+b_2x+b_1)+b_0.$$

4.33. Definíció. Az $f\in T[x]$ polinomnak az $a\in T$ elem k-szoros gyöke, ha $(x-a)^k\mid f$, de $(x-a)^{k+1}\nmid f$. A $k\in\mathbb{N}$ számot az a gyök multiplicitásának nevezzük.

4.34. Tétel. Alkalmazzuk a Horner-módszert az $f=a_nx^n+\cdots+a_1x+a_0\in T[x]$ polinomra és a $c\in T$ konstansra, majd egészítsük ki a táblázatot egy újabb, az előzőnél eggyel rövidebb sorral a szokásos Horner-módszer számolási szabályával. Folytassuk újabb, egyre rövidebb sorokkal, míg végül egy háromszög alakú táblázatot kapunk:

	a_n	a_{n-1}	a_{n-2}	$\cdots$	a_2	a_1	a_0
c				$\cdots$			d_0
c				$\cdots$		d_1	
c				$\cdots$	d_2		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\iddots$			
c			d_{n-2}				
c		d_{n-1}					
c	d_n						

A táblázat jobb szélén átlósan elhelyezkedő számok megadják annak a polinomnak az együtthatóit, amelyet f-ből az $x-c$ határozatlanra való áttéréssel kapunk (természetesen $d_0=f(c)$ és $d_n=a_n$):

$$a_nx^n+\cdots+a_1x+a_0=d_n(x-c)^n+\cdots+d_1(x-c)+d_0.$$

A táblázatból az is kiolvasható, hogy c hányszoros gyöke f-nek: az a legkisebb k egész, amelyre $d_0=d_1=\cdots=d_{k-1}=0$ és $d_k\neq 0$.

4.35. Példa. Meghatározzuk, hogy hányszoros gyöke az $f = x^5 + 4x^4 + 7x^3 + 13x^2 + 16x + 4 \in \mathbb{R}[x]$ polinomnak a -2, és felírjuk f-et $x + 2$ polinomjaként. Alkalmazzuk a Horner-módszert f-re és a $c = -2$ konstansra, amíg háromszög alakú táblázatot kapunk.

	1	4	7	13	16	4
-2	1	2	3	7	2	0
-2	1	0	3	1	0	
-2	1	-2	7	-13		
-2	1	-4	15			
-2	1	-6				
-2	1					

A táblázatból kiolvasható, hogy a -2 kétszeres gyöke f-nek, továbbá

$$f = x^5 + 4x^4 + 7x^3 + 13x^2 + 16x + 4 = (x+2)^5 - 6(x+2)^4 + 15(x+2)^3 - 13(x+2)^2 + 0(x+2) + 0.$$

Videó: **Irreducibilis polinomok**

4.36. Definíció. A $p \in T[x]$ polinom irreducibilis, ha legalább elsőfokú, és csak úgy bontható két polinom szorzatára, hogy az egyik tényező asszociált p-hez. Ekkor a másik tényező szükségképpen asszociált 1-hez; az ilyen felbontást triviális faktorizációnak nevezzük.

4.37. Definíció. A $p \in T[x]$ polinom prím, ha legalább elsőfokú, és valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat egyik tényezőjének.

4.38. Tétel. A prím és irreducibilis polinomok megegyeznek.

4.39. Tétel. Legyen T tetszőleges test. Minden nemnulla $f \in T[x]$ polinom felírható, mégpedig a tényezők sorrendjétől eltekintve egyértelműen,

$$f = ap_1 \cdots p_n$$

alakban, ahol $a \in T \setminus \{0\}$ az f főegyütthatója, $p_1, \ldots, p_n \in T[x]$ pedig irreducibilis főpolinomok.

4.40. Tétel. Bármley test felett minden elsőfokú polinom irreducibilis.

4.41. Tétel. Ha $f \in T[x]$ irreducibilis és $\deg f \geqslant 2$, akkor f-nek nincsen gyöke.

4.42. Tétel. Bármely test feletti másod- vagy harmadfokú polinom akkor és csak akkor irreducibilis, ha nincs gyöke.

Videó: **$\mathbb{C}$, $\mathbb{R}$ és $\mathbb{Q}$ feletti irreducibilis polinomok**

4.43. Tétel (Az algebra alaptétele)**.** Minden legalább elsőfokú komplex együtthatós polinomnak van gyöke a komplex számok testében.

4.44. Következmény. A komplex számok teste felett pontosan az elsőfokú polinomok az irreducibilisek.

4.45. Következmény. Minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bomlik. Ha $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ ahol $a_n \neq 0$, akkor f-nek multiplicitással számolva pontosan n gyöke van. Ha ezek a gyökök $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$, akkor $f = a_n(x - \alpha_1) \cdots (x - \alpha_n)$. Ezt nevezzük az f polinom gyöktényezős felbontásának.

4.46. Tétel. Ha $f \in \mathbb{R}[x]$ és ha $f(z) = 0$ valamely $z \in \mathbb{C}$ komplex számra, akkor $f(\bar{z}) = 0$.

4.47. Következmény. Egy valós együtthatós polinom pontosan akkor irreducibilis $\mathbb{R}[x]$-ben, ha elsőfokú, vagy olyan másodfokú polinom amelynek nincs valós gyöke.

4.48. Következmény. Minden páratlan fokszámú valós együtthatós polinomnak van valós gyöke.

4.49. Példa. Felírjuk az $f = x^5 + 2x^3 - 8x$ polinomot irreducibilis polinomok szorzataként $\mathbb{C}[x]$-ben, $\mathbb{R}[x]$-ben és $\mathbb{Q}[x]$-ben. Alakítsuk szorzattá az f polinomot.

$$f = x^5 + 2x^3 - 8x = x(x^4 + 2x^2 - 8) = x(x^2 - 2)(x^2 + 4) = x(x - \sqrt{2})(x + \sqrt{2})(x - 2i)(x + 2i)$$

Mivel minden tényező elsőfokú, így megkaptuk $\mathbb{C}[x]$-ben az irreducibilis felbontást. A 4.46. tétel alapján egy $f \in \mathbb{R}[x]$ polinom nem valós gyökei között mindig találunk konjugált párokat. Ezt felhasználva a $\mathbb{C}[x]$-beli felbontásból általában úgy kapjuk az $\mathbb{R}$ feletti felbontást, ha a nem valós gyököknek megfelelő elsőfokú polinomokat megszorozzuk a konjugáltjának megfelelő elsőfokú polinommal. A mi esetünkben $(x-2i)(x+2i) = x^2+4$ teljesül, így az $\mathbb{R}$ feletti irreducibilis felbontás:

$$f = x(x-\sqrt{2})(x+\sqrt{2})(x^2+4).$$

Mivel $\sqrt{2} \notin \mathbb{Q}$, így az irreducibilis felbontás $\mathbb{Q}[x]$-ben:

$$f = x(x^2-2)(x^2+4).$$

4.50. Tétel (Rolle tétele)**.** Legyen $f = a_n x^n + \cdots + a_1 x + a_0$ egész együtthatós polinom, azaz $f \in \mathbb{Z}[x]$. Ekkor f minden racionális gyöke $\frac{p}{q} \in \mathbb{Q}$ alakú, ahol $p \mid a_0$ és $q \mid a_n$. Speciálisan, egész együtthatós főpolinom racionális gyökei mind egész számok.

4.51. Következmény. A legfeljebb harmadfokú $\mathbb{Q}[x]$-beli polinomokról eldönthető, hogy irreducibilisek-e.

4.52. Példa. Eldöntjük az $f = 3x^3 - 7x^2 + 17x - 5$ polinomról, hogy irreduciblis-e $\mathbb{Q}[x]$-ben. Mivel f harmadfokú polinom, ha nem irreducibilis, akkor a felbontásában lennie kell elsőfokú $\mathbb{Q}[x]$-beli polinomnak is, ami azt jelenti, hogy f-nek van racionális gyöke. A 4.50. tétel alapján ha a $\frac{p}{q} \in \mathbb{Q}$ gyöke f-nek, akkor $p \mid -5$ és $q \mid 3$, így $\frac{p}{q}$ lehetséges értékei 1, -1, $\frac{1}{3}$, $-\frac{1}{3}$, 5, -5, $\frac{5}{3}$, $-\frac{5}{3}$. Mivel $f(1) = 13 \neq 0$ és $f(-1) = -17 \neq 0$, így az 1 és a -1 nem gyöke, a többi lehetséges gyök vizsgálatához használhatjuk a Horner-módszernél szereplő táblázatot.

	3	-7	17	-5
$\frac{1}{3}$	3	-6	15	0

A táblázatból leolvasható, hogy $f(\frac{1}{3}) = 0$, így az $\frac{1}{3}$ gyöke f-nek továbbá

$$f = \left(x - \frac{1}{3}\right)(3x^2 - 6x + 15).$$

Tehát az f polinom nem irreducibilis $\mathbb{Q}[x]$-ben. A $g = 3x^2-6x+15$ polinom diszkriminánsa $D = (-6)^2-4\cdot 3\cdot 15 < 0$, azaz g irreducibilis $\mathbb{R}[x]$-ben, és így $\mathbb{Q}[x]$-ben is. Tehát az f polinom egyetlen racionális gyöke az $\frac{1}{3}$.

4.53. Tétel (Schönemann-Eisenstein-féle irreducibilitási kritérium)**.** Legyen $f = a_n x^n + \cdots + a_1 x + a_0$ egész együtthatós polinom, azaz $f \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám, amelyre $p \nmid a_n$, $p \mid a_{n-1}, \ldots, p \mid a_1$, $p \mid a_0$ és $p^2 \nmid a_0$, akkor f irreducibilis $\mathbb{Q}[x]$-ben.

4.54. Példa. Az $f = x^{102} + 14x^{78} - 56x^{65} + 42x^{11} - 28$ irreducibilis $\mathbb{Q}[x]$-ben, mert a $p = 7$ prímszám kielégíti a 4.53. tételben szereplő feltételeket.

4.55. Megjegyzés. Tetszőleges fokszámú irreducibilis polinom megadható $\mathbb{Q}[x]$-ben. Például az $x^n - 2$ polinom bármely $n \in \mathbb{N}$-re irreducibilis lesz $\mathbb{Q}[x]$-ben, ugyanis $p = 2$-re teljesülnek a 4.53. tételben szereplő feltételek.

4.56. Tétel (Viète-formulák)**.** Legyenek az n-edfokú $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ fôpolinom gyökei $\alpha_1, \ldots, \alpha_n$ (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása). Ekkor fennálnak a következő összefüggések:

$$\begin{aligned}
-a_{n-1} &= \alpha_1 + \alpha_2 + \cdots + \alpha_n, \\
a_{n-2} &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n, \\
&\vdots \\
(-1)^k a_{n-k} &= \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_k}, \\
&\vdots \\
(-1)^n a_0 &= \alpha_1\alpha_2\cdots\alpha_n.
\end{aligned}$$

5. Testek

5.1. Definíció. Az S halmazt a $(T;+,\cdot)$ test résztestjének nevezzük, ha
1. $\emptyset \neq S \subseteq T$, (nemüres részhalmaz)
2. $(\forall x, y \in S)(x+y,\ x\cdot y \in S)$, (zárt T műveleteire),
3. $(S;+,\cdot)$ test, (testet alkot T műveletek megszorításával).

5.2. Tétel. Legyen S a T test részteste. Ekkor T vektorteret alkot S felett.

5.3. Példa. $\mathbb{C}$ vektortér $\mathbb{R}$ felett. Az 1, i minimális generátorrendszer (bázis), tehát $\mathbb{C}$ dimenziója 2, azaz $\mathbb{C}$ izomorf $\mathbb{R}^2$-tel mint vektortér (de természetesen nem mint test).

5.4. Példa. Az előző tételben láttuk, hogy ha S részteste T-nek, akkor T vektortér S felett. Ennek az állításnak a megfordítása még számtestek esetében sem igaz, azaz létezik olyan $\mathbb{Q} \subseteq T \subseteq \mathbb{C}$ számhalmaz, amely vektorteret alkot $\mathbb{Q}$ felett a szokásos műveletekkel, de nem test. Legyen

$$T = \left\{ r + s\cdot\left(\frac{\sqrt{3}}{2} + \frac{1}{2}i\right) : r, s \in \mathbb{Q} \right\}.$$

Könnyű ellenőrizni, hogy T vektortér $\mathbb{Q}$ felett, és $1, \frac{\sqrt{3}}{2} + \frac{1}{2}i$ bázis T-ben. Ugyanakkor, $\frac{1}{2} + \frac{\sqrt{3}}{2}i \notin T$, mivel T minden elemének képzetes része racionális. Tehát

$$\left(\frac{\sqrt{3}}{2} + \frac{1}{2}i\right)^2 = \frac{1}{2} + \frac{\sqrt{3}}{2}i \notin T,$$

azaz T nem zárt a szorzásra, csak a skalárral (racionális számokkal) való szorzásra.

5.5. Kérdések. Az alábbi állítások közül melyek igazak és melyek hamisak?
1. $\mathbb{Z}$ test.
2. $\mathbb{Q}$ test.
3. $\mathbb{R}$ test.
4. $\mathbb{C}$ test.
5. A valós függvények $\mathbb{R}^{\mathbb{R}}$ halmaza test.
6. A valós függvények $\mathbb{R}^{\mathbb{R}}$ halmaza vektorteret alkot $\mathbb{R}$ felett.
7. $\mathbb{Q}$ 1-dimenziós vektortér $\mathbb{Q}$ felett.
8. $\mathbb{R}$ 2-dimenziós vektortér $\mathbb{Q}$ felett.
9. $\mathbb{C}$ 4-dimenziós vektortér $\mathbb{Q}$ felett.
10. $\mathbb{R}$ 1-dimenziós vektortér $\mathbb{R}$ felett.
11. $\mathbb{C}$ 2-dimenziós vektortér $\mathbb{R}$ felett.
12. $\mathbb{R}$ végesdimenziós vektortér $\mathbb{Q}$ felett.
13. Az $(1,0)$, $(0,1)$ vektorrendszer bázis az $\mathbb{Q}$ feletti $\mathbb{R}^2$ vektortérben.
14. Az 1 vektorrendszer bázis a $\mathbb{C}$ feletti $\mathbb{C}$ vektortérben.
15. Az 1, $\sqrt{2}$ vektorrendszer generátorrendszer a $\mathbb{Q}$ feletti $\mathbb{R}$ vektortérben.
16. Az $1, i$ vektorrendszer bázis a $\mathbb{C}$ feletti $\mathbb{C}$ vektortérben.

5.6. Tétel. Tetszőleges T testre a $T[x]$ polinomgyűrűt a konstanspolinomok és az x polinom generálja. A konstanspolinomok a T testtel izomorf résztestet alkotnak $T[x]$-ben.

Videó: **Prím elemszámú testek**

5.7. Példa. Legyen $n \in \mathbb{Z}$ tetszőleges nemzéró szám, és tekintsük az egész számok n-el való osztásakor keletkező maradékok

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\},$$

halmazát, melynek elemeit modulo n maradékosztályok nevezzünk. Ezen a halmazon az összeadás és szorzás műveletek természetes módon definiálhatók:

$$\overline{a} + \overline{b} = \overline{a+b} \qquad \text{és} \qquad \overline{a}\cdot\overline{b} = \overline{ab}.$$

Láttuk, hogy ha n prímszám, akkor $\mathbb{Z}_n$ test.

Videó: **Polinomok maradékosztályai**

5.8. Definíció. Legyen T test és $f \in T[x]$ tetszőleges nemzéró polinom, és tekintsük a $T[x]$ elemeinek f-fel való osztásakor keletkező mardékok

$$T[x]/\langle f\rangle = \{\,\overline{g} : g \in T[x] \text{ és } \deg g < \deg f\,\}$$

halmazát, melynek elemeit modulo f maradékosztályoknak nevezzük. Ezen a halmazon az összeadás és szorzás műveletek természetes módon definiálhatók:

$$\overline{g} + \overline{h} = \overline{g+h} \qquad \text{és} \qquad \overline{g} \cdot \overline{h} = \overline{gh}.$$

5.9. Példa. Tekintsük az $f = x^2 + 1 \in \mathbb{R}[x]$ irreducibilis polinomot. Ekkor $\overline{x^5 + 2x^2} = \overline{x-2}$, mert

$$x^5 + 2x^2 \equiv x - 2 \pmod{x^2+1},$$

azaz $x^5 + 2x^2$ és $x - 2$ ugyanazt a maradékot adja f-fel osztva. Úgy is lehetett volna számolni, hogy $\overline{x^2} = \overline{-1}$, ezért $\overline{x^5 + 2x^2} = \overline{x^5} + \overline{2x^2} = \overline{x} \cdot \overline{x^2} \cdot \overline{x^2} + \overline{2} \cdot \overline{x^2} = \overline{x} \cdot \overline{-1} \cdot \overline{-1} + \overline{2} \cdot \overline{-1} = \overline{x} + \overline{-2} = \overline{x-2}$.

5.10. Tétel. Tetszőleges T testre és $f \in T[x]$ irreducibilis polinomra $T[x]/\langle f\rangle$ test. Ha f nem irreducibilis, akkor $T[x]/\langle f\rangle$ nem test, mivel nem zérusosztómentes.

5.11. Példa. Tekintsük az $f = x^2 + 1 \in \mathbb{R}[x]$ irreducibilis polinomot. Mivel f másodfokú, ezért a lehetséges maradékok legfeljebb elsőfokúak, azaz

$$\mathbb{R}[x]/\langle f\rangle = \{\,\overline{ax+b} : a, b \in \mathbb{R}\,\}.$$

A definícióban definiált műveleteket erre az esetre felírva kapjuk, hogy

$$\begin{aligned}\overline{ax+b} + \overline{cx+d} &= \overline{(a+c)x + (b+d)},\\ \overline{ax+b} \cdot \overline{cx+d} &= \overline{(ac)x^2 + (ad+bc)x + bd} = \overline{(ad+bc)x + (bd-ac)}.\end{aligned}$$

Ha azonosítjuk az $\overline{ax+b}$ maradékosztályt az $ai + b$ komplex számmal, akkor a számolási szabályok $\mathbb{R}[x]/\langle f\rangle$-ben lényegében ugyanazok mint a komplex számok esetében, ezért

$$\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}.$$

5.12. Példa. Az $f = x^2 + 1 \in \mathbb{Z}_2[x]$ polinom nem irreducibilis, mert $f = (x+1) \cdot (x+1)$. Ezért a $\mathbb{Z}_2[x]/\langle f\rangle$ struktúra nem zérusosztómentes, mivel ott $\overline{x+1} \neq \overline{0}$, de $\overline{x+1} \cdot \overline{x+1} = \overline{x^2+1} = \overline{0}$. Tehát $\mathbb{Z}_2[x]/\langle f\rangle$ nem lehet test.

Videó: **Prímhatvány elemszámú testek**

5.13. Definíció. Legyen T tetszőleges test, és $0, 1 \in T$ a zérus-, illetve az egységelem. Azt a legkisebb k pozitív egész számot, amelyre

$$k \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{\text{k-szor}} = 0$$

a test karakterisztikájának nevezzük. Ha nem létezik ilyen pozitív egész, akkor a test nulla-karakterisztikájú.

5.14. Példa. A $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ és $\mathbb{Q}[x]/\langle x^3+2\rangle$ testek karakterisztikája nulla. A $\mathbb{Z}_p$ (p prímszám) és $\mathbb{Z}_p[x]/\langle f\rangle$ ($f \in \mathbb{Z}_p[x]$ irreducibilis) testek karakterisztikája p.

5.15. Tétel. Tetszőleges test karakterisztikája vagy nulla vagy prímszám.

5.16. Definíció. Legyen T tetszőleges test. A legszűkebb $K \leqslant T$ résztestet (azaz a legszűkebb olyan részhalmazt, amely tartalmazza az egységelemet és zárt az összeadás, additív inverz, szorzás és multiplikatív inverzképzésre), a T test prímtestének nevezzük.

5.17. Példa. $\mathbb{R}$ prímteste $\mathbb{Q}$. A $\mathbb{Z}_3[x]/\langle x^2+2x+2\rangle$ test prímteste $\mathbb{Z}_3$.

5.18. Tétel. Tetszőleges test prímteste vagy izomorf $\mathbb{Z}_p$-vel, vagy $\mathbb{Q}$-val.

5.19. Következmény. Minden véges testnek prímhatvány sok eleme van.

5.20. Tétel. Tetszőleges p prímszámra és n pozitív egészre létezik n-edfokú irreducibilis polinom $\mathbb{Z}_p[x]$-ben (melynek megkeresése nem egyszerű).

5.21. Tétel. Minden véges T test izomorf a $\mathbb{Z}_p[x]/\langle f\rangle$ testtel, ahol p a T test karakterisztikája, n a T test dimenziója a prímteste felett, és $f \in \mathbb{Z}_p[x]$ tetszőleges n-edfokú irreducibilis polinom. Ennek a testnek a jele: $GF(p^n)$.

5.22. Következmény. Ha $f \in \mathbb{Z}_p[x]$ n-edfokú irreducibilis polinom, akkor a $\mathbb{Z}_p[x]/\langle f\rangle$ véges test n-dimenziós vektorteret alkot $\mathbb{Z}_p$ felett.

5.23. Példa. A $GF(2^3) \simeq \mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ test elemeit tekinthetjük úgy, mint a $\mathbb{Z}_2$ feletti 3-dimenziós vektortér elemeit:

$$\overline{0} = \overline{000}, \qquad \overline{1} = \overline{100}, \qquad \overline{x} = \overline{010}, \qquad \overline{x+1} = \overline{110},$$
$$\overline{x^2} = \overline{001}, \qquad \overline{x^2+1} = \overline{101}, \qquad \overline{x^2+x} = \overline{011}, \qquad \overline{x^2+x+1} = \overline{111}.$$

Videó: **Elemek rendje, primitív elemek**

5.24. Definíció. Legyen T tetszőleges test. Az $\alpha \in T$ nemzéró elem (multiplikatív) rendjén azt a legkisebb k pozitív egész számot értjük, és $o(\alpha)$-val jelöljük, amelyre

$$\alpha^k = \underbrace{\alpha \cdot \alpha \cdot \cdots \cdot \alpha}_{\text{k-szor}} = 1.$$

Ha nem létezik ilyen pozitív egész, akkor az elem rendje végtelen.

5.25. Tétel. Legyen T tetszőleges test, $\alpha \in T$ nemzéró elem és $k = o(\alpha)$. Ekkor
- tetszőleges $n \in \mathbb{Z}$ egészre $\alpha^n = 1 \iff k \mid n$,
- tetszőleges $m, n \in \mathbb{Z}$ egészekre $\alpha^m = \alpha^n \iff m \equiv n \pmod{k}$.

5.26. Tétel. Legyen T m-elemű véges test. Minden $\alpha \in T$ nemzéró elemre $\alpha^{m-1} = 1$, következésképpen $o(\alpha) \mid m-1$.

5.27. Következmény. A T m-elemű véges test minden eleme gyöke az $x^m - x$ polinomnak.

5.28. Definíció. Legyen T m-elemű véges test. A $\beta \in T$ nemzéró elemet primitívnek nevezzük, ha rendje $m-1$. Ekkor T minden nemzéró eleme megadható β egy hatványaként, és így

$$T = \{0, 1, \beta, \beta^2, \ldots, \beta^{m-2}\}.$$

5.29. Példa. A $T = GF(3^2) \simeq \mathbb{Z}_3[x]/\langle x^2+2x+2\rangle$ testben meghatározzuk az elemek rendjét, megadjuk a primitív elemeket, majd az egyik hatványaiként előállítjuk a test nemzéró elemeit. A 5.26. tétel alapján az elemrendek osztói $|T|-1 = 8$-nak, így a rendek lehetséges értékei az $1, 2, 4, 8$. Az egységelem rendje $o(\overline{1}) = 1$, valamint $o(\overline{2}) = 2$. Az $\overline{x}$ elemet hatványozzuk, de elég a 5.26. tétel szerinti lehetséges hatványokat tekinteni:

$$\overline{x}^2 = \overline{x^2} = \overline{x+1}, \qquad \overline{x}^4 = \overline{x^2x^2} = \overline{(x+1)(x+1)} = \overline{x^2+2x+1+1+2} = \overline{2},$$

így $o(\overline{x}) = 8$. Az előbb láttuk, hogy $\overline{x+1}^2 = \overline{2}$, tehát $o(\overline{x+1}) = 4$. Az $\overline{x+2}$ elemet hatványozzuk:

$$\overline{x+2}^2 = \overline{x^2+x+1} = \overline{2x+2}, \qquad \overline{x+2}^4 = \overline{(2x+2)(2x+2)} = \overline{x^2+2x+1} = \overline{2},$$

tehát $o(\overline{x+2}) = 8$. Mivel $\mathbb{Z}_3[x]$-ben $x \sim 2x$, $x+1 \sim 2x+2$ és $x+2 \sim 2x+1$ teljesül, ahol $\sim$ az asszociáltság reláció, továbbá a 2 páros hatványai $\mathbb{Z}_3$-ban 1-gyel egyenlők, így az asszociáltak rendje megegyezik, azaz $o(\overline{2x}) = 8$, $o(\overline{2x+2}) = 4$ és $o(\overline{2x+1}) = 8$. A $\mathbb{Z}_3[x]/\langle x^2+2x+2\rangle$ testben primitív elemek a következők: $\overline{x}$, $\overline{x+2}$, $\overline{2x}$ és $\overline{2x+1}$.
A $\mathbb{Z}_3[x]/\langle x^2+2x+2\rangle$ test nemzéró elemeit előállítjuk $\overline{x+2}$ hatványaiként, kiszámolhatók a következők:

$$\overline{x+2}^0 = \overline{1}, \qquad \overline{x+2}^1 = \overline{x+2}, \qquad \overline{x+2}^2 = \overline{2x+2}, \qquad \overline{x+2}^3 = \overline{2x},$$
$$\overline{x+2}^4 = \overline{2}, \qquad \overline{x+2}^5 = \overline{2x+1}, \qquad \overline{x+2}^6 = \overline{x+1}, \qquad \overline{x+2}^7 = \overline{x}.$$

Ennek segítségével felírható a következő logaritmus táblázat

α	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\log_{\overline{x+2}} \alpha$	0	4	7	6	1	3	5	2

A logaritmus táblázatot használva könnyebben hatványozhatók az elemek:

$$\overline{2x}^6 = \left(\overline{x+2}^3\right)^6 = \overline{x+2}^{18} = \overline{x+2}^2 = \overline{2x+2}.$$

5.30. Tétel. Minden véges testben van primitív elem (azaz véges test multiplikatív csoportja ciklikus).

5.31. Következmény. Az m-elemű véges testben a primitív elemek száma éppen $\varphi(m-1)$ (itt φ az Euler-féle függvény).

Videó: **Minimálpolinom**

5.32. Definíció. Legyen $T = GF(p^n)$ véges test (p prím) és $\alpha \in T$. Azt a legkisebb fokszámú $\mathbb{Z}_p$ feletti főpolinomot melynek α gyöke az α elem minimálpolinomjának nevezzük.

5.33. Példa. A $GF(3^2) \simeq \mathbb{Z}_3[x]/\langle x^2+2x+2\rangle$ testben határozzuk meg az $\alpha = \overline{x+2}$ elem minimálpolinomját. A hatványokat felírjuk, mint a $\mathbb{Z}_3$ feletti 2-dimenziós vektortér elemeit, és ezek között keresünk lineárisan függő vektorokat:

$$\begin{aligned}\alpha^0 &= \overline{1} = \overline{10},\\ \alpha^1 &= \overline{x+2} = \overline{21},\\ \alpha^2 &= \overline{2x+2} = \overline{22}.\end{aligned}$$

Az $\alpha^0, \alpha^1, \alpha^2$ lineárisan függő vektorrendszert alkot, ugyanis $\alpha^2 + \alpha^1 + 2\alpha^0 = 0$, ami éppen azt jelenti, hogy az $\alpha = \overline{x+2}$ gyöke a $\mathbb{Z}_3$ feletti $h = x^2+x+2$ polinomnak. Mivel $\alpha = \overline{x+2}$ ennél kisebb hatványaiból nem lehetett lineárisan függő vektorrendszert előállítani, ezért h a legkisebb fokszámú főpolinom, aminek $\overline{x+2}$ gyöke, így h minimálpolinomja $\overline{x+2}$-nek.
Megjegyezzük, hogy a $\mathbb{Z}_3[x]/\langle x^2+2x+2\rangle$ test 2-dimenziós vektortér $\mathbb{Z}_3$ felett, így bármely 3 vektor lineárisan függő, tehát a test tetszőleges elemének minimálpolinomja legfeljebb másodfokú.

5.34. Tétel. Legyen $T = GF(p^n)$ véges test (p prím) és $\alpha \in T$. Ekkor
1. α-nak létezik legfeljebb n-fokú minimálpolinomja, amelyet jelöljünk h-val,
2. h irreducibilis és egyértelműen meghatározott,
3. tetszőleges $f \in \mathbb{Z}_p[x]$ polinomra $f(\alpha) = 0 \iff h \mid f$,
4. $h \mid x^{p^n-1} - 1$.

6. Hibajavító kódolás

Videó: **Alapfogalmak**

6.1. Definíció. Az információ tároló vagy továbbító rendszerek a következő öt részre bonthatók:
1. információ forrás, pl. szöveges (TXT) vagy zenei (WAV) adat
2. kódoló, pl. tömörítő vagy CD író program
3. kommunikációs csatorna, pl. internet vagy kompakt diszk
4. dekódoló, pl. kitömörítő vagy CD lejátszó program
5. információ felhasználás, pl. szöveges (TXT) vagy zenei (WAV) adat

A továbbítandó információ általában diszkrét egységekre bontható (szöveges adat esetén karakterek sorozatára, mono zenei adat esetén 16-bites előjeles számok sorozatára), melyeket üzeneteknek nevezzük. A kódolás egy $\varphi : M \to C$ bijektív leképezés, ahol M az üzenetek, illetve C a kódszavak halmaza. Magát a C halmazt nevezzük kódnak. Mi csak olyan kódolásokkal fogunk foglalkozni, ahol mind M, mind C a $K = \{0, 1, \ldots, k-1\}$ szimbólumok ($k = 2$ esetben bitek) feletti szavakból áll, azaz $M, C \subseteq K^*$, ahol

$$K^* = \{\, a_0 a_1 \cdots a_{n-1} : n \geqslant 0, a_0, \ldots, a_{n-1} \in K \,\}.$$

A dekódolás egy $\psi : K^* \to M$ parciális leképezés. Többfajta kódolás létezik (titkosítás, tömörítés, stb.), de mi csak olyanokat vizsgálunk, melynek célja a hibajelzés és hibajavítás.

Videó: **Standard dekódoló**

6.2. Definíció. A $C \subseteq K^*$ kód blokk-kód, ha minden kódszava ugyanolyan hosszú. A kódszavak közös $n \in \mathbb{N}$ hosszát a C kód hosszának nevezzük. Ekkor természetesen $C \subseteq K^n$.

6.3. Definíció. A $C \subseteq K^n$ blokk-kód elemeit ideális esetben $\log_{|K|} |C|$ hosszúságú szavakkal is meg tudnánk különböztetni, de mi n-hosszú szavakat használunk. Tehát a C blokk-kód információs rátája (gazdaságossági együtthatója)

$$\frac{\log_{|K|} |C|}{n}.$$

6.4. Példa. A $C = \{000, 111\} \subseteq \mathbb{Z}_2^3$ kód információs rátája $\frac{\log_2 2}{3} = \frac{1}{3}$, ami durván azt jelenti, hogy egy bitnyi kódolt adat csak $\frac{1}{3}$ bitnyi információt hordoz.

6.5. Definíció. A kommunikációs csatornát szimmetrikusnak nevezzük, ha
1. a kódszavak hosszát nem változtatja meg, azaz a csatornán bemenő és kijövő szimbólumok száma ugyanaz,
2. minden szimbólumot egymástól független módon, sorrendben, azonos $p > \frac{1}{2}$ valószínűséggel helyesen továbbít, vagy $1 - p$ valószínűséggel elront, és
3. az elrontott szimbólumok azonos eséllyel kerülnek ki a helytelen szimbólumok közül.

6.6. Példa. A $K = \{0, 1, 2\}$ és $p = 80\%$ paraméterek esetén a szimmetrikus kommunikációs csatorna az 1 szimbólumot 10% valószínűséggel továbbítja 0-ként, 80% valószínűséggel 1-ként, és szintén 10% valószínűséggel továbbítja 2-ként. Ezt a bejövő szimbólumok mindegyikére hasonlóan, egymástól függetlenül végzi el.

6.7. Definíció. Az $u = u_1 \ldots u_n$ és $v = v_1 \ldots v_n \in K^n$ szavak Hamming-távolsága azoknak az $1 \leqslant i \leqslant n$ koordinátáknak a száma, ahol u és v eltér:

$$d(u, v) = |\{\, 1 \leqslant i \leqslant n : u_i \neq v_i \,\}|.$$

6.8. Tétel. Legyen $C \subseteq K^n$ blokk-kód és $v \in K^n$ szimmetrikus kommunikációs csatornából kijövő szó. Ekkor a legnagyobb valószínűséggel azt az $u \in C$ kódszót alakította át a csatorna, amelynek Hamming-távolsága minimális v-től. Ha több ilyen van, akkor azok mindegyike egyenlő valószínűséggel lehetett a bemenő kódszó.

6.9. Példa. Ha a $C = \{000, 111\}$ kód esetén a szimmetrikus kommunikációs csatornából kijövő szó $v = 010$, akkor annak a legnagyobb a valószínűsége, hogy az $u = 000$ kódszó ment be a csatornába.

6.10. Definíció. Legyen $C \subseteq K^n$ blokk-kód. Ha ismert a $\varphi : M \to C$ kódolás, akkor a $\psi : K^n \to M$ dekódoláshoz elég megadni azt a $\tau : K^n \to C$ parciális leképezést, amelyre $\tau = \psi\varphi$. Ha minden $v \in K^n$ beérkező szóra

$$v\tau = \begin{cases} u, & \text{ha } u \in C \text{ a } v \text{ szóhoz legközelebbi kódszó, és} \\ - & \text{(nem definiált), ha több kódszó van legközelebb } v\text{-hez,} \end{cases}$$

akkor a kapott dekódolást a standard hibajavító dekódolásnak nevezzük.

6.11. Példa. Legyen $C = \{101, 111, 011\}$ és $v = 100$ a kommunikációs csatornából kijövő szó. Ekkor $d(101, 100) = 1$, $d(111, 100) = 2$, $d(011, 100) = 3$, tehát a standard hibajavító dekódolás a v szót az 101 kódszóra javítja. Ha $v = 001$, akkor $d(101, 001) = 1$ és $d(011, 001) = 1$, tehát a standard hibajavító dekódolás a v szót hibásnak jelzi.

Videó: **Minimális távolság, hibajelzés és hibajavítás**

6.12. Definíció. Legyen $t \geqslant 0$ és $C \subseteq K^n$. A C kód t-hibajelző, ha bármely kódszót legfeljebb t helyen megváltoztatva az eredmény nem lehet az eredetitől különböző kódszó. A C kód t-hibajavító, ha bárhogyan is veszünk két $u \neq v$ kódszót, és azokat legfeljebb t helyen (külön-külön) megváltoztatjuk, akkor a kapott $u', v' \in K^n$ szavak különbözők.

6.13. Példa. A $C = \{000, 111\}$ kód 2-hibajelző, de nem 3-hibajelző, és 1-hibajavító, de nem 2-hibajavító.

6.14. Definíció. A $C \subseteq K^n$ blokk-kód minimális távolságán a

$$d(C) = \min\{\, d(u, v) : u, v \in C, u \neq v \,\}$$

számot értjük.

6.15. Példa. A $C = \{000, 111\}$ kód minimális távolsága 3. A $C = \{000, 011, 101, 110\}$ kód minimális távolsága 2.

6.16. Tétel. Tetszőleges C blokk-kód $d(C) - 1$-hibajelző, és $\left\lfloor \frac{d(C)-1}{2} \right\rfloor$-hibajavító. Ezek a számok a lehető legnagyobbak, azaz C nem $d(C)$-hibajelző, és nem $\left\lfloor \frac{d(C)+1}{2} \right\rfloor$-hibajavító.

6.17. Példa. A $C = \{000, 111\}$ kód $3 - 1 = 2$-hibajelző és $2/2 = 1$-hibajavító. A $C = \{000, 011, 101, 110\}$ kód $2 - 1 = 1$-hibajelző és $\lfloor 1/2 \rfloor = 0$-hibajavító.

6.18. Tétel (Hamming-korlát)**.** Ha a $C \subseteq K^n$ kód t-hibajavító, akkor

$$|K|^n \geqslant |C| \cdot \sum_{i=0}^{t} \binom{n}{i} (|K| - 1)^i.$$

6.19. Példa. Kiszámoljuk, hogy maximum hány kódszót tartalmazhat egy 7-hosszú 1-hibajavító bináris kód. Tehát $|K| = 2$, $n = 7$, $t = 1$, és

$$\sum_{i=0}^{t} \binom{n}{i} (|K| - 1)^i = \binom{7}{0} + \binom{7}{1} = 8.$$

Ez azt jelenti, hogy minden kódszó körüli 1-sugarú gömb pontosan 8 szót tartalmaz, és ezek páronként diszjunktak. Azt kaptuk, hogy $2^7 = 128 \geqslant |C| \cdot 8$, azaz $|C| \leqslant 16$. Ebből azt is megállapíthatjuk, hogy C információs rátája legfeljebb $4/7$ lehet.

6.20. Definíció. A t-hibajavító $C \subseteq K^n$ kód tökéletes, ha minden $v \in K^n$ szóhoz van tőle legfeljebb t Hamming-távolságra levő kódszó (azaz a kód eléri a Hamming-korlátját).

6.21. Példa. A $C = \{000, 111\} \subseteq \mathbb{Z}_2^3$ kód tökéletes 1-hibajavító kód, mert $2^3 = 2 \cdot (1 + 3)$.

Videó: **Lineáris kódok**

6.22. Definíció. Ha K test és $C \subseteq K^n$ altere a K feletti K^n vektortérnek, akkor C-t lineáris kódnak nevezzük.

6.23. Tétel. Legyen $C \leqslant K^n$ lineáris kód. Ekkor
1. $|C| = |K|^r$ valamely r egészre, tehát lineáris kódok esetében feltehető, hogy $M = K^r$;
2. létezik olyan $\varphi : K^r \to C$ kódolás, amely lineáris leképezés,
3. C információs rátája $\frac{r}{n}$.

6.24. Definíció. Legyen $C \leqslant K^n$ r-dimenziós lineáris kód. A $G \in K^{r \times n}$ mátrixot a C kód generátormátrixának nevezzük, ha G sorainak rendszere a C vektortér bázisát alkotja. Ekkor az $u \in K^r$ üzenet G-szerinti kódolása az $uG \in C$ kódszó.

6.25. Példa. A $C = \{000, 111\}$ lineáris kód generátormátrixa $G = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \in \mathbb{Z}_2^{1 \times 3}$.

6.26. Definíció. A C lineáris kód szisztematikus, ha van olyan generátormátrixa, amelyben az első r oszlop az $r \times r$-es egységmátrixot alkotja, azaz $G = [E_r \;\; H]$ valamely $H \in K^{r \times (n-r)}$ mátrixra.

6.27. Példa. A $C = \{0000, 1010, 0111, 1101\}$ kód szisztematikus, mivel C egy generátormátrixa $G = \left(\begin{smallmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{smallmatrix}\right) \in \mathbb{Z}_2^{2\times 4}$. Ekkor $H = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$.

6.28. Definíció. A $C, D \leqslant K^n$ lineáris kódok ekvivalensek, ha létezik olyan $\pi \in S_n$ permutáció, amelyre

$$a_1 a_2 \dots a_n \in C \iff a_{1\pi} a_{2\pi} \dots a_{n\pi} \in D.$$

6.29. Példa. A $C = \{0000, 1010, 0111, 1101\}$ és $D = \{0000, 1100, 0111, 1011\}$ kódok ekvivalensek, mert minden kódszóban a második és harmadik szimbólumot felcserélve ($\pi = (2\ 3)$) egymásba vihetők.

6.30. Tétel. Minden lineáris kód ekvivalens egy szisztematikus lineáris kóddal.

6.31. Tétel. A $C \leqslant K^n$ lineáris kód minimális távolsága éppen

$$\min\{\, d(u, 0) : u \in C \setminus \{0\}\}.$$

Videó: **Ellenőrző mátrix**

6.32. Definíció. Legyen $C \leqslant K^n$ r-dimenziós lineáris kód. A $P \in K^{n\times(n-r)}$ mátrixot a C kód ellenőrző mátrixának nevezzük, ha $u \in K^n$ akkor és csak akkor kódszó, ha $uP = 0$.

6.33. Tétel. Minden lineáris kódnak van ellenőrző mátrixa, ami egyértelműen meghatározza a kódot. A $P \in K^{n\times(n-r)}$ mátrix akkor és csak akkor ellenőrző mátrixa a $G \in K^{r\times n}$ generátormátrixú lineáris kódnak, ha oszlopvektorai lineárisan függetlenek és $GP = 0$. Ha a kód szisztematikus a $G = [E_r\ H]$ generátormátrixszal, akkor a kód egy ellenőrző mátrixa

$$P = \begin{bmatrix} -H \\ E_{n-r} \end{bmatrix}.$$

6.34. Példa. A $C = \{0000, 1010, 0111, 1101\}$ szisztematikus kód generátormátrixa

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

Tehát a kód ellenőrző mátrixa

$$P = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Videó: **Hamming-kódok**

6.35. Definíció. Legyen K tetszőleges véges test, $r \geqslant 2$,

$$n = \frac{|K|^r - 1}{|K| - 1},$$

és legyen $P \in K^{n\times r}$ olyan mátrix, melynek sorai a K^r vektortér páronként lineárisan független nemzéró vektorait tartalmazzák (pl. azon nemzéró vektorok, melyeknek az első nemnulla komponense 1). Azt a $C \leqslant K^n$ lineáris kódot, melynek P az ellenőrző mátrixa, Hamming-kódnak nevezzük, melynek dimenziója $n - r$.

6.36. Példa. Megadjuk a $K = \mathbb{Z}_2$ test feletti (azaz bináris) $\frac{2^2-1}{2-1} = 3$-hosszú Hamming-kódot. A kód egy lehetséges ellenőrzőmátrixa

$$P = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix},$$

tehát $H = \begin{pmatrix} 1 & 1 \end{pmatrix}$ és a kód generátormátrixa

$$G = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix},$$

azaz $C = \{000, 111\}$.

6.37. Példa. Megadjuk a $K = \mathbb{Z}_3$ test feletti $\frac{3^2-1}{3-1} = 4$-hosszú Hamming-kódot. A K^2 vektortér azon nemzéró vektorai, melynek az első nemnulla komponense 1, pontosan a $(1,0)$, $(1,1)$, $(1,2)$ és $(0,1)$ vektorok. Tehát a kód egy lehetséges ellenőrzőmátrixa

$$P = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 0 \\ 0 & 1 \end{pmatrix},$$

és a kód generátormátrixa

$$G = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}.$$

Ezért a kód 2-dimenziós, kilenc eleme van, mégpedig

$$C = \{0000, 1022, 2011, 0121, 1110, 2102, 0212, 1201, 2220\}.$$

A kód minimális távolsága 3 (elég megnézni a nemzéró vektorok zérótól való távolságát), tehát C 2-hibajelző és 1-hibajavító, és információs rátája $\frac{2}{4} = \frac{1}{2}$.

6.38. Példa. Megadjuk a $2^3 - 1 = 7$-hosszú, bináris Hamming-kódot. A kód egy lehetséges ellenőrzőmátrixa

$$P = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

tehát a kód generátormátrixa

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

A kód 4-dimenziós, 16 eleme van, és információs rátája $\frac{4}{7}$.

6.39. Tétel. Tetszőleges K test fölött a Hamming-kód tökéletes, 1-hibajavító és 2-hibajelző.

Videó: **Ciklikus kódok**

6.40. Definíció. A $C \subseteq K^n$ blokk-kódot ciklikusnak nevezzük, ha minden $a_1a_2\dots a_n$ kódszóra az $a_2\dots a_na_1$ szó szintén kódszó.

6.41. Megjegyzés. Legyen K tetszőleges test. Az $a_1a_2\dots a_n \in K^n$ szavakat azonosítjuk az $a_1+a_2x+\dots a_nx^{n-1}$ polinommal.

6.42. Tétel. Legyen $C \leqslant K^n$ nemtriviális (azaz $C \neq \{0\}$) ciklikus lineáris kód és $g \in C$ minimális fokszámú főpolinom kódszó. Ekkor

1. g egyértelműen meghatározott,
2. minden $h \in K^n$ szóra $h \in C \iff g \mid h$,
3. g valódi osztója az $x^n - 1$ polinomnak,
4. C dimenziója pontosan $n - \deg(g)$.

6.43. Definíció. A $C \leqslant K^n$ ciklikus lineáris kódban egyértelműen meghatározott minimális fokszámú főpolinomot a C kód generátorpolinomjának nevezzük.

6.44. Tétel. Ha g a $C \leqslant K^n$ ciklikus lineáris kód generátorpolinomja, és $r = n - \deg(g)$, akkor a C kód egy generátormátrixa

$$G = \begin{pmatrix} g \\ xg \\ x^2g \\ \vdots \\ x^{r-1}g \end{pmatrix}.$$

6.45. Példa. Tekintsük a $C = \{0000, 1010, 0101, 1111\}$ ciklikus lineáris kódot. Ekkor a generátorpolinom az 1010 szóhoz tartozó $g = 1 + x^2 \in \mathbb{Z}_2[x]$ polinom, és C egy generátormátrixa

$$G = \begin{pmatrix} g \\ xg \end{pmatrix} = \begin{pmatrix} 1010 \\ 0101 \end{pmatrix}.$$

6.46. Tétel. Ha a $g \in K[x]$ polinom valódi osztója az $x^n - 1$ polinomnak, akkor a g által generált $C = \{h \in K^n : g \mid h\}$ kód ciklikus, lineáris, és g a generátorpolinomja.

6.47. Példa. Meghatározzuk az összes 3-hosszú nemtriviális ciklikus lineáris bináris kódot. Az $x^3 - 1 \in \mathbb{Z}_2[x]$ polinom irreducibilis felbontása $x^3 - 1 = (x+1)(x^2+x+1)$. Tehát $x^3 - 1$-nek pontosan három valódi osztója van: $g_1 = x+1$, $g_2 = x^2+x+1$ és $g_3 = 1$. Ezen generátorpolinomokhoz tartozó kódok rendre a $C_1 = \{000, 110, 011, 101\}$, $C_2 = \{000, 111\}$ és $C = \mathbb{Z}_2^3$ ciklikus lineáris kódok.

Videó: **Ciklikus Hamming-kódok**

6.48. Tétel. Legyen $f \in \mathbb{Z}_2[x]$ r-edfokú irreducibilis polinom, β a $\mathbb{Z}_2[x]/\langle f \rangle$ test primitív eleme, és $g \in \mathbb{Z}_2[x]$ a β elem minimálpolinomja. Ekkor g generátorpolinomja egy $n = 2^r - 1$ hosszú ciklikus Hamming-kódnak.

6.49. Példa. Legyen $f = 1 + x + x^3 \in \mathbb{Z}_2[x]$ és $\beta = \overline{x+1} \in \mathbb{Z}_2[x]/\langle f \rangle$. Ekkor

$$\begin{aligned} \beta^2 &= \overline{(x+1)^2} = \overline{x^2+1}, \\ \beta^3 &= \overline{(x+1)(x^2+1)} = \overline{x^3+x^2+x+1} = \overline{x^2}, \end{aligned}$$

azaz $\beta^3 + \beta^2 + 1 = \overline{x^2 + (x^2+1) + 1} = 0$ és ezért β minimálpolinomja $g = x^3 + x^2 + 1$. Tehát a Hamming-kód hossza $2^3 - 1 = 7$, és generátormátrixa

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Videó: **BCH-kódok**

6.50. Definíció. Legyen $f \in K[x]$ r-edfokú irreducibilis polinom, α a $K[x]/\langle f \rangle$ test legalább n-edrendű eleme, $d \leqslant n$, és $g \in K[x]$ az $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ elemek minimálpolinomjainak legkisebb közös többszöröse. Ekkor a g által generált n-hosszú ciklikus lineáris kódot BCH-kódnak nevezzük, ahol d a kód tervezett távolsága.

6.51. Tétel (Bose, Ray-Chaudhuri, Hocquenghem)**.** Legyen C az előző definícióban megadott BCH-kód. Ekkor C

1. hossza n és $n \leqslant |K|^r - 1$,
2. minimális távolsága legalább d,
3. dimenziója legalább $n - r(d-1)$.

6.52. Példa. Tervezzünk bináris 1-hibajavító BCH-kódot. Mivel a kód 1-hibajavító, ezért a minimális távolságának 3-nak kell lennie. Olyan véges testet kell tehát keresnünk, amelyben van legalább harmadrendű elem. Tudjuk, hogy a $GF(2^k)$ testben van primitív, azaz $2^k - 1$-rendű elem, tehát a $k = 2$ jó választás. A $GF(2^2)$ testet az $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$ irreducibilis polinommal állítjuk elő. A $\mathbb{Z}_2[x]/\langle f \rangle$ testben könnyen leellenőrizhető, hogy az $\alpha = \overline{x}$ elem rendje éppen 3, mert

$$\begin{aligned} \alpha^2 &= \overline{x^2} = \overline{x+1}, \\ \alpha^3 &= \overline{x(x+1)} = \overline{x^2+x} = 1. \end{aligned}$$

Ebből azt is látjuk, hogy $1+\alpha+\alpha^2 = 0$, azaz α minimálpolinomja $g = 1+x+x^2$, és $1+\alpha^2+(\alpha^2)^2 = 1+\alpha^2+\alpha = 1$, azaz α^2 minimálpolinomja szintén $g = 1+x+x^2$. Tehát α és α^2 minimálpolinomjainak legkisebb közös többszöröse $g = 1 + x + x^2$, így a keresett kód generátormátrixa

$$G = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix},$$

azaz $C = \{000, 111\}$.

6.53. Tétel. A 3-minimális távolságú BCH-kódok éppen a ciklikus Hamming-kódok.

6.54. Tétel. A $GF(2^k)$ test tetszőleges α elemére α és α^2 minimálpolinomjai megegyezik.

6.55. Példa. Tervezzünk bináris 2-hibajavító kódot. A d minimális távolságnak most 5-nek kell lennie. Legalább ötödrendű α elemet kell keresünk és ilyen van a $GF(2^3)$ testben. Válasszuk az $f = x^3+x+1 \in \mathbb{Z}_2[x]$ irreducibilis polinomot. Tudjuk, hogy a $\mathbb{Z}_2[x]/\langle f\rangle$ test minden nemzéró elemének rendje osztója $2^3-1=7$-nek, azaz a 0-tól és 1-től különböző elemek hetedrendűek. Legyen tehát $\alpha = \overline{x}$ és $n = 7$. Ki kell számolnunk az α, α^2, α^3 és α^4 elemek minimálpolinomját, amihez α hatványaira van szükségünk:

$$\begin{aligned}
\alpha^1 &= \overline{x},\\
\alpha^2 &= \overline{x^2},\\
\alpha^3 &= \overline{x^3} = \overline{x+1},\\
\alpha^4 &= \overline{x(x+1)} = \overline{x^2+x},\\
\alpha^5 &= \overline{x(x^2+x)} = \overline{x^3+x^2} = \overline{x^2+x+1},\\
\alpha^6 &= \overline{x(x^2+x+1)} = \overline{x^3+x^2+x} = \overline{x^2+1},\\
\alpha^7 &= \overline{x(x^2+1)} = \overline{x^3+x} = \overline{1}.
\end{aligned}$$

Tehát $\alpha^3+\alpha+1=0$, azaz α minimálpolinomja x^3+x+1, és az előző tétel szerint ugyan ez a minimálpolinomja az α^2 és α^4 elemeknek is. Az α^3 minimálpolinomja x^3+x^2+1, mivel $\alpha^9+\alpha^6+1 = \alpha^2+\alpha^6+1 = 0$. A minimálpolinomok legkisebb közös többszöröse $g = (x^3+x+1)(x^3+x^2+1) = x^6+x^5+x^4+x^3+x^2+x+1$, így a keresett kód generátormátrixa $G = \begin{pmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1\end{pmatrix}$. Ennek a kódnak a minimális távolsága 7, jobb mint a tervezett, de nem valami érdekes, mert dimenziója csak 1, információs rátája pedig csak 1/7. A probléma abból adódik, hogy túl kicsi testben számoltunk.

6.56. Példa. Megint bináris 2-hibajavító kódot tervezünk, de most az $f = x^4+x^3+1 \in \mathbb{Z}_2[x]$ irreducibilis polinomot és a $\mathbb{Z}_2[x]/\langle f\rangle$ testet használva. Vegyünk az $\alpha = \overline{x} = \overline{0100}$ elemet, és számoljuk ki hatványait (a polinomok és szavak azonosítását felhasználva)

$$\begin{aligned}
\alpha^1 &= \overline{0100}, & \alpha^2 &= \overline{0010}, & \alpha^3 &= \overline{0001}, & \alpha^4 &= \overline{1001}, & \alpha^5 &= \overline{1101},\\
\alpha^6 &= \overline{1111}, & \alpha^7 &= \overline{1110}, & \alpha^8 &= \overline{0111}, & \alpha^9 &= \overline{1010}, & \alpha^{10} &= \overline{0101},\\
\alpha^{11} &= \overline{1011}, & \alpha^{12} &= \overline{1100}, & \alpha^{13} &= \overline{0110}, & \alpha^{14} &= \overline{0011}, & \alpha^{15} &= \overline{1000}.
\end{aligned}$$

Látjuk, hogy α rendje 15, azaz α primitív, és ezért n tetszőlegesen választható $d = 5$ és $o(\alpha) = 15$ között. Az is leolvasható, hogy α minimálpolinomja x^4+x^3+1, α^2 és α^4 minimálpolinomja szintén ez az előző tétel szerint, és α^3 minimálpolinomja $x^4+x^3+x^2+x+1$. Tehát a kód generátorpolinomja $g = (x^4+x^3+1)(x^4+x^3+x^2+x+1) = x^8+x^4+x^2+x+1$. Ha maximális dimenziójú kódot keresünk, akkor legyen $n = 15$. Így a kód generátormátrixa

$$G = \begin{pmatrix}
1&1&1&0&1&0&0&0&1&0&0&0&0&0&0\\
0&1&1&1&0&1&0&0&0&1&0&0&0&0&0\\
0&0&1&1&1&0&1&0&0&0&1&0&0&0&0\\
0&0&0&1&1&1&0&1&0&0&0&1&0&0&0\\
0&0&0&0&1&1&1&0&1&0&0&0&1&0&0\\
0&0&0&0&0&1&1&1&0&1&0&0&0&1&0\\
0&0&0&0&0&0&1&1&1&0&1&0&0&0&1
\end{pmatrix},$$

dimenziója $n - \deg g = 15 - 8 = 7$, és információs rátája $\frac{7}{15}$.

Videó: Reed-Solomon-kódok

6.57. Definíció. Ha a BCH-kód definíciójában $\alpha \in K$, akkor α hatványainak minimálpolinomjai mind elsőfokúak, azaz $g = (x-\alpha)(x-\alpha^2)\dots(x-\alpha^{d-1})$. A kapott kódot Reed-Solomon kódnak nevezzük, melynek dimenziója $n-d+1$.

6.58. Példa. Legyen $K = GF(2^3)$ a nyolcelemű test és $\alpha \in K$ az 6.55. példában használt hetedrendű elem, melyről tudjuk, hogy $\alpha^7 = 1$ és $\alpha^3+\alpha+1 = 0$. Tervezzünk maximális információs rátájú 2-hibajavító kódot, azaz legyen $d = 5$ és $n = 7$. Az $f \in K[x]$ hetedrendű irreducibilis polinomot meg sem kell határoznunk, mert minket csak g érdekel. Tehát

$$g = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4).$$

Mivel K karakterisztikája 2, ezért tetszőleges $a \in K$ elemre $a = -a$, azaz

$$g = (x + \alpha)(x + \alpha^2)(x + \alpha^3)(x + \alpha^4).$$

Ezt kifejtve és felhasználva az $\alpha^7 = 1$ és $\alpha^3 + \alpha + 1 = 0$ azonosságokat

$$\begin{aligned}
g &= x^4 + (\alpha + \alpha^2 + \alpha^3 + \alpha^4)x^3 + (\alpha\alpha^2 + \alpha\alpha^3 + \alpha\alpha^4 + \alpha^2\alpha^3 + \alpha^2\alpha^4 + \alpha^3\alpha^4)x^2 \\
&\quad + (\alpha\alpha^2\alpha^3 + \alpha\alpha^2\alpha^4 + \alpha\alpha^3\alpha^4 + \alpha^2\alpha^3\alpha^4)x + \alpha\alpha^2\alpha^3\alpha^4 \\
&= x^4 + (\alpha + \alpha^2 + \alpha^3 + \alpha^4)x^3 + (\alpha^3 + \alpha^4 + \alpha^5 + \alpha^5 + \alpha^6 + \alpha^7)x^2 \\
&\quad + (\alpha^6 + \alpha^7 + \alpha^8 + \alpha^9)x + \alpha^{10} \\
&= x^4 + (\alpha^3 + \alpha(1 + \alpha + \alpha^3))x^3 + (1 + \alpha^3(1 + \alpha + \alpha^3))x^2 + (\alpha + \alpha^6(1 + \alpha + \alpha^3))x + \alpha^3 \\
&= x^4 + \alpha^3x^3 + x^2 + \alpha x + \alpha^3.
\end{aligned}$$

Tehát a kapott Reed-Solomon kód generátor mátrixa

$$G = \begin{pmatrix} \alpha^3 & \alpha & 1 & \alpha^3 & 1 & 0 & 0 \\ 0 & \alpha^3 & \alpha & 1 & \alpha^3 & 1 & 0 \\ 0 & 0 & \alpha^3 & \alpha & 1 & \alpha^3 & 1 \end{pmatrix} \in K^{3\times 7},$$

dimenziója 3, információs rátája $\frac{3}{7}$ és pontosan $8^3 = 512$ kódszót tartalmaz.

7. Videók jegyzéke

Permutációk

Permutációk megadása
Permutációk szorzása
Ciklus definíciója
Ciklusokra való felbontás
Ciklusokkal való számolás
Permutációk paritása

Rang és altér

Determináns permutációkkal
Vektorrendszer rangja
Mátrixok rangja
Alterek és bázis
Alterek megadása
Alterek metszete és összege
Alterek egyértelmű megadása

Lineáris leképezések

Definíció, magtér és képtér
Leképezések mátrixa
Bázisáttérés
Sajátvektor és sajátérték

Polinomok

Alapvető definíciók
Oszthatóság
Legnagyobb közös osztó
Polinomok gyökei, Horner-elrendezés
Irreducibilis polinomok
Komplex, valós és racionális irreducibilis polinomok

Testek

Prím elemszámú testek
Polinomok maradékosztályai
Prímhatvány elemszámú testek
Elemek rendje, primitív elemek
Minimálpolinom

Hibajavító kódolás

Alapfogalmak
Standard dekódoló

Minimális távolság, hibajelzés és hibajavítás
Lineáris kódok
Ellenőrző mátrix
Hamming-kódok
Ciklikus kódok
Ciklikus Hamming-kódok
BCH-kódok
Reed-Solomon-kódok