Irreducibilis polinomok

Segédanyag *Diszkrét matematika III.* gyakorlathoz

1. Definíció. Egy (legalább elsőfokú) polinomot *irreducibilisnek* nevezünk, ha csak triviális módon (konstans kiemelésével) alakítható szorzattá.

Tehát például az x^2+1 polinom irreducibilis $\mathbb{R}$ felett, annak ellenére, hogy $2\left(\frac{1}{2}x^2+\frac{1}{2}\right)$.

2. Tétel. *Egy másod- vagy harmadfokú polinom akkor és csak akkor irreducibilis egy T test (pl. $\mathbb{Q}, \mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_5$ stb.) felett ha nincs gyöke a T testben.*

3. Tétel.

- *$\mathbb{C}$ felett pontosan az elsőfokú polinomok irreducibilisek.*
- *$\mathbb{R}$ felett pontosan az elsőfokú és az olyan másodfokú polinomok irreducibilisek, melyeknek nincs valós gyöke (diszkriminánsuk negatív).*

Racionális számok felett az irreducubilitás nem ilyen könnyen leírható. Egy tételt azonban tanulunk a témában, melyről fontos megfigyelnünk, hogy csak elegendő feltétele az irreducibilitásnak, vele egy polinom irreducibilitása nem minden esetben mutatható ki.

4. Tétel (Schönemann-Eisenstein-kritérium)**.** *Legyen $f(x) = a_n x^n + ... + a_1 x + a_0$ egész együtthatós polinom. Ha létezik olyan p prím, melyre*

$$p \nmid a_n, \quad p | a_{n-1}, a_{n-2}, \ldots, a_0, \quad p^2 \nmid a_0$$

teljesül, akkor az $f(x)$ polinom irreduciblis $\mathbb{Q}$ felett.

5. Feladat. Adjuk meg a következő polinomok irreducibilis felbontását $\mathbb{Q}, \mathbb{R}$ és $\mathbb{C}$ felett.

(a) $x^5 + x^3 - 6x$

(b) $x^5 + 8x^2$

Megoldás. Kezdjük az (a) polinommal. Érdemes a feladat szövegében is szereplő $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sorrendben haladni, mert ha találunk $\mathbb{Q}$ felett egy szorzatra bontási lehetőséget, az $\mathbb{R}$ és $\mathbb{C}$ felett is egy szorzattá bontás lesz ($\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ miatt). Hasonlóan egy $\mathbb{R}$ feletti szorzat $\mathbb{C}$ felett is szorzat. Kezdjük tehát $\mathbb{Q}$-val. Mindig azzal kezdjük, hogy megnézzük x kiemelhető-e (és ha igen hányszor) a polinomból. Jelen esetben

$$x^5 + x^3 - 6x = x(x^4 + x^2 - 6).$$

Az x (elsőfokú lévén) nem bontható tovább, tehát azt kell megvizsgálnunk, hogy vajon az $x^4 + x^2 - 6$ polinom irreducibilis-e $\mathbb{Q}$ felett. A 4. Tétel könnyen ellenőrizhetően nem alkalmazható, azonban ne felejtsük el, hogy ez nem jelenti azt, hogy a polinomunk nem irreducibilis. Vegyük észre, hogy a vizsgálandó x^4+x^2-6 polinom olyan, hogy $y=x^2$ jelöléssel az y^2+y-6 polinomba megy át, mely másodfokú, így könnyen tudjuk kezelni. Határozzuk meg ennek az irreducibilis felbontását. Gyökei

$$y_{1,2}=\frac{-1\pm\sqrt{1-4\cdot(-6)}}{2}=\frac{-1\pm5}{2}=2 \text{ és } -3,$$

tehát $y^2+y-6=(y-2)(y+3)$, melybe az $y=x^2$ összefüggést visszahelyettesítve $x^4+x^2-6=(x^2-2)(x^2+3)$ adódik, azaz ott tartunk, hogy

$$x^5+x^3-6x=x(x^2-2)(x^2+3). \tag{1}$$

A kérdés most az, hogy az x^2-2 és x^2+3 polinomok irreducibilisek-e $\mathbb{Q}$ felett? A 2. Tétel szerint elegendő a polinomok gyökeit megvizsgálnunk. A megoldóképlettel (vagy egy kis gondolkodással) azt kapjuk, hogy

$$x^2-2=(x+\sqrt{2})(x-\sqrt{2}) \quad \text{és} \quad x^2+3=(x+i\sqrt{3})(x-i\sqrt{3}). \tag{2}$$

A kapott tényezőket megfigyelve azt látjuk, hogy egyik sem $\mathbb{Q}$ feletti polinom, tehát

az x^5+x^3-6x polinom irreducibilis felbontása $\mathbb{Q}$ felett $x(x^2-2)(x^2+3)$.

Vizsgálódjunk most $\mathbb{R}$ felett. Mivel (1)-t már tudjuk, indulhatunk innen. A 2. Tétel miatt megint a másodfokú tényezők gyökei az érdekesek, de ezeket már ismerjük: (2). Látjuk, hogy csak a x^2-2 polinom felbontása valós, így ez alapján

az x^5+x^3-6x polinom irreducibilis felbontása $\mathbb{R}$ felett $x(x+\sqrt{2})(x-\sqrt{2})(x^2+3)$.

A 3. Tétel alapján a $\mathbb{C}$ feletti felbontáshoz elsőfokú tényezőket keresünk, melyek az eddigieket összevetve adódnak:

az x^5+x^3-6x polinom irreducibilis felbontása $\mathbb{C}$ felett $x(x+\sqrt{2})(x-\sqrt{2})(x+i\sqrt{3})(x-i\sqrt{3})$.

Az (a) feladatrészt megoldottuk, folytassuk a (b)-vel. Ismét a $\mathbb{Q}$ feletti felbontással kezdünk. Megint azt nézzük először, hogy x-nek milyen hatványa emelhető ki triviálisan: $x^5+8x^2=x^2(x^3+8)$. A gyakorlaton megtanultunk racionális gyököket keresni, ez alapján azt találjuk, hogy az x^3+8 polinomnak gyöke a -2, majd egy polinomosztással

$$x^3+8=(x+2)(x^2-2x+4).$$

A másodfokú tényező gyökei

$$x_{1,2}=\frac{2\pm\sqrt{4-4\cdot4}}{2}=\frac{2\pm\sqrt{-12}}{2}=\frac{2\pm2\sqrt{-3}}{2}=1\pm i\sqrt{3},$$

tehát

$$x^2-2x+4=(x-(1+i\sqrt{3}))(x-(1-i\sqrt{3})).$$

Tehát az x^2-2x+4 polinom csak komplex tényezőkre bomlik, azaz

az x^5+8x^2 polinom irreducibilis felbontása $\mathbb{Q}$ és $\mathbb{R}$ felett $x^2(x+2)(x^2-2x+4)$, $\mathbb{C}$ felett pedig $x^2(x+2)(x-(1+i\sqrt{3}))(x-(1-i\sqrt{3}))$.

□

Utolsó frissítés: 2018.11.05.