Definiáld egy (binér) művelet fogalmát!

Definíció

Egy X halmazon értelmezett művelet alatt egy $* : X^n \to X$ függvényt értünk.
Egy X halmazon értelmezett binér (kétváltozós) művelet egy $* : X \times X \to X$ függvény. Gyakran $*(x, y)$ helyett $x * y$-t írunk.

Definiáld az asszociativitás és kommutativitás fogalmát és adj példát nem asszociatív és nem kommutativ műveletre!

Definíció

A $* : X \times X \to X$ művelet
asszociatív, ha $\forall a, b, c \in X : (a * b) * c = a * (b * c)$;
kommutatív, ha $\forall a, b \in X : a * b = b * a$.

- A kivonás az egész számok halmazán nem asszociatív: $-1 = (1 - 1) - 1 \neq 1 - (1 - 1) = 1$.
- A függvények halmazán a kompozíció művelete nem kommutatív: $f(x) = x + 1$, $g(x) = x^2$: $x^2 + 1 = (f \circ g)(x) \neq (g \circ f)(x) = (x + 1)^2$.

Definiáld egy grupoid fogalmát!

Az egy binér műveletes struktúrát grupoidnak nevezzük.

Definiáld egy félcsoport , semleges elem és monoid fogalmát és adj példát olyan grupoidra , amely nem félcsoport!

Definíció

A $(G; *)$ grupoid félcsoport, ha $*$ asszociatív G-n.
Ha létezik $s \in G$: $\forall g \in G : s * g = g * s = g$,
akkor az s semleges elem (egységelem), $(G; *)$ pedig semleges elemes félcsoport (egységelemes félcsoport, monoid).

- $\mathbb{N}$ az $+$ művelettel egységelemes félcsoport $n = 0$ egységelemmel.

Definiáld az inverz , csoport , Ábel-csoportz fogalmát !

Definíció

Legyen $(G;*)$ egy egységelemes félcsoport e egységelemmel. A $g \in G$ elem inverze a $g^{-1} \in G$ elem, melyre $g * g^{-1} = g^{-1} * g = e$.
Ha minden $g \in G$ elemnek létezik inverze, akkor $(G;*)$ csoport.
Ha ezen felül $*$ kommutatív is, akkor $(G;*)$ Abel-csoport.

Definiáld a disztributivitás fogalmát!

Definíció

Legyen $(R;*,\circ)$ algebrai struktúra, ahol $*$ és $\circ$ binér műveletek. Azt mondjuk, hogy teljesül a $\circ$-nek a $*$-ra vonatkozó bal oldali disztributivitása, illetve jobb oldali disztributivitása, ha
$\forall k, l, m \in R$-re: $k \circ (l * m) = (k \circ l) * (k \circ m)$, illetve
$\forall k, l, m \in R$-re: $(l * m) \circ k = (l \circ k) * (m \circ k)$.

Definiáld a gyűrű , egységelemes és kommutatív gyűrű fogalmát fogalmát!

Definíció

Az $(R;*,\circ)$ két binér műveletes algebrai struktúra gyűrű, ha

- $(R;*)$ Abel-csoport;
- $(R;\circ)$ félcsoport;
- teljesül a $\circ$-nek a $*$-ra vonatkozó mindkét oldali disztributivitása.

Az $(R;*,\circ)$ gyűrű egységelemes gyűrű, ha R-en a $\circ$ műveletre nézve van egységelem.
Az $(R;*,\circ)$ gyűrű kommutatív gyűrű, ha a $\circ$ művelet (is) kommutatív.

Definiáld a nullelem/egységelem fogalmát gyűrűben !

Elnevezés

$(R;*,\circ)$ két binér műveletes algebrai struktúra esetén a $*$-ra vonatkozó semleges elemet nullelemnek, a $\circ$-re vonatkozó semleges elemet egységelemnek nevezzük. A nullelem szokásos jelölése 0, az egységelemé 1, esetleg e.

Definiáld a nullosztómentes gyűrű fogalmát!

Definíció

Ha egy $(R, *, \circ)$ gyűrűben $\forall r, s \in R$, $r, s \neq 0$ esetén $r \circ s \neq 0$, akkor R nullosztómentes gyűrű.

Definiáld az integritási tartomány fogalmát !

Definíció

A kommutatív, nullosztómentes gyűrűt integritási tartománynak nevezzük.

Definiáld a karakterisztika fogalmát!

Állítás

Nullosztómentes gyűrűben a nem-nulla elemek additív rendje megegyezik, és vagy egy p prímszám vagy végtelen.

Definíció

Ha az előző állításban szereplő közös rend p, akkor a gyűrű karakterisztikája p, ha a közös rend végtelen, akkor pedig 0. Jelölése: $char(R)$.

Definiáld az osztó/többszörös és az egység fogalmát!

Definíció

Az $(R; *, \circ)$ egységelemes integritási tartományban az $a, b \in R$ elemekre azt mondjuk, hogy a osztója b-nek, ha van olyan $c \in R$, amire $b = a \circ c$. Jelölése: $a|b$.

Definíció

Az egységelem osztóját egységnek nevezzük.

Definiáld a felbonthatatlan elem fogalmát !

Az *f* elem felbonthatatlan (irreducibilis), ha (*f* nem nulla és nem egység) *f*=*ab* esetén *a* vagy *b* szükségképpen egység.

Adj példát gyűrűre!

- $(\mathbb{Z}; +, \cdot)$ egységelemes kommutatív gyűrű.
- $(2\mathbb{Z}; +, \cdot)$ gyűrű, de nem egységelemes.
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ a szokásos műveletekkel egységelemes kommutatív gyűrűk.
- $\mathbb{C}^{k\times k}$ a szokásos műveletekkel egységelemes gyűrű, de nem kommutatív, ha $k > 1$.

Adj példákat végtelen testre!

Q –nál szükebb végtelen test nincs.

Mi teljesül a nullelemmel való szorzás esetén gyűrűben ? Bizonyitas !

Állítás

Legyen $(R; *, \circ)$ gyűrű $0 \in R$ nullelemmel. Ekkor $\forall r \in R$ esetén $0 \circ r = r \circ 0 = 0$.

x0 = x(0+0) = x0 + x0 és 'kivonva x0-t' mind két oldalon 0 = x0-t kapunk.

Mit mondhatunk testben a nullosztókról ? Bizonyítás !

Állítás

Test nullosztómentes.

Ha a,b nullosztó pár lenne, akkor a nem 0, b nem 0 és ab = 0, de ha A lenne a inverze, akkor Aa = e, és így Aab = b kellene hogy teljesüljön, de ab = 0 miatt Aab = A0 = 0 (az előző pont miatt).**Definiáld a polinomokat a műveletekkel !**

Definíció

Legyen $(R; +, \cdot)$ gyűrű. A gyűrű elemeiből képzett $f = (f_0, f_1, f_2, \dots)$ $(f_j \in R)$ végtelen sorozatot R fölötti polinomnak nevezzük, ha csak véges sok eleme nem-nulla.
Az R fölötti polinomok halmazát $R[x]$-szel jelöljük.
$R[x]$ elemein definiáljuk az összeadást és a szorzást.
$f = (f_0, f_1, f_2, \dots)$, $g = (g_0, g_1, g_2, \dots)$ és $h = (h_0, h_1, h_2, \dots)$ esetén
$f + g = (f_0 + g_0, f_1 + g_1, f_2 + g_2, \dots)$ és $f \cdot g = h$, ahol

$$h_k = \sum_{i+j=k} f_i g_j = \sum_{i=0}^{k} f_i g_{k-i} = \sum_{j=0}^{k} f_{k-j} g_j .$$

Milyen kapcsolat van a gyűrű és az adott gyűrű fölötti polinomgyűrű között? Bizonyitással !

Állítás

Ha az R gyűrű kommutatív, akkor $R[x]$ is kommutatív.

Állítás

$1 \in R$ egységelem esetén $e = (1, 0, 0 \ldots)$ egységeleme lesz $R[x]$-nek.

Állítás

Ha az R gyűrű nullosztómentes, akkor $R[x]$ is nullosztómentes.

$$(fg)_k = \sum_{i+j=k} f_i g_j = \sum_{j+i=k} g_j f_i = (gf)_k$$

Bizonyítás

Legyen n, illetve m a legkisebb olyan index, amire $f_n \neq 0$, illetve $g_m \neq 0$.

$$(f \cdot g)_{n+m} = \sum_{j=0}^{n+m} f_j g_{n+m-j} = \sum_{j=0}^{n-1} f_j g_{n+m-j} + f_n g_m + \sum_{j=n+1}^{n+m} f_j g_{n+m-j} =$$

$$= 0 + f_n g_m + 0 = f_n g_m \neq 0$$

Az első kettőnek nem volt bizonyitasa !

Definiáld az együttható, a főtag , konstans tag , fok fogalmát !

Jelölés

Az $f = (f_0, f_1, f_2, \ldots, f_n, 0, 0, \ldots)$, $f_n \neq 0$ polinomot $f(x) = f_0 + f_1 x + f_2 x^2 + \ldots + f_n x^n$, $f_n \neq 0$ alakba írjuk.

Definíció

Az előző pontban szereplő polinom esetén f_i-t az i-ed fokú tag együtthatójának nevezzük, f_0 a polinom konstans tagja, f_n a főegyütthatója, $f_n x^n$ a főtagja, n pedig a foka. f fokának jelölésére $deg(f)$ használatos.

Definiáld a konstans , lineáris polinom , monom , főpolinom fogalmát !

Definíció

A konstans polinomok a legfeljebb nulladfokú polinomok, a lineáris polinomok pedig a legfeljebb elsőfokú polinomok. Az $f_i x^i$ alakba írható polinomok a monomok. Ha $f \in R[x]$ polinom főegyütthatója R egységeleme, akkor f-et főpolinomnak nevezzük.

Definiáld a nullpolinomot !

Megjegyzés

A főegyüttható tehát a legnagyobb indexű nem-nulla együttható, a fok pedig ennek indexe.
A $0 = (0, 0, \dots)$ nullpolinomnak nincs legnagyobb indexű nem-nulla együtthatója, így a fokát külön definiáljuk, mégpedig $deg(0) = -\infty$.

Mit mondhatunk a polinomok összegének / szorzatának fokáról?

Megjegyzés

Könnyen látható, hogy polinomok összege és szorzata is polinom.

Állítás

Legyen $f, g \in R[x]$, $deg(f) = n$, és $deg(g) = k$. Ekkor:

- $deg(f + g) \leq \max(n, k)$;
- $deg(f \cdot g) \leq n + k$.

Bizonyítás

Legyen $h = f + g$. Ekkor $j > \max(n, k)$ esetén $h_j = 0 + 0 = 0$.
Legyen $h = f \cdot g$. Ekkor $j > n + k$ esetén

$$h_j = \sum_{i=0}^{j} f_i g_{j-i} = \sum_{i=0}^{n} f_i g_{j-i} + \sum_{i=n+1}^{j} f_i g_{j-i} = 0.$$

Adj példát, amikor a polinom összegére / szorzatára vonatkozó becslésben szigorú egyenlőtlenség teljesül !

Legyen $f(x) = x^2 + x + 1$ és $g(x) = 2x^2 + 1$ ($f,g \in \mathbb{Z}_3[x]$). Ekkor:

$$\deg(f+g)=\deg(\underline{x^2} + x + 1 + \underline{2x^2} + 1) = \deg(x + 2) = \mathbf{1} < \max(2, 2) = \mathbf{2}$$

$$\deg(f \cdot g) = \deg((\underline{x^2} + x + 1) \cdot (\underline{2x^2} + 1)) = \mathbf{1} < 2 + 2 = \mathbf{4}$$

Definiáld a helyettesítési érték , gyök , polinomfüggvény fogalmát !

Definíció

Az $f(x) = f_0 + f_1 x + f_2 x^2 + \ldots + f_n x^n \in R[x]$ polinom $r \in R$ helyen felvett helyettesítési értékén az $f(r) = f_0 + f_1 r + f_2 r^2 + \ldots + f_n r^n \in R$ elemet értjük.
$f(r) = 0$ esetén r-et a polinom gyökének nevezzük.
Az $\hat{f} : r \mapsto f(r)$ leképezés az f polinomhoz tartozó polinomfüggvény.

Adj példát , amikor különböző polinomokhoz ugyanaz a polinomfüggvény tartozik !

Megjegyzés

Ha R véges, akkor csak véges sok $R \to R$ függvény van, míg végtelen sok $R[x]$-beli polinom, így vannak olyan polinomok, amikhez ugyanaz a polinomfüggvény tartozik, például $x, x^2 \in \mathbb{Z}_2[x]$.

Példa

$f(x) = x^2 + x - 2 \in \mathbb{Z}[x]$-nek a -2 helyen felvett helyettesítési értéke $(-2)^2 + (-2) - 2 = 0$, ezért -2 gyöke f-nek.

Hogyan szól a maradékos osztás tétele? Bizonyitas !

Tétel (polinomok maradékos osztása)

Legyen R egységelemes integritási tartomány, $f, g \in R[x]$, és tegyük fel, hogy g főegyütthatója egység R-ben. Ekkor egyértelműen léteznek olyan $q, r \in R[x]$ polinomok, melyekre $f = qg + r$, ahol $deg(r) < deg(g)$.

Bizonyítás

Létezés: f foka szerinti TI: ha $deg(f) < deg(g)$, akkor $q = 0$ és $r = f$ esetén megfelelő előállítást kapunk.
Legyen f főegyütthatója f_n, g főegyütthatója g_k. $n \geq k$ esetén legyen $f^*(x) = f(x) - f_n g_k^{-1} g(x) x^{n-k}$.
$deg(f^*) < deg(f)$ (Miért?) miatt f^*-ra használhatjuk az indukciós feltevést, vagyis léteznek $q^*, r^* \in R[x]$ polinomok, amikre $f^* = q^* g + r^*$.
$f(x) = f^*(x) + f_n g_k^{-1} g(x) x^{n-k} = q^*(x) g(x) + r^*(x) + f_n g_k^{-1} g(x) x^{n-k} =$
$= (q^*(x) + f_n g_k^{-1} x^{n-k}) g(x) + r^*(x)$,
így $q(x) = q^*(x) + f_n g_k^{-1} x^{n-k}$ és $r(x) = r^*(x)$ jó választás.

Bizonyítás folyt.

Egyértelműség: Tekintsük f két megfelelő előállítását:
$f = qg + r = q^* g + r^*$, amiből:

$$g(q - q^*) = r^* - r.$$

Ha a bal oldal nem 0, akkor a foka legalább k, de a jobb oldal foka legfeljebb $k - 1$, tehát
$0 = g(q - q^*) = r^* - r$, és így
$q = q^*$ és $r = r^*$.

Definiáld a gyöktényező fogalmát !

Definíció

Ha $c \in R$ az $f \in R[x]$ polinom gyöke, akkor $(x - c) \in R[x]$ a c-hez tartozó gyöktényező.

Hogy szól a gyöktényező leválasztására vonatkozó tétel? Bizonyitas !

Következmény (gyöktényező leválasztása)

Ha $0 \neq f \in R[x]$, és $c \in R$ gyöke f-nek, akkor létezik olyan $q \in R[x]$, amire $f(x) = (x - c) q(x)$.

Bizonyítás

Osszuk el maradékosan f-et $(x-c)$-vel (Miért lehet?):

$$f(x) = q(x)(x-c) + r(x).$$

Mivel $deg(r(x)) < deg(x-c) = 1$, ezért r konstans polinom.
Helyettesítsünk be c-t, így azt kapjuk, hogy
$0 = f(c) = q(c)(c-c) + r(c) = r(c)$,
amiből $r = 0$.

Hány gyöke lehet egy polinomnak? Bizonyitás !

Következmény

Az $f \neq 0$ polinomnak legfeljebb $deg(f)$ gyöke van.

Bizonyítás

f foka szerinti TI:
$deg(f) = 0$-ra igaz az állítás (Miért?).
Ha $deg(f) > 0$, és $f(c) = 0$, akkor $f(x) = (x-c)g(x)$ (Miért?), ahol $deg(g) + 1 = deg(f)$ (Miért?). Ha d gyöke f-nek, akkor $d - c = 0$, amiből $d = c$, vagy d gyöke g-nek (Miért?). Innen következik az állítás.

Mit mondhatunk legfeljebb két , n+1 helyen megegyező , legfeljebb n-edfokú polinomról? Bizonyítás !

Következmény

Ha két, legfeljebb n-ed fokú polinomnak $n+1$ különböző helyen ugyanaz a helyettesítési értéke, akkor egyenlőek.

Bizonyítás

A két polinom különbsége legfeljebb n-ed fokú, és $n+1$ gyöke van (Miért?), ezért nullpolinom (Miért?), vagyis a polinomok egyenlőek.

Mit mondhatunk végtelen R esetén a polinomfüggvényről ? Bizonyítás !

Következmény

Ha R végtelen, akkor két különböző $R[x]$-beli polinomhoz nem tartozik ugyanaz a polinomfüggvény.

Bizonyítás

Ellenkező esetben a polinomok különbségének végtelen sok gyöke lenne (Miért?).

Definiáld az oszthatóságot , kitüntett közös osztóját polinomok körében és milyen polinomokra tudjuk biztosan alkalmazni az euklédeszi algoritmust?!

Definíció

Azt mondjuk, hogy $f, g \in R[x]$ polinomok esetén f osztója g-nek (g többszöröse f-nek), ha létezik $h \in R[x]$, amire $g = f \cdot h$.

Definíció

Az $f, g \in R[x]$ polinomok kitüntetett közös osztója (legnagyobb közös osztója) az a $d \in R[x]$ polinom, amelyre $d|f$, $d|g$, és tetszőleges $c \in R[x]$ esetén $(c|f \wedge c|g) \Rightarrow c|d$.

Test fölötti polinomgyűrűben tetszőleges nem-nulla polinommal tudunk maradékosan osztani, ezért működik a bővített euklideszi-algoritmus. Ez $f, g \in R[x]$ esetén (R test) meghatározza f és g kitüntetett közös osztóját, a $d \in R[x]$ polinomot, továbbá $u, v \in R[x]$ polinomokat, amelyekre $d = u \cdot f + v \cdot g$.

Ismertesd a bővitett euklédeszi algoritmust! Bizonyitsd helyességét !

Algoritmus

Legyen R test, $f, g \in R[x]$. Ha $g = 0$, akkor $(f, g) = f = 1 \cdot f + 0 \cdot g$, különben végezzük el a következő maradékos osztásokat:

$$\begin{aligned}
f &= q_1 g + r_1;\\
g &= q_2 r_1 + r_2;\\
r_1 &= q_3 r_2 + r_3;\\
&\vdots\\
r_{n-2} &= q_n r_{n-1} + r_n;\\
r_{n-1} &= q_{n+1} r_n.
\end{aligned}$$

Ekkor $d = r_n$ jó lesz kitüntetett közös osztónak.
Az $u_{-1} = 1,\ u_0 = 0,\ v_{-1} = 0,\ v_0 = 1$ kezdőértékekkel, továbbá az $u_k = u_{k-2} - q_k \cdot u_{k-1}$ és $v_k = v_{k-2} - q_k \cdot v_{k-1}$ rekurziókkal megkapható $u = u_n$ és $v = v_n$ polinomok olyanok, amelyekre teljesül $d = u \cdot f + v \cdot g$.

Bizonyítás

A maradékok foka természetes számok szigorúan monoton csökkenő sorozata, ezért az eljárás véges sok lépésben véget ér.
Indukcióval belátjuk, hogy $r_{-1} = f$ és $r_0 = g$ jelöléssel $r_k = u_k \cdot f + v_k \cdot g$ teljesül minden $-1 \leq k \leq n$ esetén:
$k = -1$-re $f = 1 \cdot f + 0 \cdot g$, $k = 0$-ra $g = 0 \cdot f + 1 \cdot g$.
Mivel $r_{k+1} = r_{k-1} - q_{k+1} \cdot r_k$, így az indukciós feltevést használva:
$r_{k+1} = u_{k-1} \cdot f + v_{k-1} \cdot g - q_{k+1} \cdot (u_k \cdot f + v_k \cdot g) =$
$= (u_{k-1} - q_{k+1} \cdot u_k) \cdot f + (v_{k-1} - q_{k+1} \cdot v_k) \cdot g = u_{k+1} \cdot f + v_{k+1} \cdot g$.
Tehát $r_n = u_n \cdot f + v_n \cdot g$, és így f és g közös osztói r_n-nek is osztói.
Kell még, hogy r_n osztója f-nek és g-nek.
Indukcióval belátjuk, hogy $r_n | r_{n-k}$ teljesül minden $0 \leq k \leq n+1$ esetén:
$k = 0$-ra $r_n | r_n$ nyilvánvaló, $k = 1$-re $r_{n-1} = q_{n+1} r_n$ miatt $r_n | r_{n-1}$.
$r_{n-(k+1)} = q_{n-(k-1)} r_{n-k} + r_{n-(k-1)}$ miatt az indukciós feltevést használva kapjuk az állítást, és így $k = n$, illetve $k = n+1$ helyettesítéssel $r_n | r_0 = g$, illetve $r_n | r_{-1} = f$.

Ismertesd a Horner-elrendezést !

Legyen $f(x) = f_n x^n + f_{n-1}x^{n-1} + \ldots + f_1 x + f_0$, ahol $f_n \neq 0$. Ekkor átrendezéssel a következő alakot kapjuk:
$f(x) = (\cdots((f_n \cdot x + f_{n-1}) \cdot x + f_{n-2}) \cdot x + \ldots + f_1) \cdot x + f_0$, és így
$f(c) = (\ldots((f_n \cdot c + f_{n-1}) \cdot c + f_{n-2}) \cdot c + \ldots + f_1) \cdot c + f_0$.
Vagyis $f(c)$ kiszámítható n db szorzás és n db összeadás segítségével.

	f_n	f_{n-1}	f_{n-2}	$\ldots$	f_0	
c	$\times$	$c_1 = f_n$	$c_2 = c_1 c + f_{n-1}$	$\ldots$	$c_n = c_{n-1}c + f_1$	$f(c) = c_n c + f_0$

Általánosan: $c_k = c_{k-1}c + f_{n-k+1}$, ha $1 < k \leq n$.

Adj példát olyan polinomra , amelynek különböző polinomgyűrűben különböző számú gyöke van !

Legyen $f(x) = x^2 - 1$.
$x^2 - 1 = (x - 1)(x + 1) \Rightarrow \mathbb{R}[x]$ felett -1 és 1 a gyökei f-nek, vagyis 2 gyöke van.
$\mathbb{Z}_2[x]$ felett $(x - 1)(x + 1) = (x + 1)(x + 1)$ miatt csak az 1 a gyöke f-nek.

Definiáld az algebrai derivált fogalmát és milyen tulajdonságokkal rendelkezik ? !

Definíció

Legyen R gyűrű. Az
$f(x) = f_n x^n + f_{n-1}x^{n-1} + \ldots + f_2 x^2 + f_1 x + f_0 \in R[x]$ $(f_n \neq 0)$ polinom
algebrai deriváltja az
$f'(x) = nf_n x^{n-1} + (n-1)f_{n-1}x^{n-2} + \ldots + 2f_2 x + f_1 \in R[x]$ polinom.

Állítás

Ha R egységelemes integritási tartomány, akkor az $f \mapsto f'$ algebrai deriválás rendelkezik a következő tulajdonságokkal:

1. konstans polinom deriváltja a nullpolinom;
2. az x polinom deriváltja az egységelem;
3. $(f + g)' = f' + g'$, ha $f, g \in R[x]$ (additivitás);
4. $(fg)' = f'g + fg'$, ha $f, g \in R[x]$ (szorzat differenciálási szabálya).

Mivel egyenlő elsőfokú főpolinom n-edik hatványának deriváltja? Bizonyítás !

Állítás

Ha R egységelemes integritási tartomány, $c \in R$ és $n \in \mathbb{N}^+$, akkor $((x-c)^n)' = n(x-c)^{n-1}$.

Bizonyítás

n szerinti TI:
$n = 1$ esetén $(x-c)' = 1 = 1 \cdot (x-c)^0$.
Tfh. $n = k$-ra teljesül az állítás, vagyis $((x-c)^k)' = k(x-c)^{k-1}$.
Ekkor
$((x-c)^{k+1})' = ((x-c)^k(x-c))' = ((x-c)^k)'(x-c) + (x-c)^k(x-c)' =$
$= k(x-c)^{k-1}(x-c) + (x-c)^k \cdot 1 = (x-c)^k(k+1)$.
Ezzel az állítást beláttuk.

Definiáld a többszörös gyök fogalmát !

Definíció

Legyen R egységelemes integritási tartomány, $0 \neq f \in R[x]$ és $n \in \mathbb{N}^+$.
Azt mondjuk, hogy $c \in R$ az f egy n-szeres gyöke, ha $(x-c)^n | f$, de $(x-c)^{n+1} \nmid f$.

Milyen kapcsolat van a polinom gyökei illetve a deriváltjának gyökei között ? Bizonyítás !

Tétel

Legyen R egységelemes integritási tartomány, $f \in R[x]$, $n \in \mathbb{N}^+$ és $c \in R$ az f egy n-szeres gyöke. Ekkor c az f'-nek legalább $(n-1)$-szeres gyöke, és ha $char(R) \nmid n$, akkor pontosan $(n-1)$-szeres gyöke.

Bizonyítás

Ha $f(x) = (x-c)^n g(x)$, ahol c nem gyöke g-nek, akkor
$f'(x) = ((x-c)^n)' g(x) + (x-c)^n g'(x) =$
$= n(x-c)^{n-1} g(x) + (x-c)^n g'(x) = (x-c)^{n-1}(ng(x) + (x-c)g'(x))$.
Tehát c tényleg legalább $(n-1)$-szeres gyöke f'-nek, és akkor lesz $(n-1)$-szeres gyöke, ha c nem gyöke $ng(x) + (x-c)g'(x)$-nek, vagyis $0 \neq ng(c) + (c-c)g'(c) = ng(c) + 0 \cdot g'(c) = ng(c)$. Ez pedig teljesül, ha $char(R) \nmid n$.

Adj példát olyan polinomra , amelynek van n-szeres gyöke , ami a deriváltjának is n-szeres gyöke !

Példa

Legyen $f(x) = x^4 - x \in \mathbb{Z}_3[x]$. Ekkor 1 3-szoros gyöke f-nek, mert

$$f(x) = x(x^3 - 1) \overset{\mathbb{Z}_3}{=} x(x^3 - 3x^2 + 3x - 1) = x(x-1)^3.$$
$$f'(x) = 4x^3 - 1 \overset{\mathbb{Z}_3}{=} x^3 - 3x^2 + 3x - 1 = (x-1)^3,$$

tehát 1 3-szoros gyöke f'-nek is.

Milyen alakú egy Lagrange-interpolációs alappolinom és ismertesd!?

Tétel

Legyen R test, $c_0, c_1, \ldots, c_n \in R$ különbözőek, továbbá $d_0, d_1, \ldots, d_n \in R$ tetszőlegesek. Ekkor létezik egy olyan legfeljebb n-ed fokú polinom, amelyre $f(c_j) = d_j$, ha $j = 0, 1, \ldots, n$.

Bizonyítás

Legyen

$$l_j(x) = \frac{\prod_{i \neq j}(x - c_i)}{\prod_{i \neq j}(c_j - c_i)},$$

a j-edik Lagrange-interpolációs alappolinom, és legyen

$$f(x) = \sum_{j=0}^{n} d_j l_j(x).$$

$l_j(c_i) = 0$, ha $i \neq j$, és $l_j(c_j) = 1$-ből következik az állítás.

Hogyan konstruálunk p^n elemű testet ?

Legyen K test, és f∈K[x] egy n-ed fokú (n>1) irreducibilis főpolinom. Ekkor az (f) főideál maximális ideál, így K=K[x]/(f) test.
Legyen p prím. A fenti konstrukciót alkalmazva a Z_p véges testre egy p^n elemű véges testet kapunk.

Mit mondhatunk véges testekről az elemszámmal kapcsolatban ?

Bármely véges test elemeinek száma prímhatvány, ahol a prím a test karakterisztikája.
Bármely $q = p^n$ (p prím, $n \in \mathbb{N}^+$) prímhatványra a q elemű véges testek izomorfak.

Legyen $F_9 = Z_3[x]/(x^2 + 1)$. Mik lesznek a $z^2 + 1$ eleme $F_9[z]$ polinom gyökei?

p/q alak

p = +1 és -1
q = +1 és -1

Horner módszerrel az 1 és -1 a gyöke !

Mik lehetnek egy primitív egész együtthatós polinom racionális gyökei? Bizonyitasssal !

a_i x-b_i alakú számok szorzata mi lehet ha a_ix,b_i egészek akkor a főegyütható a_i-k szorzata, a konstans b_i-k szorzata ezért csak olyan racionális b/a alakú gyökök lehetnek hogy ahol a főegyütható osztója a-nak és konstans tag osztója b-nek.

Bizonyítsd be , hogy gyök 2 nem eleme Q nak !0

Állítás

$\sqrt{2} \notin \mathbb{Q}$.

Bizonyítás

Tekintsük az $x^2 - 2 \in \mathbb{Z}[x]$ polinomot.
Ennek a $\frac{p}{q}$ alakú gyökeire $(p, q \in \mathbb{Z}, (p, q) = 1)$ teljesül, hogy $p|2$ és $q|1$, így a lehetséges racionális gyökei ± 1 és ± 2.

Hogyan jellemezhetőek test fölötti polinomgyűrűben az egységek ? Bizonyítás!

Állítás

Legyen $(F; +, \cdot)$ test. Ekkor $f \in F[x]$ pontosan akkor egység, ha $deg(f) = 0$.

Bizonyítás

$\Longleftarrow$

Ha $deg(f) = 0$, akkor f nem-nulla konstans polinom: $f(x) = f_0$. Mivel F test, ezért létezik $f_0^{-1} \in F$, amire $f_0 \cdot f_0^{-1} = 1$, így f tényleg egység.

$\Longrightarrow$

Ha f egység, akkor létezik $g \in F[x]$, amire $f \cdot g = 1$, és így $deg(f) + deg(g) = deg(1) = 0$ (Miért?), ami csak $deg(f) = deg(g) = 0$ esetén lehetséges.

Mit mondhatunk test fölötti polinomokról a gyökökkel kapcsolatban ? Bizonyíás !

Állítás

Legyen $(F; +, \cdot)$ test, és $f \in F[x]$. Ha $deg(f) \models 1$, akkor f-nek van gyöke.

Bizonyítás

Ha $deg(f) = 1$, akkor felírható $f(x) = f_1 x + f_0$ alakban, ahol $f_1 \neq 0$. Azt szeretnénk, hogy létezzen $c \in F$, amire $f(c) = 0$, vagyis $f_1 c + f_0 = 0$. Ekkor $f_1 c = -f_0$ (Miért?), és mivel létezik $f_1^{-1} \in F$, amire $f_1 \cdot f_1^{-1} = 1$ (Miért?), ezért $c = -f_0 \cdot f_1^{-1} \left(= -\frac{f_0}{f_1}\right)$ gyök lesz.

Adj példát olyan elsőfokú polinomra , amelynek nincs gyöke !

2x-1 eleme Z [x] : (Ha R nem test akkor nem feltetlenul vagy gyöke)

Mit mondhatunk a lineáris polinomokról test fölötti polinomgyűrűben felbonhatóság szempontjából ! Bizonyítás !

Állítás

Legyen $(F;+,\cdot)$ test, és $f \in F[x]$. Ha $deg(f) = 1$, akkor f felbonthatatlan.

Bizonyítás

Legyen $f = g \cdot h$. Ekkor $deg(g) + deg(h) = deg(f) = 1$ (Miért?) miatt $deg(g) = 0 \wedge deg(h) = 1$ vagy $deg(g) = 1 \wedge deg(h) = 0$. Előbbi esetben g, utóbbiban h egység a korábbi állítás értelmében.

Hogyan jellemezhetők a test fölötti másod- , illetve harmadfokú polinomok felbonhatóság szempontjából !

Állítás

Legyen $(F;+,\cdot)$ test, és $f \in F[x]$. Ha $2 \leq deg(f) \leq 3$, akkor f pontosan akkor felbontható, ha van gyöke.

Bizonyítás

$\Longleftarrow$

Ha c gyöke f-nek, akkor az $f(x) = (x-c)g(x)$ egy nemtriviális felbontás (Miért?).

$\Longrightarrow$

Mivel $2 = 0+2 = 1+1$, illetve $3 = 0+3 = 1+2$, és más összegként nem állnak elő, ezért amennyiben f-nek van nemtriviális felbontása, akkor van elsőfokú osztója. A korábbi állítás alapján ennek van gyöke, és ez nyilván f gyöke is lesz.

Hogyan jellemezzük a komplex fölötti felbonhatatlan polinomokat ? Bizonyítás !

Tétel

$f \in \mathbb{C}[x]$ pontosan akkor felbonthatatlan, ha $deg(f) = 1$.

Bizonyítás

$\Longleftarrow$

Mivel $\mathbb{C}$ a szokásos műveletekkel test, ezért korábbi állítás alapján teljesül.

$\Longrightarrow$

Indirekt tfh. $deg(f) \neq 1$. Ha $deg(f) < 1$, akkor $f = 0$ vagy f egység, tehát nem felbonthatatlan, ellentmondásra jutottunk.
$deg(f) > 1$ esetén az algebra alaptétele értelmében van gyöke f-nek. A gyöktényezőt kiemelve az $f(x) = (x - c)g(x)$ alakot kapjuk, ahol $deg(g) \geq 1$ (Miért?), vagyis egy nemtriviális szorzat-előállítást, így f nem felbonthatatlan, ellentmondásra jutottunk.

Hogyan jellemezhetők a racionális számok fölötti felbonthatatlan polinomok ?

Tétel

$f \in \mathbb{R}[x]$ pontosan akkor felbonthatatlan, ha

- $deg(f) = 1$, vagy
- $deg(f) = 2$, és f-nek nincs (valós) gyöke.

Bizonyítás

$\Longleftarrow$

Ha $deg(f) = 1$, akkor korábbi állítás alapján f felbonthatatlan.
Ha $deg(f) = 2$, és f-nek nincs gyöke, akkor f nem áll elő két elsőfokú polinom szorzataként (Miért?), vagyis csak olyan kéttényezős szorzat-előállítása lehet, melyben az egyik tényező foka 0, tehát egység.

$\Longrightarrow$

Ha f felbonthatatlan, akkor nem lehet $deg(f) < 1$. (Miért?)
Ha f felbonthatatlan, és $deg(f) = 2$, akkor tfh. van gyöke. Ekkor az ehhez tartozó gyöktényező kiemelésével egy nemtriviális felbontását kapjuk f-nek (Miért?), ami ellentmondás.

Definiáld a primitív polinom fogalmát !

Definíció

$f \in \mathbb{Z}[x]$-et primitív polinomnak nevezzük, ha az együtthatóinak a legnagyobb közös osztója 1.

Hogy szól a Schönemann – Eisenstein – tétel egész együtthatós polinomokra?

Tétel (Schönemann-Eisenstein)

Legyen $f(x) = f_n x^n + f_{n-1}x^{n-1} + \ldots + f_1 x + f_0 \in \mathbb{Z}[x]$, $f_n \neq 0$ legalább elsőfokú primitív polinom. Ha található olyan $p \in \mathbb{Z}$ prím, melyre

- $p \nmid f_n$,
- $p | f_j$, ha $0 \leq j < n$,
- $p^2 \nmid f_0$,

akkor f felbonthatatlan $\mathbb{Z}$ fölött.