2

Multzo aljebraiko afinak

2.1. Multzo aljebraiko afinak eta polinomioen idealak

Geometria aljebraikoaren helburua multzo aljebraikoak, hau da, ekuazio polinomikoen bidez emanda dauden multzoak estudiatzea da. Kapitulu honetan multzo aljebraikoen teoria espazio afinean garatuko dugu eta 4. eta 5. kapituluetan espazio proiektiboaren testuingurura hedatuko dugu gure ikerketa. Lehenengo atal honetan, multzo aljebraiko afinen oinarrizko propietateak aztertuko ditugu, eta polinomien aljebren idealekin duten lotura erakutsiko dugu.

2.1. Definizioa. Izan bitez K gorputza eta $n \in \mathbb{N}$. Orduan K^n-ri K gaineko n dimentsioko *espazio afin* deitzen diogu. Hori adierazteko $\mathbb{A}^n(K)$ idazten dugu, edo sinpleago $\mathbb{A}^n$, ez badago zalantzarik gorputza zein den. Beraz,

$$\mathbb{A}^n = \{(a_1, \ldots, a_n) \mid a_i \in K\}.$$

2.2. Notazioa. Ikusten denez, bi notazio ditugu multzo bera adierazteko, K^n eta $\mathbb{A}^n$. Noiz erabili bata eta noiz bestea?

K^n: Espazio bektorialaren egitura hartzen denean: elementuak bektore gisa ikusten ditugu.

$\mathbb{A}^n$: Espazio afinaren egitura hartzen denean: elementuak puntu gisa ikusten ditugu.

2.3. Definizioa. Izan bedi $S \subseteq K[X_1, \ldots, X_n]$ polinomioen multzoa. Orduan, *S-ren zeroen multzoa* $\mathbb{A}^n$-ren honako azpimultzo hau da:

$$V(S) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n \mid f(a_1, \ldots, a_n) = 0,\ f \in S \text{ guztietarako}\}.$$

Beraz, $V(S)$ S-ko polinomio guztiak anulatzen diren puntu afinen multzoa da.

2.4. Definizioa. Izan bedi $Y \subseteq \mathbb{A}^n$. Orduan, Y *azpimultzo aljebraiko (afina)* dela esaten dugu existitzen bada $S \subseteq K[X_1, \ldots, X_n]$, non $Y = V(S)$ baita.

Beraz, $\mathbb{A}^n$-ren azpimultzo aljebraikoak ekuazio polinomiko batzuen soluzioen multzoak dira.

2.5. Adibideak. 1) Erraz deskribatzen dira $\mathbb{A}^1$-eko multzo aljebraiko guztiak. Alde batetik, $S \subseteq K[X]$ aukeratzen dugunean, bi aukera daude:

(i) $S = \varnothing$ edo $S = \{0\}$ izatea. Orduan, $V(S) = \mathbb{A}^1$ dugu.
(ii) S-n f polinomio ez-nulu bat egotea. Orduan, f-k erro kopuru finitu bat du $\mathbb{A}^1$-en eta, ondorioz, $V(S)$ finitua da.

Alderantziz, $Y = \{a_1, \ldots, a_r\} \subseteq \mathbb{A}^1$ finitua bada, orduan $f(X) = (X - a_1) \ldots (X - a_r)$ hartuz gero, $V(f) = Y$ dugu. Laburbilduz, honako hauek dira $\mathbb{A}^1$-eko multzo aljebraikoak: $\mathbb{A}^1$ bera eta azpimultzo finituak.

2) Honako azpimultzo hauek aljebraikoak dira $\mathbb{A}^2$ planoan:

(i) Zirkunferentziak. Izan ere, (a, b) puntuan zentratutako eta r erradioko zirkunferentzia $V((X - a)^2 + (Y - b)^2 - r^2)$ multzoa da.
(ii) Parabolak, elipseak eta hiperbolak. Horiek ere bigarren mailako polinomioen bidez emanda daude.

3) $\mathbb{A}^n$ espazio afin orokorrean, azpimultzo hauek aljebraikoak dira:

(i) *Hiperplanoak*: $a_1X_1 + \cdots + a_nX_n = b$ bezalako ekuazio baten soluzioak dira.
(ii) *Hipergainazalak*: Horiek polinomio bakar baten zeroen multzoak dira, hau da, $V(f)$ modukoak, non $f \in K[X_1, \ldots, X_n]$ baita.
(iii) Azpiespazio afin guztiak, lehenengo mailako polinomioen zeroak baitira. Bestela esanda, azpiespazio afinak hiperplanoen ebakidurak dira. Aljebra linealetik dakigunez, azpiespazioaren dimentsioa d bada, nahikoak dira lehenengo mailako $n - d$ polinomio, hau da, $n - d$ hiperplano.
(iv) Puntuak: $V(X_1 - a_1, \ldots, X_n - a_n) = \{(a_1, \ldots, a_n)\}$ dugu.

Beraz, V eragile bat dugu, polinomioen azpimultzo bakoitzari espazio afinaren azpimultzo bat esleitzen diona:

$$\begin{array}{rccc} V & : & \mathcal{P}(K[X_1, \ldots, X_n]) & \longrightarrow & \mathcal{P}(\mathbb{A}^n) \\ & & S & \longmapsto & V(S). \end{array}$$

(Notazio hau erabili dugu: A multzoa bada, $\mathcal{P}(A)$ A-ren *parteen multzoa* da, hau da, A-ren azpimultzo guztiek osatzen duten multzoa.)

2.6. Teorema. *V eragileak honako propietate hauek ditu:*

(i) *V-k partekotasunak aldatzen ditu: $S \subseteq T$ bada, orduan $V(T) \subseteq V(S)$.*
(ii) *$V(S) \cap V(T) = V(S \cup T)$. Orokorki, $\cap_{i \in I} V(S_i) = V(\cup_{i \in I} S_i)$.*
(iii) *$V(S) \cup V(T) \subseteq V(S \cap T)$.*
(iv) *$V(\varnothing) = V(0) = \mathbb{A}^n$ eta $V(K[X_1, \ldots, X_n]) = V(1) = \varnothing$. Beraz, $\varnothing$ eta $\mathbb{A}^n$ multzo aljebraikoak dira.*

Froga. (i) Emanda $S \subseteq T$:

$$\begin{aligned} (a_1, \ldots, a_n) \in V(T) &\implies f(a_1, \ldots, a_n) = 0 \ \forall f \in T \\ &\overset{S \subseteq T}{\implies} f(a_1, \ldots, a_n) = 0 \ \forall f \in S \\ &\implies (a_1, \ldots, a_n) \in V(S). \end{aligned}$$

Beraz, $V(T) \subseteq V(S)$ dugu, nahi bezala.

(ii) Ikus dezagun $V(\cup_{i\in I} S_i) = \cap_{i\in I} V(S_i)$ propietate orokorra:

$$\begin{aligned}(a_1,\dots,a_n) \in V(\cup_{i\in I} S_i) &\iff f(a_1,\dots,a_n) = 0 \ \forall f \in \cup_{i\in I} S_i \\ &\iff f(a_1,\dots,a_n) = 0 \ \forall f \in S_i \ \forall i \in I \\ &\iff (a_1,\dots,a_n) \in V(S_i) \ \forall i \in I \\ &\iff (a_1,\dots,a_n) \in \cap_{i\in I} V(S_i).\end{aligned}$$

(iii) Hori zuzenean ikus daiteke edo, bestela, (i) propietatea erabiliz:

$$S \cap T \subseteq S, T \overset{\text{(i)-engatik}}{\Longrightarrow} V(S), V(T) \subseteq V(S \cap T) \implies V(S) \cup V(T) \subseteq V(S \cap T).$$

(iv) Garbi dago $V(0) = \mathbb{A}^n$ dela eta, $\varnothing \subseteq \{0\}$ denez, $V(0) \subseteq V(\varnothing)$ eta $V(\varnothing) = \mathbb{A}^n$ ondorioztatzen dugu.* Bestalde, berehalakoa da $V(K[X_1,\dots,X_n]) = V(1) = \varnothing$ dela. □

Aurreko teoreman $V(S) \cup V(T) \subseteq V(S \cap T)$ partekotasuna ikusi dugun arren, ezin da berdintza ziurtatu. Adibidez, hartu $S = \{X\}$ eta $T = \{Y\}$ $K[X,Y]$-n. Orduan $V(S \cap T) = V(\varnothing) = \mathbb{A}^2$ dugu, baina $V(S) \cup V(T)$ bakarrik da OX eta OY ardatzen bildura.

2.7. Teorema. *Izan bitez $f_1,\dots,f_r \in K[X_1,\dots,X_n]$. Orduan:*

(i) $V(f_1,\dots,f_r) = V(f_1) \cap \dots \cap V(f_r)$.
(ii) $V(f_1 \dots f_r) = V(f_1) \cup \dots \cup V(f_r)$.

Froga. (i) Hori aurreko teoremaren (ii) atalaren kasu berezi bat baino ez da.

(ii) Nahikoa da kontuan izatea biderkadura bat 0 dela baldin eta soilik baldin faktoreetako bat 0 bada. □

2.8. Teorema. *Izan bitez $S \subseteq K[X_1,\dots,X_n]$ eta $\mathfrak{a} = (S)$. Orduan, $V(S) = V(\mathfrak{a})$ dugu.*

Froga. Alde batetik, 2.6 teoremaren (i) atalagatik, $S \subseteq \mathfrak{a}$ partekotasunak $V(\mathfrak{a}) \subseteq V(S)$ inplikatzen du. Ikus dezagun alderantzizko inplikazioa. Horretarako, hartu $(a_1,\dots,a_n) \in V(S)$ eta $f \in \mathfrak{a}$, eta ikus dezagun $f(a_1,\dots,a_n) = 0$ dela. Sortutako idealaren definizioaren arabera, existitzen dira $f_1,\dots,f_r \in S$ eta $q_1,\dots,q_r \in K[X_1,\dots,X_n]$, halakoak non $f = q_1f_1 + \dots + q_rf_r$ baita. Orduan, $f_1(a_1,\dots,a_n) = \dots = f_r(a_1,\dots,a_n) = 0$ dugu eta, beraz,

$$f(a_1,\dots,a_n) = q_1(a_1,\dots,a_n)f_1(a_1,\dots,a_n) + \dots + q_r(a_1,\dots,a_n)f_r(a_1,\dots,a_n) = 0,$$

nahi bezala. □

*Absurdora eramanez ere frogatu daiteke $V(\varnothing) = \mathbb{A}^n$ dela. Izan ere, demagun $(a_1,\dots,a_n) \notin V(\varnothing)$ dela. Orduan, existituko litzateke f polinomio bat multzo hutsaren barruan, non $f(a_1,\dots,a_n) \neq 0$ baita. Hori kontraesan bat da, multzo hutsak ez baitu elementurik.

Azken teoremaren ondorioz, V eragilea idealetara murrizten badugu, oraindik ere $\mathbb{A}^n$-ren multzo aljebraiko guztiak lortzen ditugu. Hau da,

$$\begin{array}{ccccc} V & : & \{K[X_1,\dots,X_n]\text{-ren idealak}\} & \longrightarrow & \{\mathbb{A}^n\text{-ren multzo aljebraikoak}\} \\ & & \mathfrak{a} & \longmapsto & V(\mathfrak{a}) \end{array}$$

supraiektiboa da. Baina ez da injektiboa; adibidez $\mathfrak{a} = (X)$ bada, orduan $V(\mathfrak{a}) = V(\mathfrak{a}^2) = \cdots = V(\mathfrak{a}^k) = \cdots$ dugu.

2.9. Korolarioa. *Edozein multzo aljebraiko hipergainazal kopuru finitu baten ebakidura da. Bestela esanda,*

$$\begin{cases} f_1(X_1,\dots,X_n) = 0 \\ \qquad\qquad\qquad \vdots \\ f_r(X_1,\dots,X_n) = 0 \end{cases}$$

moduko sistema polinomiko baten soluzioen multzoa da.

Froga. Izan bedi $Y = V(S)$ $\mathbb{A}^n$-ren multzo aljebraiko orokorra. Jarri $\mathfrak{a} = (S)$. Orduan, Hilberten oinarriaren teoremaren arabera, existitzen dira $f_1,\dots,f_r \in K[X_1,\dots,X_n]$, halakoak non $\mathfrak{a} = (f_1,\dots,f_r)$ baita. Orain, 2.8 teorema bitan erabiliz,

$$Y = V(S) = V(\mathfrak{a}) = V(f_1,\dots,f_r)$$

dugu. Azkenik, 2.7 teorema aplikatuz,

$$Y = V(f_1) \cap \cdots \cap V(f_r)$$

hipergainazal kopuru finitu baten ebakidura gisa adierazita gelditzen da. □

Ondorengo bi teoremetan ikusten dugu zein den V eragilearen portaera idealen arteko eragiketak egiten ditugunean.

2.10. Teorema. *Izan bedi $\{\mathfrak{a}_i\}_{i\in I}$ $K[X_1,\dots,X_n]$-ren ideal-familia. Orduan,*

$$V(\sum_{i\in I} \mathfrak{a}_i) = \bigcap_{i\in I} V(\mathfrak{a}_i).$$

Froga. Gogoratu $\cup_{i\in I}\mathfrak{a}_i$ bildurak sortzen duen ideala $\sum_{i\in I}\mathfrak{a}_i$ batura dela. Hori kontuan izanik,

$$V(\sum_{i\in I} \mathfrak{a}_i) = V(\bigcup_{i\in I} \mathfrak{a}_i) = \bigcap_{i\in I} V(\mathfrak{a}_i)$$

lortzen dugu, 2.8 eta 2.6 teoremak aplikatuz, hurrenez hurren. □

2.11. Teorema. *Izan bitez $\mathfrak{a}$ eta $\mathfrak{b}$ $K[X_1,\dots,X_n]$-ren idealak. Orduan,*

$$V(\mathfrak{a}\cap\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b}).$$

FROGA. Alde batetik, $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}$ denez eta V-k partekotasunak aldatzen dituenez, $V(\mathfrak{a}) \subseteq V(\mathfrak{a} \cap \mathfrak{b}) \subseteq V(\mathfrak{ab})$ dugu. Aldatzen baditugu $\mathfrak{a}$ eta $\mathfrak{b}$ elkarrekin aurreko partekotasunean, azkenean

$$V(\mathfrak{a}) \cup V(\mathfrak{b}) \subseteq V(\mathfrak{a} \cap \mathfrak{b}) \subseteq V(\mathfrak{ab})$$

lortzen dugu. Beraz, teorema frogaturik geldituko da behin $V(\mathfrak{ab}) \subseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$ ikusita. Absurdora eramanez, demagun badagoela $(a_1, \ldots, a_n) \in V(\mathfrak{ab})$ puntu bat, ez dagoena $V(\mathfrak{a})$-n ezta $V(\mathfrak{b})$-n ere. Orduan, existitzen dira $f \in \mathfrak{a}$ eta $g \in \mathfrak{b}$, non $f(a_1, \ldots, a_n) \neq 0$ eta $g(a_1, \ldots, a_n) \neq 0$ baita. Ondorioz, $fg \in \mathfrak{ab}$ polinomioa ez da $(a_1, \ldots, a_n)$-n anulatzen. Hori kontraesan bat da, $(a_1, \ldots, a_n) \in V(\mathfrak{ab})$ da eta. □

Orain, 2.6 eta 2.11 teoremak kontuan izanik, multzo aljebraikoen propietate interesgarri hauek lortzen ditugu.

2.12. Korolarioa. (i) *Multzo aljebraikoen bildura finituak multzo aljebraikoak dira.*
(ii) *Multzo aljebraikoen ebakidura orokorrak multzo aljebraikoak dira.*

Oro har, ez da betetzen $\cup_{i \in I} V(\mathfrak{a}_i) = V(\cap_{i \in I} \mathfrak{a}_i)$ propietatea I indizeen multzoa infinitua bada. Are gehiago, ezin da ziurtatu multzo aljebraikoen bildura infinitu bat multzo aljebraikoa denik. Adibidez, jartzen badugu $V_\lambda = V(Y - \lambda X) \subseteq \mathbb{A}^2(\mathbb{R})$, $\lambda \in \mathbb{R}$ guztietarako, orduan $\cup_{\lambda \in \mathbb{R}} V_\lambda$ ez da multzo aljebraikoa. (Hori 2.3 ariketan ikusiko dugu.)

Espazio topologiko bat definitzeko, multzo irekien familia zehaztu behar da, kontuan izanik multzo irekiek bi propietate hauek bete behar dituztela:

(i) Multzo hutsa eta multzo osoa irekiak dira.
(ii) Multzo irekien bildura orokorrak eta ebakidura finituak irekiak dira.

Multzo itxiak multzo irekien osagarriak direnez, beste aukera bat multzo itxien familia zehaztea da. Orduan propietate hauek behar ditugu:

(i) Multzo hutsa eta multzo osoa itxiak dira.
(ii) Multzo itxien bildura finituak eta ebakidura orokorrak itxiak dira.

Ohartu, 2.6 teoremaren eta 2.12 korolarioaren arabera, $\mathbb{A}^n$ espazio afinean multzo aljebraikoek azken bi propietate horiek betetzen dituztela. Ondorioz, badago $\mathbb{A}^n$-ren gainean topologia bat definitzea, multzo itxi modura multzo aljebraikoak hartuz. Topologia horri *Zariskiren topologia* deitzen zaio.

Gogoan izan $\mathbb{A}^n$ espazio afina K^n baino ez dela, K gorputza izanik. Orain, $K = \mathbb{R}$ edo $\mathbb{C}$ bada, K^n-k badu berez espazio topologikoaren egitura, *ohiko topologia* erabiliz. Garrantzitsua da ohartzea Zariskiren topologia eta ohiko topologia ez datozela bat, 2.16 ariketan ikusiko dugun bezala. Zehazkiago, ohiko topologia finagoa dela ikusiko dugu, hau da, Zariskiren topologiarekin irekia (itxia) den multzo bat irekia (itxia) da ohiko topologiarekin, baina ez beti alderantziz.

2.13. Adibidea. Zein da Zariskiren topologia $\mathbb{A}^1$-en? Multzo itxiak multzo finituak dira; beraz, multzo irekiak multzo kofinituak dira eta Zariskiren topologia

topologia kofinitua da. Hori ez da egia $\mathbb{A}^2$-n K infinitua bada: zuzen baten osagarria irekia da, baina ez da kofinitua.

Espazio topologiko batean, multzo irekien $\mathcal{U}$ familia bat *multzo irekien oinarria* dela esaten dugu edozein multzo ireki $\mathcal{U}$-ko multzoen bildura gisa jar badaiteke. Antzera, multzo itxien $\mathcal{F}$ familia bat *multzo itxien oinarria* da edozein multzo itxi $\mathcal{F}$-ko multzoen ebakidura gisa jar badaiteke. Terminologia hori erabiliz, hurrengo emaitza 2.9 korolarioaren ondorio berehalakoa da.

2.14. Proposizioa. *Hipergainazalek $\mathbb{A}^n$-ren multzo itxien oinarri bat osatzen dute, Zariskiren topologiarekiko. Beraz, hipergainazalen osagarriek multzo irekien oinarri bat osatzen dute.*

Edozein espazio topologikotan bezala, $\mathbb{A}^n$-n Y multzo baten itxidura har daiteke, $\overline{Y}$ idazten dena. Zein da $\overline{Y}$-ren esanahia? Definizioz, Y barruan duten multzo itxi (hau da, aljebraiko) guztietatik txikiena da. Bereziki, $Y \subseteq \mathbb{A}^n$ multzo aljebraikoa da baldin eta soilik baldin $\overline{Y} = Y$ bada.

2.15. Adibidea. Izan bedi $Y \subseteq \mathbb{A}^2$ multzoa $X_1 = 0$ zuzenaren osagarria. Orduan, 2.5 ariketaren (iii) atalean ikusiko dugunez, Y ez da multzo aljebraikoa eta $\overline{Y} = \mathbb{A}^2$ dugu.

2.2. Hilberten Nullstellensatz-a eta $I - V$ korrespondentzia

Aurreko atalean, V eragilea definitu dugu. Aipatu dugun bezala, eragile hori polinomioen idealetatik multzo aljebraikoetara doala pentsa dezakegu. Jarraian, alderantzizko norabidean doan I eragile bat definituko dugu, eta horren oinarrizko propietateak emango ditugu.

2.16. Definizioa. Izan bedi $Y \subseteq \mathbb{A}^n$. Orduan, *Y-ren ideala* honela definitzen dugu:

$$I(Y) = \{f \in K[X_1, \ldots, X_n] \mid f(a_1, \ldots, a_n) = 0,\ (a_1, \ldots, a_n) \in Y \text{ guztietarako}\}.$$

Bestela esanda, $I(Y)$ multzoa Y-ko puntu guztien gainean anulatzen diren polinomioek osatzen dute.

Lehenengo eta behin, argitu dezagun zergatik deitu diogun "Y-ren ideala" $I(Y)$ multzoari.

2.17. Teorema. *Izan bedi $Y \subseteq \mathbb{A}^n$. Orduan, $I(Y)$ $K[X_1, \ldots, X_n]$-ren ideal erradikala da.*

Froga. Alde batetik, $I(Y)$ ez da hutsa, $0 \in I(Y)$ baitugu. Demagun $f, g \in I(Y)$ dela. Orduan, f eta g polinomioak Y-ko puntu guztietan anulatzen dira eta, beraz, $f + g$ ere bai. Horrela, $f + g \in I(Y)$ dugu. Era berean, $f \in I(Y)$ eta

$q \in K[X_1, \ldots, X_n]$ bada, orduan $qf \in I(Y)$ dugu. Ondorioz, $I(Y)$ $K[X_1, \ldots, X_n]$-ren ideala da. Erradikala dela ikusteko, demagun $f^r \in I(Y)$ dela. Orduan, $f^r(a_1, \ldots, a_n) = 0$ dugu $(a_1, \ldots, a_n) \in Y$ guztietarako eta, polinomioen balioak K gorputzean daudenez, $f(a_1, \ldots, a_n) = 0$ izan behar dugu. Horrek $f \in I(Y)$ dela frogatzen du eta, hortaz, $I(Y)$ erradikala da. □

2.18. Adibidea. Izan bedi Y multzoa $X_n = a$ ekuazioa duen hiperplanoa, hau da, azken osagaia a-ren berdina duten puntu guztien multzoa. Ikus dezagun $I(Y) = (X_n - a)$ dugula, K gorputza infinitua bada. Alde batetik, garbi dago $X_n - a \in I(Y)$ dela eta, $I(Y)$ ideala izateagatik, $\supseteq$ partekotasuna lortzen dugu. Bestetik, hartu edozein $f \in I(Y)$, eta zatitu dezagun $X_n - a$ polinomioaz X_n-rekiko. Orduan, $f = q(X_n - a) + r$ deskonposizioa dugu, $r \in K[X_1, \ldots, X_{n-1}]$ izanik. Ebaluatzen baditugu polinomioak $(a_1, \ldots, a_{n-1}, a) \in Y$ puntuen gainean, orduan $f, X_n - a \in I(Y)$ izateagatik, $r(a_1, \ldots, a_{n-1}) = 0$ lortzen dugu $a_i \in K$ guztietarako. Hurrengo teoremaren (iii) atalean ikusiko dugunez, K gorputza infinitua bada, hori bakarrik gerta daiteke $r = 0$ bada. Ondorioz, $f = q(X_n - a) \in (X_n - a)$ dugu, eta $\subseteq$ partekotasuna ere betetzen da.

Ohartu I eragile gisa ikus dezakegula:

$$\begin{array}{rccc} I & : & \mathcal{P}(\mathbb{A}^n) & \longrightarrow & \mathcal{P}(K[X_1, \ldots, X_n]) \\ & & Y & \longmapsto & I(Y). \end{array}$$

2.19. Teorema. *I eragileak honako propietate hauek ditu:*

(i) *I-k partekotasunak aldatzen ditu: $Y \subseteq Z \Longrightarrow I(Z) \subseteq I(Y)$.*
(ii) *$I(\varnothing) = K[X_1, \ldots, X_n]$.*
(iii) *K gorputza infinitua bada, $I(\mathbb{A}^n) = \{0\}$ dugu.*
(iv) *$Y, Z \subseteq \mathbb{A}^n$ badira, orduan $I(Y) \cap I(Z) = I(Y \cup Z)$ eta $I(Y) + I(Z) \subseteq I(Y \cap Z)$ dugu.*

Froga. (i) Emanda $Y \subseteq Z$:

$$\begin{aligned} f \in I(Z) &\Longrightarrow f(a_1, \ldots, a_n) = 0 \ \forall (a_1, \ldots, a_n) \in Z \\ &\overset{Y \subseteq Z}{\Longrightarrow} f(a_1, \ldots, a_n) = 0 \ \forall (a_1, \ldots, a_n) \in Y \\ &\Longrightarrow f \in I(Y). \end{aligned}$$

Beraz, $I(Y) \subseteq I(Z)$ dugu, nahi bezala.

(ii) Absurdora eramanez, demagun badagoela $f \in K[X_1, \ldots, X_n]$ polinomio bat, non $f \notin I(\varnothing)$ baita. Orduan, I eragilearen definizioaren arabera, existituko litzateke $(a_1, \ldots, a_n) \in \varnothing$ non $f(a_1, \ldots, a_n) \neq 0$ den. Hori absurdoa da, multzo hutsak ez baitu elementurik.

(iii) Hori 2.5 probleman ikusiko dugu.

(iv) Ikus dezagun $I(Y) \cap I(Z) = I(Y \cup Z)$ berdintza:

$$\begin{aligned} f \in I(Y \cup Z) &\iff f(a_1, \ldots, a_n) = 0 \ \forall (a_1, \ldots, a_n) \in Y \cup Z \\ &\iff f(a_1, \ldots, a_n) = 0 \ \forall (a_1, \ldots, a_n) \in Y \text{ eta} \\ &\qquad f(a_1, \ldots, a_n) = 0 \ \forall (a_1, \ldots, a_n) \in Z \\ &\iff f \in I(Y) \text{ eta } f \in I(Z) \\ &\iff f \in I(Y) \cap I(Z). \end{aligned}$$

Azkenik, frogatu dezagun $I(Y) + I(Z) \subseteq I(Y \cap Z)$ partekotasuna. Alde batetik, $Y \cap Z \subseteq Y, Z$ denez, (i) atala aplikatuz $I(Y), I(Z) \subseteq I(Y \cap Z)$ lortzen dugu. Orain, $I(Y \cap Z)$ ideala denez, $I(Y) + I(Z)$ batura ere $I(Y \cap Z)$-ren barruan dago. □

K gorputza finitua bada, orduan ez da egia $I(\mathbb{A}^n) = \{0\}$ denik. Izan ere, $|K| = q$ bada, $X_1^q - X_1, \ldots, X_n^q - X_n \in I(\mathbb{A}^n)$ dugu. Horren arrazoia ikusteko, ohartu $K^\times$ talde biderkakorrak $q-1$ elementu dituela. Orduan, $u \in K$, $u \neq 0$ elementu guztiek $u^{q-1} = 1$ betetzen dute.* Ondorioz, $u^q = u$ dugu $u \in K$ guztietarako eta, beraz, $X_1^q - X_1, \ldots, X_n^q - X_n \in I(\mathbb{A}^n)$.

Beste alde batetik, $I(Y) \cap I(Z)$ ebakidurak ez du zertan $I(Y)I(Z)$ biderkaduraren berdina izan. Adibidez, demagun K infinitua dela, eta hartu $Y, Z \subseteq \mathbb{A}^3$ modu honetan: Y multzoa, $X_1 = 0$ eta $X_2 = 0$ planoen bildura, eta Z, berriz, $X_1 = 0$ eta $X_3 = 0$ planoen bildura. Orduan, 2.19 teoremaren (iv) atala eta 2.18 adibidea erabiliz, $I(Y) = (X_1) \cap (X_2) = (X_1X_2)$ eta $I(Z) = (X_1) \cap (X_3) = (X_1X_3)$ lortzen dugu. Beraz, $I(Y) \cap I(Z) = (X_1X_2X_3)$ eta $I(Y)I(Z) = (X_1^2X_2X_3)$ desberdinak dira.

Oro har, ezin da ziurtatu $I(Y) + I(Z) = I(Y \cap Z)$ berdintza beteko denik. Adibidez, demagun K infinitua dela, eta hartu $Y, Z \subseteq \mathbb{A}^2$ honela: Y multzoa, $X_1 = 0$ zuzena, eta Z, berriz, Y-ren osagarria $\mathbb{A}^2$-n. Orduan, 2.18 adibidean ikusi dugun bezala, $I(Y) = (X_1)$ da. Bestetik, 2.8 ariketa erabiliz, $I(Z) = I(\mathbb{A}^2) = \{0\}$ dugu. Horrenbestez, $I(Y) + I(Z) = (X_1) + \{0\} = (X_1)$ lortzen dugu. Hala ere, $I(Y \cap Z) = I(\varnothing) = K[X_1, X_2]$ dugu, eta ez dator bat $I(Y) + I(Z)$-rekin.

Horrenbestez, bi eragile definitu ditugu, V eta I, honela ikus daitezkeenak:

$$\begin{array}{rccc} V : & \{K[X_1, \ldots, X_n]\text{-ren idealak}\} & \longrightarrow & \{\mathbb{A}^n\text{-ren multzo aljebraikoak}\} \\ & \mathfrak{a} & \longmapsto & V(\mathfrak{a}) \end{array}$$

eta

$$\begin{array}{rccc} I : & \{\mathbb{A}^n\text{-ren multzo aljebraikoak}\} & \longrightarrow & \{K[X_1, \ldots, X_n]\text{-ren idealak}\} \\ & Y & \longmapsto & I(Y). \end{array}$$

Aurretik aipatu dugun bezala, V supraiektiboa da, baina ez da injektiboa. Bestetik, garbi dago I ez dela supraiektiboa, $I(Y)$ ideal erradikala baita beti (eta ideal guztiak ez dira erradikalak). Galdera hauek sortzen zaizkigu:

*Gogoan izan taldeen propietate hau: G talde finitua bada, orduan $g^{|G|} = 1$ dugu $g \in G$ guztietarako.

(i) Ba al da I injektiboa?
(ii) Zer gertatzen da V eta I konposatzen baditugu?

2.20. Lema. *Izan bitez $S, T \subseteq K[X_1, \ldots, X_n]$ eta $Y, Z \subseteq \mathbb{A}^n$. Orduan:*

(i) *V-ren eta I-ren konposizioek partekotasunak gordetzen dituzte, hau da,*

$$S \subseteq T \Longrightarrow I(V(S)) \subseteq I(V(T))$$

eta

$$Y \subseteq Z \Longrightarrow V(I(Y)) \subseteq V(I(Z)).$$

(ii) *$S \subseteq I(V(S))$ eta $Y \subseteq V(I(Y))$.*
(iii) *$V(I(V(S))) = V(S)$ eta $I(V(I(Y))) = I(Y)$.*

Froga. (i) Hori garbi dago: V-k eta I-k partekotasunak aldatzen dituztenez, bata bestearekin konposatzean partekotasunak mantendu egingo dira.

(ii) Izan bedi $f \in S$. Frogatzeko $f \in I(V(S))$ dela, f $V(S)$-ko puntuen gainean anulatzen dela ikusi behar da. Baina, definizioz, espazio afineko puntu bat $V(S)$-n dago baldin eta puntu horretan S-ko polinomio guztiak anulatzen badira eta, bereziki, f puntu horretan anulatzen da, nahi bezala. Horrek $S \subseteq I(V(S))$ dela erakusten du. Antzera frogatzen da $Y \subseteq V(I(Y))$ partekotasuna.

(iii) Lehenengo berdintza baino ez dugu ikusiko, bestea era berean frogatzen da eta. Aurreko atalaren arabera, badakigu $S \subseteq I(V(S))$ dela. Partekotasun horri V aplikatzen badiogu, $V(I(V(S))) \subseteq V(S)$ lortzen dugu. Bestetik, aurreko atala $Y = V(S)$ multzoari aplikatzen badiogu, $V(S) \subseteq V(I(V(S)))$ alderantzizko partekotasuna dugu. □

Ez dira oro har betetzen $I(V(S)) = S$ eta $V(I(Y)) = Y$ berdintzak. Izan ere, $I(V(S))$ $K[X_1, \ldots, X_n]$-ren ideal erradikala denez, lehenengo berdintza ezin da bete S azpimultzoa ez bada ideal erradikala. Bestetik, $V(I(Y))$ $\mathbb{A}^n$-ren azpimultzo aljebraikoa denez, bigarren berdintza ere ez da inola ere beteko Y ez bada aljebraikoa.

Gauzak horrela, galdera hauek naturalak dira:

(i) $\mathfrak{a}$ $K[X_1, \ldots, X_n]$-ren ideal erradikala bada, ba al da $I(V(\mathfrak{a})) = \mathfrak{a}$? Zein da $I(V(S))$ ideala $S \subseteq K[X_1, \ldots, X_n]$ azpimultzo orokor baterako?
(ii) Y $\mathbb{A}^n$-ren azpimultzo aljebraikoa bada, betetzen da $V(I(Y)) = Y$? Zein da $V(I(Y))$ multzoa $Y \subseteq \mathbb{A}^n$ orokor baterako?

Has gaitezen (ii) ataleko galderetatik.

2.21. Teorema. *Izan bedi $Y \subseteq \mathbb{A}^n$. Orduan:*

(i) *Y multzo aljebraikoa bada, $V(I(Y)) = Y$ dugu.*
(ii) *Y orokorra bada, $V(I(Y)) = \overline{Y}$ dugu, Y-ren itxidura Zariskiren topologiarekiko.*

FROGA. (i) Baldin eta Y aljebraikoa bada, orduan $Y = V(S)$ idatz dezakegu, S polinomioen azpimultzo bat izanik. Orduan, 2.20 lema erabiliz, $V(I(Y)) = V(I(V(S))) = V(S) = Y$ dugu.

(ii) Alde batetik, 2.20 lemaren arabera $Y \subseteq V(I(Y))$ dugu. Orain, $V(I(Y))$ multzo itxia da Zariskiren topologiarekiko, aljebraikoa delako. Multzo baten itxidura multzo hori barruan duen multzo itxirik txikiena denez, $\overline{Y} \subseteq V(I(Y))$ dela ondorioztatzen dugu.

Beste alde batetik, $Y \subseteq \overline{Y}$ partekotasunari I eta V eragileak aplikatuz, bata bestearen atzetik, $V(I(Y)) \subseteq V(I(\overline{Y})) = \overline{Y}$ alderantzizko partekotasuna lortzen dugu. (Ohartu (i) atala erabili dugula $V(I(\overline{Y})) = \overline{Y}$ dela ziurtatzeko, $\overline{Y}$ multzo aljebraikoa dela kontuan hartuz.) □

2.22. Korolarioa. *$V \circ I$ konposizioa identitatea da multzo aljebraikoen gainean. Bereziki, I injektiboa da multzo aljebraikoen gainean.*

Lehenago esan dugun bezala, I ez da supraiektiboa, $I(Y)$ ideala erradikala baita beti. Beraz, I ez da bijektiboa. Hori konpontzeko asmotan, V eta I ideal erradikaletara murrizten ditugu:

$$\begin{array}{ccccc} V : & \{K[X_1,\dots,X_n]\text{-ren ideal erradikalak}\} & \longrightarrow & \{\mathbb{A}^n\text{-ren multzo aljebraikoak}\} \\ & \mathfrak{a} & \longmapsto & V(\mathfrak{a}), \end{array}$$

eta

$$\begin{array}{ccccc} I : & \{\mathbb{A}^n\text{-ren multzo aljebraikoak}\} & \longrightarrow & \{K[X_1,\dots,X_n]\text{-ren ideal erradikalak}\} \\ & Y & \longmapsto & I(Y). \end{array}$$

Ba al da orain I bijektiboa? Hori lortzeko modu bat V eta I (multzo aljebraikoetara eta ideal erradikaletara murriztuta) elkarren alderantzizkoak direla frogatzea da. Badakigu, 2.22 korolarioaren arabera, $V \circ I$ konposizioa identitatea dela multzo aljebraikoen gainean. Ba al da $I \circ V$ identitatea ideal erradikalen gainean? Baliokideki, betetzen da $I(V(\mathfrak{a})) = \mathfrak{a}$ berdintza, $\mathfrak{a}$ $K[X_1,\dots,X_n]$-ren ideal erradikala denean?

2.23. Teorema (Hilberten Nullstellensatza, bertsio gogorra)**.** *Izan bedi $\mathfrak{a}$ $K[X_1,\dots,X_n]$-ren ideala, K gorputza* aljebraikoki itxia *izanik. Orduan, $I(V(\mathfrak{a})) = \operatorname{rad}\mathfrak{a}$ dugu. Bereziki, $\mathfrak{a}$ erradikala bada, $I(V(\mathfrak{a})) = \mathfrak{a}$ dugu.*

Nullstellensatzak huts egiten du K ez bada aljebraikoki itxia. Kasu horretan, $p \in K[X]$ polinomio irreduzible bat har dezakegu, $\deg p \geq 2$ izanik. Orduan, $\mathfrak{a} = (p)$ $K[X]$-ren ideal erradikala da, baina

$$I(V(\mathfrak{a})) = I(V(p)) = I(\varnothing) = K[X_1,\dots,X_n] \neq \mathfrak{a}.$$

Hilberten Nullstellensatzaren froga honako emaitza honetan oinarritzen da, Nullstellensatzaren "bertsio ahul" deitutakoa.

2.24. Teorema (Hilberten Nullstellensatza, bertsio ahula)**.** *Izan bedi* $\mathfrak{a}$ $K[X_1, \ldots, X_n]$*-ren ideal propioa,* K *gorputza* aljebraikoki itxia *izanik. Orduan,* $V(\mathfrak{a})$ *multzo aljebraikoa ez da hutsa.*

Froga. Lehenengo eta behin, $\mathfrak{a}$ $K[X_1, \ldots, X_n]$-ren ideal propioa denez, $\mathfrak{m}$ ideal maximal baten barruan dago, 1.40 teorema erabiliz. Orain, K aljebraikoki itxia denez, 1.93 teoremaren arabera badakigu $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$ modukoa dela. Beraz, V aplikatuz

$$\{(a_1, \ldots, a_n)\} = V(\mathfrak{m}) \subseteq V(\mathfrak{a})$$

lortzen dugu, eta $V(\mathfrak{a})$ ez da hutsa. □

Garbi dago Nullstellensatzaren bertsio ahula bertsio gogorraren ondorioa dela: $V(\mathfrak{a}) = \varnothing$ balitz, $\mathfrak{a}$ ideal propioa izanik, orduan $I(V(\mathfrak{a})) = I(\varnothing) = K[X_1, \ldots, X_n] \neq \operatorname{rad} \mathfrak{a}$ izango genuke,* bertsio gogorraren kontra. Egia esan, ahul/gogor bereizketa bi bertsio horien artean itxurazkoa baino ez da, bertsio gogorra ahularen ondorioz frogatuko baitugu.

Bertsio ahulean garbiago ikusten da zein arrazoirengatik deitzen zaion *Nullstellensatz* teorema horri. Alemanez, *satz* hitzaren esanahia teorema da, *null* zero da eta *stellen*, berriz, posizioak. Beraz, *Nullstellensatz* hitzaren itzulpena zeroen teorema da, eta hori da bertsio ahulak ziurtatzen duena: ideal propio batek zeroak dituela beti. Ohartu emaitza hori gorputz aljebraikoki itxiaren definizioaren orokorpen modura ikus daitekeela, indeterminatu bat baino gehiagoren kasura. Izan ere, definizioz, gorputz bat aljebraikoki itxia da edozein polinomio ez-konstantek zeroak dituenean eta, $K[X]$ ideal nagusietako domeinuan, ideal propioak $\{0\}$ eta (f) modukoak dira, $f \in K[X]$ ez-konstantea izanik.

Bertsio gogorraren froga ikusteko, bertsio ahularen korolario hau eskura izatea komeni zaigu.

2.25. Korolarioa. *Izan bitez* K *gorputz* aljebraikoki itxia *eta*

$$\begin{cases} f_1(X_1, \ldots, X_n) = 0 \\ \qquad\qquad\qquad \vdots \\ f_r(X_1, \ldots, X_n) = 0 \end{cases}$$

ekuazio polinomikoen sistema bat K*-ren gainean. Orduan, baliokideak dira:*

(i) *Sistema horrek soluzioak ditu.*
(ii) $(f_1, \ldots, f_r)$ *ideala propioa da* $K[X_1, \ldots, X_n]$*-n.*
(iii) *Ezin da* 1 *konstantea idatzi* $f_1, \ldots, f_r$ *polinomioen multiploen batura gisa.*

*Ohartu, $\mathfrak{a}$ $K[X_1, \ldots, X_n]$-ren ideal propioa izanez gero, $\operatorname{rad} \mathfrak{a} \neq K[X_1, \ldots, X_n]$ dela. Izan ere, berdintza beteko balitz, $1 \in \operatorname{rad} \mathfrak{a}$ izango genuke eta, erradikalaren definizioagatik, $1 \in \mathfrak{a}$. Hori ez da posible, $\mathfrak{a}$ propioa baita.

FROGA. Badakigu $\mathfrak{a}$ ideal bat eraztun osoarekin bat datorrela baldin eta soilik baldin $1 \in \mathfrak{a}$ bada. Beraz, garbi dago (ii) eta (iii) baliokideak direla. Jarri $\mathfrak{a} = (f_1, \ldots, f_r)$. Orduan, (i) ataleko baieztapena $V(\mathfrak{a}) \neq \varnothing$ modura idatz daiteke. Beraz, (ii)⇒(i) inplikazioa Nullstellensatzaren bertsio ahula baino ez da. Bestalde, $V(\mathfrak{a}) \neq \varnothing$ bada, orduan $\mathfrak{a}$-k propioa izan behar du, $V(K[X_1, \ldots, X_n]) = \varnothing$ baita. □

Eman dezagun azkenik Nullstellensatzaren bertsio gogorraren froga, bertsio ahulean oinarrituz.

NULLSTELLENSATZAREN BERTSIO GOGORRAREN FROGA. Alde batetik, 2.20 lemaren arabera, badakigu $\mathfrak{a} \subseteq I(V(\mathfrak{a}))$ partekotasuna betetzen dela. Kontuan izanik $I(V(\mathfrak{a}))$ ideal erradikala dela, $\operatorname{rad} \mathfrak{a} \subseteq I(V(\mathfrak{a}))$ lortzen dugu.

Ikus dezagun alderantzizko partekotasuna. Horretarako, $f \in I(V(\mathfrak{a}))$ bada, frogatu behar dugu badagoela $m \geq 1$, non $f^m \in \mathfrak{a}$ baita. Nabaria da nahikoa dela $f \neq 0$ den kasua aztertzea. Zein da $f \in I(V(\mathfrak{a}))$ baldintzaren esanahia? Zehatz-mehatz, $\mathfrak{a}$-ko polinomioak anulatzen diren puntu guztietan f polinomioa ere anulatzen dela. Bestalde, Hilberten oinarriaren teorema erabiliz, $\mathfrak{a} = (f_1, \ldots, f_r)$ idatz dezakegu.

Orain, "Rabinovich-en trukua" delakoa erabiliko dugu. Horretarako, X_{n+1} indeterminatu berri bat sartzen dugu, eta honako sistema hau azaltzen dugu:

$$\begin{cases} f_1(X_1, \ldots, X_n) = 0 \\ \vdots \\ f_r(X_1, \ldots, X_n) = 0 \\ 1 - f(X_1, \ldots, X_n)X_{n+1} = 0. \end{cases}$$

Kontuan hartuz f_1, …, f_r anulatzen diren puntu guztietan f ere anulatzen dela, ohartzen gara sistema horrek ez duela soluziorik. Beraz, Nullstellensatzaren bertsio ahularen arabera (hobeto esanda, horren ondorioa den 2.25 korolarioaren arabera), 1 polinomio konstantea sistema horretan agertzen diren polinomioen multiploen batura da. Hau da, existitzen dira $q_0, \ldots, q_r \in K[X_1, \ldots, X_{n+1}]$, non

$$1 = q_0(X_1, \ldots, X_{n+1})(1 - f(X_1, \ldots, X_n)X_{n+1}) + q_1(X_1, \ldots, X_{n+1})f_1(X_1, \ldots, X_n) + \cdots + q_r(X_1, \ldots, X_{n+1})f_r(X_1, \ldots, X_n)$$

baita. Orain, berdintza honetan $X_{n+1} \mapsto 1/f(X_1, \ldots, X_n)$ ordezkapena eginez,

$$1 = \frac{q_1^*(X_1, \ldots, X_n)f_1(X_1, \ldots, X_n) + \cdots + q_r^*(X_1, \ldots, X_n)f_r(X_1, \ldots, X_n)}{f^m(X_1, \ldots, X_n)}$$

lortzen dugu, $q_1^*, \ldots, q_r^* \in K[X_1, \ldots, X_n]$ polinomio batzuetarako eta m berretzaileren baterako. Ondorioz,

$$f^m = q_1^* f_1 + \cdots + q_r^* f_r \in (f_1, \ldots, f_r) = \mathfrak{a},$$

nahi bezala. □

Orain, Nullstellensatzaren laguntzaz, I eta V eragileen funtsezko propietate hau eman dezakegu.

2.26. Teorema ($I-V$ korrespondentzia)**.** *Izan bedi K gorputz* aljebraikoki itxia. *Orduan, I eta V eragileak elkarren alderantzizkoak dira $\mathbb{A}^n$-ren multzo aljebraikoetara eta $K[X_1,\dots,X_n]$-ren ideal erradikaletara murrizten ditugunean eta, beraz, bijekzio bat eratzen dute bi multzo horien artean. Gainera, bijekzio horren bitartez $\mathbb{A}^n$-ko puntuak $K[X_1,\dots,X_n]$-ren ideal maximalekin lotuta daude.*

Froga. Alde batetik, K gorputza edozein izanda ere, Y multzo aljebraikoa bada $V(I(Y))=Y$ dugu, 2.21 teoremaren arabera. Bestetik, Nullstellensatza aplikatuz, $I(V(\mathfrak{a}))=\mathfrak{a}$ dugu $\mathfrak{a}$ $K[X_1,\dots,X_n]$-ren ideal erradikala bada, K aljebraikoki itxia delako. Horrek I eta V eragileak elkarren alderantzizkoak direla frogatzen du. Azkenik, 1.93 teoremaren arabera, $K[X_1,\dots,X_n]$-ren ideal maximalak $\mathfrak{m}=(X_1-a_1,\dots,X_n-a_n)$ motakoak dira, $(a_1,\dots,a_n)\in\mathbb{A}^n$ izanik. Kontuan hartuz $V(\mathfrak{m})=\{(a_1,\dots,a_n)\}$ dela, bijekzio bat lortzen dugu ideal maximalen eta puntu afinen artean. □

$I-V$ korrespondentziaren bitartez ideal erradikalak multzo aljebraiko guztiekin bijekzioan daude eta ideal maximalak, berriz, puntuekin lotuta. Orduan, galdera hau logikoa da: zein multzo aljebraikorekin daude lotuta $K[X_1,\dots,X_n]$-ren ideal lehenak? Horren erantzuna hurrengo atalean ikusiko dugu.

2.27. Oharra. Izan bedi $Y\subseteq\mathbb{A}^n$ multzo aljebraikoa. Orduan, definizioz, existitzen da $\mathfrak{a}$ polinomioen ideal bat, non $Y=V(\mathfrak{a})$ baita. Hala ere, $\mathfrak{a}$ hori ez da bakarra, eta $Y=V(\mathfrak{a})=V(\mathfrak{b})=V(\mathfrak{c})=\cdots$ izan dezakegu ideal desberdinetarako. $I-V$ korrespondentziak dio ideal horietatik *erradikala den bakar bat* dagoela, K aljebraikoki itxia bada. Adibidez, $p\in K[X_1,\dots,X_n]$ irreduziblea bada, orduan $V(p)=V(p^2)=\cdots=V(p^n)=\cdots$ dugu, baina (p) bakarrik da erradikala.

2.3. Barietateak eta osagai irreduzibleak

Zenbakien artean, zenbaki lehenak atomoak bezalakoak dira: ezin dira deskonposatu faktore ez-tribialetan. Gainera, edozein zenbaki arrunt zenbaki lehenak erabiliz eraiki daiteke, biderketaren bidez. Azken atal honetan ikusten dugun bezala, multzo aljebraikoekin antzeko zerbait gertatzen da, kasu honetan bildura jokatuz biderketaren papera.

2.28. Notazioa. Hemendik aurrera, V letra erabiliko dugu multzo aljebraikoak idazteko, eta Y $\mathbb{A}^n$-ren azpimultzo orokorretarako gordeko dugu.

2.29. Definizioa. Izan bedi V multzo aljebraiko *ez-hutsa*. Orduan, V *barietatea* edo *irreduziblea* dela esango dugu, ezin bada jarri bi multzo aljebraiko txikiagoren bildura gisa, hau da, inplikazio hau betetzen bada:

$$V=V_1\cup V_2,\ V_1 \text{ eta } V_2 \text{ aljebraikoak } \implies V_1=V \text{ edo } V_2=V.$$

Adibidez, $\operatorname{char} K \neq 2$ bada, orduan $Y^2 = X^2$ ekuazioa duen $\mathbb{A}^2$-ko kurba ez da barietatea, bi zuzenen bildura baita: $V(Y^2-X^2) = V(Y-X) \cup V(Y+X)$. (Ohartu $\operatorname{char} K \neq 2$ baldintza funtsezkoa dela bildurako bi multzo aljebraikoak desberdinak izan daitezen.) Bestalde, puntuak multzo aljebraikoak direnez, $\mathbb{A}^n$-ren azpimultzo finituen artean, puntu isolatuak baino ez dira barietateak. Nola jakin dezakegu, oro har, multzo aljebraiko bat barietatea den edo ez? Hurrengo teoreman ematen dugu erantzuna.

2.30. Lema. *Izan bitez V_1 eta V_2 multzo aljebraiko afinak, K gorputza* edozein *izanik. Orduan, $V_1 \subsetneq V_2$ bada, $I(V_2) \subsetneq I(V_1)$ dugu.*

Froga. Badakigu I-k partekotasunak aldatzen dituela. Beraz, $I(V_2) \subseteq I(V_1)$ dugu. Beteko balitz $I(V_2) = I(V_1)$, orduan $V(I(V_2)) = V(I(V_1))$ ere izango genuke eta, 2.21 teorema aplikatuz, $V_1 = V_2$ lortuko genuke, V_1 eta V_2 aljebraikoak baitira. Hori kontraesan bat denez, $I(V_2) \subsetneq I(V_1)$ izan behar dugu. □

2.31. Teorema. *Izan bedi $V \subseteq \mathbb{A}^n$ multzo aljebraikoa, K gorputza* edozein *izanik. Orduan, V barietatea da baldin eta soilik baldin $I(V)$ ideal lehena bada.*

Froga. $\Rightarrow$) Ikus dezagun $I(V)$ ideal lehena dela. Lehenengo eta behin, ohartu $I(V) \neq K[X_1, \ldots, X_n]$ dela. Izan ere, berdintza beteko balitz, orduan $V = V(I(V)) = V(K[X_1, \ldots, X_n]) = \varnothing$ izango genuke, hipotesiaren kontra. (Lehenengo berdintza V aljebraikoa izateagatik betetzen da.) Orain, demagun $fg \in I(V)$ dela, eta frogatu dezagun $f \in I(V)$ edo $g \in I(V)$ dela. Horretarako, ohartu

$$\begin{aligned} fg \in I(V) &\implies V = V(I(V)) \subseteq V(fg) = V(f) \cup V(g) \\ &\implies V = (V \cap V(f)) \cup (V \cap V(g)) \end{aligned}$$

dugula. Kontuan harturik V barietatea dela, $V = V \cap V(f)$ edo $V = V \cap V(g)$ izan behar du. Lehenengo kasua betetzen bada, orduan $V \subseteq V(f)$ dugu eta, ondorioz, $f \in I(V(f)) \subseteq I(V)$. Bigarren kasuan, $g \in I(V)$ lortzen dugu guztiz era berean. Horrenbestez, frogaturik gelditzen da lehenengo inplikazioa.

$\Leftarrow$) Lehenengo eta behin, ohartu V multzoa ez dela hutsa. Izan ere, $V = \varnothing$ balitz, orduan $I(V) = I(\varnothing) = K[X_1, \ldots, X_n]$ ez litzateke ideal lehena izango, eta hori kontraesan bat da. Orain, demagun $V = V_1 \cup V_2$ dela, V_1 eta V_2 aljebraikoak izanik, eta ikus dezagun $V_1 = V$ edo $V_2 = V$ dela. Absurdora eramanez, $V_1 \subsetneq V$ eta $V_2 \subsetneq V$ dela pentsa dezakegu. Hala bada, aurreko lema erabiliz, $I(V) \subsetneq I(V_1)$ eta $I(V) \subsetneq I(V_2)$ dugu. Aukeratu $f \in I(V_1) \setminus I(V)$ eta $g \in I(V_2) \setminus I(V)$ polinomioak. Orduan, f V_1-eko puntuen gainean anulatzen da eta g, berriz, V_2-koen gainean. Ondorioz, fg biderkadura $V = V_1 \cup V_2$ gainean anulatzen da, hau da, $fg \in I(V)$ dugu. Hori ez da posible, f eta g ez daudelako $I(V)$-n, eta $I(V)$ ideal lehena delako hipotesiaren arabera. □

2.32. Korolarioa. *Izan bedi K gorputz* aljebraikoki itxia. *Orduan $I - V$ korrespondentziaren bitartez, ideal lehenak barietateekin elkartuta daude.*

2.33. Adibideak. Adibide hauetan K gorputza aljebraikoki itxia da, Nullstellensatza erabili ahal izateko.

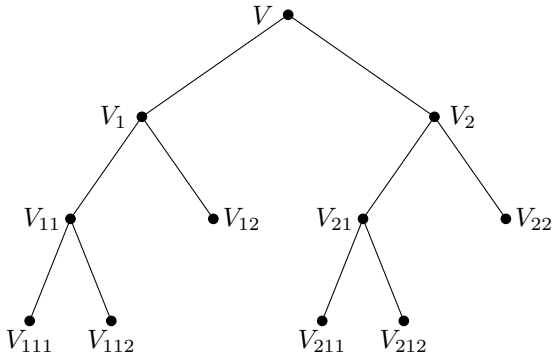
1) $V = V(Y - X^2)$ parabola barietatea da. Izan ere, $(Y - X^2)$ ideal lehena da eta, bereziki, erradikala. Beraz, $I(V) = I(V(Y - X^2)) = \mathrm{rad}(Y - X^2) = (Y - X^2)$ ideal lehena da eta V barietatea da.

2) Oro har, $V(f)$ hipergainazala barietatea da baldin eta soilik baldin f polinomio irreduzible baten berretura bada. Hori ikusteko, demagun $f = p_1^{e_1} \dots p_r^{e_r}$ dela f-ren irreduzibleetako faktorizazioa. Orduan, $I(V(f)) = \mathrm{rad}(f) = (p_1 \dots p_r)$ dugu, eta ideal hori lehena da baldin eta soilik baldin $p_1 \dots p_r$ irreduziblea bada, hots, $r = 1$ bada. Ondorioz, $V(f)$ barietatea da zehatz-mehatz f polinomio irreduzible baten berretura denean.

3) $V_1 = V(Y - X^2)$ eta $V_2 = V(Z - X^2)$ paraboloideen ebakidura barietatea da. Izan ere, $V_1 \cap V_2 = V(Y - X^2, Z - X^2)$ dugu eta $(Y - X^2, Z - X^2)$ ideal lehena da.

Demagun K gorputza aljebraikoki itxia dela. Aurreko adibideetan ikusi dugunez, $\mathfrak{a}$ ideal lehena bada, orduan $V(\mathfrak{a})$ barietatea da, $I(V(\mathfrak{a})) = \mathfrak{a}$ delako. Baina $\mathfrak{a}$ ez bada ideal lehena, ezin dugu besterik gabe esan $V(\mathfrak{a})$ barietatea ez denik. Hori ikusteko, $\mathfrak{a} = ((Y - X^2)^2)$ har dezakegu, adibidez. Orduan, $V(\mathfrak{a}) = V(Y - X^2)$ barietatea da, nahiz eta $\mathfrak{a}$ ideal lehena ez izan. Horren atzean dagoen arrazoia hau da: V multzo aljebraikoa bada, orduan $\mathfrak{a}$ ideal askorekin izan dezakegu $V = V(\mathfrak{a})$. Ideal horietariko bakar bat da erradikala, eta horixe da $I(V)$. Azken teoremak dioenez, V barietatea den edo ez jakiteko, $I(V)$ ideala aztertu behar dugu, eta ez $V = V(\mathfrak{a})$ idazteko balio duen edozein ideal.

Multzo aljebraiko bat ez bada barietatea, bi multzo aljebraiko txikiagoren bildura gisa deskonposatzen da: $V = V_1 \cup V_2$. Bi multzo horietako bat ez bada barietatea, are gehiago deskonposa dezakegu V multzoa; adibidez, $V_1 = V_{11} \cup V_{12}$ eta $V_2 = V_{21} \cup V_{22}$ izan dezakegu. Berriro ere, multzo berri horietako bat ez bada barietatea, gehiago deskonposa dezakegu. Deskonposizio-prozesu hori zuhaitz baten bitartez irudika daiteke:



Bukatuko da prozesu hori edo egon gaitezke agertzen diren multzo aljebraikoak etengabe deskonposatzen bildura modura? Bestela esanda, luza daiteke deskonposizioaren zuhaitza infinituraino?

Hurrengo teoreman ikusten dugunez, prozesua beti bukatuko da eta, beraz, hasierako multzoa barietate kopuru finitu baten bildura gisa adierazirik gelditukо da, zenbaki osoak zenbaki lehenen biderkadura gisa faktorizaturik jar daitezkeen bezala. Zenbaki osoen kasuan, faktorizazioa bakarra da. Gertatzen da gauza bera multzo aljebraiko baten barietateetako deskonposizioarekin?

2.34. Teorema. *Izan bedi $V \subseteq \mathbb{A}^n$ multzo aljebraiko ez-hutsa. Orduan:*

(i) *$V = V_1 \cup \cdots \cup V_r$ idatz daiteke, V_i guztiak barietateak izanik.*

(ii) *Deskonposizio hori ez bada* erredundantea*, hau da, $V_i \not\subseteq V_j$ betetzen bada $i \neq j$ guztietarako, orduan bakarra da, ordena salbu. Hori dela eta, V_i barietateei V-ren* osagai irreduzible *deitzen zaie.*

Froga. (i) Aurretik aipatu dugun bezala, deskonposizioaren zuhaitza infinituraino luzatzeko posibilitatea baztertu behar dugu. Bestela, zuhaitzak adar infinitu bat izango du. Orduan, adar horretako erpinetan agertzen diren multzo aljebraikoek kate hertsiki beherakor infinitu bat osatuko dute:

$$V = W_0 \supsetneq W_1 \supsetneq W_2 \supsetneq \cdots \supsetneq W_i \supsetneq \cdots .$$

Kate horri I eragilea aplikatuz eta 2.30 lema kontuan hartuz, $K[X_1, \ldots, X_n]$-ren idealen kate hertsiki gorakor bat dugu,

$$I(V) = I(W_0) \subsetneq I(W_1) \subsetneq I(W_2) \subsetneq \cdots \subsetneq I(W_i) \subsetneq \cdots ,$$

eta hori ezinezkoa da, Hilberten oinarriaren teorema dela eta. Horrek multzo aljebraiko baten deskonposizioaren existentzia frogatzen du, barietateen bildura gisa. Deskonposizioak erredundantziarik ez izatea nahi badugu, nahikoa da $V_i \subseteq V_j$ betetzen dela ikusten dugun bakoitzean V_i multzoa deskonposiziotik kentzea.

(ii) Demagun $V = V_1 \cup \cdots \cup V_r = W_1 \cup \cdots \cup W_s$ dela, bi deskonposizioak ez-erredundanteak izanik. Har dezagun V_1 multzo aljebraikoa eta ikus dezagun badagoela $i \in \{1, \ldots, s\}$, non $V_1 = W_i$ baita. Hori bi deskonposizioetako multzo aljebraiko guztiekin egin daitekeenez, alde bateko eta besteko multzoak bat datozela ondorioztatuko dugu, eta teorema frogaturik gelditukо da. Ohartu

$$V_1 = V_1 \cap V = V_1 \cap (W_1 \cup \cdots \cup W_s) = (V_1 \cap W_1) \cup \cdots \cup (V_1 \cap W_s)$$

dugula. Orain, V_1 barietatea izateagatik, existitzen da i non $V_1 = V_1 \cap W_i$ baita, hau da, $V_1 \subseteq W_i$ baita. Argudio bera W_i-ri aplikatuz, lortzen dugu badagoela j, non $W_i \subseteq V_j$ baita. Orduan, $V_1 \subseteq V_j$ dugu eta, $V = V_1 \cup \cdots \cup V_r$ deskonposizioan erredundantziarik ez dagoenez, $j = 1$ dugu nahitaez. Beraz, $V_1 \subseteq W_i$ eta $W_i \subseteq V_1$ dugu, eta ondorioz $V_1 = W_i$, nahi bezala. □

Adibidez, K aljebraikoki itxia bada, $V(Y^2 - X^2)$-ren osagai irreduzibleak $V(Y - X)$ eta $V(Y + X)$ dira.

2.35. Korolarioa. *Izan bitez K gorputz aljebraikoki itxia eta $\mathfrak{a}$ $K[X_1, \ldots, X_n]$-ren ideal erradikal propioa. Orduan:*

(i) *$\mathfrak{a} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$ idatz daiteke, $\mathfrak{p}_i$ guztiak ideal lehenak izanik.*

(ii) *Deskonposizio hori ez bada* erredundantea*, hau da,* $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ *betetzen bada* $i \neq j$ *guztietarako, orduan bakarra da, ordena salbu. Hori dela eta,* $\mathfrak{p}_i$ *ideal lehenei* $\mathfrak{a}$*-ren* osagai lehen *deitzen zaie.*

Froga. Hori aurreko teoremaren "itzulpen" zuzena da, $I - V$ korrespondentzia erabiliz. Gogoan izan korrespondentzia horren bitartez multzo aljebraikoak ideal erradikalekin elkartuta daudela eta barietateak, berriz, ideal lehenekin lotuta. □