

Testek

(előadásvázlat, 2016. november 29.)

Maróti Miklós

Ennek az előadásnak a megértéséhez a következő fogalmakat kell tudni: **test**, **test additív és multiplikatív csoportja**, **zéruseleme**, és **egységeleme**, **struktúrák izomorfája**.

Az előadáshoz ajánlott jegyzet:

- Czédli Gábor: *Boole-függvények*, Polygon Kiadó, Szeged, 1995.
- Szendrei Ágnes: *Diszkrét matematika*, Polygon Kiadó, Szeged, 1994–2002.

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).

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

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).

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. 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.

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.

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

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

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

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

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

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

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

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

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

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 $\overline{x^5 + 2x^2} = \overline{x^5 + 2x^2} = \overline{x \cdot x^2 \cdot x^2 + 2 \cdot x^2} = \overline{x \cdot \overline{-1} \cdot \overline{-1} + 2 \cdot \overline{-1}} = \overline{x + \overline{-2}} = \overline{x-2}$.

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.

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

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

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.

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

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

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

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 .

15. Tétel. *Tetszőleges test karakterisztikája vagy nulla vagy prímszám.*

16. Definíció. Legyen T tetszőleges test. A legszűkebb $K \leq T$ 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.

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

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

19. Következmény. *Minden véges testnek prímszámú sok eleme van.*

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

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)**.*

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.*

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

$$\begin{array}{cccc} \bar{0} = \overline{000}, & \bar{1} = \overline{100}, & \bar{x} = \overline{010}, & \overline{x+1} = \overline{110}, \\ \overline{x^2} = \overline{001}, & \overline{x^2+1} = \overline{101}, & \overline{x^2+x} = \overline{011}, & \overline{x^2+x+1} = \overline{111}. \end{array}$$

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

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

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

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 $\alpha^m = \alpha^n \iff m \equiv n \pmod{k}$.*

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

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

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

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

29. Példa. A $T = \text{GF}(3^2) \simeq \mathbb{Z}_3[x]/\langle x^2 + 2x + 2 \rangle$ testben meghatározzuk az elemek rendjét, megadjuk a primitív elemeket, majd az egyik hatványaiként előállítjuk a test nemzéró elemeit. A 26. tétel alapján az elemrendek osztói $|T| - 1 = 8$ -nak, így a rendek lehetséges értékei az 1, 2, 4, 8. Az egységelem rendje $o(\bar{1}) = 1$, valamint $o(\bar{2}) = 2$. Az \bar{x} elemet hatványozzuk, de elég a 26. tétel szerinti lehetséges hatványokat tekinteni:

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

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

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

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:

$$\begin{aligned} \overline{x+2}^0 &= \overline{1}, & \overline{x+2}^1 &= \overline{x+2}, & \overline{x+2}^2 &= \overline{2x+2}, & \overline{x+2}^3 &= \overline{2x}, \\ \overline{x+2}^4 &= \overline{2}, & \overline{x+2}^5 &= \overline{2x+1}, & \overline{x+2}^6 &= \overline{x+1}, & \overline{x+2}^7 &= \overline{x}. \end{aligned}$$

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:

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

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

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

32. Definíció. Legyen $T = \text{GF}(p^n)$ 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.

33. Példa. A $\text{GF}(3^2) \simeq \mathbb{Z}_3[x]/\langle x^2+2x+2 \rangle$ 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.

34. Tétel. Legyen $T = \text{GF}(p^n)$ 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) $h \mid x^{p^n} - 1$.