4

Faktorizazioa polinomioen eraztunetan

4.1. Gaussen lema eta haren ondorioak

Gai honetan, gure helburua da polinomioen irreduzibilitatea aztertzea eta idealak lehenak edo maximalak diren erabakitzeko metodoak garatzea, $A[X]$ bezalako polinomioen eraztunetan, A faktorizazio bakarreko domeinua izanik. Arduratuko garen beste problema bat izango da $A[X]$ ere faktorizazio bakarreko domeinua dela frogatzea. Ohartu kuestio horiek berak $A[X_1, \ldots, X_n]$ moduko eraztunetan ere aztertu ahal izango ditugula, $A[X_1, \ldots, X_n]$ beti ikus baitaiteke $B[X_i]$ moduan, $B = A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$ izanik (hau da, X_i indeterminatuari rol nagusia emanez, eta gainerako indeterminatuak konstatetzat hartuz). Askotan, A-ren tokian K gorputz bat jarriko dugu. Dena den, horrek ez digu uzten analisia $K[X]$-ren kasura murrizten. Izan ere, $n \geq 2$ bada, $K[X_1, \ldots, X_n]$ eraztuna $B[X_i]$ moduan jartzen dugunean, B ez da gorputza (baina bai faktorizazio bakarreko domeinua). Hala ere, proposatutako problemei erantzuteko, paper garrantzitsua jokatuko du A-ren zatikien gorputzak. Horri K deitzen badiogu, orduan ikusiko dugu $f \in A[X]$ polinomio bat irreduziblea den edo ez jakiteko nahikoa dugula $K[X]$-n lan egitea. Ez da beti gertatuko f $A[X]$-n irreduziblea dela baldin eta soilik baldin $K[X]$-n irreduziblea bada, baina lotura hertsia egongo da bi kasuen artean.

Polinomioen irreduzibilitateari dagokionez, oinarrizko emaitza batzuk ezagunak ditugu, $K[X]$ polinomioen eraztunetan balio dutenak, K *gorputza baldin bada*:

(P0) Ez da aztertu behar polinomio konstante bat irreduziblea den edo ez, bi aukera besterik ez baitago: 0 izatea edo unitatea izatea.
(P1) $\deg f = 1$ bada, f irreduziblea da $K[X]$-n.
(P2) $\deg f \geq 2$ bada eta f-k erro bat badu K-n, f ez da irreduziblea $K[X]$-n.
(P3) $\deg f = 2$ edo 3 bada eta f-k ez badu errorik K-n, f irreduziblea da $K[X]$-n.

Orain, A faktorizazio bakarreko domeinua bada, zein puntutaraino jarraitzen dute egiazkoak izaten propietate horiek $A[X]$ eraztunean?

Hasteko, (P0) propietateari dagokionez, azpimarratu behar dugu konstante bat irreduziblea izan daitekeela. Adibidez, $\mathbb{Z}[X]$-n 2 konstantea irreduziblea da: ez da

nulua, ez da unitatea, eta ezin da adierazi biderkadura gisa unitaterik erabili gabe. Oro har, emaitza hau dugu.

4.1. Proposizioa. *Izan bitez A integritate-domeinua eta $a \in A$. Orduan, a $A[X]$-n irreduziblea da baldin eta soilik baldin A-n irreduziblea bada.*

Froga. Alde batetik, 1.37 teorema kontuan hartuz, gauza bera da esatea a A-n ez-nulua eta ez-unitatea dela edo $A[X]$-n ez-nulua eta ez-unitatea dela. Beraz, nahikoa dugu baliokidetasun hau frogatzea: a unitaterik erabili gabe faktorizatzen da A-n baldin eta soilik baldin unitaterik erabili gabe faktorizatzen bada $A[X]$-n. Hori berehala ondorioztatzen da kontuan hartzen badugu beste propietate hau, A integritate-domeinua izateagatik betetzen dena (argudiatu polinomioen mailarekin): $a = fg$ faktorizatzen badugu, $f, g \in A[X]$ izanik, orduan $f, g \in A$ dira. □

Azter dezagun orain (P1) propietatea adibide batzuen bitartez.

4.2. Adibideak. 1) $f(X) = 2X+2$ ez da irreduziblea $\mathbb{Z}[X]$-n, lehenengo mailakoa den arren. Izan ere, $f(X) = 2(X + 1)$ dugu, eta ez 2 ez $X + 1$ ez dira unitateak $\mathbb{Z}[X]$-n. Jakina, faktorizazio horrek ez du gezurtatzen $f(X)$-ren irreduzibilitatea $\mathbb{Q}$-ren gainean, 2-a unitatea baita $\mathbb{Q}[X]$-n.

2) Izan bedi $f(X, Y) = XY + Y \in K[X, Y]$. Ikusten badugu $K[X, Y]$ eraztuna $K[Y][X]$ gisa, hau da, polinomioak X-rekiko bakarrik ikusiz, orduan f lehenengo mailakoa da, baina ez da irreduziblea. Izan ere, $f(X, Y) = Y(X + 1)$ dugu eta Y ez da unitatea $K[Y][X]$-n. Hala ere, $f(X, Y)$ irreduziblea da $K[Y][X]$-ren ordez $K(Y)[X]$ erabiltzen badugu. Kasu horretan, koefizienteak $K(Y)$ gorputzean ($K[Y]$-ren zatikien gorputza dena) hartzen ditugu, eta horretan Y unitatea da. Beraz, $f(X, Y) = Y(X + 1)$ faktorizazioa ez dugu kontuan hartu behar $K(Y)[X]$-ren kasuan, faktoreetako bat unitatea baita.

Aurreko adibideek erakusten duten bezala, (P1) propietatea ez da oro har betetzen A faktorizazio bakarreko domeinua bada. Gainera, K A-ren zatikien gorputza bada, orduan $f \in A[X]$ polinomio baten portaera irreduzibilitateari dagokionez desberdina izan daiteke $A[X]$ eta $K[X]$ eraztunetan. Garbi dago nondik datorren diferentzia hori: f-k A-n dagoen faktore konstante bat izan dezake, A-n unitatea ez dena, baina jakina K-n unitatea izango dena edonola ere.

Ikus dezagun orain zer gertatzen den (P2) propietatearekin. Demagun $f \in A[X]$ polinomioak a erroa duela A-n. Zatiketaren algoritmoa erabiltzen badugu $f(X)$ $X - a$-rekin zatitzeko, orduan $f(X) = q(X)(X - a) + r$ lortzen dugu, r konstantea izanik. Berdintza horretan $X = a$ ordezkapena eginez, $r = f(a) = 0$ lortzen dugu. Beraz, $f(X) = q(X)(X - a)$ dugu. Gainera, $\deg f \geq 2$ denez, q ezin da konstantea izan. Orain, A integritate-domeinua denez, 1.37 teorema aplika dezakegu, eta q ez da unitatea. Horren arabera, f polinomioa ez da irreduziblea $A[X]$-n. Laburbilduz, emaitza hau frogatu dugu.

4.3. Proposizioa. *Izan bitez A integritate-domeinua eta $f \in A[X]$. Orduan, f-k $a \in A$ erro bat badu, $X - a$ polinomioa f-ren faktore bat da $A[X]$-n, eta* $\deg f \geq 2$ *bada, f ez da irreduziblea $A[X]$-n.*

Egia esan, aurrerago frogatuko dugunez (ikusi 4.16 proposizioa), A faktorizazio-bakarreko domeinua bada, orduan f-k erro bat badu A-ren *zatikien gorputzean*, oraindik ere lehenengo mailako faktore bat lortuko dugu $A[X]$-n.

Aipa dezagun, azkenik, (P3) propietatea ere faltsua dela faktorizazio bakarreko domeinu baten gainean. Adibidez, $f(X) = 2X^2 + 2 = 2(X^2 + 1)$ ez da irreduziblea $\mathbb{Z}[X]$-n, nahiz eta bigarren mailakoa izan eta $\mathbb{Z}$-n errorik ez izan. Baina, (P3) propietateagatik, f irreduziblea da $\mathbb{Q}[X]$-n. Era berean, $f(X, Y) = YX^2 + Y = Y(X^2 + 1)$ ez da irreduziblea $\mathbb{R}[Y][X]$-n, $\mathbb{R}(Y)[X]$-n bada ere. Ohartu, X-rekiko polinomio gisa begiratuta, f-k ez duela errorik $\mathbb{R}(Y)$-n (eta, beraz, are gutxiago $\mathbb{R}[Y]$-n). Hori egiaztatzeko, X-ren ordez $\mathbb{R}(Y)$-ko elementu orokor bat jarri behar dugu, hau da, $g(Y)/h(Y)$ moduko zatiki bat, eta ikusi behar dugu emaitza ezin dela 0 izan. Baina

$$Y\left(\frac{g(Y)}{h(Y)}\right)^2 + Y = 0 \iff Y\left(\frac{g(Y)^2}{h(Y)^2} + 1\right) = 0 \iff g(Y)^2 + h(Y)^2 = 0$$

dugu, eta hori ezinezkoa da g-k eta h-k koefiziente errealak dituztelako eta $h \neq 0$ delako. Berriro ere, kontradibideak unitatea ez den konstante bat erabiliz eman ditugu. Beranduago ikusiko dugunez, hori da horrelako adibideak lortzeko modu bakarra. Hori dela eta, kontzeptu hau sartzen dugu.

4.4. Definizioa. Izan bitez A faktorizazio bakarreko domeinua eta $f \in A[X]$. Orduan, f *jatorrizkoa* dela esango dugu bere koefizienteen zatitzaile komunetako handiena 1 bada.

4.5. Oharrak. Izan bitez A faktorizazio bakarreko domeinua eta K A-ren zatikien gorputza.

1) Demagun $f \in A[X]$ polinomioa ez dela jatorrizkoa. Orduan, f-ren koefizienteen zatitzaile komunetako handiena d bada, $f = dg$ idatz dezakegu, eta $g \in A[X]$ jatorrizkoa da.

2) Demagun $f \in K[X]$ dela. Orduan, f-ren koefizienteen izendatzaileen multiplo komunetako txikienaz biderkatuz $g \in A[X]$ polinomio bat lortuko dugu. Aurreko oharrean bezala, $g = dh$ idatz dezakegu, $d \in A$ izanik eta $g \in A[X]$ jatorrizkoa izanik. Laburbilduz, $f = \frac{a}{b}\, g$ jar dezakegu, $a/b \in K$ izanik eta $g \in A[X]$ jatorrizkoa izanik.

3) Askotan erabiliko dugu propietate hau: $af = bg$ bada, $a, b \in A$ izanik, eta $f, g \in A[X]$ jatorrizkoak izanik, orduan $a \sim b$ dugula. Hori ikusteko, nahikoa da af-ren koefizienteen zatitzaile komunetako handiena eta bg-ren koefizienteena kalkulatzea, eta gogoratzea zenbaki berberen bi edozein zatitzaile komunetako handien elkartuak direla.

4.6. Adibideak. 1) Izan bedi $f(X) = 6X^3 + 10X^2 + 15 \in \mathbb{Z}[X]$. Orduan, f jatorrizkoa da.

2) Izan bedi $f(X) = 4X^3 + 2X^2 + 6 \in \mathbb{Z}[X]$. Orduan, f ez da jatorrizkoa, koefizienteen zatitzaile komunetako handiena 2 baita. Ohartu $f(X) = 2 \cdot (2X^3 + X^2 + 3)$ jar dezakegula, $g(X) = 2X^3 + X^2 + 3$ jatorrizkoa izanik.

3) Izan bedi $f(X) = \frac{2}{3}X^3 + \frac{4}{7}X + 2 \in \mathbb{Q}[X]$. Polinomio hori 21ez biderkatuz, $g(X) = 14X^3 + 12X + 42 \in \mathbb{Z}[X]$ polinomioa lortzen dugu, ez dena jatorrizkoa, koefizienteen zatitzaile komunetako handiena 2 baita. Beraz,

$$f(X) = \frac{2}{21}(7X^3 + 6X + 21)$$

dugu, eta $h(X) = 7X^3 + 6X + 21 \in \mathbb{Z}[X]$ jatorrizkoa da.

4) Izan bitez K gorputza eta $f(X,Y) = X + XY + X^2Y^2 \in K[X,Y]$. Orduan, $K[X,Y] = K[X][Y]$ jartzen dugunean, hau da, koefizienteen eraztuna $K[X]$ dela ulertzen dugunean (ohartu faktorizazio bakarreko domeinua dela), f ez da jatorrizkoa, $\operatorname{zkh}(X, X, X^2) = X$ baita. Hala ere, $K[X,Y] = K[Y][X]$ jarriz gero, orduan koefizienteak $Y + 1$ eta Y^2 dira, eta f jatorrizkoa da.

4.7. Lema (Gaussen Lema)**.** *Izan bitez A faktorizazio bakarreko domeinua eta $f, g \in A[X]$ jatorrizko polinomioak. Orduan, fg ere jatorrizkoa da.*

Froga. Absurdora eramanez, demagun $h = fg$ ez dela jatorrizkoa. Orduan, existitzen da $p \in A$ elementu irreduziblea, h-ren koefiziente guztiak zatitzen dituena. Beste alde batetik, f eta g jatorrizkoak izateagatik, p-k ez ditu f-ren eta g-ren koefiziente guztiak zatitzen. Idatzi $f(X) = \sum_{i\geq 0} a_i X^i$ eta $g(X) = \sum_{i\geq 0} b_i X^i$, eta aukeratu r eta s indize txikienak $p \nmid a_r$ eta $p \nmid b_s$ den moduan. Orduan, X^{r+s} berreturaren koefizientea h polinomioan

$$a_{r+s}b_0 + \cdots + a_{r+1}b_{s-1} + a_r b_s + a_{r-1}b_{s+1} + \cdots + a_0 b_{r+s}$$

da eta, esan dugunez, p-ren multiploa da. Ohartu $a_{r+s}b_0 + \cdots + a_{r+1}b_{s-1}$ p-ren multiploa dela, p-k $b_0, \ldots, b_{s-1}$ zatitzen dituelako; era berean, $a_{r-1}b_{s+1} + \cdots + a_0 b_{r+s}$ ere p-ren multiploa da. Ondorioz, $a_r b_s$ p-ren multiploa da. Orain, A faktorizazio bakarreko domeinua denez eta p irreduziblea denez, $p \mid a_r$ edo $p \mid b_s$ dugu. Hori r-ren eta s-ren aukeraketaren kontra doa. □

Nabaria da Gaussen Lemaren alderantzizkoa betetzen dela: fg biderkadura jatorrizkoa bada, orduan bai f bai g jatorrizkoak dira. (Polinomio horietako baten koefizienteek $d \in A$ faktore komuna badute, orduan d faktore komuna da fg biderkaduraren koefizienteetan.)

Jarraian Gaussen Lemaren ondorio garrantzitsu batzuk aterako ditugu. Hasteko, oso korolario interesgarria aurkezten dugu: $f \in A[X]$ jatorrizko polinomio bat $K[X]$-ko polinomioekin faktorizatzen bada, orduan polinomio horiek zatiki egoki batzuekin biderkatuz, f $A[X]$-n faktorizatzea lor dezakegu.

4.8. Korolarioa. *Izan bitez A faktorizazio bakarreko domeinua, K A-ren zatikien gorputza, eta $f \in A[X]$. Demagun $f = f_1 \dots f_r$ faktorizazioa dugula, f_i guztiak $K[X]$-n izanik. Orduan, existitzen dira $\lambda_i \in K$ non:*

(i) *$g_i = \lambda_i f_i$ polinomioak $A[X]$-n daude, $i = 1, \dots, r$ guztietarako.*
(ii) *$f = g_1 \dots g_r$.*

Froga. Badakigu, 4.5 oharretako 2) atalean ikusi dugun bezala, $f_i = \dfrac{a_i}{b_i} f_i^*$ idatz dezakegula, $a_i, b_i \in A$ izanik, eta $f_i^* \in A[X]$ jatorrizkoa izanik. Era berean, $f = ef^*$ jar dezakegu, $e \in A$ izanik, eta $f^* \in A[X]$ jatorrizkoa izanik. Beraz,

$$ef^* = f = f_1 \dots f_r = \frac{a_1}{b_1} f_1^* \dots \frac{a_r}{b_r} f_r^* \quad \Longrightarrow \quad b_1 \dots b_r e f^* = a_1 \dots a_r f_1^* \dots f_r^*.$$

Orain, f^* jatorrizkoa da eta, Gaussen Lemaren arabera, $f_1^* \dots f_r^*$ ere bai. Kontuan hartzen badugu 4.5 oharretako 3) atala, $b_1 \dots b_r e \sim a_1 \dots a_r$ dela ondorioztatzen dugu, hau da, existitzen dela $u \in A^\times$ non $a_1 \dots a_r = u b_1 \dots b_r e$ baita. Orduan,

$$f = \frac{a_1}{b_1} f_1^* \dots \frac{a_r}{b_r} f_r^* = f_1^* \dots f_{r-1}^* \cdot \frac{a_1 \dots a_r}{b_1 \dots b_r} f_r^* = f_1^* \dots f_{r-1}^* \cdot u e f_r^*$$

dugu, $f_1^*, \dots, f_{r-1}^*, ue f_r^* \in A[X]$ izanik. Beraz, $\lambda_i = b_i/a_i$ jartzen badugu $i = 1, \dots, r-1$ denean eta $\lambda_r = ueb_r/a_r$, korolarioa frogaturik gelditzen da. □

Egia esan, azken korolarioaren frogak informazio zehaztuagoa ematen du g_i polinomioei buruz: $i = 1, \dots, r-1$ denean, $g_i = f_i^*$ f_i-ren "jatorrizko osagaia" da. Emaitza hori eskura izatea interesatzen zaigu, $r = 2$ den kasuan.

4.9. Korolarioa. *Izan bitez A faktorizazio bakarreko domeinua, K A-ren zatikien gorputza, eta $f \in A[X]$. Demagun $g \in K[X]$ polinomioak f zatitzen duela $K[X]$-n, eta idatz dezagun $g = \dfrac{a}{b} g^*$, $a, b \in A$ izanik eta $g^* \in A[X]$ jatorrizkoa izanik. Orduan, g^* polinomioak f zatitzen du $A[X]$-n.*

Orain, erlazionatuko ditugu polinomio baten irreduzibilitatea faktorizazio bakarreko domeinu baten gainean eta bere zatikien gorputzaren gainean.

4.10. Teorema. *Izan bitez A faktorizazio bakarreko domeinua eta K A-ren zatikien gorputza. Orduan, $f \in A[X]$ polinomio* ez-konstantea *bada, baliokideak dira:*

(i) *f irreduziblea da $A[X]$-n.*
(ii) *f irreduziblea da $K[X]$-n eta jatorrizkoa da.*

Froga. (i) ⇒ (ii). Lehenengo eta behin, ikus dezagun f jatorrizkoa dela. Izan ere, f ez bada jatorrizkoa, orduan $f = dg$ dugu, $d \in A$ ez-unitatea izanik eta $g \in A[X]$ ez-konstantea izanik. Orain, 1.37 teoremaren arabera, d eta g ez dira $A[X]$-ren unitateak. Hori kontraesana, f irreduziblea baita $A[X]$-n.

Ikus dezagun orain f $K[X]$-n irreduziblea dela. Alde batetik, f ez da unitatea $K[X]$-n, ez baita konstantea. Absurdora eramanez, demagun $f = gh$ dugula, $g, h \in K[X]$ eta $\deg g, \deg h \geq 1$ izanik. Orain, 4.8 korolarioa erabiliz, $f = g^* h^*$ faktorizazio bat lortzen dugu, $g^*, h^* \in A[X]$ polinomioak g-ren eta h-ren multiploak

izanik, K-ren elementu egoki batzuekin biderkatuz. Bereziki, $\deg g^*, \deg h^* \geq 1$ dugu, eta g^* eta h^* ez dira unitateak $A[X]$-n, ez baitira konstanteak. Horrela, kontraesan bat lortu dugu, f irreduziblea baita $A[X]$-n.

(ii) $\Rightarrow$ (i). Demagun $f = gh$ dela, $g, h \in A[X]$ izanik, eta ikus dezagun g edo h unitateak direla $A[X]$-n. Alde batetik, $\deg g, \deg h \geq 1$ betetzen bada, orduan g eta h ez dira unitateak $K[X]$-n, eta $f = gh$ deskonposizioak kontraesango luke f-ren irreduzibilitatea $K[X]$-n. Beraz, g edo h polinomioetako bat konstantea da eta, f jatorrizkoa denez, konstante horrek A-n (eta, beraz, $A[X]$-n) unitatea izan behar du. □

Orain, gai honetako teorema nagusietako bat aurkezten dugu.

4.11. Teorema. *Izan bedi A faktorizazio bakarreko domeinua. Orduan, $A[X]$ ere faktorizazio bakarreko domeinua da.*

Froga. Izan bedi $f \in A[X]$ ez-nulua eta ez-unitatea, eta frogatu dezagun $A[X]$-ko irreduzibleen biderkadura gisa adieraz daitekeela. Baldin eta $f \in A$ bada, orduan A faktorizazio bakarreko domeinua izateagatik, f A-ko irreduzibleen biderkadura gisa jar dezakegu. Ohartu A-ko elementu horiek $A[X]$-n ere irreduzibleak direla, 4.1 proposizioaren arabera. Orain, demagun $\deg f \geq 1$ dela. Orduan, $f = f_1 \dots f_r$, $K[X]$-ko polinomio irreduzibleen biderkadura gisa jar dezakegu. Faktorizazio horri 4.8 korolarioa aplikatzen badiogu, orduan $f = g_1 \dots g_r$ idatz dezakegu, $g_i = \lambda_i f_i \in A[X]$ izanik $\lambda_i \in K$ batzuetarako. Orduan, f_i $K[X]$-n irreduziblea denez, g_i $K[X]$-n irreduziblea da eta, 4.10 teorema aplikatuz, $A[X]$-n ere irreduziblea da. Horrela, g $A[X]$-ko polinomio irreduzibleen biderkadura gisa adieraztea lortu dugu.

Orain, demagun

$$a_1 \dots a_q f_1 \dots f_r = b_1 \dots b_s g_1 \dots g_t \tag{4.1}$$

bi faktorizazio berdin ditugula $A[X]$-ko irreduzibleetan, $a_i, b_j \in A$ izanik eta $f_i, g_j \in A[X]$ ez-konstanteak izanik. Ohartu f_i eta g_j polinomioak jatorrizkoak direla, 4.10 teoremaren arabera. Gaussen Lema aplikatuz, $f_1 \dots f_r$ eta $g_1 \dots g_t$ biderkadurak ere jatorrizkoak dira eta, orduan, (4.1)-era itzulita,

$$a_1 \dots a_q \sim b_1 \dots b_s$$

dugu. Orain, A faktorizazio bakarreko domeinua denez, $q = s$ dugu, eta existitzen da $\pi \in S_q$ non $a_i \sim b_{\pi(i)}$ baita $i = 1, \dots, q$ guztietarako. Bestalde,

$$f_1 \dots f_r \sim g_1 \dots g_t$$

dugu. Orain, f_i eta g_j polinomioak irreduzibleak dira $K[X]$-n, $A[X]$-n irreduzibleak eta jatorrizkoak baitira. Beraz, $K[X]$ faktorizazio bakarreko domeinua denez, $r = t$ dugu eta existitzen dira $\lambda_1, \dots, \lambda_r \in K$ eta $\pi' \in S_r$ non $f_i = \lambda_i g_{\pi'(i)}$ baita. Baina, $f_i, g_{\pi'(i)} \in A[X]$ jatorrizkoak direnez, aukera bakarra $\lambda_i \in A^\times$ izatea da. Horrela, $f_i \sim g_{\pi'(i)}$ dugu $A[X]$-n, eta bukatu dugu frogatzen irreduzibleetako deskonposizioaren bakartasuna. □

4.12. Oharra. Frogatzeko $f \in A[X]$ edozein polinomio $A[X]$-ko irreduzibleen biderkadura gisa jar daitekeela, beste aukera bat hurrengoa da. Idatz dezagun $f = dg$ moduan, $d \in A$ izanik eta $g \in A[X]$ jatorrizkoa izanik. Orduan, A faktorizazio bakarreko domeinua izateagatik, d elementua A-ko irreduzibleen biderkadura gisa jar dezakegu, eta elementu horiek $A[X]$-n ere irreduzibleak dira. Beraz, nahikoa dugu g polinomio jatorrizkoa $A[X]$-ko irreduzibleen biderkadura gisa adieraztea. Horretarako, hartu

$$g = g_1 \dots g_r \tag{4.2}$$

faktorizazio bat, $g_i \in A[X]$ eta ez-unitateak izanik. Orduan, g jatorrizkoa denez, g_i faktore guztiek jatorrizkoak izan behar dute; horrez gain unitateak ez direnez, $\deg g_i \geq 1$ izango dugu $i = 1, \dots, r$ guztietarako. Ondorioz, r, (4.2)-ko faktoreen kopurua, gehienez jota $\deg g$ izango da. Hori dela eta, har dezakegu faktorizazio hori ahal den faktore kopuru handienarekin. Horrela egiten dugunean, garbi dago g_i guztiek irreduzibleak izan behar dutela: g_i-ren bat ez-unitateen biderkadura gisa jarri ahal izango balitz, orduan faktore gehiago dituen g-ren faktorizazio bat lortuko genuke.

Aurreko teorema behin eta berriz aplikatuz, korolario hau dugu.

4.13. Korolarioa. *Baldin eta A faktorizazio bakarreko domeinua bada, orduan $A[X_1, \dots, X_n]$ ere faktorizazio bakarreko domeinua da. Bereziki, K gorputza bada, orduan $K[X_1, \dots, X_n]$ faktorizazio bakarreko domeinua da.*

Ikus dezagun orain nola erabil daitekeen 4.10 teorema (P1) eta (P3) propietateak konpontzeko faktorizazio bakarreko domeinu baten gainean. Froga berehalakoa da.

4.14. Proposizioa. *Izan bitez A faktorizazio bakarreko domeinua eta $f \in A[X]$ jatorrizkoa. Orduan:*

(i) $\deg f = 1$ *bada, f irreduziblea da $A[X]$-n.*
(ii) $\deg f = 2$ *edo* 3 *bada eta f-k ez badu errorik A-ren zatikien gorputzean, orduan f irreduziblea da $A[X]$-n.*

4.15. Adibidea. Izan bitez K gorputza eta $f(X, Y) = X^3Y + X^2Y + 1 \in K[X, Y]$. Ikusten badugu $K[X, Y]$ eraztuna $K[X][Y]$ gisa, orduan $f(X, Y) = (X^3 + X^2)Y + 1$ lehenengo mailakoa da Y-rekiko. Horrez gain jatorrizkoa denez, f irreduziblea da $K[X, Y]$-n.

Oso inportantea da, aurreko korolarioaren (ii) atalean, f-k ez duela errorik izan behar *A-ren zatikien gorputzean*, eta ez bakarrik A-n. Adibidez, $f(X) = 4X^2 - 1 \in \mathbb{Z}[X]$ polinomioa jatorrizkoa da eta ez du errorik $\mathbb{Z}$-n, baina faktorizatu egiten da: $f(X) = (2X + 1)(2X - 1)$. Arazoa da ez duela errorik $\mathbb{Z}$-n, baina bai $\mathbb{Q}$-n. Antzeko adibide bat eman dezakegu bi indeterminaturekin. Jarri $f(X, Y) = Y^2X^2 - 1 \in K[Y][X]$, jatorrizkoa dena. Ohartu f-k, X-rekiko begiratuta, ez duela

errorik $K[Y]$-n; bestela, existituko litzateke $g(Y) \in K[Y]$ non $Y^2 g(Y)^2 = 1$ den, eta hori ezinezkoa da. Hala ere, $f(X,Y) = (YX+1)(YX-1)$ faktorizatu egiten da. Problema dator f-k $K(Y)$-n erroak dituelako, $\pm 1/Y$ alegia.

Beraz, A faktorizazio bakarreko domeinua bada eta $f \in A[X]$ polinomioak erro bat badu K zatikien gorputzean, orduan f $A[X]$-n faktorizatzen da. Badakigu, erroa $a \in A$ denean, $X - a$ faktorea dugula. Ikus dezagun zein den zehatz-mehatz faktorea erroa $a/b \in K$ bada.

4.16. Proposizioa. *Izan bitez A faktorizazio bakarreko domeinua, K A-ren zatikien gorputza, eta $f \in A[X]$. Baldin eta f-k $a/b \in K$ erro bat badu, eta a/b zatiki laburtezina bada, orduan $bX - a$ polinomioak f zatitzen du $A[X]$-n.*

Froga. Ezaguna da $X - a/b$ polinomioak f zatitzen duela $K[X]$ eraztunean. Orduan, $X - a/b = \dfrac{1}{b}(bX - a)$ dugu, eta $bX - a \in A[X]$ jatorrizkoa da, a/b zatikia laburtezina izateagatik. Orain, 4.9 korolarioa erabiliz, $bX - a$ polinomioak f zatitzen du $A[X]$-n. □

Esan bezala, $f \in A[X]$ polinomio baten irreduzibilitatea aztertzeko, interesatzen zaigu jakitea ea errorik duen A-ren zatikien gorputzean. Lan horretan, ondorengo emaitza lagungarria izango da. Ohartu ezaguna dela dagoeneko $\mathbb{Z}$-ren kasuan, "Ruffiniren erregelarekin" batera erabili ohi baita.

4.17. Teorema. *Izan bitez A faktorizazio bakarreko domeinua, K A-ren zatikien gorputza, eta $f \in A[X]$. Orduan:*

(i) *$a/b \in K$ f-ren erroa bada, zatiki hori laburtezina izanik, orduan a-k f-ren gai askea zatitzen du eta b-k, berriz, f-ren koefiziente nagusia zatitzen du.*

(ii) *f monikoa bada, orduan f-k K-n dituen erro guztiak A-n daude.*

Froga. (i) Jarri $f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$, $a_i \in K$ izanik $i = 0, \ldots, n$ guztietarako. Orduan, X-ren ordez a/b jartzen badugu eta izendatzaileak garbitzen baditugu,

$$a_n a^n + a_{n-1}a^{n-1}b + \cdots + a_1 a b^{n-1} + a_0 b^n = 0$$

lortzen dugu, a/b f-ren erroa izateagatik. Berdintza horretatik, $a_n a^n$ b-ren multiploa dela eta $a_0 b^n$ a-ren multiploa dela ondorioztatzen dugu. Orduan,

$$a \mid a_0 b^n \text{ eta } \operatorname{zkh}(a,b) = 1 \quad \Longrightarrow \quad a \mid a_0$$

dugu, 3.22 proposizioa erabiliz. Antzera lortzen da $b \mid a_n$ dela.

(ii) Emaitza hori (i) atalaren ondorio berehalakoa da. Izan ere, f monikoa bada, orduan $b \mid 1$ dugu eta, beraz, b A-ren unitatea da. Horrela, $a/b = ab^{-1} \in A$ dugu. □

4.18. Adibideak. Azken teoremako (i) atalak f polinomioaren K-ren gaineko balizko erroak mugatu egiten ditu. Adibidez, $f(X) = 4X^7 + X + 1 \in \mathbb{Z}[X]$ hartuz

gero, bere erro arrazional *posibleak* ± 1, $\pm 1/2$ eta $\pm 1/4$ dira. Horiekin proba eginez, ikusten dugu ez direla f-ren erroak eta, horrenbestez, baiezta dezakegu f-k ez duela erro arrazionalik. Argudio horrek berak erakusten du nola lor ditzakegun $f \in \mathbb{Z}[X]$ polinomio orokor baten erro *arrazional* guztiak. (Beste problema bat da erro konplexu guztiak ematea, ez dena oro har posible.)

Orain, 4.17 teorema 4.14 proposizioarekin batera erabil dezakegu polinomioen irreduzibilitatea aztertzeko.

4.19. Adibidea. Izan bedi $f(X) = 2X^3 + X - 1 \in \mathbb{Z}[X]$. Hirugarren mailakoa eta jatorrizkoa denez, $\mathbb{Z}[X]$-n (edo, gauza bera dena, $\mathbb{Q}[X]$-n) aztertu nahi badugu f-ren irreduzibilitatea, nahikoa da ikustea $\mathbb{Q}$-n errorik duen edo ez. Orain, 4.17 teoremaren arabera, $a/b \in \mathbb{Q}$ zatiki laburtezina f-ren erroa bada, orduan $a \mid -1$ eta $b \mid 2$ dugu. Horrenbestez, f-ren erro arrazional posibleak ± 1 eta $\pm 1/2$ dira. Balio horiek f-ren adierazpenean ordezkatuz, konturatzen gara horietatik bat ere ez dela f-ren erroa. Ondorioz, f irreduziblea da $\mathbb{Z}[X]$-n eta $\mathbb{Q}[X]$-n.

4.20. Korolarioa. *Izan bitez A faktorizazio bakarreko domeinua eta $f \in A[X]$* monikoa*, $\deg f = 2$ edo 3 izanik. Orduan, f-k ez badu errorik A-n, irreduziblea da $A[X]$-n.*

4.2. Irreduzibilitaterako irizpideak

Atal honetan emaitza batzuk emango ditugu, itxura berezia duten polinomio batzuen irreduzibilitatea frogatzeko balio dutenak (faktorizazio bakarreko domeinu baten gainean, edo horren zatikien gorputzaren gainean).

Hasteko, Eisensteinen irizpidea aurkeztuko dugu. Irizpide horren frogan, eta aurrerago emango dugun beste irizpide batean ere, garrantzitsuak izango dira polinomioen eraztunen arteko homomorfismo berezi batzuk. Horiek polinomioen koefizienteak ideal batekiko laburtuz lortzen dira. Zehazkiago, A eraztuna bada eta $\mathfrak{a}$ A-ren ideala bada, orduan

$$\begin{array}{rccc} \varphi & : & A[X] & \longrightarrow & A/\mathfrak{a}[X] \\ & & a_0 + a_1X + \cdots + a_nX^n & \longmapsto & \overline{a_0} + \overline{a_1}X + \cdots + \overline{a_n}X^n \end{array} \tag{4.3}$$

eraztun-homomorfismoa dugu. Homomorfismo horien ezaugarri berezi bat da $\deg f \geq \deg \varphi(f)$ betetzen dela $f \in A[X]$ guztietarako. Ohartu, edozein kasutan, ez dela oro har bi mailen arteko berdintza beteko, f-ren koefiziente nagusia $\overline{0}$ bihur baitaiteke $A/\mathfrak{a}$-n.

4.21. Teorema (Eisensteinen irizpidea)**.** *Izan bitez A faktorizazio bakarreko domeinua eta $f(X) = a_nX^n + \cdots + a_0 \in A[X]$. Demagun badagoela $p \in A$ elementu irreduziblea, baldintza hauek betetzen dituena:*

(i) $p \mid a_0$, $p^2 \nmid a_0$.

(ii) $p \mid a_1, \dots, p \mid a_{r-1}$, $p \nmid a_r$, *non* $r \leq n$ *baita.*

Orduan, $A[X]$*-ko* f*-ren faktorizazioan badago maila* r *edo handiagoa duen faktore irreduzible bat. Bereziki,* $r = n$ *bada eta* f *jatorrizkoa bada, orduan* f *irreduziblea da* $A[X]$*-n.*

Froga. Izan bedi $\mathfrak{p} = (p)$ A-ren ideala. Orduan, A faktorizazio bakarreko domeinua denez eta $p \in A$ irreduziblea denez, $\mathfrak{p}$ A-ren ideal lehena da. Beraz, $A/\mathfrak{p}$ integritate-domeinua da. Izan bedi $\varphi : A[X] \longrightarrow A/\mathfrak{p}[X]$ polinomioen koefizienteak $\mathfrak{p}$ moduluarekiko laburtuz lortzen den eraztun-homomorfismoa. Orduan,

$$\varphi(f) = \overline{a_n}X^n + \cdots + \overline{a_r}X^r + \overline{a_{r-1}}X^{r-1} + \cdots + \overline{a_0} = X^r(\overline{a_n}X^{n-r} + \cdots + \overline{a_r})$$

dugu, $\overline{a_0} = \cdots = \overline{a_{r-1}} = \overline{0}$ baita, $p \mid a_0, \dots, a_{r-1}$ izateagatik. Beraz, $X^r \mid \varphi(f)$ dugu. Gainera, $\overline{a}_r \neq \overline{0}$ da, $p \nmid a_r$ delako, eta ondorioz $\varphi(f) \neq \overline{0}$ dugu.

Izan bedi $f = f_1 \dots f_t$ f-ren faktorizazioa $A[X]$-ren irreduzibleetan. Orduan, $\varphi(f) = \varphi(f_1) \dots \varphi(f_t)$ dugu, eta

$$X^r \mid \varphi(f_1) \dots \varphi(f_t).$$

Orain, baieztatzen dugu ezin dela gertatu $X \mid \varphi(f_j)$ eta $X \mid \varphi(f_k)$ izatea, $j \neq k$ bi baliotarako. Izan ere, bestela balitz, horrek esan nahi luke p-k f_j-ren eta f_k-ren gai askeak zatitzen dituela. Baina f-ren gai askea f_i guztien gai askeen biderkadura denez, orduan $p^2 \mid a_0$ izango genuke, hipotesiaren kontra doana.

Beraz, $X^r \mid \varphi(f_1) \dots \varphi(f_t)$ dugu, baina X-k faktore horietako bat baino ezin du zatitu. Zatigarritasun-propietate horiek $A/\mathfrak{p}[X]$-n betetzen dira. Jakingo bagenu $A/\mathfrak{p}$ faktorizazio bakarreko domeinua dela, orduan $A/\mathfrak{p}[X]$ ere faktorizazio bakarreko domeinua litzateke, eta goiko baldintzek inplikatuko lukete badagoela $i \in \{1, \dots, t\}$ non $X^r \mid \varphi(f_i)$ baita. Baina $A/\mathfrak{p}$ zatidurari buruz dakigun guztia da integritate-domeinua dela, ez faktorizazio bakarreko domeinua denik. Hala ere, arazo horri konponbide erraza eman diezaiokegu: har dezagun $A/\mathfrak{p}$-ren zatikien gorputza, L, eta errepika dezagun aurreko argudioa $L[X]$-n lan eginez, $A/\mathfrak{p}[X]$-ren ordez. Orduan, modu berean $X^r \mid \varphi(f_i)$ lortzen dugu. Orain zatigarritasun-propietate hori $L[X]$-n betetzen da, eta ez $A/\mathfrak{p}[X]$-n, baina froga bukatzeko behar dugun argudioan ez du axola.

Izan ere, $\varphi(f) \neq \overline{0}$ denez, $\varphi(f_i) \neq \overline{0}$ dugu. Orduan, $X^r \mid \varphi(f_i)$ izateagatik $\deg \varphi(f_i) \geq r$ dela ondorioztatzen dugu. Hortik $\deg f_i \geq r$ lortzen dugu (gogoratu zein portaera duen polinomioen mailak φ bezalako homomorfismoetan), eta aurkitu dugu $A[X]$-ko f-ren faktorizazioan maila r edo handiago duen faktore irreduzible bat, nahi bezala. □

Eisensteinen irizpidea aplikatzean, kontuan izan ohar sinple hau: edozein elementuk 0 zatitzen duenez, konprobatzen dugunean p elementu irreduzibleak polinomioaren zein koefiziente zatitzen dituen, bakarrik erreparatu behar diegu 0 ez diren koefizienteei (hau da, polinomioa idaztean agertzen diren koefizienteei).

4.22. Adibideak. 1) Izan bedi $f(X) = X^4 + 2X^3 + 4X + 2 \in \mathbb{Z}[X]$. Eisensteinen irizpidea erabiltzen badugu, $p = 2$ hartuta, f $\mathbb{Z}[X]$-n irreduziblea dela ondorioztatzen dugu. Ez da gauza bera gertatzen $g(X) = 3X^5 + 6X^2 + 12X + 30$ polinomioarekin, nahiz eta $p = 2$ zenbaki lehenarekin Eisensteinen irizpidearen baldintza guztiak bete. Baiezta dezakegu g-k $\mathbb{Z}[X]$-n bosgarren mailako faktore irreduzible bat duela, baina horrek ez du esan nahi g $\mathbb{Z}[X]$-n irreduziblea denik, g ez baita jatorrizkoa. Izan ere, $g(X) = 3(X^5 + 2X^2 + 4X + 10)$ da g-ren faktorizazioa $\mathbb{Z}[X]$-n (ohartu bosgarren mailako faktorea dugula, Eisensteinen irizpideak ziurtatzen duen bezala). Bestalde, g irreduziblea da $\mathbb{Q}[X]$-n.

2) Izan bedi $f(X, Y) = X^5Y + X^5 + Y^5 + Y \in K[X, Y]$. Polinomio hori X-rekiko ikusten badugu, hau da, koefizienteak $K[Y]$-n hartuz, orduan $f(X, Y) = (Y + 1)X^5 + Y^5 + Y \in K[Y][X]$ idazten dugu. Eisensteinen irizpidea aplikatu nahi badugu, $Y^5 + Y$ gai askearen zatitzaile irreduzible bat behar dugu (irreduziblea $K[Y]$-n, jakina), karratura jasorik $Y^5 + Y$ zatitzen ez duena. Aukera bat Y indeterminatua bera hartzea da. Orduan, f-k $K[Y][X] = K[X, Y]$-n X-rekiko bosgarren mailakoa den faktore irreduzible bat duela ondorioztatzen dugu. Hori dela eta, f $K[X, Y]$-n irreduziblea den edo ez jakiteko, $K[Y][X]$-n jatorrizkoa den aztertu behar dugu. Horretarako, $\operatorname{zkh}(Y + 1, Y^5 + Y)$ kalkulatu behar dugu. Hori $Y + 1$ izango da $Y + 1$-ek $g(Y) = Y^5 + Y$ zatitzen badu, eta 1 bestela. Badakigunez, $Y + 1$-ek $g(Y)$ zatitzen du baldin eta soilik baldin $g(-1) = 0$ bada. Kasu honetan $g(-1) = -2$ denez,

$$\begin{cases} g(-1) = 0, & \operatorname{char} K = 2 \text{ bada;} \\ g(-1) \neq 0, & \operatorname{char} K \neq 2 \text{ bada.} \end{cases}$$

Ondorioz,

$$\operatorname{zkh}(Y + 1, Y^5 + Y) = \begin{cases} Y + 1, & \operatorname{char} K = 2 \text{ bada;} \\ 1, & \operatorname{char} K \neq 2 \text{ bada.} \end{cases}$$

Horrela, bi kasu hauek ditugu:

(i) $\operatorname{char} K \neq 2$ bada, f jatorrizkoa da $K[Y][X]$-n eta, hortaz, irreduziblea $K[X, Y]$-n.

(ii) $\operatorname{char} K = 2$ bada, orduan f ez da jatorrizkoa $K[Y][X]$-n eta, beraz, ez da irreduziblea $K[X, Y]$-n. Kasu honetan $Y^5 + Y = Y(Y^4 + 1) = Y(Y + 1)^4$ dugu eta honako hau da f-ren faktorizazioa $K[X, Y]$-ren irreduzibleetan:

$$f(X, Y) = (Y + 1)(X^5 + Y(Y + 1)^3).$$

3) Azter dezagun $f(X) = X^4 - X^3 + 2X + 2$ polinomioaren irreduzibilitatea $\mathbb{Z}[X]$-n. Eisensteinen irizpidea aplikatzen badugu $p = 2$ hartuta, badakigu f-k hirugarren mailako edo maila altuagoko faktore irreduzible bat duela $\mathbb{Z}[X]$-n. Bestalde, f jatorrizkoa denez, ez du faktore konstanterik (unitateez aparte). Beraz, bi aukera baino ez daude:

(i) $f(X)$ irreduziblea da $\mathbb{Z}[X]$-n.

(ii) $f(X) = g(X)h(X)$, non $g(X), h(X) \in \mathbb{Z}[X]$, $\deg g = 1$ eta $\deg h = 3$ baita.

Azken kasua beteko balitz, f-k $\mathbb{Q}$-n erro bat izango luke. Orain, 4.17 teoremaren arabera, f-k $\mathbb{Q}$-n izan ditzakeen erro bakarrak ± 1 eta ± 2 dira. Horiekin probatuz,

ikusten dugu ez direla f-ren erroak eta, horrenbestez, f $\mathbb{Z}[X]$-n irreduziblea dela ondorioztatzen dugu.

Beste batzuetan, $A[X]$-n irreduzibilitatea lortzeko, koefizienteak A-ren zatidura batera pasatzen ditugu, hurrengo teorema hau erabiliz.

4.23. Teorema (Koefizienteen laburketa ideal batekiko)**.** *Izan bitez A faktorizazio bakarreko domeinua, $\mathfrak{p}$ A-ren ideal lehena, eta $\varphi : A[X] \longrightarrow A/\mathfrak{p}[X]$ polinomioen koefizienteak $\mathfrak{p}$ moduluarekiko laburtzen dituen eraztun-homomorfismoa, (4.3)-n bezala. Demagun $f \in A[X]$ polinomioak bi baldintza hauek betetzen dituela:*

(i) *f jatorrizkoa da.*
(ii) *$\deg \varphi(f) = \deg f$ da.*

Orduan, $\varphi(f)$ irreduziblea bada $A/\mathfrak{p}[X]$-n, f irreduziblea da $A[X]$-n.

Froga. Absurdora eramanez, demagun $f = gh$ faktorizazioa dugula $A[X]$-n, g eta h ez-unitateak izanik. Orduan, f jatorrizkoa denez, g eta h ezin dira konstanteak izan, hau da, $\deg g, \deg h \geq 1$ dugu. Bestalde, φ aplikatuz, $\varphi(f) = \varphi(g)\varphi(h)$ dugu eta, orduan,

$$\deg \varphi(f) = \deg \varphi(g) + \deg \varphi(h) \leq \deg g + \deg h = \deg f.$$

Baina, hipotesiaren arabera $\deg \varphi(f) = \deg f$ denez, nahitaez $\deg \varphi(g) = \deg g$ eta $\deg \varphi(h) = \deg h$ dugu. Bereziki, $\varphi(g)$ eta $\varphi(h)$ ez dira konstanteak. Orain, $A/\mathfrak{p}$ integritate-domeinua izateagatik, $\varphi(g)$ eta $\varphi(h)$ ez dira unitateak $A/\mathfrak{p}[X]$ eraztunean. Horrela, $\varphi(f) = \varphi(g)\varphi(h)$ faktorizazioa ikusita, $\varphi(f)$ ez da irreduziblea $A/\mathfrak{p}[X]$-n. Kontraesan horrek teorema frogatzen du. □

Normalean, azken teorema $\mathfrak{m}$ ideal maximal batekin erabiliko dugu. Orduan, irreduzibilitatea $A[X]$-n aztertzeko, $A/\mathfrak{m}[X]$ eraztunera pasa gaitezke, eta kasu hori errazagoa izango da, $A/\mathfrak{m}$ gorputza baita.

4.24. Notazioa. Gehienetan, $\varphi(f)$ polinomioa adierazteko $\overline{f}$ idatziko dugu, notazio erraztearren. Ohartu $\overline{f}$ hori ikur bat besterik ez dela. Horretan, f-ren gaineko marrak koefizienteak laburtzen direla gogorarazten digu, eta ez du adierazten f-ren irudia hartzen ari garenik $A[X]$-ren zatidura batean. Izan ere, φ aplikazioa $A[X]$-tik $A/\mathfrak{p}[X]$-ra doa, eta koefizienteak dira zatidura batera pasatzen direnak, ez polinomioak. Beraz, arretaz ibili behar da $A[X]$-ko polinomio bat $f(X)$ moduan idazten dugunean; orduan, $\varphi(f(X))$ idazteko $\overline{f}(X)$ idatzi behar dugu, eta ez $\overline{f(X)}$.

Azken teoremaren baldintzak beharrezkoak dira, erraz ikus dezakegun bezala. Adibideak $A = \mathbb{Z}$ eta $\mathfrak{p} = 2\mathbb{Z}$ hartuz emango ditugu. Alde batetik, $f(X) = 3X + 3$ ez da irreduziblea $\mathbb{Z}[X]$-n, nahiz eta $\overline{f}(X) = X + \overline{1} \in \mathbb{Z}/2\mathbb{Z}[X]$ irreduziblea den eta $\deg \overline{f} = \deg f$ den. Beraz, polinomioa jatorrizkoa izateko baldintza ezinbestekoa da. Bestetik, $g(X) = 2X^2 + X$ polinomio jatorrizkoa ez da irreduziblea $\mathbb{Z}[X]$-n, nahiz eta $\overline{g}(X) = X$ irreduziblea den $\mathbb{Z}/2\mathbb{Z}[X]$-n. Kasu horretan, arazoa da $\deg \overline{g} < \deg g$ dugula.

Bestalde, 4.23 teoreman ezin dugu $\mathfrak{p}$ ideal lehenaren ordez $\mathfrak{a}$ A-ren ideal orokor bat jarri. Hartu, adibidez, $A = \mathbb{Z}$, $\mathfrak{a} = 4\mathbb{Z}$ eta $f(X) = 2X^2 + X$. Orduan, $\overline{f}(X) = \overline{2}X^2 + X = (\overline{2}X + \overline{1})X$ irreduziblea da $\mathbb{Z}/4\mathbb{Z}[X]$ eraztunean, $\overline{2}X + \overline{1}$ unitatea baita (1.13 adibideetan ikusi genuen bezala) eta X irreduziblea baita. Hala ere, $f(X)$ ez da irreduziblea $\mathbb{Z}[X]$-n.

4.25. Adibidea. Izan bedi $f(X) = X^4 - X + 1 \in \mathbb{Z}[X]$. Polinomio hori 2 moduluarekiko (hau da, $2\mathbb{Z}$ idealarekiko) laburtzen badugu, orduan $\overline{f}(X) = X^4 + X + \overline{1} \in \mathbb{F}_2[X]$ lortzen dugu. Azken polinomio hori irreduziblea da $\mathbb{F}_2[X]$-n. Izan ere, $\overline{f}$-k ez du errorik $\mathbb{F}_2 = \{\overline{0}, \overline{1}\}$ gorputzean eta, ondorioz, faktorizatuko balitz, bigarren mailako bi irreduzibleren biderkadura litzateke. Orain, erraz ikusten da $\mathbb{F}_2[X]$-n bigarren mailako irreduzible bakarra dagoela, $X^2 + X + \overline{1}$ alegia. Beraz, $\overline{f}$ faktorizatuko balitz,

$$\overline{f}(X) = (X^2 + X + \overline{1})^2 = X^4 + X^2 + \overline{1}$$

izango genuke, eta hori ez da egia. Horrela, $\overline{f}$ irreduziblea da, eta 4.23 teoremaren baldintzak betetzen direnez, f irreduziblea da $\mathbb{Z}[X]$-n.

4.3. Polinomio homogeneoen faktorizazioa bi indeterminatutan

Kapitulu hau bukatzeko, polinomio homogeneoen faktorizazioa aztertuko dugu. Polinomio horiek oso rol garrantzitsua dute geometria aljebraikoa espazio proiektiboaren gainean garatzen denean. Ikusiko dugunez, bi indeterminatuko polinomio homogeneo baten faktorizazioa lortzeko, nahikoa da indeterminatu bakarreko polinomio egoki bat faktorizatzen jakitea. Has gaitezen polinomio homogeneoaren definizioarekin.

4.26. Definizioa. Izan bitez A eraztuna eta $f \in A[X_1, \ldots, A_n]$. Orduan, f *homogeneoa* dela diogu f-ren adierazpenean koefiziente ez-nulua duten monomio guztiek maila oso bera badute.

Adibidez, $f(X, Y) = X^2 + 3XY + 2Y^2$ homogeneoa da eta $g(X, Y) = X^2 + 3X^2Y^2 + 2Y^2$ ez da homogeneoa. Ikus dezagun $f(X, Y)$ faktore linealetan deskonposatzen dela. Izan ere,

$$f(X,Y) = X^2 + 3XY + 2Y^2 = Y^2\left(\left(\frac{X}{Y}\right)^2 + 3\left(\frac{X}{Y}\right) + 2\right) = Y^2 h\left(\frac{X}{Y}\right)$$

dugu, $h(T) = T^2 + 3T + 2$ izanik. (Ohartu $h(T) = f(T, 1)$ dela.) Orain, $h(T)$ polinomioak $T = -1$ eta $T = -2$ erroak dituenez, $h(T) = (T + 1)(T + 2)$ faktorizazioa dugu. Beraz,

$$f(X,Y) = Y^2\left(\frac{X}{Y} + 1\right)\left(\frac{X}{Y} + 2\right) = (X + Y)(X + 2Y)$$

deskonposizioa lortzen dugu. Era berean argudiatuz, ondorengo teorema frogatu daiteke. Gogoratu $h(T) \in K[T]$ polinomio bat K-ren gainean *banatzen dela* esaten dugula faktore linealen biderkadura gisa deskonposatzen bada $K[T]$-n. Bestela esanda, $\deg h = n$ bada, h K-ren gainean banatzen da baldin eta soilik baldin h-k n erro baditu K gorputzean, erro bakoitza bere anizkoiztasuna beste aldiz kontatuz gero.

4.27. Teorema. *Izan bedi $f(X,Y) \in K[X,Y]$ polinomio homogeneoa eta jarri $h(T) = f(T,1) \in K[T]$. Orduan:*

(i) *$f(X,Y)$ $K[X]$-n faktorizatzen da baldin eta soilik baldin $h(T)$ $K[T]$-n faktorizatzen bada.*

(ii) *$f(X,Y)$ faktore linealen biderkadura gisa deskonposatzen da $K[X]$-n baldin eta soilik baldin $h(T)$ K-ren gainean banatzen bada. Hala bada, eta h-ren erroak K-n $\lambda_1, \dots, \lambda_n$ badira (bakoitza bere anizkoiztasuna beste aldiz errepikaturik), orduan*

$$f(X,Y) = (X - \lambda_1 Y) \dots (X - \lambda_n Y)$$

dugu. (Ohartu faktore guztiak homogeneoak direla.)

Gogoratu K gorputza *aljebraikoki itxia* dela polinomio ez-konstante guztiek erroren bat badute K-n. Horren ondorioz, $K[X]$-ko polinomio guztiak faktore linealetan deskonposatzen dira (hau da, K-ren gainean banatzen dira) eta lehenengo mailako polinomioak dira $K[X]$-ko irreduzible bakarrak. Aljebraren Oinarrizko Teorema delakoak baieztatzen du $\mathbb{C}$, zenbaki konplexuen gorputza, aljebraikoki itxia dela.

4.28. Korolarioa. *K gorputz aljebraikoki itxia bada, orduan $K[X,Y]$-ko polinomio homogeneo guztiak faktore linealetan deskonposatzen dira, horiek ere homogeneoak izanik.*

Emaitza hori ez da betetzen polinomioa ez bada homogeneoa. Adibidez, $f(X,Y) = X^3 + Y^2 + 1$ irreduziblea da $K[X,Y]$-n, K edozein gorputz izanik, eta beraz ezin da faktore linealetan deskonposatu.

Azken korolarioa ez da egiazkoa polinomioek hiru indeterminatu edo gehiago erabiltzen badituzte. Adibidez, $\operatorname{char} K \neq 2$ bada, $f(X,Y,Z) = X^2 + Y^2 + Z^2$ irreduziblea da (4.7 ariketan ikusiko dugu hori) eta, beraz, ezin da faktore linealetan deskonposatu.

Nola faktorizatzen da $X^n - Y^n$ polinomio homogeneoa? Ikusita 4.27 teoremako emaitza, erantzuna $h(T) = T^n - 1$ polinomioaren deskonposizioak emango digu. Polinomio horren erroak, hau da, $\zeta^n = 1$ betetzen duten ζ elementuak, *unitatearen n. erroak* dira. Erraz egiazta daiteke unitatearen erroek talde bat osatzen dutela biderketarekiko. Talde hori, finitua denez, ziklikoa da. (Oro har, K gorputza bada, $K^\times$-ren azpitalde finitu guztiak ziklikoak direla frogatu daiteke.) Horrek esan nahi du unitatearen erro guztiak erro bakar baten berretura gisa jar daitezkeela.

Ez dago formula orokorrik jakiteko unitatearen zenbat n. erro dituen gorputz batek. Adibidez, $\mathbb{R}$-k unitatearen bi erro karratu ditu, 1 eta -1, baina unitatearen erro kubiko bakarra, 1 erro tribiala. Oro har, n bikoitia bada, $\mathbb{R}$-k unitatearen bi n. erro ditu eta, n bakoitia bada, bakar bat. Bestalde, K gorputzaren karakteristika p zenbaki lehena bada, orduan $n = p^m$ p-ren berretura bada, K-n dagoen unitatearen n. erro bakarra 1 da,

$$T^n - 1 = T^{p^m} - 1 = (T-1)^{p^m}$$

baitugu.

Beste alde batetik, K gorputza aljebraikoki itxia bada, orduan unitatearen n erro daude K-n, anizkoiztasunak kontuan hartuz gero. Horrez gain $\operatorname{char} K \nmid n$ baldintza badugu (adibidez, $\operatorname{char} K = 0$ bada), orduan erro horiek guztiak desberdinak dira. Kasu horretan, ζ unitatearen n. erroen taldearen sortzailea bada, ζ unitatearen *jatorrizko n. erroa* dela esaten dugu.* Orduan, unitatearen erro guztiak $1, \zeta, \dots, \zeta^{n-1}$ dira eta

$$T^n - 1 = (T-1)(T-\zeta)\dots(T-\zeta^{n-1})$$

dugu. Beraz, 4.27 teoremaren arabera, honako hau da $X^n - Y^n$ polinomioaren faktorizazioa:

$$X^n - Y^n = (X-Y)(X-\zeta Y)\dots(X-\zeta^{n-1}Y).$$

Hori da faktorizazioa, adibidez, $\mathbb{C}[X]$-n. Kasu horretan,

$$\zeta = e^{2\pi i/n} = \cos\frac{2\pi}{n} + i\,\sin\frac{2\pi}{n}$$

unitatearen jatorrizko n. erroa har dezakegu. Adibidez, $\omega = -1/2 + i\,\sqrt{3}/2$ unitatearen jatorrizko erro kubikoa da eta i, jatorrizko laugarren erroa. Ondorioz,

$$\begin{aligned} X^3 - Y^3 &= (X-Y)(X-\omega Y)(X-\omega^2 Y) \\ &= (X-Y)\left(X - \left(-\frac{1}{2} + i\,\frac{\sqrt{3}}{2}\right)Y\right)\left(X - \left(-\frac{1}{2} - i\,\frac{\sqrt{3}}{2}\right)Y\right) \end{aligned}$$

eta

$$X^4 - Y^4 = (X-Y)(X+Y)(X-iY)(X+iY)$$

faktorizazioak ditugu $\mathbb{C}[X]$-n.

Zer gertatzen da K aljebraikoki itxia eta $\operatorname{char} K \mid n$ bada? Orduan, halabeharrez, $\operatorname{char} K = p$ zenbaki lehena da. Idatz dezagun $n = mp^t$, $p \nmid m$ izanik. Orduan,

$$T^n - 1 = T^{mp^t} - 1 = (T^m - 1)^{p^t}$$

dugu. Kontuan izanik K-ren karakteristikak ez duela m zatitzen, orduan aurreko atalaren arabera, K-k badu unitatearen jatorrizko m. erro bat, dei diezaiogun ζ,

*K gorputza aljebraikoki itxia bada eta $\operatorname{char} K \nmid n$ bada, K-k unitatearen $\varphi(n)$ jatorrizko n. erro ditu, n ordenako talde zikliko batek $\varphi(n)$ sortzaile baititu. Hor $\varphi(n)$ Eulerren funtzioa da. Zehazkiago, ζ jatorrizko n. erroa bada, orduan gainerako jatorrizko erro guztiak ζ^k modukoak dira, $1 \le k \le n$ eta $\operatorname{zkh}(k,n) = 1$ izanik.

eta hori erabiliz, badakigu nola faktorizatzen den $T^m - 1$ polinomioa. Beraz, kasu horretan,

$$T^n - 1 = (T-1)^{p^t}(T-\zeta)^{p^t} \dots (T-\zeta^{m-1})^{p^t}$$

dugu eta, ondorioz,

$$X^n - Y^n = (X-Y)^{p^t}(X-\zeta Y)^{p^t} \dots (X-\zeta^{m-1}Y)^{p^t}.$$

Horrela, guztiz erabakita gelditzen da $X^n - Y^n$ polinomioaren faktorizazioa gorputz aljebraikoki itxi baten gainean.