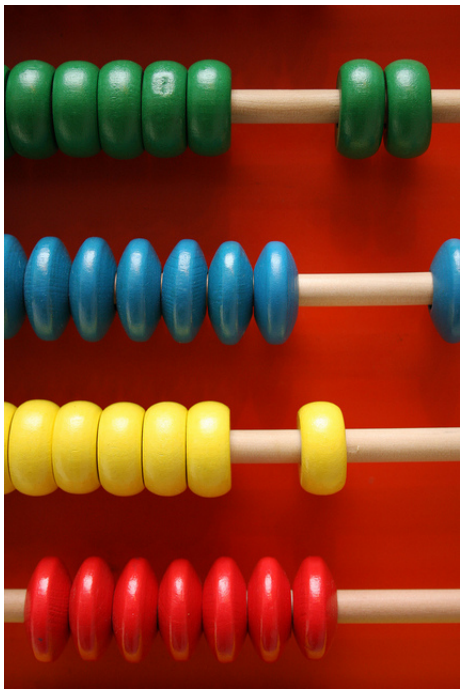
MATEMATIKARAKO SARRERA

OCW 2015



Leire Legarreta Solaguren
EHU-ko Zientzia eta Teknologia Fakultatea
Matematika Saila

6 GAIA: POLINOMIOAK

Polinomioen eraztuna. Polinomio biren zatitzaile komunetatiko haundiena. Euclidesen Algoritmoa. Polinomioen faktorizazioa. Irreduzibilitateko irizpideak. Batugai soiletako zatikien deskonposizioa.

1 Polinomioen eraztuna

Definizioa. *Izan bedi K gorputza. (Normalean K bezala, $\mathbb{Q}$ zenbaki arrazionalen gorputza, $\mathbb{R}$ zenbaki errealen gorputza edo $\mathbb{C}$ zenbaki konplexuen gorputza hartuko ditugu. Azken gorputza hori hurrengoko gaian aztertuko da). K gorputzeko koefizientedun polinomio deitzen zaio ondoko adierazpen honi,*

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

non $a_0, a_1, \ldots, a_n$, K gorputzeko elementuak diren. Eskalar hauek, $(a_0, \ldots, a_n)$, polinomioaren koefizienteak deitzen dira, eta x hizkia, polinomioaren ezezaguna, indeterminatua edo aldagaia deitzen da. Koefiziente berdinak dituzten bi polinomio berdinak direla esaten da, eta polinomio baten koefiziente guztiak zero direnean, polinomio honi polinomio hutsa deitzen zaio. Polinomio bat konstantea dela esaten da, baldin eta edozein $i \geq 1$ indizerako, $a_i = 0$ bada. Bestalde, K gorputzeko koefizientedun polinomioak osatzen duten multzoa, $K[x]$ moduan adierazten da.

Definizioa. *Izan bedi $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[x]$ polinomioa. Definizioz, $a_i \neq 0$ baldintza betetzen duen i indize haundienari, polinomioaren maila deitzen zaio, eta $dg(f(x))$ ikurra bitartez adierazten da. Gainera, konbenioz, polinomio hutsak ez dauka mailarik eta zeroren desberdinak diren polinomio konstante guztien maila zero da. Gainera, kasu honetan, baldin eta a_n koefizientea 1 bada, $f(x)$ polinomio monikoa dela esaten da.*

Definizioa. *Izan bitez $f(x), g(x) \in K[x]$ bi polinomio, hau da, $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ eta $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n + \cdots + b_mx^m$, eta demagun orokortasuna galdu gabe $m > n$ dela, eta $a_n \neq 0, b_m \neq 0$ direla. Definitzen dira, $K[x]$ multzoan ondoko bi eragiketa:*

(i) *Polinomioen batuketa:*

$$f(x)+g(x) = (a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\cdots+(a_n+b_n)x^n+b_{n+1}x^{n+1}+$$

$$\cdots + b_mx^m$$

(ii) *Polinomioen biderketa:*

$$f(x).g(x) = a_0b_0+(a_0b_1+a_1b_0)x+(a_0b_2+a_1b_1+a_2b_0)x^2+\cdots+(a_nb_m)x^{n+m}$$

$$= \sum_{j=0}^{n+m}(\sum_{k=0}^{j} a_k b_{j-k})x^j.$$

Bestalde, $dg(f(x)+g(x)) \leq max\{dg(f(x)), dg(g(x))\}$*, eta* $dg(f(x)g(x)) = dg(f(x))+dg(g(x))$.

Teorema. *Izan bedi* $(K,+,.)$ *gorputza. Orduan,* $(K[x],+,.)$ *identitatedun eraztun trukakorra da. Bestalde,* $\mathcal{U}(K[x]) = \{$*Polinomio konstante ez nuluak*$\}$ *osatutako multzoa da, eta* $(\mathcal{U}(K[x]),.)$ *talde egitura du.*

Teorema. Zatiketa Algoritmoa.

Izan bitez $f(x), g(x) \in K[x]$ *bi polinomio, non* $dg(g(x)) = m > 0$ *eta* $dg(f(x)) \geq dg(g(x))$ *diren. Orduan, existitzen dira* $q(x), r(x) \in K[x]$ *bi polinomio bakarrak, non* $f(x) = g(x)q(x) + r(x)$ *den,* $dg(r(x)) < dg(g(x))$ *edo* $r(x) = 0$ *izanik.*

Froga 1.1. *Definitzen dugu ondoko* P *multzoa:* $P = \{f(x)-g(x)k(x) : k(x) \in K[x]\}$. *Nola* P *multzoa ez hutsa den, definitzen dugu* $r(x)$ *maila txikiena duen* P *multzoko elementu bat. Bereziki,* $r(x) = f(x)-g(x)q(x)$, $q(x) \in K[x]$ *polinomioren batetarako. Orduan,* $f(x) = g(x)q(x) + r(x)$, $q(x), r(x) \in K[x]$ *izanik. Ondoren, ikus dezagun* $dg(r(x)) < dg(g(x))$ *edo* $r(x) = 0$ *dela. Demagun* $r(x) \neq 0$ *dela eta dei diezaiogun* $dg(r(x)) = n \geq 0$. *Ikus dezagun* $n < m$ *dela. Absurdura eramanez, demagun* $n \geq m$ *edo* $n - m \geq 0$ *dela. Idatz dezagun* $r(x) = b_0 + b_1x + \cdots + b_nx^n$ *eta* $g(x) = a_0 + a_1x + \cdots + a_mx^m$.

Defini dezagun orain ondoko polinomioa,

$$h(x) = f(x) - g(x)q(x) - \frac{b_n}{a_m}x^{n-m}g(x) = r(x) - \frac{b_n}{a_m}x^{n-m}(a_0 + a_1x + \cdots + a_mx^m)$$

$$= b_0 + \cdots + b_nx^n - \frac{b_n}{a_m}x^{n-m}(a_0 + a_1x + \cdots + a_{m-1}x^{m-1}) - \frac{b_n}{a_m}x^{n-m}a_mx^m,$$

n *baino maila txikiagoa duen polinomioa izanik.*

Gainera, $h(x) = f(x) - g(x)(q(x) - \frac{b_n}{a_m}x^{n-m}) \in P$ *dago, eta hau ezinezkoa da,* $dg(r(x)) = n$ *maila txikiena duen polinomio hartu dugulako baldintza horiek betez. Beraz,* $n < m$.

Bestalde, demagun orain existitzen direla polinomioen bi bikote $(q_1(x), r_1(x))$ *eta* $(q_2(x), r_2(x))$ *non* $f(x) = g(x)q_1(x) + r_1(x), dg(r_1(x)) < dg(g(x))$ *edo* $r_1(x) = 0$, *eta* $f(x) = g(x)q_2(x) + r_2(x), dg(r_2(x)) < dg(g(x))$ *edo* $r_2(x) = 0$ *izanik. Orduan* $g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x)$ *dugu, eta alde bietan mailak hartuz ondokoa ondorioztatzen dugu:* $dg(g(x)) + dg(q_1(x) - q_2(x)) = dg(r_2(x) - r_1(x)) \leq$

max$(r_2(x), r_1(x)) < m$*, eta aldi berean, ezker aldeko maila* $\geq m + 0 = m$*. Ondorioz,* $q_1(x) - q_2(x) = 0$ *eta* $r_1(x) - r_2(x) = 0$*, hau da,* $q_1(x) = q_2(x)$ *eta* $r_1(x) = r_2(x)$*.*

Definizioa. *Izan bitez* $f(x), g(x) \in K[x]$ *bi polinomio.* $f(x)$ *polinomioak* $g(x)$ *polinomioa zatitzen duela, edo* $g(x)$ *polinomioaren zatitzailea dela esaten da, existitzen denean* $q(x) \in K[x]$ *non* $g(x) = f(x)q(x)$ *den. Aurreko adierazpen hori,* $f(x)|g(x)$ *edo* $f|g$ *bitartez adierazten da.*

Definizioa. *Izan bitez* $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[x]$ *polinomioa eta* $\alpha \in K$*.* α*-n,* $f(x)$ *polinomioaren balioa deitzen zaio,* $f(x)$ *polinomioan* x *aldagaia* α*-gatik ordezkatuz lortzen den* K*-ko elementuari, eta hori,* $f(\alpha)$ *bidez adierazten da. Bestalde,* $f(\alpha) = 0$ *denean,* α*,* $f(x)$*, polinomioaren erroa edo zeroa dela esaten da.*

Teorema. *Izan bitez* $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[x]$ *polinomioa eta* $\alpha \in K$*.* α*,* $f(x)$ *polinomioaren erroa da baldin eta soilik baldin* $(x - \alpha)$ *binomioak,* $f(x)$ *polinomioa zatitzen badu. Honez gain,* $f(x)$ *zati* $(x - \alpha)$ *polinomioen zatiketaren hondarra* $f(\alpha)$ *da.*

Froga 1.2. $\Longrightarrow$*) Demagun* α*,* $f(x)$ *polinomioaren erro bat dela. Orduan,* $dg(f(x)) \geq 1$*. Nola* $dg(x - \alpha) = 1$ *den,* $f(x)$ *eta* $(x - \alpha)$ *polinomioei zatiketa algoritmoa aplikatuz ondokoa dugu,* $f(x) = (x-\alpha)q(x)+r(x)$ *non* $dg(r(x)) < dg(x-\alpha)$ *edo* $r(x) = 0$ *den. Demagun orduan* $f(x) = (x - \alpha)q(x) + a_0$ *dela. Nola* $f(\alpha) = (\alpha - \alpha)q(\alpha) + a_0 = 0$ *den,* $a_0 = 0$ *edo* $r(x) = 0$ *dela ondorioztatzen da.*

$\Longleftarrow$*) Baldin eta* $(x - \alpha) \mid f(x)$ *bada, orduan* $f(x) = (x - \alpha)q(x)$ *eta ondorioz,* $f(\alpha) = (\alpha - \alpha)q(\alpha) = 0$ *da, hau da,* α*,* $f(x)$*-ren erro bat da.*

Teorema. *Izan bedi* $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[x]$ *polinomioa non* $dg(f(x)) = n$ *den. Orduan,* $f(x)$ *polinomioak* K *gorputzean, gehienez* n *erro ditu.*

Froga 1.3. *Froga* n *gaineko indukzioz egingo dugu. Baldin eta* $dg(f(x)) = 0$ *bada, orduan* $f(x)$*-k ez dauka errorik. Baldin eta* $dg(f(x)) = 1$ *bada, orduan* $f(x) = ax + b$ *eta* $x = -\frac{b}{a}$*,* $f(x)$*-ren erro bakarra da. Demagun orain* $dg(f(x)) = n > 1$ *dela, eta demagun teoremaren tesia egia dela* n *baino maila txikiagoa duten polinomio guztietarako. Orain, demagun* $f(x)$ *polinomioak gutxienez* $a \in K$ *erro bat duela. Kontrako kasuan, teorema jadanik frogatuta egongo litzateke. Orain* $f(x)$ *eta* $(x - a)$ *polinomioei zatiketa algoritmoa aplikatuz ondokoa dugu,* $f(x) = (x - a)q(x) + r(x)$ *non* $dg(r(x)) = 0 < dg(x - a)$ *edo* $r(x) = 0$ *diren. Nola* a*,* $f(x)$ *polinomioaren erro bat den, aurreko teoremagatik* $x - a \mid f(x)$ *dela dakigu, eta ondorioz* $r(x) = 0$*. Beraz,* $f(x) = (x - a)q(x)$ *dugu,* $q(x) \in K[x]$ *eta* $dg(q(x)) = n - 1$ *izanik. Beraz,* $q(x)$ *polinomioari hipotesi induktiboa aplikatuz, badakigu polinomio honek gehienez* $n - 1$ *erro dituela* K *gorputzean, eta nola* $f(x)$ *polinomioaren erroak* K *gorputzean,* a *eta* $q(x)$*-ren* K *gorputzeko erroak diren, orduan* $f(x)$ *polinomioak gehienez* $1 + (n - 1) = n$ *erro ditu* K *gorputzean.*

Adibidea. $f(x) = x^3 - 1 = (x-1)(x^2+x+1)$ *polinomioak erro bakarra du* $\mathbb{R}$ *gorputzean.*

2 Polinomio biren zatitzaile komunetatiko haundiena. Euclidesen Algoritmoa

Definizioa. *Izan bitez* $f(x), g(x) \in K[x] - \{0\}$ *bi polinomio. Polinomio bi hauen zatitzaile komunetatiko haundiena deitzen zaio ondoko baldintzak betetzen dituen* $d(x)$ *polinomio bati:*

(i) $d(x)|f(x)$ *eta* $d(x)|g(x)$

(ii) *Existituko balitz* $l(x) \in K[x]$ *non* $l(x)|f(x)$ *eta* $l(x)|g(x)$*, orduan* $l(x)|d(x)$

(iii) $d(x)$ *polinomio monikoa hartzen da.*

Gainera, $d(x) = zkh(f(x), g(x))$ *edo* $d(x) = zkh(f, g) = (f, g)$ *denotatzen da.*

Teorema. *Beti existitzen da hutsak ez diren* $f(x), g(x) \in K[x]$ *edozein bi polinomioen* $d(x)$ *zatitzaile komunetatiko haundiena, eta honelako beste bat* $d'(x)$*, existituko balitz, bi hauek proportzionalak dira. Gainera, Bezòut-en identitateren bidez, existitzen dira* $\alpha(x), \beta(x) \in K[x]$ *non* $zkh(f(x), g(x)) = d(x) = \alpha(x)f(x) + \beta(x)g(x)$ *den.*

Froga 2.1. *Definitzen dugu ondoko* P *multzoa:*

$P = \{\alpha(x)f(x) + \beta(x)g(x) \mid \alpha(x), \beta(x) \in K[x]\}$*. Ohartu* $\alpha(x) = 0$ *eta* $\beta(x) = 1$ *hartuta,* $0f(x) + 1g(x) = g(x) \in P$*; bestalde,* $\alpha(x) = 1$ *eta* $\beta(x) = 0$ *hartuta,* $1f(x)+0g(x) = f(x) \in P$*, eta* $\alpha(x) = 0$ *eta* $\beta(x) = 0$ *hartuta,* $0f(x)+0g(x) = 0 \in P$ *daudela.*

P *multzoan hutsak ez diren polinomioak existitzen direnez gero, horretatik maila txikiena duen polinomio bat aukeratzen dugu,* $d_0(x)$ *izenekoa (eta orokortasuna galdu gabe, suposa genezake* $d_0(x)$ *monikoa dela). Orduan,* $d_0(x)$ *polinomio honentzako existitzen dira* $\alpha_0(x), \beta_0(x) \in K[x]$ *zeinentzat,*

$$d_0(x) = \alpha_0(x)f(x) + \beta_0(x)g(x).$$

Froga dezagun $d_0(x) = zkh(f(x), g(x)) = (f, g)$ *dela.*

(i) Lehenengo eta behin ikus dezagun $d_0(x) \mid f(x)$ *dela. (Ondoren, modu berdinean ikus daiteke* $d_0(x) \mid g(x)$ *dela.)* $f(x)$ *eta* $d_0(x)$ *polinomioei zatiketa algoritmoa aplikatuz, existitzen dira* $q(x), r(x) \in K[x]$ *non*

$$f(x) = d_0(x)q(x) + r(x), dg(r(x)) < dg(d_0(x)) \text{ edo } r(x) = 0 \text{ izanik .}$$

Orain, suposatzen baldin badugu $r(x) \neq 0$ *dela, orduan*

$$r(x) = f(x) - (\alpha_0(x)f(x) + \beta_0(x)g(x))q(x) = f(x) - \alpha_0(x)f(x)q(x) - \beta_0(x)g(x)q(x)$$

$$= f(x)(1 - \alpha_0(x)q(x)) + g(x)(-\beta_0(x)q(x)) \in P,$$

eta hau ezinezkoa da, $dg(r(x)) < dg(d_0(x))$ *delako, eta kontutan harturik* $d_0(x)$*-ren definizioa. Beraz,* $r(x) = 0$ *da eta ondorioz,* $d_0(x) \mid f(x)$.

(ii) Demagun orain existitzen dela $l(x) \in K[x]$ *non* $l(x)|f(x)$ *eta* $l(x)|g(x)$ *diren. Ikus dezagun* $l(x)|d_0(x)$ *dela. Nola* $l(x)|f(x)$*, orduan* $l(x)|\alpha_0(x)f(x)$*, eta nola* $l(x)|g(x)$*, orduan* $l(x)|\beta_0(x)g(x)$ *dugu. Ondorioz,* $l(x) \mid \alpha_0(x)f(x) + \beta_0(x)g(x) = d_0(x)$*, nahi genuen bezala.*

(iii) Aukeratu dugu $d_0(x)$ *polinomio monikoa.*

Demagun existitzen dela beste $d'(x) \in K[x]$*,* $f(x)$ *eta* $g(x)$*-ren zatitzaile komunetako haundienaren propietate berdinak betetzen dituen polinomio bat. Orduan,* $d_0(x)$*-k (i) propietatea betetzeagatik,* $d_0(x) \mid f(x)$ *eta* $d_0(x) \mid g(x)$*. Bestalde,* $d'(x)$*-k (ii) propietatea betetzeagatik,* $d_0(x) \mid d'(x)$ *dugu. Analogoki,* $d'(x)$*-k (i) propietatea betetzeagatik,* $d'(x) \mid f(x)$ *eta* $d'(x) \mid g(x)$*. Orain,* $d_0(x)$*-k (ii) propietatea betetzeagatik,* $d'(x) \mid d_0(x)$ *dugu. Hau da,* $d'(x) = d_0(x)c_1(x)$ *eta* $d_0(x) = d'(x)c_2(x)$*,* $c_1(x), c_2(x) \in K[x]$ *izanik. Orduan,* $d'(x) = d'(x)c_2(x)c_1(x)$*, eta* $c_1(x) = k_0 \in K$ *eta* $c_2(x) = 1/k_0 \in K$ *izan behar dute. Azkenik,* $d'(x)$ *eta* $d_0(x)$ *biak monikoak direnez gero, derrigorrez,* $k_0 = 1 = 1/k_0$ *dugu, hau da,* $d'(x) = d_0(x)$.

Propietateak. (i) *Baldin eta* $f(x)|g(x)$ *bada, orduan* $zkh(f(x), g(x)) = f(x)$.

(ii) *Baldin eta* $f(x) = g(x)q(x) + r(x)$ *bada,* $dg(r(x)) < dg(g(x))$ *izanik, orduan* $zkh(f(x), g(x)) = zkh(g(x), r(x))$.

Froga 2.2. *(ii) atalaren froga. Deitu* $d(x) = zkh(f(x), g(x))$ *eta ikusi dezagun ere* $d(x) = zkh(g(x), r(x))$ *dela. Nola* $d(x) \mid g(x)$*, orduan* $d(x) \mid g(x)q(x)$*, eta nola baita ere* $d(x) \mid f(x)$*,* $d(x) \mid (f(x) - g(x)q(x)) = r(x)$ *ondorioztatzen da. Bereziki,* $d(x) \mid g(x)$ *eta* $d(x) \mid r(x)$*. Demagun orain existitzen dela* $l(x) \in K[x]$ *non* $l(x) \mid g(x)$ *eta* $l(x) \mid r(x)$ *diren. Orduan,* $l(x) \mid g(x)q(x)$ *eta* $l(x) \mid (g(x)q(x) + r(x))$*, hau da,* $l(x) \mid f(x)$*. Orain, nola* $l(x) \mid f(x)$ *eta* $l(x) \mid g(x)$*, eta nola* $d(x) = zkh(f(x), g(x))$*-k bigarren propietatea betetzen duen,* $l(x) \mid d(x)$ *dela ondorioztatzen da. Azkenik,* $d(x)$ *monikoa denez,* $d(x) = zkh(g(x), r(x))$ *dela ondorioztatzen da.*

Teorema. *Euklidesen Algoritmoa.*

Izan bitez $f(x), g(x) \in K[x] - \{0\}$*,* $dg(f(x)) \geq dg(g(x)) = m > 0$ *izanik, eta izan bitez* $c_1(x), c_2(x), \ldots, c_n(x), c_{n+1}(x) \in K[x]$ *eta* $r_1(x), r_2(x), \ldots, r_n(x) \in K[x] - \{0\}$*, ondoko baldintzak betetzen dituzten polinomioak,*

$$f(x) = c_1(x)g(x) + r_1(x), dg(r_1(x)) < dg(g(x))$$

$$g(x) = c_2(x)r_1(x) + r_2(x), dg(r_2(x)) < dg(r_1(x))$$
$$r_1(x) = c_3(x)r_2(x) + r_3(x), dg(r_3(x)) < dg(r_2(x))$$
$$\vdots$$
$$\vdots$$
$$r_{n-2}(x) = c_n(x)r_{n-1}(x) + r_n(x), dg(r_n(x)) < dg(r_{n-1}(x))$$
$$r_{n-1}(x) = c_{n+1}(x)r_n(x) + r_{n+1}(x) = c_{n+1}(x)r_n(x) + 0 = c_{n+1}(x)r_n(x).$$

Orduan, behin eta berriz, arinago ikusitako (ii) propietatea aplikatuz, zkh$(f(x), g(x)) = (f(x), g(x)) = (g(x), r_1(x)) = (r_1(x), r_2(x)) = (r_2(x), r_3(x)) = \cdots = (r_{n-1}(x), r_n(x)) = (r_n(x), 0) = r_n(x)$ *dugu.*

Adibidea. *zkh*$(x^5-1, x^3+x-2) = (x^3+x-2, 2x^2+x-3) = (2x^2+x-3, \frac{11x}{4}-\frac{11}{4}) = \frac{11x}{4} - \frac{11}{4} \cong x - 1$

3 Polinomioen faktorizazioa

Definizioa. *Izan bedi* $f(x) \in K[x] - \{0\}$. *Definizioz* $f(x)$ *polinomioa* K *gorputzaren gainean irreduziblea edo laburtezina dela esaten da, existitzen ez badira* $g(x), h(x) \in K[x]$ *halakoak, non* $f(x) = g(x)h(x)$ *eta* $1 \leq dg(g(x)), dg(h(x)) < dg(f(x))$ *baldintzak betetzen dituzten. Kontrako kasuan,* $f(x)$ *polinomioa erreduziblea edo laburgarria* K *gorputz gainean dela esaten da.*

Propietateak. (i) *Edozein* K *gorputzean* 1*go mailako polinomio guztiak irreduzibleak dira.*

(ii) *Baldin eta* $f(x) \in K[x]$ *irreduziblea bada,* $dg(f(x)) \geq 2$ *izanik, orduan* $f(x)$*-k ez du zerorik* K *gorputzean.*

(iii) *Ez edukitzeak zerorik* K *gorputzean, ez du derrigortzen* $f(x)$ *polinomioa irreduziblea izatera. Kontsideratu adibidez,* $f(x) = (x^2+1)^2 = (x^2+1)(x^2+1)$ *polinomioa, eta ohartu ez duela errorik* $\mathbb{R}$*-n. Aurreko atalaren alderantzizkoa bakarrik betetzen da,* $dg(f(x)) = 2$ *edo* 3 *denean. (Frogapena ariketa bezala uzten dugu.)*

Teorema. *Izan bedi* $f(x) \in K[x]$ *polinomio ez konstantea. Orduan, existitzen dira* $f_1(x), \ldots, f_t(x) \in K[x]$ *polinomio irreduzibleak, non* $f(x) = f_1(x) \ldots f_t(x)$ *den. Gainera,* $f(x)$*-ren beste faktorizazio bat existituko balitz, hau da,* $f(x) = g_1(x) \ldots g_s(x)$ *balitz, non* $g_1(x), \ldots, g_s(x) \in K[x]$ *polinomio irreduzibleak diren, orduan* $s = t$ *da, eta ordena eta proportziozko konstanteak salbu, edozein* i *baliorako,* $f_i(x) = g_i(x)$ *betetzen da.*

Definizioa. *Izan bedi $f(x) \in K[x]$ polinomio ez konstantea. Orduan $f(x)$, lehenengo mailako $K[x]$-ko polinomioen biderketa bezala faktorizatzen denean, $f(x)$, $K[x]$ eraztunean guztiz zatitzen dela esaten da.*

Definizioa. *Izan bitez $f(x) \in K[x]$ polinomioa eta $\alpha \in K$, $f(x)$-ren erroa. Demagun existitzen dela $m \in \mathbb{N}$, non $(x-\alpha)^m | f(x)$ den, baina $(x-\alpha)^{m+1}$ polinomioak ez duelarik $f(x)$ zatitzen. Orduan, definizioz α erroaren anizkoiztasuna m dela esaten da. Gainera, $m = 1$ denean, α erro bakuna deitzen da, eta $m > 1$ denean, α erro anizkoitza dela esaten da.*

Definizioa. *Izan bedi $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in K[x]$ polinomioa. Definizioz, $f(x)$ polinomioaren, polinomio deribatua deitzen diogu ondoko adierazpenari: $f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$. Modu berdinean definitzen dira beste orden bateko polinomio deribatuak.*

Teorema. *Izan bitez $f(x) \in K[x]$ polinomioa eta $\alpha \in K$, $f(x)$-ren erro bat. $K[x]$ eraztunean, $f(x)$ polinomioarekiko α erroaren anizkoiztasuna m da baldin eta soilik baldin $f(\alpha) = f'(\alpha) = \ldots = f^{(m-1)'}(\alpha) = 0$ eta $f^{(m)'}(\alpha) \neq 0$ betetzen bada.*

Froga 3.1. *Ariketa bezala uzten dugu.*

4 Irreduzibilitateko irizpideak

Proposizioa. *Proposizio honetan polinomio bat irreduziblea den ala ez jakiteko irizpide batzuk aztertuko edo enuntziatuko ditugu. Izan bedi $f(x) \in K[x]$.*

(i) *Izan bedi $f(x) \in K[x]$ eta demagun $dg(f(x)) = 2$ edo 3 dela. Orduan, $f(x)$, K gainean irreduziblea da baldin eta soilik baldin $f(x)$ polinomioak ez baditu errorik K-n.*

Arinago aipatutako irizpide bat da.

Adibidez, $x^2 + 1$ laburtezina da $\mathbb{R}$ gainean.

(ii) *Izan bedi $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ eta demagun $dg(f(x)) \geq 2$ dela. Orduan, $\mathbb{Q}$ gorputzaren gainean $f(x)$ polinomioaren erroren bat egotekotan, erro hori $\frac{r}{s}$ motatakoa da, non $r \mid a_0, s \mid a_n$, $r, s \in \mathbb{Z}$ eta $zkh(r,s) = 1$ diren. (Irizpide honen froga ariketa bezala uzten da.)*

Ondorioz, $f(x) = 2x^3 - x^2 + 8x + 1 \in \mathbb{Z}[x]$ polinomioak erro arrazional bat izatekotan, hori, $1, -1, 1/2$ eta $-1/2$ izan daiteke, eta nola $f(1) \neq 0$, $f(-1) \neq 0, f(1/2) \neq 0, f(-1/2) \neq 0$ diren, $f(x)$-k ez duela erro arrazionalik ondoriztatzen da.

(iii) Gauss-en Lema.

Izan bedi $f(x) \in \mathbb{Z}[x]$. *Orduan* $\mathbb{Q}[x]$ *eraztunean* $f(x)$ *polinomioa,* $g(x)$ *eta* $h(x) \in \mathbb{Q}[x]$ *polinomioen biderketa gisa adieraz daiteke,* $1 \leq dg(g(x)), dg(h(x)) < dg(f(x))$ *izanik, baldin eta soilik baldin* $\mathbb{Z}[x]$ *multzoan,* $f(x)$ *polinomioa aurreko polinomio biren maila berdineko* $\mathbb{Z}[x]$*-ko bi polinomioen biderketa bezala adierazten bada.*

Adibidez, $f(x) = x^4 - 2x^2 + 8x + 1 \in \mathbb{Z}[x]$ *polinomioak ez du onartzen erro arrazionalik, eta* $\mathbb{Z}[x]$*-ko bigarren mailako bi polinomioen deskonposaketa onartuko balu,* $f(x) = (x^2 + ax + b)(x^2 + cx + d)$ *izango litzateke, ondoko baldintzak betez,*

$$bd = 1, bc + da = 8, d + b + ac = -2 \text{ eta } a + c = 0.$$

Nola aurreko sistema bateraezina den, $f(x)$*,* $\mathbb{Q}$ *gorputz gainean laburtezina edo irreduziblea dela ondorioztatzen da.*

(iv) Einseinstein-en iripizde orokortua

Izan bitez $p \in \mathbb{N}$ *(zenbaki lehena) eta* $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$. *Demagun,*

(a) $p \mid a_0, p \mid a_1, \ldots, p \mid a_{r-1}$*, non* $1 \leq r \leq n$ *den,*

(b) $p^2 \nmid a_0$*,*

(c) $p \nmid a_r$*.*

Orduan, $f(x)$ *polinomioak* $\mathbb{Z}[x]$ *eraztunean* r *edo* r *baino maila haundiagoko faktore irreduzible bat onartzen du. Bereziki,* $r = n$ *denean,* $f(x)$ *irreduziblea da* $\mathbb{Q}[x]$ *gainean.*

Har dezagun $f(x) = x^6 - 25x^5 + 3x^2 + 12 \in \mathbb{Z}[x]$ *polinomioa, eta* $p = 3$ *zenbaki lehena ondoko baldintzak betetzen dituena,*

(a) $3 \mid 12, 3 \mid 0, 3 \mid 3, 3 \mid 0, 3 \mid 0$*,*

(b) $9 \nmid 12$

(c) $3 \nmid -25$*.*

Beraz, $f(x)$ *polinomioak onartzen du* $\mathbb{Z}[x]$ *multzoan* 5 *edo* 6 *mailako faktore irreduzible bat. Bestalde,* 5 *mailako faktore irreduzible bat onartuko balu, orduan* $f(x)$ *polinomioak erroren bat izango luke* $\mathbb{Q}$*-n, eta badakigu froga daitekeela* $f(x)$*-k ez duela erro arrazionalik. Ondorioz,* $f(x)$*-k* 6 *mailako faktore irreduzible bat onartzen du, hau da,* $f(x)$ *irreduzible da* $\mathbb{Q}$ *gainean.*

5 Batugai soiletako zatikien deskonposizioa

Teorema. *Izan bitez $f(x), g(x) \in K[x]$ halakoak, non $g(x)$ faktorizatu egiten den elkarrekiko lehenak diren faktore bitan: $g(x) = p(x)q(x), (p(x), q(x)) = 1$, eta demagun $dg(f(x)) \geq dg(g(x))$ dela. Orduan, $f(x)/g(x)$ zatikia modu bakar batez adieraz daiteke ondoko eran,*

$$\frac{f(x)}{g(x)} = h(x) + \frac{u(x)}{q(x)} + \frac{v(x)}{p(x)},$$

$h(x), u(x), v(x) \in K[x], dg(u(x)) < dg(q(x)), dg(v(x)) < dg(p(x))$.

Froga 5.1. *Froga dezagun badagoela horrelako adierazpena. Hasteko, zatiketa euklidearra erabiliz, badaude $h(x), r(x) \in K[x]$ polinomioak, non $f(x) = h(x)g(x) + r(x)$, eta $dg(r(x)) < dg(g(x))$ diren. Bereziki, $\frac{f(x)}{g(x)} = h(x) + \frac{r(x)}{g(x)}$.*

Orain, $zkh(p(x), q(x)) = 1$ denez, Bezòuten identitateagatik, existitzen dira $\rho(x), \phi(x) \in K[x]$ polinomioak non $\rho(x)p(x) + \phi(x)q(x) = 1$ den. Beraz, aurreko adierazpena $r(x)$-gatik biderkatuz, $r(x)\rho(x)p(x) + r(x)\phi(x)q(x) = r(x)$ dugu. Orain, aplika diezaiogun Euclidesen algoritmoa $r(x)\rho(x)$ eta $q(x)$ polinomioei.

Orduan, $r(x)\rho(x) = \alpha(x)q(x) + u(x)$, non $dg(u(x)) < dg(q(x))$ eta $\alpha(x), u(x) \in K[x]$ diren.

Orain, $(\alpha(x)q(x)+u(x))p(x)+r(x)\phi(x)q(x) = u(x)p(x)+(\alpha(x)p(x)+r(x)\phi(x))q(x) = r(x)$ dugu, eta hemendik $v(x) = \alpha(x)p(x)+r(x)\phi(x)$ definituz, $u(x)p(x)+v(x)q(x) = r(x)$ lortzen dugu. Ikus dezagun ondoren, $dg(v(x)) < dg(p(x))$ dela, eta ondoren ohartu dena frogatuta dugula.

Izan ere,

$$dg(v(x)q(x)) = dg(r(x) - u(x)p(x)) \leq max(dg(r(x)), dg(u(x)p(x)))$$

$$< dg(q(x)p(x)) = dg(g(x)).$$

Ohartu aurreko desberdintzan, $dg(u(x)) < dg(q(x))$, $g(x) = p(x)q(x)$ eta $dg(r(x)) < dg(g(x))$ baldintzak erabili izan ditugula.

Orain, bakartasuna frogatzeko, demagun horrelako bigarren adierazpen bat dugula. Lehenengo kasuan egin ditugun eraikuntzak funtsean bakarrak direnez, horrelako adierazpena bakarra da. Bestela, horrelako biren diferentziak hartuta, aski da frogatzea, 0 polinomioaren adierazpen bakarra, $h(x) = u(x) = v(x) = 0$ polinomioen bitartez lortzen dela.

Korolarioa. *Izan bitez $f(x), g(x) \in K[x]$ halakoak, non $g(x) \neq 0$ den. Izan bedi $g(x) = p_1(x)^{e_1} \cdots p_t(x)^{e_t}$, $g(x)$ polinomioaren faktore irreduzible desberdinetako faktorizazioa. Orduan $f(x)/g(x)$ zatikia modu bakar batez adieraz daiteke era honetan,*

$$\frac{f(x)}{g(x)} = h(x) + \frac{u_{11}(x)}{p_1(x)} + \cdots + \frac{u_{1e_1}(x)}{p_1(x)^{e_1}} + \cdots + \frac{u_{t1}(x)}{p_t(x)} + \cdots + \frac{u_{te_t}(x)}{p_t(x)^{e_t}},$$

$$u_{ij} \in K[x], dg(u_{ij}(x)) < dg(p_i(x)).$$

Proposizioa. *Izan bitez* $u(x), p(x) \in K[x]$ *non* $p(x) \neq 0$ *den. Orduan,* $u(x)$ *modu bakar batez adieraz daiteke* $p(x)$ *oinarriarekiko ondoko eran,*

$$u(x) = u_0(x) + u_1(x)p(x) + u_2(x)p(x)^2 + \cdots + u_t(x)p(x)^t, dg(u_i(x)) < dg(p(x)).$$

Froga 5.2. *Ariketa bezala uzten da.*