A POLINOMOK SZÁMELMÉLETE

1. Oszthatóság, asszociáltság, legnagyobb közös osztó

Legyen R egy tetszőleges integritástartomány (azaz kommutatív, egységelemes és zérusosztómentes gyűrű). Ekkor az R feletti polinomok is integritástartományt alkotnak (jelölés: $R[x]$). Speciálisan, ha T test (a továbbiakban T mindig egy tetszőleges testet jelöl), akkor $T[x]$ integritástartomány. A legfontosabb példák: $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}_p[x]$ (ahol p prímszám). Minden $f \in T[x]$ polinomhoz tartozik egy $f: T \to T$, $c \mapsto f(c)$ polinomfüggvény, amit szintén f-fel jelölünk, de ez nem egyezik meg az f polinommal! A következő példa mutatja, hogy véges testek fölött különböző polinomokhoz tartozhat ugyanaz a polinomfüggvény, ezért nagyon fontos, hogy ne keverjük össze a polinomot a polinomfüggvénnyel! (Végtelen test fölött ilyen nem fordulhat elő (miért?), de ott sem szabad összemosni a két fogalmat.)

Példa. Az $f = x$, $g = x^2 \in \mathbb{Z}_2[x]$ polinomok nyilván különbözőek (még a fokszámuk sem egyforma), de ugyanaz a polinomfüggvény tartozik hozzájuk:

$$f(\overline{0}) = \overline{0} = g(\overline{0}) \quad \text{és} \quad f(\overline{1}) = \overline{1} = g(\overline{1}).$$

Test feletti polinomok körében az oszthatóság hasonlóan értelmezhető, mint az egész számok körében, és hasonló tulajdonságokkal rendelkezik.

Definíció (ism.). Az $f \in T[x]$ polinom ***osztója*** a $g \in T[x]$ polinomnak (jelölés: $f \mid g$), ha létezik olyan $h \in T[x]$ polinom amelyre $g = fh$.

Definíció (ism.). Az f és g polinomok ***asszociáltak*** (jelölés: $f \sim g$), ha $f \mid g$ és $g \mid f$.

Tétel (ism.). *A polinomok oszthatósága reflexív és tranzitív, de általában nem antiszimmetrikus. Az antiszimmetria helyett a következőt mondhatjuk: tetszőleges $f, g \in T[x]$ polinomokra $f \sim g \iff \exists c \in T \setminus \{0\} : g = cf$. Ha $f \mid g$ és $g \neq 0$, akkor* $\deg f \leq \deg g$.

Tétel (ism.). *Az asszociáltság ekvivalenciareláció $T[x]$-en. A nulla osztályát kivéve minden asszociáltsági osztály tartalmaz pontosan egy főpolinomot.*

Megjegyzés. Asszociált polinomokat nem érdemes (sőt nem is lehet) megkülönböztetni, ha csak az oszthatóságot vizsgáljuk. Ha az oszthatósági relációt az asszociáltsági osztályok halmazán értelmezzük, akkor már nemcsak reflexív és tranzitív, hanem antiszimmetrikus is lesz, azaz részbenrendezés. A kapott $(T[x]/\sim; |)$ részbenrendezett halmaz legkisebb eleme $1/\sim = T \setminus \{0\}$, legnagyobb eleme $0/\sim = \{0\}$. Az egész számok gyűrűjében minden asszociáltsági osztály $\{a, -a\}$ alakú, tehát minden osztályban van egy (és csak egy) nemnegatív szám. Ha minden asszociáltsági osztályt a nemnegatív elemével reprezentálunk, akkor az $(\mathbb{N}_0; |)$ részbenrendezett halmazt kapjuk, ami lényegében ugyanaz, mint a $(\mathbb{Z}/\sim; |)$ részbenrendezett halmaz. Test feletti polinomgyűrű esetén minden asszociáltsági osztály (a nulláét kivéve) pontosan egy főpolinomot tartalmaz, itt tehát asszociáltság erejéig mindig dolgozhatunk főpolinomokkal.

Tétel (ism.). *Bármely $f \in T[x]$ és $\alpha \in T$ esetén*

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

Tétel (ism.). *Ha $f, g \in T[x]$, és $g \neq 0$, akkor léteznek olyan egyértelműen meghatározott q és $r \in T[x]$ polinomok, amelyekre $f = qg + r$ és* $\deg r < \deg g$.

Definíció (ism.). A $d \in T[x]$ polinom ***legnagyobb közös osztója*** az f és $g \in T[x]$ polinomoknak, ha teljesül a következő két feltétel:

(1) $d \mid f$ és $d \mid g$;
(2) $\forall k \in T[x] : (k \mid f \text{ és } k \mid g) \implies k \mid d$.

Hasonlóan definiálható polinomok ***legkisebb közös többszöröse*** is.

Megjegyzés. A legnagyobb közös osztó a definíciója a következőképpen is értelmezhető. Tetszőleges $f \in T[x]$ polinomra jelölje D_f az f polinom összes osztóinak halmazát: $D_f = \{k \in T[x] : k \mid f\}$. Ekkor $D_f \cap D_g$ nem más, mint f és g közös osztóinak halmaza, $\operatorname{lnko}(f, g)$ pedig ennek az oszthatóság szerint részbenrendezett halmaznak a legnagyobb eleme. Pontosabban, mivel az oszthatóság csak asszociáltság erejéig antiszimmetrikus, a teljesen precíz megfogalmazás úgy szól, hogy $\operatorname{lnko}(f, g)$ asszociáltsági osztálya a $((D_f \cap D_g)/\sim; |)$ részbenrendezett halmaz legnagyobb eleme. Innen is látszik, hogy a legnagyobb közös osztó csak asszociáltság erejéig van meghatározva; megállapodás szerint általában főpolinomot választunk (így már egyértelmű az lnko). Nemnulla polinomok esetén $\operatorname{lnko}(f, g)$ úgy is definiálható, mint f és g legnagyobb fokszámú közös osztója (asszociáltság erejéig). (Miért nem jó ez a definíció $\operatorname{lnko}(0, 0)$ esetén?)

Tétel (ism.). *Bármely két $f, g \in T[x]$ polinomnak létezik legnagyobb közös osztója és legkisebb közös többszöröse, és ezek asszociáltság erejéig egyértelműen meghatározottak. A legnagyobb közös osztó kiszámítható az euklideszi algoritmussal.*

2. Kétismeretlenes lineáris „diofantoszi” egyenlet

Tétel. *Az $f,g\in T[x]$ polinomok legnagyobb közös osztója mindig kifejezhető f és g „lineáris kombinációjaként”:*

$$\exists u,v\in T[x]:\ \ fu+gv=\operatorname{lnko}(f,g)\,. \tag{2.1}$$

Biz. A bizonyítás nagyon hasonló a 2.3. Tétel (utolsó állításának) bizonyításához. Ha $f=0$ vagy $g=0$, akkor az állítás triviális. Tegyük fel tehát, hogy $f,g\neq 0$, és tekintsük az összes $fu+gv$ alakú polinomok I halmazát:

$$I=\{fu+gv:u,v\in T[x]\}\,.$$

Nyilván $0\in I$, de vannak I-ben nemzéró polinomok is (például f és g). Legyen d az $I\setminus\{0\}$ halmaz (egyik) legkisebb fokszámú eleme. Mivel $d\in I$, vannak olyan $u_0,v_0\in T[x]$ polinomok, amelyekre $fu_0+gv_0=d$. Megmutatjuk, hogy $d\sim\operatorname{lnko}(f,g)$. A legnagyobb közös osztó definíciójának második pontja nyilván teljesül d-re: ha $k\mid f$ és $k\mid g$, akkor $k\mid fu_0+gv_0=d$. A definíció első pontjához igazolnunk kell, hogy $d\mid f$. Tegyük fel, hogy $d\nmid f$; ekkor ha f-et maradékosan osztjuk d-vel, a keletkező r maradék nem lesz nulla: $f=qd+r$, ahol $\deg r<\deg d$ és $r\neq 0$. Az r polinom is eleme az I halmaznak, hiszen $r=f-qd=f-q(fu_0+gv_0)=f(1-qu_0)+g(-qv_0)$. Mivel r nem nulla, és foka szigorúan kisebb d fokánál, ellentmondást kaptunk, hiszen d minimális fokszámú eleme volt az $I\setminus\{0\}$ halmaznak. Ez az ellentmondás azt mutatja, hogy $d\mid f$, és hasonlóan bizonyítható a $d\mid g$ oszthatóság is. Ezzel beláttuk, hogy d eleget tesz a legnagyobb közös osztó definíciójának, azaz $d\sim\operatorname{lnko}(f,g)$; másrészt $d=fu_0+gv_0$, és ez igazolja a tétel állítását. □

Megjegyzés. Figyeljük meg, hogy a bizonyítás nem úgy történt, hogy vettük f és g legnagyobb közös osztóját, és megmutattuk róla, hogy előáll $fu+gv$ alakban, hanem vettünk az ilyen alakú nemnulla polinomok közül egy minimális fokszámút, és arról mutattuk meg, hogy nem más, mint $\operatorname{lnko}(f,g)$. Tehát tulajdonképpen bebizonyítottuk, hogy létezik bármely két $f,g\in T[x]$ polinomnak legnagyobb közös osztója (ha eddig nem tudtuk volna).

Definíció. Azt mondjuk, hogy az $f,g\in T[x]$ polinomok ***relatív prímek***, ha $\operatorname{lnko}(f,g)\sim 1$. Jelölés: $f\perp g$.

Tétel. *Tetszőleges $f,g,h\in T[x]$ polinomok esetén, ha $f\perp g$, akkor $f\mid gh\iff f\mid h$.*

Biz. A bizonyítás nagyon hasonló a 2.5. Tétel bizonyításához. Az nyilvánvaló, hogy $f\mid h\implies f\mid gh$ (ehhez nincs is szükség az $f\perp g$ feltevésre). A másik irány bizonyításához tegyük fel, hogy $f\mid gh$, és írjuk fel f és g legnagyobb közös osztóját (2.1) szerint $\operatorname{lnko}(f,g)\sim 1=fu+gv$ alakban. Szorozzuk be az egyenlőséget h-val: $h=fhu+ghv$. Világos, hogy $f\mid fhu$, és az $f\mid gh$ feltevésünk miatt $f\mid ghv$ is teljesül. Tehát az összeg mindkét tagja osztható f-fel, és ez mutatja, hogy $f\mid h$. □

Tétel. *Tetszőleges $f,g,h\in T[x]$ polinomok esetén, ha $\operatorname{lnko}(f,g)\nsim 0$, akkor*

$$f\mid gh\iff \frac{f}{\operatorname{lnko}(f,g)}\mid h. \tag{2.2}$$

Biz. A bizonyítás nagyon hasonló a 2.6. Tétel bizonyításához. Legyen $d\sim\operatorname{lnko}(f,g)\nsim 0$, továbbá legyen $f=f_0d$ és $g=g_0d$ (miért tudjuk f-et és g-t így felírni alkalmas $f_0,g_0\in T[x]$ polinomokkal?). Először megmutatjuk, hogy $f_0\perp g_0$. Ismét (2.1)-et használva d felírható $d=fu+gv=d(f_0u+g_0v)$ alakban. Egyszerűsítve[1] d-vel azt kapjuk, hogy $f_0u+g_0v=1$. Ebből már következik, hogy $f_0\perp g_0$, hiszen f_0 és g_0 bármely k közös osztójára $k\mid f_0u+g_0v=1$, tehát $k\sim 1$. A bizonyítandó (2.2) állítás így fest: $f_0d\mid g_0dh\iff f_0\mid h$; a bal oldalt d-vel egyszerűsítve ezt átfogalmazhatjuk úgy, hogy $f_0\mid g_0h\iff f_0\mid h$. Ez pedig már következik az előző tételből, hiszen $f_0\perp g_0$. □

Tétel. *Legyen T egy test és $f,g,h\in T[x]$ (nemnulla) polinomok. Ekkor az $fu+gv=h$ kétismeretlenes lineáris „diofantoszi” egyenlet akkor és csak akkor oldható meg az ismeretlen $u,v\in T[x]$ polinomokra nézve, ha $\operatorname{lnko}(f,g)\mid h$. Ha (u_0,v_0) egy megoldás, akkor bármely $t\in T[x]$ esetén az alábbi (u,v) pár is megoldás, továbbá minden megoldás előáll ilyen alakban a $t\in T[x]$ polinom alkalmas megválasztásával:*

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

Biz. A bizonyítás nagyon hasonló a 2.7. Tétel bizonyításához. Tegyük fel, hogy $f,g\neq 0$; ekkor $d:=\operatorname{lnko}(f,g)\neq 0$. Először azt igazoljuk, hogy az egyenlet megoldhatóságának szükséges és elegendő feltétele $d\mid h$. Az elegendőség bizonyításához tegyük fel, hogy $d\mid h$; ekkor $h=dh_0$ alkalmas $h_0\in T[x]$ polinommal. Először (2.1) szerint keressünk olyan $\widetilde{u},\widetilde{v}\in T[x]$ polinomokat, amelyekre $d=f\widetilde{u}+g\widetilde{v}$, majd szorozzuk be mindkét oldalt h_0-lal: $h=dh_0=f(\widetilde{u}h_0)+g(\widetilde{v}h_0)$. Ez azt jelenti, hogy $u=\widetilde{u}h_0$ és $v=\widetilde{v}h_0$ megoldása az egyenletnek. A másik irány igazolásához tegyük fel, hogy van megoldás, azaz $fu+gv=h$ teljesül valamely $u,v\in T[x]$ polinomokra. Tudjuk, hogy $d\mid f,g$ (miért?), és ebből következik, hogy $d\mid fu+gv=h$. Tehát a $d\mid h$ feltétel nemcsak elegendő, hanem szükséges is az egyenlet megoldhatóságához.

---

[1] Figyelem: nem leosztunk, hanem egyszerűsítünk! A $T[x]$ polinomgyűrűben nincs definiálva az osztás művelete (a racionális törtek $T(x)$ testében már igen, de erre nincs szükségünk). Minden integritástartományban, így $T[x]$-ben is érvényes ez az egyszerűsítési szabály: ha $ac=bc$ és $c\neq 0$, akkor $a=b$. Ezt a nullosztómentességre támaszkodva könnyű igazolni (HF). A tételben szereplő $\frac{f}{\operatorname{lnko}(f,g)}$ kifejezést sem kell osztásként értelmezni; ez csak egy jelölés az f_0 polinomra.

A tétel másik állításának igazolásához tegyük fel, hogy van egy (u_0, v_0) megoldásunk; tudjuk, hogy ekkor $d \mid h$. Írjuk fel szokás szerint az f, g polinomokat $f = f_0 d$, $g = g_0 d$ alakban. Jelölje M az egyenlet összes megoldásainak halmazát: $M = \{(u, v) : fu + gv = h\} \subseteq T[x] \times T[x]$. Azt kell bizonyítanunk, hogy

$$(u, v) \in M \iff \exists t \in T[x] : u = u_0 + g_0 t,\ v = v_0 - f_0 t.$$

A „ $\Longrightarrow$ ” irány igazolásához tegyük fel, hogy $(u, v) \in M$. Korábban feltettük azt is, hogy (u_0, v_0) is egy megoldás, tehát $fu + gv = h = fu_0 + gv_0$. Rendezés után azt kapjuk, hogy $f(u - u_0) = g(v_0 - v)$. Itt a jobb oldal szemlátomást osztható g-vel, ezért $g \mid f(u - u_0)$. Ebből (2.2) alapján következik, hogy $g_0 \mid u - u_0$. Az oszthatóság definíciója szerint ez azt jelenti, hogy van olyan $t \in T[x]$ polinom, amelyre $u - u_0 = g_0 t$. Ezzel megkaptuk, hogy $u = u_0 + g_0 t$, a v-re vonatkozó formulát pedig egyszerű visszahelyettesítéssel nyerjük: $g(v_0 - v) = f(u - u_0) = fg_0 t$, tehát $v_0 - v = f_0 t$ (miért?), amiből rögtön adódik, hogy $v = v_0 - f_0 t$.

A „ $\Longleftarrow$ ” irány igazolásához tegyük fel, hogy $u = u_0 + g_0 t,\ v = v_0 - f_0 t$. Csak be kell helyettesíteni az egyenetbe, hogy lássuk, hogy (u, v) valóban megoldás: $fu + gv = f(u_0 + g_0 t) + g(v_0 - f_0 t) = fu_0 + gv_0 + (fg_0 - gf_0)t = fu_0 + gv_0$ (miért lesz $fg_0 - gf_0 = 0$?), ez pedig valóban egyenlő h-val, hiszen feltettük, hogy (u_0, v_0) egy megoldása az egyenletnek. □

Példa (20b). Számítsuk ki az f és g polinomok legnagyobb közös osztóját, és adjuk meg az $fu + gv = \operatorname{lnko}(f, g)$ egyenlet egy megoldását az $\mathbb{R}[x]$ polinomgyűrűben. Az lnko segítségével határozzuk meg f és g komplex gyökeit.

$$f = x^4 + 2x^3 - x^2 - 4x - 2, \qquad g = x^4 + x^3 - x^2 - 2x - 2$$

Megoldás: Hajtsuk végre az euklideszi algoritmust az f és g polinomokra (amelyik polinomnak van „neve”, arra mindig a nevével hivatkozunk a jobb átláthatóság kedvéért):

	osztandó	=	hányados · osztó	+	maradék
(1)	f	=	$1 \cdot g$	+	$x^3 - 2x$
(2)	g	=	$(x+1) \cdot (x^3 - 2x)$	+	$\boxed{x^2 - 2}$
(3)	$x^3 - 2x$	=	$x \cdot (x^2 - 2)$	+	0

A legnagyobb közös osztó az utolsó nemnulla maradék: $\operatorname{lnko}(f, g) \sim \boxed{x^2 - 2}$. Ezzel a polinommal f és g is osztható:

$$f = \left(\boxed{x^2 - 2}\right) \cdot (x^2 + 2x + 1) \quad \text{és} \quad g = \left(\boxed{x^2 - 2}\right) \cdot (x^2 + x + 1).$$

Ebből rögtön megkapjuk f és g gyökeit (multiplicitással):

$$f \text{ gyökei: } \sqrt{2}, -\sqrt{2}, -1, -1; \qquad g \text{ gyökei: } \sqrt{2}, -\sqrt{2}, -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} - \frac{\sqrt{3}}{2}i.$$

Megfigyelhetjük, hogy f és g közös gyökei ugyanazok, mint $\operatorname{lnko}(f, g)$ gyökei.

A „diofantoszi” egyenlet megoldásához fejezzük ki a maradékot az euklideszi algoritmus során elvégzett mindegyik osztásnál (az utolsót kivéve):

	maradék	=	osztandó	−	hányados · osztó
(1)	$x^3 - 2x$	=	f	−	g
(2)	$\operatorname{lnko}(f, g) \sim \boxed{x^2 - 2}$	=	g	−	$(x+1) \cdot (x^3 - 2x)$

Az a célunk, hogy mindegyik maradékot f és g segítségével írjuk fel $(fu + gv$ alakban). Az első osztás maradéka máris ilyen alakban van: $x^3 - 2x = f - g$. Ezt behelyettesíthetjük a második osztás maradékának fenti felírásában $x^3 - 2x$ helyére:

$$\operatorname{lnko}(f, g) \sim \boxed{x^2 - 2} = g - (x+1) \cdot (x^3 - 2x) = g - (x+1) \cdot (f - g) = (-x - 1) \cdot f + (x + 2) \cdot g.$$

Ebből leolvashatjuk az $fu + gv = \operatorname{lnko}(f, g)$ egyenlet egy megoldását: $u = -x - 1$, $v = x + 2$.

Példa. Számítsuk ki az f és g polinomok legnagyobb közös osztóját, és adjuk meg az $fu + gv = \overline{1}$ egyenlet egy megoldását a $\mathbb{Z}_7[x]$ polinomgyűrűben.

$$f = x^4 + \overline{2}x^3 + \overline{5}x^2 + \overline{2}x + \overline{5}, \qquad g = \overline{2}x^3 + \overline{4}x^2 + \overline{4}x$$

Megoldás: Hajtsuk végre az euklideszi algoritmust az f és g polinomokra (amelyik polinomnak van „neve”, arra mindig a nevével hivatkozunk a jobb átláthatóság kedvéért):

	osztandó	=	hányados · osztó	+	maradék
(1)	f	=	$\overline{4}x \cdot g$	+	$\overline{3}x^2 + \overline{2}x + \overline{5}$
(2)	g	=	$(\overline{3}x + \overline{4}) \cdot (\overline{3}x^2 + \overline{2}x + \overline{5})$	+	$\overline{2}x + \overline{1}$
(3)	$\overline{3}x^2 + \overline{2}x + \overline{5}$	=	$(\overline{5}x + \overline{2}) \cdot (\overline{2}x + \overline{1})$	+	$\boxed{\overline{3}}$
(4)	$\overline{2}x + \overline{1}$	=	$(\overline{3}x + \overline{5}) \cdot \overline{3}$	+	$\overline{0}$

(Az utolsó osztást ki is hagyhattuk volna, mert $\overline{3} \sim \overline{1}$, tehát bármilyen polinomot osztunk is $\overline{3}$-sal, mindig $\overline{0}$ lesz a maradék.) A legnagyobb közös osztó az utolsó nemnulla maradék: $\operatorname{lnko}(f,g) \sim \boxed{\overline{3}} \sim \overline{1}$.

A diofantoszi egyenlet megoldásához fejezzük ki a maradékot az euklideszi algoritmus során elvégzett mindegyik osztásnál (az utolsót kivéve):

	maradék	$=$	osztandó	$-$	hányados $\cdot$ osztó
(1)	$\overline{3}x^2+\overline{2}x+\overline{5}$	$=$	f	$-$	$\overline{4}x \cdot g$
(2)	$\overline{2}x+\overline{1}$	$=$	g	$-$	$(\overline{3}x+\overline{4}) \cdot (\overline{3}x^2+\overline{2}x+\overline{5})$
(3)	$\operatorname{lnko}(f,g) \sim \boxed{\overline{3}}$	$=$	$\overline{3}x^2+\overline{2}x+\overline{5}$	$-$	$(\overline{5}x+\overline{2}) \cdot (\overline{2}x+\overline{1})$

Az a célunk, hogy mindegyik maradékot f és g segítségével írjuk fel ($fu+gv$ alakban). Az első osztás maradéka már ilyen alakban van. Ezt behelyettesíthetjük a második osztás maradékának fenti felírásába:

$$\overline{2}x+\overline{1} = g-(\overline{3}x+\overline{4})\cdot(\overline{3}x^2+\overline{2}x+\overline{5}) = g-(\overline{3}x+\overline{4})\cdot(f-\overline{4}x\cdot g) = (\overline{4}x+\overline{3})\cdot f+(\overline{5}x^2+\overline{2}x+\overline{1})\cdot g.$$

A harmadik osztás maradékának fenti felírásába behelyettesítjük az első két osztás maradékának f és g segítségével felírt alakját:

$$\begin{aligned}\operatorname{lnko}(f,g) \sim \boxed{\overline{3}} &= \overline{3}x^2+\overline{2}x+\overline{5}-(\overline{5}x+\overline{2})\cdot(\overline{2}x+\overline{1}) = \\ &= (f-\overline{4}x\cdot g)-(\overline{5}x+\overline{2})\cdot\Big((\overline{4}x+\overline{3})\cdot f+(\overline{5}x^2+\overline{2}x+\overline{1})\cdot g\Big) = \\ &= (x^2+\overline{5}x+\overline{2})\cdot f+(\overline{3}x^3+x^2+x+\overline{5})\cdot g.\end{aligned}$$

Azt kaptuk, hogy

$$(x^2+\overline{5}x+\overline{2})\cdot f+(\overline{3}x^3+x^2+x+\overline{5})\cdot g = \overline{3}$$

Már majdnem készen vagyunk, de nekünk nem $\overline{3}$-t, hanem $\overline{1}$-t kell felírnunk $fu+gv$ alakban. (Mivel $\overline{3} \sim \overline{1}$, mindkettő „egyformán jó” legnagyobb közös osztónak, de a feladatban most konkrétan $\overline{1}$ szerepelt.) Ehhez be kell szoroznunk az egyenlőséget $\overline{3}$ multiplikatív inverzével, vagyis $\overline{5}$-sal:

$$(\overline{5}x^2+\overline{4}x+\overline{3})\cdot f+(x^3+\overline{5}x^2+\overline{5}x+\overline{4})\cdot g = \overline{1}$$

Ebből leolvashatjuk az $fu+gv=\overline{1}$ egyenlet egy megoldását: $u=\overline{5}x^2+\overline{4}x+\overline{3}$, $v=x^3+\overline{5}x^2+\overline{5}x+\overline{4}$.

3. Kongruenciareláció, maradékosztályok

Definíció. Tetszőleges $f,g,m \in T[x]$ esetén azt mondjuk, hogy f ***kongruens*** g***-vel modulo*** m (jelölés $f \equiv g \pmod m$), ha $m \mid f-g$.

Megjegyzés. Egész számoknál fel szoktuk tenni, hogy $m \geq 2$. Itt semmilyen kikötést nem tettünk a modulusra, ezért előfordulnak „degenerált” esetek is. Ha $m=0$, akkor $f \equiv g \pmod m \iff f=g$ (miért?). Ha pedig $m \sim 1$ (azaz m nemzéró konstans polinom), akkor $f \equiv g \pmod m$ teljesül minden $f,g \in T[x]$ esetén (miért?).

Tétel. *Ha $0 \neq m \in T[x]$, akkor tetszőleges $f,g \in T[x]$ polinomok esetén $f \equiv g \pmod m$ akkor és csak akkor teljesül, ha f és g ugyanazt a maradékot adja m-mel osztva.*

Biz. A bizonyítás nagyon hasonló a 2.9. Tétel bizonyításához (HF). □

Tétel. *A* mod m *kongruencia ekvivalenciareláció $T[x]$-en, továbbá tetszőleges $f_1,g_1,f_2,g_2 \in T[x]$ esetén érvényesek az alábbiak:*

$$\left.\begin{aligned} f_1 &\equiv g_1 \pmod m \\ f_2 &\equiv g_2 \pmod m \end{aligned}\right\} \implies f_1 \pm f_2 \equiv g_1 \pm g_2,\ f_1 \cdot f_2 \equiv g_1 \cdot g_2 \pmod m.$$

Biz. A bizonyítás nagyon hasonló a 2.10. Tétel bizonyításához; itt is ugyanúgy lehet visszavezetni a kongruencia tulajdonságait az oszthatóság tulajdonságaira, mint az egész számok körében (HF). □

Tétel. *Tetszőleges $f,g,h \in T[x]$ esetén az $fu \equiv h \pmod m$* **lineáris kongruencia** *akkor és csak akkor oldható meg (az ismeretlen $u \in T[x]$ polinomra nézve), ha $\operatorname{lnko}(f,m) \mid h$.*

Biz. A bizonyítás nagyon hasonló a 2.17. Tétel (első állításának) bizonyításához; itt is ugyanúgy lehet visszavezetni a lineáris kongruenciát kétismeretlenes lineáris „diofantoszi” egyenletre, mint az egész számok körében (HF). □

Definíció. A mod m kongruenciához tartozó ekvivalenciaosztályokat modulo m ***maradékosztályoknak*** nevezzük. Az $f \in T[x]$ polinomot tartalmazó modulo m maradékosztályt $\overline{f}$ jelöli: $\overline{f} = \{g \in T[x] : f \equiv g \pmod m\}$. A maradékosztályok halmazát (vagyis a modulo m kongruenciához tartozó faktorhalmazt) $T[x]/(m)$ jelöli, azaz $T[x]/(m) = \{\overline{f} : f \in T[x]\}$.

Megjegyzés. A $T[x]/(m)$ halmaz a $\mathbb{Z}_m$ halmaz analogonja, csak itt kicsit csúnyább a jelölés. A jelölésnek megvan a pontos magyarázata: (m) jelöli az m polinom által generált *főideált* a $T[x]$ polinomgyűrűben, $T[x]/(m)$ pedig az ehhez az ideálhoz tartozó *faktorgyűrűje* $T[x]$-nek. Ezeket a fogalmakat majd absztrakt algebrából tanuljuk. Lehetne $\mathbb{Z}_m$ helyett is $\mathbb{Z}/(m)$-et írni, de ott szokás az egyszerűbb $\mathbb{Z}_m$ jelölést használni.

Definíció. A modulo m maradékosztályok halmazán értelmezzük az összeadást, az additív inverz képzését és a szorzást a következőképpen: tetszőleges $f, g \in T[x]$ esetén legyen $\overline{f} + \overline{g} = \overline{f+g}$, $-\overline{g} = \overline{-g}$, $\overline{f} \cdot \overline{g} = \overline{f \cdot g}$.

Állítás. *A fenti műveletek jóldefiniáltak, azaz maradékosztályok összege (addditív inverze, szorzata) nem függ attól, hogy az egyes maradékosztályokból melyik elemet választjuk reprezentánsnak, és ezekkel a műveletekkel $T[x]/(m)$ kommutatív egységelemes gyűrűt alkot (**maradékosztály-gyűrű**). Ha $\deg m = n \geq 1$, akkor a $T[x]/(m)$ maradékosztály-gyűrű minden eleme egyértelműen felírható az alábbi alakban:*

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \qquad (a_{n-1}, \ldots, a_1, a_0 \in T).$$

Biz. A bizonyítás nagyon hasonló a 2.13. Tétel bizonyításához; itt is a kongruencia tulajdonságai garantálják, hogy a maradékosztályok összege, additív inverze és szorzata jóldefiniált, és itt is ugyanúgy lehet visszavezetni a műveleti tulajdonságokat a $T[x]$ gyűrűbeli tulajdonságokra, mint ahogy a $\mathbb{Z}_m$ halmazon definiált műveletek tulajdonságait visszavezettük az egész számok megfelelő műveleti tulajdonságaira (HF). A tétel utolsó állítása annak a ténynek felel meg, hogy $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$, és azon múlik, hogy ha egy tetszőleges $f \in T[x]$ polinomot maradékosan osztunk az n-edfokú m polinommmal, akkor a maradék mindig egy legfeljebb $(n-1)$-edfokú polinom lesz, továbbá a maradék egyértelműen meghatározott. Tehát minden $f \in T[x]$ polinomhoz létezik egy és csak egy $f_1 \in T[x]$ polinom, amelyre $f \equiv f_1 \pmod m$ és $\deg f_1 \leq n-1$. □

Tétel. *Az $\overline{f} \in T[x]/(m)$ maradékosztálynak akkor és csak akkor létezik multiplikatív inverze, ha f és m relatív prímek.*

Biz. A bizonyítás nagyon hasonló a 2.19. Tétel bizonyításához; itt is a lineáris kongruencia megoldhatósági kritériumát kell alkalmazni (HF). □

Következmény. *A $T[x]/(m)$ maradékosztály-gyűrű akkor és csak akkor test, ha m irreducibilis T felett.*

Biz. A bizonyítás nagyon hasonló a 2.21. Következmény bizonyításához; csak a „degenerált” eseteket külön meg kell nézni.

- Ha $m = 0$, akkor m nem irreducibilis, és $T[x]/(m)$ valóban nem test, mert minden $f \in T[x]$ polinomra $\overline{f} = \{f\}$, tehát $T[x]/(m)$ lényegében ugyanaz, mint $T[x]$ (szaknyelven: a $T[x]/(m)$ és $T[x]$ gyűrűk *izomorfak* egymással), márpedig $T[x]$ nem test (miért?).
- Ha $m \sim 1$, akkor m megint csak nem irreducibilis, és $T[x]/(m)$ valóban nem test (miért?).
- Ha $\deg m \geq 1$ és m nem irreducibilis, akkor van nemtriviális felbontása: $m = fg$, ahol $1 \leq \deg f, \deg g < \deg m$ (lásd az 5.6. Állítást). Ekkor $\overline{f}, \overline{g} \neq \overline{0}$, de $\overline{f} \cdot \overline{g} = \overline{0}$, tehát $T[x]/(m)$ nem test (sőt, még csak nem is integritástartomány).
- Ha m irreducibilis, akkor $T[x]/(m)$ kommutatív egységelemes gyűrű, amelynek legalább két eleme van (miért?), tehát ahhoz, hogy belássuk, hogy $T[x]/(m)$ test, elég ellenőrizni, hogy minden nemnulla elemének van multiplikatív inverze. Legyen tehát $\overline{0} \neq \overline{f} \in T[x]/(m)$, és keressük $\overline{f}$ multiplikatív inverzét. Mivel m irreducibilis és $m \nmid f$ (miért?), ezért $f \perp m$ (miért?). Az előző tétel szerint ekkor $\overline{f}$-nak valóban létezik multiplikatív inverze.

□

4. Irreducibilis polinomok, irreducibilis faktorizáció

Definíció (ism.). 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; ilyenkor ***triviális faktorizáció***ról beszélünk.) Formálisan:

$$\forall f, g \in T[x] : p = fg \implies (p \sim f \text{ vagy } p \sim g).$$

Állítás (ism.). *Legyen T egy test és $p \in T[x]$. A p polinom akkor és csak akkor irreducibilis T felett, ha legalább elsőfokú, és nem bontható $\deg p$-nél kisebb fokszámú polinomok szorzatára:*

$$\nexists f, g \in T[x] : \; p = f \cdot g \quad \text{és} \quad 1 \leq \deg f, \deg g < \deg p.$$

Megjegyzés. Gyűrűk felett ez általában nem igaz! Például a $p = 2x \in \mathbb{Z}[x]$ polinom nem irreducibilis $\mathbb{Z}$ felett, mert a $p = 2 \cdot x$ felbontás itt nem triviális (miért?).

Definíció (ism.). A $p \in T[x]$ polinom ***prím***, ha legalább elsőfokú, és valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat egyik tényezőjének. Formálisan:

$$\forall f, g \in T[x] : p \mid fg \implies (p \mid f \text{ vagy } p \mid g).$$

Tétel (ism.). *Test feletti polinomokra az irreducibilitás és a prímtulajdonság ekvivalens.*

Állítás (ism.). *Tetszőleges T testre és $f \in T[x]$ polinomra...*

- $\deg f = 1$ *esetén f irreducibilis T felett, és van gyöke T-ben;*
- $\deg f \in \{2, 3\}$ *esetén f pontosan akkor irreducibilis T felett, ha nincs gyöke T-ben;*
- $\deg f \geq 4$ *esetén ha f irreducibilis T felett, akkor nincs gyöke T-ben.*

Megjegyzés (ism.). Az utolsó pontbeli implikáció megfordítása nem igaz: ha $\deg f \geq 4$, akkor önmagában az a tény, hogy f-nek nincs gyöke T-ben még nem garantálja, hogy f irreducibilis T felett (keressünk példát!).

Tétel (ism.). *Test feletti polinomgyűrűben minden legalább elsőfokú polinom felbomlik irreducibilis polinomok szorzatára, és ez a felbontás lényegében (azaz a tényezők sorrendjétől és asszociáltságtól eltekintve) egyértelmű.*

Megjegyzés. A felbontás tényezők sorrendjétől és asszociáltságtól eltekintve egyértelmű voltát a következőképpen lehet permutációk segítségével precízen megfogalmazni: Ha $p_1 \cdot \ldots \cdot p_n$ és $q_1 \cdot \ldots \cdot q_m$ ugyanazon polinom két irreducibilis faktorizációja, akkor $n = m$, és létezik olyan $\pi \in S_n$ permutáció, hogy $p_i \sim q_{\pi(i)}$ minden $i = 1, \ldots, n$ esetén.

Tétel (ism.). *Minden legalább elsőfokú komplex együtthatós polinomnak van gyöke a komplex számok testében.*

Következmény (ism.). *A komplex számok teste felett pontosan az elsőfokú polinomok irreducibilisek.*

Következmény (ism.). *Minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bomlik. Ha $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ $(n \geq 1, a_n \neq 0)$, akkor f-nek multiplicitással számolva pontosan n gyöke van. Ha ezek a gyökök $\alpha_1, \ldots, \alpha_n$ (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása), akkor $f = a_n (x - \alpha_1) \cdots (x - \alpha_n)$. Ezt nevezzük a polinom* ***gyöktényezős felbontásának****.*

Tétel (ism.). *Egy valós együtthatós polinom pontosan akkor irreducibilis a valós számok teste felett, ha elsőfokú, vagy olyan másodfokú polinom, melynek nincs valós gyöke. Tehát az $\mathbb{R}$ feletti irreducibilis polinomok a következők:*

- $ax + b$ $(a, b \in \mathbb{R}, a \neq 0)$;
- $ax^2 + bx + c$ $\left(a, b, c \in \mathbb{R}, a \neq 0, b^2 - 4ac < 0\right)$.