Algebrai alapismeretek az *Algebrai síkgörbék* c. tárgyhoz

1. Integritástartományok, oszthatóság

1.1. Definíció. *A nullaosztómentes, egységelemes kommutatív gyűrűket* **integritástartománynak** *nevezzük.*

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

1.2. Definíció. *Legyen a, b a D integritástartomány két eleme. Azt mondjuk, hogy a* **osztja** *b-***t,** *ha létezik $c \in D$ elem, amelyre $ac = b$; jelöléssel $a|b$. Amennyiben $a|b$ és $b|a$ 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. példa. $\mathbb{Z}$ egységei ± 1, míg $D[X_1, \ldots, X_n]^* = D^*$.

1.3. Definíció. *Azt mondjuk, hogy a D integritástartomány a eleme* **irreducibilis,** *ha minden $b|a$ elemre $b \sim a$ vagy $b \sim 1$ teljesül. Továbbá, ha $a|bc$-ből következik, hogy $a|b$ vagy $a|c$, akkor* **prímelemről** *beszélünk.*

Könnyen meggondolható, hogy definíció szerint minden prímelem irreducibilis. Ennek megfordítása azonban nem minden integritástartomány 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.)

1.4. Definíció. *Azokat az integritástartományokat, amelyekben minden irreducibilis elem prím,* **Gauss-gyűrűknek** *nevezzük.*

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

1.6. 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. □

1.7. Következmény. *A D integritástartomány feletti $D[X_1, \dots, X_n]$ polinomgyűrűben egyértelmű faktorizáció áll fenn. Pontosabban, bármely $f \in D[X_1, \dots, X_n]$ 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 integritástartomány 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:

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

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

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

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

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

Minden n-változós racionális törtfüggvény $\frac{f(X_1, \dots, X_n)}{g(X_1, \dots, X_n)}$ 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 $(x_1, \dots, x_n) \in D^n$ behelyettesítés, melyre $f(x_1, \dots, x_n) \neq 0$ és $g(x_1, \dots, x_n) = 0$. Racionális törtfüggvények leképezésként való értelmezésére a továbbiakban nem lesz szükségünk.

2. 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. 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 komolyabb zavart nem okoz.

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

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

2.2. 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 $h_1, \dots, h_n$ 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 $f|gh$ oszthatóságból következik, hogy minden i esetén $r_i \le s_i + t_i$; $\deg(v) < \deg(f)$ 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.

$$\begin{array}{lcccccc}
\text{konst.:} & a_n u_m + & & & b_m v_n & & \\
X: & a_{n-1}u_m + a_n u_{m-1} + & & & b_{m-1}v_n + b_m v_{n-1} & & \\
 & \vdots & & & \vdots & & \\
X^{m-1}: & a_{n-m+1}u_m + & \cdots & a_n u_1 + & b_1 v_n + b_2 v_{n-1} + & \cdots & \\
X^m: & a_{n-m}u_m + & \cdots & a_{n-1}u_1 + & b_0 v_n + b_1 v_{n-1} + & \cdots & \\
 & \vdots & & & \vdots & & \\
X^{n-1}: & a_1 u_m + a_2 u_{m-1} + & \cdots & & & \cdots + & b_m v_1 \\
X^n: & a_0 u_m + a_1 u_{m-1} + & \cdots & & & \cdots + & b_{m-1} v_1 \\
 & \vdots & & & \vdots & & \\
X^{n+m-1}: & & & a_0 u_1 + & & & b_0 v_1
\end{array}$$

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:

$$\left.\begin{array}{lcccccc}
0 = & a_n U_m + & & & b_m V_n & & \\
0 = & a_{n-1}U_m + a_n U_{m-1} + & & & b_{m-1}V_n + b_m V_{n-1} & & \\
 & \vdots & & & & & \\
0 = & a_{n-m+1}U_m + & \cdots & a_n U_1 + & b_1 V_n + b_2 V_{n-1} + & \cdots & \\
0 = & a_{n-m}U_m + & \cdots & a_{n-1}U_1 + & b_0 V_n + b_1 V_{n-1} + & \cdots & \\
 & \vdots & & & & & \\
0 = & a_1 U_m + a_2 U_{m-1} + & \cdots & & & \cdots + & b_m V_1 \\
0 = & a_0 U_n + a_1 U_{m-1} + & \cdots & & & \cdots + & b_{m-1} V_1 \\
 & \vdots & & & & & \\
0 = & & & a_0 U_1 + & & & b_0 V_1
\end{array}\right\} \qquad (1)$$

Az (1) egyenletrendszer együtthatóiból készített mátrix

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

2.3. Definíció. *A (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.

$$R_{f,g} = \det \begin{pmatrix} a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & \cdots & 0 \\ \vdots & & \ddots & & & \ddots & \vdots \\ 0 & 0 & \cdots & a_0 & a_1 & \cdots & a_n \\ b_0 & \cdots & b_m & 0 & 0 & \cdots & 0 \\ 0 & b_0 & \cdots & b_m & 0 & \cdots & 0 \\ & & \ddots & & \ddots & & \\ & & & \ddots & & \ddots & \\ 0 & 0 & 0 & 0 & b_0 & \cdots & b_m \end{pmatrix} \tag{3}$$

2.4. Állítás (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 az (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 az (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. □

2.2. 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.

3. Kétváltozós polinomok alaptulajdonságai

A mi esetünkben a rezultánsok a kétváltozós polinomok vizsgálatakor nyernek különös jelentőséget. Tekintsük ugyanis a $D = \mathbb{C}[Y]$ integritástartományt, ekkor $D[X] = \mathbb{C}[X, Y]$. Másszóval az $f(X, Y), g(X, Y) \in \mathbb{C}[X, Y]$ n-edfokú, illetve m-edfokú kétváltozós polinomok felírhatók

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

alakban, ahol $a_i(Y), b_j(Y)$ egyváltozós komplex együtthatós polinomok. Igaz továbbá, hogy $\deg(a_i) \leq i$, $\deg(b_j) \leq j$. Ebben az esetben f és g rezultánsa $\mathbb{C}$ feletti polinom:

$$R_{f,g}(Y) = \det \begin{pmatrix} a_0(Y) & \cdots & a_n(Y) & \cdots & 0 \\ & \ddots & & \ddots & \\ 0 & \cdots & a_0(Y) & \cdots & a_n(Y) \\ b_0(Y) & \cdots & b_m(Y) & \cdots & 0 \\ & \ddots & & \ddots & \\ 0 & \cdots & b_0(Y) & \cdots & b_m(Y) \end{pmatrix} \in \mathbb{C}[Y]. \tag{4}$$

A rezultánsok alaptétele ekkor két jelentéssel bír.

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

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

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

3.3. Állítás. *Legyen az $f(X,Y), g(X,Y) \in \mathbb{C}[X,Y]$ polinomok foka n illetve m. Ekkor az $R_{f,g}(Y)$ rezultáns foka legfeljebb nm.*

Bizonyítás. Jelölje c_{ij} a (4) mátrix i-dik sorának j-dik elemét, ekkor

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

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 $\{1, \ldots, n+m\}$ 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

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

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

4. Rezultánsok, folytatás

Ebben a fejezetben a 2.2 állítást élesítjük. Ehhez visszatérünk az utolsó előtti fejezetben használt jelöléseinkhez. Legyen tetszőleges D integritástartomány, $g(X)$, $f(X)$ tetszőleges D feletti n, illetve m-edfokú polinomok:

4.1. Állítás. *Tetszőleges $f, g \in D[X]$ polinomokhoz léteznek $u, v \in D[X]$ polinomok úgy, hogy* $\deg(u) < \deg(g)$, $\deg(v) < \deg(f)$ *és a rezultánsra fennáll* $R_{f,g} = u(X)f(X) + v(X)g(X)$.

Bizonyítás. Legyen $n = \deg(f), m = \deg(m)$ és írjuk fel a polinomjainkat

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n, a_0 \neq 0,$$
$$g(X) = b_0X^m + b_1X^{m-1} + \cdots + b_m, b_0 \neq 0.$$

alakban. Végezzük el a (3) képletben szereplő mátrixon az alábbi átalakítást: minden $k = 1, \ldots, n+m-1$ értékre adjuk hozzá az utolsó oszlophoz a k-dik oszlop X^{n+m-k}-szorosát. Ekkor nyilván a mátrix determinánsának értéke változatlanul $R_{f,g}$. Másrészről az utolsó oszlopban szereplő elemek rendre

$$\begin{aligned}
a_0X^{n+m-1}+a_1X^{n+m-2}+\cdots\ +a_nX^m &= X^{m-1}f(X)\\
a_0X^{n+m-2}+\cdots+a_{n-1}X^m+a_nX^{m-1} &= X^{m-2}f(X)\\
&\vdots\\
a_0X^n+\quad\cdots\quad+a_n &= f(X)\\
b_0X^{n+m-1}+b_1X^{n+m-2}+\cdots\ +b_mX^n &= X^{n-1}g(X)\\
b_0X^{n+m-2}+\cdots+b_{m-1}X^n+b_mX^{n-1} &= X^{n-2}g(X)\\
&\vdots\\
b_0X^n+\quad\cdots\quad+b_m &= g(X)
\end{aligned}$$

Jelölje c_j a j-dik sor utolsó eleméhez tartozó kiegészítő adjungált aldeterminánst. Mivel az utolsó oszlop kivételével a mátrixban mindenhol D-beli elemek szerepelnek, ezért $c_j \in D$ minden $j = 1, \ldots, n+m$ esetén. A mátrix determinánsát az utolsó oszlopa szerint kifejtve kapjuk, hogy

$$\begin{aligned}
R_{f,g} &= c_1X^{m-1}f(X) + \cdots + c_mf(X) +\\
&\qquad c_{m+1}X^{n-1}g(X) + \cdots + c_{n+m}g(X)\\
&= u(X)f(X) + v(X)g(X),
\end{aligned}$$

ahol

$$u(X) = c_1X^{m-1} + c_2X^{m-2} + \cdots + c_m,$$
$$v(X) = c_{m+1}X^{n-1} + c_{m+2}X^{n-2} + \cdots + c_{n+m}.$$

D feletti egyváltozós polinomok. Mivel a fokszámokra kitett feltétel nyilvánvalóan teljesül, az állítást bebizonyítottuk. □

Az állításunk súlya akkor válik igazán érzékelhetővé, ha megfogalmazzuk kétváltozós polinomokra.

4.2. Következmény. *Legyenek* $f(X,Y), g(X,Y) \in \mathbb{C}[X,Y]$ *kétváltozós komplex együtthatós polinomok. Jelölje* $n = \deg_X(f)$, $m = \deg_X(g)$ *az* f *és* g X*-beli fokát. Ekkor léteznek* $a(X,Y), b(X,Y) \in \mathbb{C}[X,Y]$ *polinomok, melyekre* $\deg_X(a) < m$, $\deg_X(b) < n$ *és*

$$R_{f,g}(Y) = a(X,Y)f(X,Y) + b(X,Y)g(X,Y). \qquad \square$$

Ennek felhasználásával belátjuk az alábbi kulcsfontosságú tételt.

4.3. Tétel. *Legyen* $f(X,Y) \in \mathbb{C}[X,Y]$ *irreducibilis komplex együtthatós polinom és tegyük fel, hogy a* $g(X,Y) \in \mathbb{C}[X,Y]$ *polinomra teljesül* $g(x,y) = 0$ *valahányszor* $f(x,y) = 0$ *a komplex* $x, y \in \mathbb{C}$ *értékekre. Ekkor* f *osztja* g*-t.*

Bizonyítás. I. eset: $f(X,Y) \equiv 0$. Ekkor minden $x, y \in C$ esetén $f(x,y) = g(x,y) = 0$, azaz $g(X,Y)$ is azonosan 0, melynek minden polinom osztója.

II. eset: $f(X,Y) = f(Y)$ nem függ X-től. Mivel $f(Y)$ komplex együtthatós és irreducibilis, feltétlenül elsőfokúnak kell lennie: $f(Y) = f(X,Y) = a_0Y + a_1$, $a_0, a_1 \in \mathbb{C}$. Írjuk g-t $g(X,Y) = b_0(Y)X^m + \cdots + b_m(Y)$ alakba. A feltétel szerint a

$$g(X, -\frac{a_1}{a_0}) = b_0(-\frac{a_1}{a_0})X^m + \cdots + b_m(-\frac{a_1}{a_0})$$

egyváltozós polinom azonosan nulla, azaz $-\frac{a_1}{a_0}$ gyöke minden $b_i(Y)$-nak ($i = 0, \ldots, m$). Más szóval $f(Y) = a_0Y + a_1$ osztja az összes $b_i(Y)$-t, tehát $f \mid g$ is teljesül.

III. eset: $n = \deg_X(f) > 0$. Írjuk f-et $f(X,Y) = a_0(Y)X^n + \cdots + a_n(Y)$ alakba. Mivel $a_0(Y) \not\equiv 0$, véges sok komplex szám kivételével $a_0(y) \neq 0$. Rögzítsünk tetszőleges egy ilyen $y \in \mathbb{C}$ értéket, ekkor az $f(X,y)$ egyváltozós komplex polinom foka pontosan $n > 0$. Az algebra alaptétele szerint létezik $x \in C$ komplex szám, mely gyöke ennek, azaz $f(x,y) = 0$ teljesül. Ekkor azonban a feltételünk szerint $g(x,y) = 0$ szintén fennáll, ami a 4 következmény szerint azt jelenti, hogy $R_{f,g}(y) = 0$.

Az látjuk tehát, hogy véges sok komplex szám kivételével az $R_{f,g}(Y)$ egyváltozós polinom helyettesítési értéke nulla, ami csak úgy lehetséges, ha $R_{f,g}(Y) \equiv 0$. A 3.1 tétel szerint ekkor f-nek és g-nek van X-ben nem konstans $d(X,Y)$ közös komponense: $d \mid f, g$. Mivel azonban f irreducibilis, f és d asszociáltak kell legyenek, azaz $f \mid g$ is teljesül. $\square$