Eranskina 3

Polinomio Irreduzibleak. Polinomioen Faktorizazioa

Definizioa 3.0.1. *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 3.0.2. *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 3.0.3 (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 3.0.4. *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 3.0.5. *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 3.0.6 (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 3.0.7 (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) $p^2 \nmid a_0$.

(iii) $p \nmid a_r$.

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

Teorema 3.0.8 (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.*