Kommutatív algebra és algebrai geometria jegyzetvázlat (nem végleges)

Nagy Gábor Péter
BME Algebra Tanszék

2020. szeptember 22.

Tartalomjegyzék

1. fejezet

Bevezetés

1.1. Magasabb fokú egyenletrendszerek

Legyen K test, $f_1, \dots, f_m \in K[X_1, \dots, X_n]$ polinomok és tekintsük a

$$\begin{cases} f_1(x_1, \dots, x_n) & = 0 \\ f_2(x_1, \dots, x_n) & = 0 \\ & \vdots \\ f_m(x_1, \dots, x_n) & = 0 \end{cases} \tag{1.1}$$

egyenletrendszer megoldásainak M halmazát K^n-ben. Ennek az összefoglalónak a célja az M alapvető geometriai tulajdonságainak megadása, valamint az ehhez szükséges algebrai eszköztár kiépítése.

Fontos speciális esetek:

(1) Minden f_i polinom elsőfokú. Ekkor n ismeretlenes, m egyenletből álló lineáris egyenletrendszerünk van. Ennek megoldáshalmaza vagy üres, vagy

$$\{\boldsymbol{v_0} + t_1\boldsymbol{v}_1 + \cdots + t_k\boldsymbol{v}_k \mid t_1, \dots, t_k \in K\}$$

alakú, ahol $0 \leq k \leq n$ és $\boldsymbol{v}_1, \dots, \boldsymbol{v}_k$ lineáris független vektorok K^n-ben. Ha $k = 0$, akkor (1.1) megoldása egyértelmű. A megoldás Gauss-Jordan eliminációval történik.

(2) $n = m = 1$, azaz egyetlen egy változós $f(X)$ polinom gyökeit keressük. Tegyük fel, hogy $f \neq 0$. és legyen $d = \deg(f)$. Mivel $f(c) = 0$ akkor és csak akkor, ha $X - c$ osztja f-et, ezért az $f(X)$ gyökeinek keresése egyenértékű az elsőfokú tényezőinek meghatározásával. Ez általában nehéz feladat. Ami könnyű: legfeljebb d elsőfokú tényező van, azaz a gyökök száma legfeljebb d.

Definíció szerint *algebrailag zárt test* felett minden (elsőfokú, nem zéró) polinom lineáris tényezőkre bomlik. Azaz *multiplicitással számolva* a gyökök száma pontosan d. Minden K testnek van (izomorfia erejéig egyértelmű) algebrai lezártja; jelölés $\overline{K}$. A komplex számok $\mathbb{C}$ teste algebrailag zárt.

(3) A változók száma $n = 1$, az egyenletek száma $m \geq 2$. Ekkor m darab egyváltozós polinom legnagyobb közös osztóját keressük. (Majd alkalmazzuk az előző pontban tett megfontolásokat.) Ez visszavezethető két egyváltozós polinom legnagyobb közös osztójának megkeresésére, amire az *euklideszi algoritmus* egy hatékony eljárást biztosít. Az algoritmus kis módosítással azokat az $u(X), v(X)$ polinomokat is meghatározza, amelyekre

$$u(X)f(X) + v(X)g(X) = \gcd(f, g).$$

(4) $n = 2$ kétváltozós eset. Legyen $f(X, Y)$ K feletti kétváltozós polinom. A K feletti $\Gamma : f(X, Y) = 0$ *(affin) algebrai görbe* alatt a

$$\Gamma = \{(x, y) \in K^2 \mid f(x, y) = 0\}$$

halmazt értjük. Például az egyenesek ($aX + bY + c = 0$), vagy a kör ($X^2 + Y^2 - 1 = 0$) algebrai görbék. Az

$$\begin{cases} f(X, Y) & = 0 \\ g(X, Y) & = 0 \end{cases}$$

egyenletrendszer megoldásai megfelelnek a két algebrai görbe metszéspontjainak. Ez könnyen megoldható abban a speciális esetben, ha a két görbe közül valamelyik $Y = \varphi(X)$ *explicit alakban* van megadva. Általánosabban, ha vannak olyan $u_1(t), u_2(t), v_1(t), v_2(t)$ polinomok, ahol $u_2, v_2 \neq 0$ és *formálisan* teljesül

$$f\left(\frac{u_1(t)}{u_2(t)}, \frac{v_1(t)}{v_2(t)}\right) = 0,$$

akkor azt mondjuk, hogy

$$\begin{cases} X & = \frac{u_1(t)}{u_2(t)}, \\ Y & = \frac{v_1(t)}{v_2(t)} \end{cases}$$

a Γ algebrai görbe *racionális paraméterezése.* Például az egységkör racionálisan paraméterezhető:

$$\begin{cases} X & = \frac{t^2-1}{t^2+1}, \\ Y & = \frac{2t}{t^2+1}. \end{cases}$$

A metszéspontok keresése ebben az esetben is visszavezethető az egyváltozós esetre.

1.2. Integritástartományok, oszthatóság

1.2.1. Definíció. A nullaosztómentes, egységelemes kommutatív gyűrűket **integritástartománynak** (i.t.) nevezzük.

1.2.1. Példa. Integritástartományra a legismertebb példa az egész számok $\mathbb{Z}$ halmaza. Másik fontos példa a D i.t. feletti n változós $D[X_1, \ldots, X_n]$ polinomgyűrű.

1.2.2. Definíció. Legyen a, b a D i.t. két eleme. Azt mondjuk, hogy a **osztja** b**-t,** ha létezik $c \in D$ elem, amelyre $ac = b$; jelöléssel $a \mid b$. Amennyiben $a \mid b$ és $b \mid a$ egyidőben fennáll, **asszociált** elemekről beszélünk, és az $a \sim b$ jelölést használjuk. Az 1 egységelemmel asszociált elemeket D **egységeinek** nevezzük, ezek halmazát általában D^* jelöli.

Könnyű meggondolni, hogy az $a, b \in D$ elemek akkor és csak akkor asszociáltak, ha $a = bu$ és $b = av$ teljesül valamely $u, v \in D^*$ egységekre.

1.2.2. Példa. $\mathbb{Z}$ egységei ± 1, míg $D[X_1, \ldots, X_n]^* = D^*$.

1.2.3. Definíció. Azt mondjuk, hogy a D i.t. a eleme **irreducibilis,** ha minden $b \mid a$ elemre $b \sim a$ vagy $b \sim 1$ teljesül. Továbbá, ha a nem 0 vagy egység, és $a \mid bc$-ből következik, hogy $a \mid b$ vagy $a \mid c$, akkor **prímelemről** beszélünk.

Könnyen meggondolható, hogy definíció szerint minden prímelem irreducibilis. Ennek megfordítása azonban nem minden i.t. esetén igaz. (Pl. a $\mathbb{Z}[\sqrt{-5}]$ gyűrűben $3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ teljesül, azaz 3 irreducibilis, de nem prím.)

1.2.4. Definíció. Azokat az integritástartományokat nevezzük **Gauss-gyűrűknek** vagy **egyértelmű faktorizációs tartománynak (UFD),** amelyekben minden irreducibilis elem prím.

1.2.5. Állítás (Gauss tétele)**.** Ha D Gauss-gyűrű, akkor a $D[X]$ polinomgyűrű is Gauss-gyűrű. □

1.2.6. Következmény. Ha D Gauss-gyűrű, akkor

$$D[X_1, \ldots, X_n] = D[X_1, \ldots, X_{n-1}][X_n]$$

is Gauss-gyűrű. Speciálisan, minden test feletti n-változós polinomgyűrű Gauss-gyűrű. □

1.2.7. Következmény. A D i.t. feletti $D[X_1, \ldots, X_n]$ polinomgyűrűben egyértelmű faktorizáció áll fenn. Pontosabban, bármely $f \in T[X_1, \ldots, X_n]$ polinom sorrend és asszociáltság erejéig egyértelműen meghatározott módon felírható véges sok irreducibilis polinom $f = g_1 \cdots g_m$ szorzataként.

Bizonyítás. A fokszámok tulajdonságai miatt nyilvánvaló, hogy f felbomlik véges sok irreducibilis elem szorzatára; a Gauss-tulajdonság szerint ez prímelemek szorzatát jelenti. Ha felírunk két ilyen faktorizációt, $f = g_1 \cdots g_m = h_1 \cdots h_k$, akkor a prímtulajdonság szerint g_1 osztja valamelyik h_i, ami azt jelenti, hogy asszociáltak. Hasonlóan folytatva az $f^* = g_2 \cdots g_m$ polinomra azt kapjuk, hogy $m = k$ és minden g_i asszociált valamely h_j-hez. □

Legyen D i.t. és definiáljuk a T halmazt az alábbi módon. T elemeit $\frac{a}{b}$ alakba írjuk, ahol $a \in D$ és $b \in D \setminus \{0\}$. Az $\frac{a}{b}, \frac{c}{d} \in T$ elemeket egyenlőknek tekintjük, ha

$ad = bc$ teljesül D-ben. Az $\frac{a}{1}$ elemeket a-val is jelölhetjük, ilyen módon $D \subseteq T$ áll fenn.

A négy alapműveletet az alábbi módon értelmezzük T-n:

$$\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad \frac{a}{b} : \frac{c}{d} = \frac{ad}{bc},$$

az osztás esetén $c \neq 0$-t feltételezve.

1.2.8. Állítás. A fenti módon értelmezett T halmaz a négy alapművelettel testet alkot. □

1.2.9. Definíció. A fenti módon értelmezett T halmazt a D integritástaromány **hányadostestének** nevezzük.

1.2.3. Példa. $\mathbb{Z}$ hányadosteste a racionális számok $\mathbb{Q}$ teste. A $D[X_1, \ldots, X_n]$ polinomgyűrű hányadosteste a $D(X_1, \ldots, X_n)$ **racionális törtfüggvények** teste.

Minden n-változós racionális törtfüggvény $\frac{f(X_1, \ldots, X_n)}{g(X_1, \ldots, X_n)}$ alakba írható, ahol feltehető, hogy f-nek és g-nek nincsenek nem konstans közös tényezői. A fent ismertetett eljárás szerint ezt a törtalakú felírást elsősorban **formálisan** kell értelmezni, azaz egyszerű jelsorozatnak kell tekinteni. A névben szereplő „függvény" szó zavart okozhat, hiszen a várakozásainktól eltérően egy racionális törtfüggvény **nem határoz meg** egy $D^n \to D$ leképezést. Ennek oka, hogy lehetséges olyan $(x_1, \ldots, x_n) \in D^n$ behelyettesítés, melyre $f(x_1, \ldots, x_n) \neq 0$ és $g(x_1, \ldots, x_n) = 0$. Racionális törtfüggvények leképezésként való értelmezésére a továbbiakban nem lesz szükségünk.

1.2.1. Feladat. Oldjuk meg az alábbi feladatokat:

a) Számológép használata nélkül számoljuk ki az alábbiakat: $\gcd(60, 32)$, $\gcd(3, 2)$, $\gcd(3, 1)$, $\gcd(3, 0)$, $\gcd(0, 0)$, $\gcd(199\,411\,161\,721, 366\,124\,068\,217)$.

b) Ossza el maradékosan az $f = 2x^5 - 4x^3 + 2x^2 - x + 2$ polinomot a $g = x^2 + x + 1$ polinommal.

c) Legyen $f = x^6 - 1$, $g = x^4 + 2x^3 + 2x^2 - 2x - 3$. Adja meg az $I = \langle f, g \rangle$ ideál egy generátorelemét. Teljesül $x^5 + x^3 + x^2 - 7 \in I$? Mutassa meg, hogy $h = x^4 + 2x^2 - 3 \in I$ és írja fel h-t az f és g lineáris kombinációjaként.

d) Számolja ki az

$$f_1 = x^5 - 2x^4 - x^2 + 2x,$$
$$f_2 = x^7 + x^6 - 2x^4 - 2x^3 + x + 1,$$
$$f_3 = x^6 - 2x^5 + x^4 - 2x^3 + x^2 - 2x$$

polinomok legnagyobb közös osztóját.

e) Legyen K test. Mutassa meg, hogy a $K[X, Y]$ gyűrű $\langle x, y \rangle$ ideálja nem generálható egyetlen elemmel. (Tehát $K[X, Y]$ nem *főideálgyűrű*.)

f) Legyen K test, $c \in K$, $f \in K[X_1, \ldots, X_n]$. Mutassuk meg, hogy $X_n - c$ akkor és csak akkor osztja f-et, ha $f(X_1, \ldots, X_{n-1}, c)$ a nulla polinom.

2. fejezet

A rezultáns fogalma

2.1. Egyváltozós polinomok, rezultáns

Ebben a fejezetben D tetszőleges Gauss-gyűrűt jelöl, T pedig D hányadostestét. Nyilván $D \subseteq T$ és $D[X] \subseteq T[X]$, sőt általában $D[X] \subset T[X]$. Ez azt jelenti, hogy D feletti polinomok esetén elvben különbséget kell tennünk $D[X]$-beli és $T[X]$-beli oszthatóság között, hiszen előforduhat, hogy $T[X]$-ben van, míg $D[X]$-ben nincs olyan h elem, amelyre $f = gh$ teljesül.

2.1.1. Példa. Legyen $D = \mathbb{Z}$, $T = \mathbb{Q}$, $f(X) = X^2$, $g(X) = 2X$. Ekkor $h(X) = \frac{1}{2}X \in \mathbb{Q}[X]$ esetén $f = gh$, egész együtthatós h pedig nem létezik.

Az alábbi állítás mutatja, hogy ez a jelenség elméleti szempontból komolyabb zavart nem okoz.

2.1.1. Állítás. Legyen $f(X) \in D[X]$ olyan nem konstans polinom, amely D felett irreducibilis. Ekkor $f(X)$ irreducibilis $T[X]$-ben is. □

Általában a polinomok irreducibilis tényezőkre bontása fontos, de nehéz feladat. Ennek egy jól kezelhető részfeladata két polinom nem konstans közös tényezőinek meghatározása. Test feletti egy változós polinomgyűrűben ezt az euklideszi osztás teszi lehetővé. A nehézség $D[X]$ esetén adódik, amiben nem feltétlenül tudjuk elvégezni az euklideszi osztást.

A továbbiakban D feletti polinomok nem konstans közös tényezőivel kapcsolatosan vizsgálódunk.

2.1.2. Állítás. Az $f, g \in D[X]$ polinomoknak akkor és csak akkor van nem konstans közös tényezőjük, ha léteznek $u, v \in D[X]$ polinomok úgy, hogy $\deg(u) < \deg(g)$, $\deg(v) < \deg(f)$, és teljesül $uf + vg = 0$.

Bizonyítás. Tegyük fel, hogy $d \in D[X]$ nem konstans közös tényező, azaz fennáll $g = u^*d$ és $f = v^*d$ valamely $u^*, v^* \in D[X]$ polinomokra. Mivel $\deg(d) > 0$, ezért $\deg(u^*) < \deg(g)$, $\deg(v^*) < \deg(f)$. Teljesül továbbá $u^*f - v^*g = u^*v^*d - v^*u^*d = 0$.

A fordított irányhoz tegyük fel, hogy $uf + vg = 0$ teljesül az állításban szereplő feltételekkel. Az irreducibilis felbontás tulajdonsága szerint léteznek $h_1, \ldots, h_n$

páronként nem asszociált irreducibilis polinomok, melyekre $f = uh_1^{r_1} \cdots h_n^{r_n}$, $v = vh_1^{s_1} \cdots h_n^{s_n}$ és $g = wh_1^{t_1} \cdots h_n^{t_n}$ áll fenn valamely r_i, s_i, t_i nem negatív egészekkel és $u, v, w \in D^*$ egységekkel. Az $f \mid vg$ oszthatóságból következik, hogy minden i esetén $r_i \leq s_i + t_i$; $\deg(v) < \deg(f)$ pedig azt eredményezi, hogy valamelyik j indexre $\deg(h_j) > 0$ és $s_j < r_j$. Ekkor azonban $r_j, t_j > 0$, azaz h_j nem konstans közös tényezője f-nek és g-nek. □

Legyen $n = \deg(f)$, $m = \deg(g)$ és írjuk fel az $f, g, u, v \in D[X]$ polinomokat

$$\begin{aligned} f(X) &= a_0X^n + a_1X^{n-1} + \cdots + a_n, \\ g(X) &= b_0X^m + b_1X^{m-1} + \cdots + b_m, \\ u(X) &= u_1X^{m-1} + u_2X^{m-2} + \cdots + u_m, \\ v(X) &= v_1X^{n-1} + v_2X^{n-2} + \cdots + v_n. \end{aligned}$$

Az $u(X)f(X) + v(X)g(X)$ polinom együtthatói a következők.

$$\begin{array}{lcccccc}
\text{konst.:} & a_nu_m+ & & & & b_mv_n & \\
X: & a_{n-1}u_m+a_nu_{m-1}+ & & & & b_{m-1}v_n+b_mv_{n-1} & \\
 & \vdots & & & & \vdots & \\
X^{m-1}: & a_{n-m+1}u_m+ & \cdots & a_nu_1+ & b_1v_n+b_2v_{n-1}+\cdots & & \\
X^m: & a_{n-m}u_m+ & \cdots & a_{n-1}u_1+ & b_0v_n+b_1v_{n-1}+\cdots & & \\
 & \vdots & & & \vdots & & \\
X^{n-1}: & a_1u_m+a_2u_{m-1}+\cdots & & & & \cdots+ & b_mv_1 \\
X^n: & a_0u_m+a_1u_{m-1}+\cdots & & & & \cdots+b_{m-1}v_1 & \\
 & \vdots & & & \vdots & & \\
X^{n+m-1}: & & & a_0u_1+ & & & b_0v_1
\end{array}$$

Ez azt jelenti, hogy az $uf + vg = 0$ tulajdonsággal rendelkező $u(X), v(X)$ polinomok létezése egyenértékű az alábbi $(n+m)$-változós, $n+m$ egyenletből álló lineáris egyenletrendszer nem triviális megoldásának létezésével:

$$\left.\begin{array}{lcccccc}
0 = & a_nU_m+ & & & & b_mV_n & \\
0 = & a_{n-1}U_m+a_nU_{m-1}+ & & & & b_{m-1}V_n+b_mV_{n-1} & \\
 & \vdots & & & & & \\
0 = & a_{n-m+1}U_m+ & \cdots & a_nU_1+ & b_1V_n+b_2V_{n-1}+\cdots & & \\
0 = & a_{n-m}U_m+ & \cdots & a_{n-1}U_1+ & b_0V_n+b_1V_{n-1}+\cdots & & \\
 & \vdots & & & & & \\
0 = & a_1U_m+a_2U_{m-1}+\cdots & & & & \cdots+ & b_mV_1 \\
0 = & a_0U_n+a_1U_{m-1}+\cdots & & & & \cdots+b_{m-1}V_1 & \\
 & \vdots & & & & & \\
0 = & & & a_0U_1+ & & & b_0V_1
\end{array}\right\} \quad (2.1)$$

A (2.1) egyenletrendszer együtthatóiból készített mátrix

$$\begin{pmatrix} a_n & 0 & \cdots & 0 & b_m & 0 & \cdots & 0 \\ a_{n-1} & a_n & \cdots & 0 & b_{m-1} & b_m & \cdots & 0 \\ \vdots & \vdots & \ddots & & & & \ddots & \\ a_0 & a_1 & \cdots & a_n & & & \cdots & b_{m-1} \\ 0 & a_0 & \cdots & a_{n-1} & & & \cdots & b_{m-2} \\ & & \ddots & \vdots & & & & \vdots \\ 0 & 0 & \cdots & a_0 & 0 & 0 & \cdots & b_0 \end{pmatrix}. \tag{2.2}$$

2.1.3. Definíció. A (2.2) mátrix determinánsát az $f(X), g(X)$ polinomok **rezultánsának** nevezzük, és $R_{f,g}$-vel jelöljük.

A rezultáns értéke D-beli elem, hiszen az $a_i, b_j \in D$ elemekből adódik az összeadás és a szorzás műveleteinek felhasználásával. A rezultáns felírásakor praktikus okokból gyakran az alábbi mátrixalakot használjuk.

$$R_{f,g} = \det \begin{pmatrix} a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & \cdots & 0 \\ \vdots & & \ddots & & & \ddots & \vdots \\ 0 & 0 & \cdots & a_0 & a_1 & \cdots & a_n \\ b_0 & \cdots & b_m & 0 & 0 & \cdots & 0 \\ 0 & b_0 & \cdots & b_m & 0 & \cdots & 0 \\ & & \ddots & & \ddots & & \\ & & & \ddots & & \ddots & \\ 0 & 0 & 0 & 0 & b_0 & \cdots & b_m \end{pmatrix} \tag{2.3}$$

2.1.4. Tétel (Rezultánsok alaptétele)**.** Az D feletti $f(X), g(X)$ polinomoknak akkor és csak akkor van D feletti nem konstans közös tényezőjük, ha az $R_{f,g}$ rezultánsuk 0.

Bizonyítás. Tekintsük a (2.1) egyenletrendszert T felett, ekkor a T feletti nem triviális megoldás létezése ekvivalens $R_{f,g} = 0$-val. Mivel T a D hányadosgyűrűje, ezért az egyenletrendszer T feletti nem triviális mogoldásának megléte maga után vonja D feletti nem triviális megoldás meglétét. (Elegendő felszorozni a nevezők legkisebb közös többszörösével.)

Másrészről a (2.1) D feletti nem triviális megoldása egyenértékű olyan D feletti $u(X), v(X)$ polinomok létezésével, amelyekre teljesül $uf + vg = 0$, $\deg(u) < \deg(g)$, $\deg(v) < \deg(f)$. Mint láttuk, ilyen D feletti polinomok akkor és csak akkor léteznek, ha f-nek és g-nek van D feletti közös tényezője. □

2.1.1. Megjegyzés. Vegyük észre, hogy a rezultások alaptétele és a többi rezultánsra vonatkozó eredmény igaz marad, ha csak az a_0, b_0 elemek egyikéről követeljük meg, hogy nullától különbözzék. Más szóval ha $n = \deg(f)$, akkor $m > \deg(g)$ esetén is teljesülnek az elmondottak.

2.1.2. Példa. Legyen $D = \mathbb{Z}$, $f(X) = X^3 - X$, $g(X) = X^2 + 2X - 3$. Ekkor

$$R_{f,g} = \det \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 \\ -1 & 0 & -3 & 2 & 1 \\ 0 & -1 & 0 & -3 & 2 \\ 0 & 0 & 0 & 0 & -3 \end{pmatrix} = 0.$$

Valóban, $X - 1$ közös tényezője f-nek és g-nek.

2.2. Eliminációelméleti alkalmazás

2.2.1. Lemma. Legyen A $n \times n$-es mátrix D-beli elemekkel és $\boldsymbol{b} \in D^n$. Legyen $\det(A) \neq 0$ és jelölje $\boldsymbol{x}$ az $A\boldsymbol{x} = \boldsymbol{b}$ lineáris egyenletrendszer egyértelmű megoldását. Ekkor $\boldsymbol{x}$ koordinátái $x_i = \tilde{x}_i / \det(A)$ alakúak, ahol $\tilde{x}$ az A és $\boldsymbol{b}$ elemeinek egész együtthatós polinomjaiként áll elő. Speciálisan, minden i-re $\tilde{x}_i \in D$.

Bizonyítás. Jelölje A^* az A mátrix adjungáltját, erre teljesül $A^*A = \det(A)I$. A $\tilde{\boldsymbol{x}} = A^*\boldsymbol{b}$ elem koordinátái A és $\boldsymbol{b}$ elemeinek egész együtthatós polinomjaiként állnak elő. Teljesül továbbá

$$\tilde{\boldsymbol{x}} = A^*\boldsymbol{b} = A^*A\boldsymbol{x} = \det(A)\boldsymbol{x},$$

azaz $A\boldsymbol{x} = \boldsymbol{b}$ megoldása $\tilde{\boldsymbol{x}} / \det(A)$. □

2.2.2. Tétel. Adott $f, g \in D[X]$ polinomokhoz léteznek $A, B \in D[X]$ polinomok, melyekre

$$Af + Bg = R_{f,g}.$$

Az A, B együtthatói f és g együtthatóinak egész együtthatós polinomjai. Speciálisan, $A, B \in D[X]$.

Bizonyítás. Ha $R_{f,g} = 0$, akkor az állítás nyilván igaz az $A = B = 0$ választás mellett. Tegyük fel a továbbiakra nézve, hogy $R_{f,g} \neq 0$. Az előző fejezet jelöléseit megtartva tekintsük a (2.1) egyenletrendszer alábbi módosítását:

$$\left.\begin{array}{rcccccccc} 1 = & a_nU_m+ & & & & b_mV_n & & & \\ 0 = & a_{n-1}U_m+a_nU_{m-1}+ & & & & b_{m-1}V_n+b_mV_{n-1} & & & \\ \vdots & & & & & & & & \\ 0 = & a_{n-m+1}U_m+ & \cdots & & a_nU_1+ & b_1V_n+b_2V_{n-1}+\cdots & & & \\ 0 = & a_{n-m}U_m+ & \cdots & & a_{n-1}U_1+ & b_0V_n+b_1V_{n-1}+\cdots & & & \\ \vdots & & & & & & & & \\ 0 = & a_1U_m+a_2U_{m-1}+\cdots & & & & & \cdots+ & b_mV_1 & \\ 0 = & a_0U_n+a_1U_{m-1}+\cdots & & & & & \cdots+ & b_{m-1}V_1 & \\ \vdots & & & & & & & & \\ 0 = & & & & a_0U_1+ & & & b_0V_1 & \end{array}\right\} \quad (2.4)$$

Ennek együtthatóiból képzett mátrix determinánsa $R_{f,g} \neq 0$. Lemma 2.2.1 szerint (2.4) egyértelmű megoldása $\tilde{u}_i / R_{f,g}$, $\tilde{v}_j / R_{f,g}$ alakú, ahol $\tilde{u}_i, \tilde{v}_j$ az $a_0, \ldots, b_0, \ldots$ értékek egész együtthatós polinomjai. A belőlük alkotott

$$A = \tilde{u}_1 X^{m-1} + \cdots + \tilde{u}_m, \qquad B = \tilde{v}_1 X^{n-1} + \cdots + \tilde{v}_n$$

polinomokra

$$\frac{A}{R_{f,g}} f + \frac{B}{R_{f,g}} g = 1,$$

azaz $Af + Bg = R_{f,g}$ teljesül. □

Végezetül bemutatjuk a rezultáns egy fontos alkalmazását algebrai görbék paraméterezésével kapcsolatosan.

2.2.3. Definíció. Legyen $\Gamma : f(X, Y) = 0$ algebrai görbe és $u(t) = \frac{u_1(t)}{u_2(t)}, v(t) = \frac{v_1(t)}{v_2(t)} \in \mathbb{K}(t)$ racionális törtfüggvények. Azt mondjuk, hogy az $(u(t), v(t))$ pár *paraméterezi* Γ-t, ha az $f(u(t), v(t))$ racionális törtfüggvény azonosan 0.

Megjegyezzük, hogy nem minden algebrai görbét tudunk racionális törtfüggvényekkel paraméterezni. Továbbá, ha létezik is ilyen, az algebrai görbe paraméterezése távolról sem egyértelmű.

2.2.1. Példa.

1. Az $X^2 + Y^2 = 1$ egységkört az

$$(u(t), v(t)) = \left(\frac{t^2 - 1}{t^2 + 1}, \frac{2t}{t^2 + 1} \right)$$

pár paraméterezi. Megjegyezzük, hogy a $(1, 0)$ pont nem áll elő $(u(t), v(t))$ alakban, azaz a paraméterezés nem feltétlenül szürjektív.

2. Az $Y^2 = X^3 + X^2$ köbös görbét az $(u(t), v(t)) = (t^2 - 1, t(t^2 - 1))$ pár paraméterezi. Ebben az esetben a $t = 1$ és $t = -1$ paraméterekhez ugyanaz a $(0, 0)$ görbepont tartozik. Tehát, a paraméterezés nem feltétlenül injektív.

Tekintsük most az $u(t), v(t) \in \mathbb{K}(X)$ racionális törtfüggvényeket és vizsgáljuk meg, hogy ezek milyen algebrai görbét paramétereznek. Ehhez az

$$X = u(t) = \frac{u_1(t)}{u_2(t)},$$
$$Y = v(t) = \frac{v_1(t)}{v_2(t)}$$

egyenletrendszerből kell eliminálni t-t. Definiáljuk a

$$g(X, Y, t) = X u_2(t) - u_1(t), \qquad h(X, Y, t) = Y v_2(t) - v_1(t)$$

háromváltozós komplex együtthatós polinomokat. Legyen

$$f(X, Y) = R_{g,h}(X, Y)$$

ezek t szerinti rezultánsa; nyilván $f(X,Y) \in \mathbb{K}[X,Y]$. Mivel

$$g(u(t),v(t)) \equiv h(u(t),v(t)) \equiv 0,$$

ezért a 2.2.2 tétel miatt $f(u(t),v(t)) \equiv 0$. Tehát $\Gamma : f(X,Y) = 0$ a keresett algebrai görbe.

2.3. Kétváltozós polinomok alaptulajdonságai

A mi esetünkben a rezultánsok a kétváltozós polinomok vizsgálatakor nyernek különös jelentőséget. Legyen $\mathbb{K}$ tetszőleges algebrailag zárt test. Tekintsük a $D = \mathbb{K}[Y]$ integritástartományt, ekkor $D[X] = \mathbb{K}[X,Y]$. Más szóval az $f(X,Y), g(X,Y) \in \mathbb{K}[X,Y]$ kétváltozós polinomok felírhatók

$$f(X,Y) = a_0(Y)X^n + a_1(Y)X^{n-1} + \ldots + a_n(Y),$$
$$g(X,Y) = b_0(Y)X^m + b_1(Y)X^{m-1} + \ldots + b_m(Y)$$

alakban, ahol $n = \deg_X(f)$, $m = \deg_X(g)$, és $a_i(Y), b_j(Y)$ egyváltozós $\mathbb{K}$-beli együtthatós polinomok. Igaz továbbá, hogy $\deg(a_i) \leq i$, $\deg(b_j) \leq j$. Ebben az esetben f és g rezultánsa $\mathbb{K}$ feletti polinom:

$$R_{f,g}(Y) = \det \begin{pmatrix} a_0(Y) & \cdots & a_n(Y) & \cdots & 0 \\ & \ddots & & \ddots & \\ 0 & \cdots & a_0(Y) & \cdots & a_n(Y) \\ b_0(Y) & \cdots & b_m(Y) & \cdots & 0 \\ & \ddots & & \ddots & \\ 0 & \cdots & b_0(Y) & \cdots & b_m(Y) \end{pmatrix} \in \mathbb{K}[Y]. \tag{2.5}$$

A rezultánsok alaptétele ekkor két jelentéssel bír.

2.3.1. Állítás. Az $f(X,Y), g(X,Y)$ polinomoknak pontosan akkor van X-ben nem konstans közös tényezőjük, ha az X szerinti $R_{f,g}(Y)$ rezultáns polinom azonosan nulla. □

2.3.2. Állítás. Az $y \in \mathbb{K}$ rögzített elem pontosan akkor gyöke az $R_{f,g}(Y)$ rezultáns polinomnak, ha az $f(X,y), g(X,y) \in \mathbb{K}[X]$ polinomoknak van közös gyökük, azaz ha létezik $x \in \mathbb{K}$ szám, amelyre egyidejűleg teljesül $f(x,y) = 0$ és $g(x,y) = 0$. □

Kétváltozós polinomok rezultánsának egy fontos tulajdonságát mondja ki az alábbi állítás.

2.3.3. Állítás. Legyen az $f(X,Y), g(X,Y) \in \mathbb{K}[X,Y]$ polinomok totális foka n illetve m. Írjuk f-et és g-t

$$f(X,Y) = a_0(Y)X^n + a_1(Y)X^{n-1} + \ldots + a_n(Y),$$
$$g(X,Y) = b_0(Y)X^m + b_1(Y)X^{m-1} + \ldots + b_m(Y)$$

alakba és tegyük fel, hogy $a_0 = a_0(Y)$ vagy $b_0 = b_0(Y)$ konstans polinomok közül valamelyik nem nulla. Ekkor az $R_{f,g}(Y)$ rezultáns foka legfeljebb nm.

Bizonyítás. A 2.1.1 megjegyzés alapján alkalmazhatjuk a rezultánsok alaptételét. Jelölje c_{ij} a (2.5) mátrix i-dik sorának j-dik elemét, ekkor

$$c_{ij} = \begin{cases} a_{j-i}(Y) & \text{ha } 1 \le i \le m, i \le j \le n+i, \\ b_{j-i+m}(Y) & \text{ha } m+1 \le i \le m+n, i-m \le j \le n-m+i, \\ 0 & \text{különben.} \end{cases}$$

Ekkor

$$\deg(c_{ij}) \le \begin{cases} j-i & \text{ha } 1 \le i \le m, i \le j \le n+i, \\ j-i+m & \text{ha } m+1 \le i \le m+n, i-m \le j \le n-m+i, \\ -\infty & \text{különben.} \end{cases}$$

Tekintsük az $R_{f,g}(Y)$ determináns kiszámításakor adódó összeg tetszőleges tagját, ez $\pm c_{1\pi(1)} \cdots c_{n+m,\pi(n+m)}$ alakú az $\{1, \dots, n+m\}$ halmaz valamilyen π permutációjára. Ha valamelyik $c_{i\pi(i)}$ tényező nulla, akkor ez a tag nem játszik szerepet $R_{f,g}(Y)$ értékében. Tegyük fel, hogy minden tényező különbözik nullától. Ekkor

$$\begin{aligned} \deg(\pm c_{1\pi(1)} \cdots c_{n+m,\pi(n+m)}) &= \sum_{i=1}^{n+m} \deg(c_{i\pi(i)}) \\ &\le \sum_{i=1}^{m} (\pi(i) - i) + \sum_{i=m+1}^{n+m} (\pi(i) - i + m) \\ &= nm + \sum_{i=1}^{n+m} (\pi(i) - i) \\ &= nm + \sum_{i=1}^{n+m} \pi(i) - \sum_{i=1}^{n+m} i \\ &= nm. \end{aligned}$$

Azaz a determináns kiszámításakor minden nem nulla tag foka legfeljebb nm, vagyis $\deg(R_{f,g}(Y)) \le nm$. □

2.4. Feladatok

2.4.1. Feladat. Legyen $f(X) = X^3 + aX + b$. Mutassuk meg, hogy $R_{f,f'} = 4a^3 + 27b^2$.

2.4.2. Feladat. Legyen

$$\begin{aligned} f &= X^2Y - 3XY^2 + X^2 - 3XY, \\ g &= X^3Y + X^3 - 4Y^2 - 3Y + 1. \end{aligned}$$

a) Számolja ki $R_{f,g}(Y)$-t.

b) Számolja ki $R_{f,g}(X)$-et. Mit mond az eredmény f-ről és g-ről?

2.4.3. Feladat. Legyen $f(Y) = a_0Y^m + a_1Y^{m-1} + \cdots + a_m$ és $g(Y) = Y - b$. Mutassuk meg, hogy ekkor $R_{f,g} = \pm f(b)$.

2.4.4. Feladat. A rezultáns segítségével keressük meg az alábbi paraméterezésben megadott görbék $f(X, Y)$ polinomját:

$$\begin{aligned} &(a) \quad x(t) = t^4, && y(t) = t + t^2, \\ &(b) \quad x(t) = t^2 + t^3, && y(t) = t^4, \\ &(c) \quad x(t) = \frac{t^2}{1+t^2}, && y(t) = \frac{t^3}{1+t^2}. \end{aligned}$$

[*Útmutatás:* Tekintsük az $f(X, Y, t) = X - x(t)$, $g(X, Y, t) = Y - y(t)$ polinomokat és a rezultáns segítségével küszöböljük ki a t ismeretlent.]

2.5. Rezultánsok alkalmazása irreducibilis görbékre

2.5.1. Tétel. Legyenek $\Gamma : f(X, Y) = 0$, $\Delta : g(X, Y) = 0$ algebrai görbék egy algebrailag zárt $\mathbb{K}$ test feletti síkon. Tegyük fel, hogy f irreducibilis és $\Gamma \subseteq \Delta$. Ekkor $f \mid g$.

Bizonyítás. Írjuk f-et $f = a_0(Y)X^n + \cdots + a_n$ alakba, ahol $a_0(Y) \neq 0$. Először tegyük fel, hogy $n = 0$, azaz f nem függ Y-tól. Ekkor $f = Y - c$ az irreducibilitás miatt. Megfelelő $h(X, Y)$ polinomra $g(X, Y) = (Y - c)h(X, Y) + g(X, c)$, és $\Gamma \subseteq \Delta$ miatt $g(X, c) = 0$, azaz $Y - c \mid g$.

Tegyük most fel, hogy $n \geq 1$ és $f \nmid g$. Ez utóbbiból adódik, hogy f-nek és g-nek nincsenek X-ben nem konstans közös tényezői, tehát $R_{f,g}(Y) \neq 0$. Vegyünk egy $y \in \mathbb{K}$ elemet, amelyre $a_0(y) \neq 0$ és $R_{f,g}(y) \neq 0$. Az $f(X, y)$ egyváltozós polinom nem konstans, így létezik $x \in \mathbb{K}$, amelyre $f(x, y) = 0$, azaz $(x, y) \in \Gamma \subseteq \Delta$ és $g(x, y) = 0$. Ekkor x közös gyöke $f(X, y)$-nak és $g(X, y)$-nak, ami ellentmond $R_{f,g}(y) \neq 0$-nak. □

Ugyanezt a tételt megfogalmazhatjuk többváltozós polinomokra is. A bizonyítást az olvasóra bízzuk.

2.5.2. Tétel. Legyen $\mathbb{K}$ algebrailag zárt test, $f(X_1, \ldots, X_n) \in \mathbb{K}[X_1, \ldots, X_n]$ irreducibilis polinom és tegyük fel, hogy a $g(X_1, \ldots, X_n) \in \mathbb{K}[X_1, \ldots, X_n]$ polinom minden $(x_1, \ldots, x_n) \in \mathbb{K}^n$ specializációjára $f(x_1, \ldots, x_n) = 0$ maga után vonja $g(x_1, \ldots, x_n) = 0$ teljesülését. Ekkor $f \mid g$.

2.6. A rezultáns szorzatra bontása (szorgalmi)

Szokásunkhoz híven tekintsük az

$$\begin{aligned} f(X) &= a_0X^n + a_1X^{n-1} + \cdots + a_n, \\ g(X) &= b_0X^m + b_1X^{m-1} + \cdots + b_m \end{aligned}$$

polinomokat, azonban most a $a_0, \dots, a_n, b_0, \dots, b_m$ szimbólumok $\mathbb{K}$ feletti változókat jelölnek, azaz

$$f(X), g(X) \in \mathbb{K}[X, a_0, \dots, a_n, b_0, \dots, b_m].$$

Ekkor a két polinom $R_{f,g}$ rezultánsa az $a_0, \dots, a_n, b_0, \dots, b_m$ változóknak egész együtthatós polinomja. Könnyű látni továbbá, hogy $R_{f,g}$ homogén m-edfokú az $a_0, \dots, a_n$, és homogén n-edfokú a $b_0, \dots, b_m$ változókban.

2.6.1. Állítás. Az $R_{f,g} \in \mathbb{K}[a_0, \dots, a_n, b_0, \dots, b_m]$ polinom irreducibilis.

Bizonyítás. Alkalmazzunk $n + m$ szerinti teljes indukciót. Ha $n = m = 1$, akkor $R_{f,g} = a_0 b_1 - a_1 b_0$ irreducibilis. Tegyük fel, hogy $m > 1$ és legyen

$$R_{f,g} = S_1 \cdot S_2 \cdot \ldots \cdot S_k$$

felbontás irreducibilis tényezőkre. Legyen $g_1(X) = g(X)|_{b_0=0} = b_1 X^{m-1} + \cdots + b_m$. Az indukciós feltétel szerint R_{f,g_1} irreducibilis. Egyrészt

$$R_{f,g}|_{b_0=0} = a_0 R_{f,g_1}$$

irreducibilis felbontás. Másrészt

$$R_{f,g}|_{b_0=0} = S_1|_{b_0=0} \cdot S_2|_{b_0=0} \cdot \ldots \cdot S_k|_{b_0=0}.$$

A kettő összevetéséből következik, hogy

$$S_i = \begin{cases} \alpha + b_0(\cdots), & \text{vagy} \\ \alpha a_0 + b_0(\cdots), & \text{vagy} \\ \alpha R_{f,g_1} + b_0(\cdots), & \text{vagy} \\ \alpha a_0 R_{f,g_1} + b_0(\cdots), & \end{cases}$$

ahol $\alpha \in \mathbb{K}^*$. Mivel azonban homogén polinom tényezői is homogének, ezért $S_i = \alpha + b_0(\cdots)$ és $S_i = \alpha a_0 + b_0(\cdots)$ nem lehetséges. Azonban a_0-nak valamelyik $S_i|_{b_0=0}$ tényezőben elő kell fordulnia, így azt kapjuk, hogy valamely i-re $S_i = \alpha a_0 R_{f,g_1} + b_0(\cdots)$. Ebből azonban adódik $k = i = 1$, azaz $R_{f,g}$ irreducibilis. □

2.6.2. Állítás. Jelöljenek $U_1, \dots, U_n, V_1, \dots, V_m$ $\mathbb{K}$ feletti változókat és definiáljuk a

$$f(X) = (X - U_1) \cdots (X - U_n),$$
$$g(X) = (X - V_1) \cdots (X - V_m)$$

$\mathbb{K}[X, U_1, \dots, U_n, V_1, \dots, V_m]$-beli polinomokat. Ekkor

$$R_{f,g} = \prod_{i,j=0}^{n,m} (U_i - V_j).$$

Bizonyítás. Az f-ben X^{n-i}-nak az a_i együtthatója az $U_1, \dots, U_n$ változók i-edfokú elemi szimmetrikus polinomja. Hasonlóan g-ben az X^{m-j} együtthatója a $V_1, \dots, V_m$ változók j-edfokú elemi szimmetrikus polinomja. A 2.3.3 állítás bizonyításában látottak szerint megmutathatjuk, hogy $R_{f,g}$ homogén nm-fokú homogén polinomja $U_1, \dots, V_m$-nek.

Megmutatjuk, hogy $\prod_{i,j=0}^{n,m}(U_i - V_j)$ is osztja $R_{f,g}$-t. Nyilván elegendő belátni a rögzített $1 \le i \le n$ és $1 \le j \le m$ indexekre. Az $U_1, \dots, V_m$ változók tetszőleges $u_1, \dots, v_m \in \mathbb{K}$ specializálásánál $u_i = v_j$ esetén a rezultáns értéke 0 lesz. Mivel $U_i - V_j$ irreducibilis, így alkalmazhatjuk a 2.5.2 tételt, és kapjuk, hogy $U_i - V_j \mid R_{f,g}$. Ebből, és a fokszámok egyezéséből adódik, hogy valamely $\alpha \in \mathbb{K}$ konstansra

$$R_{f,g} = \alpha \prod_{i,j=0}^{n,m}(U_i - V_j).$$

Specializáljuk az $U_1, \dots, U_n$ változókat csupa 0-val. Ekkor $f(X) = X^n$ és

$$R_{f,g} = \det \begin{pmatrix} 1 & \cdots & 0 & 0 & \cdots & 0 \\ & \ddots & & & & \\ 0 & \cdots & 1 & 0 & \cdots & 0 \\ 1 & \cdots & b_{m-1} & b_m & \cdots & 0 \\ & & & & \ddots & \\ 0 & \cdots & 1 & b_1 & \cdots & b_m \end{pmatrix} = b_m^n = ((-1)^m V_1 \cdots V_m)^n.$$

Másrészről

$$\prod_{i,j=0}^{n,m}(0 - V_j) = ((-1)^m V_1 \cdots V_m)^n,$$

tehát $\alpha = 1$. □

Megjegyezzük, hogy ha

$$f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n,$$
$$g(X) = b_0 X^m + b_1 X^{m-1} + \cdots + b_m$$

polinomok tetszőleges D integritástartományból vett együtthatókkal, akkor is tekinthetjük az $u_1, \dots, u_n, v_1, \dots, v_m$ gyökeiket a D hányadostestének algebrai lezártjában. Bármennyire is absztrakt konstrukciók ekkor a gyökök, a szimmetrikus polinomjaik visszaadják az $a_0, \dots, b_m \in D$ elemeket, azaz a $\prod(u_i - v_j)$ szorzat a rezultáns D-beli értéke. Speciálisan, ha az $a_0, \dots, b_m$ együtthatók $\mathbb{K}$ feletti változók, akkor $D = \mathbb{K}[a_0, \dots, b_m]$.

A fejezetben eddig vizsgált polinomok főegyütthatója 1 volt. A továbbiakat egyszerűsítendő gondoljuk meg az általános főegyüttható esetét.

2.6.1. Feladat. Legyen $f(X) = a_0(X - u_1) \cdots (X - u_n)$, $g(X) = b_0(X - v_1) \cdots (X - v_m)$. Ekkor

$$R_{f,g} = a_0^m b_0^n \prod_{i,j=0}^{n,m}(u_i - v_j).$$

A következő két állításhoz legyenek

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n,$$
$$g(X) = b_0X^m + b_1X^{m-1} + \cdots + b_m,$$
$$h(X) = c_0X^k + c_1X^{k-1} + \cdots + c_k$$

polinomok változó együtthatókkal.

2.6.3. Állítás. $R_{fg,h} = R_{f,h}R_{g,h}$.

Bizonyítás. Legyen $D = \mathbb{K}[a_0, \ldots, c_k]$ és $\mathbb{L}$ a D hányadostestének algebrai lezártja. Legyenek $u_1, \ldots, u_n$, $v_1, \ldots, v_m$ és $w_1, \ldots, w_k$ az f, g, h gyökei $\mathbb{L}$-ban. Az fg főegyütthatója a_0b_0, foka $n + m$ és gyökei $u_1, \ldots, v_m$. Az állítás következik a 2.6.1 feladat állításából. □

2.6.4. Állítás. $R_{f,g} \mid R_{f,g+fh}$.

Bizonyítás. Tekintsük $R_{f,g}$-t és $R_{f,g+fh}$-t mint komplex együtthatós polinomokat. Az $a_0, \ldots, a_n, b_0, \ldots, b_m$ változók bármely olyan $\mathbb{C}$-beli specifikációja, melyre $R_{f,g} = 0$, olyan komplex együtthatós f, g polinomoknak felel meg, melyeknek van közös gyökük. Ekkor azonban tetszőleges $h \in \mathbb{C}[X]$ polinom esetén az $f, g + fh$ polinomoknak is van közös gyökük, azaz $R_{f,g+fh} = 0$. $R_{f,g}$ irreducibilitásából (2.6.1 állítás) és a 2.5.2 tételből következik $R_{f,g} \mid R_{f,g+fh}$. □

3. fejezet

Affin sokaságok

Bevezető

Legyen K test, $f_1, \dots, f_m \in K[X_1, \dots, X_n]$ polinomok és tekintsük a

$$\begin{cases} f_1(x_1, \dots, x_n) & = 0 \\ f_2(x_1, \dots, x_n) & = 0 \\ & \vdots \\ f_m(x_1, \dots, x_n) & = 0 \end{cases}$$

egyenletrendszer megoldásainak M halmazát K^n-ben. Ennek az összefoglalónak a célja az M alapvető geometriai tulajdonságainak megadása, valamint az ehhez szükséges algebrai eszköztár kiépítése.

3.1. Ideálok

Ebben a fejezetben A egységelemes kommutatív gyűrűt jelöl.

3.1.1. Definíció. Az $I \subseteq A$ részhalmazt *ideálnak* nevezzük, ha additív részcsoport és minden $a \in A$ elemre $aI \subseteq I$ („szívóhatás"); jelölés $I \lhd A$. Az $a + I = \{a + x \mid x \in I\}$ részhalmazok I *mellékosztályai*; a mellékosztályok halmazát A/I jelöli. Az A/I halmaz az

$$\begin{aligned} (a + I) + (b + I) &= (a + b) + I, \\ (a + I) - (b + I) &= (a - b) + I, \\ (a + I)(b + I) &= ab + I \end{aligned}$$

műveletekre nézve alkotja A *faktorgyűrűjét*. Az $A \to A/I$, $a \mapsto a + I$ leképezést az I ideál szerint *természetes homomorfizmusnak* nevezzük.

Az A *triviális ideáljai* $\{0\}$ és A. Ideálok metszete ideál. Két $I, J \lhd A$ ideál összegét és szorzatát

$$\begin{aligned} I + J &= \{x + y \mid x \in I, y \in J\}, \\ IJ &= \{x_1y_1 + \dots + x_ny_n \mid x_i \in I, y_i \in J\} \end{aligned}$$

definiálja, ezek szintén A ideáljai. Legyen B gyűrű. A $\varphi : A \to B$ gyűrűhomomorfizmus

$$\ker(\varphi) = \{a \in A \mid \varphi(a) = 0\}$$

magja ideál A-ban. Az egységelemes kommutatív gyűrűkre vonatkozó izomorfia tételek az alábbi tulajdonságokat rögzítik.

(IT-1) $\mathrm{Im}(\varphi) \cong A/\ker(\varphi)$.

(IT-2) Ha B részgyűrű A-ban és $I \lhd A$, akkor $B \cap I \lhd B$ és $(B+I)/I \cong B/(B \cap I)$.

(IT-3) Legyen $I \lhd A$. A/I részgyűrűi és ideáljai megfelelnek az A gyűrű I-t tartalmazó részgyűrűinek és ideáljainak. Ha $J \supseteq I$ ideál A-ban, akkor $J/I \lhd A/I$ és $(A/I)/(J/I) \cong A/J$.

3.1.2. Definíció. Egy $S \subseteq A$ részhalmaz esetén az *S által generált ideál* az S-et tartalmazó legszűkebb I ideál; jelelölés $I = \langle S \rangle$. Az egyetlen elem által generált ideálokat *főideáloknak* nevezzük. Ha A minden ideálja főideál, akkor *A főideálgyűrű.*

Teljesül

$$\langle S \rangle = \{a_1 x_1 + \cdots + a_n x_n \mid a_i \in A, x_i \in S\}. \tag{3.1}$$

Ha $S = \{x_1, \ldots, x_k\}$ véges halmaz, akkor

$$\langle S \rangle = \langle x_1, \ldots, x_k \rangle = \{a_1 x_1 + \cdots + a_k x_k \mid a_i \in A, x_i \in S\};$$

az ilyen ideálokat *végesen generált ideálnak* mondjuk.

3.1.1. Feladat. a) A triviális ideálok főideálok.

b) Az A gyűrű akkor és csak akkor test, ha csak triviális ideáljai vannak.

c) Tetszőleges $n \in \mathbb{Z}$ esetén $\langle n \rangle = n\mathbb{Z} \lhd \mathbb{Z}$ főideál; $\mathbb{Z}/n\mathbb{Z}$ a modulo n maradékosztályok gyűrűje.

d) A $K[X,Y]$ polinomgyűrűben az $I = \langle X, Y \rangle$ ideál a nulla konstanstagú polinomokból áll. I végesen generált, de nem főideál.

e) A $K[X_1, X_2, \ldots]$ végtelen változós polinomgyűrűben az $I = \langle X_1, X_2, \ldots \rangle$ ideál a nulla konstanstagú polinomokból áll; I nem végesen generált.

f) $\mathbb{Z}$ és $K[X]$ főideálgyűrűk.

3.2. Affin sokaságok

Ebben a fejezetben K tetszőleges testet jelöl. A nyomtatott $X, Y, Z, T, X_1, X_2, \ldots$ nagy betűk változókat, az $x, y, t, x_1, x_2, \ldots$ kis betűk rögzített K-beli elemeket fognak jelölni.

3.2.1. Definíció. (i) Legyen $S \subseteq K[X_1, \ldots, X_n]$. A

$$\mathscr{V}(S) = \{(x_1, \ldots, x_n) \in K^n \mid \forall f \in S : f(x_1, \ldots, x_n) = 0\}$$

halmazt az S *zéróhalmazának* nevezzük.

(ii) Ha $S = \{f_1, \ldots, f_m\}$ véges halmaz, akkor a $\mathscr{V}(S) = \mathscr{V}(f_1, \ldots, f_m)$ zéróhalmazt K feletti *affin sokaságnak* nevezzük.

(iii) Ha $f \in K[X_1, \ldots, X_n]$, akkor $\mathscr{V}(f)$-et $n = 2$ esetén *algebrai síkgörbének*, $n \geq 3$ esetén pedig *algebrai felületnek* is nevezzük.

(iv) Legyen $U \subseteq K^n$ tetszőleges részhalmaz. Az

$$\mathscr{I}(U) = \{f \in K[X_1, \ldots, X_n] \mid \forall (x_1, \ldots, x_n) \in U : f(x_1, \ldots, x_n) = 0\}$$

halmazt az U *eltűnési ideáljának* nevezzük.

A $\mathscr{V}$ és $\mathscr{I}$ hozzárendelések alábbi tulajdonságai nyilvánvalóak:

1) Az eltűnési ideál csakugyan ideál $K[X_1, \ldots, X_n]$-ben.

2) $\mathscr{V}(1) = \emptyset$ és $\mathscr{I}(\emptyset) = \langle 1 \rangle$.

3) $\mathscr{V}(\mathscr{I}(U)) \subseteq U$ és $\mathscr{I}(\mathscr{V}(S)) \subseteq (S)$.

4) $S_1 \subseteq S_2 \Longrightarrow \mathscr{V}(S_1) \supseteq \mathscr{V}(S_2)$.

5) $U_1 \subseteq U_2 \Longrightarrow \mathscr{I}(U_1) \supseteq \mathscr{I}(U_2)$. Ha U_1, U_2 affin sokaságok, akkor a fordított irány is teljesül.

Csak a legutolsó állítást indokoljuk. Legyen $U_2 = \mathscr{V}(f_1, \ldots, f_m)$. Ha $\mathscr{I}(U_1) \supseteq \mathscr{I}(U_2)$, akkor minden i-re $f_i \in \mathscr{I}(U_1)$, azaz minden f_i eltűnik U_1-en. Tehát $U_1 \subseteq \mathscr{V}(f_1, \ldots, f_m) = U_2$.

3.2.2. Állítás. Legyenek $U_1, \ldots, U_n$ végtelen halmazok K-ban és tegyük fel, hogy az $f \in K[X_1, \ldots, X_n]$ polinom eltűnik az $U_1 \times \cdots \times U_n$ halmazon. Ekkor $f = 0$ azonosan nulla. Speciálisan, $\mathscr{I}(U_1 \times \cdots \times U_n) = \langle 0 \rangle$.

Bizonyítás. Ha $n = 1$, akkor a feltétel szerint f-nek végtelen sok gyöke van, így $f = 0$. Alkalmazzunk indukciót n és tegyük fel, hogy $n - 1$-re igaz az állítás. Ha f nem függ X_n-től, akkor az indukciós feltétel szerint $f = 0$. Tegyük fel, hogy f nem konstans X_n-ben és legyen $d = \deg_{X_n}(f) > 0$. Írjuk f-et X_n polinomjaként:

$$f = a_0(X_1, \ldots, X_{n-1})X_n^d + \cdots + a_d(X_1, \ldots, X_{n-1}), \quad a_0 \neq 0.$$

Az indukciós feltétel miatt léteznek $u_1 \in U_1, \ldots, u_{n-1} \in U_{n-1}$ elemek, amire $a_0(u_1, \ldots, u_{n-1}) \neq 0$. Ez azt jelenti, hogy az $f(u_1, \ldots, u_{n-1}, X_n)$ nem konstans ($d > 0$ fokú) egyváltozós polinom X_n változóban. Mivel U_n végtelen, így van olyan $u_n \in U_n$ elem, amire $f(u_1, \ldots, u_n) \neq 0$. Ezzel beláttuk, hogy az $U_1 \times \cdots \times U_n$ halmazon eltűnő polinom szükségszerűen konstans nulla. □

3.2.3. Következmény. Ha K végtelen test, $f \in K[X_1, \ldots, X_n]$ és minden $(x_1, \ldots, x_n) \in K^n$ esetén $f(x_1, \ldots, x_n) = 0$, akkor $f = 0$.

3.2.4. Állítás. Legyenek $V = \mathscr{V}(f_1, \ldots, f_s)$ és $W = \mathscr{V}(g_1, \ldots, g_t)$ affin sokaságok. Ekkor

$$V \cap W = \mathscr{V}(f_1, \ldots, f_s, g_1, \ldots, g_t),$$
$$V \cup W = \mathscr{V}(f_i g_j \mid i = 1, \ldots, s,\ j = 1, \ldots, t).$$

Ebből adódóan $V \cap W$ és $V \cup W$ maguk is affin sokaságok.

Bizonyítás. Nyilván $\boldsymbol{x} \in V \cap W$ akkor és csak akkor, ha minden i, j-re $f_i(\boldsymbol{x}) = 0$ és $g_j(\boldsymbol{x}) = 0$. Az is világos, hogy $\boldsymbol{x} \in V \cup W$ esetén minden i, j-re $f_i(\boldsymbol{x})g_j(\boldsymbol{x}) = 0$. Tegyük fel, hogy $\boldsymbol{x} \notin V \cup W$. Ekkor valamilyen i-re $f_i(\boldsymbol{x}) \neq 0$ és valamilyen j-re $g_j(\boldsymbol{x}) \neq 0$, azaz $f_i(\boldsymbol{x})g_j(\boldsymbol{x}) \neq 0$. □

3.2.1. Feladat. a) Legyenek $f_1, \ldots, f_s, g_1, \ldots, g_t \in K[X_1, \ldots, X_n]$. Ha $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, akkor $\mathscr{V}(f_1, \ldots, f_s) = \mathscr{V}(g_1, \ldots, g_t)$.

b) $\langle X + Y, X - Y \rangle = \langle X, Y \rangle$.

c) $\langle X + XY, Y + XY, X^2, Y^2 \rangle = \langle X, Y \rangle$.

d) $\langle 2X^2 + 3Y^2 - 11, X^2 - Y^2 - 3 \rangle = \langle X^2 - 4, Y^2 - 1 \rangle$.

e) $\mathscr{I}(\mathscr{V}(X^n, Y^m)) = \langle X, Y \rangle$.

3.3. Hilbert-féle bázis tétel

Ebben a fejezetben a Hilbert-féle bázis tételt bizonyítjuk be. Hilbert idejében a „bázis" szó generátor elemet jelentett. A bemutatott bizonyítás S. Lang: Algebra könyvének IV.4 fejezetéből van. A tétel lényeges következménye lesz, hogy egy test feletti n-változós polinomgyűrű ideáljai végesen generáltak. Megjegyezzük, hogy a bizonyítás nem konstruktív, tehát ebben a formában nem ad algoritmust az ideál generátorelemeinek meghatározására. Ilyen algoritmust később, a Groebner-bázisok elméletének bemutatásakor fogunk megismerni.

3.3.1. Definíció. Az R egységelemes kommutatív gyűrűt *Noether-félének* nevezzük, ha minden ideálja végesen generált.

3.3.1. Példa. Nyilván minden főideálgyűrű Noether-féle, így Noether-gyűrűk a testek, illetve a test feletti egy változós polinomgyűrűk.

3.3.2. Tétel (Hilbert-féle bázis tétel)**.** Ha R Noether-féle, akkor az egyváltozós $R[X]$ polinomgyűrű is Noether-féle.

Bizonyítás. Legyen $I \lhd R[X]$, belátjuk, hogy I végesen generált. Jelölje J_k az 0-t és azon $a \in R$ elemeket tartalmazó halmazt, amely elemek előállnak I-beli k-adfokú

$$aX^k + a_1X^{k-1} + \cdots + a_k$$

polinomok főegyütthatójaként.

1. lépés: J_k ideál. Ha $a, b \in J_k$, akkor $a \pm b \in J_k$, mivel ezek a megfelelő polinomok összegének vagy különbségének főegyütthatói. Ha $a \in J_k$ és $b \in R$, akkor ba a megfelelő polinom b-szeresének főegyütthatója. Tehát csakugyan $J_k \lhd R$. Példának okárt gondoljuk meg, hogy $J_0 = R \cap I$.

2. lépés: $J_0 \subseteq J_1 \subseteq J_2 \subseteq \cdots$ egymásba ágyazott ideálok. Az $a \in J_k$ elem polinomját X-el szorozva olyan $k+1$ fokú polinomot kapunk, aminek főegyütthatója a, azaz $a \in J_{k+1}$.

3. lépés: $J \lhd R$. Tekintsük a

$$J = \cup_{k=0}^{\infty} J_k$$

halmazt. Az $a_1, a_2 \in J$ elemek valamely $k_1, k_2 \geq 0$ indexekre $a_1 \in J_{k_1}$ és $a_2 \in J_{k_2}$. Ekkor $a_1 \pm a_2 \in J_{k_1+k_2} \subseteq J$. Az $a \in J$, $b \in R$ elemekre $a \in J_k$ és $ab \in J_k \subseteq J$ teljesül. Tehát csakugyan $J \lhd R$.

4. lépés: $J = J_r$ valamilyen r indexre. Az R Noether-tulajdonsága miatt $J = \langle a_1, \ldots, a_n \rangle$ végesen generált. Minden $i = 1, \ldots, n$ indexhez létezik $k_i \geq 0$ úgy, hogy $a_i \in J_{k_i}$. Ha $r = k_1 + \cdots + k_n$, akkor $a_i \in J_r$ minden i-re, azaz $J = J_r = J_{r+2} = \cdots$.

Legyenek

$$\begin{array}{ll} a_{01}, \ldots, a_{0n_0} & \text{a } J_0 \text{ ideál generátorelemei,} \\ a_{11}, \ldots, a_{1n_1} & \text{a } J_1 \text{ ideál generátorelemei,} \\ & \vdots \\ a_{r1}, \ldots, a_{rn_r} & \text{a } J_r \text{ ideál generátorelemei.} \end{array}$$

Minden $i = 0, \ldots, r$ és $j = 1, \ldots, n_i$ indexre legyen f_{ij} olyan I-beli polinom, amelynek foka i és főegyütthatója a_{ij}. Jelölje $\tilde{I}$ az f_{ij} polinomok által generált ideált $R[X]$-ben. Nyilván $\tilde{I} \leq I$.

5. lépés: Adott $0 \neq f \in I$ polinomhoz konstruálunk $g \in \tilde{I}$ polinomot, amire $\deg(f) = \deg(g)$ és f, g főegyütthatói megegyeznek. Legyen $d = \deg(f)$, $0 \neq \alpha \in R$ az f főegyütthatója, azaz $f = \alpha X^d + \cdots$. Tegyük először fel, hogy $d \leq r$. Mivel $\alpha \in J_d$, léteznek $c_1, \ldots, c_{n_d} \in R$ elemek, melyekre

$$\alpha = c_1 a_{d,1} + c_2 a_{d,2} + \cdots + c_{n_d} a_{dn_d}.$$

Legyen

$$g = c_1 f_{d,1} + c_2 f_{d,2} + \cdots + c_{n_d} f_{dn_d} \in R[X].$$

Ekkor valóban $g \in \tilde{I}$, $\deg(g) = d$ és g főegyütthatója α. Ha $d > r$, akkor $\alpha \in J_r$ és megfelelő $c_i \in R$ együtthatókkal

$$\alpha = c_1 a_{r,1} + c_2 a_{r,2} + \cdots + c_{r_d} a_{dn_d},$$

és a

$$g = (c_1 f_{r,1} + c_2 f_{r,2} + \cdots + c_{n_r} f_{rn_r}) X^{d-r}$$

polinom megfelelő elem $\tilde{I}$-ben.

6. lépés: Megmutatjuk, hogy $I = \tilde{I}$, azaz I végesen generált. Tegyük fel, hogy $I \neq \tilde{I}$ és legyen $f \in I \setminus \tilde{I}$ minimális fokszámú polinom. Az 5. lépésben ismertetett módon konstruáljunk egy $g \in \tilde{I}$ polinomot, melyre $\deg(f) = \deg(g)$ és f, g főegyütthatói egyenlők. Erre $f - g \in I \setminus \tilde{I}$ és $\deg(f - g) < \deg(f)$, ami ellentmond f választásának. Ezzel a bizonyítást befejeztük. □

A változók számára vonatkozó indukcióval következik az alábbi állítás.

3.3.3. Következmény. Legyen K test. A $K[X_1, \ldots, X_n]$ polinomgyűrű minden ideálja végesen generált.

Egy további lényeges következmény az alábbi:

3.3.4. Állítás. Legyen K test. A következő fogalmak megegyeznek:

(i) A $\mathscr{V}(S) \subseteq K^n$ zéróhalmaz, ahol $S \subseteq K[X_1, \ldots, X_n]$.

(ii) A $\mathscr{V}(I) \subseteq K^n$ zéróhalmaz, ahol $I \lhd K[X_1, \ldots, X_n]$.

(iii) A $\mathscr{V}(f_1, \ldots, f_m) \subseteq K^n$ affin sokaság, ahol $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$.

Bizonyítás. Egyrészt $\mathscr{V}(S) = \mathscr{V}(I)$, ahol $I = \langle S \rangle$ a generált ideál. Másrészt a Hilbert-tétel miatt $I = (f_1, \ldots, f_m)$ végesen generált. □

Mint a bevezetőben említettük, a polinomgyűrűkre vonatkozó kérdések algoritmikus megválaszolásával továbbra is adósak vagyunk. A legfontosabb ilyen kérdés az ideálbeli tartalmazás eldöntése.

(*) Adott $f_1, \ldots, f_m, g \in K[X_1, \ldots, X_n]$ polinomok. Igaz-e, hogy $g \in \langle f_1, \ldots, f_m \rangle$?

Ennek segítségével ideálok egyenlőségét, illetve részhalmazként való tartalmazását meg tudjuk válaszolni.

3.4. Lineáris és affin transzformációk

Ebben a fejezetben K^n a K feletti n-dimenziós oszlopvektorok halmazát, $K^{m \times n}$ pedig a K feletti $m \times n$-es mátrixok halmazát jelöli.

3.4.1. Definíció. A K^n tér *affin leképezése* alatt egy $\alpha : \boldsymbol{x} \mapsto A\boldsymbol{x} + \boldsymbol{b}$ leképezést értünk, ahol $A \in K^{n \times n}$ és $\boldsymbol{b} \in K^n$. Ha $\boldsymbol{b} = 0$, akkor α *lineáris*. Ha $A = I$, akkor α *eltolás*. Ha A invertálható, akkor α-t *affin*, illetve *lineáris transzformációnak* nevezzük.

3.4.2. Állítás. Az affin transzformációk csoportot alkotnak. Ebben a csoportban a lineáris transzformációk részcsoportot, az eltolások pedig egy Abel-féle normálosztót alkotnak.

Bizonyítás. Az $\alpha : \boldsymbol{x} \mapsto A\boldsymbol{x} + \boldsymbol{b}$ affin transzformáció inverze $\boldsymbol{x}' \mapsto A^{-1}\boldsymbol{x}' - A^{-1}\boldsymbol{b}$. Az $\alpha_1 : \boldsymbol{x} \mapsto A_1\boldsymbol{x} + \boldsymbol{b}_1$ és $\alpha_2 : \boldsymbol{x} \mapsto A_2\boldsymbol{x} + \boldsymbol{b}_2$ affin transzformációk szorzata $\boldsymbol{x} \mapsto A_1A_2\boldsymbol{x} + A_1\boldsymbol{b}_2 + \boldsymbol{b}_1$. Megmutatjuk még, hogy az eltolások normálosztót alkotnak. Legyen $\alpha : \boldsymbol{x} \mapsto A\boldsymbol{x} + \boldsymbol{b}$ affin transzformáció és $\tau : \boldsymbol{x} \mapsto \boldsymbol{x} + \boldsymbol{u}$ eltolás. Ekkor

$$\alpha\tau\alpha^{-1} : \boldsymbol{x} \mapsto A((A^{-1}\boldsymbol{x}' - A^{-1}\boldsymbol{b}) + \boldsymbol{u}) + \boldsymbol{b} = \boldsymbol{x} + A\boldsymbol{u}$$

eltolás az $A\boldsymbol{u}$ vektorral. □

3.4.3. Definíció. A K^n tér α affin transzformáció által a $K[\boldsymbol{X}] = K[X_1, \ldots, X_n]$ polinomgyűrűn *indukált* α^* *leképezés* az $f(\boldsymbol{X})$ polinomhoz az $f(\alpha^{-1}(\boldsymbol{X}))$ polinomot rendeli.

Ha $\alpha : \boldsymbol{x} \mapsto A\boldsymbol{x} + \boldsymbol{b}$ affin transzformáció, akkor érdemes α^*-ra úgy gondolni, hogy $g = \alpha^* f$ akkor és csak akkor, ha $g(A\boldsymbol{X} + \boldsymbol{b}) = f(\boldsymbol{X})$. Más szóval, $f(\boldsymbol{X})$-et megkapjuk $g(\boldsymbol{Y})$-ból az $\boldsymbol{Y} = A\boldsymbol{X} + \boldsymbol{b}$ *behelyettesítéssel.*

3.4.4. Állítás. Legyen α affin transzformáció. Ekkor $\alpha^* : K[\boldsymbol{X}] \to K[\boldsymbol{X}]$ olyan gyűrűhomomorfizmus, ami megőrzi a polinomok totális fokát. Teljesül továbbá $(\alpha\beta)^* = \alpha^*\beta^*$ és $(\alpha^{-1})^* = (\alpha^*)^{-1}$.

Bizonyítás. Könnyű meggondolni, hogy α^* gyűrűhomomorfizmus, és azt is, hogy elsőfokú kifejezés behelyettesítése nem növeli a totális fokot. Tehát $\deg(f) \leq \deg(\alpha^* f)$ és mivel α és α^* invertálhatóak, így $\deg(f) = \deg(\alpha^* f)$.

$$\begin{aligned}((\alpha^*\beta^*)f)(\boldsymbol{X}) &= (\alpha^*(\beta^* f))(\boldsymbol{X}) \\ &= (\beta^* f)(\alpha^{-1}\boldsymbol{X}) \\ &= f(\beta^{-1}\alpha^{-1}\boldsymbol{X}) \\ &= f((\alpha\beta)^{-1}\boldsymbol{X}) \\ &= ((\alpha\beta)^*)f)(\boldsymbol{X}).\end{aligned}$$

$(\alpha^{-1})^* = (\alpha^*)^{-1}$ hasonlóan adódik. □

Affin transzformációkat használhatunk arra, hogy polinomiális egyenleteket és egyenletrendszereket egyszerűbb alakra hozzunk. Például eltolással elérhetjük, hogy egy adott f polinom konstans tagja nulla legyen. Ez pontosan azt jelenti, hogy az origó benne van lesz a $\mathscr{V}(f)$ algebrai felületben. Általánosabban teljesül az alábbi állítás:

3.4.5. Állítás. Legyen α affin transzformáció és $f_1, \ldots, f_m \in K[\boldsymbol{X}]$ polinomok. Ekkor

$$\alpha(\mathscr{V}(f_1, \ldots, f_m)) = \mathscr{V}(\alpha^* f_1, \ldots, \alpha^* f_m).$$

Speciálisan, affin transzformációk algebrai sokaságokat algebrai sokaságokban képeznek.

Bizonyítás. Csakugyan,

$$\begin{aligned}\boldsymbol{x} \in \alpha(\mathscr{V}(f_1,\dots,f_m)) &\Leftrightarrow \alpha^{-1}(\boldsymbol{x}) \in \mathscr{V}(f_1,\dots,f_m)\\ &\Leftrightarrow f_1(\alpha^{-1}(\boldsymbol{x})) = \dots = f_m(\alpha^{-1}(\boldsymbol{x})) = 0\\ &\Leftrightarrow (\alpha^* f_1)(\boldsymbol{x}) = \dots = (\alpha^* f_m)(\boldsymbol{x}) = 0\\ &\Leftrightarrow \boldsymbol{x} \in \mathscr{V}(\alpha^* f_1,\dots,\alpha^* f_m).\end{aligned}$$

Megjegyezzük, hogy mivel α^* gyűrűautomorfizmus, így polinomideálokat polinomideálokba képez, azaz az állítás $\alpha(\mathscr{V}(I)) = \mathscr{V}(\alpha^* I)$ alakban is írható. □

Könnyű meggondolni, hogy az affin transzformációk tranzitívan hatnak a sík egyenesein, azaz bármely egyenes elvihető bármely egyenesbe affin transzformációval. Azt sem nehéz látni, hogy $K = \mathbb{R}$ esetén bármely irreducibilis másodfokú polinom $Y - X^2$ vagy $X^2 \pm Y^2 \pm 1$ alakra hozható. Ezeket az irreducubilis másodfokú görbék ($\mathbb{R}$ feletti) affin kanonikus alakjának hívjuk.

3.4.1. Feladat. a) Határozzuk meg azt az affin transzformációt, ami az $5X - 3Y + 1$ egyenest az $Y = 0$ egyenesbe viszi.

b) Határozzuk meg azt az eltolást, mely a $K : X^2 + Y^2 + 4X + Y - 1 = 0$ másodrendű görbéből eliminálja az X-es és Y-os tagok együtthatóit.

c) Határozzuk meg azt az eltolást, mely a $K : X^2 - X + 4Y - 1 = 0$ másodrendű görbéből eliminálja az X-es tag együtthatóját és a konstanst.

d) Határozzuk meg annak az origó körüli forgatásnak az α szögét, mely a $K : X^2 - XY + 3Y^2 + 4X - 2Y = 0$ másodrendű görbéből eliminálja az XY-os tag együtthatóját.

e) Határozzunk meg egy olyan affin transzformációt, amely az alábbi másodrendű görbéket affin kanonikus alakba viszi.

   (1) $K : X^2 - 2XY - 8Y^2 + 18Y = 0$,

   (2) $K : X^2 + 4XY + 4Y^2 - 2X - 8Y + 5 = 0$,

   (3) $K : 9X^2 + 36Y^2 - 12X - 24Y + 4 = 0$.

f) Határozzuk meg a $K : 3X^2 + 10XY + 3Y^2 + 10X + 14Y + 8 = 0$ elfajuló másodrendű görbe affin kanonikus alakját.

3.4.2. Feladat. Tegyük fel, hogy $\mathrm{char}(K) \neq 2, 3$ és $a_{02} \neq 0$. Mutassuk meg, hogy az

$$X^3 + a_{20}X^2 + a_{11}XY + a_{02}Y^2 + a_{10}X + a_{01}Y + a_{00} = 0$$

egyenletű harmadfokú görbe affin transzformációval

$$Y^2 = X^3 + aX + b$$

alakúra hozható. [*Útmutatás:* 1) $-a_{02}^3$-el leosztva elérhető $a_{02} = -1$. 2) Eliminálják az XY és Y tagokat. 3) Eliminálják az X^2 tagot.]

3.5. Hilbert-féle normalizálási lemma

A Hilbert-féle normalizálási lemma egy végesen generált kommutatív algebráknak egy viszonylag elvont tulajdonságát mondja ki, amire nekünk ebben az általánosságban nem lesz szükségünk. Viszont a bizonyítás egy meglehetősen elemi észrevételen alapszik, amit a következő tétel mond ki.

3.5.1. Tétel (Hilbert-féle normalizálási lemma)**.** Legyen K végtelen test, $0 \neq f \in K[X_1, \ldots, X_n]$ polinom és $d = \deg(f)$. Ekkor létezik a K^n tér olyan α lineáris transzformációja, melyre $\alpha^* f$-ben az X_n^d monóm együtthatója nem nulla.

A bizonyítás előtt definiáljuk a *homogén polinom* fogalmát.

3.5.2. Definíció. Azt mondjuk, hogy az $f(X_1, \ldots, X_n)$ polinom *d-fokú homogén polinom,* ha minden monómjának totális foka d.

3.5.3. Lemma. Az $f(X_1, \ldots, X_n)$ polinom akkor és csak akkor d-fokú homogén, ha a T határozatlanra teljesül az

$$f(TX_1, \ldots, TX_n) = T^d f(X_1, \ldots, X_n)$$

polinomiális egyenlőség.

Bizonyítás. Elegendő meggondolni, hogy egy monóm esetén az egyenlőség akkor és csak akkor teljesül, ha a monóm totális foka d. □

Legyen f n változós, d totális fokú polinom:

$$f = \sum_{\substack{i_1,\ldots,i_n \geq 0 \\ i_1+\cdots+i_n \leq d}} a_{i_1 \cdots i_n} X_1^{i_1} \cdots X_n^{i^n}.$$

Definiáljuk f r-fokú homogén komponensét, mint az r totális fokú monómok összege:

$$f_r = \sum_{\substack{i_1,\ldots,i_n \geq 0 \\ i_1+\cdots+i_n = r}} a_{i_1 \cdots i_n} X_1^{i_1} \cdots X_n^{i^n}.$$

Ekkor f egyértelmű módon a homogén komponenseinek

$$f = f_0 + f_1 + \cdots + f_d$$

összegeként írható. Megjegyezzük még, hogy lineáris transzformációk d-fokú homogén polinomokat ugyanilyenbe visznek, és megőrzik a polinomok homogén komponenseit.

Szükségünk van még az eltolások polinomokon vett hatásának közelebbi leírására.

3.5.4. Lemma. A d-fokú $f(T_1, \ldots, T_n)$ polinomra teljesül

$$f(T_1 + b_1, \ldots, T_n + b_n) = f(T_1, \ldots, T_n) + O(d-1),$$

ahol $O(d-1)$ legfeljebb $(d-1)$-fokú monómokból áll.

Bizonyítás. Mivel f monómok lineáris kombinációja, elegendő megmutatni egyetlen $T_1^{i_1} \cdots T_n^{i_n}$ monómra:

$$(T_1 + b_1)^{i_1} \cdots (T_n + b_n)^{i_n} = T_1^{i_1} \cdots T_n^{i_n} + O(d-1),$$

ami nyilván teljesül. □

A 3.5.1 Tétel bizonyítása. Mivel f nem nulla, az f_d d-fokú homogén komponens értelmezett. Legyen X_i egy változó, ami előfordul f_d-ben. A változók permutációjával (ami lineáris transzformáció) elérhető, hogy f_d-ben előforduljon X_n. Ez azt jelenti, hogy $f_d(X_1, \ldots, X_{n-1}, 1) \neq 0$. Mivel K végtelen, a 3.2.3 Következmény szerint léteznek $\lambda_1, \ldots, \lambda_{n-1} \in K$ értékek, amikre $c = f_d(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$. Tekintsük most az $\alpha : \boldsymbol{x} \mapsto \boldsymbol{x}'$ affin transzformációt, ahol

$$\begin{aligned} x_1' &= x_1 - \lambda_1 x_n, \\ x_2' &= x_2 - \lambda_2 x_n, \\ &\vdots \\ x_{n-1}' &= x_{n-1} - \lambda_{n-1} x_n, \\ x_n' &= x_n. \end{aligned}$$

Az α^{-1} transzformáció

$$\begin{aligned} x_1 &= x_1' + \lambda_1 x_n', \\ x_2 &= x_2' + \lambda_2 x_n', \\ &\vdots \\ x_{n-1} &= x_{n-1}' + \lambda_{n-1} x_n', \\ x_n &= x_n'. \end{aligned}$$

A 3.5.4 Lemmát használva $T_i = \lambda_i X_n'$, $b_i = X_i'$, $(i = 1, \ldots, n-1)$, és $T_n = X_n'$, $b_n = 0$ értékekkel, adódik:

$$\begin{aligned} f(X_1' + \lambda_1 X_n', \ldots, X_{n-1}' + \lambda_{n-1} X_n', X_n') &= f(\lambda_1 X_n', \ldots, \lambda_{n-1} X_n', X_n') + O_{X_n'}(d-1) \\ &= f_d(\lambda_1 X_n', \ldots, \lambda_{n-1} X_n', X_n') + O_{X_n'}(d-1) \\ &= f_d(\lambda_1, \ldots, \lambda_{n-1}, 1)(X_n')^d + O_{X_n'}(d-1) \\ &= c(X_n')^d + O_{X_n'}(d-1). \end{aligned}$$

Ezt azt jelenti, hogy az $(\alpha^* f)(X_1, \ldots, X_n) = cX_n^d + O_{X_n'}(d-1)$, ami $c \neq 0$ miatt pont a bizonyítandó állítás. □

3.6. Hilbert-féle zérushely tétel (Nullstellensatz)

Ebben a fejezetben bebizonyítjuk a Hilbert-féle zérushely tétel gyenge, majd erős változatát. A bizonyítás a lehető legelemibb, E. Arrondo: Another Elementary Proof of the Nullstellensatz c. cikkét követi (American Mathematical Monthly 113, 2006/2).

3.6.1. Tétel (Gyenge Nullstellensatz)**.** Legyen K algebrailag zárt és $I \lhd K[X_1, \dots, X_n]$ valódi ideál. Ekkor létezik $(a_1, \dots, a_n) \in K^n$ úgy, hogy minden $f \in I$ esetén $f(a_1, \dots, a_n) = 0$.

Bizonyítás. n szerinti indukciót alkalmazunk. $n = 1$ esetén $I = \langle g \rangle$ főideál, ahol g nem konstans. K algebrai zártsága miatt g-nek van $a_1 \in K$ gyöke, ezért bármely $f \in I$ esetén $f = gh$ és $f(a_1) = 0$, azaz az állítás teljesül.

Legyen $n > 1$. Feltehetjük, hogy létezik $d > 0$ fokú $g \in I$ polinom, amiben az X_n^d monóm együtthatója nem nulla. Valóban, legyen $h \in I$ tetszőleges $d > 0$ fokú polinom és legyen α a 3.5.1 Tétel szerinti lineáris transzformáció. Ekkor $\alpha^* h \in \alpha^*(I)$. Továbbá, ha $\alpha^*(I)$-re megmutatjuk, hogy $\alpha(\mathcal{V}(I)) = \mathcal{V}(\alpha^*(I)) \neq \emptyset$, akkor nyilván $\mathcal{V}(I) \neq \emptyset$, pont a bizonyítandó állítás. Írjuk az említett g polinomot

$$g = g_0 X_n^d + g_1 X_n^{d-1} + \cdots + g_d$$

alakban, ahol $g_i \in K[X_1, \dots, X_{n-1}]$. A feltétel szerint $\deg(g_i) \leq i$ és $g_0 \in K \setminus \{0\}$.

Legyen $I' = I \cap K[X_1, \dots, X_{n-1}]$ azon polinomok halmaza, amik nem függenek az X_n változótól. Mivel $I' \lhd K[X_1, \dots, X_{n-1}]$ és $1 \notin I'$, az indukciós hipotézis szerint léteznek $a_1, \dots, a_{n-1} \in K$ értékek, melyekre $f(a_1, \dots, a_{n-1}) = 0$ minden $f \in I'$ esetén. (Megjegyezzük, hogy $I' = 0$ lehetséges.)

Tekintsük az egyváltozós polinomok

$$J = \{f(a_1, \dots, a_{n-1}, X_n) \mid f \in I\}$$

halmazát, ez ideál $K[X_n]$-ben. Ha $J \neq \langle 1 \rangle$, akkor a bizonyítás elején elmondottak szerint valamely $a_n \in K$ elemre teljesül $(a_1, \dots, a_n) \in \mathcal{V}(I)$, és készen vagyunk. Tegyük tehát fel, hogy $1 \in J$, azaz valamely $f \in I$ polinomra $f(a_1, \dots, a_{n-1}, X_n) = 1$. Írjuk fel f-et X_n polinomjaként:

$$f = f_0 X_n^m + f_1 X_n^{m-1} + \cdots + f_m,$$

ahol $f_i \in K[X_1, \dots, X_{n-1}]$. Az $f(a_1, \dots, a_{n-1}, X_n) = 1$ egyenlőségből

$$f_0(a_1, \dots, a_{n-1}) = \cdots = f_{m-1}(a_1, \dots, a_{n-1}) = 0 \tag{3.2}$$

és

$$f_m(a_1, \dots, a_{n-1}) = 1 \tag{3.3}$$

következik. Vizsgáljuk a g és f polinomok X_n változó szerinti

$$R_{g,f} = \det \begin{pmatrix} g_0 & g_1 & \cdots & g_d & 0 & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{d-1} & g_d & 0 & \cdots & 0 \\ \vdots & & \ddots & & & \ddots & & \\ 0 & 0 & \cdots & g_0 & g_1 & \cdots & g_{d-1} & g_d \\ f_0 & f_1 & \cdots & f_{m-1} & f_m & 0 & \cdots & 0 \\ 0 & f_0 & \cdots & f_{m-2} & f_{m-1} & f_m & \cdots & 0 \\ & & \ddots & & & & \ddots & \\ 0 & 0 & 0 & f_0 & f_1 & \cdots & f_{m-1} & f_m \end{pmatrix}$$

rezultánsát. Egyrészt $R_{g,f} \in K[X_1, \ldots, X_{n-1}]$. Másrészt megfelelő

$$A, B \in K[X_1, \ldots, X_n]$$

polinomokra

$$R_{g,f} = Ag + Bf,$$

azaz $R_{g,f} \in I$. Ezekből adódik $R_{g,f} \in I'$, tehát $R_{g,f}(a_1, \ldots, a_{n-1}) = 0$. Ezzel szemben, ha az $R_{g,f}$ determináns M mátrixát nézzük, akkor (3.2) és (3.3) egyenlőségek miatt az $X_i = a_i$ helyettesítéssel M felső trianguláris mátrix lesz, melynek főátlójában m darab $g_0 \neq 0$ és d darab 1-es áll. Ebből $R_{g,f}(a_1, \ldots, a_{n-1}) = g_0^m \neq 0$ következik, ami ellentmondás. □

A gyenge zérushely tételből a Rabinowitsch-féle trükkel tudjuk egyszerűen levezetni az erős zérushely tételt. Ennek kimondásához előbb be kell vezetnünk a *gyökideál* fogalmát.

3.6.2. Definíció. Legyen R egységelemes kommutatív gyűrű és $I \triangleleft R$ ideál. Az I *gyökideálja* a

$$\sqrt{I} = \{a \in R \mid a^m \in I \text{ valamely } m \text{ természetes számra}\}$$

részhalmaz.

3.6.3. Állítás. Ha R egységelemes kommutatív gyűrű és $I \triangleleft R$, akkor $\sqrt{I} \triangleleft R$.

Bizonyítás. Nyilván $a^m \in I$ és $x \in R$ esetén $(ax)^m = a^m x^m \in I$, azaz a szívóhatás teljesül $\sqrt{I}$-re. Ha pedig $a^m, b^k \in I$, akkor minden $0 \leq i \leq m + k$ értékre $a^i \in I$ vagy $b^{m+k-i} \in I$, így a binomiális tétel miatt $(a \pm b)^{m+k} \in I$. Más szóval $\sqrt{I}$ additív részcsoport R-ben. □

3.6.4. Tétel (Erős Nullstellensatz)**.** Ha K algebrailag zárt és $I \triangleleft K[X_1, \ldots, X_n]$, akkor $\mathscr{I}(\mathscr{V}(I)) = \sqrt{I}$.

Bizonyítás. Nyilván $\sqrt{I} \subseteq \mathscr{I}(\mathscr{V}(I))$, úgyhogy csak a visszafele irányt kell megmutatni. A Hilbert-féle bázis tétel szerint I végesen generált. Tegyük fel, hogy $I = \langle g_1, \ldots, g_m \rangle$ és $f \in \mathscr{I}(\mathscr{V}(I))$. Legyen T új változó és vizsgáljuk a $J = \langle g_1, \ldots, g_m, Tf - 1 \rangle$ ideált a $K[X_1, \ldots, X_n, T]$ gyűrűben. Azt állítjuk, hogy $\mathscr{V}(J) = \emptyset$. Valóban, tegyük fel, hogy $(x_1, \ldots, x_n, t) \in K^{n+1}$ értékekre

$$g_1(x_1, \ldots, x_n) = \cdots = g_m(x_1, \ldots, x_n) = tf(x_1, \ldots, x_n) - 1 = 0.$$

Az első m egyenlőségből $\boldsymbol{x} \in \mathscr{V}(I)$ következik, míg az utolsóból $f(\boldsymbol{x}) \neq 0$, ami ellentmond az $f \in \mathscr{I}(\mathscr{V}(I))$ feltételnek.

A gyenge zérushely tétel szerint $\mathscr{V}(J) = \emptyset$ miatt $1 \in J$, azaz találunk olyan $h_0, h_1, \ldots, h_m \in K[X_1, \ldots, X_n, T]$ polinomokat, amikre

$$1 = g_1 h_1 + \cdots + g_m h_m + (Tf - 1)h_0. \tag{3.4}$$

Legyen N a legnagyobb hatvány, amivel T előfordul valamelyik h_i-ben. Ekkor $f^N h_i$ tekinthető $X_1, \ldots, X_n$ és fT polinomjának:

$$f(X_1, \ldots, X_n)^N h_i(X_1, \ldots, X_n, T) = H_i(X_1, \ldots, X_n, fT).$$

Átszorozva (3.4)-t f^N-el:

$$f^N = \sum_{i=1}^{m} g_i(X_1, \ldots, X_n) H_i(X_1, \ldots, X_n, fT) + (fT - 1) H_0(X_1, \ldots, X_n, fT).$$

A $T = 1/f$ helyettesítéssel adódik ebből, hogy

$$f^N = \sum_{i=1}^{m} g_i(X_1, \ldots, X_n) H_i(X_1, \ldots, X_n, 1) \in I,$$

azaz $f \in \sqrt{I}$ a tétel állításának megfelelően. □

3.6.1. Feladat. Határozzuk meg az alábbi U ponthalmazok $\mathscr{I}(U)$ eltűnési ideálját $K[X, Y]$-ban:

a) $U = \{(0,0)\}$

b) $U = \{(5,-3)\}$

c) $U = \{(-1,0),(2,0)\}$

d) $U = \{(-1,-1),(-1,1),(1,-1),(1,1)\}$

e) $U = \{(n,0) \mid n \in \mathbb{Z}\}$

3.6.2. Feladat. Legyen $U = \{(-1,0),(1,0),(1,1)\}$ és $J = \langle X^2 + Y^2 - 1, Y(Y-1)\rangle$.

a) Mutassuk meg, hogy $U = \mathscr{V}(J)$.

b) Mutassuk meg, hogy $(XY)^2 \in J$, de $XY \notin J$.

c) Határozzuk meg az $\mathscr{I}(U) = \mathscr{I}(\mathscr{V}(J)) = \sqrt{J}$ eltűnési ideált.

4. fejezet

Irreducibilis harmadrendű görbék

Bevezető

Ebben a részben K tetszőleges algebrailag zárt testet jelöl. Ha nem írjuk máshogyan expliciten, akkor a feladatokban feltesszük, hogy K karakterisztikája 0. A jelölésünkben $f, g, h, \cdots$ tetszőleges két változós $f(X,Y)$, $g(X,Y)$, $h(X,Y), \cdots$ polinomot, míg $F, G, H, \ldots$ ezek $F(X,Y,Z)$, $G(X,Y,Z)$, $H(X,Y,Z), \ldots$ homogenizáltját jelöli.

Algebrai görbe alatt valójában mindig projektív görbét fogunk érteni. Ez azt jelenti, hogy a $\Gamma : f(X,Y) = 0$ affin görbéhez is hozzávesszük a végtelen távoli egyenesre eső pontjait és nem teszünk különbséget az $f(X,Y) = 0$ és az $F(X,Y,Z) = 0$ görbék között.

4.1. Görbék metszete

4.1.1. A metszési multiplicitás

4.1.1. Tétel („kis Bézout-tétel”)**.** Legyenek Γ, Δ közös komponens nélküli n, illetve m-edfokú algebrai görbék. Ekkor $|\Gamma \cap \Delta| \leq nm$.

Bizonyítás. Tegyük fel, hogy $P_1, \ldots, P_{nm+1} \in \Gamma \cap \Delta$ különböző pontok. Vegyük fel úgy a homogén koordinátarendszert, hogy egyik görbe sem megy át az $E(1,0,0)$ ponton, minden $1 \leq i < j \leq nm+1$ esetén $P_i \notin \ell_\infty$ és $E \notin P_iP_j$. Ez azt jelenti, hogy $P_i = P_i(x_i, y_i, 1)$ és az $y_1, \ldots, y_{nm+1}$ értékek mind különbözőek. Másrészről az y_i gyöke az $R_{f,g}(Y)$ rezultáns polinomnak. Mivel $\deg(R_{f,g}(Y)) \leq nm$, ebből $R_{f,g}(Y) = 0$ következik, azaz van f-nek és g-nek Y-ban nem konstans $h(X,Y)$ közös tényezője. Speciálisan, Γ-nak és Δ-nak $h = 0$ közös komponense. □

4.1.2. Definíció. Legyenek Γ, Δ közös komponens nélküli algebrai görbék a komplex projektív síkon. Azt mondjuk, hogy Γ és Δ *megengedett helyzetben* van a projektív koordinátarendszerre nézve, ha

(a) egyik sem megy át az $E(1,0,0)$ ponton és

(b) semelyik két metszéspontjuk nem kollineáris E-vel.

4.1.1. Megjegyzés. (a) A kis Bézout-tétel miatt projektív lineáris transzformációval bármely két közös komponens nélküli görbe megengedett helyzetbe hozható. Itt lényeges, hogy a közös projektív pontjaik száma véges.

(b) Közönséges koordinátarendszerben az E az x-tengely végtelen távoli pontja.

(c) $E \notin \Gamma \cup \Delta$ azt jelenti, hogy a két görbe F, G polinomjai tartalmazzák az X^n, X^m monómokat.

(d) Ebből következik, hogy $\deg F = \deg_X F$ és $\deg G = \deg_X G$.

(e) Ezért az X szerinti $R_{F,G}(Y,Z)$ rezultáns nm-edfokú homogén polinom.

Legyenek $\Gamma : F = 0$, $\Delta : G = 0$ algebrai görbék megengedett helyzetben. Ekkor a rezultánsuk nm lineáris tényező szorzatára bomlik:

$$R_{F,G}(Y,Z) = \prod_{i=1}^{k} (w_i Y - v_i Z)^{s_i}, \qquad s_1 + \cdots + s_k = nm,$$

ahol a (v_i, w_i) „gyökök" nem egymás skalárszorosai. Mivel $R_{F,G}(v_i, w_i) = 0$, ezért $F(X, v_i, w_i)$ és $G(X, v_i, w_i)$ polinomoknak van u_i közös gyökük, ami a $P_i(u_i, v_i, w_i)$ metszéspontnak felel meg. Ha u_i' másik közös gyök lenne, akkor a $P_i(u_i, v_i, w_i)$ és $P_i'(u_i', v_i, w_i)$ metszéspontok kollineárisak lennének E-vel, ami nem lehet. Így tehát kölcsönösen egyértelműen megfeleltethetjük $R_{F,G}(Y,Z)$ „gyökeit" a két görbe metszéspontjaival.

4.1.3. Definíció (Metszési multiplicitás megengedett helyzetben)**.** Legyenek a Γ, Δ görbék megengedett helyzetben a fenti jelölésekkel. A két görbe P_i-beli *metszési multiplicitása* definíció szerint

$$i(\Gamma \cap \Delta; P_i) = s_i.$$

4.1.4. Tétel (A metszési multiplicitás projektív invarianciája)**.** Legyenek Γ, Δ közös komponens nélküli algebrai görbék, $P \in \Gamma \cap \Delta$ és φ projektív lineáris transzformáció. Legyen $\Gamma' = \varphi(\Gamma)$, $\Delta' = \varphi(\Delta)$ és $P' = \varphi(P)$. Tegyük fel, hogy Γ és Δ, illetve Γ' és Δ' megengedett helyzetben vannak. Ekkor $i(\Gamma \cap \Delta; P) = i(\Gamma' \cap \Delta'; P')$.

Bizonyítás. Nehéz, eltekintünk tőle. □

4.1.5. Definíció (Metszési multiplicitás általános fogalma)**.** Legyenek Γ, Δ közös komponens nélküli görbék és φ projektív lineáris transzformáció, melyre $\varphi(\Gamma)$ és $\varphi(\Delta)$ megengedett helyzetben lesznek. Ekkor a P pont esetén

$$i(\Gamma \cap \Delta; P) = i(\varphi(\Gamma), \varphi(\Delta); \varphi(P)).$$

4.1.2. Megjegyzés. (a) A projektív invariancia miatt $i(\Gamma \cap \Delta; P)$ nem függ φ választásától.

(b) $i(\Gamma \cap \Delta; P) = 0$ akkor és csak akkor, ha $P \notin \Gamma \cap \Delta$.

4.1.1. Feladat. Legyen $\Gamma : f(X,Y) = 0$ algebrai görbe, $\ell : Y = mX + b$ egyenes és $P = P(0,0)$. Mutassuk meg, hogy $i(\Gamma \cap \ell; P)$ pontosan a 0 gyök multiplicitása az $f(X, mX + b)$ polinomban. Más szóval, $i(\Gamma \cap \ell; P) = k$ akkor és csak akkor, ha $f(X, mX + b) = X^k(c + \cdots)$ valamilyen $c \neq 0$ konstanssal. [Útmutatás: Használjuk a rezultáns $R_{f,X-c} = \pm f(c)$ tualjdonságát.]

4.1.6. Állítás. Legyen Γ görbe, ℓ egyenes és P pont. Ha $i(\Gamma \cap \ell; P) = 1$, akkor P Γ sima pontja és ℓ különbözik a Γ P-beli érintőjétől.

Bizonyítás. Feltehetjük, hogy $P = P(0,0)$. Mivel $i(\Gamma \cap \ell; P) > 0$, $P \in \Gamma \cap \ell$, azaz $\ell : Y = mX$ és $\Gamma : 0 = f(X,Y) = a_{10}X + a_{01}Y + \cdots$. A 4.1.1 feladat szerint

$$f(X, mX) = (a_{10} + ma_{01})X + X^2(\cdots)$$

nem osztható X^2-el, vagyis $a_{10} + ma_{01} \neq 0$. Ez pontosan azt jelenti, hogy ℓ különbözik a Γ origóbeli $a_{10}X + a_{01}Y = 0$ érintőjétől. □

4.1.2. Bézout tétele

4.1.7. Tétel (Bézout tétele)**.** Legyenek Γ, Δ közös komponens nélküli n, illetve m-edfokú algebrai görbék a komplex projektív síkon. Ekkor metszési multiplicitással számolva a két görbének pontosan nm közös pontja van.

Bizonyítás. Triviális. □

4.1.2. Feladat. (a) Gondoljuk meg, hogy miért fontos az alaptest algebrai zártsága és miért a projektív síkon vizsgáljuk a görbék metszetét.

(b) Gondoljuk meg, hogy a Bézout-tétel

$$\sum_P i(\Gamma \cap \Delta; P) = \deg \Gamma \cdot \deg \Delta$$

alakban is kimondható, ahol a szummázás a sík összes pontjára történik.

4.1.8. Állítás. Egy n-edfokú irreducibilis görbének legfeljebb $n(n-1)$ szinguláris pontja van.

Bizonyítás. Legyen $\Gamma : f(X,Y) = 0$ irreducibilis n-edfokú görbe. Ekkor $\Delta = \frac{\partial f}{\partial X}(X,Y) = 0$ legfeljebb $n-1$ fokú és a szinguláris pontok $\Gamma \cap \Delta$-n vannak. Mivel Γ irreducibilis, így nincs közös komponens. □

A szinguláris pontokra vonatkozó korlát általában jelentősen csökkenthető. Számunkra a harmadfokú görbék esete lényeges.

4.1.9. Állítás. Egy harmadfokú irreducibilis görbének legfeljebb egy szinguláris pontja van.

Bizonyítás. Legyen Γ harmadfokú görbe aminek van két P, Q szinguláris pontja. Legyen $\ell = PQ$. A 4.1.6 állításból következik $i(\Gamma \cap \ell; P) \geq 2$ és $i(\Gamma \cap \ell; Q) \geq 2$. Ez azt jelenti, hogy Γ-nak és ℓ-nek multiplicitással számolva legalább 4 közös pontja van. A Bézout-tétel szerint ekkor van közös komponensük, ami ellentmond Γ irreducibilitásának. □

Vizsáljuk meg az irreducibilis harmadrendű görbe lehetséges szinguláris pontját. Felhetejük, hogy ez az origó. A görbe affin egyenlete ekkor

$$f(X,Y) = f_2(X,Y) + f_3(X,Y),$$

ahol f_d a d-edfokú homogén komponens. Ha $f_2 \equiv 0$, akkor f három homogén lineáris tényező szorzatára bomlik, ami ellentmond az irreducibilitásnak. Az $f_2(X,Y)$ másodfokú homogén rész két homogén lineáris tényező szorzatára bomlik:

$$f_2(X,Y) = (u_1X - v_1Y)(a_2X - v_2Y).$$

Ha a két tényező egymás skalárszorosa, azaz $f_2 = (uX - vY)^2$ teljes négyzet, akkor a szingularitást *"csőr" típusúnak* mondjuk. Ha f_2 tényezői lineárisan függetlenek, akkor *közönséges szingularitásról beszélünk.* Az $u_iX - y_iY = 0$ (nem feltétlenül különböző) egyeneseket ($i = 1, 2$) a szinguláris ponthoz húzott *érintőknek* nevezzük. Meggondolhatjuk, hogy a szinguláris pontban az érintőnek nevezett egyenes metszési multiplicitása legalább 3.

4.2. Harmadrendű görbék

4.2.1. Inflexiós pontok

4.2.1. Definíció. A Γ görbe P sima pontját *inflexiós pontnak* nevezzük, ha a P-beli t érintőre $i(\Gamma \cap t; P) \geq 3$.

4.2.1. Feladat. Mutassuk meg, hogy ha $f(X) \in K[X]$ és $\Gamma : Y = f(X)$, akkor az $(x, f(x))$ pont akkor és csak akkor inflexiós, ha $f''(x) = 0$.

4.2.2. Feladat. Határozza meg az $Y = X^3$, $Y^2 = X^3$ és $Y^2 = X^3 + X^2$ görbék szinguláris és inflexiós pontjait a projektív síkon.

4.2.2. Állítás. Tegyük fel, hogy $\mathrm{char}(K) \neq 2, 3$. Legyen Γ irreducibilis harmadrendű görbe, melynek az y-tengely végtelen távoli pontjában szinguláris pontja van, és itt a végtelen távoli egyenes érinti. Mutassuk meg, hogy Γ egyenlete

$$Y = u(X), \qquad \text{vagy} \qquad Y = \frac{u(X)}{X - \alpha} \qquad (\deg(u) = 3)$$

attól függően, hogy a szinguláris pont „csőr" típusú vagy közönséges.

Bizonyítás. Válasszuk meg úgy a homogén koordinátarendszert, hogy az y-tengely $U(0,1,0)$ végtelen távoli pontja a görbe szinguláris pontja, és az $\ell_\infty : Z = 0$ végtelen távoli egyenes érintő. Tekintsük a harmedrendű görbe általános homogén egyenletét:

$$F(X,Y,Z) = a_{30}X^3 + a_{21}X^2Y + a_{12}XY^2 + a_{03}Y^3 + \\ a_{20}X^2Z + a_{11}XYZ + a_{02}Y^2Z + a_{10}XZ^2 + a_{01}YZ^2 + a_{00}Z^3 = 0$$

Ekkor $F(X,Y,0)$ lineáris tényezők szorzatára bomlik. A korábban látott $i(\Gamma \cap \ell_\infty; U) \geq 3$ tulajdonság miatt $F(X,Y,0) = (uX - vY)^3$ teljes köb. Mivel $F(0,1,0) = 0$, így $F(X,Y,0) = a_{30}X^3$ és $a_{21} = a_{12} = 0$. Feltehető $a_{30} = 1$, azaz

$$F(X,Y,Z) = X^3 + a_{20}X^2Z + a_{11}XYZ + a_{10}XZ^2 + a_{01}YZ^2 + a_{00}Z^3 = 0.$$

A $Z = 1$ helyettesítéssel és átrendezve az affin egyenletre adódik

$$Y(a_{11}X + a_{01}) = u_1(X),$$

ahol $u_1(X)$ harmadfokú polinom X-ben. Ha $a_{11} = a_{01} = 0$, akkor Γ három egyenes uniója, ami ellentmond Γ irreducibilitásának. Ha $a_{11} = 0$, akkor Γ egyenlet $Y = u(X)$, ha $a_{11} \neq 0$, akkor $Y = u(X)/(X - \alpha)$ alakra hozható, ahol $u(X)$ az $u_1(X)$ skalárszorosa. Közvetlen számolással adódik a két esetben a szingularitás típusa. □

4.2.3. Feladat. Legyen Γ szinguláris ponttal rendelkező irreducibilis harmadrendű görbe. Mutassuk meg, hogy Γ-nak 3 vagy 1 inflexiós pontja van, attól függően, hogy a szinguláris pontja „csőr" típusú vagy közönséges. [Útmutatás: Tekintsük Γ-t $Y = u(X)$ vagy $Y = X^2 + u_1X + u_2 + u_3/X$ alakban.]

4.2.2. A 9–pont-tétel

4.2.4. Feladat. Mutassuk meg, hogy az általános n-edfokú 3-változós homogén polinom együtthatóinak száma $\binom{n+1}{2}$. [Útmutatás: Számoljuk meg azon (i,j) párokat, melyekre $i,j \geq 0$ egészek és $i + j \leq n$.]

4.2.3. Állítás. Legyen n pozitív egész, $N = \frac{n(n+1)}{2} - 1$ és $P_1, \ldots, P_N$ projektív pontok. Ekkor létezik egy Γ n-edfokú görbe, ami átmegy a $P_1, \ldots, P_N$ pontokon.

Bizonyítás. A 4.2.4 feladat szerint a keresett $F(X,Y,Z)$ n-edfokú homogén polinomnak $N+1$ együtthatója van. Ha $x,y,z \in K$, akkor az $F(x,y,z) = 0$ feltétel egy homogén lineáris egyenletet jelent F együtthatóira. Az adott N pont egy N egyenletből álló, $N+1$ ismeretlenes homogén lineáris egyenletrendszert határoz meg. Ennek bármely nemtriviális megoldása egy olyan F polinomot ad meg, melynek $\Gamma : F = 0$ görbéje tartalmazza a $P_1, \ldots, P_N$ pontokat. □

Legyenek $\Gamma : F = 0$, $\Delta : G = 0$ algebrai görbék. A Γ és Δ által *kifeszített görbesor* elemei az $\alpha F + \beta G = 0$ egyenletű görbék, ahol $\alpha, \beta \in K$ konstansok, $(\alpha, \beta) \neq (0,0)$.

4.2.5. Feladat. A Γ és Δ által kifeszített görbesor bármely eleme tartalmazza Γ és Δ közös pontjait.

4.2.4. Tétel (9–pont-tétel)**.** Legyen $r_0, r_1, r_2, s_0, s_1, s_2$ hat különböző egyenes. Definiáljuk a $P_{ij} = r_i \cap s_j$ pontokat, $i,j \in \{0,1,2\}$. Tegyük fel, hogy a kilenc P_{ij} pont mind különböző. Ekkor bármely olyan harmadrendű görbe, amely átmegy a kilenc pont közül nyolcon, átmegy a kilencediken is.

Bizonyítás. Tegyük fel, hogy Γ harmadrendű és átmegy nyolc ponton a kilencből. Az egyenesek átszámozásával elérhetjük, hogy a hiányzó kilencedik pont a P_{22}. Először tegyük fel, hogy r_0 komponense Γ-nak. Ekkor $\Gamma = r_0 \cup C$, ahol C egy (esetleg reducibilis) másodrendű görbe. Mivel $P_{10}, P_{11}, P_{12} \in C$, a Bézout-tétel miatt r_1 komponense C-nek: $C = r_1 \cup \ell$ egy ℓ egyenesre. A feltétel szerint $P_{20}, P_{21} \in \ell$, tehát $\ell = r_2$. Ez azt jelenti, hogy $\Gamma = r_0 \cup r_1 \cup r_2$, vagyis $P22 \in \Gamma$.

Tegyük most fel, hogy r_0 nem komponense Γ-nak és rögzítsünk egy $Q \in r_0 \setminus \Gamma$ pontot. Ilyenkor nyilván $Q \notin s_0 \cup s_1 \cup s_2$. Legyenek F, S_0, S_1, S_2 a Γ-t illetve az s_0, s_1, s_2 egyeneseket meghatározó polinomok. Az elmondottak szerint

$$F(Q), S_0(Q), S_1(Q), S_2(Q) \neq 0,$$

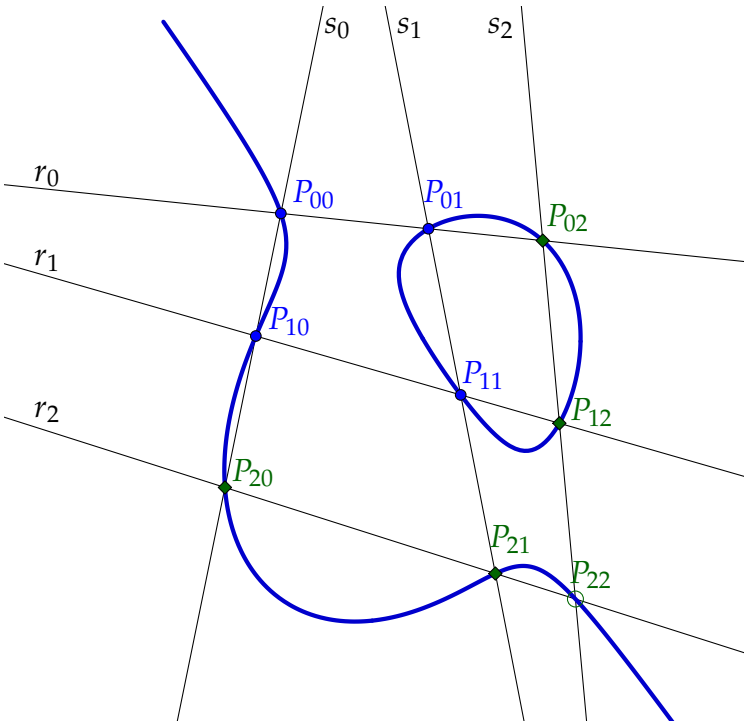
így valamely $\alpha \in K$ nem nulla konstansra

$$F(Q) - \alpha S_0(Q)S_1(Q)S_2(Q) = 0.$$

Legyen Δ az $F - \alpha S_0S_1S_2 = 0$ elem a Γ és az $s_0 \cup s_1 \cup s_2$ görbék által kifeszített görbesorban. Egyrészt Δ harmadfokú és átmegy azon a nyolc ponton, amin Γ. Másrészt $|\Delta \cap r_0| \geq 4$, tehát Δ-nak komponense r_0. A korábban vizsgált esetben már láttuk, hogy ebből következik $\Delta = r_0 \cup r_1 \cup r_2$, azaz $P_{22} \in \Delta$. Ebből adódik

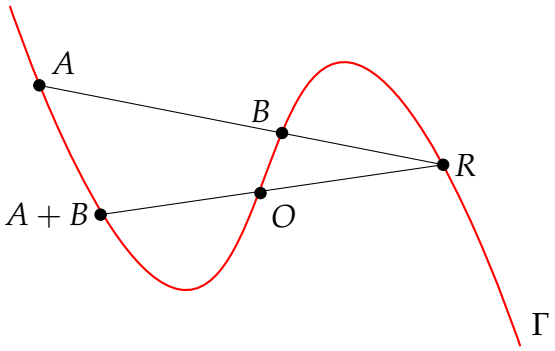
$$0 = F(P_{22}) - \alpha S_0(P_{22})S_1(P_{22})S_2(P_{22}) = F(P_{22}),$$

vagyis $P_{22} \in \Gamma$. □



4.2.3. Összeadás a harmadrendű görbén

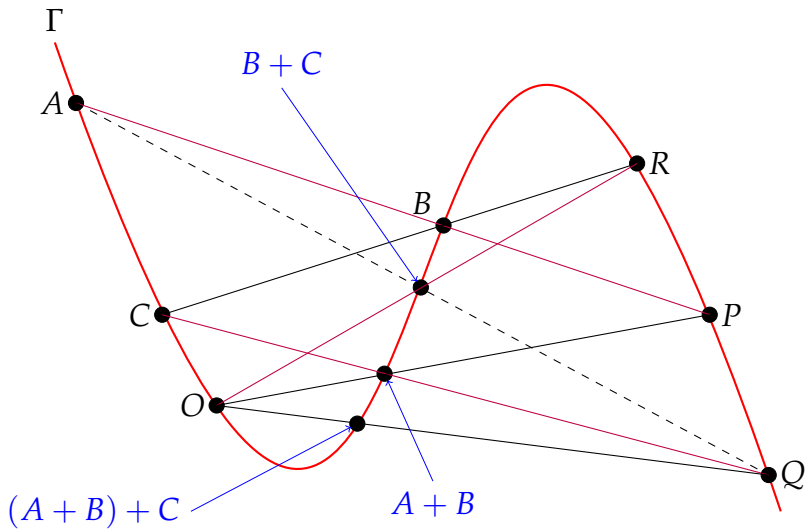
4.2.5. Definíció (Összeadás a harmadrendű görbén)**.** Legyen Γ irreducibilis harmadrendű görbe és jelölje Γ^* a sima pontok halmazát. Rögzítsük az $O \in \Gamma^*$ pontot. Adott $A, B \in \Gamma^*$ pontok $A + B$ összegét az alábbi ábra szerint értelmezzük.



Itt az $R \in \Gamma$ pontot az AB szelő „harmadik metszéspontjának" nevezzük. Arról van ugyanis szó, hogy a Bézout-tétel szerint multiplicitással számolva minden egyenes három pontban metszi Γ-t. Ha $A, B \in \Gamma$, akkor az AB szelőn két metszéspont adott, és a metszési multiplicitást is figyelembe véve kell lennie egy harmadik metszéspontnak. Elképzelhető, hogy $A = R$, amennyiben az AB szelő érinti Γ-t A-ban. Ha pedig $A = B$, akkor az AB szelő alatt a Γ A-beli érintőjét értjük.

4.2.6. Feladat. Gondoljuk meg, hogy az imént művelet jól definiált, invertálható, és teljesülnek $O + A = A$ és $A + B = B + A$.

Az $A + B$ művelet asszociativitása közel sem triviális, az alfejezet hátralévő részében ezzel foglalkozunk.



Vegyük fel Γ-n az O, A, B, C pontokat és szerkesszük meg a P, Q, R és $A + B$, $B + C$, $(A + B) + C$ pontokat az ábrán látható módon. Az

$$(A + B) + C = A + (B + C)$$

azonosság azzal ekvivalens, hogy az $A, B + C, Q$ pontok kollineárisak, vagy más szóval, hogy az $O(B + C)R$ egyenes és az AQ egyenes a Γ-n metszik egymást. Megmutatjuk, hogy ez következik a 9–pont-tételből abban az esetben, ha az ábrán

szereplő összes görbepont különböző. Az általános esetet nem bizonyítjuk, de megjegyezzük, hogy a $K = \mathbb{C}$ esetben folytonossági megfontolásokkal viszonylag egyszerűen belátható.

Legyen

$$\begin{aligned} r_0 &= ABP, & r_1 &= C(A+B)Q, & r_2 &= O(B+C)R, \\ s_0 &= CBR, & s_1 &= O(A+B)P, & s_2 &= AQ \end{aligned}$$

hat egyenes, ezek $r_i \cap s_j$ metszéspontjai $O, A, B, C, P, Q, R, A+B, (A+B)+C$, valamint $r_2 \cap s_2$. Tudjuk, hogy Γ tartalmazza az első nyolc pontot, így a 9–pont-tétel miatt tartalmazza $r_2 \cap s_2$-t is. Ezzel beláttuk (kicsit hiányosan) a következő tételt:

4.2.6. Tétel (Lamé tétele)**.** Legyen K tetszőleges test, Γ irreducibilis harmadrendű algebrai görbe a K feletti projektív síkon. Jelölje Γ^* a sima pontok halmazát és legyen $O \in \Gamma^*$. A korábban definiált művelettel $(\Gamma^*, +, O)$ Abel-csoport. □

Majd látni fogjuk, hogy a harmadrendű görbék inflexiós pontjai kiemelt szerepet játszanak a görbék geometriájának megértésében.

4.2.7. Feladat. (a) Legyen $\Gamma : Y = X^3$ és $O = (0,0)$. Mutassa meg, hogy $(\Gamma^*, +, O) \cong (K, +)$.

(b) Legyen $\Gamma : Y^2 = X^3 + X^2$ és $O = (0:1:0)$. Mutassa meg, hogy $(\Gamma^*, +, O) \cong (K^*, \cdot)$.

4.2.8. Feladat. Jelöljön Γ irreducibilis harmadrendű görbét.

(a) Tegyük fel, hogy $O \in \Gamma$ inflexiós pont. Mutassa meg, hogy $A, B, C \in \Gamma^*$ akkor és csak akkor kollineárisak, ha $A + B + C = O$.

(b) Tegyük fel, hogy $O \in \Gamma$ inflexiós pont. Mutassa meg, hogy $A \in \Gamma$ akkor és csak akkor inflexiós pont, ha $3A = O$.

(c) Mutassa meg, hogy ha az ℓ egyenes átmegy Γ két inflexiós pontján, akkor átmegy egy harmadikon is.

4.2.4. A Hesse-féle görbe

4.2.9. Feladat. Legyen $A = (a_{ij})$ 3×3-as mátrix, $F(X_1, X_2, X_3)$, $G(X_1, X_2, X_3)$ polinomok, melyekre $G(X_1, X_2, X_3) = F(a_{11}X_1 + \cdots, a_{21}X_1 + \cdots, a_{31}X_1 + \cdots)$. Ekkor minden $m \geq 0$ egészre és $j_1, \ldots, j_m \in \{1, 2, 3\}$ indexre teljesül

$$\frac{\partial^m G}{\partial X_{j_1} \cdots \partial X_{j_m}} = \sum_{k_1, \ldots, k_m = 1}^{3} a_{k_1 j_1} \cdots a_{k_m j_m} \frac{\partial^m F}{\partial X_{k_1} \cdots \partial X_{k_m}}.$$

[*Útmutatás:* Teljes indukció m-re. Az $m = 0$ eset triviális. Az $m = 1$ eset az érdekes.]

Megjegyezzük, hogy a fenti feltétel F-re és G a korábbi jelölésünkkel $G(\boldsymbol{X}) = F(A\boldsymbol{X})$, vagy $\alpha^* G = F$.

4.2.7. Lemma. Legyen $A = (a_{ij})$ 3×3-as mátrix, $F(X_1, X_2, X_3)$, $G(X_1, X_2, X_3)$ polinomok, melyekre $G(X_1, X_2, X_3) = F(a_{11}X_1 + \cdots, a_{21}X_1 + \cdots, a_{31}X_1 + \cdots)$. Ekkor

$$\begin{pmatrix} \frac{\partial^2 G}{\partial X_1^2} & \frac{\partial^2 G}{\partial X_1 \partial X_2} & \frac{\partial^2 G}{\partial X_1 \partial X_3} \\ \frac{\partial^2 G}{\partial X_1 \partial X_2} & \frac{\partial^2 G}{\partial X_2^2} & \frac{\partial^2 G}{\partial X_2 \partial X_3} \\ \frac{\partial^2 G}{\partial X_1 \partial X_3} & \frac{\partial^2 G}{\partial X_2 \partial X_3} & \frac{\partial^2 G}{\partial X_3^2} \end{pmatrix} = A^T \begin{pmatrix} \frac{\partial^2 F}{\partial X_1^2} & \frac{\partial^2 F}{\partial X_1 \partial X_2} & \frac{\partial^2 F}{\partial X_1 \partial X_3} \\ \frac{\partial^2 F}{\partial X_1 \partial X_2} & \frac{\partial^2 F}{\partial X_2^2} & \frac{\partial^2 F}{\partial X_2 \partial X_3} \\ \frac{\partial^2 F}{\partial X_1 \partial X_3} & \frac{\partial^2 F}{\partial X_2 \partial X_3} & \frac{\partial^2 F}{\partial X_3^2} \end{pmatrix} A,$$

ahol a bal oldalba $\boldsymbol{X}$-et, a jobb oldalba pedig $A\boldsymbol{X}$-et kell behelyettesíteni. (A^T pedig az A mátrix transzponáltját jelöli.) □

4.2.8. Definíció (Hesse-féle polinom)**.** A

$$H_F = H_F(X, Y, Z) = \det \begin{pmatrix} \frac{\partial^2 F}{\partial X^2} & \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial X \partial Z} \\ \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial Y^2} & \frac{\partial^2 F}{\partial Y \partial Z} \\ \frac{\partial^2 F}{\partial X \partial Z} & \frac{\partial^2 F}{\partial Y \partial Z} & \frac{\partial^2 F}{\partial Z^2} \end{pmatrix}$$

polinomot az $F(X, Y, Z)$ homogén polinom Hesse-féle polinomjának nevezzük.

4.2.9. Állítás. (i) Ha F homogén n-edfokú, akkor H_F homogén $3(n-2)$-edfokú polinom.

(ii) Ha $A = (a_{ij})$, $G(X_1, X_2, X_3) = F(a_{11}X_1 + \cdots, a_{21}X_1 + \cdots, a_{31}X_1 + \cdots)$, akkor

$$H_G(X_1, X_2, X_3) = \det(A)^2 H_F(a_{11}X_1 + \cdots, a_{21}X_1 + \cdots, a_{31}X_1 + \cdots).$$

Bizonyítás. Az egyetlen nehézség $H_F \not\equiv 0$; csak a $\deg F = 3$ esetre látjuk majd be. □

4.2.10. Definíció (A Hesse-féle görbe)**.** A $\Gamma : F = 0$ algebrai görbe Hesse-féle görbéje $H_F = 0$.

4.2.11. Állítás. A Hesse-görbe projektív invariáns, azaz Γ projektív képének a Hesse-görbéje a $H_F = 0$ Hesse-görbe projektív képe.

Bizonyítás. Legyen $\varphi_A : \boldsymbol{x} \mapsto A\boldsymbol{x}$ projektív lineáris transzformáció és $\Gamma : G = 0$. Ekkor $\varphi_A(\Gamma)$ egyenlete $F = \varphi_A^* G = 0$, ahol $F(\boldsymbol{X}) = (\varphi_A^* G)(\boldsymbol{X}) = G(A^{-1}\boldsymbol{X})$.

$$\begin{aligned} (\varphi_A^* H_G)(\boldsymbol{X}) &= H_G(A^{-1}\boldsymbol{X}) \\ &= \det(A)^2 \cdot H_F(\boldsymbol{X}) \\ &= \det(A)^2 \cdot H_{\varphi_A^* G}(\boldsymbol{X}). \end{aligned}$$

Ez a számolás mutatja, hogy a $\varphi_A^* H_G$ és a $H_{\varphi_A^* G}$ polinomok csak egy konstans szorzóban különböznek. Míg $\varphi_A^* H_G = 0$ a Γ Hesse-görbéjének a képe, addig $H_{\varphi_A^* G} = 0$ a Γ képének a Hesse-görbéje. □

A Hesse-polinom mátrixa első két oszlopának X, Y-szorosát a harmadik oszlop Z-szereséhez adva:

$$ZH_F = \det \begin{pmatrix} \frac{\partial^2 F}{\partial X^2} & \frac{\partial^2 F}{\partial X \partial Y} & (n-1)\frac{\partial F}{\partial X} \\ \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial Y^2} & (n-1)\frac{\partial F}{\partial Y} \\ \frac{\partial^2 F}{\partial X \partial Z} & \frac{\partial^2 F}{\partial Y \partial Z} & (n-1)\frac{\partial F}{\partial Z} \end{pmatrix}.$$

Hasonlóan, az utóbbi mátrix első két sorának X, Y-szorosát a harmadik sor Z-szereséhez adva:

$$Z^2 H_F = \det \begin{pmatrix} \frac{\partial^2 F}{\partial X^2} & \frac{\partial^2 F}{\partial X Y} & (n-1)\frac{\partial F}{\partial X} \\ \frac{\partial^2 F}{\partial X Y} & \frac{\partial^2 F}{\partial Y^2} & (n-1)\frac{\partial F}{\partial Y} \\ (n-1)\frac{\partial F}{\partial X} & (n-1)\frac{\partial F}{\partial Y} & n(n-1)F \end{pmatrix}.$$

Most áttérve az $f(X, Y) = F(X, Y, 1)$ inhomogén polinomra és átrendezve a determináns sorait és oszlopait kapjuk a Hesse-polinom inhomogén alakját:

$$H_f = H_f(X, Y) = \det \begin{pmatrix} n(n-1)f & (n-1)\frac{\partial f}{\partial X} & (n-1)\frac{\partial f}{\partial Y} \\ (n-1)\frac{\partial f}{\partial X} & \frac{\partial f}{\partial X^2} & \frac{\partial f}{\partial X Y} \\ (n-1)\frac{\partial f}{\partial Y} & \frac{\partial f}{\partial X Y} & \frac{\partial f}{\partial Y^2} \end{pmatrix}.$$

4.2.12. Állítás. Amennyiben Γ az $f = 0$ affin alakban van megadva, úgy a Hesse-görbe egyenlete $H_f = 0$.

Bizonyítás. Csakugyan, $H_f(X, Y) = H_F(X, Y, 1)$. □

4.2.13. Tétel (Inflexiós pontok és a Hesse-görbe kapcsolata)**.** A $\Gamma : F = 0$ görbe P sima pontja akkor és csak akkor inflexiós pont, ha rajta van a $H_F = 0$ Hesse-görbén.

Bizonyítás. A projektív invariancia miatt $P(0, 0)$ feltehető $Y = 0$ **érintővel.** Ekkor $f(X, Y) = Y + aX^2 + bXY + cY^2 + \cdots$ és P inflexiós $\Leftrightarrow$ $a = 0$. Másrészt $H_f(0, 0) = \det \begin{pmatrix} 0 & 0 & (n-1) \\ 0 & 2a & b \\ (n-1) & b & 2c \end{pmatrix} = -2(n-1)^2 a$. □

A Hesse-görbét **Otto Hesse** (1811-1874) német matematikusról nevezték el. (Nem összetévesztendő **Helmut Hasse** (1898-1979) német matematikussal, aki szintén fontos eredményeket ért el az algebrai görbék elméletében.)

4.2.5. Harmadrendű görbe normálalakja

4.2.14. Tétel. Irreducibilis harmadrendű görbének van inflexiós pontja.

Bizonyítás. Már láttuk azt az esetet, ha van szinguláris pont. Ha nincs, akkor tetszőleges metszéspont a Hesse-görbével inflexiós. □

4.2.10. Feladat. Legyen Γ irreducibilis harmadrendű görbe.

(a) Mutassuk meg, hogy ha az y-tengely végtelen távoli pontja Γ inflexiós pontja és a végtelen távoli egyenes érintője, akkor Γ egyenlete $Y^2 + \alpha XY + \beta Y = u(X)$ alakú, ahol $\deg(u) = 3$.

(b) Mutassuk meg, hogy a projektív koordinátarendszer megfelelő megválasztásával Γ egyenlete $Y^2 = u(X)$ alakra hozható, ahol $\deg(u) = 3$.

(c) Mutassuk meg, hogy az $Y^2 = u(X)$ görbének akkor és csak akkor van szinguláris pontja, ha u-nak van többszörös gyöke.

4.2.15. Tétel. A projektív koordinátarendszer megfelelő megválasztásával a Γ irreducibilis harmadrendű görbe egyenlete az alábbi alakok egyikére hozható:

(i) $Y^2 = X^3$ és Γ-nak „fordulópont" típusú szingularitása van.

(ii) $Y^2 = X^3 + X^2$ és Γ-nak közönséges szingularitása van.

(iii) $Y^2 = X(X-1)(X-c)$, ahol $c \in \mathbb{K} \setminus \{0,1\}$. Ekkor Γ-nak nincs szinguláris pontja.

Bizonyítás. Legyen $\Gamma : Y^2 = u(X) = \gamma(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$ és alkalmazzuk az

$$\begin{cases} X' = \frac{1}{\alpha_2-\alpha_1}X - \frac{\alpha_1}{\alpha_2-\alpha_1}, \\ Y' = \frac{1}{\sqrt{\gamma(\alpha_2-\alpha_1)^3}}Y, \end{cases} \qquad \begin{cases} X = (\alpha_2-\alpha_1)X' + \alpha_1, \\ Y = \sqrt{\gamma(\alpha_2-\alpha_1)^3}Y' \end{cases}$$

affin transzformációt. Ekkor $Y^2 = \gamma(\alpha_2-\alpha_1)^3(Y')^2$ és

$$u(X) = u((\alpha_2-\alpha_1)X' + \alpha_1) = \gamma(\alpha_2-\alpha_1)^3 X'(X'-1)(X'-c),$$

amiből adódik $(Y')^2 = X'(X'-1)(X'-c)$. □

4.2.16. Tétel (Weierstrass-féle normálalak)**.** Legyen K algebrailag zárt test, $\operatorname{char} K \neq 2, 3$. Ekkor a projektív koordinátarendszer megfelelő megválasztásával bármely sima harmadrendű görbe egyenlete

$$Y^2 = X^3 + aX + b$$

alakra hozható, ahol $4a^3 + 27b^2 \neq 0$. Ezt az egyenletet a görbe *Weierstrass-féle normálalakjának* nevezzük.

Bizonyítás. Az $Y^2 = u_0X^3 + u_1X^2 + u_2X + u_3$ alakból $X' = X - \frac{u_1}{3u_0}$, $Y' = Y$ transzformációval az X^2 tagot eliminálјuk, majd $X'' = u_0^{-1}X'$, $Y'' = u_0^{-1}Y'$ helyettesítéssel a kívánt $Y^2 = X^3 + aX + b$ alakra hozzuk. Az $u(X) = X^3 + aX + b$ és $u'(X) = 3X^2 + a$ polinomok rezultánsa $4a^3 + 27b^2$, azaz $4a^3 + 27b^2 = 0$ akkor és csak akkor, ha $u(X)$-nek van többszörös gyöke. Tehát a $4a^3 + 27b^2 \neq 0$ feltétel garantálja, hogy a görbének ne legyen szinguláris pontja. □

4.2.17. Tétel. Algebrailag zárt test felett a sima harmadrendű görbének pontosan 9 inflexiós pontja van.

Bizonyítás. Legyen Γ sima harmadrendű görbe és Δ a Hesse-görbéje. A Bézout-tétel szerint $\Gamma \cap \Delta$ nem üres. Elegendő megmutatni, hogy bármely P inflexiós pontban a metszési multiplicitás $i(\Gamma \cap \Delta; P) = 1$. Feltehető, hogy $P = (0,1,0)$ és $\Gamma : Y^2 = X^3 + X + b$ Weierstrass-féle normál alakban van megadva. Közvetlen számolással adódik, hogy a Hesse-görbe egyenlete

$$\Delta : H_f = 8(3XY^2 + 3aX^2 + 9bX - a^2) = 0,$$

és a metszési multiplicitás $(0,1,0)$-ban egyszeres. □

4.2.11. Feladat. Legyen ε harmadik egységgyök, azaz $\varepsilon^2 + \varepsilon + 1 = 0$. Mutassuk meg, hogy tetszőleges $\alpha^3 \neq 27$ esetén a $\Gamma : X^3 + Y^3 + Z^3 - \alpha XYZ = 0$ görbe inflexiós pontjai

$$\begin{array}{lll} P_{00} = (0,1,-1), & P_{01} = (1,0,-1), & P_{02} = (1,-1,0), \\ P_{10} = (0,1,-\varepsilon), & P_{11} = (1,0,-\varepsilon^2), & P_{12} = (1,-\varepsilon,0), \\ P_{20} = (0,1,-\varepsilon^2), & P_{21} = (1,0,-\varepsilon), & P_{22} = (1,-\varepsilon^2,0). \end{array}$$

5. fejezet

Feladatok

5.1. Feladatok az 1. zh-ra

5.1.1. Feladat. Oldjuk meg az alábbi feladatokat:

a) Számológép használata nélkül számoljuk ki az alábbiakat: $\gcd(60, 32)$, $\gcd(3, 2)$, $\gcd(3, 1)$, $\gcd(3, 0)$, $\gcd(0, 0)$, $\gcd(199\,411\,161\,721, 366\,124\,068\,217)$.

b) Ossza el maradékosan az $f = 2x^5 - 4x^3 + 2x^2 - x + 2$ polinomot a $g = x^2 + x + 1$ polinommal.

c) Legyen $f = x^6 - 1$, $g = x^4 + 2x^3 + 2x^2 - 2x - 3$. Adja meg az $I = \langle f, g \rangle$ ideál egy generátorelemét. Teljesül $x^5 + x^3 + x^2 - 7 \in I$? Mutassa meg, hogy $h = x^4 + 2x^2 - 3 \in I$ és írja fel h-t az f és g lineáris kombinációjaként.

d) Számolja ki az

$$\begin{aligned} f_1 &= x^5 - 2x^4 - x^2 + 2x, \\ f_2 &= x^7 + x^6 - 2x^4 - 2x^3 + x + 1, \\ f_3 &= x^6 - 2x^5 + x^4 - 2x^3 + x^2 - 2x \end{aligned}$$

polinomok legnagyobb közös osztóját.

e) Legyen K test. Mutassa meg, hogy a $K[X, Y]$ gyűrű $\langle X, Y \rangle$ ideálja nem generálható egyetlen elemmel. (Tehát $K[X, Y]$ nem *főideálgyűrű*.)

f) Legyen K test, $c \in K$, $f \in K[X_1, \ldots, X_n]$. Mutassuk meg, hogy $X_n - c$ akkor és csak akkor osztja f-et, ha $f(X_1, \ldots, X_{n-1}, c)$ a nulla polinom.

5.1.2. Feladat. Legyen $f(X) = X^3 + aX + b$. Mutassuk meg, hogy $R_{f,f'} = 4a^3 + 27b^2$.

5.1.3. Feladat. Legyen

$$\begin{aligned} f &= X^2Y - 3XY^2 + X^2 - 3XY, \\ g &= X^3Y + X^3 - 4Y^2 - 3Y + 1. \end{aligned}$$

a) Számolja ki $R_{f,g}(Y)$-t.

b) Számolja ki $R_{f,g}(X)$-et. Mit mond az eredmény f-ről és g-ről?

5.1.4. Feladat. Legyen $f(Y) = a_0Y^m + a_1Y^{m-1} + \cdots + a_m$ és $g(Y) = Y - b$. Mutassuk meg, hogy ekkor $R_{f,g} = \pm f(b)$.

5.1.5. Feladat. A rezultáns segítségével keressük meg az alábbi paraméterezésben megadott görbék $f(X, Y)$ polinomját:

$$\begin{aligned} &(a) \quad x(t) = t^4, && y(t) = t + t^2, \\ &(b) \quad x(t) = t^2 + t^3, && y(t) = t^4, \\ &(c) \quad x(t) = \frac{t^2}{1+t^2}, && y(t) = \frac{t^3}{1+t^2}. \end{aligned}$$

[*Útmutatás:* Tekintsük az $f(X, Y, t) = X - x(t)$, $g(X, Y, t) = Y - y(t)$ polinomokat és a rezultáns segítségével küszöböljük ki a t ismeretlent.]

5.1.6. Feladat. a) A triviális ideálok főideálok.

b) Az A gyűrű akkor és csak akkor test, ha csak triviális ideáljai vannak.

c) Tetszőleges $n \in \mathbb{Z}$ esetén $\langle n \rangle = n\mathbb{Z} \lhd \mathbb{Z}$ főideál; $\mathbb{Z}/n\mathbb{Z}$ a modulo n maradékosztályok gyűrűje.

d) A $K[X, Y]$ polinomgyűrűben az $I = \langle X, Y \rangle$ ideál a nulla konstanstagú polinomokból áll. I végesen generált, de nem főideál.

e) A $K[X_1, X_2, \ldots]$ végtelen változós polinomgyűrűben az $I = \langle X_1, X_2, \ldots \rangle$ ideál a nulla konstanstagú polinomokból áll; I nem végesen generált.

f) $\mathbb{Z}$ és $K[X]$ főideálgyűrűk.

5.1.7. Feladat. Legyen K nulla karakterisztikájú test.

a) Legyenek $f_1, \ldots, f_s, g_1, \ldots, g_t \in K[X_1, \ldots, X_n]$. Ha $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, akkor $\mathcal{V}(f_1, \ldots, f_s) = \mathcal{V}(g_1, \ldots, g_t)$.

b) $\langle X + Y, X - Y \rangle = \langle X, Y \rangle$.

c) $\langle X + XY, Y + XY, X^2, Y^2 \rangle = \langle X, Y \rangle$.

d) $\langle 2X^2 + 3Y^2 - 11, X^2 - Y^2 - 3 \rangle = \langle X^2 - 4, Y^2 - 1 \rangle$.

e) $\mathcal{I}(\mathcal{V}(X^n, Y^m)) = \langle X, Y \rangle$.

5.1.8. Feladat. Legyen K nulla karakterisztikájú test.

a) Határozzuk meg azt az affin transzformációt, ami az $5X - 3Y + 1$ egyenest az $Y = 0$ egyenesbe viszi.

b) Határozzuk meg azt az eltolást, mely a $K : X^2 + Y^2 + 4X + Y - 1 = 0$ másodrendű görbéből eliminálja az X-es és Y-os tagok együtthatóit.

c) Határozzuk meg azt az eltolást, mely a $K : X^2 - X + 4Y - 1 = 0$ másodrendű görbéből eliminálja az X-es tag együtthatóját és a konstanst.

d) Határozzuk meg annak az origó körüli forgatásnak az α szögét, mely a $K : X^2 - XY + 3Y^2 + 4X - 2Y = 0$ másodrendű görbéből eliminálja az XY-os tag együtthatóját.

e) Határozzunk meg egy olyan affin transzformációt, amely az alábbi másodrendű görbéket affin kanonikus alakba viszi.

(1) $K : X^2 - 2XY - 8Y^2 + 18Y = 0$,

(2) $K : X^2 + 4XY + 4Y^2 - 2X - 8Y + 5 = 0$,

(3) $K : 9X^2 + 36Y^2 - 12X - 24Y + 4 = 0$.

f) Határozzuk meg a $K : 3X^2 + 10XY + 3Y^2 + 10X + 14Y + 8 = 0$ elfajuló másodrendű görbe affin kanonikus alakját.

5.1.9. Feladat. Tegyük fel, hogy $\mathrm{char}(K) \neq 2, 3$ és $a_{02} \neq 0$. Mutassuk meg, hogy az

$$X^3 + a_{20}X^2 + a_{11}XY + a_{02}Y^2 + a_{10}X + a_{01}Y + a_{00} = 0$$

egyenletű harmadfokú görbe affin transzformációval

$$Y^2 = X^3 + aX + b$$

alakúra hozható. [*Útmutatás:* 1) $-a_{02}^3$-el leosztva elérhető $a_{02} = -1$. 2) Eliminálják az XY és Y tagokat. 3) Eliminálják az X^2 tagot.]

5.1.10. Feladat. Határozzuk meg az alábbi U ponthalmazok $\mathscr{I}(U)$ eltűnési ideálját $K[X, Y]$-ban:

a) $U = \{(0, 0)\}$

b) $U = \{(5, -3)\}$

c) $U = \{(-1, 0), (2, 0)\}$

d) $U = \{(-1, -1), (-1, 1), (1, -1), (1, 1)\}$

e) $U = \{(n, 0) \mid n \in \mathbb{Z}\}$

5.1.11. Feladat. Legyen $U = \{(-1, 0), (1, 0), (0, 1)\}$ és $J = \langle X^2 + Y^2 - 1, Y(Y - 1)\rangle$.

a) Mutassuk meg, hogy $U = \mathscr{V}(J)$.

b) Mutassuk meg, hogy $(XY)^2 \in J$, de $XY \notin J$.

c) Határozzuk meg az $\mathscr{I}(U) = \mathscr{I}(\mathscr{V}(J)) = \sqrt{J}$ eltűnési ideált.

5.2. Feladatok a 2. zh-ra

5.2.1. Feladat. Adjuk meg azt a negyedfokú $f(X)$ polinomot, amelynek a gyökei pontosan az $X^2+Y^2=1$ és az $Y^2-2XY-X^2=0$ görbék metszéspontjainak az abszcisszái.

5.2.2. Feladat. Adjuk meg a $25X_1^2-X_2^2-X_3^2=0$ görbének a $P_1(1,7,1)$ és $P_2(1,-1,7)$ pontokat összekötő egyenessel vett metszéspontjait.

5.2.3. Feladat. Adjuk meg az alábbi görbepárok metszéspontjait.

(a) $X(Y^2-XZ)-Y^3=0$ és $Y^4+Y^3Z-X^2Y^2=0$.

(b) $X^3-Y^3-2XYZ=0$ és $2X^3-4X^2Y-3XY^2-Y^3-2X^2Z=0$.

(c) $X^4+Y^4+Y^2Z^2=0$ és $X^4+Y^4-2Y^3Z-2X^2YZ-XY^2Z+Y^2Z^2=0$.

5.2.4. Feladat. Adjuk meg az alábbi görbék szinguláris pontjait.

(a) $XZ^2-Y^3+XY^2=0$.

(b) $(X+Y+Z)^3-27XYZ=0$.

(c) $X^2Y^2+36XZ^3+24YZ^3+108Z^4=0$.

5.2.5. Feladat. Adjuk meg az alábbi görbék szinguláris pontjait a komplex projektív síkon:

(a) $X^3+Y^3=3XY$ (Descartes-féle levél),

(b) $(X^2+Y^2)(X-1)^2=X^2$ (Nikomédész-féle konhoisz),

(c) $(X^2+Y^2)^3=4X^2Y^2$ (Négylevelű lóhere).

Rajzoljuk le ezeket a görbéket a valós projektív síkon.

5.2.6. Feladat. Adjuk meg az alábbi görbék szinguláris pontjait és a szinguláris pontokban az érintőket:

(a) $Y^3-Y^2+X^3-X^2+3XY^2+3X^2Y+2XY=0$,

(b) $X^4+Y^4-X^2Y^2=0$,

(c) $X^3+Y^3-3X^2-3Y^2+3XY+1=0$,

(d) $Y^2+(X^2-5)(4X^4-20X^2+25)=0$.

5.2.7. Feladat. Vizsgáljuk meg az

$$X^2Y^5-X^5Y^2-2XY^5Z+X^5Z^2+Y^5Z^2-X^3YZ^3+2\alpha X^2Y^2Z^3-XY^3Z^3=0$$

($\alpha\in\mathbb{C}$) görbe szingularitásait az $(1,0,0)$, $(0,1,0)$ és $(0,0,1)$ pontokban.

5.2.8. Feladat. A k mely értékeire lesz az $X^3 + Y^3 + Z^3 + k(X + Y + Z)^3 = 0$ görbének egy vagy annál több szinguláris pontja? Határozzuk meg a szinguláris pontokat a k ezen értékeire.

5.2.9. Feladat. Legyen $\Gamma : f(X, Y) = 0$ algebrai görbe, $\ell : Y = mX + b$ egyenes és $P = P(0, 0)$. Mutassuk meg, hogy $i(\Gamma \cap \ell; P)$ pontosan a 0 gyök multiplicitása az $f(X, mX + b)$ polinomban. Más szóval, $i(\Gamma \cap \ell; P) = k$ akkor és csak akkor, ha $f(X, mX + b) = X^k(c + \cdots)$ valamilyen $c \neq 0$ konstanssal. [Útmutatás: Használjuk a rezultáns $R_{f,X-c} = \pm f(c)$ tulajdonságát.]

5.2.10. Feladat. Mutassuk meg, hogy az általános n-edfokú 3-változós homogén polinom együtthatóinak száma $\binom{n+1}{2}$. [Útmutatás: Számoljuk meg azon (i, j) párokat, melyekre $i, j \geq 0$ egészek és $i + j \leq n$.]

5.2.11. Feladat. Határozza meg az $Y = X^3$, $Y^2 = X^3$ és $Y^2 = X^3 + X^2$ görbék szinguláris és inflexiós pontjait a projektív síkon.

5.2.12. Feladat. (a) Legyen $\Gamma : Y = X^3$ és $O = (0, 0)$. Mutassa meg, hogy $(\Gamma^*, +, O) \cong (K, +)$.

(b) Legyen $\Gamma : Y^2 = X^3 + X^2$ és $O = (0 : 1 : 0)$. Mutassa meg, hogy $(\Gamma^*, +, O) \cong (K^*, \cdot)$.

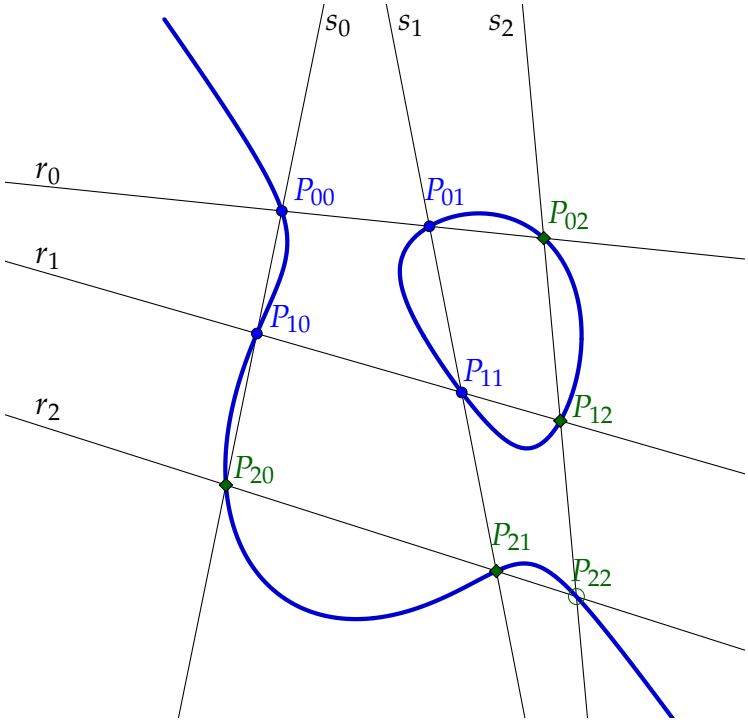
5.2.13. Feladat. Jelöljön Γ irreducibilis harmadrendű görbét.

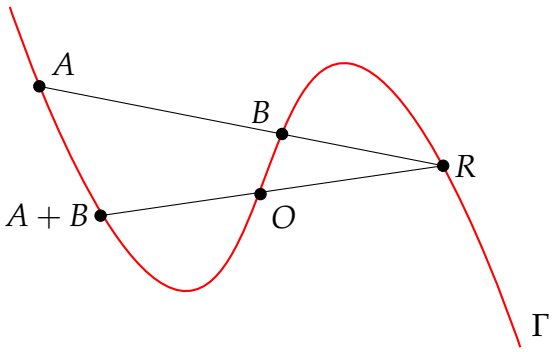
(a) Tegyük fel, hogy $O \in \Gamma$ inflexiós pont. Mutassa meg, hogy $A, B, C \in \Gamma^*$ akkor és csak akkor kollineárisak, ha $A + B + C = O$.

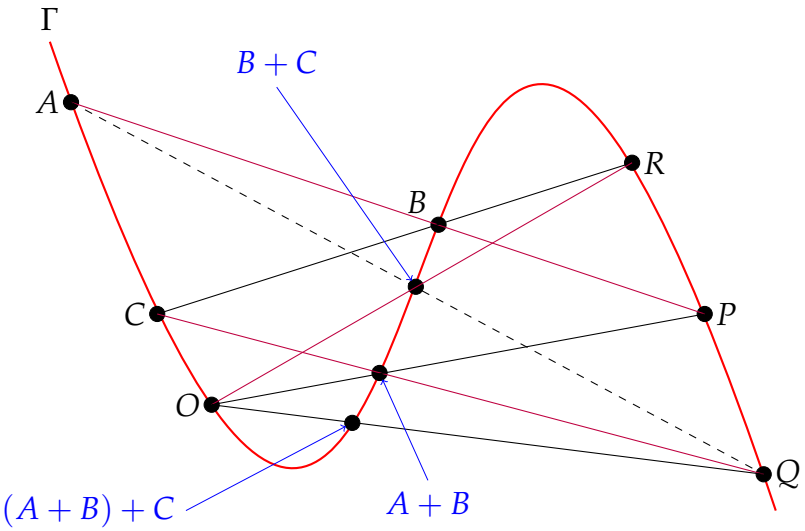
(b) Tegyük fel, hogy $O \in \Gamma$ inflexiós pont. Mutassa meg, hogy $A \in \Gamma$ akkor és csak akkor inflexiós pont, ha $3A = O$.

(c) Mutassa meg, hogy ha az ℓ egyenes átmegy Γ két inflexiós pontján, akkor átmegy egy harmadikon is.

5.3. Ábrák


s_0
s_1
s_2
r_0
r_1
r_2
P_{00}
P_{01}
P_{02}
P_{10}
P_{11}
P_{12}
P_{20}
P_{21}
P_{22}


A
B
R
$A+B$
O
Γ


Γ
$B+C$
A
R
B
C
P
O
Q
$(A+B)+C$
$A+B$