Testek

(előadásvázlat, 2008. május 6.)

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

7. Definíció. Legyen T tetszőleges test, és $0, 1 \in T$ az 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 $\mathbb{Z}_3[x]/\langle x^2 + \overline{2}x + \overline{2}\rangle$ test prímteste $\{\overline{0}, \overline{1}, \overline{2}\}$.

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 $\mathbb{Z}_p[x]/\langle f\rangle$ testel, 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. 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.

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

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

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

20. 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

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

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

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

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

24. 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) $h \mid x^{p^n-1} - 1$.