Testek

(előadásvázlat, 2012. november 4.)

Maróti Miklós

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

Az előadáshoz ajánlott jegyzet:

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

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

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

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

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

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

2. Definíció. Legyen T test és $f \in T[x]$ tetszőleges nemzéró polinom, és tekintsük az egész számok 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:

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

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

4. 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. 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

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

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

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

6. 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.

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

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

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

8. 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.

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

10. 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.

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

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

13. Következmény. *Minden véges testnek prímhatvány sok eleme van.*

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

15. 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:* $\mathrm{GF}(p^n)$.

16. 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.*

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

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

18. Tétel. *Legyen T tetszőleges test. Az $\alpha \in T$ nemzéró elem (multiplikatív) rendjén azt a legkisebb k pozitív egész számot értjük, és $\mathrm{o}(\alpha)$-val jelöljük, amelyre*

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

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

19. Tétel. *Legyen T tetszőleges test, $\alpha \in T$ nemzéró elem és $k = \mathrm{o}(\alpha)$. Ekkor*

- *tetszőleges $n \in \mathbb{Z}$ egészre $\alpha^n = 1 \iff k \mid n$,*
- *tetszőleges $m, n \in \mathbb{Z}$ egészekre $\alpha^m = \alpha^n \iff m \equiv n \pmod{k}$.*

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

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

22. 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

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

23. Példa. A $T = \mathrm{GF}(3^2) \simeq \mathbb{Z}_3[x]/\langle x^2+2x+2\rangle$ testben meghatározzuk az elemek rendjét, megadjuk a primitív elemeket, majd az egyik hatványaiként előállítjuk a test nemzéró elemeit. A 20. tétel alapján az elemrendek osztói $|T|-1 = 8$-nak, így a rendek lehetséges értékei az $1, 2, 4, 8$. Az egységelem rendje $\mathrm{o}(\overline{1}) = 1$, valamint $\mathrm{o}(\overline{2}) = 2$. Az $\overline{x}$ elemet hatványozzuk, de elég a 20. 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 $\mathrm{o}(\overline{x}) = 8$. Az előbb láttuk, hogy $\overline{x+1}^2 = \overline{2}$, tehát $\mathrm{o}(\overline{x+1}) = 4$. 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 $\mathrm{o}(\overline{x+2}) = 8$. 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 $\mathrm{o}(\overline{2x}) = 8$, $\mathrm{o}(\overline{2x+2}) = 4$ és $\mathrm{o}(\overline{2x+1}) = 8$. 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:

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

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

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

26. Definíció. Legyen $T = \mathrm{GF}(p^n)$ 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.

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

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

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.

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