1. Gaia 1

Polinomioen Eraztunak

[1]

Izan bedi $(E, +, \cdot)$ identitatedun eraztuna.

Definizioa 1.0.1. *Izan bitez x ezezaguna eta $a_0, ..., a_n \in E$. Orduan hurrengo expresioa E gaineko* **polinomioa** *deitzen da:*

$$a_0 + a_1 x + ... + a_n x^n$$

$a_0, ..., a_n$ *polinomioaren* **koefizienteak** *deitzen dira.*

Oharra 1.0.2. $x^0 = 1_E$ *eta* $a_k = 0_E$ *bada* $a_k x^k = 0$ *baldintzak onartzen baditugu orduan aurreko polinomioa batukariaren bidez idatzi ahal da:*

$$a_0 + a_1 x + ... + a_n x^n = \sum_{i=0}^{n} a_k x^k$$

Izan bedi $E[x] = \{E$ gaineko polinomioak $\}$. Gai honetan multzo honen propietate interesgarrienak ikusiko ditugu. Lehengo eragiketak definituko ditugu.

Definizioa 1.0.3. *Izan bitez $f(x) = \sum a_i x^i$ eta $g(x) = \sum b_i x^i$ E gaineko polinomioak. f eta g-ren* **batura**, *$f + g$ denotatuko duguna, ondorengo polinomioa da:*

$$f(x) + g(x) = \sum (a_i + b_i) x^i.$$

Erraz konprobatzen da $(E[x], +)$ talde abeldarra dela.

[1]OCW Proiektua. Txomin Ramirez eta M. Asun Garcia

[2]

Definizioa 1.0.4. *Izan bitez $f(x) = \sum a_i x^i$ eta $g(x) = \sum b_i x^i$ E gaineko polinomioak. f eta g-ren* **biderkadura**, *$f \cdot g$ denotatuko duguna, ondorengo polinomioa da:*

$$f(x) \cdot g(x) = \sum c_k x^k.$$

non $c_k = \sum_{i=0}^{k} a_i b_{k-i}$ den.

Erraz konprobatzen da biderketak propietate elkarkorra eta elementu neutroa dituela $E[x]$ multzoan. Gainera $(E[x], +, \cdot)$ propietate banakorrak betetzen ditu. Ondorioz, $(E[x], +, \cdot)$ identitatedun eraztuna da.

Definizioa 1.0.5. $(E[x], +, \cdot)$ *identitatedun eraztuna E gaineko* **polinomioen eraztuna** *deitzen da.*

Adibideak 1.0.6. $Z[x] \subseteq Q[x] \subseteq R[x] \subseteq C[x]$

Definizioa 1.0.7. *Izan bedi $f(x) = \sum a_i x^i \in E[x]$ polinomio ez-nulua. f-ren maila, $deg(f)$ denotatuko duguna, hurrengo balioa da:*

$$deg(f) = \max\{i \in (N) \quad | \quad a_i \neq 0\}$$

Ohartu $deg(f) = 0$ dela baldin eta soilik baldin $f(x) = a_0$ polinomio konstantea bada.

Oharra 1.0.8. *$f(x) = 0_E$ deneko kasuan $deg(f) = -\infty$ dela esaten da eta suposatzen da hurrengo propietateak betetzen direla: $-\infty < a$, $-\infty + b = b$ eta $-\infty \cdot d = -\infty$.*

Teorema 1.0.9. *Izan bitez $f(x) = \sum a_i x^i$ eta $g(x) = \sum b_i x^i$ E gaineko polinomioak. Orduan betetzen dira hurrengo baieztapenak:*

(i) $deg(f + g) \leq \max\{deg(f), deg(g)\}$ eta maila desberdinekoak badira orduan berdintza betetzen da.

(ii) $deg(f \cdot g) \leq deg(f) + deg(g)$.

Frogapena 1.0.10. *Bietako bat polinomio nulua bada orduan, argi eta garbi, bi baieztapenak betetzen dira. Demagun biak direla polinomio ez-nuluak: $f(x) = \sum_{i=0}^{n} a_i x^i, a_n \neq 0_E$ eta $g(x) = \sum_{i=0}^{m} b_i x^i, b_m \neq 0_E$.*

(i) Hiru kasu desberdinduko ditugu:

[2] OCW Proiektua. Txomin Ramirez eta M. Asun Garcia

[3]

1.- $n < m$ *bada* $f(x) + g(x) = \sum_{i=0}^{n}(a_i + b_i)x^i + \sum i = n + 1^m b_i x^i$ *denez* $deg(f + g) = m$ *eta* $\max\{deg(f), deg(g)\} = m$ *da, beraz berdintza betetzen da.*

2.- $m < n$ *bada* $f(x) + g(x) = \sum_{i=0}^{m}(a_i + b_i)x^i + \sum i = m + 1^n a_i x^i$ *denez* $deg(f + g) = n$ *eta* $\max\{deg(f), deg(g)\} = n$ *da, beraz berdintza betetzen da.*

3.- $m = n$ *bada orduan* $f(x) + g(x) = \sum_{i=0}^{n}(a_i + b_i)x^i$ *eta* $a_n, b_n \not{0}_E$ *izanik ezin dugu zihurtatu* $a_n + b_n$ *ere desberdin* 0_E *izango denik. Beraz,* $deg(f + g) \leq n$ *eta* $\max\{deg(f), deg(g)\} = n$*. Honekin bukatzen dugu lehenengo atalaren frogapena.*

(ii) $f(x) \cdot g(x) = (a_0 + a_1x + ... + a_nx^n) \cdot (b_0 + b_1x + ... + b_mx^m) = a_0b_o + ... + a_nb_mx^{n+m}$ *denez nahiz eta* $a_n, b_n \not{0}_E$ *izan ezin dugu, eraztun batean,* a_nb_m *ere* 0_E*-ren desberdina izango denik.*

Oharra 1.0.11. *$E = K$ gorputza bada orduan erraz frogatzen da $a_n, b_n \not{0}_K$ izanik a_nb_m ere 0_K-ren desberdina izango dela. Beraz, $E = K$ gorputza bada orduan aurreko teoremako bigarren formulan* **berdintza** *betetzen da.*

Definizioa 1.0.12. *Izan bedi $f(x) = a_0 + a_1x + ... + a_nx^n$ E gaineko polinomioa maila n izanik. Orduan $a_n \neq 0_E$ f-ren* **koefiziente zuzendaria** *deitzen da. Koefiziente zuzendaria 1_E bada orduan f* **polinomio monikoa** *dela esaten da.*

Hemendik aurrera $E = K$ gorputza dela suposatuko dugu.

Teorema 1.0.13 (Zatiketaren Algoritmoa K [x]**.** *Eraztunean] Izan bitez $f(x), g(x) \in K[x]$, $g(x)$ polinomio ez-nulua izanik. Orduan $\exists! q(x), r(x) \in K[x]$ non:*

$$f(x) = g(x)q(x) + r(x), deg(r) < deg(g) \text{ izanik }.$$

Frogapena 1.0.14. *1.- Existentzia. Bi kasu bereiztuko ditugu:*

(i) $deg(f) < deg(g)$ bada orduan $f(x) = g(x) \cdot 0_K + f(x)$ eta aurkitu ditugu $q(x) = 0_K$ eta $r(x) = f(x)$ polinomioak.

(ii) Demagun $n = deg(f) \geq deg(g) = m$. Orduan n gaineko indukzioa erabiliko dugu. Horretarako, $f(x) = \sum_{i=0}^{n} a_ix^i, a_n \neq 0_K$ eta $g(x) = \sum_{i=0}^{m} b_ix^i, b_m \neq 0_K$ badira, hurrengo eragiketa egiterakoan $f(x) - a_n(b_m)^{-1}x^{n-m}g(x) = f_1(x)$ polinomioa lortuko dugu, bere maila f-ren maila baino txikiagoa izanik. Beraz $deg(f_1) < deg(g)$ betetzen bada frogapena amaitu dugu $f(x) = a_n(b_m)^{-1}x^{n-m}g(x) + f_1(x)$ delako, beste kasuan, indukzioa aplikatuz $f_1(x)$ polinomioarentzat aurkitu ahal dira $q_1(x), r_1(x) \in K[x]$ non $f_1(x) = g(x)q_1(x) + r_1(x)$ den $deg(r_1) <$

[3]OCW Proiektua. Txomin Ramirez eta M. Asun Garcia

[4]

$< deg(g)$ *betetzen delarik. Ondorioz,* $f(x) = (a_n(b_m)^{-1}x^{n-m} + q_1(x))g(x) + r_1(x)$ *frogapena amaitzen delarik.*

2.- Bakartasuna. Demagun, alde batetik, $q_1(x)$ *eta* $r_1(x)$ *polinomioak existitzen direla non:*

$$f(x) = g(x)q_1(x) + r_1(x), deg(r_1) < deg(g).$$

Eta bestetik, existitzen direla $q_2(x)$ *eta* $r_2(x)$ *polinomioak non:*

$$f(x) = g(x)q_2(x) + r_2(x), deg(r_2) < deg(g).$$

Orduan $g(x)q_1(x)+r_1(x) = f(x) = g(x)q_2(x)+r_2(x)$ *betetzen denez* $g(x)(q_1(x)-q_2(x)) = r_2(x) - r_1(x)$ *beteko da. Orain mailak hartuz,* $deg(r_2 - r_1) \geq deg(g)$*. Baina, bestalde,* $deg(r_2 - r_1) \leq \max\{deg(r_2), deg(r_1\} < deg(g)$ *ere betetzen da. Aurrekoarekin konparatuz, aukera bakarra* $r_2(x) = r_1(x)$ *betetzea da eta orduan* $q_1(x) = q_2(x)$ *ere bete beharko da.*

Definizioa 1.0.15. *Izan bitez* $f(x), g(x) \in K[x]$*.* g*-k* f **zatitzen** *duela esango dugu baldin eta existitzen bada* $q(x) \in K[x]$ *polinomioa non* $f(x) = g(x)q(x)$ *betetzen den, hau da* $f(x)$ *eta* $g(x)$*-ren arteko zatiketaren hondarra* 0_K *bada. Kasu honetan,* $f(x)$ $g(x)$*-ren multiploa dela esaten da ere.*

Definizioa 1.0.16. *Izan bitez* $f(x) \in K[x]$ *eta* $\alpha \in K$*.* α f*-ren* **erroa** *dela esaten da* $f(\alpha) = 0_K$ *bada.*

Adibideak 1.0.17. x^2+1 *polinomioak ez du errorik* Q*-n ezta* R*-n ere. Baina* C*-n bi erro dauzka:* $i, -i$*.*

Teorema 1.0.18. *Izan bitez* $f(x) \in K[x]$ *eta* $\alpha \in K$*. Orduan hurrengo baliokidetasuna betetzen da:*

$$\alpha \ f\text{-ren erroa da} \ \Leftrightarrow (x-\alpha)/f(x)$$

Frogapena 1.0.19. *1.-* $\Leftarrow$*. Demagun* α f*-ren erroa dela. Orduan,* $f(x)$ (x_α)*-rekin zatituz:*

$$f(x) = (x-\alpha)q(x) + r(x), deg(r) < deg(x-\alpha) = 1$$

Beraz $r(x) = \lambda$ *konstantea da. Eta, hipotesia erabiliz,* $0_K = f(\alpha) = (\alpha - \alpha)q(\alpha) + \lambda$ *lortzen dugu. Hau da,* $(x-\alpha)/f(x)$*.*

2.- $\Rightarrow$*. Demaguna* $(x-\alpha)/f(x)$ *betetzen dela. Orduan existitzen da* $q(x) \in K[x]$ *non* $f(x) = (x-\alpha)q(x)$ *den. Beraz* $f(\alpha) = (\alpha-\alpha)q(\alpha) = 0_K$*.*

[4]OCW Proiektua. Txomin Ramirez eta M. Asun Garcia

[5]

Teorema 1.0.20 (Aljebraren Oinarrizko Teorema). *Izan bedi $f(x) \in C[x]$ polinomio ez-konstantea. Orduan $f(x)$-ren erro guztiak C-n daude.*

Teorema 1.0.21. *Izan bedi $f(x) = a_0 + a_1 x + ... + a_n x^n \in Z[x]$ polinomioa. Orduan $f(x)$-ren erro arrazional, r/s, posibleak hauek dira:*

- *(i)* $(r, s) = 1$.
- *(ii)* r/a_0.
- *(iii)* s/a_n.

Frogapena 1.0.22. *r/s $f(x)$-ren erro arrazionala da baldin eta soilik baldin $f(r/s) = 0$ bada. Orduan:*

$$a_0 + a_1 r/s + a_2 (r/s)^2 + ... + a_n (r/s)^n = 0$$

Eragiketak eginez:

$$a_0 s^n + a_1 r s^{n-1} + a_2 r^2 s^{n-2} + ... + a_n r^n = 0$$

Alde batetik:

$$a_n r^n 0 = -s(a_0 s^{n-1} + a_1 r s^{n-2} + ... + a_{n-1} r^{n-1})$$

Orduan $s/a_n r^n$ baina $(r, s) = 1$ betetzen denez s/a_n.

Era berean:

$$a_0 s^n = -r(a_1 s^{n-1} + ... + a_n r^{n-1})$$

Orduan $r/a_0 s^n$ eta $(r, s) = 1$ denez r/a_0.

[5]OCW Proiektua. Txomin Ramirez eta M. Asun Garcia