Eötvös Loránd Tudományegyetem
Természettudományi Kar

Fehér Zsombor

Affin algebrai görbék

BSc Matematikus Szakdolgozat

Témavezető:

Némethi András

Geometriai Tanszék

Budapest, 2018

Tartalomjegyzék

Bevezetés

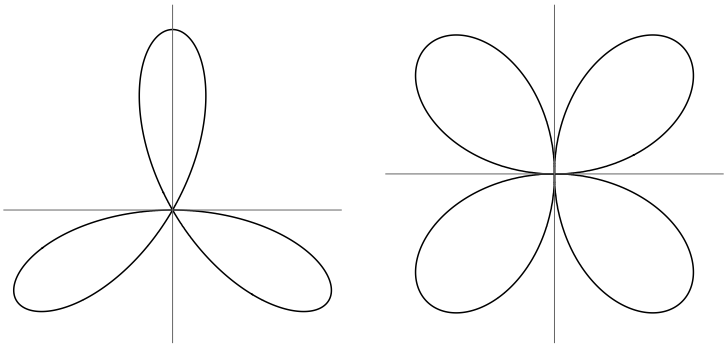
Az algebrai geometria tárgyalására többféle lehetőség van. Mi most egy olyan utat választunk, amely teljesen precíz algebrai alapokra helyezi az elméletet, és mentes mindenfajta szemléletes magyarázkodástól. Aki ehelyett inkább a geometriai tartalomra kíváncsi, és nem zavarja, hogy gyakran a szemléletre kell hagyatkoznia, annak bátran ajánlom a [2] könyvet.

Dolgozatomban végig az [1] könyv felépítését követtem, azt kiegészítettem, egyes bizonyításoknál részletesebb magyarázatokkal. Mivel az [1]-ben rengeteg állítás feladat formájában van kitűzve, majd a nehezebb tételek bizonyításában rendszerint hivatkozni szokott a feladatokra, ezért a használni kívánt feladatokat be is bizonyítottam.

Motiváló példaként tekintsük az

$$F = (X^2 + Y^2)^2 + 3X^2Y - Y^3, \quad G = (X^2 + Y^2)^3 - 4X^2Y^2$$

polinomokat. Lerajzolva a síkon ezek gyökhelyeit, a lenti két ábrát kapjuk. Megfigyelhetjük, hogy mintha F az origón 3-szor is keresztülmenne, G pedig 4-szer. Úgy látjuk, hogy mintha az origóban is definiálni lehetne a görbék érintőit, F-nek 3 különböző érintőjét, míg G-nek csak 2 különböző érintőjét, de mintha mindkettő kétszeres multiplicitással szerepelne. Azt is megkérdezhetjük, hányszoros multiplicitással metszik egymást az F és G görbék az origóban. Ehhez persze definiálnunk kell, mit értünk metszési multiplicitás alatt, melyet egy rezultánssal akár most rögtön megtehetnénk, de egy másik, sokkal organikusabb definícióhoz fogunk eljutni a dolgozat végén.



Az első fejezetben az n-dimenziós affin algebrai halmazokat vizsgáljuk. Definiáljuk a V és I operátorokat, majd a fejezet végére, a Nullstellensatz segítségével belátjuk, hogy ezek egymás inverzei valamilyen értelemben.

A második fejezet első felében irreducibilis algebrai halmazok koordinátagyűrűit, lokális gyűrűit tanulmányozzuk. A második felében tovább folytatjuk az algebrai alapok előkészítését a következő fejezethez.

A harmadik fejezetben definiáljuk végre az affin síkgörbéket, szinguláris pontokat, érintőket. Megmutatjuk, hogy a görbe egy pontjának multiplicitása és a lokális gyűrűje szoros kapcsolatban van. Megfogalmazunk tulajdonságokat, amit két görbe metszési multiplicitásától elvárunk, majd algebrai eszközeinkkel felvértezve, összes eddigi tudásunkat felhasználva bebizonyítjuk, hogy ezeknek a feltételeknek pontosan egy definíció tesz eleget.

Ezek után természetes módon következne például Bézout tétele, amely azonban a projektív görbék sajátossága, így erre már nem térünk ki. Az érdeklődőknek ajánljuk [1] további fejezeteit.

1. fejezet

Algebrai halmazok

1.1. Algebrai előismeretek

Röviden áttekintjük a szükséges algebrai előismereteket. Ezen fogalmak és a kimondott állítások bizonyítása megtalálható például a [3] könyvben.

Az 1.8. alfejezettől kezdődően k mindig algebrailag zárt testet jelöl. A természetes számok halmaza $\mathbb{N} = \{0, 1, \ldots\}$. Struktúrák izomorfiáját néha $\cong$ jelöli.

A továbbiakban *gyűrű* alatt mindig kommutatív, egységelemes gyűrűt értünk. Gyűrűk közötti *homomorfizmus* tehát egy olyan művelettartó leképezés, mely az egységelemet az egységelembe viszi. Egy R gyűrű *hányadosteste* egy olyan K test, melyre $R \subset K$, és minden $x \in K$ előáll $x = a/b$, $a, b \in R$ alakban.

1.1.1. Tétel. *Ha az R gyűrű nullosztómentes, akkor létezik hányadosteste, ami izomorfia erejéig egyértelmű.*

Az R feletti n-változós *polinomok* halmazát $R[X_1, \ldots, X_n]$ jelöli. Ez izomorf $R[X_1, \ldots, X_{n-1}][X_n]$-nel. $n = 1, 2, 3$ esetén gyakran az $R[X]$, $R[X, Y]$, $R[X, Y, Z]$ jelölésekkel élünk. Egy $X_1^{i_1} \ldots X_n^{i_n}$ *monom* foka $i_1 + \ldots + i_n$. Egy polinom *homogén*, ha benne minden monom foka azonos. Minden $F \in R[X_1, \ldots, X_n]$ előáll $F = F_0 + F_1 + \ldots + F_d$ alakban, ahol $\deg F_i = i$ homogén polinomok. Ha $F_d \neq 0$, akkor a polinom *foka* $\deg F = d$, $F = 0$ foka 0. F *konstans tagja* F_0, és F *konstans*, ha $F = F_0$. Ha R nullosztómentes, $0 \neq F, G \in R[X]$, akkor $\deg(FG) = \deg F + \deg G$. Az $F = a_d X^d + \ldots + a_0 \in R[X]$ polinom *főegyütthatójának* hívjuk az a_d-t, ha $a_d \neq 0$, $F = 0$ főegyütthatója 0. Az F *normált*, ha $a_d = 1$. Ha K test, akkor a $K[X_1, \ldots, X_n]$ gyűrű hányadostestét $K(X_1, \ldots, X_n)$ jelöli, és a K feletti n-változós *racionális törtfüggvények testének* hívjuk.

Ha $r_1, \ldots, r_n \in R$, akkor $F(r_1, \ldots, r_n) \in R$ jelöli az F polinom helyettesítési értékét. Általánosabban, ha $s_1, \ldots, s_n \in S$, és van egy természetes $\varphi\colon R \to S$ gyűrűhomomorfizmus, akkor létezik egy olyan $\widetilde{\varphi}\colon R[X_1, \ldots, X_n] \to S$ homomorfizmus, melyre $\widetilde{\varphi}(r) = \varphi(r)$ minden $r \in R$-re, és $\widetilde{\varphi}(X_i) = s_i$. Ekkor $F(s_1, \ldots, s_n)$ jelöli a $\widetilde{\varphi}(F) \in S$ elemet.

Az $a, b \in R$ elemekre a *osztója* b-nek, $a \mid b$, ha létezik $t \in R$, hogy $at = b$. Az $a \in R$ elem *egység*, ha minden elemnek osztója. Az a *irreducibilis*, ha nem 0, nem egység, és $a = bc$, $b, c \in R$ esetén b vagy c egység. Az $a, b \in R$ elemek egymással *relatív prímek*, ha minden közös osztójuk egység. Az R nullosztómentes gyűrű *alaptételes*

(UFD), ha minden nem nulla elem felírható irreducibilis elemek szorzataként, és ez a felírás sorrendtől és egységszeresektől eltekintve egyértelmű. Az $a \in R$ *prímtényezős felbontása* $a = p_1^{n_1} \dots p_r^{n_r}$, ahol $p_i \in R$ irreducibilis, n_i pozitív egész, és p_i nem egységszerese p_j-nek $(i \neq j)$.

1.1.2. Tétel (Gauss-lemma)**.** a) *Ha az R gyűrű hányadosteste K, és $F \in R[X]$ irreducibilis, akkor $K[X]$-ben is irreducibilis.*

b) *Ha $F, G \in R[X]$ relatív prímek, akkor $K[X]$-ben is relatív prímek.*

1.1.3. Tétel. a) *Ha R alaptételes gyűrű, akkor $R[X]$ is alaptételes.*

b) *Ha K test, akkor $K[X_1, \dots, X_n]$ alaptételes.*

I ideál az R gyűrűben, $I \lhd R$, ha I zárt az összeadásra, és minden $r \in R$-rel való szorzásra. Ha $\varphi\colon R \to S$ gyűrűhomomorfizmus, akkor *magja*, $\varphi^{-1}(0) = \operatorname{Ker} \varphi \lhd R$ ideál. φ képét $\operatorname{Im} \varphi$ jelöli. *I valódi*, ha $I \neq R$. *I maximális*, ha $I \subsetneq J \lhd R$ esetén $J = R$. *I prímideál*, ha $ab \in I$ esetén $a \in I$ vagy $b \in I$. Az $S \subset R$ halmaz által *generált* ideál $I = \{\sum_{i=1}^{n} a_i s_i \mid n \in \mathbb{N}, a_i \in R, s_i \in S\}$. Egy ideál *végesen generált*, ha véges $S = \{f_1, \dots, f_r\}$ halmaz generálja, ekkor azt írjuk, $I = (f_1, \dots, f_r)$.

Egy ideál *főideál*, ha egy elem generálja. Egy gyűrű *főideálgyűrű* (PID), ha minden ideálja főideál. $\mathbb{Z}$ és $K[X]$, ahol K test, főideálgyűrűk. Minden főideálgyűrű alaptételes. Az UFD-beli $I = (a)$ főideál pontosan akkor prímideál, ha a irreducibilis, 0, vagy egység.

Ha $I \lhd R$, akkor tekinthető az R/I *faktorgyűrű*, melynek elemei az ekvivalenciaosztályok az $a \sim b$, ha $a - b \in I$ ekvivalenciareláció mellett. Az a-t tartalmazó osztályt gyakran az a I-maradékjának hívjuk, és $a + I$-vel vagy $\overline{a}$-val jelöljük. R/I-n a műveleteket természetes módon úgy definiáljuk, hogy a $\pi\colon R \to R/I, a \mapsto \overline{a}$ leképezés gyűrűhomomorfizmus legyen. Ha $\varphi\colon R \to S$ szürjektív gyűrűhomomorfizmus, akkor φ indukál egy $R/\operatorname{Ker} \varphi \cong S$ izomorfizmust. Ha K test, $I \lhd K[X_1, \dots, X_n]$, akkor $\pi(K) \subset K[X_1, \dots, X_n]/I$ egy K-val izomorf részgyűrű, így $K[X_1, \dots, X_n]/I$ egy K feletti vektortérnek is tekinthető.

1.1.4. Állítás. *I pontosan akkor prímideál, ha R/I nullosztómentes. I pontosan akkor maximális ideál, ha R/I test. Minden maximális ideál prímideál.*

Az $a \in R$ elem *gyöke* az $F \in R[X]$ polinomnak, ha $F(a) = 0$. Ekkor $F = (X - a)G$ valamely (egyértelmű) $G \in R[X]$ polinommal. Ha R nullosztómentes és $F \in R[X]$ foka d, akkor F-nek legfeljebb d különböző gyöke lehet. A k test *algebrailag zárt*, ha minden $F \in k[X]$ nem konstans polinomnak van gyöke. Ekkor $F = c \prod_{i=1}^{d} (X - a_i)^{m_i}$ alakú, ahol $c, a_i \in k$, és m_i az a_i gyök *multiplicitása*. Ha $\deg F = d$, k algebrailag zárt, akkor multiplicitással számolva F-nek pontosan d gyöke van. A komplex számok halmaza algebrailag zárt. Minden algebrailag zárt test végtelen.

Ha R gyűrű, akkor az M *R-modulusnak* az $1 \cdot m = m$ feltételt is teljesítenie kell, ahol 1 az R egységeleme, $m \in M$. Ha $I \lhd R$, akkor I R-modulus az R-beli szorzással. Ha $R \subset S$ gyűrűk, akkor S R-modulus az S-beli szorzással. Ha M R-modulus, akkor $N \subset M$ *részmodulusa* M-nek, ha $an \in N$ minden $a \in R, n \in N$ esetén. Ha $S \subset M$ tetszőleges halmaz, akkor $\{\sum_{i=1}^{m} r_i s_i \mid m \in \mathbb{N}, r_i \in R, s_i \in S\}$ az S által *generált részmodulus*. Ha $S = \{s_1, \dots, s_n\}$ véges, akkor ezt $\sum_{i=1}^{n} Rs_i$-vel jelöljük. M *végesen generált*, ha $M = \sum_{i=1}^{n} Rs_i$ valamely $s_i \in M$ elemekre. Ha $N \subset M$ részmodulus,

akkor képezhető az M/N faktormodulus, és a $\varphi\colon M \to M/N$, $m \mapsto \overline{m}$ leképezés ekkor R-modulushomomorfizmus.

Ha R gyűrű, és $F \in R[X]$, $F = \sum_{i=0}^{d} a_i X^i$, akkor F X szerinti (parciális) *deriváltja* $\partial_X F = \sum_{i=1}^{d} a_i i X^{i-1}$. Ha $F \in R[X_1, \ldots, X_n]$, akkor $\partial_{X_i} F$ értelmezéséhez F-et $S[X_i]$-belinek tekintjük, ahol $S = R[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$. Ha $F \in R[X]$, $a \in R$, akkor $\partial_X(F(X+a)) = (\partial_X F)(X+a)$.

Ha $R_1, \ldots, R_n$ gyűrűk, akkor $R_1 \times \ldots \times R_n$ gyűrű a koordinátánkénti műveletekkel, ezt hívjuk a gyűrűk *direkt szorzatának*, és $\prod_{i=1}^{n} R_i$-vel is jelöljük. Ekkor a $\pi_i\colon \prod_{j=1}^{n} R_j \to R_i$, $(a_1, \ldots, a_n) \mapsto a_i$ természetes projekciók gyűrűhomomorfizmusok. Ha $\varphi_i\colon R \to R_i$ tetszőleges gyűrűhomomorfizmusok, akkor egyértelműen létezik egy olyan $\varphi\colon R \to \prod_{i=1}^{n} R_i$ homomorfizmus, melyre $\pi_i \circ \varphi = \varphi_i$ minden i-re. Ha $K \subset R_i$ test, és R_i véges dimenziós K felett, akkor $\dim_K \left(\prod_{i=1}^{n} R_i\right) = \sum_{i=1}^{n} \dim_K(R_i)$.

1.2. Affin algebrai halmazok

Definíció. a) Legyen k test, $n \geq 1$ egész szám. A k fölötti n-dimenziós *affin téren* a k-beli n-esek halmazát, azaz a $k \times \ldots \times k$ direkt szorzatot értjük, és $\mathbb{A}^n = \mathbb{A}^n(k)$-val jelöljük. $\mathbb{A}^n$ elemeit *pontoknak* hívjuk, $\mathbb{A}^1$ az affin egyenes, $\mathbb{A}^2$ az affin sík.

b) Egy $F \in k[X_1, \ldots, X_n]$ polinomnak a $P = (a_1, \ldots, a_n) \in \mathbb{A}^n(k)$ pont *gyöke* (F *eltűnik* P-ben), ha $F(P) = F(a_1, \ldots, a_n) = 0$.

c) Ha $\deg F \geq 1$, akkor az F gyökeinek $V(F)$ halmazát az F által definiált *hiperfelületnek* nevezzük. Ha $\deg F = 1$, akkor $V(F)$-et *hipersíknak* nevezzük, $n = 2$ esetén *egyenesnek*.

d) Általánosabban, ha $S \subset k[X_1, \ldots, X_n]$ polinomok tetszőleges halmaza, akkor

$$V(S) = \{P \in \mathbb{A}^n(k) \mid \forall F \in S\text{-re } F(P) = 0\}.$$

Tehát $V(S) = \bigcap_{F \in S} V(F)$. Ha $S = \{F_1, \ldots, F_r\}$, akkor a $V(F_1, \ldots, F_r) = V(\{F_1, \ldots, F_r\})$ jelöléssel élünk.

Definíció. A $V \subset \mathbb{A}^n$ ponthalmazt *affin algebrai halmaznak* hívjuk, ha $V = V(S)$ valamely S polinomhalmazra.

1.2.1. Állítás. a) *Ha $I \subset J$, akkor $V(I) \supset V(J)$.*

b) *Ha az $S \subset k[X_1, \ldots, X_n]$ által generált ideál $I \lhd k[X_1, \ldots, X_n]$, akkor $V(S) = V(I)$. Tehát minden algebrai halmaz előáll $V(I)$ alakban, ahol I ideál.*

c) *Ha $\{I_\alpha \mid \alpha \in A\}$ ideálok családja, akkor $V\left(\bigcup_{\alpha \in A} I_\alpha\right) = \bigcap_{\alpha \in A} V(I_\alpha)$. Tehát algebrai halmazok tetszőleges metszete is algebrai.*

d) *Ha F, G polinomok, $V(FG) = V(F) \cup V(G)$. Általában, ha I, J ideálok, $V(I) \cup V(J) = V(\{FG \mid F \in I, G \in J\})$. Tehát algebrai halmazok véges uniója is algebrai.*

e) *$V(0) = \mathbb{A}^n(k)$, $V(1) = \emptyset$, $V(X_1 - a_1, \ldots, X_n - a_n) = \{(a_1, \ldots, a_n)\}$. Tehát $\mathbb{A}^n$ bármely véges halmaza algebrai.*

Bizonyítás. (a) Ha P gyöke minden $F \in J$-nek, akkor minden $F \in I$-nek is.

(b) $V(S) \supset V(I)$ a) szerint. Ha $F \in I$, akkor $F = \sum_{i=1}^{r} a_i F_i$, ahol $a_i \in k[X_1, \ldots, X_n]$, $F_i \in S$, így ha P minden S-belinek gyöke, akkor F-nek is.

(c) P pontosan akkor gyöke minden $F \in \bigcup_{\alpha \in A} I_\alpha$-nak, ha minden α-ra gyöke minden $F \in I_\alpha$-nak.

(d) P pontosan akkor gyöke FG-nek, ha F-nek vagy G-nek gyöke. Ha $P \in V(I)$, akkor gyöke minden $F \in I$-nek, így gyöke minden FG-nek. Ha $P \in V(J)$, ugyancsak gyöke minden FG-nek. Megfordítva, ha $P \notin V(I) \cup V(J)$, akkor van olyan $F \in I$, és van olyan $G \in J$, melyeknek P nem gyöke. Ekkor P nem gyöke FG-nek sem.

(e) A 0 polinomnak minden pont gyöke, az 1-nek semelyik. Az $X_i - a_i$ polinomok egyetlen közös gyöke az $(a_1, \ldots, a_n)$ pont. Így d) szerint minden véges ponthalmaz algebrai. □

1.2.2. Példák. a) $\mathbb{A}^1$ algebrai részhalmazai a véges halmazok, és $\mathbb{A}^1$.

b) $V = \{(t, t^2, t^3) \in \mathbb{A}^3(k) \mid t \in k\}$ algebrai halmaz.

c) $V = \{(\cos t, \sin t) \in \mathbb{A}^2(\mathbb{R}) \mid t \in \mathbb{R}\}$ algebrai halmaz.

d) Legyen $C = V(F) \subset \mathbb{A}^2$ kétdimenziós affin hiperfelület, $\deg F = n$, és $L \subset \mathbb{A}^2$ egy egyenes. Ha $L \not\subset C$, akkor $L \cap C$ legfeljebb n pontból áll.

e) $U = \{(x, y) \in \mathbb{A}^2(\mathbb{R}) \mid y = \sin x\}$ nem algebrai halmaz.

f) $U = \{(x, y) \in \mathbb{A}^2(\mathbb{C}) \mid |z|^2 + |w|^2 = 1\}$ nem algebrai halmaz.

Bizonyítás. (a) Azt már láttuk, hogy ezek valóban algebrai halmazok. Legyen $V = V(I) \subset \mathbb{A}^1$ algebrai, ahol $I \lhd k[X]$. Ha $I = (0)$, akkor $V = \mathbb{A}^1$. Különben létezik $F \in I$ nem konstans polinom, ekkor $(F) \subset I$, így $V(F) \supset V(I) = V$. De F-nek csak véges sok gyöke van, így $V(F)$ véges, tehát V is véges.

(b) $V = V(X^2 - Y, X^3 - Z)$.

(c) $V = V(X^2 + Y^2 - 1)$.

(d) Tegyük fel, hogy $L = V(Y - aX - b)$, $a, b \in k$. Legyen $G = F(X, aX + b) \in k[X]$. Ekkor $V(G) \subset \mathbb{A}^1$ algebrai, így a) szerint $V(G)$ véges, vagy $\mathbb{A}^1$. Ha $V(G) = \mathbb{A}^1$ lenne, akkor $F(x, ax + b) = G(x) = 0$ lenne minden $x \in k$-ra, de ekkor $L \subset C$ teljesülne. Tehát $V(G)$ véges, ráadásul legfeljebb n pontú, mivel $\deg G \leq n$. Tehát $F(x, ax + b) = 0$ legfeljebb n $x \in k$-ra, azaz $L \cap C$ legfeljebb n pontú. Ha L nem $V(Y - aX - b)$ alakú, akkor $V(X - aY - b)$ alakú, és a bizonyítás a $G = F(aY + b, Y)$ polinommal ugyanúgy megy.

(e) Tegyük fel, hogy $U = V(I)$ algebrai, és legyen $L = V(Y)$. Mivel minden $n \in \mathbb{Z}$-re $(n\pi, 0) \in U$, ezért $L \cap U$ végtelen. Minden $F \in I$ esetén $C = V(F) \supset V(I) = U$, így $L \cap C$ is végtelen, ami d) szerint csak $L \subset C$ esetén lehet. Tehát minden $F \in I$ eltűnik az L egyenesen, ezért $L \subset V(I) = U$, ami ellentmondás, mert $(\pi/2, 0) \notin U$.

(f) Vegyük az $L = V(Y)$ egyenest, ekkor $L \cap U = \{(x, 0) \mid |x|^2 = 1\}$ végtelen halmaz, de nem a teljes L, ami megint ellentmondásra vezet. □

1.3. Ponthalmaz ideálja

Tetszőleges X ponthalmazra tekinthetjük azon polinomok halmazát, melyek X-en eltűnnek. Ezek a polinomok nyilván ideált alkotnak.

Definíció. Ha $X \subset \mathbb{A}^n(k)$, akkor az X ponthalmaz *ideálja*

$$I(X) = \{F \in k[X_1, \ldots, X_n] \mid \forall P \in X\text{-re } F(P) = 0\}.$$

1.3.1. Állítás. a) *Ha $X \subset Y$, akkor $I(X) \supset I(Y)$.*

b) $I(\emptyset) = k[X_1, \ldots, X_n]$, $I(\{(a_1, \ldots, a_n)\}) = (X_1 - a_1, \ldots, X_n - a_n)$.

c) *Ha k végtelen, akkor $I(\mathbb{A}^n(k)) = (0)$.*

d) *$S \subset I(V(S))$ tetszőleges S polinomhalmazra. $X \subset V(I(X))$ tetszőleges X ponthalmazra.*

e) *$V(I(V(S))) = V(S)$. Tehát ha V algebrai halmaz, akkor $V(I(V)) = V$.*

f) *$I(V(I(X))) = I(X)$. Tehát ha $I = I(X)$ alakú, akkor $I(V(I)) = I$.*

Bizonyítás. (a) Ha F eltűnik Y-on, akkor X-en is.

(b) Ha $F \in (X_1 - a_1, \ldots, X_n - a_n)$, akkor F eltűnik $(a_1, \ldots, a_n)$-ben. Megfordítva, tegyük fel, hogy $F(a_1, \ldots, a_n) = 0$. Legyen $G = F(X_1 + a_1, \ldots, X_n + a_n)$, ekkor $G(0, \ldots, 0) = 0$. Ezért G konstans tagja 0, így $G \in (X_1, \ldots, X_n)$, azaz $G = \sum_{i=1}^n F_i X_i$ alkalmas F_i polinomokkal. Tehát $F = G(X_1 - a_1, \ldots, X_n - a_n) = \sum_{i=1}^n F_i(X_1 - a_1, \ldots, X_n - a_n)(X_i - a_i)$, azaz $F \in (X_1 - a_1, \ldots, X_n - a_n)$.

(c) $I(\mathbb{A}^n) = (0)$-t n szerinti indukcióval bizonyítjuk. $n = 1$-re, ha $F \in k[X]$ minden pontban eltűnik, akkor végtelen sok gyöke van, tehát $F = 0$. Tegyük fel, hogy $F \in k[X_1, \ldots, X_n]$-nek minden $(a_1, \ldots, a_n) \in \mathbb{A}^n$ pont gyöke. Legyen $F = \sum_{i=0}^d F_i X_n^i$, ahol $F_i \in k[X_1, \ldots, X_{n-1}]$. Ha valamelyik $F_i(a_1, \ldots, a_{n-1}) \neq 0$, akkor $F(a_1, \ldots, a_{n-1}, X_n)$-nek csak véges sok gyöke lehetne, ezért mindegyik F_i eltűnik $\mathbb{A}^{n-1}$-en. Az indukciós feltevés szerint így mindegyik $F_i = 0$, tehát $F = 0$.

(d) Ha $F \in S$, akkor minden $P \in V(S)$-re $F(P) = 0$, így $F \in I(V(S))$. Ha $P \in X$, akkor minden $F \in I(X)$-re $F(P) = 0$, így $P \in V(I(X))$.

(e) $V(S) \subset V(I(V(S)))$ d) szerint. $S \subset I(V(S))$ d) szerint, így az 1.2.1.a) Állítás alapján $V(S) \supset V(I(V(S)))$.

(f) $I(X) \subset I(V(I(X)))$ d) szerint. $X \subset V(I(X))$ d) szerint, így a) alapján $I(X) \supset I(V(I(X)))$. □

Definíció. Ha I ideál az R gyűrűben, akkor I *radikálja*

$$\mathrm{Rad}(I) = \{a \in R \mid a^n \in I \text{ valamely } n \text{ pozitív egészre}\}.$$

I radikálideál, ha $\mathrm{Rad}(I) = I$.

1.3.2. Állítás. a) *$I \subset \mathrm{Rad}(I)$. Így az I ideál pontosan akkor radikálideál, ha $a^n \in I$ esetén $a \in I$.*

b) *Ha I ideál, akkor $\mathrm{Rad}(I)$ is ideál, sőt radikálideál.*

c) *Minden prímideál radikálideál.*

d) *Tetszőleges $X \subset \mathbb{A}^n$ ponthalmazra $I(X)$ radikálideál.*

e) *Ha $I \lhd k[X_1, \ldots, X_n]$, akkor $\mathrm{Rad}(I) \subset I(V(I))$, és $V(I) = V(\mathrm{Rad}(I))$. Tehát minden algebrai halmaz $V(J)$ alakú, ahol J radikálideál.*

Bizonyítás. (a) Ha $a \in I$, akkor $a^1 \in I$, így $a \in \mathrm{Rad}(I)$. Tehát $\mathrm{Rad}(I) = I$ ekvivalens azzal, hogy $\mathrm{Rad}(I) \subset I$, azaz $a^n \in I$ esetén $a \in I$.

(b) Ha $a, b \in \mathrm{Rad}(I)$, akkor $a^n, b^m \in I$. Így $(a+b)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} a^i b^{n+m-i} \in I$, hiszen minden i-re a^i vagy b^{n+m-i} I-beli. Tehát $a+b \in \mathrm{Rad}(I)$. Ha $a \in \mathrm{Rad}(I)$, $a^n \in I$, akkor tetszőleges r-re $(ar)^n = a^n r^n \in I$, így $ar \in \mathrm{Rad}(I)$. Tehát $\mathrm{Rad}(I)$ ideál. Ha $a^n \in \mathrm{Rad}(I)$, akkor $a^{nm} \in I$, tehát $a \in \mathrm{Rad}(I)$, így a) szerint $\mathrm{Rad}(I)$ radikálideál.

(c) Ha I prímideál, akkor $a^n \in I$ esetén $a \in I$, így a) szerint I radikálideál.

(d) Ha $F^r \in I(X)$, akkor $I(X)$ definíciója szerint $F(P)^r = 0$ minden $P \in X$-re, ezért $F(P) = 0$ minden $P \in X$-re, tehát $F \in I(X)$. Így a) szerint $I(X)$ radikálideál.

(e) Ha $F \in \mathrm{Rad}(I)$, $F^r \in I$, akkor $V(I)$ definíciója szerint $F(P)^r = 0$ minden $P \in V(I)$-re, ezért $F(P) = 0$ minden $P \in V(I)$-re, tehát $F \in I(V(I))$. Mivel $I \subset \mathrm{Rad}(I) \subset I(V(I))$, ezért $V(I) \supset V(\mathrm{Rad}(I)) \supset V(I(V(I))) = V(I)$ 1.3.1.a) és 1.3.1.e) szerint. $J = \mathrm{Rad}(I)$ b) alapján radikálideál. □

1.3.3. Állítás. a) *A V, W algebrai halmazokra $V = W$ pontosan akkor, ha $I(V) = I(W)$.*

b) *Legyen V algebrai halmaz, $P \notin V$ pont. Ekkor létezik olyan F polinom, amely V-n eltűnik, és $F(P) = 1$.*

c) *Legyen V algebrai halmaz, $P_1, \ldots, P_r \notin V$ különböző pontok. Ekkor léteznek olyan $F_1, \ldots, F_r \in I(V)$ polinomok, melyekre $F_i(P_i) = 1$ és $F_i(P_j) = 0$ minden $i \neq j$ esetén.*

d) *Legyen V algebrai halmaz, $P_1, \ldots, P_r \notin V$ különböző pontok, és $a_1, \ldots, a_r \in k$. Ekkor létezik olyan $G \in I(V)$, melyre $G(P_i) = a_i$.*

Bizonyítás. (a) Ha $I(V) = I(W)$, akkor 1.3.1.e) miatt $V = V(I(V)) = V(I(W)) = W$.

(b) $V \cup \{P\}$ is algebrai halmaz, $V \cup \{P\} \neq V$, így a) szerint $I(V \cup \{P\}) \neq I(V)$. De $I(V \cup \{P\}) \subset I(V)$, tehát létezik $F \in I(V)$, $F \notin I(V \cup \{P\})$. Ekkor $F(P) \neq 0$, így az $F/F(P)$ polinom megfelelő.

(c) Alkalmazzuk b)-t a $V \cup \{P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_r\}$ algebrai halmazra és a P_i pontra.

(d) Vegyük c) szerint az $F_1, \ldots, F_r$ polinomokat, és legyen $G = \sum_{i=1}^{r} a_i F_i$. □

1.3.4. Állítás. *Legyen k algebrailag zárt, $F \in k[X_1, \ldots, X_n]$ nem konstans. Ekkor*

a) $\mathbb{A}^n \setminus V(F)$ *végtelen, ha $n \geq 1$.*

b) $V(F)$ *végtelen, ha $n \geq 2$.*

Bizonyítás. (a) Tegyük fel, hogy $\mathbb{A}^n \setminus V(F) = \{P_1, \ldots, P_r\}$ véges, legyen P_i első koordinátája a_i. Ekkor $\mathbb{A}^n = V(F) \cup P_1 \cup \ldots \cup P_r \subset V(F) \cup V(X_1 - a_1) \cup \ldots \cup V(X_1 - a_r) = V(F \cdot (X_1 - a_1) \ldots (X_1 - a_r))$. Mivel k végtelen, ezért 1.3.1.c) szerint $F \cdot (X_1 - a_1) \ldots (X_1 - a_r) = 0$, ellentmondás.

(b) Legyen $F = \sum_{i=0}^{d} G_i X_1^d$, $G_i \in k[X_2, \ldots, X_n]$. Mivel F nem konstans, feltehető, hogy $G_d \neq 0$, $d \geq 1$. Ekkor a) szerint végtelen sok $(x_2, \ldots, x_n) \in \mathbb{A}^{n-1}$-re $G_d(x_2, \ldots, x_n) \neq 0$. Ilyenkor $F(X, x_2, \ldots, x_n) \in k[X]$ legalább elsőfokú polinom, így mivel k algebrailag zárt, ezért létezik $x_1 \in k$, melyre $F(x_1, \ldots, x_n) = 0$. Tehát $V(F)$ végtelen. □

1.3.5. Állítás. *Legyen k test, $a_1, \dots, a_n \in k$, és $I = (X_1 - a_1, \dots, X_n - a_n) \lhd k[X_1, \dots, X_n]$. Ekkor*

a) *$k[X_1, \dots, X_n]/I$ természetes módon izomorf k-val.*

b) *I maximális ideál.*

Bizonyítás. (a) Legyen $a = (a_1, \dots, a_n) \in \mathbb{A}^n$, és legyen $\varphi\colon k[X_1, \dots, X_n] \to k$, $F \mapsto F(a)$. Ekkor φ gyűrűhomomorfizmus, és φ szürjektív, mert k-n az identitás. $\varphi(F) = 0$, azaz $F(a) = 0$ az 1.3.1.b) Állítás alapján ekvivalens azzal, hogy $F \in I$. Tehát $\operatorname{Ker}\varphi = I$, és így φ izomorfizmust indukál $k[X_1, \dots, X_n]/I$ és k között.

(b) Mivel $k[X_1, \dots, X_n]/I$ test, ezért I maximális ideál. □

1.4. Hilbert bázistétele

Definíció. Az R gyűrű *Noether-gyűrű*, ha minden ideálja végesen generált.

1.4.1. Tétel (Hilbert bázistétele)**.** *Ha R Noether-gyűrű, akkor $R[X]$ is Noether-gyűrű.*

Bizonyítás. Legyen $I \lhd R[X]$. Legyen $J \subset R$ az I-beli polinomok főegyütthatóinak halmaza. Ekkor $J \lhd R$, mert I is ideál volt. Mivel R Noether, ezért J-t véges sok eleme generálja, így léteznek olyan $F_1, \dots, F_r \in R[X]$ polinomok, melyek főegyütthatói generálják J-t.

Legyen $N > \deg F_i$ minden i-re, és legyen minden $m \leq N$-re $J_m \lhd R$ azon $F \in I$ polinomok főegyütthatóinak halmaza, melyekre $\deg F \leq m$. Mivel R Noether, ezért léteznek olyan $F_{m1}, \dots, F_{mr_m} \in R[X]$ polinomok, melyek főegyütthatói generálják J_m-et. Megmutatjuk, hogy ezen véges sok F_i és F_{mj} polinom generálja I-t.

Tegyük fel, hogy nem generálja, legyen $G \in I$ minimális fokú, amely nem áll így elő. Ha $\deg G > N$, akkor találhatók olyan $Q_i \in R[X]$ polinomok, hogy $\sum_{i=1}^{r} Q_i F_i$ és G főegyütthatója megegyezik, hiszen J-t generálják az F_i-k főegyütthatói. Ekkor $\deg(G - \sum_{i=1}^{r} Q_i F_i) < \deg G$, ezért $G - \sum_{i=1}^{r} Q_i F_i$ generálva van, de ekkor G is generálva van, ellentmondás.

Ha $\deg G = m \leq N$, akkor találhatók olyan $Q_j \in R[X]$ polinomok, hogy $\sum_{j=1}^{r_m} Q_j F_{mj}$ és G főegyütthatója megegyezik, hiszen J_m-et generálják az F_{mj}-k főegyütthatói. Ekkor $\deg(G - \sum_{j=1}^{r_m} Q_j F_{mj}) < \deg G$, ezért $G - \sum_{j=1}^{r_m} Q_j F_{mj}$ generálva van, de ekkor G is generálva van, ellentmondás. □

1.4.2. Következmény. *Ha k test, akkor $k[X_1, \dots, X_n]$ Noether.*

Bizonyítás. k Noether, hiszen ideáljai csak a (0) és (1). Így n-szer alkalmazva az előző tételt, $k[X_1] \dots [X_n]$ is Noether. □

1.4.3. Következmény. *Minden algebrai halmaz előáll $V(F_1, \dots, F_r)$ alakban, azaz véges sok hiperfelület metszeteként.*

Bizonyítás. Ha $V \subset \mathbb{A}^n$ algebrai halmaz, akkor az 1.2.1.b) Állítás szerint $V = V(I)$ alakú, ahol $I \lhd k[X_1, \dots, X_n]$. Az előző következmény szerint $I = (F_1, \dots, F_r)$, így ismét 1.2.1.b)-t használva $V = V(I) = V(F_1, \dots, F_r)$. □

1.4.4. Állítás. *Legyen R gyűrű, $I \lhd R$, $\pi\colon R \to R/I$ a természetes faktorleképezés.*

a) *Ha $J' \lhd R/I$, akkor $J = \pi^{-1}(J') \lhd R$ egy I-t tartalmazó ideál.*

b) *Ha $I \subset J \lhd R$, akkor $J' = \pi(J) \lhd R/I$.*

Tehát egy természetes bijekció van R/I ideáljai és R I-t tartalmazó ideáljai között. Legyenek J' és J egymásnak megfelelő ideálok.

c) *J pontosan akkor radikálideál, ha J' az.*

d) *J pontosan akkor prímideál, ha J' az.*

e) *J pontosan akkor maximális ideál, ha J' az.*

f) *Ha J végesen generált ideál, akkor J' is.*

g) *Ha R Noether, akkor R/I is Noether.*

Bizonyítás. (a) Mivel $\pi(I) = \{0\} \subset J'$, ezért $I \subset \pi^{-1}(J') = J$. Ha $a, b \in J$, akkor $\overline{a}, \overline{b} \in J'$, így $\overline{a+b} \in J'$, ezért $a + b \in J$. Ha $a \in J, r \in R$, akkor $\overline{a} \in J'$, így $\overline{ra} \in J'$, ezért $ra \in J$.

(b) Ha $\overline{a}, \overline{b} \in J'$, akkor $a, b \in J$, így $a + b \in J$, ezért $\overline{a} + \overline{b} \in J'$. Ha $\overline{a} \in J'$, $\overline{r} \in R/I$, akkor $a \in J, r \in R$, így $ra \in J$, ezért $\overline{ra} \in J'$.

Megmutatjuk, hogy a $J' \lhd R/I$ ideálok halmaza és az $I \subset J \lhd R$ ideálok halmaza közötti bijekciót π és π^{-1} szolgáltatja. Mivel π szürjektív, ezért $\pi(\pi^{-1}(J')) = J'$ minden J'-re. Mivel $\operatorname{Ker}\pi = I \subset J$, ezért ha $\overline{a} = \overline{b}$ és $a \in J$, akkor $b = a + (b - a) \in J$, így $\pi^{-1}(\pi(J)) = J$ minden I-t tartalmazó J-re.

(c) Ha J radikálideál, $\overline{a}^n \in J'$, akkor $a^n \in J$, így $a \in J$, ezért $\overline{a} \in J'$, tehát J' radikálideál. Ha J' radikálideál, $a^n \in J$, akkor $\overline{a}^n \in J'$, így $\overline{a} \in J'$, ezért $a \in J$, tehát J radikálideál.

(d) Ha J prímideál, $\overline{a}\overline{b} \in J'$, akkor $ab \in J$, így $a \in J$ vagy $b \in J$, ezért $\overline{a} \in J'$ vagy $\overline{b} \in J'$, tehát J' prímideál. Ha J' prímideál, $ab \in J$, akkor $\overline{a}\overline{b} \in J'$, így $\overline{a} \in J'$ vagy $\overline{b} \in J'$, ezért $a \in J$ vagy $b \in J$, tehát J prímideál.

(e) Ha J maximális, $J' \subsetneq M' \lhd R/I$, akkor $J \subsetneq \pi^{-1}(M') \lhd R$, így $\pi^{-1}(M') = R$, ezért $M' = R/I$, tehát J' maximális. Ha J' maximális, $J \subsetneq M \lhd R$, akkor $J' \subsetneq \pi(M) \lhd R/I$ (mert $I \subset J$ miatt $I \subset M$ is teljesül), így $\pi(M) = R/I$, ezért $M = R$, tehát J maximális.

(f) Mivel J végesen generált, $J = (a_1, \ldots, a_n)$, ezért minden $b \in J$ előáll $b = \sum_{i=1}^n r_i a_i$, $r_i \in R$ alakban, így $\overline{b} = \sum_{i=1}^n \overline{r_i}\overline{a_i}$, ezért $J' = (\overline{a_1}, \ldots, \overline{a_n})$ is végesen generált.

(g) Ha $J' \lhd R/I$, akkor $J = \pi^{-1}(J') \lhd R$, és mivel R Noether, ezért J végesen generált, így f) szerint J' is végesen generált, tehát R/I Noether. □

1.5. Irreducibilis komponensek

Definíció. A $V \subset \mathbb{A}^n$ algebrai halmaz *reducibilis*, ha $V = V_1 \cup V_2$ alakban felírható, ahol $V_1, V_2 \neq V$ algebrai halmazok. V *irreducibilis*, ha nem reducibilis.

1.5.1. Állítás. *Ha $V \subset \mathbb{A}^n$ irreducibilis, és $V = V_1 \cup \ldots \cup V_r$, ahol V_i algebrai halmazok, akkor valamelyik $V_i = V$.*

Bizonyítás. r szerinti indukcióval. $r = 1$ esetén $V = V_1$. Tegyük fel, hogy $V = V_1 \cup \ldots \cup V_r$, és $V_1 \neq V$. az 1.2.1.d) Állítás szerint $W = V_2 \cup \ldots \cup V_r$ is algebrai halmaz, ezért $W = V$, mert különben $V = V_1 \cup W$ reducibilis volna. Az indukciós feltevést W-re alkalmazva kapjuk, hogy valamelyik $V_i = W = V$. □

1.5.2. Állítás. *A $V \subset \mathbb{A}^n$ algebrai halmaz pontosan akkor irreducibilis, ha $I(V)$ prímideál.*

Bizonyítás. Átfogalmazva: V pontosan akkor reducibilis, ha $I(V)$ nem prímideál.

Ha V reducibilis, akkor $V = V_1 \cup V_2$, $V_i \neq V$. Ekkor 1.3.3.a) alapján $I(V_i) \neq I(V)$. Mivel $V_i \subset V$, $I(V_i) \supset I(V)$, ezért létezik $F_i \in I(V_i)$, $F_i \notin I(V)$. Ekkor F_1F_2 eltűnik V_1-en és V_2-n is, így V-n is, $F_1F_2 \in I(V)$, de $F_1, F_2 \notin I(V)$. Tehát $I(V)$ nem prímideál.

Ha $I(V)$ nem prímideál, akkor léteznek $F_1, F_2 \notin I(V)$ polinomok, melyekre $F_1F_2 \in I(V)$. Legyen $V_i = V \cap V(F_i)$. Mivel F_i nem tűnik el V-n, ezért $V_i \neq V$. Ekkor $V(F_1) \cup V(F_2) = V(F_1F_2) \supset V(I(V)) = V$ az 1.2.1.d), a), és 1.3.1.e) Állítások szerint. Tehát $V_1 \cup V_2 = V$, és így V reducibilis. □

1.5.3. Állítás. a) *Legyen R Noether-gyűrű, és $\mathcal{I}$ tetszőleges nemüres családja az R-beli ideáloknak. Ekkor $\mathcal{I}$-nek létezik maximális eleme, azaz olyan $I \in \mathcal{I}$, melyre $I \subsetneq J$ esetén $J \notin \mathcal{I}$.*

b) *Legyen $\mathcal{V}$ tetszőleges nemüres családja $\mathbb{A}^n$ algebrai halmazainak. Ekkor $\mathcal{V}$-nek létezik minimális eleme, azaz olyan $V \in \mathcal{V}$, melyre $W \subsetneq V$ esetén $W \notin \mathcal{V}$.*

Bizonyítás. (a) Tegyük fel, hogy nincs maximális eleme. A kiválasztási axiómát használva válasszunk $\mathcal{I}$ minden nemüres $\mathcal{J}$ részhalmazából egy $g(\mathcal{J})$ ideált. Legyen $I_0 = g(\mathcal{I})$, és mivel I_n nem maximális, legyen $I_{n+1} = g(\{I \in \mathcal{I} \mid I_n \subsetneq I\})$. Tehát $I_0 \subsetneq I_1 \subsetneq \ldots$. Legyen $I = \bigcup_{n=0}^{\infty} I_n$, ekkor $I \lhd R$. Mivel R Noether, ezért $I = (f_1, \ldots, f_r)$ végesen generált. Elég nagy n-re $f_1, \ldots, f_r \in I_n$, így $I \subseteq I_n \subsetneq I_{n+1} \subseteq I$, ellentmondás.

(b) Legyen $\mathcal{I} = \{I(V) \mid V \in \mathcal{V}\}$. Ekkor $\mathcal{I}$ elemei $k[X_1, \ldots, X_n]$-beli ideálok, és $k[X_1, \ldots, X_n]$ Noether az 1.4.2. Következmény szerint. Ezért a) szerint van $\mathcal{I}$-nek maximális eleme, legyen ez $I(V)$, ahol $V \in \mathcal{V}$. Ekkor V minimális eleme $\mathcal{V}$-nek, mert ha $W \subsetneq V$, $W \in \mathcal{V}$, akkor $I(W) \in \mathcal{I}$ és W algebrai, így $I(W) \supsetneq I(V)$ 1.3.1.a) és 1.3.3.a) alapján, ami ellentmond $I(V)$ maximalitásának. □

1.5.4. Tétel. *Legyen $V \subset \mathbb{A}^n$ algebrai halmaz. Ekkor (sorrendtől eltekintve) egyértelműen léteznek olyan irreducibilis $V_1, \ldots, V_m$ algebrai halmazok, melyekre $V = V_1 \cup \ldots \cup V_m$, és $V_i \not\subset V_j$, ha $i \neq j$.*

Bizonyítás. Legyen $\mathcal{V}$ azon $W \subset \mathbb{A}^n$ algebrai halmazok családja, melyek nem állnak elő irreducibilisek uniójaként. Ha $\mathcal{V}$ nemüres, akkor az 1.5.3.b) Állítás szerint létezik minimális W eleme. Mivel $W \in \mathcal{V}$, ezért W nem irreducibilis, így $W = W_1 \cup W_2$, ahol $W_1, W_2 \neq W$. Ekkor $W_i \subsetneq W$ miatt $W_i \notin \mathcal{V}$, tehát W_i előáll irreducibilisek uniójaként, de ekkor $W_1 \cup W_2$ is irreducibilisek uniója, ellentmondás. Tehát $\mathcal{V}$ üres.

Tehát minden V előáll $V_1 \cup \ldots \cup V_r$ alakban, ahol V_i irreducibilis. Ha itt valamely $i \neq j$-re $V_i \subset V_j$, akkor dobjuk el V_i-t. Ezt ismételgetve kapunk egy olyan $V_1 \cup \ldots \cup V_m$ előállítást, melyre $V_i \not\subset V_j$, ha $i \neq j$.

Tegyük fel, hogy $V = V_1 \cup \ldots \cup V_m = W_1 \cup \ldots \cup W_p$ két megfelelő előállítása V-nek. Ekkor $V_i = V \cap V_i = \bigcup_{j=1}^{p}(W_j \cap V_i)$, és V_i irreducibilis, ezért az 1.5.1. Állítás szerint valamelyik $W_j \cap V_i = V_i$, azaz $V_i \subset W_{j(i)}$ valamely $j(i)$-re. Ugyanígy, mivel W_j irreducibilis, ezért $W_j \subset V_{i(j)}$ valamely $i(j)$-re. De $V_i \subset W_{j(i)} \subset V_{i(j(i))}$ csak $i = i(j(i))$ esetén teljesülhet, ezért $V_i = W_{j(i)}$ minden i-re, és $i \circ j$ az identitás. Ugyanígy, mivel $W_j \not\subset W_k$, ha $j \neq k$, ezért $j \circ i$ az identitás. Tehát a j függvény bijekció $\{1, \ldots, m\}$ és $\{1, \ldots, p\}$ között, amelyre $V_i = W_{j(i)}$ minden i-re, ezért a két felbontás csak sorrendben különbözik egymástól. □

Definíció. Az előző tételben szereplő V_i halmazok a V *irreducibilis komponensei*, a $V_1 \cup \ldots \cup V_m$ előállítást a V *irreducibilis komponensekre való felbontásának* nevezzük.

1.6. A sík algebrai részhalmazai

Mielőtt tovább építenénk az általános elméletet, megállunk egy pillanatra, és leírjuk az $\mathbb{A}^2(k)$ sík algebrai részhalmazait.

1.6.1. Állítás. *Ha $F, G \in k[X, Y]$ relatív prímek, akkor $V(F) \cap V(G)$ véges ponthalmaz.*

Bizonyítás. Mivel F és G relatív prímek $k[X][Y]$-ban, ezért az 1.1.2. Tétel alapján $k(X)[Y]$-ban is relatív prímek. Mivel $k(X)$ test, ezért $k(X)[Y]$ főideálgyűrű, így $(F, G) = (H)$ valamely $H \in k(X)[Y]$-ra. De F és G relatív prímek $k(X)[Y]$-ban, ezért H egység, így $(F, G) = (1)$. Tehát léteznek olyan $R, S \in k(X)[Y]$ polinomok, hogy $RF + SG = 1$. R és S együtthatói előállnak $k[X]$-beli polinomok hányadosaiként, ezen nevezők szorzata egy olyan $0 \neq D \in k[X]$, hogy $DR = A, DS = B \in k[X][Y]$. Ekkor $AF + BG = D$.

Így ha $(x, y) \in V(F) \cap V(G)$, akkor $D(x) = A(x, y)F(x, y) + B(x, y)G(x, y) = 0$. Azonban D-nek csak véges sok gyöke van, ezért $V(F) \cap V(G)$ pontjainak X-koordinátái közt csak véges sok érték fordulhat elő. Ugyanígy látható be, hogy ugyanez igaz az Y-koordinátákra is. Tehát $V(F) \cap V(G)$ véges halmaz. □

1.6.2. Állítás. *Legyen $F \in k[X, Y]$ irreducibilis, melyre $V(F)$ végtelen. Ekkor*

a) $I(V(F)) = (F)$.

b) $V(F)$ *irreducibilis.*

Bizonyítás. (a) $(F) \subset I(V(F))$ világos. Amennyiben $G \in I(V(F))$, akkor $V(G) \supset V(I(V(F))) = V(F)$, így $V(F) \cap V(G) \supset V(F)$ végtelen. Az előző állítás miatt így F-nek és G-nek van közös osztója, és mivel F irreducibilis, ezért $F \mid G$. Tehát $G \in (F)$, és így $I(V(F)) \subset (F)$.

(b) Mivel $k[X, Y]$ alaptételes, és F irreducibilis, ezért (F) prímideál. Így az 1.5.2. Állítás szerint $V(F)$ irreducibilis, mert a) alapján $I(V(F)) = (F)$ prímideál. □

1.6.3. Állítás. *Legyen k végtelen. Ekkor $\mathbb{A}^2(k)$-nak az irreducibilis algebrai részhalmazai a következők: $\mathbb{A}^2$, $\emptyset$, $\{P\}$, $V(F)$, ahol $P \in \mathbb{A}^2$, és $F \in k[X, Y]$ olyan irreducibilis polinom, melyre $V(F)$ végtelen.*

Bizonyítás. $\mathbb{A}^2$ irreducibilis, mert 1.3.1.c) szerint $I(\mathbb{A}^2) = (0)$, ami prímideál. $\emptyset$ és $\{P\}$ definíció szerint nem lehetnek reducibilisek, $V(F)$ pedig az előző állítás szerint irreducibilis.

Legyen $V \subset \mathbb{A}^2$ irreducibilis algebrai halmaz. Ha $I(V) = (0)$, akkor $V = V(I(V)) = \mathbb{A}^2$. Ha V véges, akkor csak 0 vagy 1 pontú lehet. Különben legyen $F \in I(V)$ nem konstans. Mivel $I(V)$ prímideál, ezért ha $F = F_1 \dots F_r$ az F irreducibilisek szorzataként való felírása, akkor valamelyik $F_i \in I(V)$. Ha $G \in I(V)$, akkor $F_i \mid G$, mert különben $V = V(I(V)) \subset V(F_i, G) = V(F_i) \cap V(G)$ véges az 1.6.1. Állítás alapján. Tehát $I(V) = (F_i)$, és $V = V(I(V)) = V(F_i)$, ahol F_i irreducibilis, és $V(F_i)$ végtelen. □

1.6.4. Állítás. *Legyen k algebrailag zárt, és az $F \in k[X,Y]$ nem konstans polinom prímtényezős felbontása $F = F_1^{n_1} \dots F_r^{n_r}$. Ekkor*

a) *$V(F) = V(F_1) \cup \dots \cup V(F_r)$ a $V(F)$ irreducibilis komponensekre való felbontása.*

b) *$I(V(F)) = (F_1 \dots F_r)$.*

Bizonyítás. (a) Mivel k algebrailag zárt, ezért az 1.3.4.b) Állítás szerint $V(F_i)$ végtelen. Így az 1.6.2. Állítás miatt $I(V(F_i)) = (F_i)$ és $V(F_i)$ irreducibilis. Ha valamely $i \neq j$-re $V(F_i) \subset V(F_j)$ lenne, akkor $(F_i) = I(V(F_i)) \supset I(V(F_j)) = (F_j)$, azaz $F_i \mid F_j$ teljesülne, ami ellentmondás. Mivel $F(P) = F_1(P)^{n_1} \dots F_r(P)^{n_r} = 0$ pontosan akkor, ha valamelyik $F_i(P) = 0$, ezért $V(F) = V(F_1) \cup \dots \cup V(F_r)$. Itt $V(F_i)$ irreducibilis és $V(F_i) \not\subset V(F_j)$, ezért ez valóban az irreducibilis komponensekre való felbontás.

(b) $I(V(F)) = I(\bigcup_{i=1}^r V(F_i)) = \bigcap_{i=1}^r I(V(F_i)) = \bigcap_{i=1}^r (F_i) = (F_1 \dots F_r)$, mert egy polinom pontosan akkor osztható az $F_1, \dots, F_r$ polinomok mindegyikével, ha osztható $F_1 \dots F_r$-rel. □

1.7. Végességi feltételek, egész elemek

Definíció. Legyenek $R \subset S$ gyűrűk.

a) *S modulus-véges* R felett, ha $S = \sum_{i=1}^n Rv_i$ valamely $v_i \in S$ elemekre, azaz S végesen generált R-modulus.

b) Ha $v_1, \dots, v_n \in S$, akkor $R[v_1, \dots, v_n]$ azon $\varphi\colon R[X_1, \dots, X_n] \to S$ gyűrűhomomorfizmus képét jelöli, amely R-en az identitás, és $\varphi(X_i) = v_i$. Ez egyben a legkisebb részgyűrűje S-nek, ami tartalmazza R-et, és a $v_1, \dots, v_n$ elemeket.

S gyűrű-véges R felett, ha $S = R[v_1, \dots, v_n]$ valamely $v_i \in S$ elemekre.

c) Ha $R = K, S = L$ testek, $v_1, \dots, v_n \in L$, akkor $K(v_1, \dots, v_n)$ a $K[v_1, \dots, v_n]$ hányadostestét jelöli, mint L-nek része. Ez egyben a legkisebb részteste L-nek, ami tartalmazza K-t, és a $v_1, \dots, v_n$ elemeket.

L végesen generált testbővítése K-nak, ha $L = K(v_1, \dots, v_n)$ valamely $v_i \in K$ elemekre.

1.7.1. Példák. a) Ha S modulus-véges R felett, akkor gyűrű-véges.

b) Ha az L test gyűrű-véges a K test felett, akkor L végesen generált testbővítése K-nak.

c) $R[X]$ gyűrű-véges R felett, de nem modulus-véges.

d) $K(X)$ végesen generált testbővítése K-nak, de nem gyűrű-véges K felett.

Bizonyítás. (a) Ha $S = \sum_{i=1}^{n} Rv_i$, akkor $S = R[v_1, \ldots, v_n]$.

(b) Ha $L = K[v_1, \ldots, v_n]$ test, akkor $L = K(v_1, \ldots, v_n)$.

(c) Tegyük fel, hogy $R[X] = \sum_{i=1}^{n} Rv_i$, ahol $v_i \in R[X]$. Ha $\deg f > \deg v_i$ minden i-re, akkor f nem állhat elő $f = \sum_{i=1}^{n} r_i v_i$, $r_i \in R$ alakban, ellentmondás.

(d) Tegyük fel, hogy $K(X) = K[v_1, \ldots, v_n]$, ahol $v_i \in K(X)$. Legyen $b \in K[X]$ a v_i elemek nevezőinek szorzata, ekkor $bv_i \in K[X]$. Mivel $\frac{1}{Xb+1} \in K(X)$, ezért előáll $\frac{1}{Xb+1} = F(v_1, \ldots, v_n)$, $F \in K[X_1, \ldots, X_n]$ alakban. Ha $\deg F = m$, akkor $\frac{b^m}{Xb+1} = b^m F(v_1, \ldots, v_n) = G(bv_1, \ldots, bv_n)$ valamely $G \in K[X][X_1, \ldots, X_n]$ polinomra, így $\frac{b^m}{Xb+1} \in K[X]$. Ez ellentmondás, mert a nevező legalább elsőfokú polinom, és a számláló minden irreducibilis osztója osztja b-t, így nem osztja az $Xb + 1$ nevezőt, ez tehát egy egyszerűsíthetetlen tört. □

1.7.2. Állítás. *Legyenek $R \subset S \subset T$ gyűrűk.*

a) *Ha T modulus-véges S felett, és S modulus-véges R felett, akkor T modulus-véges R felett.*

b) *Ha T gyűrű-véges S felett, és S gyűrű-véges R felett, akkor T gyűrű-véges R felett.*

c) *Ha R, S, T testek, T végesen generált testbővítése S-nek, és S végesen generált testbővítése R-nek, akkor T végesen generált testbővítése R-nek.*

Bizonyítás. (a) Ha $T = \sum_{i=1}^{n} Sv_i$, $S = \sum_{j=1}^{m} Rw_j$, akkor minden $t \in T$ előáll $t = \sum_{i=1}^{n} s_i v_i$, $s_i \in S$ alakban, és itt mindegyik s_i előáll $s_i = \sum_{j=1}^{m} r_{ij} w_j$, $r_{ij} \in R$ alakban. Tehát $t = \sum_{i=1}^{n} \sum_{j=1}^{m} r_{ij} w_j v_i$, így $T = \sum_{i,j} Rw_j v_i$, azaz T modulus-véges R felett.

(b) $T = S[v_1, \ldots, v_n]$, $S = R[w_1, \ldots, w_m]$ esetén $T = R[w_1, \ldots, w_m, v_1, \ldots, v_n]$, hiszen a legkisebb gyűrű, ami tartalmazza $R[w_1, \ldots, w_m]$-et és a $v_1, \ldots, v_n$ elemeket, ugyanaz, mint a legkisebb gyűrű, ami tartalmazza R-et és a $w_1, \ldots, w_m, v_1, \ldots, v_n$ elemeket.

(c) $T = S(v_1, \ldots, v_n)$, $S = R(w_1, \ldots, w_m)$ esetén $T = R(w_1, \ldots, w_m, v_1, \ldots, v_n)$, hiszen a legkisebb test, ami tartalmazza $R(w_1, \ldots, w_m)$-et és a $v_1, \ldots, v_n$ elemeket, ugyanaz, mint a legkisebb test, ami tartalmazza R-et és a $w_1, \ldots, w_m, v_1, \ldots, v_n$ elemeket. □

Definíció. Legyenek $R \subset S$ gyűrűk, $v \in S$. Azt mondjuk, hogy v *egész* R felett, ha létezik olyan $F = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in R[X]$ normált polinom, melyre $F(v) = 0$. Ha R, S testek, azt is mondjuk ilyenkor, hogy v *algebrai* R felett.

S *egész* R felett, ha minden $v \in S$ egész R felett. Ha R, S testek, azt is mondjuk ilyenkor, hogy S *algebrai bővítése* R-nek.

1.7.3. Állítás. *Legyenek $R \subset S$ gyűrűk, $v \in S$. Ekkor a következők ekvivalensek:*

(1) *v egész R felett.*
(2) *$R[v]$ modulus-véges R felett.*
(3) *Létezik olyan R', melyre $R[v] \subset R' \subset S$, és R' modulus-véges R felett.*

Bizonyítás. (1 $\Rightarrow$ 2) Ha $v^n + a_{n-1}v^{n-1} + \ldots + a_0 = 0$, akkor $v^n \in \sum_{i=0}^{n-1} Rv^i$. Ha $m \in \mathbb{N}$-re $v^m \in \sum_{j=0}^{n-1} Rv^i$, akkor $v^m = \sum_{i=0}^{n-1} r_i v^i$ valamely $r_i \in R$ elemekre, így $v^{m+1} = r_{n-1}v^n + \sum_{i=0}^{n-2} r_i v^{i+1} \in \sum_{i=0}^{n-1} Rv^i$. Tehát indukcióval $v^m \in \sum_{i=0}^{n-1} Rv^i$ adódik minden $m \in \mathbb{N}$-re, és így $R[v] = \sum_{i=0}^{n-1} Rv^i$, azaz $R[v]$ modulus-véges R felett.

(2 $\Rightarrow$ 3) $R' = R[v]$ megfelel.

(3 $\Rightarrow$ 1) $R' = \sum_{i=1}^{n} Rw_i$ valamely $w_i \in R'$ elemekkel. Ekkor $vw_i \in R'$, így előáll $vw_i = \sum_{j=1}^{n} a_{ij}w_j$ alakban, ahol $a_{ij} \in R$. Legyen $A = (a_{ij})$ $n \times n$-es mátrix, I az $n \times n$-es egységmátrix, $w = (w_i)$ $n \times 1$-es vektor. Ekkor $vw = Aw$, azaz $(Iv - A)w = 0$. Belátjuk, hogy $\det(Iv - A) = 0$, és mivel ez éppen egy $v^n + b_{n-1}v^{n-1} + \ldots + b_0 = 0$ alakú egyenletet ad, készen leszünk.

Ha $B = \operatorname{adj}(Iv - A)$ jelöli az $Iv - A$ mátrix előjeles aldeterminánsaiból álló adjungált mátrixát, akkor a determináns kifejtési tételének következményeként $B(Iv - A) = \det(Iv - A)I$. Mivel $1 \in R[v] \subset R' = \sum_{i=1}^{n} Rw_i$, ezért $1 = rw$ alakban felírható valamely r $1 \times n$-es vektorral. Ezért $0 = rB(Iv - A)w = r\det(Iv - A)w = \det(Iv - A)$, tehát v egész R felett. □

1.7.4. Következmény. *Ha $R \subset S$ gyűrűk, akkor S-nek az R felett egész elemei egy részgyűrűt alkotnak, ami tartalmazza R-et.*

Bizonyítás. Legyenek $a, b \in S$ egészek R felett, ekkor az előző állítás szerint $R[a]$ modulus-véges R felett, és mivel b egész $R[a]$ felett is, így $R[a][b] = R[a, b]$ modulus-véges $R[a]$ felett. Az 1.7.2.a) Állítás alapján ezért $R[a, b]$ modulus-véges R felett. Mivel $R' = R[a, b]$, $v \in \{a + b, -a, 0, ab, 1\}$ esetén $R[v] \subset R'$, ezért az előző állítás szerint v egész R felett, tehát az egész elemek valóban részgyűrűt alkotnak. □

1.7.5. Állítás. *Legyen K test, és $L = K(X)$. Ekkor*

a) *L minden $K[X]$ felett egész eleme $K[X]$-ben van.*

b) *Nincs olyan $0 \neq b \in K[X]$, melyre minden $z \in L$-hez létezik $n \in \mathbb{N}$, hogy $b^n z$ egész $K[X]$ felett.*

Bizonyítás. (a) Legyen $z \in L$, $z^n + a_{n-1}z^{n-1} + \ldots + a_0 = 0$, $a_i \in K[X]$. Ekkor $z = F/G$, ahol $F, G \in K[X]$ relatív prímek, és $F^n + a_{n-1}F^{n-1}G + \ldots + a_0G^n = 0$. Így G minden irreducibilis osztója osztja F^n-t, ezért osztja F-et, ami csak úgy lehet, ha G egység. Tehát $z \in K[X]$.

(b) Tegyük fel, hogy b ilyen, legyen $z = \frac{1}{Xb+1}$. Ekkor létezik n, hogy $\frac{b^n}{Xb+1}$ egész $K[X]$ felett, ami a) szerint csak úgy lehet, ha $\frac{b^n}{Xb+1} \in K[X]$. Ez viszont ellentmondás, mert ez egy egyszerűsíthetetlen tört (mint azt az 1.7.1.d) Példa bizonyításában is láttuk). □

1.7.6. Állítás. *Legyenek $K \subset L$ testek, $v \in L$, $L = K(v)$. Legyen $\varphi\colon K[X] \to L$ az a gyűrűhomomorfizmus, melyre $\varphi(X) = v$, és K-n az identitás.*

a) *Ha $\operatorname{Ker}\varphi = (0)$, akkor L izomorf a $K(X)$ racionális törtfüggvények testével.*

b) *Ha $\operatorname{Ker}\varphi \neq (0)$, akkor $L = K[v]$.*

Bizonyítás. (a) Mivel φ injektív, ezért $K[X]$ izomorf φ képével, $K[v]$-vel. Ezért a hányadostesteik is izomorfak: $K(X)$ izomorf $K(v) = L$-lel.

(b) Mivel $K[X]$ PID, ezért $\operatorname{Ker}\varphi = (F)$, ahol $0 \neq F \in K[X]$. Ekkor $K[X]/(F)$ izomorf φ képével, $K[v]$-vel. Mivel $K[v]$ nullosztómentes, ezért (F) prímideál, így

F irreducibilis, vagy egység. Mivel $\varphi(1) = 1$, ezért $1 \notin \operatorname{Ker}\varphi = (F)$, tehát F nem egység. Ha $(F) \subset I \lhd K[X]$, akkor $K[X]$ PID lévén $I = (G)$, $G \in K[X]$, ezért $G \mid F$. Ez viszont F irreducibilitása miatt azt jelenti, hogy G egység vagy F egységszerese, azaz $I = K[X]$ vagy $I = (F)$. Tehát (F) maximális ideál, és ezért $K[X]/(F)$ test, azaz $K[v] = K(v) = L$. □

1.7.7. Tétel (Zariski)**.** *Ha K, L testek, és L gyűrű-véges K felett, akkor L modulus-véges K felett.*

Bizonyítás. Legyen $L = K[v_1, \ldots, v_n]$, n szerinti indukcióval bizonyítunk. Ha $n = 0$, akkor $L = K$ modulus-véges K felett. Legyen $n \geq 1$, és tegyük fel, hogy $n - 1$ elemre tudjuk az állítást. Legyen $K_1 = K(v_1)$. Mivel $L = K[v_1][v_2, \ldots, v_n] \subset K(v_1)[v_2, \ldots, v_n] \subset K(v_1)(v_2, \ldots, v_n) = L$, ezért $L = K_1[v_2, \ldots, v_n]$. Az indukciós feltétel alapján tehát L modulus-véges K_1 felett. Ha v_1 algebrai K felett, azaz van olyan $0 \neq F \in K[X]$, melyre $F(v) = 0$, akkor az 1.7.6. Állításban $\operatorname{Ker}\varphi \neq (0)$, ezért $K_1 = K[v_1]$. Mivel v_1 egész K felett, ezért 1.7.3. szerint K_1 modulus-véges K felett, így 1.7.2.a) alapján L modulus-véges K felett.

Ha v_1 nem algebrai K felett, akkor az 1.7.6. Állításban $\operatorname{Ker}\varphi = (0)$, ezért K_1 izomorf $K(X)$-szel. Mivel $K_1[v_2, \ldots, v_n]$ modulus-véges K_1 felett, ezért 1.7.3. szerint $2 \leq i \leq n$ esetén v_i egész K_1 felett. $v_1 \in K_1$ miatt persze v_1 is egész K_1 felett. Tehát mindegyik v_i kielégít egy $v_i^{n_i} + a_{i1}v_i^{n_i-1} + \ldots = 0$ alakú egyenletet, ahol $a_{ij} \in K(v_1)$. Legyen $b \in K[v_1]$ az a_{ij} elemek nevezőinek szorzata, ekkor

$$(bv_i)^{n_i} + (ba_{i1})(bv_i)^{n_i-1} + (b^2a_{i2})(bv_i)^{n_i-2} + \ldots = 0,$$

ahol a $b^j a_{ij}$ együtthatók már $K[v_1]$-beliek, ezért bv_i egész $K[v_1]$ felett. Az 1.7.4. Következmény alapján a bv_i elemek tetszőleges $K[v_1]$-együtthatós polinomja is egész $K[v_1]$ felett. Ha $z = F(v_1, \ldots, v_n)$, $F \in K[X_1, \ldots, X_n]$, $\deg F = m$, akkor $b^m z = b^m F(v_1, \ldots, v_n) = G(bv_1, \ldots, bv_n)$ valamely $G \in K[v_1][X_1, \ldots, X_n]$ polinommal, így $b^m z$ egész $K[v_1]$ felett. Tehát minden $z \in K[v_1, \ldots, v_n]$ esetén, speciálisan minden $z \in K_1$-re létezik olyan $m \in \mathbb{N}$, hogy $b^m z$ egész $K[v_1]$ felett. Azonban K_1 izomorf $K(X)$-szel, és $K[v_1]$ képe ezen izomorfiánál $K[X]$, így ez ellentmond az 1.7.5.b) Állításnak. □

1.7.8. Állítás. *Ha k algebrailag zárt test, akkor önmagán kívül nincs modulus-véges testbővítése.*

Bizonyítás. Ha $k \subset L$ test, L modulus-véges k felett, akkor az 1.7.3. Állítás szerint L minden eleme egész, azaz algebrai k felett. Tehát ha $a \in L$, akkor a gyöke egy $0 \neq F \in k[X]$ polinomnak. Mivel k algebrailag zárt, ezért $F = (X - b_1) \ldots (X - b_r)$, $b_i \in k$ alakban F gyöktényezőkre bomlik. Mivel $F(a) = 0$, ezért valamely i-re $a = b_i \in k$. Tehát $L = k$. □

1.8. A Hilbert-féle Nullstellensatz

Ettől a fejezettől kezdve k mindig algebrailag zárt testet jelöl.

1.8.1. Tétel (Gyenge Nullstellensatz)**.** *Ha $I \lhd k[X_1, \ldots, X_n]$ valódi ideál, akkor $V(I) \neq \emptyset$.*

Bizonyítás. Legyen $\mathcal{I} = \{J \lhd k[X_1, \dots, X_n] \mid I \subset J \neq k[X_1, \dots, X_n]\}$, mivel I valódi ideál, ezért $\mathcal{I} \neq \emptyset$. Az 1.5.3.a) Állítás szerint $\mathcal{I}$-nek létezik maximális J eleme. Ha belátjuk, hogy $V(J) \neq \emptyset$, akkor $I \subset J$ miatt $V(I) \supset V(J)$, tehát $V(I) \neq \emptyset$.

Mivel J maximális ideál, ezért $L = k[X_1, \dots, X_n]/J$ test. Ebben k tekinthető résztestnek. Ha X_i J-maradékát $\overline{X_i}$ jelöli, akkor $L = k[\overline{X_1}, \dots, \overline{X_n}]$. Tehát L gyűrűvéges k felett, így az 1.7.7. Tétel szerint L modulus-véges k felett. Mivel k algebrailag zárt, ezért az 1.7.8. Állítás szerint $L = k$.

Tehát mindegyik i-re létezik olyan $a_i \in k$, hogy $\overline{X_i} = a_i$, azaz $X_i - a_i \in J$, így $(X_1 - a_1, \dots, X_n - a_n) \subset J$. De az 1.3.5.b) Állítás alapján $(X_1 - a_1, \dots, X_n - a_n)$ maximális ideál. Ezért $(X_1 - a_1, \dots, X_n - a_n) = J$, és $V(J) = \{(a_1, \dots, a_n)\}$, tehát $V(I) \neq \emptyset$. □

1.8.2. Tétel (Nullstellensatz)**.** *Ha $I \lhd k[X_1, \dots, X_n]$, akkor $I(V(I)) = \mathrm{Rad}(I)$.*

Bizonyítás. 1.3.2.e) alapján $\mathrm{Rad}(I) \subset I(V(I))$. Legyen $G \in I(V(I))$, azaz G eltűnik $V(I)$-n, azt kell belátnunk, hogy $G \in \mathrm{Rad}(I)$.

Mivel $k[X_1, \dots, X_n]$ Noether, ezért $I = (F_1, \dots, F_r)$, $F_i \in k[X_1, \dots, X_n]$. Így $V(I) = V(F_1, \dots, F_r)$, ezért G eltűnik minden olyan pontban, ahol $F_1, \dots, F_r$ mindegyike eltűnik. Legyen $J = (F_1, \dots, F_r, X_{n+1}G - 1) \lhd k[X_1, \dots, X_n, X_{n+1}]$. Ekkor $V(J) \subset \mathbb{A}^{n+1}$ üres, mert ha $P \in \mathbb{A}^{n+1}$-re mindegyik $F_i(P) = 0$, akkor $G(P) = 0$, így $(X_{n+1}G - 1)(P) = -1$. Ezért a Gyenge Nullstellensatz szerint J nem lehet valódi ideál, azaz $1 \in J$.

Tehát $1 = \sum_{i=1}^{r} A_i F_i + B(X_{n+1}G - 1)$ alkalmas $A_i, B \in k[X_1, \dots, X_{n+1}]$ polinomokkal. Alkalmazzunk $X_{n+1} = 1/Y$ helyettesítést, majd szorozzunk fel egy kellően nagy Y-hatvánnyal:

$$1 = \sum_{i=1}^{r} A_i\Big(X_1, \dots, X_n, \frac{1}{Y}\Big)F_i + B\Big(X_1, \dots, X_n, \frac{1}{Y}\Big)\Big(\frac{G}{Y} - 1\Big),$$

$$Y^m = \sum_{i=1}^{r} C_i(X_1, \dots, X_n, Y)F_i + D(X_1, \dots, X_n, Y)(G - Y),$$

ahol $C_i, D \in k[X_1, \dots, X_n, Y]$. Végül Y helyébe G-t írva

$$G^m = \sum_{i=1}^{r} C_i(X_1, \dots, X_n, G)F_i.$$

Itt $C_i(X_1, \dots, X_n, G) \in k[X_1, \dots, X_n]$, ezért $G^m \in (F_1, \dots, F_r) = I$, azaz $G \in \mathrm{Rad}(I)$. □

1.8.3. Következmény. a) *Ha $I \lhd k[X_1, \dots, X_n]$ radikálideál, akkor $I(V(I)) = I$. Tehát a radikálideálok természetes módon bijekcióban állnak az algebrai halmazokkal.*

b) *Ha $I \lhd k[X_1, \dots, X_n]$ prímideál, akkor $V(I)$ irreducibilis. Tehát a prímideálok bijekcióban állnak az irreducibilis algebrai halmazokkal.*

c) *A maximális ideálok a pontoknak felelnek meg.*

Bizonyítás. (a) Ha I radikálideál, akkor $I = \mathrm{Rad}(I) = I(V(I))$ a Nullstellensatz szerint. A V függvény radikálideálhoz algebrai halmazt rendel, az I függvény 1.3.2.d) szerint algebrai halmazhoz radikálideált. 1.3.1.e) alapján $V \circ I$ az identitás, és most láttuk be, hogy a radikálideálokon $I \circ V$ is identitás. Tehát I és V bijekciók.

(b) Ha I prímideál, akkor 1.3.2.c) szerint I radikálideál, így a) alapján $I(V(I)) = I$. Tehát $I(V(I))$ prímideál, így 1.5.2. szerint $V(I)$ irreducibilis. A V függvény tehát prímideálhoz irreducibilis algebrai halmazt rendel, az I függvény 1.5.2. szerint irreducibilis algebrai halmazhoz prímideált. $I \circ V$ és $V \circ I$ most is identitás, tehát I és V bijekciók.

(c) Ezen bijekciónál $\{(a_1, \ldots, a_n)\}$ képe 1.3.1.b) szerint $(X_1 - a_1, \ldots, X_n - a_n)$, ami 1.3.5.b) alapján maximális ideál. Ha I maximális ideál, akkor a Gyenge Nullstellensatz miatt $V(I) \neq \emptyset$. De $V(I)$ nem lehet legalább 2 pontú, mert akkor valamelyik P pontját véve $\emptyset \neq \{P\} \subsetneq V(I)$, így 1.3.3.a) szerint $k[X_1, \ldots, X_n] \neq I(\{P\}) \supsetneq I(V(I))$. Mivel minden maximális ideál prímideál (1.1.4. Állítás), így radikálideál, ezért a) alapján $I(V(I)) = I$, de ez ellentmond annak, hogy I maximális ideál. Tehát $V(I)$ 1 pontú, így a V függvény maximális ideálhoz pontot rendel, ezek tehát bijekcióban állnak. □

1.8.4. Következmény. *Legyen az $F \in k[X_1, \ldots, X_n]$ nem konstans polinom prímtényezős felbontása $F = F_1^{n_1} \ldots F_r^{n_r}$. Ekkor*

a) *$V(F) = V(F_1) \cup \ldots \cup V(F_r)$ a $V(F)$ irreducibilis komponensekre való felbontása.*

b) *$I(V(F)) = (F_1 \ldots F_r)$.*

c) *Az irreducibilis $F \in k[X_1, \ldots, X_n]$ polinomok (egységszerestől eltekintve) és az irreducibilis hiperfelületek $\mathbb{A}^n$-ben természetes bijekcióban állnak.*

Bizonyítás. (a) Mivel $F(P) = 0$ pontosan akkor, ha valamelyik $F_i(P) = 0$, ezért $V(F) = V(F_1) \cup \ldots \cup V(F_r)$. Mivel F_i irreducibilis, ezért (F_i) prímideál, így 1.8.3.b) alapján $V(F_i)$ irreducibilis. Mivel (F_i) radikálideál, ezért 1.8.3.a) alapján $I(V(F_i)) = (F_i)$, így ha valamely $i \neq j$-re $V(F_i) \subset V(F_j)$ lenne, akkor $(F_i) = I(V(F_i)) \supset I(V(F_j)) = (F_j)$, azaz $F_i \mid F_j$ teljesülne, ami ellentmondás.

(b) $I(V(F)) = I(\bigcup_{i=1}^r V(F_i)) = \bigcap_{i=1}^r I(V(F_i)) = \bigcap_{i=1}^r (F_i) = (F_1 \ldots F_r)$.

(c) Ha F irreducibilis, akkor a) szerint $V(F)$ irreducibilis hiperfelület, és b) szerint $I(V(F)) = (F)$. Ha $V(G)$ irreducibilis hiperfelület, és $G = G_1^{n_1} \ldots G_r^{n_r}$, akkor a) szerint $r = 1$, $G = G_1^{n_1}$, és b) szerint $I(V(G)) = (G_1)$. Tehát I és V bijekcióba állítják az irreducibilis hiperfelületeket és az (F) ideálokat, ahol F irreducibilis. □

1.8.5. Következmény. *Legyen $I \lhd k[X_1, \ldots, X_n]$. Ekkor*

a) *$V(I)$ pontosan akkor véges halmaz, ha $k[X_1, \ldots, X_n]/I$ véges dimenziós, mint k feletti vektortér.*

b) *$|V(I)| \leq \dim_k(k[X_1, \ldots, X_n]/I)$.*

Bizonyítás. (b) Legyenek $P_1, \ldots, P_r \in V(I)$ különböző pontok. Az 1.3.3.c) Állítást $V = \emptyset$-ra alkalmazva, léteznek olyan $F_1, \ldots, F_r \in k[X_1, \ldots, X_n]$ polinomok, melyekre $F_i(P_i) = 1$ és $F_i(P_j) = 0$ minden $i \neq j$ esetén. Legyen $\overline{F_i}$ az F_i I-maradéka. Ha $\sum_{i=1}^r \lambda_i \overline{F_i} = 0$, $\lambda_i \in k$, akkor $\sum_{i=1}^r \lambda_i F_i \in I$, ezért $0 = \sum_{i=1}^r \lambda_i F_i(P_j) = \lambda_j$ minden j-re. Tehát $\overline{F_1}, \ldots, \overline{F_r}$ lineárisan függetlenek k felett, így $r \leq \dim_k(k[X_1, \ldots, X_n]/I)$.

Tehát ha $V(I) = \{P_1, \dots, P_r\}$ véges, akkor $|V(I)| \leq \dim_k(k[X_1, \dots, X_n]/I)$, ha pedig $V(I)$ végtelen, akkor $r \leq \dim_k(k[X_1, \dots, X_n]/I)$ minden $r \in \mathbb{N}$-re, azaz $\dim_k(k[X_1, \dots, X_n]/I)$ is végtelen.

(a) Ha $k[X_1, \dots, X_n]/I$ véges dimenziós, akkor b) szerint $V(I)$ véges. Megfordítva, ha $V(I) = \{P_1, \dots, P_r\}$ véges, és $P_i = (a_{i1}, \dots, a_{in})$, akkor legyen minden $1 \leq j \leq n$-re $G_j = (X_j - a_{1j}) \dots (X_j - a_{rj}) \in k[X_j]$. Ekkor G_j mindegyik P_i-ben eltűnik, így $G_j \in I(V(I))$. A Nullstellensatz szerint $I(V(I)) = \mathrm{Rad}(I)$, így létezik n_j, hogy $G_j^{n_j} \in I$. Legyen m nagyobb mindegyik n_j-nél, ekkor $G_j^m \in I$ minden j-re. I-maradékot véve $\overline{G_j}^m = 0$. Mivel G_j egy r-edfokú normált polinomja X_j-nek, ezért ez azt jelenti, hogy $\overline{X_j}^{rm}$ előáll $\overline{1}, \overline{X_j}, \dots, \overline{X_j}^{rm-1}$ egy k-lineáris kombinációjaként. Indukcióval adódik (mint 1.7.3. bizonyításában), hogy minden $t \in \mathbb{N}$-re $\overline{X_j}^t$ előáll ezek lineáris kombinációjaként. Így minden $F \in k[X_1, \dots, X_n]$-re $\overline{F}$ előáll a $\{\overline{X_1}^{i_1} \dots \overline{X_n}^{i_n} \mid 0 \leq i_j < rm\}$ halmaz elemeinek k-lineáris kombinációjaként, azaz $k[X_1, \dots, X_n]/I$-nek ez egy véges generátorrendszere. □

2. fejezet

Algebrai varietások

2.1. A koordinátagyűrű

Az irreducibilis affin algebrai halmazokat ezentúl *varietásoknak* hívjuk.

Minden gyűrűnek és testnek részgyűrűje lesz a k algebrailag zárt test. Így a $\varphi\colon R \to S$ gyűrűhomomorfizmusokról ezentúl azt is megköveteljük, hogy $\varphi(\lambda) = \lambda$ legyen minden $\lambda \in k$-ra.

Definíció. Ha $\emptyset \neq V \subset \mathbb{A}^n$ varietás, akkor V *koordinátagyűrűje* a

$$\Gamma(V) = k[X_1, \ldots, X_n]/I(V).$$

Ha V tetszőleges halmaz, akkor $\mathcal{F}(V, k)$ jelöli a V-ből k-ba képező függvények halmazát. A pontonkénti összeadással és szorzással $\mathcal{F}(V, k)$ gyűrűvé válik. Ebben k részgyűrűként jelenik meg, ha a konstans λ függvényt azonosítjuk a $\lambda \in k$ elemmel.

Definíció. Ha $V \subset \mathbb{A}^n$ varietás, akkor az $f \in \mathcal{F}(V, k)$ függvényt *V-n értelmezett polinomfüggvénynek* hívjuk, ha létezik $F \in k[X_1, \ldots, X_n]$, melyre $f(P) = F(P)$ minden $P \in V$-re.

A polinomfüggvények $\mathcal{F}(V, k)$ egy részgyűrűjét alkotják, mely tartalmazza k-t. Az F, G polinomok ugyanazt a polinomfüggvényt határozzák meg pontosan akkor, ha $(F-G)(P) = 0$ minden $P \in V$-re, azaz $F - G \in I(V)$. Ezért $\Gamma(V)$ azonosítható a V-n értelmezett polinomfüggvények gyűrűjével, $\Gamma(V) \subset \mathcal{F}(V, k)$. $\Gamma(V)$ egy elemére tehát kétféleképpen tekinthetünk: mint polinomok egy ekvivalenciaosztályára, vagy mint egy V-n értelmezett függvényre.

2.2. Polinomiális leképezések

Definíció. Ha $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ algebrai halmazok, akkor egy $\varphi\colon V \to W$ leképezést *polinomiális leképezésnek* hívunk, ha léteznek $T_1, \ldots, T_m \in k[X_1, \ldots, X_n]$ polinomok, hogy $\varphi(P) = (T_1(P), \ldots, T_m(P))$ minden $P \in V$-re. Ezt úgy is jelöljük, hogy $\varphi = (T_1, \ldots, T_m)$ V-n.

Ha $\varphi\colon V \to W$ tetszőleges leképezés, akkor φ természetes módon indukál egy $\widetilde{\varphi}\colon \mathcal{F}(W, k) \to \mathcal{F}(V, k)$ gyűrűhomomorfizmust az $f \mapsto f \circ \varphi$ hozzárendeléssel. Ha

φ varietások közti polinomiális leképezés, akkor $\widetilde{\varphi}$ $\Gamma(W)$-re való megszorítása egy $\widetilde{\varphi}\colon \Gamma(W) \to \Gamma(V)$ gyűrűhomomorfizmust ad, mert ha $\varphi = (T_1, \dots, T_m)$ V-n, és $f \in \Gamma(W)$ az F polinom W-re vett megszorítása, akkor $\widetilde{\varphi}(f) = f \circ \varphi$ az $F(T_1, \dots, T_m)$ polinom V-re vett megszorítása.

Ha $T\colon \mathbb{A}^n \to \mathbb{A}^m$ polinomiális leképezés, akkor egyértelműen léteznek olyan $T_i \in k[X_1, \dots, X_n]$ polinomok, hogy $T = (T_1, \dots, T_m)$, mert ha $T_i(P) = S_i(P)$ minden $P \in \mathbb{A}^n$-re, akkor $T_i - S_i \in I(\mathbb{A}^n) = (0)$ 1.3.1.c) szerint.

2.2.1. Állítás. *Legyenek $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ varietások. Ekkor a $\varphi\colon V \to W$ polinomiális leképezések és az $\alpha\colon \Gamma(W) \to \Gamma(V)$ gyűrűhomomorfizmusok között bijekciót teremt a $\varphi \mapsto \widetilde{\varphi}$ leképezés.*

Bizonyítás. Legyen $\alpha\colon \Gamma(W) \to \Gamma(V)$ homomorfizmus, és legyenek $T_1, \dots, T_m \in k[X_1, \dots, X_n]$ olyanok, hogy $\alpha(X_i + I(W)) = T_i + I(V)$. Ekkor $T = (T_1, \dots, T_m)$ egy $T\colon \mathbb{A}^n \to \mathbb{A}^m$ polinomiális leképezés. T indukál egy $\widetilde{T}\colon \Gamma(\mathbb{A}^m) \to \Gamma(\mathbb{A}^n)$ homomorfizmust. Mivel $I(\mathbb{A}^r) = (0)$, ezért $\widetilde{T}$ valójában egy $k[X_1, \dots, X_m] \to k[X_1, \dots, X_n]$ függvény.

Mivel α gyűrűhomomorfizmus, és $\lambda \in k$-ra $\alpha(\lambda) = \lambda$, ezért tetszőleges $F \in k[X_1, \dots, X_m]$-re

$$\begin{aligned}\alpha(F + I(W)) &= F(\alpha(X_1 + I(W)), \dots, \alpha(X_m + I(W))) = \\ &= F(T_1 + I(V), \dots, T_m + I(V)) = F \circ T + I(V).\end{aligned}$$

Így ha $F \in I(W)$, akkor $0 = \alpha(0) = \alpha(F + I(W)) = F \circ T + I(V)$, tehát $\widetilde{T}(F) = F \circ T \in I(V)$.

Tegyük fel, hogy valamely $P \in V$-re $T(P) \notin W$, ekkor 1.3.3.b) szerint létezik olyan $F \in I(W)$, melyre $F(T(P)) = 1$, ami ellentmond annak, hogy $F \in I(W)$ esetén $F \circ T$ eltűnik V-n. Ezért $P \in V$ esetén $T(P) \in W$, így T megszorítása V-re egy $\alpha^\star\colon V \to W$ polinomiális leképezés. Noha T nem volt egyértelmű, de T_i $I(V)$-maradéka egyértelmű volt, ezért a V-re való megszorításuk, $\alpha^\star$ is egyértelmű.

Ekkor $\widetilde{\alpha^\star} = \alpha$, mert $f \in \Gamma(W)$, $f = F + I(W)$ esetén $\widetilde{\alpha^\star}(f) = f \circ \alpha^\star = F \circ T + I(V) = \alpha(F + I(W)) = \alpha(f)$. Ha pedig $\varphi\colon V \to W$, $\varphi = (F_1, \dots, F_m)$ polinomiális leképezés, akkor $(\widetilde{\varphi})^\star = \varphi$, mert $T_i + I(V) = \widetilde{\varphi}(X_i + I(W)) = (X_i + I(W)) \circ \varphi = F_i + I(V)$, így $T = (T_1, \dots, T_m)$ V-re való megszorítása ugyanaz, mint $(F_1, \dots, F_m)$ V-re való megszorítása, ami pedig φ. Tehát az $\alpha \mapsto \alpha^\star$ és $\varphi \mapsto \widetilde{\varphi}$ leképezések egymás inverzei, így bijekciók. □

Definíció. A $\varphi\colon V \to W$ varietások közti polinomiális leképezés *izomorfizmus*, ha létezik olyan $\psi\colon W \to V$ polinomiális leképezés, hogy $\psi \circ \varphi$ az identitás V-n, és $\varphi \circ \psi$ az identitás W-n.

2.2.2. Állítás. a) *Ha $\varphi\colon V \to W$, $\omega\colon W \to Z$ varietások közti polinomiális leképezések, akkor $\omega \circ \varphi$ is polinomiális leképezés, és $\widetilde{\omega \circ \varphi} = \widetilde{\varphi} \circ \widetilde{\omega}$.*

b) *A V, W varietások pontosan akkor izomorfak, ha $\Gamma(V), \Gamma(W)$ gyűrűizomorfak (k-t tartva). Ha $\varphi\colon V \to W$ izomorfizmus, akkor $\widetilde{\varphi}\colon \Gamma(W) \to \Gamma(V)$ gyűrűizomorfizmus.*

Bizonyítás. (a) Ha $\varphi = (T_1, \dots, T_m)$ V-n, $\omega = (S_1, \dots, S_r)$ W-n, akkor $\omega \circ \varphi = (S_1(T_1, \dots, T_m), \dots, S_r(T_1, \dots, T_m))$ V-n, ahol $S_i(T_1, \dots, T_m) \in k[X_1, \dots, X_n]$ polinomok. Minden $f \in \Gamma(Z)$-re $\widetilde{\omega \circ \varphi}(f) = f \circ \omega \circ \varphi = \widetilde{\omega}(f) \circ \varphi = \widetilde{\varphi}(\widetilde{\omega}(f))$.

(b) Amennyiben $\varphi\colon V \to W$ és $\omega\colon W \to V$ mutatja V és W izomorfiáját, akkor $\widetilde{\varphi}\colon \Gamma(W) \to \Gamma(V)$ és $\widetilde{\omega}\colon \Gamma(V) \to \Gamma(W)$ mutatja $\Gamma(V)$ és $\Gamma(W)$ izomorfiáját, hiszen a) szerint $\widetilde{\varphi} \circ \widetilde{\omega} = \widetilde{\omega \circ \varphi} = \widetilde{\mathrm{id}_V} = \mathrm{id}_{\Gamma(V)}$ és $\widetilde{\omega} \circ \widetilde{\varphi} = \widetilde{\varphi \circ \omega} = \widetilde{\mathrm{id}_W} = \mathrm{id}_{\Gamma(W)}$.

Ha $\Gamma(V)$ és $\Gamma(W)$ izomorfak, akkor az előző állítás szerint ezen izomorfizmusok $\widetilde{\varphi}\colon \Gamma(W) \to \Gamma(V)$ és $\widetilde{\omega}\colon \Gamma(V) \to \Gamma(W)$ alakúak valamely $\varphi\colon V \to W$ és $\omega\colon W \to V$ polinomiális leképezésekkel. Mivel $\widetilde{\omega \circ \varphi} = \widetilde{\varphi} \circ \widetilde{\omega} = \mathrm{id}_{\Gamma(V)} = \widetilde{\mathrm{id}_V}$, és az előző állítás szerint a hullám leképezés bijekció, ezért $\omega \circ \varphi = \mathrm{id}_V$, és mivel $\widetilde{\varphi \circ \omega} = \widetilde{\omega} \circ \widetilde{\varphi} = \mathrm{id}_{\Gamma(W)} = \widetilde{\mathrm{id}_W}$, ezért $\varphi \circ \omega = \mathrm{id}_W$. Tehát V és W izomorfak. □

2.2.3. Állítás. a) *Ha $\varphi\colon V \to W$ polinomiális leképezés, és $X \subset W$ algebrai halmaz, akkor $\varphi^{-1}(X) \subset V$ algebrai halmaz.*

b) *Ha $\varphi\colon V \to X$ polinomiális leképezés, V irreducibilis, és φ szürjektív, akkor X irreducibilis.*

Bizonyítás. (a) $P \in \varphi^{-1}(X)$ pontosan akkor, ha $\varphi(P) \in X = V(I(X))$, azaz minden $F \in I(X)$-re $F(\varphi(P)) = 0$. Így $\varphi^{-1}(X) = V(\{F \circ \varphi \mid F \in I(X)\})$.

(b) Tegyük fel, hogy $X = X_1 \cup X_2$ reducibilis, $X_i \neq X$. Ekkor $V = \varphi^{-1}(X) = \varphi^{-1}(X_1) \cup \varphi^{-1}(X_2)$, és a) szerint $\varphi^{-1}(X_i)$ algebrai halmaz. Mivel φ szürjektív, és $X_i \neq X$, ezért létezik olyan $P_i \in V$, hogy $\varphi(P_i) \notin X_i$, azaz $P_i \notin \varphi^{-1}(X_i)$. Tehát $\varphi^{-1}(X_i) \neq V$, így V reducibilis, ellentmondás. □

2.2.4. Példák. a) $V = \{(t, t^2, t^3) \in \mathbb{A}^3 \mid t \in k\}$ varietás.

b) Ha $V \subset \mathbb{A}^n$ varietás, $f \in \Gamma(V)$, akkor f grafikonja,

$$G(f) = \{(a_1, \dots, a_{n+1}) \in \mathbb{A}^{n+1} \mid (a_1, \dots, a_n) \in V, a_{n+1} = f(a_1, \dots, a_n)\}$$

varietás, mely izomorf V-vel.

c) Legyen $V = V(X^3 - Y^2) \subset \mathbb{A}^2$, $\varphi\colon \mathbb{A}^1 \to V$, $t \mapsto (t^2, t^3)$. Ekkor φ bijekció, de nem izomorfizmus. Sőt, V és $\mathbb{A}^1$ más polinomiális leképezéssel sem izomorf.

Bizonyítás. (a) Mivel $\mathbb{A}^1$ irreducibilis, és $\varphi\colon \mathbb{A}^1 \to V$, $t \mapsto (t, t^2, t^3)$ szürjektív polinomiális leképezés, ezért 2.2.3.b) alapján V irreducibilis.

(b) $(a_1, \dots, a_n) \mapsto (a_1, \dots, a_n, f(a_1, \dots, a_n))$ és $(a_1, \dots, a_n, a_{n+1}) \mapsto (a_1, \dots, a_n)$ polinomiális leképezések mutatják az izomorfizmust.

(c) φ valóban V-be képez, mert $(t^2)^3 - (t^3)^2 = 0$, és φ injektív, mert ha $(x, y) = (t^2, t^3)$, akkor $x = 0$ esetén $t = 0$, $x \neq 0$ esetén $t = y/x$. φ szürjektív, mert ha $(x, y) \in V$, akkor $x^3 - y^2 = 0$, így $x = 0$ esetén $\varphi(0) = (0, 0) = (x, y)$, míg $x \neq 0$ esetén $\varphi(y/x) = (y^2/x^2, y^3/x^3) = (x^3/x^2, y^3/y^2) = (x, y)$. Tehát φ bijekció.

Tegyük fel, hogy φ izomorfizmus, ekkor 2.2.2.b) szerint $\widetilde{\varphi}\colon \Gamma(V) \to \Gamma(\mathbb{A}^1)$ gyűrűizomorfizmus. De $\Gamma(\mathbb{A}_1) = k[T]$, és $\overline{F} \in \Gamma(V)$ esetén $\widetilde{\varphi}(\overline{F}) = F \circ \varphi = F(T^2, T^3)$, ezért $\widetilde{\varphi}$ képe $k[T^2, T^3]$, így $\widetilde{\varphi}$ nem szürjektív, ellentmondás.

Tegyük fel, hogy $\omega\colon \mathbb{A}^1 \to V$, $\omega = (F, G)$ izomorfizmus, ekkor $\widetilde{\omega}\colon \Gamma(V) \to k[T]$ gyűrűizomorfizmus, és $\widetilde{\omega}$ képe $k[F, G] \subset k[T]$. Mivel ω V-be képez, ezért minden $t \in k$-ra $F(t)^3 - G(t)^2 = 0$, így $F^3 - G^2 = 0$. Mivel ω szürjektív, ezért van olyan

$a \in k$, hogy $F(a) = G(a) = 0$. Legyen a F-nek n-szeres, G-nek m-szeres gyöke, ekkor $F^3 = G^2$-nek $3n = 2m$-szeres gyöke. Ezért $n \geq 2$ és $m \geq 3$. Tehát $(T-a)^2 \mid F$, $(T-a)^3 \mid G$, ezért $T - a \notin k[F, G]$, így $\widetilde{\omega}$ nem szürjektív, ellentmondás. □

2.3. Affin koordinátacserék

Definíció. Legyen $T\colon \mathbb{A}^n \to \mathbb{A}^m$, $T = (T_1, \ldots, T_m)$ polinomiális leképezés.

a) Ha $F \in k[X_1, \ldots, X_m]$ polinom, akkor F^T jelöli a $\widetilde{T}(F) = F(T_1, \ldots, T_m) \in k[X_1, \ldots, X_n]$ polinomot.

b) Ha $I \lhd k[X_1, \ldots, X_m]$ ideál, akkor $I^T \lhd k[X_1, \ldots, X_n]$ jelöli az $\{F^T \mid F \in I\}$ által generált ideált.

c) Ha $V \subset \mathbb{A}^m$ algebrai halmaz, akkor V^T jelöli a $T^{-1}(V) \subset \mathbb{A}^n$ halmazt.

2.3.1. Állítás. *Itt V^T algebrai halmaz, és ha $V = V(I)$, akkor $V^T = V(I^T)$. Ha $V = V(F)$, akkor $V^T = V(F^T)$.*

Bizonyítás. $P \in V^T = T^{-1}(V)$ pontosan akkor, ha $T(P) \in V = V(I)$, azaz minden $F \in I$-re $0 = F(T(P)) = F^T(P)$, tehát $P \in V(\{F^T \mid F \in I\}) = V(I^T)$. □

Definíció. a) A $T\colon \mathbb{A}^n \to \mathbb{A}^n$, $T = (T_1, \ldots, T_n)$ polinomiális leképezés egy *affin koordinátacsere*, ha T bijekció, és mindegyik T_i elsőfokú.

b) Ha $P, Q \in \mathbb{A}^n$ különböző pontok, akkor a P, Q pontokon átmenő *egyenes* a $\{P + t(Q - P) \mid t \in k\}$ halmaz.

2.3.2. Állítás. a) *$T\colon \mathbb{A}^n \to \mathbb{A}^n$ pontosan akkor affin koordinátacsere, ha felírható $T = T'' \circ T'$ alakban, ahol T' invertálható lineáris transzformáció az $\mathbb{A}^n$ vektortéren, és T'' egy eltolás.*

b) *Ha T és U affin koordinátacsere $\mathbb{A}^n$-en, akkor $T \circ U$ és T^{-1} is az.*

c) *Ha a P, Q pontokon átmenő egyenes L, és T affin koordinátacsere, akkor $T(L)$ a $T(P), T(Q)$ pontokon átmenő egyenes.*

d) *Legyen $P, P' \in \mathbb{A}^2$, L_1, L_2 két különböző egyenes P-n át, L_1', L_2' két különböző egyenes P'-n át. Ekkor létezik olyan T affin koordinátacsere, hogy $T(P) = P'$, $T(L_1) = L_1'$, és $T(L_2) = L_2'$.*

Bizonyítás. (a) Ha $T = (T_1, \ldots, T_n)$, $T_i = b_i + \sum_{j=1}^n a_{ij} X_j$, akkor legyen $T_i' = \sum_{j=1}^n a_{ij} X_j$, $T_i'' = b_i + X_i$, $T' = (T_1', \ldots, T_n')$, $T'' = (T_1'', \ldots, T_n'')$. Ekkor $T = T'' \circ T'$, és mivel T-nek és a T'' eltolásnak van inverze, ezért $T' = T''^{-1} \circ T$ is invertálható. Megfordítva, minden $T'' \circ T'$ egy affin koordinátacsere.

(b) $T \circ U = (T_1(U_1, \ldots, U_n), \ldots, T_n(U_1, \ldots, U_n)$, ahol $T_i(U_1, \ldots, U_n)$ legfeljebb elsőfokú, és mivel T, U invertálható, $T \circ U$ is, és $T_i(U_1, \ldots, U_n)$ pontosan elsőfokú. Ha $T = T'' \circ T'$, ahol T' lineáris, T'' eltolás, akkor

$$T^{-1} = T'^{-1} \circ T''^{-1} = T'^{-1}(X_1 - b_1, \ldots, X_n - b_n) = T'^{-1}(X_1, \ldots, X_n) - T'^{-1}(b_1, \ldots, b_n),$$

ami egy bijektív lineáris transzformáció, majd egy eltolás, tehát T^{-1} affin koordinátacsere.

(c) $T(P+t(Q-P)) = T''(T'(P+t(Q-P))) = T''(T'(P)+t(T'(Q)-T'(P))) = T(P)+t(T'(Q)-T'(P)) = T(P)+t(T(Q)-T(P))$.

(d) Legyen először $P=(0,0)$, $L_1 = V(Y)$, és $L_2 = V(X)$. Legyenek $Q_i' \in L_i'$ P'-től különböző pontok, $P'=(b_1,b_2)$, $Q_i' = (a_{1i}+b_1, a_{2i}+b_2)$. Legyen

$$T = (a_{11}X + a_{12}Y + b_1, a_{21}X + a_{22}Y + b_2).$$

Ekkor $T(0,0) = P'$, $T(1,0) = Q_1'$, és $T(0,1) = Q_2'$. Így c) szerint $T(L_1) = L_1'$ és $T(L_2) = L_2'$. Mivel L_1', L_2' különbözők, ezért T invertálható, azaz affin koordinátacsere.

Ha P, L_1, L_2 tetszőleges, akkor az előzőek szerint vannak olyan T, U affin koordinátacserék, melyek $((0,0), V(Y), V(X))$-et rendre (P, L_1, L_2)-be és (P', L_1', L_2')-be viszik. Így b) szerint $U \circ T^{-1}$ is affin koordinátacsere, amely (P, L_1, L_2)-t (P', L_1', L_2')-be viszi. □

2.4. A lokális gyűrű

Ha V varietás, akkor 1.5.2. szerint $I(V)$ prímideál, így $\Gamma(V)$ nullosztómentes. Ezért $\Gamma(V)$-nek van hányadosteste (1.1.1. Tétel).

Definíció. Legyen $V \subset \mathbb{A}^n$ varietás. Ekkor

a) $\Gamma(V)$ hányadostestét $k(V)$ jelöli, és a *V-n értelmezett racionális törtfüggvények testének* hívjuk.

b) Ha $f \in k(V)$ racionális törtfüggvény, $P \in V$, akkor azt mondjuk, hogy f *értelmezve* van P-ben, ha létezik olyan $a, b \in \Gamma(V)$, $f = a/b$ felírás, melyre $b(P) \neq 0$.

c) Ha $P \in V$, akkor $\mathcal{O}_P(V)$ jelöli azon V-n értelmezett racionális törtfüggvények halmazát, melyek értelmezve vannak P-ben. Ezt hívjuk *V P-beli lokális gyűrűjének.*

d) Ha $f \in k(V)$, akkor azon $P \in V$ pontok halmaza, melyekben f nincs értelmezve, az *f pólushalmaza.*

Felhívjuk a figyelmet arra, hogy többféle, akár lényegesen különböző módokon is fel lehet írni egy $f \in k(V)$ racionális törtfüggvényt $f = a/b$ alakban. Tehát f akkor van értelmezve P-ben, ha találunk olyan nevezőt, melynek P nem gyöke. Például $V = V(XW - YZ) \subset \mathbb{A}^4$ esetén $\Gamma(V) = k[X,Y,Z,W]/(XW-YZ)$ 1.8.4.b) alapján. Jelölje $\overline{X}, \overline{Y}, \overline{Z}, \overline{W} \in \Gamma(V)$ az X, Y, Z, V maradékosztályait, ekkor $f = \overline{X}/\overline{Y} = \overline{Z}/\overline{W} \in k(V)$. Ezért f értelmezve van $P = (x,y,z,w) \in V$-ben akár $y \neq 0$, akár $w \neq 0$ esetén is.

Ha V varietás, és $f, g \in k(V)$ értelmezve vannak $P \in V$-ben, akkor $f = a/b$, $g = c/d$, $b(P), d(P) \neq 0$, így $fg, -f, f+g$ is értelmezve vannak P-ben. Minden $f \in \Gamma(V)$ értelmezve van P-ben. Így $\mathcal{O}_P(V)$ egy olyan részgyűrűje $k(V)$-nek, mely tartalmazza $\Gamma(V)$-t:

$$k \subset \Gamma(V) \subset \mathcal{O}_P(V) \subset k(V).$$

2.4.1. Állítás. a) *Ha V varietás, $f \in k(V)$, akkor f pólushalmaza egy algebrai halmaz.*

b) *Ha V varietás, akkor* $\Gamma(V) = \bigcap_{P\in V} \mathcal{O}_P(V)$.

Bizonyítás. (a) Legyen $V \subset \mathbb{A}^n$, és jelölje tetszőleges $G \in k[X_1, \ldots, X_n]$ $I(V)$-maradékát $\overline{G} \in \Gamma(V)$. Legyen $J_f = \{G \in k[X_1, \ldots, X_n] \mid \overline{G}f \in \Gamma(V)\}$. Mivel $\overline{0}f \in \Gamma(V)$, ezért $I(V) \subset J_f$, így $P \in V(J_f)$ esetén $P \in V(I(V)) = V$. De $P \in V(J_f)$ pontosan akkor, ha minden G-re $\overline{G}f \in \Gamma(V)$ esetén $G(P) = 0$, azaz f minden lehetséges nevezőjének gyöke P. Tehát f pólushalmaza $V(J_f)$.

(b) $\Gamma(V) \subset \bigcap_{P\in V} \mathcal{O}_P(V)$ világos. Ha $f \in \bigcap_{P\in V} \mathcal{O}_P(V)$, azaz f minden pontban értelmezve van, akkor f pólushalmaza üres, így a) szerint $V(J_f) = \emptyset$. De J_f ideál, ezért a Gyenge Nullstellensatz szerint J_f nem valódi, azaz $1 \in J_f$. Tehát $\overline{1}\cdot f \in \Gamma(V)$, azaz $f \in \Gamma(V)$. □

Ha $f \in \mathcal{O}_P(V)$, $f = \overline{A}/\overline{B} = \overline{C}/\overline{D}$, $A, B, C, D \in k[X_1, \ldots, X_n]$, $\overline{B}(P), \overline{D}(P) \neq 0$, akkor $\overline{AD - BC} = 0$, így $AD - BC \in I(V)$, ezért $(AD - BC)(P) = 0$, azaz $\overline{A}(P)/\overline{B}(P) = \overline{C}(P)/\overline{D}(P)$. Így definiálható $f(P)$.

Definíció. Legyen V varietás, és $P \in V$.

a) Ha $f \in \mathcal{O}_P(V)$, akkor f P-beli *helyettesítési értéke* $f(P) = a(P)/b(P)$, ahol $f = a/b$, $a, b \in \Gamma(V)$, $b(P) \neq 0$.

b) A V *P-beli maximális ideáljának* hívjuk a következőt:

$$\mathfrak{m}_P(V) = \{f \in \mathcal{O}_P(V) \mid f(P) = 0\}.$$

Mivel az $\mathcal{O}_P(V) \to k$, $f \mapsto f(P)$ leképezés gyűrűhomomorfizmus, melynek magja $\mathfrak{m}_P(V)$, ezért $\mathfrak{m}_P(V)$ ideál, és $\mathcal{O}_P(V)/\mathfrak{m}_P(V)$ izomorf k-val. Az $f \in \mathcal{O}_P(V)$ pontosan akkor egység, ha $f(P) \neq 0$. Ugyanis $f(P) = a(P)/b(P) \neq 0$ esetén $b/a \in \mathcal{O}_P(V)$ az f inverze, és ha f-nek g inverze, akkor $1 = (fg)(P) = f(P)g(P)$, tehát $f(P) \neq 0$. Ezért $\mathfrak{m}_P(V)$ éppen az $\mathcal{O}_P(V)$ nemegységeiből áll.

Definíció. Az R gyűrűt *lokális gyűrűnek* hívjuk, ha a nemegységek ideált alkotnak R-ben.

2.4.2. Állítás. *Az R gyűrű pontosan akkor lokális, ha R-ben van egy egyértelmű maximális ideál, mely R minden valódi ideálját tartalmazza.*

Bizonyítás. Tegyük fel, hogy $\mathfrak{m}$ egy ilyen maximális ideál. Ekkor $\mathfrak{m}$-nek minden a nemegységet tartalmaznia kell, mert (a) valódi ideál. Megfordítva, ha $\mathfrak{m}$ minden nemegységet tartalmaz, akkor minden valódi ideál $\mathfrak{m}$-nek része, hiszen valódi ideál egységeket nem tartalmazhat. Ugyanakkor $\mathfrak{m}$ nem tartalmazhat egységeket, mert akkor $\mathfrak{m} = R$ lenne. Tehát $\mathfrak{m}$ mindenképpen egyenlő a nemegységek halmazával. Így az, hogy létezik $\mathfrak{m}$ maximális ideál, mely minden valódi ideált tartalmaz, ekvivalens azzal, hogy a nemegységek halmaza ideált alkot, azaz R lokális. □

2.4.3. Állítás. *Ha V varietás, $P \in V$, akkor $\mathcal{O}_P(V)$ nullosztómentes, lokális, Noether-gyűrű, melynek maximális ideálja $\mathfrak{m}_P(V)$.*

Bizonyítás. Mivel $\mathcal{O}_P(V) \subset k(V)$ és $k(V)$ test, ezért $\mathcal{O}_P(V)$ nullosztómentes. $\mathcal{O}_P(V)$ lokális, mert a nemegységek halmaza $\mathfrak{m}_P(V)$, ami egy ideál $\mathcal{O}_P(V)$-ben.

Mivel $k[X_1,\dots,X_n]$ Noether, ezért 1.4.4.g) szerint $\Gamma(V)=k[X_1,\dots,X_n]/I(V)$ is Noether. Legyen $I\lhd\mathcal{O}_P(V)$. Ekkor $I\cap\Gamma(V)\lhd\Gamma(V)$, így $I\cap\Gamma(V)=(f_1,\dots,f_r)$, $f_i\in\Gamma(V)$. Megmutatjuk, hogy $f_1,\dots,f_r\in\mathcal{O}_P(V)$ generálják I-t. Legyen $f\in I$, ekkor f értelmezve van P-ben, így létezik $b\in\Gamma(V)$, melyre $b(P)\neq 0$ és $bf\in\Gamma(V)$. Tehát $bf\in I\cap\Gamma(V)$, ezért $bf=\sum_{i=1}^r a_if_i$, $a_i\in\Gamma(V)$. Így $f=\sum_{i=1}^r\frac{a_i}{b}f_i$, ahol $b(P)\neq 0$ miatt $\frac{a_i}{b}\in\mathcal{O}_P(V)$. Tehát valóban, $I=(f_1,\dots,f_r)$ végesen generált, így $\mathcal{O}_P(V)$ Noether. □

2.4.4. Állítás. a) *Legyen $\varphi\colon V\to W$ varietások közti polinomiális leképezés és $\widetilde{\varphi}\colon\Gamma(W)\to\Gamma(V)$, $f\mapsto f\circ\varphi$ a neki megfelelő gyűrűhomomorfizmus a koordinátagyűrűk között. Legyen $P\in V$, $\varphi(P)=Q\in W$. Ekkor $\widetilde{\varphi}$ egyértelműen kiterjed $\widetilde{\varphi}\colon\mathcal{O}_Q(W)\to\mathcal{O}_P(V)$ gyűrűhomomorfizmussá. Továbbá $\widetilde{\varphi}(\mathfrak{m}_Q(W))\subset\mathfrak{m}_P(V)$.*

b) *Legyen $T\colon\mathbb{A}^n\to\mathbb{A}^n$ affin koordinátacsere, $V\subset\mathbb{A}^n$ varietás, $Q\in V^T$, és $T(Q)=P$. Ekkor a $T\colon V^T\to V$ megszorítás által indukált $\widetilde{T}\colon\mathcal{O}_P(V)\to\mathcal{O}_Q(V^T)$ gyűrűizomorfizmus, melyre $\widetilde{T}(\mathfrak{m}_P(V))=\mathfrak{m}_Q(V^T)$.*

Bizonyítás. (a) Ha $a/b\in\mathcal{O}_Q(W)$, $a,b\in\Gamma(W)$, $b(Q)\neq 0$, akkor legyen $\widetilde{\varphi}(a/b)=\widetilde{\varphi}(a)/\widetilde{\varphi}(b)=(a\circ\varphi)/(b\circ\varphi)$. Ez jóldefiniált, hiszen ha $a/b=c/d$, akkor $ad-bc=0\in\Gamma(W)$, így $(ad-bc)\circ\varphi=0\in\Gamma(V)$, ezért $(a\circ\varphi)/(b\circ\varphi)=(c\circ\varphi)/(d\circ\varphi)$, és $b(\varphi(P))=b(Q)\neq 0$ miatt $\widetilde{\varphi}(a/b)\in\mathcal{O}_P(V)$. Továbbá gyűrűhomomorfizmus, és $\widetilde{\varphi}$ kiterjesztése csak ez lehet. Ha $f\in\mathfrak{m}_Q(W)$, akkor $f=a/b$, $a(Q)=0$, $b(Q)\neq 0$, így $\widetilde{\varphi}(f)(P)=a(\varphi(P))/b(\varphi(P))=a(Q)/b(Q)=0$, azaz $\widetilde{\varphi}(f)\in\mathfrak{m}_P(V)$.

(b) Legyen T inverze az U affin koordinátacsere. Ekkor a) szerint kiterjednek $\widetilde{T}\colon\mathcal{O}_P(V)\to\mathcal{O}_Q(V^T)$ és $\widetilde{U}\colon\mathcal{O}_Q(V^T)\to\mathcal{O}_P(V)$ homomorfizmusokká. Mivel 2.2.2.a) szerint $\widetilde{T}\circ\widetilde{U}$ a $\Gamma(V^T)$-n és $\widetilde{U}\circ\widetilde{T}$ a $\Gamma(V)$-n az identitás, ezért $\mathcal{O}_Q(V^T)$-n és $\mathcal{O}_P(V)$-n is az identitások, tehát $\widetilde{T}$ izomorfizmus. Továbbá a) szerint $\mathfrak{m}_Q(V^T)=\widetilde{T}(\widetilde{U}(\mathfrak{m}_Q(V^T)))\subset\widetilde{T}(\mathfrak{m}_P(V))\subset\mathfrak{m}_Q(V^T)$. □

2.5. Diszkrét értékelésgyűrűk

Definíció. Az R nullosztómentes gyűrű *diszkrét értékelésgyűrű* (DVR), ha létezik $t\in R$ irreducibilis elem, melyre minden $0\neq z\in R$ egyértelműen felírható $z=ut^n$ alakban, ahol $u\in R$ egység, $n\in\mathbb{N}$. A t elemet *uniformizáló paraméternek* nevezzük.

2.5.1. Példa. Legyen $V=\mathbb{A}^1$, ekkor $\Gamma(V)=k[X]$ hányadosteste $k(V)=k(X)$. Ha $a\in k$, akkor $\mathcal{O}_a(V)$ DVR a $t=X-a$ uniformizáló paraméterrel.

Bizonyítás. Ha $0\neq z\in\mathcal{O}_a(V)$, $z=F/G$, akkor legyen $F=(X-a)^nH$, ahol $X-a$ nem osztja H-t, ekkor $u=H/G$ egység, mert $H(a)\neq 0$ miatt $G/H\in\mathcal{O}_a(V)$. Tehát $z=u(X-a)^n$, és ez a felírás egyértelmű. □

Ha $V\subset\mathbb{A}^2$ varietás, akkor az előző példához hasonlóan tekinteni akarjuk, hogy egy V-n értelmezett $f\in\Gamma(V)$ függvénynek bizonyos $P\in V$ pont „hányszoros gyöke”. Ehhez fogjuk a diszkrét értékelésgyűrűket használni: ha $f=ut^n$, ahol u egység és t a fenti $X-a$ polinomhoz hasonlóan megadott alkalmas elem, annak lesz a szemléletes jelentése az, hogy P n-szeres gyök. Ezért kellett az $\mathcal{O}_P(V)$ lokális gyűrűt

definiálnunk, ami gyakran DVR lesz, mint azt látni fogjuk. Ugyanis abban a pillanatban, hogy kidobtuk azon $g/h \in k(V)$ törteket, melyekre $h(P) = 0$, az $\mathcal{O}_P(V)$ olyan diszkrét értékelésgyűrűvé vált, melynek uniformizáló paraméterének kitevője azt fogja kifejezni, hogy P hányszoros gyök.

2.5.2. Állítás. *Legyen R nullosztómentes gyűrű, nem test. Ekkor R pontosan akkor DVR, ha R lokális Noether-gyűrű, és a maximális ideálja főideál.*

Bizonyítás. Ha R DVR a t uniformizáló paraméterrel, akkor $\mathfrak{m} = (t)$ a nemegységek halmaza, hiszen az egységek nem lehetnek oszthatók t-vel, és R DVR lévén minden nemegység ut^n, $n \geq 1$ alakú. Mivel $\mathfrak{m}$ ideál, ezért R lokális, és az $\mathfrak{m}$ maximális ideálja főideál. Legyen $(0) \neq I \lhd R$, és legyen

$$c = \min\{n \in \mathbb{N} \mid \text{van } z \in I, z = ut^n, u \text{ egység}\}.$$

Ekkor minden I-beli elem osztható t^c-vel, és valamely u egységre $ut^c \in I$, így $I = (t^c)$. Tehát R PID, így Noether.

Legyen R lokális Noether-gyűrű, és a maximális ideálja $\mathfrak{m} = (t)$, megmutatjuk, hogy t uniformizáló paraméter. Ekkor t nem egység, és mivel R nem test, $t \neq 0$, így mivel $\mathfrak{m}$ maximális, ezért t irreducibilis. Tegyük fel, hogy $z = ut^n = vt^m$, $n \geq m$, u, v egység. Ekkor $ut^{n-m} = v$ egység, így $n = m$ és $u = v$, azaz z előállítása egyértelmű. Tegyük fel, hogy $0 \neq z \in R$ nem áll elő ut^n alakban. Ekkor z nem egység, így $z \in \mathfrak{m} = (t)$, ezért $z = z_1 t$, $z_1 \in R$. Ekkor z_1 sem egység, különben z előállna a megfelelő alakban, így $z_1 = z_2 t$, $z_2 \in R$, tehát $z = z_2 t^2$. Ha $z = z_n t^n$, akkor z_n nem egység, így $z_n = z_{n+1} t$, és $z = z_{n+1} t^{n+1}$, tehát minden n-re van olyan $z_n \in R$, hogy $z_{n+1} | z_n$ és $z = z_n t^n$. Ekkor $(z_1) \subset (z_2) \subset \ldots$ ideálok egy családja az R Noether-gyűrűben, így az 1.5.3.a) Állítás szerint létezik (z_n) maximális eleme, de ekkor $(z_n) = (z_{n+1})$ miatt $z_{n+1} t = z_n \,|\, z_{n+1}$, így mivel R nullosztómentes, $t \,|\, 1$, ellentmondás. Tehát minden $0 \neq z \in R$ előáll ut^n alakban, így R DVR. □

Ha R DVR, és t, s uniformizáló paraméterek, akkor $t = us^n$ és $s = vt^m$, u, v egység, így $t = uv^n t^{nm}$, ezért az egyértelműség miatt $1 = nm$, tehát $n = m = 1$, azaz t, s egymás egységszeresei.

Legyen R DVR, K az R hányadosteste. Ha t uniformizáló paraméter, akkor minden $a \in K$ előáll $a = z_1/z_2$, $z_i \in R$ alakban, ahol $z_i = u_i t^{n_i}$, $n_i \in \mathbb{N}$. Így minden $a \in K$ előáll $a = ut^n$, u egység, $n \in \mathbb{Z}$ alakban. Ez a felírás egyértelmű, hiszen $a = ut^n = vt^m$, $n, m \in \mathbb{Z}$, $n \geq m$ esetén $ut^{n-m} = v$, tehát $u = v$, $n = m$. És ha s egy másik uniformizáló paraméter, akkor az t egységszerese, így $a = ut^n = vs^n$, tehát az n kitevők azonosak. Ezek miatt definiálható az a elem rendje.

Definíció. Ha R DVR, K az R hányadosteste, és $a \in K$, akkor $a \neq 0$ *rendje* $\mathrm{ord}(a) = n$, ahol $a = ut^n$, $u \in R$ egység, $t \in R$ uniformizáló paramétere R-nek, és $n \in \mathbb{Z}$. Legyen továbbá $\mathrm{ord}(0) = \infty$.

2.6. Ideálok szorzata

Definíció. Legyen R gyűrű.

a) Ha $I, J \lhd R$, akkor IJ jelöli az $\{ab \mid a \in I, b \in J\}$ által generált ideált.

b) Ha $I_1, \ldots, I_n \lhd R$, akkor $I_1 \ldots I_n$ jelöli az $\{a_1 \ldots a_n \mid a_i \in I_i\}$ által generált ideált. Ha $I \lhd R$, akkor $I^n = I \ldots I$. Legyen $I^0 = R$.

c) Ha $R \subset S$ gyűrű, $I \lhd R$, akkor IS jelöli az I által generált ideált S-ben.

d) Ha $I, J \lhd R$, akkor $I + J = \{a + b \mid a \in I, b \in J\}$.

e) Az $I, J \lhd R$ ideálok *komaximálisak*, ha $I + J = R$.

2.6.1. Állítás. *Legyen R gyűrű, $I, J \lhd R$, $I_1, \ldots, I_N \lhd R$, $n \geq 0$.*

a) *Ha I-t generálja az $A \subset I$, J-t generálja a $B \subset J$ halmaz, akkor IJ-t generálja az $\{ab \mid a \in A, b \in B\}$ halmaz.*

b) $I_1 \ldots I_N = (\ldots((I_1 I_2) I_3) \ldots) I_N$.

c) *Ha $I = (a_1, \ldots, a_r)$, akkor I^n-t generálja az $\{a_1^{i_1} \ldots a_r^{i_r} \mid i_1 + \ldots + i_r = n\}$ halmaz.*

d) $R = I^0 \supset I^1 \supset I^2 \supset \ldots$.

e) *$I + J$ a legkisebb ideál R-ben, ami tartalmazza I-t és J-t.*

f) $(I_1 + I_2)J = I_1 J + I_2 J$.

g) $(I_1 \ldots I_N)^n = I_1^n \ldots I_N^n$.

h) *Ha $R \subset S$ gyűrű, akkor $I^n S = (IS)^n$.*

i) *Ha I végesen generált és $I \subset \mathrm{Rad}(J)$, akkor $I^m \subset J$ valamely m-re.*

Bizonyítás. (a) Azt kell megmutatnunk, hogy

$$IJ = (ij \mid i \in I, j \in J) = (ab \mid a \in A, b \in B) = AB.$$

Világos, hogy $IJ \supset AB$. Mivel minden $i \in I$ előáll $i = \sum_{s=1}^{n} r_s a_s$, $r_s \in R$, $a_s \in A$ és minden $j \in J$ előáll $j = \sum_{t=1}^{m} q_t b_t$, $q_t \in R$, $b_t \in B$ alakban, ezért minden $ij = \sum_{s=1}^{n} \sum_{t=1}^{m} r_s q_t a_s b_t \in AB$, így $IJ \subset AB$.

(b) Azonnal adódik a)-ból.

(c) Indukcióval adódik a)-ból és b)-ből.

(d) Ha $a_1, \ldots, a_{n+1} \in I$, akkor $(a_1 a_2) a_3 \ldots a_{n+1} \in I^n$, így $I^{n+1} \subset I^n$.

(e) $I + J$ valóban ideál, mert zárt az összegre, és minden $r \in R$-rel való szorzásra. És ha egy ideál tartalmaz minden $a \in I, b \in J$ elemet, akkor az $a + b$ elemeket is tartalmazza.

(f) $(I_1 + I_2)J$-t az $(a_1 + a_2)b$ elemek generálják, ahol $a_i \in I_i$,$b \in J$, és $a_1 b + a_2 b \in I_1 J + I_2 J$, így $(I_1 + I_2)J \subset I_1 J + I_2 J$. Mivel $(I_1 + I_2)J \supset I_1 J$ és $(I_1 + I_2)J \supset I_2 J$, így e) szerint $(I_1 + I_2)J \supset I_1 J + I_2 J$.

(g) Mindkét oldalt a) és b) szerint a $\{\prod_{i=1}^{N} \prod_{j=1}^{n} a_{ij} \mid a_{ij} \in I_i\}$ halmaz generálja.

(h) $(IS)^n$-t a) és b) szerint az $A = \{a_1 \ldots a_n \mid a_i \in I\}$ halmaz generálja S-ben, és mivel $I^n = (A)_R$ az A által R-ben generált ideál, így $I^n S = (A)_R S = ((A)_R)_S = (A)_S$ szintén az A által S-ben generált ideál.

(i) Legyen $I = (a_1, \ldots, a_r)$, ekkor $a_i^{n_i} \in J$ alkalmas n_i-re. Legyen $m = n_1 + \ldots + n_r$, ekkor $m = i_1 + \ldots + i_r$ esetén valamelyik $i_j \geq n_j$, így $a_1^{i_1} \ldots a_r^{i_r} \in J$, ezért c) alapján $I^m \subset J$. □

2.6.2. Állítás. *Legyen R gyűrű.*

a) *Tetszőleges I, J-re $IJ \subset I \cap J$.*

b) *Ha* $I, J \lhd R$ *komaximálisak, akkor* $IJ = I \cap J$.

c) *Ha* $I, J \lhd R$ *komaximálisak, akkor* I *és* J^2 *is komaximálisak.*

d) *Ha* $I, J \lhd R$ *komaximálisak, akkor* I^n *és* J^m *is komaximálisak.*

e) *Tegyük fel, hogy* $I_1, \ldots, I_N \lhd R$ *és minden* i*-re* I_i *és* $J_i = \bigcap_{j \neq i} I_j$ *komaximálisak. Ekkor* $I_1^n \cap \ldots \cap I_N^n = (I_1 \cap \ldots \cap I_N)^n$.

f) $I, J \lhd k[X_1, \ldots, X_n]$ *pontosan akkor komaximálisak, ha* $V(I) \cap V(J) = \emptyset$.

Bizonyítás. (a) $IJ \subset I$ és $IJ \subset J$.

(b) Ha $I + J = R$, akkor $I \cap J = (I \cap J)R = (I \cap J)(I + J) = (I \cap J)I + (I \cap J)J$ 2.6.1.f) alapján. $(I \cap J)I + (I \cap J)J \subset JI + IJ = IJ$, így $I \cap J \subset IJ \subset I \cap J$ a) szerint.

(c) Mivel $I + J = R$, létezik $a \in I, b \in J$, hogy $a + b = 1$, azaz $a = 1 - b$. Így $a(1 + b) = 1 - b^2$, azaz $a(1 + b) + b^2 = 1$, ahol $a(1 + b) \in I, b^2 \in J^2$, ezért $I + J^2 = R$.

(d) Indukcióval c) szerint I^{2^N} és J^{2^M} komaximálisak, és ha $n \leq 2^N, m \leq 2^M$, akkor 2.6.1.d) alapján $I^n + J^m \supset I^{2^N} + J^{2^M} = R$.

(e) N szerinti indukcióval, $N = 1$ nyilvánvaló. Ha $I_1, \ldots, I_{N+1}$ teljesíti a fenti komaximalitási feltételeket, akkor $I_1, \ldots, I_N$ is teljesíti. Mivel d) alapján I_{N+1}^n és $(I_1 \cap \ldots \cap I_N)^n$ komaximálisak, így az indukciós feltevés és b) szerint

$$I_1^n \cap \ldots \cap I_N^n \cap I_{N+1}^n = (I_1 \cap \ldots \cap I_N)^n \cap I_{N+1}^n = (I_1 \cap \ldots \cap I_N)^n I_{N+1}^n.$$

Ez 2.6.1.g) és b) alapján

$$(I_1 \cap \ldots \cap I_N)^n I_{N+1}^n = ((I_1 \cap \ldots \cap I_N)I_{N+1})^n = (I_1 \cap \ldots \cap I_N \cap I_{N+1})^n.$$

(f) Ha I, J komaximálisak, akkor $I + J = k[X_1, \ldots, X_n]$, így $V(I) \cap V(J) = V(I \cup J) = V(I + J) = \emptyset$. Ha $\emptyset = V(I) \cap V(J) = V(I + J)$, akkor a Gyenge Nullstellensatz szerint $I + J = k[X_1, \ldots, X_n]$. □

2.6.3. Állítás. a) *Ha* $R = k[X_1, \ldots, X_r]$, $I = (X_1, \ldots, X_r) \lhd R$, *akkor* I^n*-t az* n*-edfokú monomok generálják.* R/I^n *bázisa a* $B = \{\overline{F} \mid \deg F < n \text{ monom}\}$ *halmaz* k *felett.*

b) *Ha* $I = (X, Y) \lhd k[X, Y]$, *akkor* $\dim_k(k[X, Y]/I^n) = \frac{n(n+1)}{2}$.

Bizonyítás. (a) I^n generátora 2.6.1.c) miatt az $\{X_1^{i_1} \ldots X_r^{i_r} \mid i_1 + \ldots + i_r = n\}$ halmaz. Így minden polinom I^n-maradéka megegyezik egy n-nél kisebb fokú polinom maradékával, tehát B generátorrendszer. B lineáris független, mert ha $B = \{\overline{F_1}, \ldots, \overline{F_m}\}$, $\deg F_i < n$, és $\lambda_1\overline{F_1} + \ldots + \lambda_m\overline{F_m} = 0$, akkor az n-nél kisebb fokú $\lambda_1\overline{F_1} + \ldots + \lambda_m\overline{F_m} \in I^n$, így mindegyik $\lambda_i = 0$.

(b) $k[X, Y]/I^2$ bázisa a) szerint az $\{\overline{X^i Y^j} \mid i + j < n\}$, ennek elemszáma pedig $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$. □

2.6.4. Állítás. a) *Legyen* R *gyűrű,* $I, J \lhd R$, $I \subset J$. *Ekkor van egy természetes, szürjektív* $R/I \to R/J$ *gyűrűhomomorfizmus.*

b) *Legyenek* $R \subset S$ *gyűrűk,* $I \lhd R$. *Ekkor van egy természetes* $R/I \to S/IS$ *gyűrűhomomorfizmus.*

Bizonyítás. (a) Legyen $\varphi\colon R/I \to R/J$, $a+I \mapsto a+J$, ez jóldefiniált, homomorfizmus, és szürjektív.

(b) Legyen $\varphi\colon R/I \to S/IS$, $a+I \mapsto a+IS$, ez jóldefiniált, homomorfizmus. □

2.6.5. Állítás. a) *Legyen $V \subset \mathbb{A}^n$ varietás, $P \in V$, $\mathcal{O} = \mathcal{O}_P(V)$, $J \lhd \Gamma(V)$. Ekkor $J\mathcal{O} = \{f/g \mid f \in J, g \in \Gamma(V), g(P) \neq 0\}$.*

b) *Legyen $V \subset \mathbb{A}^n$ varietás, $P = (0,\dots,0) \in V$, $\mathcal{O} = \mathcal{O}_P(V)$, $\mathfrak{m} = \mathfrak{m}_P(V)$. Legyen $I = (x_1,\dots,x_n) \lhd \Gamma(V)$, ahol $x_i = X_i + I(V)$. Ekkor $\mathfrak{m}^r = I^r\mathcal{O}$ minden r-re.*

c) *Legyen $V \subset \mathbb{A}^n$ varietás, $P \in V$, és legyen $I(V) \subset J \lhd k[X_1,\dots,X_n]$. Legyen $J' \lhd \Gamma(V)$ a J képe (1.4.4.b) szerint). Ekkor van egy természetes*

$$\mathcal{O}_P(\mathbb{A}^n)/J\mathcal{O}_P(\mathbb{A}^n) \to \mathcal{O}_P(V)/J'\mathcal{O}_P(V)$$

gyűrűizomorfizmus.

d) *Speciálisan $\mathcal{O}_P(\mathbb{A}^n)/I(V)\mathcal{O}_P(\mathbb{A}^n) \cong \mathcal{O}_P(V)$.*

Bizonyítás. (a) Ha $f \in J$, $g(P) \neq 0$, akkor $1/g \in \mathcal{O}$, így $f/g \in J\mathcal{O}$, tehát $H = \{f/g \mid f \in J, g \in \Gamma(V), g(P) \neq 0\} \subset J\mathcal{O}$. Másrészt $H \lhd \mathcal{O}$, mert először is $\frac{a}{b} \in \mathcal{O}$, $b(P) \neq 0$ esetén $\frac{a}{b}\frac{f}{g} \in H$, mert $af \in J$ és $(bg)(P) \neq 0$, másodszor $f_i \in J$, $g_i(P) \neq 0$ esetén $\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1g_2+f_2g_1}{g_1g_2} \in H$, mert $f_1g_2 + f_2g_1 \in J$ és $(g_1g_2)(P) \neq 0$. Tehát H ideál, és mivel $J \subset H$, így $J\mathcal{O} \subset H$.

(b) Mivel $\mathfrak{m} = \{f/g \mid f,g \in \Gamma(V), f(P) = 0, g(P) \neq 0\}$, és $f = F + I(V)$ esetén $f(P) = 0$ pontosan akkor, ha $F(P) = 0$, azaz $F \in (X_1,\dots,X_n)$, azaz $f \in I$, ezért a) szerint $\mathfrak{m} = I\mathcal{O}$. Így 2.6.1.h) alapján $I^r\mathcal{O} = (I\mathcal{O})^r = \mathfrak{m}^r$.

(c) Legyen $f,g \in k[X_1,\dots,X_n]$, $g(P) \neq 0$ esetén

$$\varphi\colon \mathcal{O}_P(\mathbb{A}^n) \to \mathcal{O}_P(V)/J'\mathcal{O}_P(V), \quad \frac{f}{g} \mapsto \frac{f+I(V)}{g+I(V)} + J'\mathcal{O}_P(V).$$

Ez jóldefiniált, mert $\frac{f}{g} = \frac{f_1}{g_1}$ esetén $fg_1 - f_1g = 0 \in I(V)$, így $\frac{f+I(V)}{g+I(V)} = \frac{f_1+I(V)}{g_1+I(V)}$. φ szürjektív, gyűrűhomomorfizmus, megmutatjuk, hogy $\operatorname{Ker}\varphi = J\mathcal{O}_P(\mathbb{A}^n)$.

Ha $z \in J\mathcal{O}_P(\mathbb{A}^n)$, akkor a) szerint $z = \frac{f}{g}$, $f \in J$, $g(P) \neq 0$, így $f + I(V) \in J'$, ezért $\frac{f+I(V)}{g+I(V)} \in J'\mathcal{O}_P(V)$, tehát $\varphi(z) = 0$. Megfordítva, ha $z = \frac{f}{g}$, $g(P) \neq 0$, $\varphi(z) = 0$, akkor $\frac{f+I(V)}{g+I(V)} \in J'\mathcal{O}_P(V)$, így a) szerint $\frac{f+I(V)}{g+I(V)} = \frac{a+I(V)}{b+I(V)}$, ahol $a \in J$, $b(P) \neq 0$. Tehát $fb - ag \in I(V) \subset J \subset J\mathcal{O}_P(\mathbb{A}^n)$, ezért $\frac{fb-ag}{bg} \in J\mathcal{O}_P(\mathbb{A}^n)$, így $\frac{f}{g} + J\mathcal{O}_P(\mathbb{A}^n) = \frac{a}{b} + J\mathcal{O}_P(\mathbb{A}^n) = 0$, azaz $z = \frac{f}{g} \in J\mathcal{O}_P(\mathbb{A}^n)$.

Tehát $\operatorname{Ker}\varphi = J\mathcal{O}_P(\mathbb{A}^n)$, és így $\mathcal{O}_P(\mathbb{A}^n)/J\mathcal{O}_P(\mathbb{A}^n) \cong \mathcal{O}_P(V)/J'\mathcal{O}_P(V)$ természetes izomorfizmus.

(d) $J = I(V)$ esetén $J' = (0)$, így $\mathcal{O}_P(\mathbb{A}^n)/I(V)\mathcal{O}_P(\mathbb{A}^n)$ és $\mathcal{O}_P(V)/J'\mathcal{O}_P(V) = \mathcal{O}_P(V)$ c) szerint izomorfak. □

2.7. Ideálok, melyek gyökhalmaza véges

2.7.1. Tétel. *Legyen $I \lhd k[X_1,\dots,X_n]$, és tegyük fel, hogy $V(I) = \{P_1,\dots,P_N\}$ véges. Legyen $\mathcal{O}_i = \mathcal{O}_{P_i}(\mathbb{A}^n)$, ekkor létezik egy természetes izomorfizmus:*

$$k[X_1,\dots,X_n]/I \cong \prod_{i=1}^{N} \mathcal{O}_i/I\mathcal{O}_i.$$

Bizonyítás. Legyen $I_i = I(\{P_i\})$, $R = k[X_1, \dots, X_n]/I$, $R_i = \mathcal{O}_i/IO_i$. A természetes $\varphi_i \colon R \to R_i$ homomorfizmusok (2.6.4.b) Állítás) indukálnak egy $\varphi \colon R \to \prod_{i=1}^N R_i$ homomorfizmust. Megmutatjuk, hogy φ izomorfizmus.

A Nullstellensatz szerint $\operatorname{Rad}(I) = I(V(I)) = I(\{P_1, \dots, P_N\}) = \bigcap_{i=1}^N I_i$. Mivel $k[X_1, \dots, X_n]$ Noether, így a 2.6.1.i) Állítás alapján $\left(\bigcap_{i=1}^N I_i\right)^d \subset I$ valamely d-re. Mivel $V\left(\bigcap_{j\neq i} I_j\right) \cap V(I_i) = V(I(\{P_1, \dots, P_{i-1}, P_{i+1}, \dots, P_N\})) \cap V(I(\{P_i\}) = \{P_1, \dots, P_{i-1}, P_{i+1}, \dots, P_N\} \cap \{P_i\} = \emptyset$, ezért a 2.6.2.f) Állítás szerint $\bigcap_{j\neq i} I_j$ és I_i komaximálisak minden i-re. Így a 2.6.2.e) Állítás alapján $\bigcap_{i=1}^N I_i^d = \left(\bigcap_{i=1}^N I_i\right)^d \subset I$.

Az 1.3.3.c) Állítás szerint léteznek olyan $F_i \in k[X_1, \dots, X_n]$ polinomok, hogy $F_i(P_i) = 1$ és $F_i(P_j) = 0$, ha $i \neq j$. Legyen $E_i = 1 - (1 - F_i^d)^d$. Ekkor $F_i^d \mid E_i$, és mivel $F_i \in I_j$, ezért $E_i \in I_j^d$, ha $i \neq j$. Továbbá $(1-F_j^d)(P_j) = 0$, azaz $1-F_j^d \in I_j$, így $1-E_j = (1-F_j^d)^d \in I_j^d$. Tehát $(1-E_j) - \sum_{i\neq j} E_i \in I_j^d$, ezért $1-\sum_{i=1}^N E_i \in \bigcap_{j=1}^N I_j^d \subset I$. Másrészt $E_i - E_i^2 = E_i(1-E_i) \in \left(\bigcap_{j\neq i} I_j^d\right) I_i^d \subset \bigcap_{j=1}^N I_j^d \subset I$. Harmadrészt $i \neq j$ esetén $E_iE_j \in \left(\bigcap_{j\neq i} I_j^d\right) I_i^d \subset I$.

Legyen $e_i = E_i + I \in R$, ekkor $\sum_{i=1}^N e_i = 1$, $e_i = e_i^2$, és $e_ie_j = 0$, ha $i \neq j$.

Megmutatjuk, hogy ha $G \in k[X_1, \dots, X_n]$, $g = G + I$, és adott i-re $G(P_i) \neq 0$, akkor $g \mid e_i$. Feltehető, hogy $G(P_i) = 1$, mert ha $\lambda = 1/G(P_i) \in k$, és $\lambda g \mid e_i$, akkor $g \mid e_i$. Legyen $H = 1 - G$, ekkor $H \in I_i$, így $E_iH^d \in \left(\bigcap_{j\neq i} I_j^d\right) I_i^d \subset I$. Tehát $E_i - E_iH^d = E_i(1-H)(1 + H + \ldots + H^{d-1})$, így $e_i = e_ig(1 + h + \ldots + h^{d-1})$, ezért $g \mid e_i$.

Tegyük fel, hogy $\varphi(f) = 0$, $f = F + I \in R$. Ekkor minden i-re $0 = \varphi_i(f) = F + I\mathcal{O}_i$, azaz $F \in I\mathcal{O}_i$, ezért 2.6.5.a) alapján létezik olyan $G_i \in k[X_1, \dots, X_n]$, $G_i(P_i) \neq 0$, hogy $FG_i \in I$. Legyen $t_i \in R$ olyan, hogy $g_it_i = e_i$. Ekkor $f = \sum_{i=1}^N e_if = \sum_{i=1}^N t_ig_if = 0$, tehát φ injektív.

Mivel $E_i(P_i) = 1$, ezért $1/E_i \in \mathcal{O}_i$, így $\varphi_i(e_i) = E_i + I\mathcal{O}_i$ egység R_i-ben. Mivel $0 = \varphi_i(e_ie_j) = \varphi_i(e_i)\varphi_i(e_j)$, ezért $\varphi_i(e_j) = 0$, ha $i \neq j$. Így $1 = \varphi_i(1) = \varphi_i\left(\sum_{j=1}^N e_j\right) = \varphi_i(e_i) = E_i + I\mathcal{O}_i$. Legyen $z = \left(\ldots, \frac{H_i}{G_i} + I\mathcal{O}_i, \ldots\right) \in \prod_{i=1}^N R_i$, $G_i(P_i) \neq 0$, és legyen $t_i = T_i + I \in R$ olyan, hogy $g_it_i = e_i$. Ekkor $G_iT_i - E_i \in I \subset I\mathcal{O}_i$, így $1 = E_i + I\mathcal{O}_i = G_iT_i + I\mathcal{O}_i$, ezért $T_i(P_i) \neq 0$, és $\frac{H_i}{G_i} + I\mathcal{O}_i = \frac{H_iT_i}{G_iT_i} + I\mathcal{O}_i = \frac{H_iT_i + I\mathcal{O}_i}{G_iT_i + I\mathcal{O}_i} = H_iT_i + I\mathcal{O}_i$. Így $\varphi_i\left(\sum_{j=1}^N h_jt_je_j\right) = \varphi_i(h_it_i) = H_iT_i + I\mathcal{O}_i = \frac{H_i}{G_i} + I\mathcal{O}_i$ minden i-re, ezért $\varphi\left(\sum_{j=1}^N h_jt_je_j\right) = z$, tehát φ szürjektív. □

2.8. Egzakt sorok

Definíció. a) Legyenek $\varphi \colon M_1 \to M_2$, $\psi \colon M_2 \to M_3$ R-modulushomomorfizmusok. Azt mondjuk, hogy $M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3$ *egzakt sor*, ha $\operatorname{Im}\varphi = \operatorname{Ker}\psi$.

b) Legyenek $\varphi_i \colon M_i \to M_{i+1}$ R-modulushomomorfizmusok. Azt mondjuk, hogy $M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} \ldots \xrightarrow{\varphi_n} M_{n+1}$ *egzakt sor*, ha $\operatorname{Im}\varphi_i = \operatorname{Ker}\varphi_{i+1}$ minden $1 \leq i < n$ esetén.

Vegyük észre, hogy minden M R-modulusra egyértelműen léteznek $0 \longrightarrow M$ és $M \longrightarrow 0$ modulushomomorfizmusok. Így $M_1 \xrightarrow{\varphi} M_2 \longrightarrow 0$ pontosan akkor egzakt, ha φ szürjektív, és $0 \longrightarrow M_1 \xrightarrow{\varphi} M_2$ pontosan akkor egzakt, ha φ injektív.

2.8.1. Állítás. *Legyenek V_1, V_2, V_3 k feletti véges dimenziós vektorterek, azaz k-modulusok, és tegyük fel, hogy a $0 \longrightarrow V_1 \xrightarrow{\varphi} V_2 \xrightarrow{\psi} V_3 \longrightarrow 0$ sor egzakt. Ekkor* $\dim V_1 + \dim V_3 = \dim V_2$.

Bizonyítás. Mivel ψ szürjektív, $\operatorname{Im}\psi = V_3$, és mivel φ injektív, ezért $\dim V_1 = \dim \operatorname{Im}\varphi = \dim \operatorname{Ker}\psi$. Mivel ψ lineáris leképezés, így a lineáris algebrai dimenziótétel alapján $\dim V_2 = \dim \operatorname{Ker}\psi + \dim \operatorname{Im}\psi = \dim V_1 + \dim V_3$. □

2.8.2. Állítás. a) *Legyenek $N \subset M$ modulusok, $\pi\colon M \to M/N$ a természetes homomorfizmus, és $\varphi\colon M \to M'$ olyan modulushomomorfizmus, melyre $\varphi(N) = 0$. Ekkor egyértelműen létezik olyan $\overline{\varphi}\colon M/N \to M'$ modulushomomorfizmus, melyre $\varphi = \overline{\varphi} \circ \pi$.*

b) *Ha $P \subset N \subset M$ modulusok, akkor léteznek természetes $M/P \to M/N$ és $N/P \to M/P$ modulushomomorfizmusok. Ezekkel egzakt sor a*

$$0 \longrightarrow N/P \longrightarrow M/P \longrightarrow M/N \longrightarrow 0.$$

c) *Ha $U \subset V \subset W$ vektorterek, W/U véges dimenziós, akkor*

$$\dim(W/U) = \dim(W/V) + \dim(V/U).$$

d) *Ha $J \subset I$ ideálok az R gyűrűben, akkor van egy természetes*

$$0 \longrightarrow I/J \longrightarrow R/J \longrightarrow R/I \longrightarrow 0$$

egzakt sora R-modulusoknak

e) *Ha $\mathcal{O}$ lokális gyűrű az $\mathfrak{m}$ maximális ideállal, akkor van egy természetes*

$$0 \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \longrightarrow \mathcal{O}/\mathfrak{m}^{n+1} \longrightarrow \mathcal{O}/\mathfrak{m}^n \longrightarrow 0$$

egzakt sora $\mathcal{O}$-modulusoknak.

Bizonyítás. (a) Legyen $\overline{\varphi}(a+N) = \varphi(a)$, ekkor $a+N = b+N$ esetén $a-b \in N$ így $\varphi(a) - \varphi(b) = 0$, tehát $\overline{\varphi}$ jóldefiniált, modulushomomorfizmus, és $\varphi = \overline{\varphi} \circ \pi$. Másfelől $\varphi = \overline{\varphi} \circ \pi$ miatt $\overline{\varphi}$ csak ez lehet.

(b) A természetes $\pi\colon M \to M/N$ homomorfizmusra $P \subset N$ miatt $\pi(P) = 0$, így a) szerint $\overline{\pi}\colon M/P \to M/N$. Mivel $N \subset M$, ezért $N/P \subset M/P$, ez a φ beágyazás a természetes modulushomomorfizmus. Ekkor φ injektív és $\overline{\pi}$ szürjektív. $\operatorname{Ker}\overline{\pi} = \{a+P \mid \pi(a) = 0\} = \{a+P \mid a \in N\} = N/P = \operatorname{Im}\varphi$, tehát a sor egzakt.

(c) b) szerint $0 \longrightarrow V/U \longrightarrow W/U \longrightarrow W/V \longrightarrow 0$ természetes egzakt sor, így a 2.8.1. Állítás miatt készen vagyunk.

(d) $J \subset I \subset R$ R-modulusok, így b) szerint kész.

(e) $\mathfrak{m}^{n+1} \subset \mathfrak{m}^n$ ideálok $\mathcal{O}$-ban, így d) szerint kész. □

2.8.3. Állítás. *Legyen R DVR az $\mathfrak{m}$ maximális ideállal, és legyen $k \subset R$ úgy, hogy $\pi\colon k \to R/\mathfrak{m}$, $\lambda \mapsto \lambda + \mathfrak{m}$ gyűrűizomorfizmus. Ekkor*

a) *$\mathfrak{m}^n/\mathfrak{m}^{n+1}$ k-modulus, és $\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = 1$ minden $n \geq 0$-ra.*

b) *$\dim_k(R/\mathfrak{m}^n) = n$ minden $n \geq 0$-ra.*

c) *Legyen* $z \in R$. *Ekkor* $\operatorname{ord}(z) = n$ *pontosan akkor, ha* $(z) = \mathfrak{m}^n$. *Tehát* $\operatorname{ord}(z) = \dim_k(R/(z))$.

Bizonyítás. (a) Mivel $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ R-modulus, és $k \subset R$, ezért k-modulus is. Ha R uniformizáló paramétere t, akkor $\mathfrak{m} = (t)$. Ezért 2.6.1.c) szerint $\mathfrak{m}^n = (t^n)$ és $\mathfrak{m}^{n+1} = (t^{n+1})$. Legyen $\varphi\colon k \to \mathfrak{m}^n/\mathfrak{m}^{n+1}$, $\lambda \mapsto \lambda t^n + (t^{n+1})$, ekkor φ gyűrűhomomorfizmus. Ha $\varphi(\lambda) = 0$, akkor $t^{n+1} \mid \lambda t^n$, azaz $t \mid \lambda$, így $\pi(\lambda) = 0$, és mivel π injektív, $\lambda = 0$, tehát φ injektív. Legyen $z \in \mathfrak{m}^n/\mathfrak{m}^{n+1}$, $z = w + \mathfrak{m}^{n+1}$, $w \in \mathfrak{m}^n$, ekkor $w = vt^n$, $v \in R$. Mivel π szürjektív, létezik $\lambda \in k$, $\lambda + \mathfrak{m} = v + \mathfrak{m}$, ekkor $\lambda - v \in (t)$, így $\lambda t^n - vt^n \in (t^{n+1})$, ezért $\varphi(\lambda) = \lambda t^n + (t^{n+1}) = vt^n + (t^{n+1}) = z$, tehát φ szürjektív. Így φ izomorfizmus, és $\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \dim_k(k) = 1$.

(b) n szerinti indukcióval, $n = 0$-ra $R/\mathfrak{m}^n = R/R = \{0\}$, és $\dim_k(\{0\}) = 0$. Mivel $\mathfrak{m}^{n+1} \subset \mathfrak{m}^n \subset R$ vektorterek k felett, ezért 2.8.2.c) szerint $\dim_k(R/\mathfrak{m}^{n+1}) = \dim_k(R/\mathfrak{m}^n) + \dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = n + 1$ az indukciós feltevés és a) alapján.

(c) Ha $n \in \mathbb{N}$, akkor $\operatorname{ord}(z) = n$ ekvivalens azzal, hogy $z = ut^n$, u egység, azaz $(z) = (t^n)$, azaz $(z) = \mathfrak{m}^n$. Tehát b) alapján, ha $z \neq 0$, akkor $\operatorname{ord}(z) = n$ esetén $\dim_k(R/(z)) = \dim_k(R/\mathfrak{m}^n) = n$, míg $z = 0$ esetén $\operatorname{ord}(z) = \infty$ és $\dim_k(R/(z)) = \infty$, mert b) miatt minden n-re $\dim_k(R) \geq \dim_k(R/\mathfrak{m}^n) = n$. □

3. fejezet

Síkgörbék lokális tulajdonságai

3.1. Szinguláris pontok, érintők

Definíció. a) Az $F, G \in k[X,Y]$ polinomok *ekvivalensek*, ha $F = \lambda G$ valamely $0 \neq \lambda \in k$-ra. Ez egy ekvivalenciareláció, a $k[X,Y] \setminus \{0\}$ halmaz e szerinti ekvivalenciaosztályait nevezzük *affin síkgörbéknek*. Gyakran nem beszélünk ekvivalenciaosztályról, és csak annyit mondunk például, hogy „az $Y^2 - X^3$ görbe", sőt néha „az $Y^2 = X^3$ görbe".

b) Egy síkgörbe *foka* az ekvivalenciaosztályba eső polinomok közös foka. Az elsőfokú síkgörbék az *egyenesek*.

c) Ha $F \in k[X,Y]$ prímtényezős felbontása $F = F_1^{n_1} \dots F_r^{n_r}$, akkor az F_i görbéket az F *komponenseinek* hívjuk, n_i az F_i komponens *multiplicitása* F-ben.

d) Ha $F \in k[X,Y]$ irreducibilis, akkor a $V(F)$ varietásra és a $\Gamma(V(F))$, $k(V(F))$, $\mathcal{O}_P(V(F))$, $\mathfrak{m}_P(V(F))$ struktúrákra ezentúl az F, $\Gamma(F)$, $k(F)$, $\mathcal{O}_P(F)$, $\mathfrak{m}_P(F)$ jelöléseket is használjuk.

Vegyük észre, hogy ha $F = F_1^{n_1} \dots F_r^{n_r}$, akkor az F_i komponensek $V(F)$-ből leolvashatók (1.6.4. Állítás), de az n_i multiplicitások nem.

3.1.1. Állítás. *Ha $F \in k[X,Y]$ homogén, nem konstans, akkor F lineáris tényezőkre bomlik.*

Bizonyítás. Legyen $F = Y^r G$, ahol Y nem osztja G-t, $\deg G = n$. Legyen $g = G(X,1)$, ekkor $G = G(X/Y,1)Y^n = g(X/Y)Y^n$. Mivel Y nem osztja G-t, ezért $\deg g = n$, és mivel k algebrailag zárt, $g = c(X - a_1)\dots(X - a_n)$, ahol $c, a_i \in k$. Így $F = Y^r G = cY^r(X - a_1 Y)\dots(X - a_n Y)$. □

Definíció. Legyen F síkgörbe, és $P = (a,b)$.

a) $P \in F$ *sima pontja* F-nek, ha F parciális deriváltjaira $\partial_X F(P) \neq 0$ vagy $\partial_Y F(P) \neq 0$. Ha P nem sima pont, akkor P *szinguláris pontja* F-nek.

Legyen $Q = (0,0)$, $F = F_m + F_{m+1} + \dots + F_n$, ahol $\deg F_i = i$ homogén, és $F_m \neq 0$.

b) Az F_m polinomot az F polinom *min-részének* nevezzük.

c) Az F síkgörbe *multiplicitása* Q-ban $m_Q(F) = m$. Ha $m = 1,2,3$, akkor azt is mondjuk, hogy Q egyszeres, dupla, illetve tripla pontja F-nek.

d) Mivel F_m kétváltozós homogén polinom, ezért $m > 0$ esetén 3.1.1. szerint $F_m = L_1^{e_1} \dots L_s^{e_s}$ lineáris tényezőkre bomlik, ahol L_i, L_j különböző egyenesek $i \neq j$-re. Az L_i egyeneseket az F *Q-beli érintőinek* nevezzük, e_i az L_i érintő *multiplicitása*. Ha L olyan Q-n átmenő egyenes, mely egyik L_i-vel sem azonos, akkor azt mondjuk, hogy L érintési multiplicitása 0.

Legyen $T = (X + a, Y + b)$ az az eltolás, mely $Q = (0, 0)$-t $P = (a, b)$-be viszi, ekkor $F^T = F(X + a, Y + b)$.

e) F multiplicitása P-ben $m_P(F) = m_Q(F^T)$, azaz írjuk fel az F^T polinomot $F^T = G_m + G_{m+1} + \ldots + G_n$, $\deg G_i = i$ homogén, $G_m \neq 0$ alakban, ekkor $m_P(F) = m$.

f) Ha $G_m = L_1^{e_1} \dots L_s^{e_s}$, $L_i = c_i X + d_i Y$, akkor a $c_i(X - a) + d_i(Y - b)$ egyeneseket hívjuk az F *P-beli érintőinek*. A P-n átmenő L egyenes érintési *multiplicitása* legyen az L^T egyenes Q-beli érintési multiplicitása.

3.1.2. Példa. A bevezetőbeli F, G polinomok min-része

$$F_3 = 3X^2Y - Y^3 = Y(\sqrt{3}X - Y)(\sqrt{3}X + Y), \quad G_4 = -4X^2Y^2,$$

amely pontosan megfelel a szemléletes képünknek az origóbeli érintőkről.

3.1.3. Állítás. a) *$P \in F$ pontosan akkor, ha $m_P(F) > 0$.*

b) *P sima pont pontosan akkor, ha $m_P(F) = 1$.*

c) *Ha $P = (a, b)$ sima pont, akkor F P-beli érintője a következő egyenes:*

$$\partial_X F(P)(X - a) + \partial_Y F(P)(Y - b) = 0.$$

d) *Ha $F = F_1 \dots F_r$, $P \in F$, akkor $m_P(F) = \sum_{i=1}^r m_P(F_i)$. Speciálisan P pontosan akkor sima pontja F-nek, ha P pontosan egy F_i komponensnek része, F_i egyszeres komponense F-nek, és P sima pontja F_i-nek.*

e) *Ha az L egyenes F_i-nek e_i-szeres érintője P-ben, akkor $F_1 \dots F_r$-nek $\sum_{i=1}^r e_i$-szeres érintője.*

Bizonyítás. (a) Legyen $Q = (0, 0)$ és T a $T(Q) = P$ eltolás. Ekkor $P \in F$ pontosan akkor, ha $0 = F(P) = F(T(Q)) = F^T(Q)$, az $F^T = G_0 + G_1 + \ldots + G_n$ ($\deg G_i = i$ homogén) felírással ez azt jelenti, hogy $G_0 = 0$, azaz $0 < m_Q(F^T) = m_P(F)$.

(b) Mivel $F^T = F(X + a, Y + b)$, ezért $\partial_X(F^T)(Q) = \partial_X F(P)$, $\partial_Y(F^T)(Q) = \partial_Y F(P)$, és $P \in F$ pontosan akkor, ha $Q \in F^T$. Így F-nek P pontosan akkor sima pontja, ha F^T-nek Q sima pontja. Ha $F^T = c + dX + eY + G_2 + \ldots + G_n$, akkor Q pontosan akkor sima pont, ha $Q \in F^T$ azaz $c = 0$, és $\partial_X(F^T)(Q) = d \neq 0$ vagy $\partial_Y(F^T)(Q) = e \neq 0$. Ez éppen azt jelenti, hogy $G_0 = 0$ és $G_1 \neq 0$, azaz $m_P(F) = m_Q(F^T) = 1$.

(c) Mivel $F^T = dX + eY + G_2 + \ldots + G_n$, ahol $(d, e) \neq (0, 0)$, ezért F^T Q-beli érintője $G_1 = dX + eY$, így F P-beli érintője $d(X - a) + e(Y - b)$, ahol $d = \partial_X(F^T)(Q) = \partial_X F(P)$ és $e = \partial_Y(F^T)(Q) = \partial_Y F(P)$.

(d) $F^T = F_1 \dots F_r \circ T = F_1^T \dots F_r^T$. Mivel F_i^T min-része $m_P(F_i)$ fokú, és F^T min-része megegyezik az F_i^T tényezők min-részeinek szorzatával, ezért $m_P(F) = m_Q(F^T) = \sum_{i=1}^r m_P(F_i)$. Így ha $F = F_1^{n_1} \dots F_r^{n_r}$ prímtényezős felbontás, akkor

$m_P(F) = 1$ pontosan akkor, ha valamelyik $m_P(F_i) = 1$, $n_i = 1$, és a többi $m_P(F_j) = 0$.

(e) Mivel L^T az F_i^T min-részének lineáris tényezős felbontásában e_i kitevővel szerepel, ezért F^T min-részében $\sum_{i=1}^r e_i$ kitevővel. □

3.2. Multiplicitás és lokális gyűrű

3.2.1. Tétel. *Legyen F irreducibilis síkgörbe, $P \in F$. Ekkor minden elég nagy n-re*

$$m_P(F) = \dim_k(\mathfrak{m}_P(F)^n/\mathfrak{m}_P(F)^{n+1}).$$

Speciálisan, F multiplicitása P-ben leolvasható az $\mathcal{O}_P(F)$ lokális gyűrűből.

Bizonyítás. Legyen $\mathcal{O} = \mathcal{O}_P(F)$, $\mathfrak{m} = \mathfrak{m}_P(F)$. Ekkor 2.4.3 szerint $\mathcal{O}$ lokális gyűrű az $\mathfrak{m}$ maximális ideállal, így 2.8.2.e) szerint

$$0 \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \longrightarrow \mathcal{O}/\mathfrak{m}^{n+1} \longrightarrow \mathcal{O}/\mathfrak{m}^n \longrightarrow 0$$

egzakt sora k-modulusoknak. Elég tehát megmutatni, hogy $n \geq m_P(F)$ esetén $\dim_k(\mathcal{O}/\mathfrak{m}^n) = nm_P(F) + s$ valamely s konstanssal, mert ekkor 2.8.1. szerint

$$\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \dim_k(\mathcal{O}/\mathfrak{m}^{n+1}) - \dim_k(\mathcal{O}/\mathfrak{m}^n) = m_P(F).$$

Legyen $Q = (0,0)$, $T(Q) = P$ affin koordinátacsere, ekkor 2.4.4.b) szerint $\widetilde{T}\colon \mathcal{O}_P(F) \to \mathcal{O}_Q(F^T)$ izomorfizmus, melynél $\mathfrak{m}_P(F)$ képe $\mathfrak{m}_Q(F^T)$, és definíció szerint $m_P(F) = m_Q(F^T)$. Ezért feltehető, hogy $P = (0,0)$.

Ekkor a 2.6.5.b) Állítás alapján $\mathfrak{m}^n = i^n\mathcal{O}$, ahol $i = (x,y) \lhd \Gamma(F)$, $x = X + (F)$, $y = Y + (F)$. Legyen $I = (X,Y) \lhd k[X,Y]$, ekkor $V(I^n, F) = \{P\}$ véges, így a 2.7.1. Tétel alapján

$$k[X,Y]/(I^n,F) \cong \mathcal{O}_P(\mathbb{A}^2)/(I^n,F)\mathcal{O}_P(\mathbb{A}^2).$$

A 2.6.5.c) Állítás szerint pedig, mivel az $(F) \subset (I^n,F) \lhd k[X,Y]$ ideál képe $(i^n) \lhd \Gamma(F)$, ezért

$$\mathcal{O}_P(\mathbb{A}^2)/(I^n,F)\mathcal{O}_P(\mathbb{A}^2) \cong \mathcal{O}_P(F)/(i^n)\mathcal{O}_P(F) = \mathcal{O}/\mathfrak{m}^n.$$

Tehát $\dim_k(\mathcal{O}/\mathfrak{m}^n) = \dim_k(k[X,Y]/(I^n,F))$.

Legyen $m = m_P(F) \leq n$. Ekkor 3.1.3.d) szerint $m_P(FG) = m_P(F) + m_P(G) = m + m_P(G)$, és mivel $I^r = \{G \in k[X,Y] \mid m_P(G) \geq r\}$, ezért $FG \in I^n$ pontosan akkor, ha $n \leq m_P(FG) = m + m_P(G)$, azaz $G \in I^{n-m}$. 2.6.4.a) alapján létezik egy természetes $\varphi\colon k[X,Y]/I^n \to k[X,Y]/(I^n,F)$ gyűrűhomomorfizmus, és legyen $\psi\colon k[X,Y]/I^{n-m} \to k[X,Y]/I^n$, $G + I^{n-m} \mapsto FG + I^n$. Ekkor az előző észrevétel szerint ψ jóldefiniált és injektív k-lineáris leképezés. Így a k-modulusok

$$0 \longrightarrow k[X,Y]/I^{n-m} \xrightarrow{\psi} k[X,Y]/I^n \xrightarrow{\varphi} k[X,Y]/(I^n,F) \longrightarrow 0$$

sora egzakt, mert ψ injektív, φ szürjektív, és $\operatorname{Ker}\varphi = \{H + I^n \mid H \in (I^n,F)\} = \{H + I^n \mid H \in (F)\} = \{FG + I^n \mid G \in k[X,Y]\} = \operatorname{Im}\psi$. A 2.6.3.b) Állítás

szerint $\dim_k(k[X,Y]/I^n) = \frac{n(n+1)}{2}$ és $\dim_k(k[X,Y]/I^{n-m}) = \frac{(n-m)(n-m+1)}{2}$, ezért 2.8.1. alapján

$$\dim_k(k[X,Y]/(I^n,F)) = \frac{n(n+1)}{2} - \frac{(n-m)(n-m+1)}{2} = nm - \frac{m(m-1)}{2},$$

tehát $\dim_k(\mathcal{O}/\mathfrak{m}^n) = nm + s$ minden $n \geq m$-re, és így készen vagyunk. □

3.2.2. Tétel. *Legyen F irreducibilis síkgörbe, $P \in F$. Ekkor P pontosan akkor sima pontja F-nek, ha $\mathcal{O}_P(F)$ DVR. Ha P sima pont és L olyan P-n átmenő egyenes, mely nem érinti P-ben F-et, akkor $\ell = L + (F) \in \mathcal{O}_P(F)$ uniformizáló paraméter.*

Bizonyítás. Legyen P sima pont, L nem érintő P-ben. A 2.3.2.d) Állítás szerint van olyan T affin koordinátacsere, mely $Q = (0,0)$-t és az X, Y egyeneseket rendre P-be, L-be, és F P-beli érintőjébe viszi. A 2.4.4.b) Állítás alapján $\widetilde{T}\colon \mathcal{O}_P(F) \to \mathcal{O}_Q(F^T)$ gyűrűizomorfizmus, így $\mathcal{O}_P(F)$ pontosan akkor DVR, ha $\mathcal{O}_Q(F^T)$ az, és ℓ pontosan akkor uniformizáló paramétere $\mathcal{O}_P(F)$-nek, ha $\widetilde{T}(\ell) = (L+(F))\circ T = L\circ T + (F^T) = X + (F^T)$ uniformizáló paramétere $\mathcal{O}_Q(F^T)$-nek. Ezért feltehető, hogy $P = (0,0)$, $L = X$, és F P-beli érintője Y.

Ekkor $F = Y + F_2 + \ldots$, mert F P-beli érintője Y. Így $F = YG - X^2H$ valamely $G = 1 + G_1 + \ldots \in k[X,Y]$ és $H \in k[X]$ polinomokkal. Ezért az (F)-maradékot kisbetűvel jelölve, $yg = x^2h$, ahol $g(P) \neq 0$. Mivel $P = (0,0)$, ezért a 2.6.5.b) Állítás szerint $\mathfrak{m}_P(F) = (x,y) \lhd \mathcal{O}_P(F)$. De $h/g \in \mathcal{O}_P(F)$ miatt $y = x^2h/g \in (x)$, így $(x,y) = (x)$. A 2.4.3. Állítás szerint $\mathcal{O}_P(F)$ nullosztómentes, lokális és Noether, és most láttuk be, hogy a maximális ideálja $\mathfrak{m}_P(F) = (x)$ főideál. Ezért a 2.5.2. Állítás alapján $\mathcal{O}_P(F)$ DVR. És mivel $\mathfrak{m}_P(F) = (x)$, ezért az $L = X$ egyenes $\Gamma(F)$-beli képe uniformizáló paraméter.

Megfordítva, ha $\mathcal{O}_P(F)$ DVR, akkor $\mathcal{O}_P(F)/\mathfrak{m}_P(F)$ természetes módon izomorf k-val, így a 2.8.3.a) Állítás szerint $1 = \dim_k(\mathfrak{m}_P(F)^n/\mathfrak{m}_P(F)^{n+1}) = m_P(F)$ az előző tétel alapján, ha n elég nagy. Tehát P sima pontja F-nek. □

Definíció. a) Legyen F irreducibilis síkgörbe, $P \in F$ sima pont. Ekkor ord_P^F jelöli az $\mathcal{O}_P(F)$ DVR által definiált $a \mapsto \mathrm{ord}(a)$ rendfüggvényt $k(F)$-en. Ha $G \in k[X,Y]$, $g = G + (F) \in \Gamma(F)$, akkor gyakran $\mathrm{ord}_P^F(G)$-t írunk $\mathrm{ord}_P^F(g)$ helyett.

b) Ha F reducibilis síkgörbe, $P \in F$ sima pont, és F_i az F P-t tartalmazó komponense, akkor ord_P^F-et írunk $\mathrm{ord}_P^{F_i}$ helyett.

3.2.3. Állítás. *Legyen P sima pont az F síkgörbén, L P-n átmenő egyenes.*

a) *Ha L nem érinti F-et P-ben, akkor* $\mathrm{ord}_P^F(L) = 1$.

b) *Ha L érinti F-et P-ben, akkor* $\mathrm{ord}_P^F(L) > 1$.

Bizonyítás. (a) Az előző tétel szerint L képe uniformizáló paraméter $\mathcal{O}_P(F_i)$-ben, így a rendje 1.

(b) Feltehető, hogy F irreducibilis, $P = (0,0)$, és $L = Y$, mert $T(Q) = P$ affin koordinátacserével $\mathcal{O}_P(F)$ és $\mathcal{O}_Q(F^T)$ olyan izomorfiáját kapjuk, melyben $\widetilde{T}(L + (F)) = L^T + (F^T)$, azaz L $\mathcal{O}_P(F)$-beli képének megfelel L^T $\mathcal{O}_Q(F^T)$-beli képe, és így $\mathrm{ord}_P^F(L) = \mathrm{ord}_Q^{F^T}(L^T)$. Ekkor az előző tétel bizonyításában látottak alapján L képe $y = x^2h/g$, ahol $h/g \in \mathcal{O}_P(F)$. Ezért $\mathrm{ord}_P^F(L) = \mathrm{ord}_P^F(x^2) + \mathrm{ord}_P^F(h/g) \geq 2$. □

3.3. Metszési multiplicitás

Legyenek F, G síkgörbék, $P \in \mathbb{A}^2$. Definiálni fogunk egy $I(P, F \cap G)$-vel jelölt metszési multiplicitási számot. Ehhez először megadunk 7 tulajdonságot, amit elvárunk a metszési multiplicitástól, majd bebizonyítjuk, hogy ezek már egyértelműen meghatározzák azt. Eközben egy viszonylag egyszerű algoritmust is készíteni fogunk $I(P, F \cap G)$ kiszámítására.

Tulajdonságok. Bármely F, G síkgörbékre és P pontra

(1) $I(P, F \cap G) \in \mathbb{N}$, ha F-nek és G-nek nincs azonos komponense P-n keresztül, és $I(P, F \cap G) = \infty$, ha van.

(2) $I(P, F \cap G) = 0$ pontosan akkor, ha $P \notin F \cap G$. $I(P, F \cap G)$ csak F és G P-t tartalmazó komponenseitől függ.

(3) Ha $T\colon \mathbb{A}^2 \to \mathbb{A}^2$ affin koordinátacsere, $T(Q) = P$, akkor $I(P, F \cap G) = I(Q, F^T \cap G^T)$.

(4) $I(P, F \cap G) = I(P, G \cap F)$.

(5) $I(P, F \cap G) \geq m_P(F)m_P(G)$, és $I(P, F \cap G) = m_P(F)m_P(G)$ pontosan akkor, ha F-nek és G-nek nincs azonos érintője P-ben.

(6) $F = F_1^{r_1} \dots F_n^{r_n}$, $G = G_1^{s_1} \dots G_m^{s_m}$-re $I(P, F \cap G) = \sum_{i=1}^{n} \sum_{j=1}^{m} r_i s_j I(P, F_i \cap G_j)$.

(7) $I(P, F \cap G) = I(P, F \cap (G + AF))$ tetszőleges $A \in k[X, Y]$ esetén.

Ha F vagy G nem nulla konstans, akkor (2) alapján $I(P, F \cap G) = 0$. (5) egyik speciális esete az, hogy ha P sima pontja F-nek és G-nek, és F P-beli érintője különbözik G P-beli érintőjétől, akkor $I(P, F \cap G) = 1$ legyen. (7) egy jelentése pedig az, hogy ha F irreducibilis, akkor $I(P, F \cap G)$ csak G $\Gamma(F)$-beli $g = G + (F)$ képétől függjön.

3.3.1. Tétel. *Egyértelműen létezik egy olyan $I(P, F \cap G)$ metszési multiplicitási szám, mely minden F, G síkgörbére és P pontra definiálva van, és teljesíti az* (1)–(7) *tulajdonságokat. Ez a következő képlettel adható meg:*

$$I(P, F \cap G) = \dim_k(\mathcal{O}_P(\mathbb{A}^2)/(F, G)).$$

Bizonyítás. (Egyértelműség.) Tegyük fel, hogy $I(P, F \cap G)$ minden F, G, P-re definiálva van, és teljesíti az (1)–(7) tulajdonságokat. Megadunk egy algoritmust az $I(P, F \cap G)$ kiszámítására, ebből nyilván következik az egyértelműség.

(3) miatt feltehető, hogy $P = (0, 0)$. Ha F-nek és G-nek van közös komponense P-n keresztül, akkor (1) miatt $I(P, F \cap G) = \infty$ és készen vagyunk, így feltehető, hogy nincs közös komponensük, és ezért $I(P, F \cap G)$ véges. Legyen $I(P, F \cap G) = n$, n szerinti rekurzióval adjuk meg az algoritmust. Ha $I(P, F \cap G) = 0$, akkor ez (2) miatt $P \notin F \cap G$-ből leolvasható. Tegyük fel, hogy $I(P, A \cap B) < n$ esetén van algoritmusunk $I(P, A \cap B)$ kiszámítására. Legyen az $F(X, 0), G(X, 0) \in k[X]$ polinomok foka rendre r és s, ahol $\deg 0 = 0$. (4) miatt feltehető, hogy $r \leq s$.

Ha $r = 0$, akkor $F(X, 0)$ konstans, így $P \in F$ miatt konstans 0, ezért $Y \mid F$, azaz $F = YH$, így (6) miatt

$$I(P, F \cap G) = I(P, Y \cap G) + I(P, H \cap G).$$

Legyen $G(X,0) = a_0X^m + a_1X^{m+1} + \ldots$, $a_0 \neq 0$, ekkor

$$I(P, Y \cap G) \overset{(7)}{=} I(P, Y \cap G(X,0)) \overset{(6)}{=} I(P, Y \cap X^m) + I(P, Y \cap a_0 + a_1X + \ldots) \overset{(2)}{=}$$
$$= I(P, Y \cap X^m) \overset{(5)}{=} m,$$

mert Y és X^m érintői különböznek P-ben, Y multiplicitása P-ben 1, X^m multiplicitása P-ben m. Mivel $P \in G$, ezért $m \geq 1$, így $I(P, H \cap G) < n$, amely kiszámítására a feltevésünk szerint már van algoritmusunk.

Ha $r > 0$, akkor feltehető, hogy $F(X,0), G(X,0)$ normált polinomok, mert tetszőleges konstanssal felszorozhatunk. Legyen $H = G - X^{s-r}F$. Ekkor $\deg H(X,0) = t < s$ és (7) miatt $I(P, F \cap G) = I(P, F \cap H)$. Ezt ismételgetve (és az F, H sorrendjét felcserélve, ha $t < r$) véges sok lépésben eljutunk egy olyan A, B párhoz, melyre $I(P, F \cap G) = I(P, A \cap B)$ és $\deg A = 0$, ezt az esetet az előző bekezdés szerint ki tudjuk számítani.

(Létezés.) Legyen $I(P, F \cap G) = \dim_k(\mathcal{O}_P(\mathbb{A}^2)/(F,G))$, megmutatjuk, hogy ez teljesíti (1)–(7)-et. Legyen $\mathcal{O} = \mathcal{O}_P(\mathbb{A}^2)$.

(2) Ha $P \notin F \cap G$, például $P \notin F$, akkor $1/F \in \mathcal{O}$, így $1 \in (F,G)$, és $I(P, F \cap G) = \dim_k(\mathcal{O}/\mathcal{O}) = 0$. Megfordítva, ha $I(P, F \cap G) = 0$, akkor $(F,G) = \mathcal{O}$, ezért $1 \in (F,G)$, így nem lehet $P \in F \cap G$. Ha $F = F_1F_2$, $G = G_1G_2$, ahol F_1, G_1 a P-n átmenő komponensek szorzata, $F_2(P), G_2(P) \neq 0$, akkor F_2, G_2 egységek $\mathcal{O}$-ban, így $(F,G) = (F_1, G_1)$.

(3) Ha $T(Q) = P$ affin koordinátacsere, akkor $\widetilde{T}\colon \mathcal{O}_P(\mathbb{A}^2) \to \mathcal{O}_Q(\mathbb{A}^2)$ izomorfizmus a 2.4.4.b) Állítás szerint, melynél F, G képe F^T, G^T, így

$$\mathcal{O}_P(\mathbb{A}^2)/(F,G) \cong \mathcal{O}_Q(\mathbb{A}^2)/(F^T, G^T),$$

ezért $I(P, F \cap G) = I(Q, F^T \cap G^T)$.

(4) Nyilvánvaló, mert $(F,G) = (G,F)$.

(7) $(F,G) = (F, G + AF)$.

A továbbiakban (3) és (2) miatt feltehetjük, hogy $P = (0,0)$, és hogy F és G minden komponense áthalad P-n.

(1) Ha F-nek és G-nek nincs azonos komponense, akkor az 1.6.1. Állítás szerint $V(F,G) = V(F) \cap V(G)$ véges, így az 1.8.5.a) Következmény szerint $k[X,Y]/(F,G)$ véges dimenziós k felett. Másrészt, mivel $V(F,G)$ véges, ezért a 2.7.1. Tétel alapján $\dim_k(k[X,Y]/(F,G)) = \sum_{i=1}^{N} \dim_k(\mathcal{O}_i/(F,G)\mathcal{O}_i) \geq \dim_k(\mathcal{O}/(F,G)) = I(P, F \cap G)$, tehát $I(P, F \cap G)$ véges.

Ha F-nek és G-nek H közös komponense, akkor $(F,G) \subset (H)$, így 2.6.4.a) szerint létezik egy természetes szürjektív $\mathcal{O}/(F,G) \to \mathcal{O}/(H)$ homomorfizmus, tehát $I(P, F \cap G) \geq \dim_k(\mathcal{O}/(H))$. A 2.6.5.d) Állítás alapján $\mathcal{O}/(H) \cong \mathcal{O}_P(H) \supset \Gamma(H)$, és mivel 1.3.4.b) szerint $V(H)$ végtelen halmaz, ezért 1.8.5.b) alapján $\dim_k(\Gamma(H)) = \infty$, így $I(P, F \cap G) \geq \dim_k(\mathcal{O}/(H)) \geq \dim_k(\Gamma(H)) = \infty$.

(6) Elég megmutatni (4) szerint, hogy $I(P, F \cap GH) = I(P, F \cap G) + I(P, F \cap H)$. Feltehető, hogy F-nek és GH-nak nincs közös komponense, különben (1) szerint mindkét oldal végtelen. Legyen 2.6.4.a) szerint $\varphi\colon \mathcal{O}/(F,GH) \to \mathcal{O}/(F,G)$ a természetes szürjektív homomorfizmus, és legyen

$$\psi\colon \mathcal{O}/(F,H) \to \mathcal{O}/(F,GH), \quad z + (F,H) \mapsto Gz + (F,GH).$$

Ekkor ψ jóldefiniált, mert $z \in (F,H)$ esetén $Gz \in (F,GH)$, és ψ k-lineáris. A 2.8.1. Állítás miatt elég megmutatni, hogy a

$$0 \longrightarrow \mathcal{O}/(F,H) \xrightarrow{\psi} \mathcal{O}/(F,GH) \xrightarrow{\varphi} \mathcal{O}/(F,G) \longrightarrow 0$$

sor egzakt. φ szürjektív, és

$$\begin{aligned}\operatorname{Ker}\varphi = \{w + (F,GH) \mid w \in (F,G)\} = \{w + (F,GH) \mid w \in (G)\} = \\ = \{Gz + (F,GH) \mid z \in \mathcal{O}\} = \operatorname{Im}\psi.\end{aligned}$$

Tegyük fel, hogy $0 = \psi(z + (F,H)) = Gz + (F,GH)$, ekkor $Gz = uF + vGH$, $u,v \in \mathcal{O}$. Legyen $S \in k[X,Y]$ a z,u,v nevezőinek szorzata, ekkor $S(P) \neq 0$, és $Sz = A$, $Su = B$, $Sv = C$ polinomok. Mivel $GA = BF + CGH \in k[X,Y]$, és F,G relatív prímek, ezért $G \mid B$, azaz $B = DG$, $D \in k[X,Y]$. Így $A = DF + CH$, tehát $z = \frac{D}{S}F + \frac{C}{S}H \in (F,H)$. Így ψ injektív, és a sor egzakt.

(5) Legyen $m = m_P(F)$, $n = m_P(G)$, $I = (X,Y) \lhd k[X,Y]$. Tekintsük a következő diagramot:

$$\begin{array}{ccccccc} k[X,Y]/I^n \times k[X,Y]/I^m & \xrightarrow{\psi} & k[X,Y]/I^{m+n} & \xrightarrow{\varphi} & k[X,Y]/(I^{m+n},F,G) & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \alpha} & & \\ & & \mathcal{O}/(F,G)\mathcal{O} & \xrightarrow{\pi} & \mathcal{O}/(I^{m+n},F,G)\mathcal{O} & \longrightarrow & 0 \end{array}$$

ahol φ, π, és α a természetes gyűrűhomomorfizmusok 2.6.4. szerint, és

$$\psi(A + I^n, B + I^m) = AF + BG + I^{m+n}.$$

ψ jóldefiniált, mert $F \in I^m$, $G \in I^n$ miatt $A \in I^n$, $B \in I^m$ esetén $AF + BG \in I^{n+m}$. φ és π szürjektívek. Mivel $V(I^{m+n},F,G) \subset \{P\}$, ezért a 2.7.1. Tétel szerint α izomorfizmus. A felső sor egzakt, mert

$$\begin{aligned}\operatorname{Ker}\varphi = \{H + I^{m+n} \mid H \in (I^{m+n},F,G)\} = \{H + I^{m+n} \mid H \in (F,G)\} = \\ = \{AF + BG + I^{m+n} \mid A,B \in k[X,Y]\} = \operatorname{Im}\psi.\end{aligned}$$

Így

$$\dim_k \operatorname{Ker}\varphi = \dim_k \operatorname{Im}\psi \leq \dim_k(k[X,Y]/I^n) + \dim_k(k[X,Y]/I^m),$$

és mivel véges dimenziósak, ezért itt egyenlőség pontosan akkor áll, ha ψ injektív. Továbbá φ-re a dimenziótétel szerint

$$\dim_k \operatorname{Ker}\varphi + \dim_k(k[X,Y]/(I^{m+n},F,G)) = \dim_k(k[X,Y]/I^{m+n}).$$

Mindezeket és a 2.6.3.b) Állítást felhasználva

$$\begin{aligned} I(P,F \cap G) &= \dim_k(\mathcal{O}/(F,G)\mathcal{O}) \geq \dim_k(\mathcal{O}/(I^{m+n},F,G)\mathcal{O}) = \\ &= \dim_k(k[X,Y]/(I^{m+n},F,G)) = \dim_k(k[X,Y]/I^{m+n}) - \dim_k \operatorname{Ker}\varphi \geq \\ &\geq \dim_k(k[X,Y]/I^{m+n}) - \dim_k(k[X,Y]/I^n) + \dim_k(k[X,Y]/I^m) = \\ &= \frac{(m+n)(m+n+1)}{2} - \frac{n(n+1)}{2} - \frac{m(m+1)}{2} = mn \end{aligned}$$

Tehát $I(P, F \cap G) \geq mn$, és $I(P, F \cap G) = mn$ pontosan akkor, ha mindkét helyen egyenlőség áll, azaz π és ψ injektív. Ha ψ injektív, akkor a lenti 3.3.2.c) Állítás szerint F-nek és G-nek nincs közös érintője P-ben. Megfordítva, ha F-nek és G-nek különböző érintői vannak P-ben, akkor 3.3.2.b) szerint $I^{m+n} \subset (F, G)\mathcal{O}$, így π az identitás, és 3.3.2.c) szerint ψ injektív, tehát $I(P, F \cap G) = mn$. □

3.3.2. Állítás. a) *Legyenek $L_1, L_2, \ldots$ és $M_1, M_2, \ldots$ homogén elsőfokú polinomok $k[X, Y]$-ban, melyre minden i, j-re L_i és M_j különböző egyenes. Legyen U a homogén d-edfokú $k[X, Y]$-beli polinomok vektortere k felett, és legyen $A_{i,j} = L_1 L_2 \ldots L_i M_1 M_2 \ldots M_j$ $(i, j \geq 0)$. Ekkor $B = \{A_{i,j} \mid i + j = d\}$ bázisa U-nak.*

b) *Ha F-nek és G-nek nincs közös érintője P-ben, akkor $I^d \subset (F, G)\mathcal{O}$ minden $d \geq m + n - 1$ esetén.*

c) *ψ pontosan akkor injektív, ha F-nek és G-nek nincs közös érintője P-ben.*

Bizonyítás. (a) Mivel U egy bázisa az $\{X^d, X^{d-1}Y, \ldots, Y^d\}$, így $\dim_U = d + 1$, és mivel B elemszáma $d + 1$, ezért elég megmutatni, hogy B elemei lineárisan függetlenek. Tegyük fel, hogy $\lambda_0 A_{0,d} + \lambda_1 A_{1,d-1} + \ldots + \lambda_d A_{d,0} = 0$, $\lambda_j \in k$. i szerinti indukcióval bizonyítjuk, hogy $\lambda_i = 0$. $i = 0$-ra, mivel L_1 osztja az $A_{1,d-1}, \ldots, A_{d,0}$ polinomokat, és nem osztja $A_{0,d} = M_1 \ldots M_d$-t, ezért $\lambda_0 = 0$. Tegyük fel, hogy $\lambda_0 = \ldots = \lambda_{i-1} = 0$. Ekkor $\lambda_i A_{i,d-i} + \ldots + \lambda_d A_{d,0} = 0$, és mivel $L_1 \ldots L_{i+1}$ osztja az $A_{i+1,d-i-1}, \ldots, A_{d,0}$ polinomokat, és nem osztja $A_{i,d-i} = L_1 \ldots L_i M_1 \ldots M_{d-i}$-t, ezért $\lambda_i = 0$. Tehát mindegyik $\lambda_i = 0$, így B lineáris független rendszer, tehát bázis.

(b) Mivel F-nek és G-nek nincs közös komponense, ezért 1.6.1. szerint $V(F, G) = \{P, Q_1, \ldots, Q_s\}$ véges. Legyen 1.3.3.c) szerint H olyan polinom, melyre $H(Q_i) = 0$, $H(P) = 1$. Ekkor $HX, HY \in I(V(F, G))$, így a Nullstellensatz szerint létezik N, melyre $(HX)^N, (HY)^N \in (F, G)$. Mivel $H(P) \neq 0$, ezért $1/H^N \in \mathcal{O}$, így $X^N, Y^N \in (F, G)\mathcal{O}$. Tehát $I^{2N} \subset (F, G)\mathcal{O}$.

Legyen $2N \geq d \geq m + n - 1$, lefelé haladó d szerinti indukcióval bizonyítjuk, hogy $I^d \subset (F, G)\mathcal{O}$. $d \geq 2N$-re $I^d \subset I^{2N} \subset (F, G)\mathcal{O}$. Tegyük fel, hogy $d + 1$-re igaz, bizonyítjuk d-re. Legyenek az F érintői P-ben $L_1, \ldots, L_m$, a G érintői pedig $M_1, \ldots, M_n$. Legyen $L_{m+i} = L_m$, $M_{n+i} = M_n$ minden $i \geq 0$-ra. Ekkor a) szerint $B = \{A_{i,j} \mid i + j = d\}$ bázisa U-nak. Így elég megmutatni, hogy $i + j = d$ esetén $A_{i,j} \in (F, G)\mathcal{O}$, ekkor ugyanis $U \subset (F, G)\mathcal{O}$, és így $I^d = (U) \subset (F, G)\mathcal{O}$.

Mivel $i + j = d \geq m + n - 1$, ezért $i \geq m$ vagy $j \geq n$. Legyen például $i \geq m$, ekkor $A_{i,j} = L_1 \ldots L_m C$, ahol $\deg C = d - m$ homogén. Továbbá $F = L_1 \ldots L_m + F^\star$, ahol $F^\star$-ban minden tag foka legalább $m + 1$. Tehát $A_{i,j} = (F - F^\star)C$. Itt $FC \in (F, G)\mathcal{O}$ nyilvánvaló, és mivel $F^\star C$-ben minden tag foka legalább $(m + 1) + (d - m) = d + 1$, ezért $F^\star C \in I^{d+1} \subset (F, G)\mathcal{O}$ az indukciós feltevés miatt. Tehát $A_{i,j} \in (F, G)\mathcal{O}$ minden $i + j = d$-re, és így $I^d \in (F, G)\mathcal{O}$.

(c) Tegyük fel, hogy az érintők különbözők, és hogy $\psi(A + I^n, B + I^m) = 0$, azaz $AF + BG \in I^{m+n}$. Legyen az A, B, F, G polinomok min-része A_r, B_s, F_m, G_n. Tegyük fel, hogy $r < n$ vagy $s < m$. Ekkor AF min-része $A_r F_m$, BG min-része $B_s G_m$, így mivel valamelyik $m + n$-nél kisebb fokú, ezért $AF + BG \in I^{m+n}$ csak úgy teljesülhet, ha $r + m = s + n$ és $A_r F_m + B_s G_n = 0$. Mivel F és G P-beli érintői különbözők, ezért F_m és G_n relatív prímek. Így $G_n \mid A_r$ és $F_m \mid B_s$, így $r \geq n$ és $s \geq m$, ami ellentmond feltevésünknek. Tehát $A \in I^n$ és $B \in I^m$, ezért ψ injektív.

Megfordítva, tegyük fel, hogy L közös érintője F-nek és G-nek P-ben. Ekkor $F_m = LF^\star_{m-1}$ és $G_n = LG^\star_{n-1}$. Tehát $G^\star_{n-1} \notin I^n$ és $F^\star_{m-1} \notin I^m$, melyekre

$$\psi(G^\star_{n-1} + I^n, -F^\star_{m-1} + I^m) = G^\star_{n-1}F - F^\star_{m-1}G + I^{m+n} =$$
$$= G^\star_{n-1}F_m - F^\star_{m-1}G_n + I^{m+n} = G^\star_{n-1}LF^\star_{m-1} - F^\star_{m-1}LG^\star_{n-1} + I^{m+n} = 0,$$

így ψ nem injektív. Ezzel a 3.3.2. Állítás és a 3.3.1. Tétel bizonyítását befejeztük. □

Megjegyezzük, hogy a tétel egyértelműségi részének bizonyításában nem használtuk az (1)–(7) tulajdonságok minden elemét, például az (5) tulajdonságnak csak az $I((0,0), X \cap Y) = 1$ esete kellett. Kimondunk még két tulajdonságot.

3.3.3. Állítás. a) *Ha P sima pontja F-nek, akkor $I(P, F \cap G) = \mathrm{ord}_P^F(G)$.*

b) *Ha F, G relatív prímek, akkor $\sum_{P \in \mathbb{A}^2} I(P, F \cap G) = \dim_k(k[X,Y]/(F,G))$.*

Bizonyítás. (a) Feltehető (2) alapján, hogy F irreducibilis. Legyen $g = G + (F) \in \mathcal{O}_P(F)$, ekkor a 2.8.3.c) Állítás szerint $\mathrm{ord}_P^F(g) = \dim_k(\mathcal{O}_P(F)/(g))$. Mivel $(F,G) \lhd k[X,Y]$-nak 1.4.4.b)-ben a $(g) \lhd \Gamma(F)$ ideál felel meg, ezért a 2.6.5.c) Állítás szerint $\mathcal{O}_P(\mathbb{A}^2)/(F,G) \cong \mathcal{O}_P(F)/(g)\mathcal{O}_P(F)$, így

$$\dim_k(\mathcal{O}_P(F)/(g)) = \dim_k(\mathcal{O}_P(\mathbb{A}^2)/(F,G)) = I(P, F \cap G).$$

(b) Mivel $F \cap G$ véges, ezért (2) szerint csak véges sok nem nulla tag van az összegben, nevezetesen $P \in F \cap G$ esetén. Mivel $V(F,G)$ véges, ezért 1.8.5.a) szerint $k[X,Y]/(F,G)$ véges dimenziós, így a 2.7.1. Tétel szerint $\dim_k(k[X,Y]/(F,G)) = \sum_{P \in F \cap G} \dim_k(\mathcal{O}_P(\mathbb{A}^2)/(F,G)) = \sum_{P \in F \cap G} I(P, F \cap G)$. □

Az algoritmus, amit a bizonyításban megadtunk, egyszerű aritmetikára vezeti vissza $I(P, F \cap G)$ számítását, ami minden esetben működik. Azonban az (5) és (7) tulajdonságok kreatív használatával gyakran időt spórolhatunk, mint azt a következő példa is mutatja.

3.3.4. Példa. Megválaszoljuk a bevezetőben feltett kérdést a metszési multiplicitásról. Legyen tehát $F = (X^2+Y^2)^2 + 3X^2Y - Y^3$, $G = (X^2+Y^2)^3 - 4X^2Y^2$, és $P = (0,0)$. Legyen $G - (X^2+Y^2)F = -4X^2Y^2 - (X^2+Y^2)(3X^2Y - Y^3) = Y(-3X^4 - 2X^2Y^2 - 4X^2Y + Y^4) = YA$. Ekkor

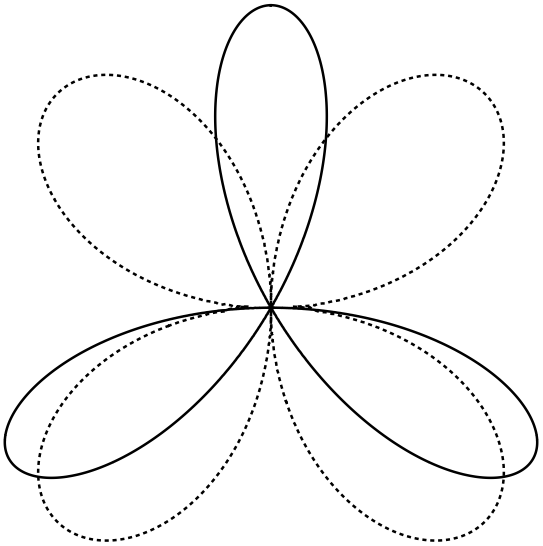
$$I(P, F \cap G) \overset{(7)}{=} I(P, F \cap YA) \overset{(6)}{=} I(P, F \cap Y) + I(P, F \cap A),$$
$$I(P, F \cap Y) \overset{(7)}{=} I(P, X^4 \cap Y) \overset{(5)}{=} 4.$$

$I(P, F \cap A)$-hoz az általános algoritmus lépését használjuk. Mivel $F(X,0) = X^4$ és $A(X,0) = -3X^4$, ezért legyen $A + 3F = Y(5X^2 + 4X^2Y + 5Y^3 - 3Y^2) = YB$. Ekkor

$$I(P, F \cap A) \overset{(7)}{=} I(P, F \cap YB) \overset{(6)}{=} I(P, F \cap Y) + I(P, F \cap B).$$

Mivel F min-része $Y(3X^2 - Y^2)$, B min-része $5X^2 - 3Y^2$, és ezek relatív prímek, ezért F-nek és B-nek nincs közös érintője P-ben, így $I(P, F \cap B) \overset{(5)}{=} m_P(F)m_P(B) = 3 \cdot 2$.

Tehát $I(P, F \cap G) = 14$. Érdemes megfigyelni, hogy az intuitív metszési multiplicitás fogalmunk alapján hogyan jön össze ez a 14-szeres metszéspont az origóban.



Irodalomjegyzék

[1] WILLIAM FULTON, *Algebraic Curves, An Introduction to Algebraic Geometry*, 2008, http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf

[2] GERD FISCHER, *Plane Algebraic Curves*, American Mathematical Society, 2001

[3] KISS EMIL, *Bevezetés az algebrába*, Typotex, 2007