Eranskina 1

Polinomioen Eraztunak

1.1 Definizioa

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

Definizioa 1.1.1. *Izan bitez x ezezaguna eta $a_0, ..., a_n \in E$. Orduan hurrengo expresioa E gaineko* **polinomioa** *deitzen da:*

$$a_0 + a_1x + ... + a_nx^n$$

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

Oharra 1.1.2. *$x^0 = 1_E$ eta $a_k = 0_E$ bada $a_kx^k = 0$ baldintzak onartzen baditugu orduan aurreko polinomioa batukariaren bidez idatzi ahal da:*

$$a_0 + a_1x + ... + a_nx^n = \sum_{i=0}^{n} a_kx^k$$

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

Definizioa 1.1.3. *Izan bitez $f(x) = \sum a_ix^i$ eta $g(x) = \sum b_ix^i$ 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.

Definizioa 1.1.4. *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 1.1.5. $(E[x],+,\cdot)$ *identitatedun eraztuna* E *gaineko* **polinomioen eraztuna** *deitzen da.*

Adibideak 1.1.6. $\mathbb{Z}[x]\subseteq\mathbb{Q}[x]\subseteq\mathbb{R}[x]\subseteq\mathbb{C}[x]$

1.2 Zatigarritasuna

Definizioa 1.2.1. *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:*

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

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

Oharra 1.2.2. $f(x)=0_E$ *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 1.2.3. *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) $deg(f\cdot g)\leq deg(f)+deg(g)$.

Oharra 1.2.4. *$E = K$ gorputza bada orduan erraz frogatzen da $a_n, b_n \not/ 0_K$ izanik $a_n b_m$ ere 0_K-ren desberdina izango dela. Beraz, $E = K$ gorputza bada orduan aurreko teoremako bigarren formulan* **berdintza** *betetzen da.*

Definizioa 1.2.5. *Izan bedi $f(x) = a_0 + a_1 x + ... + a_n x^n$ 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 1.2.6 (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:*

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

Definizioa 1.2.7. *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 1.2.8. *Izan bitez $f(x) \in K[x]$ eta $\alpha \in K$. α f-ren* **erroa** *dela esaten da $f(\alpha) = 0_K$ bada.*

Adibideak 1.2.9. *$x^2 + 1$ polinomioak ez du errorik $\mathbb{Q}$-n ezta $\mathbb{R}$-n ere. Baina $\mathbb{C}$-n bi erro dauzka: $i, -i$.*

Teorema 1.2.10. *Izan bitez $f(x) \in K[x]$ eta $\alpha \in K$. Orduan hurrengo baliokidetasuna betetzen da:*

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

Teorema 1.2.11 (Aljebraren Oinarrizko Teorema)**.** *Izan bedi $f(x) \in \mathbb{C}[x]$ polinomio ez-konstantea. Orduan $f(x)$-ren erro guztiak $\mathbb{C}$-n daude.*

Teorema 1.2.12. *Izan bedi $f(x) = a_0 + a_1 x + ... + a_n x^n \in \mathbb{Z}[x]$ polinomioa. Orduan $f(x)$-ren erro arrazional, r/s, posibleak hauek dira:*

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

1.3 Polinomio Irreduzibleak. Polinomioen Faktorizazioa

Definizioa 1.3.1. *Izan bedi $p(x) \in K[X]$ ez-konstantea. $p(x)$* `polinomio irreduziblea` *dela esaten da baldin eta bi polinomioen biderkadura bezala jartzerakoan aukera bakarra bietako bat konstantea izatea baldin bada.*

Polinomio irreduzibleak hurrengo propietatea betetzen dute.

Teorema 1.3.2. *Izan bitez $p(x), f(x), g(x) \in K[X]$. Demagun $p(x)$ irreduziblea dela eta $p(x)/f(x)g(x)$ orduan $p(x)/f(x)$ edo $p(x)/g(x)$.*

Hurrengo teoreman ikusiko dugu polinomioak irreduzibleen biderkadura moduan adierazi ahal direla.

Teorema 1.3.3 (Polinomioen Faktorizazioa)**.** *Izan bedi $f(x) \in K[X]$ ez-konstantea. Orduan existitzen dira $p_1(x), ..., p_n(x) \in K[X]$ polinomio irreduzibleak non:*

$$f(x) = p_1(x) \cdots p_n(x)$$

Gainera, adierazteko modua bakarra da polinomio irreduzibleen ordena eta konstanteak salbu.

Hurrengo ondorioa dugu.

Ondorioa 1.3.4. *Izan bedi $f(x) \in K[X]$ non $\deg(f) = m$ den. Orduan f-ren faktorizazioan gehienez m polinomio irreduzibleak agertu ahal dira.*

Azkenik, irreduzibilitate erizpide batzuk ikusiko ditugu:

Teorema 1.3.5. *Izan bedi $f(x) \in K[X]$ non $2 \leq \deg(f) \leq 3$ den. Orduan f irreduziblea da baldin eta soilik baldin f-k K gorputzean errorik ez badu.*

Teorema 1.3.6 (Gaussen Lema)**.** *Izan bedi $f(x) \in \mathbb{Z}[X]$. $f(x)$ $\mathbb{Q}[X]$ eraztunean r eta s mailako bi polinomioen biderkadura da baldin eta soilik baldin $f(x)$ $\mathbb{Z}[X]$ r eta s mailako bi polinomioen biderkadura bada.*

Teorema 1.3.7 (Eisensteinen Erizpide Orokortua)**.** *Izan bedi p zenbaki lehena eta $f(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[X]$ non $a_n \neq 0$ den. Demagun existitzen dela $r \in \{1, ..., n\}$ non:*

(i) p/a_i $i = 0, ..., r-1$.

(ii) $p^2 \not| a_0$.

(iii) $p \not| a_r$.

Orduan f-ren faktorizazioan agertuko da maila r edo handiagoa duen polinomio irreduziblea.

Teorema 1.3.8 (Erredukzioa m moduluarekiko)**.** *Izan bitez $f(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[X]$ eta $\overline{f}(x) = \overline{a_0} + \overline{a_1}x + ... + \overline{a_n}x^n \in \mathbb{Z}/m\mathbb{Z}[X]$. $\overline{f}(x)$ irreduziblea bada $\mathbb{Z}/m\mathbb{Z}[X]$ eraztunean orduan $f(x)$ irreduziblea da $\mathbb{Z}[X]$ eraztunean.*