1.9. Ariketak

1.1. Izan bitez A eraztuna eta $\mathfrak{a}$ A-ren ideala. Orduan, $\mathfrak{a}$-ren *erradikala*, $\operatorname{rad}\mathfrak{a}$ edo $\sqrt{\mathfrak{a}}$ ikurren bitartez adierazten duguna, honela definitzen da:

$$\operatorname{rad}\mathfrak{a} = \{a \in A \mid \exists r \geq 1 \text{ non } a^r \in \mathfrak{a}\}.$$

(i) Frogatu $\operatorname{rad}\mathfrak{a}$ A-ren ideal erradikala dela, are gehiago, $\mathfrak{a}$ barruan duten ideal erradikaletatik txikiena dela.

(ii) Frogatu $\mathfrak{a}$ erradikala dela baldin eta soilik baldin $\operatorname{rad}\mathfrak{a} = \mathfrak{a}$ bada.

(iii) Demagun orain A faktorizazio bakarreko domeinua dela, eta hartu $a \in A$. Izan bedi $a = p_1^{e_1} \dots p_r^{e_r}$ a-ren faktorizazioa elementu irreduzibleetan, p_i guztiak ez-elkartuak izanik. (Bi elementu $x, y \in A$ *elkartuak* direla esaten da existitzen bada $u \in A$ unitatea, halakoa non $y = ux$ baita.) Frogatu $\operatorname{rad}(a) = (p_1 \dots p_r)$ dela.

(iv) Izan bedi K gorputz aljebraikoki itxia. Kalkulatu ondorengo idealen erradikala $K[X,Y]$ aljebran: $(X^4+2X^2Y+Y^2)$, (X^4-Y^4), (X^6-Y^6), (X^n, Y^m) non $n, m \in \mathbb{N}$ baita, $(Y+X^2, Y-X^2)$, $(Y+X^2, Y-X^3)$. (Batzuetan erantzuna gorputzaren karakteristikaren araberakoa da.)

1.2. Izan bitez $\varphi : A \longrightarrow B$ eraztun (edo K-aljebra) homomorfismoa eta $\mathfrak{a}$ A-ren ideala.

(i) Ikusi, adibide baten bitartez, $\varphi(\mathfrak{a})$-k ez duela zertan B-ren ideala izan.

(ii) Hala ere, φ supraiektiboa den baldintzapean, $\varphi(\mathfrak{a})$ B-ren ideala da. Gainera, $\mathfrak{a} = (a_1, \dots, a_n)$ bada, orduan $\varphi(\mathfrak{a}) = (\varphi(a_1), \dots, \varphi(a_n))$ dugu.

1.3. Demagun $\varphi : A \longrightarrow B$ eraztun (edo K-aljebra) isomorfismoa dela, eta izan bitez $\mathfrak{a}$ A-ren ideala eta $\mathfrak{b} = \varphi(\mathfrak{a})$, B-ren ideala dena. Frogatu $A/\mathfrak{a} \cong B/\mathfrak{b}$ betetzen dela.

1.4. Izan bedi A integritate-domeinua.

(i) Baldin eta A finitua bada, frogatu A gorputza dela. (Laguntza: Ikusteko $a \neq 0$ elementuak alderantzizkoa duela, kontuan hartu $f : A \longrightarrow A$ aplikazioa, non $f(x) = ax$ baita.)

(ii) Era berean, A dimentsio finituko aljebra bada, orduan gorputza da.

1.5. Izan bedi K gorputza.

(i) Izan bedi $g(X) \in K[X]$ polinomio ez-konstante finkoa. Frogatu edozein $f(X) \in K[X]$ modu honetan idatz daitekeela,

$$f(X) = \sum_{i \geq 0} r_i(X) g(X)^i,$$

r_i polinomio guztien maila g-rena baino txikiagoa izanik. Ohartu antzekotasuna zenbaki oso baten garapenarekin, oinarri finko batekiko eginda. Lortu adierazpide hori $g(X) = X^2 + 1$ eta $f(X) = X^6 + X^5 + X + 1$ polinomioen kasuan.

(ii) Izan bitez orain $g_1(X_1), \dots, g_n(X_n)$ indeterminatu bananduak dituzten polinomio ez-konstanteak. Frogatu edozein $f \in K[X_1, \dots, X_n]$ modu honetan idatz daitekeela,

$$f(X_1, \dots, X_n) = \sum_{i_1, \dots, i_n \geq 0} r_{i_1, \dots, i_n}(X_1, \dots, X_n) g_1(X_1)^{i_1} \dots g_n(X_n)^{i_n},$$

$r_{i_1, \dots, i_n}$ polinomio bakoitzaren maila X_j indeterminatuarekiko $g_j(X_j)$-ren maila baino txikiagoa izanik.

(iii) Bereziki, aurreko atala $g_j(X_j) = X_j - a_j$ moduko polinomioekin aplikatzen badugu, $a_j \in K$ konstanteak harturik, orduan edozein $f \in K[X_1, \dots, X_n]$ modu honetan garatu daiteke:

$$f(X_1, \dots, X_n) = \sum_{i_1, \dots, i_n \geq 0} \lambda_{i_1, \dots, i_n} (X_1 - a_1)^{i_1} \dots (X_n - a_n)^{i_n},$$

$\lambda_{i_1, \dots, i_n}$ guztiak eskalarrak izanik. Horri f-ren garapena deituko diogu, $X_1 - a_1, \dots, X_n - a_n$-ren berreturetan. Ikusi garapen hori lortzeko beste modu bat, f-ren adierazpen arruntean (hau da, $X_1, \dots, X_n$-ren berreturetako garapenean) X_i indeterminatu bakoitzaren tokian $X_i - a_i + a_i$ idatziz.

1.6. Izan bedi K gorputza. Teorian ikusi dugu $K[X^2, X^3] = \left\{ \sum_i a_i X^i \mid a_1 = 0 \right\}$ dela. Eman ondorengo azpialjebren antzeko deskribapen bat:

(i) $K[X^2, X^n]$, n bakoitia izanik.
(ii) $K[X^4, X^6]$.
(iii) $K[X^3, X^7, X^8]$.

1.7. Dakigunez, $f(X) \in K[X]$ n-garren mailako polinomioa bada, orduan

$$K[X]/(f(X)) = \left\{ \overline{a_0 + a_1 X + \dots + a_{n-1} X^{n-1}} \mid a_i \in K \right\}$$

dugu, errepikapenik gabe. Ondorioz, $\{\overline{1}, \overline{X}, \dots, \overline{X}^{n-1}\}$ $K[X]/(f(X))$-ren K-oinarria da eta $\dim_K K[X]/(f(X)) = n$ dugu. Problema honetan $K[X, Y]$-ren kasua aztertzen dugu, ideal nagusi batez zatitzean.

(i) Izan bedi $n \in \mathbb{N}$ eta demagun $f(X, Y) = X^n + g(Y)$ itxurakoa dela. Frogatu

$$K[X, Y]/(f(X, Y)) = \left\{ \overline{a_0(Y) + a_1(Y) X + \dots + a_{n-1}(Y) X^{n-1}} \mid a_i(Y) \in K[Y] \right\}$$

dela, errepikapenik gabe. Ondorioztatu $\dim_K K[X, Y]/(f(X, Y)) = \infty$ dela.

(ii) Eman $K[X, Y]/(XY)$ K-aljebraren oinarri bat.

(iii) Aztertu $f(X, Y)$ polinomio orokor baten kasua: idatzi $K[X, Y]/(f(X, Y))$-ko elementuak errepikapenik gabe, eman K-oinarri bat eta ondorioztatu $\dim_K K[X, Y]/(f(X, Y)) = \infty$ dela. (Atal honetarako, komenigarria da 3. gaian agertzen diren ordena monomialak erabiltzea.)

(iv) Zer esan dezakegu, ordea, $K[X, Y]/(X^m, Y^n)$ aljebraren kasuan, $m, n \in \mathbb{N}$ izanik?

1.8. Izan bitez A K-aljebra eta $X_1, \dots, X_n$ indeterminatuak. Ohartu $A[X_1, \dots, X_n]$ ere K-aljebra dela.

(i) Definitu A-aljebraren kontzeptua eta eman $A[X_1, \ldots, X_n]$-ren propietate unibertsala.

(ii) Demagun $\mathfrak{a}$ A-ren ideala dela eta izan bedi $\mathfrak{b}$ $\mathfrak{a}$-k $A[X_1, \ldots, X_n]$ eraztunean sortzen duen ideala. Nolakoak dira $\mathfrak{b}$-ko elementuak? Frogatu isomorfismo hau betetzen dela:

$$\frac{A[X_1, \ldots, X_n]}{\mathfrak{b}} \cong \frac{A}{\mathfrak{a}}[X_1, \ldots, X_n].$$

(Kontuan hartu aurreko atala homomorfismo egoki bat definitzeko.)

1.9. Izan bitez $A \subseteq B$ eraztun-hedadura eta $\mathfrak{a}$ A-ren ideala. Orduan, $\mathfrak{a}$-k B eraztunean $\mathfrak{b}$ ideal bat sortzen du.

(i) Deskribatu $\mathfrak{b}$-ko elementuak $\mathfrak{a}$-ko elementuen funtzioan.

(ii) Demagun orain $\mathfrak{a}$ A-ren ideal lehena dela. Ikusi, adibide erraz baten bitartez, $\mathfrak{b} = B$ gerta daitekeela eta, beraz, $\mathfrak{b}$ ez-lehena izan daitekeela. Are gehiago, $\mathfrak{b}$ B-n propioa izanda ere, ez du zertan B-ren ideal lehena izan. Hori ikusteko, frogatu $2\mathbb{Z}[i]$ ez dela $\mathbb{Z}[i]$-ren ideal lehena, nahiz eta $2\mathbb{Z}$ $\mathbb{Z}$-n lehena izan.

(iii) Hartu orain $A = K[X_1, \ldots, X_m]$ eta $B = K[X_1, \ldots, X_n]$, $m \leq n$ izanik. Frogatu kasu horretan ez dela aurreko atalekoa bezalakorik gertatzen, hau da, $\mathfrak{a}$ lehena bada $\mathfrak{b}$ ere lehena dela. (Erabili aurreko ariketa.) Egia al da $\mathfrak{a}$ maximala denean $\mathfrak{b}$ ere maximala denik?

Azken propietateak hurrengo ondorioa du polinomioen idealekin lan egitean. Demagun $f_1, \ldots, f_r$ polinomioak direla. Orduan, $(f_1, \ldots, f_r)$ idazten dugunean nolabaiteko anbiguotasuna dago, ez dugulako zehazten polinomioen zein eraztunen gainean hartzen ari garen ideala. Eskuarki, $f_1, \ldots, f_r$ polinomioetan agertzen diren indeterminatuekin lan egingo dugu, gehiagorik hartu gabe, baina litekeena da batzuetan indeterminatu gehiago hartu nahi izatea. Adibidez, $(X+Y, X^2+Z)$ idazten dugunean, tazituki ulertzen dugu $K[X,Y,Z]$-n hartzen dugula ideala, baina $K[X,Y,Z,T]$-n ere zentzua du sinbolo horrek eta *beste multzo desberdin bat* litzateke. Azken atalak esaten digu, lehena izateko propietateari dagokionez, ez duela garrantzirik zein eraztun hartzen dugun lan-eremu, beti erantzun bera lortuko dugulako. Horregatik, hurrengo ariketan ez dugu zehazten polinomioen zein eraztunen gainean hartzen diren idealak, eta idealen polinomio sortzaileak baino ez ditugu ematen.

1.10. Aztertu ondorengo idealak lehenak diren edo ez: (X^3+Y^2+Z), $(X^3-3XYZ+Y^3+Z^3)$, $(X^5+XYZ^5+Y^5ZT^5)$, $(Y-X^2, Z-X^3)$, $(X-YZ, Z-XY)$, $(Y-X^2, Z-X^3, T-X^4-Y-Z)$.

1.11. Izan bedi $n \in \mathbb{N}$. Aztertu noiz den lehena $(X_1^2 + \cdots + X_n^2)$ ideala. (Indukzioaren bidez argudiatu, eta bereizi $\operatorname{char} K = 2$ eta $\operatorname{char} K \neq 2$ kasuak.)

1.12. Izan bitez K gorputza eta $X_1, \ldots, X_n$ indeterminatuak. Frogatu, n-ren gaineko indukzioa erabiliz,

$$\big(X_2 - g_1(X_1), X_3 - g_2(X_1, X_2), \ldots, X_n - g_{n-1}(X_1, \ldots, X_{n-1})\big)$$

moduko ideal guztiak lehenak direla.

1.13. Deskribatu $K[X,Y]/(XY)$ aljebraren ideal lehen guztiak eta ikusi, $(X)/(XY)$ eta $(Y)/(XY)$ izan ezik, maximalak direla denak.

1.14. Izan bitez K gorputza eta $h(X) \in K[X]$.

(i) Frogatu $K[X,Y]/(Y-h(X)) \cong K[X]$ isomorfismoa.

(ii) Izan bedi $\mathfrak{a}$ $K[X,Y]$-ren ideala eta demagun $Y-h(X) \in \mathfrak{a}$ dela. Aurreko atala erabiliz, ikusi existitzen dela $f(X) \in K[X]$, halakoa non $\mathfrak{a} = (Y - h(X), f(X))$ baita. Gainera, $\mathfrak{a}$ ideal lehena da baldin eta soilik baldin $f(X)$ irreduziblea bada.

(iii) Aztertu ondorengo idealak lehenak diren edo ez $\mathbb{Q}[X,Y]$-n, $\mathbb{R}[X,Y]$-n eta $\mathbb{C}[X,Y]$-n: $(Y-X^2, X-Y^2)$, $(Y-X^2, X-Y^2+1)$, $(Y-X^2, X+Y+1)$, $(Y-X^2, Y^3-X^6+X)$, $(Y-X^2, Y^3-X^6+1)$.

(iv) Berriro ere (i) ataleko isomorfismoa erabiliz, frogatu

$$(Y-h(X), f(X)) \cap (Y-h(X), g(X)) = (Y-h(X), \mathrm{mkt}(f(X), g(X)))$$

dela. Kalkulatu $(Y-X^2, Y^2-X) \cap (Y-X^2, Y-X^3)$ ebakidura.

(v) Baldin eta $p, f, g \in K[X_1, \ldots, X_n]$ bada, ziurta daiteke $(p,f) \cap (p,g) = (p, \mathrm{mkt}(f,g))$ denik?

1.15. Izan bedi K gorputza.

(i) Frogatu Y^2-X^3 polinomioa irreduziblea dela eta, beraz, (Y^2-X^3) $K[X,Y]$-ren ideal lehena dela.

(ii) Izan bedi T beste indeterminatu bat. Frogatu

$$K[X,Y]/(Y^2-X^3) \cong K[T^2, T^3]$$

aljebra isomorfismoa. (Iradokizuna: Definitu $K[X,Y] \longrightarrow K[T]$ homomorfismo egoki bat.) Ohartu horrela ere ondoriozta daitekeela (Y^2-X^3) ideal lehena dela.

(iii) Azken isomorfismo hori erabiliz, frogatu $\overline{X}$ eta $\overline{Y}$ elementu irreduzibleak direla $K[X,Y]/(Y^2-X^3)$ zatiduran. Saiatu emaitza hori zuzenean frogatzen, $K[X,Y]/(Y^2-X^3)$-n lan eginez.

(iv) Ondorioztatu $K[X,Y]/(Y^2-X^3)$ ez dela faktorizazio bakarreko domeinua. Beraz, faktorizazio bakarreko domeinu baten zatidura batek ez du zertan faktorizazio bakarreko domeinua izan, nahiz eta integritate-domeinua izan.

(v) Frogatu aurreko ataletako emaitza guztiak $Y^n - X^m$ polinomioaren kasuan ere egiazkoak direla, $n, m > 1$ eta $(n,m) = 1$ izanez gero. Zer gertatzen da $n = 1$ edo $m = 1$ den kasuan?

1.16. Izan bitez $A = K[X,Y]/(Y^2-X^3)$ eta L A-ren zatikien gorputza. Frogatu $\overline{Y}/\overline{X} \in L$ elementu osoa dela A-ren gainean, eta ondorioztatu A ez dela faktorizazio bakarreko domeinua. (Emaitza hori aurreko probleman beste modu batean frogatu dugu.) Ikusi argudio hori $A = K[X,Y]/(Y^n - X^m)$ aljebrari ere aplika dakiokeela,

$n, m > 1$ eta $(n, m) = 1$ den baldintzapean. Zer gertatzen da $n = 1$ edo $m = 1$ bada?

1.17. Teorian, K aljebraikoki itxia den baldintzapean, $K[X_1, \dots, X_n]$-ren ideal maximalen deskribapena eman dugu, Zariskiren leman oinarrituz. Ohartu, bestalde, Zariskiren leman K gorputza edozein izan daitekeela, ez duela aljebraikoki itxia izan behar. Problema honetan Zariskiren lemaren froga alternatibo bat ematen dugu, K kontagarria ez denean balio duena. Adibidez, $\mathbb{C}$-ren edo $\mathbb{R}$-ren kasurako balio du.

(i) Izan bedi momentuz K edozein gorputz. Frogatu $\{1/(X - a) \mid a \in K\} \subseteq K(X)$ multzoa linealki independentea dela. Beraz, $\dim_K K(X)$ K-ren kardinala baino handiago edo berdin da.

(ii) Izan bedi A K-aljebra finituki sortua. Frogatu $\dim_K A$ kontagarria dela.

(iii) Demagun orain K gorputza ez dela kontagarria. Aurreko bi atalak konbinatuz, ondorioztatu Zariskiren lema.

1.18. Izan bedi $A \neq \{0\}$ eraztuna. Orduan, A *eraztun lokala* dela diogu A-k ideal maximal bakarra badu. Adibidez, A edozein eraztun bada eta $\mathfrak{p}$ A-ren edozein ideal lehen bada, orduan $A_{\mathfrak{p}}$ eraztun lokala da, bere ideal maximal bakarra $\mathfrak{p}A_{\mathfrak{p}}$ izanik.

(i) Noiz dira $\mathbb{Z}/n\mathbb{Z}$ eta $K[X]/(f(X))$ zatidurak eraztun lokalak? Frogatu $K[X, Y]/(X^n, Y^m)$ eraztun lokala dela $n, m \geq 1$ bada.

(ii) Izan bitez A eraztun lokala eta $\mathfrak{m}$ bere ideal maximal bakarra. Frogatu $A^\times = A \setminus \mathfrak{m}$ dela. (Laguntza: $x \in A \setminus \mathfrak{m}$ bada, zer esan dezakegu (x) idealari buruz?) Baldin eta A integritate-domeinua bada, ondorioztatu $A_{\mathfrak{m}} \cong A$ isomorfismoa. Beraz, $\mathfrak{m}$-tik kanpoko elementuak unitateak badira, $\mathfrak{m}$-rekiko lokalizatzeak ez du ezer berririk ematen. (Zentzuzkoa dirudi, lokalizatzearen helburua $A \setminus \mathfrak{m}$-ko elementuak unitate bihurtzea baita.)

1.19. Izan bitez A eraztuna eta $\mathfrak{p}$ A-ren ideal lehena. Orduan $\mathfrak{p}A_{\mathfrak{p}}$ $A_{\mathfrak{p}}$-ren ideal maximala da eta, beraz, $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ gorputza da.

(i) Frogatu $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ eta $A/\mathfrak{p}$-ren zatikien gorputza isomorfoak direla. Bereziki, $\mathfrak{m}$ A-ren ideal maximala bada, orduan $A_{\mathfrak{m}}/\mathfrak{m}A_{\mathfrak{m}} \cong A/\mathfrak{m}$ isomorfismoa dugu.

(ii) Zein gorputz lortzen dira kasu hauetan: $A = \mathbb{Z}$, $\mathfrak{p} = (p)$, p zenbaki lehena izanik; $A = \mathbb{Z}[X]$ eta $\mathfrak{p} = (X)$; $A = K[X, Y]$ eta $\mathfrak{p} = (X)$, K gorputza izanik; $A = K[X, Y]$ eta $\mathfrak{p} = (X, Y)$?