Resultants and discriminants

Arkadiusz Płoski

December 2016
This article is an extended version of a lecture delivered at the University of Laguna in June 2010.

1 Introduction

Let $\mathbb{A}$ be a ring (commutative with identity). We may form matrices and determinants with elements of $\mathbb{A}$. Let $\mathbf{M}$ be a square matrix. Replacing the elements of $\mathbf{M}$ by its cofactors and then transposing the obtained matrix we get the matrix $\mathbf{M}^\wedge$ such that

$$\mathbf{M}\mathbf{M}^\wedge = \mathbf{M}^\wedge\mathbf{M} = (\det\mathbf{M})\mathbf{I},$$

where $\mathbf{I}$ is the identity matrix. We call the above formula Cramer's Rule. Let $\mathbb{A}[T]$ be the ring of polynomials in one variable T. For any integer $N > 0$ we denote by $\mathbb{A}[T]^{(N)}$ the set of all polynomials of degree $< N$. Thus any element of $\mathbb{A}[T]^{(N)}$ is of the form

$$c_1T^{N-1} + c_2T^{N-2} + \ldots + c_N \quad \text{with } c_j \in \mathbb{A} \text{ for } j = 1, \ldots, N$$

and $\mathbb{A}[T]^{(N)}$ is a free module of rank N. For any sequence of N polynomials from $\mathbb{A}[T]^{(N)}$:

$$f_i = c_{i1}T^{N-1} + c_{i2}T^{N-2} + \ldots + c_{iN},\ i = 1, \ldots, N$$

we consider the matrix

$$\mathbf{M}(f_1, \ldots, f_N) = [c_{ij}]_{i,j=1,\ldots,N}$$

and the determinant

$$\det(f_1, \ldots, f_N) = \det\mathbf{M}(f_1, \ldots, f_N)$$

From the well-known properties of determinant we get

Property 1.1. *Let $i \in \{1, \ldots, N\}$. Then $f_i \mapsto \det(f_1, \ldots, f_N)$ is an $\mathbb{A}$–linear mapping from $\mathbb{A}[T]^{(N)}$ to $\mathbb{A}$*

Property 1.2. *Let S_N be the set of all permutations of $\{1, \ldots, N\}$. Then for any $\sigma \in S_N$:*

$$\det(f_{\sigma(1)}, \ldots, f_{\sigma(N)}) = (sgn\sigma)\det(f_1, \ldots, f_N)$$

Property 1.3. $\det(T^{N-1}, \ldots, 1) = 1$

Property 1.4. *If $f_i \in \mathbb{A}[T]^{(N)}$ are all of the degree strictly less than $N-1$ then* $\det(f_1, \ldots, f_N) = 0$

Moreover, we have

Property 1.5. *If $\mathbb{A}$ is an integral domain, then $\det(f_1, \ldots, f_N) = 0$ if and only if there are elements $a_1, \ldots, a_N \in \mathbb{A}$ not all equal zero such that $a_1 f_1 + \ldots + a_N f_N = 0$*

Let us write

$$\begin{bmatrix} f_1 \\ \vdots \\ f_N \end{bmatrix} = \mathbf{M}(f_1, \ldots, f_N) \begin{bmatrix} T^{N-1} \\ \vdots \\ 1 \end{bmatrix}$$

Using Cramer's Rule we get

Property 1.6.

$$\det(f_1, \ldots, f_N) \begin{bmatrix} T^{N-1} \\ \vdots \\ 1 \end{bmatrix} = \mathbf{M}^{\wedge}(f_1, \ldots, f_N) \begin{bmatrix} f_1 \\ \vdots \\ f_N \end{bmatrix}$$

which implies

Property 1.7. *For any polynomial $h \in \mathbb{A}[T]^{(N)}$ there are constants $a_1, \ldots, a_N \in \mathbb{A}$ such that* $\det(f_1, \ldots, f_N)h = a_1 f_1 + \ldots + a_N f_N$

2 First properties of resultant

Let $n, m \geq 0$ be integers such that $n > 0$ or $m > 0$. For any pair of polynomials

$$f(T) = a_0 T^n + a_1 T^{n-1} + \ldots + a_n,$$

$$g(T) = b_0 T^m + b_1 T^{m-1} + \ldots + b_m$$

we define the **Sylvester matrix**

$$\underset{n,m}{\mathbf{S}}(f, g) = \mathbf{M}(T^{m-1}f, T^{m-2}f, \ldots, f, T^{n-1}g, T^{n-2}g, \ldots, g)$$

and the **resultant**

$$\underset{n,m}{R}(f, g) = \det \underset{n,m}{\mathbf{S}}(f, g)$$

Therefore $\underset{n,m}{R}(f, g)$ is an element of the ring $\mathbb{A}$.

Remark 2.1. The Sylvester matrix is a square matrix with $m+n$ rows and $m+n$ columns.

$$\underset{0,m}{\mathbf{S}}(f,g) = \mathbf{M}(T^{m-1}f,\ldots,f)$$

$$\underset{n,0}{\mathbf{S}}(f,g) = \mathbf{M}(T^{n-1}g,\ldots,g)$$

The following proposition follows easily from the properties of determinant listed in Introduction.

Proposition 2.2.

(i) $\underset{n,m}{R}(af,bg) = a^m b^n \underset{n,m}{R}(f,g)$,

(ii) $\underset{n,m}{R}(f,g) = (-1)^{nm} \underset{m,n}{R}(g,f)$,

(iii) $\underset{n,0}{R}(f,b_0) = b_0^n$, $\underset{0,m}{R}(a_0,g) = a_0^m$,

(iv) *if* $f \in \mathbb{A}[T]^{(n)}$ *and* $g \in \mathbb{A}[T]^{(m)}$, *then* $\underset{n,m}{R}(f,g) = 0$,

(v) *For any* $h \in \mathbb{A}[T]^{(n+m)}$ *there are polynomials* $u \in \mathbb{A}[T]^{(m)}$ *and* $v \in \mathbb{A}[T]^{(m)}$ *such that* $\underset{n,m}{R}(f,g)h = uf + vg$

Proof. Use 1.1, 1.2, 1.3 and 1.4. □

Proposition 2.3. *Suppose that* $\mathbb{A}$ *is an integral domain. Then* $\underset{n,m}{R}(f,g) = 0$ *if and only if there are polynomials* $u \in \mathbb{A}[T]^{(m)}$ *and* $v \in \mathbb{A}[T]^{(n)}$ *such that* $u \neq 0$ *or* $v \neq 0$ *and* $uf + vg = 0$ *in* $\mathbb{A}[T]$

Proof. By 1.5 the resultant $\underset{n,m}{R}(f,g) = \det(T^{m-1}f,\ldots,f,T^{n-1}g,\ldots,g)$ is equal to 0 if and only if there is a non–zero sequence $\tilde{a}_0,\ldots,\tilde{a}_m,\tilde{b}_0,\ldots,\tilde{b}_n \in \mathbb{A}$ such that $\tilde{a}_0T^{m-1}f + \ldots + \tilde{a}_m f + \tilde{b}_0 T^{n-1}g + \ldots + \tilde{b}_n g = 0$. It suffices to take $u = \tilde{a}_0 T^{m-1} + \ldots + \tilde{a}_m$ and $v = \tilde{b}_0 T^{n-1} + \ldots + \tilde{b}_n$. □

Proposition 2.4. *Suppose that* $\mathbb{A}$ *is a factorial ring. Let* $f = a_0T^n + \ldots + a_n$, $a_0 \neq 0$, $n > 0$ *and* $g = b_0T^m + \ldots + b_m$. *Then* $\underset{n,m}{R}(f,g) = 0$ *if and only if the polynomials* f, g *have a common divisor of degree* > 0.

Proof. If $f = \tilde{u}\phi$, $g = \tilde{v}\phi$ in $\mathbb{A}[T]$ where $\deg\phi > 0$, then $\tilde{u} \neq 0$ and $\tilde{v}f - \tilde{u}g = 0$ where $\deg\tilde{u} < \deg f = n$ and $\deg\tilde{v} \leq \deg g < m$. From 2.3 we have that $\underset{n,m}{R}(f,g) = 0$.

Now suppose that $\underset{n,m}{R}(f,g) = 0$. By Proposition 2.3 we get that $uf + vg = 0$ where $u \neq 0$ or $v \neq 0$ and $\deg u < m$, $\deg v < n$. Since $f \neq 0$ we have that $v \neq 0$. The ring $\mathbb{A}[T]$ being factorial there exists a prime factor ϕ of f ($\deg v < n = \deg f$) such that ϕ divides g □

3 The resultant $\underset{n,m}{R}(f,g)$ as a polynomial in coefficients of f and g

Let us begin with

Property 3.1. *Let $f = a_0T^n + \ldots + a_n$, $g = b_0T^m + \ldots + b_m$ where $n, m > 0$. Write $\underset{n,m}{\boldsymbol{S}}(f,g) = [c_{ij}]_{i,j=1,\ldots,m+n}$. Then*

(i) Let $i \in \{1,\ldots,m\}$. Then

$$c_{ij} = \begin{cases} a_{j-i} & \text{for } j \in \{i,\ldots,i+n\} \\ 0 & \text{for } j \notin \{i,\ldots,i+n\} \end{cases}$$

(ii) Let $i \in \{m+1,\ldots,m+n\}$. Then

$$c_{ij} = \begin{cases} b_{j-i+m} & \text{for } j \in \{i-m,\ldots,i\} \\ 0 & \text{for } j \notin \{i-m,\ldots,i\} \end{cases}$$

Proof. Follows directly from the definition of $\underset{n,m}{\mathbf{S}}(f,g)$. $\square$

Property 3.2. *Let $S_{n,m}$ be the set of permutation defined as follows: $\sigma \in S_{n,m}$ if and only if $\sigma \in S_{n+m}$ and $i \le \sigma(i) \le i+n$ for $i = 1,\ldots,m$ and $k \le \sigma(k+m) \le k+m$ for $k = 1,\ldots,n$. Then*

$$\underset{n,m}{R}(f,g) = \sum_{\sigma \in S_{n,m}} (sgn\sigma) a_{\sigma(1)-1} \ldots a_{\sigma(m)-m} b_{\sigma(m+1)-1} \ldots b_{\sigma(m+n)-n}$$

Proof. By the classical definition of determinant and Property 3.1 we get

$$\begin{aligned} \underset{n,m}{R}(f,g) &= \sum_{\sigma \in S_{n+m}} (\mathrm{sgn}\ \sigma) c_{1,\sigma(1)} \ldots c_{m+n,\sigma(m+n)} = \\ &= \sum_{\sigma \in S_{n,m}} (\mathrm{sgn}\ \sigma) a_{\sigma(1)-1} \ldots a_{\sigma(m)-m} b_{\sigma(m+1)-1} \ldots b_{\sigma(m+n)-n} \end{aligned}$$

$\square$

Example 3.3. Let us calculate the resultant of polynomials $f = a_0T^2 + a_1T + a_2$ and $g = b_0T^2 + b_1T + b_2$. Observe that a permutation $\sigma \in S_4$ belongs to $S_{2,2}$ if and only if $\sigma(1) \neq 4$, $\sigma(2) \neq 1$, $\sigma(3) \neq 4$ and $\sigma(4) \neq 1$.
We have

$$\underset{2,2}{R}(f,g) = \sum_{\sigma \in S_{2,2}} (\mathrm{sgn}\ \sigma) a_{\sigma(1)-1} a_{\sigma(2)-2} b_{\sigma(3)-1} b_{\sigma(4)-2}$$

It is easy to check that $S_{2,2}$ contains 8 permutations. We get

σ	sgn σ	$\sigma(1)-1,\sigma(2)-2,$ $\sigma(3)-1,\sigma(4)-2$	$(\text{sgn }\sigma)a_{\sigma(1)-1}a_{\sigma(2)-2}a_{\sigma(3)-1}a_{\sigma(4)-2}$
$1,2,3,4$	$+1$	$0,0,2,2$	$a_0^2b_2^2$
$1,4,2,3$	$+1$	$0,2,1,1$	$a_0a_1b_1^2$
$2,3,1,4$	$+1$	$1,1,0,2$	$a_1^2b_0b_2$
$3,4,1,2$	$+1$	$2,2,0,1$	$a_2^2b_0^2$
$3,2,1,4$	-1	$2,0,0,2$	$-a_2a_0b_0b_2$
$2,4,1,3$	-1	$1,2,0,1$	$-a_1a_2b_0b_1$
$1,3,2,4$	-1	$0,1,1,2$	$-a_0a_1b_1b_2$
$1,4,3,2$	-1	$0,2,2,0$	$-a_0a_2b_2b_0$

Hence

$$\underset{2,2}{R}(f,g) = a_0^2b_2^2 + a_0a_2b_1^2 + a_1^2b_0b_2 + a_2^2b_0^2 - 2a_0a_2b_0b_2 - a_1a_2b_0b_1 - a_0a_1b_1b_2$$

Let $\overrightarrow{A} = (A_0, A_1, \ldots, A_n)$ and $\overrightarrow{B} = (B_0, B_1, \ldots, B_m)$ be variables and let us consider the polynomials

$$F(\overrightarrow{A}, T) = A_0T^n + A_1T^{n-1} + \ldots + A_n$$
$$G(\overrightarrow{B}, T) = B_0T^m + A_1T^{m-1} + \ldots + A_m$$

with coefficients in the ring $\mathbb{Z}[\overrightarrow{A}, \overrightarrow{B}]$.
Let $R(\overrightarrow{A}, \overrightarrow{B}) = \underset{n,m}{R}(F,G)$. By Property 3.2 we can write

$$R(\overrightarrow{A}, \overrightarrow{B}) = \sum_{\sigma \in S_{n,m}} (\text{sgn }\sigma) A_{\sigma(1)-1} \ldots A_{\sigma(m)-m} B_{\sigma(m+1)-1} \ldots B_{\sigma(m+n)-n}$$

From the above formula we get basic properties of the polynomial $R(\overrightarrow{A}, \overrightarrow{B})$.

Property 3.4. *The resultant $R(\overrightarrow{A}, \overrightarrow{B})$ is a homogeneous polynomial in $\overrightarrow{A}$ of degree m and a homogeneous polynomial in $\overrightarrow{B}$ of degree n.*

Proof. Obvious. □

Property 3.5. *If we put weight $A_i = i$ for $0 \le i \le n$ and weight $B_j = j$ for $0 \le j \le m$ then the weight of any term of $R(\overrightarrow{A}, \overrightarrow{B})$ is equal to mn.*

Proof. We have

$$\begin{aligned}
&\text{weight}\left(A_{\sigma(1)-1} \ldots A_{\sigma(m)-m} B_{\sigma(m+1)-1} \ldots B_{\sigma(m+n)-n}\right) = \\
&= \sum_{i=1}^{m} (\sigma(i) - i) + \sum_{j=1}^{n} (\sigma(m+j) - j) = \\
&= \sum_{i=1}^{m+n} \sigma(i) - \sum_{i=1}^{m} i - \sum_{j=1}^{n} j = \sum_{i=1}^{m+n} i - \sum_{i=1}^{m} i - \sum_{j=1}^{n} j = mn
\end{aligned}$$

□

Property 3.6. *The resultant $R(\overrightarrow{A}, \overrightarrow{B})$ is a $\mathbb{Z}$–linear combination of the monomials $A_0^{i_0} A_1^{i_1} \dots A_n^{i_n} B_0^{j_0} \dots B_m^{j_m}$, where $i_0 + \dots + i_n = m$, $j_0 + \dots + j_m = n$, $i_1 + 2i_2 + \dots + ni_n + j_1 + 2j_2 + \dots + mj_m = mn$. Moreover, $R(\overrightarrow{A}, \overrightarrow{B}) = A_0^m B_m^n + \dots + (-1)^{mn} A_n^m B_0^n$, where the dots denote the terms which don't cancel with two exhibited monomials.*

Proof. The first part of Property 3.6 follows from Properties 3.4 and 3.5. The established terms correspond to the permutations $(1, 2, \dots, m+n)$ and $(n+1, n+2, \dots, n+m, 1, 2, \dots, n) \in S_{n,m}$ $\square$

Property 3.7. *Let $f = a_0 T^n + \dots + a_n$, $g = b_0 T^m + \dots + b_m \in \mathbb{A}[T]$, where $n, m \geq 0$, then*

$$\underset{n,m}{R}(f, g) = R(a_0, \dots, a_n, b_0, \dots, b_m)$$

Remark 3.8.

$$R(A_0, \dots, A_n, B_0) = B_0^n, \quad R(A_0, B_0, \dots, B_m) = A_0^m$$

4 The resultant in terms of roots

We keep the notation introduced above. Let $\overrightarrow{X} = (X_1, \dots, X_n)$, $\overrightarrow{Y} = (Y_1, \dots, Y_m)$ be variables and put

$$f = \prod_{i=1}^{n} (T - X_i) = T^n + a_1(\overrightarrow{X}) T^{n-1} + a_n(\overrightarrow{X}) \in \mathbb{Z}[\overrightarrow{X}][T]$$
$$g = \prod_{j=1}^{m} (T - Y_j) = T^m + b_1(\overrightarrow{Y}) T^{m-1} + b_m(\overrightarrow{Y}) \in \mathbb{Z}[\overrightarrow{X}][T]$$

Lemma 4.1. *Let $r(\overrightarrow{X}, \overrightarrow{Y}) = \underset{n,m}{R}(f, g)$. Then*

(i) $r(\overrightarrow{X}, \overrightarrow{Y}) \in \mathbb{Z}[\overrightarrow{X}, \overrightarrow{Y}]$ is a homogeneous polynomial of degree mn,

(ii) $r(\overrightarrow{X}, 0) = b_m(\overrightarrow{Y})^n = (-1)^{mn} Y_1 \dots Y_m$,

(iii) For each pair (i, j): $X_i - X_j$ divides $r(\overrightarrow{X}, \overrightarrow{Y})$ in $\mathbb{Z}[\overrightarrow{X}, \overrightarrow{Y}]$.

Proof. Assertions (i) and (ii) follow from Property 3.6. To check (iii) let us write by Proposition 2.2(v): $r(\overrightarrow{X}, \overrightarrow{Y}) = u(\overrightarrow{X}, \overrightarrow{Y}, T) \prod_{i=1}^{n} (T - X_i) + u(\overrightarrow{X}, \overrightarrow{Y}, T) \prod_{j=1}^{m} (T - Y_j) \in \mathbb{Z}[\overrightarrow{X}, \overrightarrow{Y}]$. Substituting X_i for T $(i = 1, \dots, n)$ we get that $X_i - Y_j$ divides $r(\overrightarrow{X}, \overrightarrow{Y})$. $\square$

Proposition 4.2. *With the notation introduced above*

(i) $\underset{n,m}{R}(f, g) = \prod_{i=1}^{n} \prod_{j=1}^{m} (X_i - Y_j)$,

(ii) $\underset{n,m}{R}\big(f, B_0T^m + B_1T^{m-1} + \ldots + B_m\big) = \prod_{i=1}^n (B_0X_i^m + B_1X_i^{m-1} + \ldots + B_m)$

Proof. Obviously the differences $X_i - Y_j$ are different primes in $\mathbb{Z}[\overrightarrow{X}, \overrightarrow{Y}]$. Therefore we may write

$$r(\overrightarrow{X}, \overrightarrow{Y}) = a\prod_{i=1}^{n}\prod_{j=1}^{m}(X_i - Y_j) \text{ in } \mathbb{Z}[\overrightarrow{X}, \overrightarrow{Y}]$$

We have that $a \in \mathbb{Z}$ since the product of differences is homogeneous form of degree mn like $r(\overrightarrow{X}, \overrightarrow{Y})$ (Lemma 4.1(i)). Substituting 0 for variables $Y_1, \ldots, Y_m$ we get $r(\overrightarrow{X}, 0) = a\prod_{i=1}^n \prod_{j=1}^m (-Y_j) = a(-1)^{mn}Y_1 \ldots Y_m$ whence $a = 1$ by Lemma 4.1(ii).
To check the second part of Proposition 4.2 observe that both sides of equality 4.2(ii) are homogeneous in $\overrightarrow{B} = (B_0, B_1, \ldots, B_m)$ of degree n. Therefore it suffices to check 4.2(ii) for monic polynomials $T^m + B_1T^{m-1} + \ldots + B_m$. By the first part of the proposition

$$\begin{aligned}
&\underset{n,m}{R}\left(\prod_{i=1}^{n}(T - X_i), T^m + b_1(\overrightarrow{Y})T^{m-1} + \ldots + b_m(\overrightarrow{Y})\right) = \\
&= \underset{n,m}{R}\left(\prod_{i=1}^{n}(T - X_i), \prod_{j=1}^{m}(T - Y_j)\right) = \\
&= \prod_{i=1}^{n}\prod_{j=1}^{m}(X_i - Y_j) = \prod_{i=1}^{n}(X_i^m + b_1(\overrightarrow{Y})X_i^{m-1} + \ldots + b_m(\overrightarrow{Y}))
\end{aligned}$$

and we get the formula

$$\begin{aligned}
&\underset{n,m}{R}\left(\prod_{i=1}^{n}(T - X_i), T^m + B_1T^{m-1} + \ldots + B_m\right) = \\
&= \prod_{i=1}^{n}(X_i^m + B_1X_i^{m-1} + \ldots + B_m)
\end{aligned}$$

by the algebraic independence of elementary symmetric polynomials $b_1(\overrightarrow{Y}), \ldots, b_m(\overrightarrow{Y})$. ◻

Corollary 4.3. *Let $f(T) = a_0(T - c_1)\ldots(T - c_n) \in \mathbb{A}[T]$ and let $g(T) \in \mathbb{A}[T]$ be a polynomial of degree $\leq m$. Then*

$$\underset{n,m}{R}(f, g) = a_0^m \prod_{i=1}^{n} g(c_i)$$

Proof. Let $\tilde{f}(T) = (T - c_1)\dots(T - c_n)$. Then

$$\underset{n,m}{R}(f,g) = \underset{n,m}{R}(a_0\tilde{f}, g) = a_0^m \underset{n,m}{R}(\tilde{f}, g) = a_0^m \prod_{i=1}^{n} g(c_i)$$

The last equality follows from Proposition 4.2(ii): since the both sides of (ii) are polynomials in $X_1, \dots, X_n$ we can substitute c_1 for X_1, …, c_n for X_n. $\square$

Corollary 4.4. *Let $f(T) = a_0(T - c_1)\dots(T - c_n)$ and $g(T) = b_0(T - d_1)\dots(T - d_m)$, Then*

$$\underset{n,m}{R}(f,g) = a_0^m b_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(c_i - d_j)$$

Proof. Use Proposition 4.2(i). $\square$

5 The resultant and norm

Let $f(T) = T^n + a_1T^{n-1} + \dots + a_n,\ n > 0$ and $g(T) = b_0T^m + b_1T^{m-1} + \dots + b_m,\ m \geq 0$ be polynomials with coefficients in the ring $\mathbb{A}$. Applying the Euclidean division to $T^k g(T)$ and $f(T)$ we get

$$T^k g(T) \equiv c_{k,0} + c_{k,1}T + \dots + c_{k,n-1}T^{n-1} \mod f(T) \text{ for } k = 0, 1, \dots, n-1$$

Proposition 5.1. $\underset{n,m}{R}(f,g) = \det[c_{k,l}]_{k,l=0,1,\dots,n-1}$

Proof. It suffices to check the proposition for polynomials $F(1, \overrightarrow{A'}, T) = T^n + A_1T^{n-1} + \dots + A_n$ and $G(\overrightarrow{B}, T) = B_0T^m + \dots + B_m$ where $\overrightarrow{A'} = (A_1, \dots, A_n)$ and $\overrightarrow{B} = (B_0, \dots, B_m)$ are variables. Then we have

$$\begin{aligned} T^k G(\overrightarrow{B}, T) &\equiv c_{k,0}(\overrightarrow{A'}, \overrightarrow{B}) + c_{k,1}(\overrightarrow{A'}, \overrightarrow{B})T + \dots + \\ &\quad + c_{k,n-1}(\overrightarrow{A'}, \overrightarrow{B})T^{n-1} \mod F(1, \overrightarrow{A'}, T),\ \text{for } k = 0, 1, \dots, n-1 \end{aligned}$$

Therefore

$$\begin{gathered} \left(c_{k,0}(\overrightarrow{A'}, \overrightarrow{B}) - G(\overrightarrow{B}, T)\right) + \dots + c_{0,n-1}(\overrightarrow{A'}, \overrightarrow{B})T^{n-1} \mod F(1, \overrightarrow{A'}, T) \\ \vdots \\ c_{n-1,0}(\overrightarrow{A'}, \overrightarrow{B}) + \dots + \left(c_{n-1,n-1}(\overrightarrow{A'}, \overrightarrow{B}) - G(\overrightarrow{B}, T)\right)T^{n-1} \mod F(1, \overrightarrow{A'}, T) \end{gathered}$$

By Cramer's rule we get

$$\det\left[c_{k,l}(\overrightarrow{A'}, \overrightarrow{B}) - \delta_{k,l}G(\overrightarrow{B}, T)\right] \equiv 0 \mod F(1, \overrightarrow{A'}, T)$$

Let $P(\overrightarrow{A'}, \overrightarrow{B}, Z) = \det \left[c_{k,l}(\overrightarrow{A'}, \overrightarrow{B}) - \delta_{k,l} Z \right] \in \mathbb{Z}[\overrightarrow{A'}, \overrightarrow{B}][Z]$ Then

$$P(\overrightarrow{A'}, \overrightarrow{B}, Z) = (-1)^n Z^n + \text{terms of degree} < n \text{ in } Z,$$

and

$$P(\overrightarrow{A'}, \overrightarrow{B}, G(\overrightarrow{B}, T)) \equiv 0 \mod F(1, \overrightarrow{A'}, T)$$

Let $a(\overrightarrow{X}) = (a_1(\overrightarrow{X}), \ldots, a_n(\overrightarrow{X}))$ be elementary symmetric functions in $\overrightarrow{X} = (X_1, \ldots, X_n)$. Then $F(1, a(\overrightarrow{X}), X_i) = 0$ (for $i = 1, \ldots, n$) and $P(a(\overrightarrow{X}), \overrightarrow{B}, G(\overrightarrow{B}, X_i)) = 0$ for $i = 1, \ldots, n$. Therefore we get $P(a(\overrightarrow{X}), \overrightarrow{B}, Z) = (-1)^n (Z - G(\overrightarrow{B}, X_1)) \ldots (Z - G(\overrightarrow{B}, X_n))$ which implies the identity

$$\det \left[c_{k,l}(a(\overrightarrow{X}), \overrightarrow{B}) \right] = G(\overrightarrow{B}, X_1) \ldots G(\overrightarrow{B}, X_n)$$

By Proposition 4.2(ii) $R(1, a(\overrightarrow{X}), \overrightarrow{B}) = G(\overrightarrow{B}, X_1) \ldots G(\overrightarrow{B}, X_n)$, therefore

$$\det \left[c_{k,l}(a(\overrightarrow{X}), \overrightarrow{B}) \right] = R(1, a(\overrightarrow{X}), \overrightarrow{B})$$

and

$$\det \left[c_{k,l}(\overrightarrow{A'}, \overrightarrow{B}) \right] = R(1, \overrightarrow{A'}, \overrightarrow{B})$$

by algebraic independence of elementary symmetric functions. $\square$

Remark 5.2. Let $\mathbb{B} = {}^{\mathbb{A}}/_{(f(T))}$. Then $\mathbb{B}$ is a finite free module with basis $[1]$, $[T]$, ..., $[T^{n-1}]$ where $[p(T)]$ is the image of $p(T) \in \mathbb{A}[T]$ by the homomorphism $\mathbb{A}[T] \mapsto \mathbb{B}$. Proposition 5.1 can be rewritten in the following form

$$\text{Norm}_{\mathbb{B}/\mathbb{A}}([g(T)]) = \underset{n,m}{R}(f, g).$$

6 The resultant and Jacobian

For any sequence of polynomials $P_1, \ldots, P_r \in \mathbb{A}[X_1, \ldots, X_n]$ we consider the Jacobian matrix

$$\frac{J(P_1, \ldots, P_r)}{J(X_1, \ldots, X_n)} = \begin{bmatrix} \frac{\partial P_1}{\partial X_1} & \frac{\partial P_2}{\partial X_1} & \ldots & \frac{\partial P_r}{\partial X_1} \\ \vdots & & & \\ \frac{\partial P_1}{\partial X_n} & \frac{\partial P_2}{\partial X_n} & \ldots & \frac{\partial P_r}{\partial X_n} \end{bmatrix}$$

Let $F(\overrightarrow{A}, T) = A_0 T^n + \ldots + A_n$, $G(\overrightarrow{B}, T) = B_0 T^m + \ldots + B_m$ and let us consider the identity

$$F(\overrightarrow{A}, T) G(\overrightarrow{B}, T) = Q_0(\overrightarrow{A}, \overrightarrow{B}) T^{m+n} + Q_1(\overrightarrow{A}, \overrightarrow{B}) T^{m+n-1} + \ldots + Q_{m+n}(\overrightarrow{A}, \overrightarrow{B})$$

in the ring $\mathbb{Z}[\overrightarrow{A}, \overrightarrow{B}][T]$ $(\star)$

One has $Q_0(\overrightarrow{A}, \overrightarrow{B}) = A_0B_0$, $Q_1(\overrightarrow{A}, \overrightarrow{B}) = A_0B_1 + A_1B_0$, …, $Q_{m+n}(\overrightarrow{A}, \overrightarrow{B}) = A_nB_m$

Proposition 6.1. *Let $R(\overrightarrow{A}, \overrightarrow{B})$ be the resultant of polynomials $F(\overrightarrow{A}, T)$, $G(\overrightarrow{A}, T)$. Then*

$$R(\overrightarrow{A}, \overrightarrow{B}) = (-1)^{mn} \det \frac{J(Q_1, \ldots, Q_{m+n})}{J(A_1, \ldots, A_n, B_1, \ldots, B_m)}$$

Proof. Differentiating the identity $(\star)$ with respect to the variables $B_1, \ldots, B_m, A_1, \ldots, A_n$ we get

$$\begin{aligned}
T^{m-1}F(\overrightarrow{A}, T) &= \frac{\partial Q_1}{\partial B_1}T^{m+n-1} + \frac{\partial Q_2}{\partial B_1}T^{m+n-2} + \ldots + \frac{\partial Q_{m+n}}{\partial B_1} \\
&\vdots \\
F(\overrightarrow{A}, T) &= \frac{\partial Q_1}{\partial B_m}T^{m+n-1} + \frac{\partial Q_2}{\partial B_m}T^{m+n-2} + \ldots + \frac{\partial Q_{m+n}}{\partial B_m} \\
T^{n-1}G(\overrightarrow{B}, T) &= \frac{\partial Q_1}{\partial A_1}T^{m+n-1} + \frac{\partial Q_2}{\partial A_1}T^{m+n-2} + \ldots + \frac{\partial Q_{m+n}}{\partial A_1} \\
&\vdots \\
G(\overrightarrow{B}, T) &= \frac{\partial Q_1}{\partial A_n}T^{m+n-1} + \frac{\partial Q_2}{\partial A_n}T^{m+n-2} + \ldots + \frac{\partial Q_{m+n}}{\partial A_n}
\end{aligned}$$

We see that the Sylwester matrix of the pair $F(\overrightarrow{A}, T), G(\overrightarrow{B}, T) \in \mathbb{Z}[\overrightarrow{A}, \overrightarrow{B}][T]$ is

$$\frac{J(Q_1, \ldots, Q_{m+n})}{J(B_1, \ldots, B_m, A_1, \ldots, A_n)}$$

and its determinant $R(\overrightarrow{A}, \overrightarrow{B})$ equals to

$$(-1)^{mn}\frac{J(Q_1, \ldots, Q_{m+n})}{J(A_1, \ldots, A_n, B_1, \ldots, B_m)}$$

□

Remark 6.2. The formula for the resultant proved above is of the kind "well-known and worth being known better". We don't know any classical text with this formula. The first reference (in the case of monic polynomials) we found is John's Nash article [Nash 1952]

7 Discriminants

Let us consider the general polynomial $F(\overrightarrow{A}, T) = A_0T^n + A_1T^{n-1} + \ldots + A_n$, $\overrightarrow{A} = (A_0, \ldots, A_n)$ of degree $n > 0$ and its derivative $\frac{dF}{dT}(\overrightarrow{A}, T) = nA_0T^{n-1} +$

$(n-1)A_1T^{n-2} + \ldots + A_{n-1}$. Then

$$\underset{n,n-1}{R}\left(F, \frac{dF}{dT}\right) = R(A_0, \ldots, A_n, nA_0, \ldots, A_{n-1}) \in \mathbb{Z}[\overrightarrow{A}]$$

Lemma 7.1. *The variable A_0 divides $\underset{n,n-1}{R}\left(F, \frac{dF}{dT}\right)$ in the ring $\mathbb{Z}[\overrightarrow{A}]$.*

Proof. The first column of the Sylvester matrix of the pair $F, \frac{dF}{dT}$ is

$$\begin{bmatrix} A_0 \\ \vdots \\ nA_0 \\ \vdots \end{bmatrix}$$

where the dots replace zeros. Whence follows the lemma. □

By Lemma 7.1 there is a unique polynomial $D_n(\overrightarrow{A}) \in \mathbb{Z}[\overrightarrow{A}]$ such that

$$\underset{n,n-1}{R}(A_0, \ldots, A_n, nA_0, \ldots, A_{n-1}) = (-1)^{\binom{n}{2}} A_0 D_n(\overrightarrow{A}) \in \mathbb{Z}[\overrightarrow{A}]$$

We call $D_n(\overrightarrow{A})$ the discriminant of the general polynomial $F(\overrightarrow{A}, T)$.

Remark 7.2. By definition $\binom{n}{2} = \frac{n(n-1)}{2}$, in particular $\binom{1}{2} = 0$ and it is easy to check that $D_1(A_0, A_1) = 1$. A simple calculation (exercise!) shows that $D_2(A_0, A_1, A_2) = A_1^2 - 4A_0A_2$.

Proposition 7.3. *The discriminant $D_n(\overrightarrow{A}) \in \mathbb{Z}[\overrightarrow{A}]$ is a homogeneous polynomial of degree $2n-2$. If weight $A_i = i$ for $i = 0, 1, \ldots, n$ then the weight of any term of $D_n(\overrightarrow{A})$ is equal to $n(n-1)$.*

Proof. Let Z be a variable. Prom Property 3.4 we get

$$R(ZA_0, \ldots, ZA_n, nZA_0, \ldots, ZA_{n-1}) = Z^{2n-1}R(A_0, \ldots, A_n, nA_0, \ldots, A_{n-1})$$

in $\mathbb{Z}[\overrightarrow{A}, Z]$. Now from the definition of the dicriminant we obtain

$$D_n(ZA_0, \ldots, ZA_n) = Z^{2n-2}D_n(A_0, \ldots, A_n)$$

which proves the first part of the proposition. The second part we prove in a similar way using Property 3.5. □

Let $\mathbb{A}$ be a ring without zero divisors. For any polynomial $f(T) = a_0T^n + a_1T^{n-1} + \ldots + a_n \in \mathbb{A}[T]$ of degree $n > 0$ we put $D(f) = D_n(a_0, a_1, \ldots, a_n) \in \mathbb{A}$ and call $D(f)$ discriminant of f.

Property 7.4.
$$\underset{n,n-1}{R}(f,f') = (-1)^{\binom{n}{2}} a_0 D(f)$$

Proof. Obvious. $\square$

Property 7.5. *If $f(T) = a_0(T-c_1)\dots(T-c_n)$, $a_0 \neq 0$ in $\mathbb{A}[T]$, then*
$$D(f) = a_0^{2n-2} \prod_{1\leq i<j\leq n} (c_i - c_j)^2$$

Proof. By Corollary 4.3 we have that $\underset{n,n-1}{R}(f,f') = a_0^{n-1} f'(c_1)\dots f'(c_n)$. Since
$$f(T) = a_0(T-c_2)\dots(T-c_n) + \dots + a_0(T-c_1)\dots(T-c_{n-1})$$
we get
$$\begin{aligned} f'(c_1) &= a_0(c_1-c_2)\dots(c_1-c_n) \\ f'(c_2) &= (-1)a_0(c_1-c_2)(c_2-c_3)\dots(c_2-c_n) \\ &\vdots \\ f'(c_n) &= (-1)^{n-1}(c_1-c_n)(c_2-c_n)\dots(c_{n-1}-c_n) \end{aligned}$$
and
$$\underset{n,n-1}{R}(f,f') = a_0^{n-1}(-1)^{\binom{n}{2}} a_0^n \prod_{1\leq i<j\leq n}(c_i-c_j)^2$$
It suffices to apply Property 7.4 $\square$

Remark 7.6. Let $f(T) = a_0T^n + a_1T^{n-1} + \dots + a_n \in \mathbb{A}[T]$. Suppose that $f'(T) = na_0(T-d_1)\dots(T-d_{n-1})$ in $\mathbb{A}[T]$, $na_0 \neq 0$. Then
$$D(f) = (-1)^{\binom{n}{2}} n^n a_0^{n-1} f(d_1)\dots f(d_{n-1}) \text{ (exercise!)}$$

Property 7.7. *If $f(T), g(T) \in \mathbb{A}[T]$ are of degree $n > 0$ and $m > 0$ respectively then*
$$D(fg) = D(f)D(g)\underset{n,m}{R}(f,g)^2$$

Proof. Let $\tilde{\mathbb{A}}$ be an extension of the ring $\mathbb{A}$ such that $f(T) = a_0(T-c_1)\dots(T-c_n)$, $g(T) = b_0(T-d_1)\dots(T-d_m)$ with $a_0 \neq 0$ and $b_0 \neq 0$. Then the property follows from Property 7.5 and Corollary 4.4 $\square$

In the sequel we need the following

Lemma 7.8. *Suppose that $\mathbb{A}$ is a factorial ring of characteristic zero and let $f(T) = a_0T^n + a_1T^{n-1} + \ldots + a_n \in \mathbb{A}[T]$ be a polynomial of degree $n > 0$. Then for every irreducible polynomial $p(t) \in \mathbb{A}[T]$ of degree > 0: p^2 divides f if and only if p divides f and f'*

Proof. If $f = p^2h$, then $f' = p(2p'h + ph)$ and p divides f and f'. Suppose that p divides f and f' and write $f = pg$ in $\mathbb{A}[T]$. Then $f' = p'g + pg'$ and p divides $p'g$ since p divides f'. The polynomial p is of degree > 0, consequently if does not divide p' and p divides g; in $\mathbb{A}[T]$ any irreducible element is prime. Thus p^2 divides f which proves the lemma. $\square$

Proposition 7.9. *Let $f(T) = a_0T^n + a_1T^{n-1} + \ldots + a_n \in \mathbb{A}[T]$, $a_0 \neq 0$ be a polynomial with coefficients in a factorial ring $\mathbb{A}$ of characteristic zero. Then $D(f) = 0$ if and only if f has a multiple factor of degree > 0 in $\mathbb{A}[T]$.*

Proof. By Property 7.4 the condition $D(f) = 0$ means that $\underset{n,n-1}{R}(f, f') = 0$. Use Proposition 2.4 and Lemma 7.8 $\square$

APPENDIX

A Hensel's Lemma

Let $\mathbb{K}[[\overrightarrow{X}]]$ be the ring of formal power series in n variables $\overrightarrow{X} = (X_1, \ldots, X_n)$ with coefficients in a field $\mathbb{K}$. Let $\overrightarrow{P} = (P_1, \ldots, P_m) \in \mathbb{K}[[\overrightarrow{X}]][\overrightarrow{Y}]^m$ be a sequence of m polynomials in m variables $\overrightarrow{Y} = (Y_1, \ldots, Y_m)$ and let $\vec{c} = (c_1, \ldots, c_m) \in \mathbb{K}^m$

Lemma A.1 (Implicit Function Theorem for polynomials with coefficients in the ring of formal power series)**.** *Suppose that $\overrightarrow{P}(\overrightarrow{0}, \vec{c}) = \overrightarrow{0}$ and $\frac{J(P_1,\ldots,P_m)}{J(Y_1,\ldots,Y_m)}(\overrightarrow{0}, \overrightarrow{c}) \neq 0$. Then there exists a unique sequence of formal power series $\vec{y}(\vec{x}) = (y_1(\vec{x}), \ldots, y_m(\vec{x})) \in \mathbb{K}[[\vec{x}]]^m$ such that $\vec{y}(\overrightarrow{0}) = \vec{c}$ and $\overrightarrow{P}(\vec{x}, \vec{y}(\vec{x})) = \overrightarrow{0}$ in $\mathbb{K}[[\vec{x}]]^m$.*

Proof. Use the Implicit Functions Theorem for formal power series to the system of equations $\overrightarrow{P}(\overrightarrow{X}, \vec{c} + \overrightarrow{Z}) = \overrightarrow{0}$ with unknowns $\overrightarrow{Z} = (Z_1, \ldots, Z_m)$. $\square$

Proposition A.2 (Hensel's Lemma)**.** *Let $F(\overrightarrow{X}, Y) \in \mathbb{K}[[\overrightarrow{X}]][Y]$ be a polynomial in Y of degree $N > 1$. Suppose that $F(\overrightarrow{0}, Y) = (Y^n + a_1Y^{n-1} + \ldots + a_n)(b_0Y^m + b_1Y^{m-1} + \ldots + b_m)$ in $\mathbb{K}[Y]$ where $n, m > 0$, $n + m = N$ is a decomposition of $F(\overrightarrow{0}, Y)$ in $\mathbb{K}[Y]$ into the **coprime** factors.*
Then

$$F(\overrightarrow{X}, Y) = (Y^n + a_1(\overrightarrow{X})Y^{n-1} + \ldots + a_n(\overrightarrow{X}))(b_0(\overrightarrow{X})Y^m + b_1(\overrightarrow{X})Y^{m-1} + \ldots + b_m(\overrightarrow{X})) \text{ in } \mathbb{K}[[\overrightarrow{X}]][Y],$$

where $a_i(\overrightarrow{0}) = a_i$ for $i = 1, \ldots, n$ and $b_j(\overrightarrow{0}) = b_j$ for $j = 0, \ldots, m$. The above factorization is unique.

Proof. Let $F(\overrightarrow{X}, Y) = c_0(\overrightarrow{X})Y^N + c_1(\overrightarrow{X})Y^{N-1} + \ldots + c_N(\overrightarrow{X})$, $c_0(\overrightarrow{X}) \neq 0$. If the decomposition of $F(\overrightarrow{X}, Y)$ exists we have $b_0(\overrightarrow{X}) = c_0(\overrightarrow{X})$. The substitution 1 for A_0 and $c_0(\overrightarrow{X})$ for B_0 in the identity

$$(A_0T^n + A_1T^{n-1} + \ldots + A_n)(B_0T^m + B_1T^{m-1} + \ldots + B_m) = \\ Q_0(A,B)T^{n+m} + Q_1(A,B)T^{n+m-1} + \ldots + Q_{n+m}(A,B)$$

gives

$$(T^n + A_1T^{n-1} + \ldots + A_n)(c_0(\overrightarrow{X})T^m + B_1T^{m-1} + \ldots + B_m) = \\ c_0(\overrightarrow{X})T^{n+m} + Q_1(1, A_1, \ldots, A_n, c_0(\overrightarrow{X}), B_1, \ldots, B_m)T^{n+m-1} + \ldots \\ + Q_{n+m}(1, A_1, \ldots, A_n, c_0(\overrightarrow{X}), B_1, \ldots, B_m)$$

To get the factorization of $F(\overrightarrow{X}, Y)$ state in Hensel's Lemma we have to solve in $\mathbb{K}[[\overrightarrow{X}]]$ the system of equations

$$\begin{aligned} Q_1(1, A_1, \ldots, A_n, c_0(\overrightarrow{X}), B_1, \ldots, B_m) - c_1(\overrightarrow{X}) &= 0 \\ Q_2(1, A_1, \ldots, A_n, c_0(\overrightarrow{X}), B_1, \ldots, B_m) - c_2(\overrightarrow{X}) &= 0 \\ &\vdots \\ Q_{n+m}(1, A_1, \ldots, A_n, c_0(\overrightarrow{X}), B_1, \ldots, B_m) - c_{n+m}(\overrightarrow{X}) &= 0 \end{aligned}$$

with unknowns $A_1, \ldots, A_n, B_1, \ldots, B_m$. Let $\vec{a} = (a_1, \ldots, a_n)$, $\vec{b} = (b_1, \ldots, b_m)$. Using Proposition 6.1 we check that the above system satisfies the assumptions of Lemma A.1 at point $(\overrightarrow{0}, \vec{a}, \vec{b})$. Therefore there exists unique power series $a_1(\overrightarrow{X}), \ldots, a_n(\overrightarrow{X}), b_1(\overrightarrow{X}), \ldots, b_m(\overrightarrow{X})$ such that

$$Q_k(1, a_1(\overrightarrow{X}), \ldots, a_n(\overrightarrow{X}), c_0(\overrightarrow{X}), b_1(\overrightarrow{X}), \ldots, b_m(\overrightarrow{X})) = c_k(\overrightarrow{X})$$

for $k = 1, \ldots, n+m$ and $a_i(\overrightarrow{0}) = a_i,\ i = 1, \ldots n$, $b_j(\overrightarrow{0}) = b_j,\ j = 1, \ldots m$. $\square$

Corollary A.3 (The Weierstrass Preparation Theorem for Polynomials)**.** *Let $F(\overrightarrow{X}, Y) \in \mathbb{K}[[\overrightarrow{X}]][Y]$ be a polynomial of degree $N > 0$ and let $M = ord_0 F(\overrightarrow{0}, Y)$. Suppose that $0 < M < +\infty$. Then*

$$F(\overrightarrow{X}, Y) = (Y^m + a_1(\overrightarrow{X})Y^{M-1} + \ldots + a_M(\overrightarrow{X}))U(\overrightarrow{X}, Y) \ \textit{in}\ \mathbb{K}[[\overrightarrow{X}]][Y],$$

where $a_i(\overrightarrow{0}) = 0$ for $i = 1, \ldots, M$ and $U(\overrightarrow{0}, 0) \neq 0$. The above factorization is unique.

Proof. Let $F(\overrightarrow{X}, Y) = c_0(\overrightarrow{X})Y^N + c_1(\overrightarrow{X})Y^{N-1} + \ldots + c_N(\overrightarrow{X})$. Then

$$F(\overrightarrow{0}, Y) = c_0(\overrightarrow{0})Y^N + c_1(\overrightarrow{0})Y^{N-1} + \ldots + c_{N-M}(\overrightarrow{0})Y^M = \\ Y^M \left(c_0(\overrightarrow{0})Y^{N-M} + \ldots + c_{N-M}(\overrightarrow{0})\right),$$

where $c_{N-M}(\overrightarrow{0}) \neq 0$. If $M = N$ then we put $U(\overrightarrow{X}, Y) = c_0(\overrightarrow{X})$ and the corollary is obvious. If $M < N$ then we use Hensel's Lemma A.2. $\square$

B Bezout's Theorem for affine plane curves

Let $\mathbb{K}$ be any algebraically closed field. For any two power series $F, G \in \mathbb{K}[[X,Y]]$ we consider their intersection multiplicity $i_0(F,G)$ (see [Pł 2013], Section 3).

Proposition B.1. *Let $F(X,Y) = Y^n + a_1(X)Y^{n-1} + \ldots + a_n(X) \in \mathbb{K}[[X]][Y]$ be a distinguished polynomial and let $R(X)$ be Y–resultant of $F(X,Y)$ and $G(X,Y)$. Then*

$$\mathit{ord}\, R(X) = i_0(F,G)$$

Proof. see [Pł 2013], Proposition 3.9 $\square$

For any polynomials $F, G \in \mathbb{K}[X,Y]$ and for any point $p = (a,b) \in \mathbb{K}^2$ we put

$$i_p = i_0(F(a+X, b+Y), G(a+X, b+Y)).$$

Note that $i_p(F,G) > 0$ if and only if $F(p) = G(p) = 0$.

Theorem B.2 (Affine Bezout's Theorem)**.** *Let $F(X,Y)$ and $G(X,Y)$ be coprime polynomials of degree $m > 0$ and $n > 0$ with coefficients in an algebraically closed field $\mathbb{K}$. Then*

(i) $\sum_{p \in \mathbb{K}^2} i_p(F,G) \leq mn$,

(ii) $\sum_{p \in \mathbb{K}^2} i_p(F,G) = mn$ *if and only if the system of equations* $F^+ = G^+ = 0$ *have only the trivial solution* $x = y = 0$.

The proof of Bezout's theorem is based on properties of intersection multiplicity, especially on Proposition B.1.

Proposition B.3. *Let F, G be polynomials of degree $m, n > 0$ such that $\mathit{deg}_Y F = m$ and $\mathit{deg}_Y G = n$. Let $R(X) = Y$–resultant of polynomials $F(X,Y)$, $G(X,Y)$. Then for any $a \in \mathbb{K}$:*

(i) $\mathit{ord}_a R(X) = \sum_{p \in \{a\} \times \mathbb{K}} i_p(F,G)$,

(ii) $\mathit{deg}\, R(X) = \sum_{p \in \mathbb{K}^2} i_p(F,G)$

Proof. Formula (ii) follows from (i) since deg $R(X) = \sum_{a \in \mathbb{K}} \mathrm{ord}_a R(X)$. To check (i) it suffices to consider the case $a = 0$ since $\mathrm{ord}_a R(X) = \mathrm{ord}_0 R(X+a)$ and $R(X+a)$ is the Y–resultant of polynomials $F(a+X,Y)$, $G(a+X,Y)$. Suppose that $a = 0$. If $\mathrm{ord}_0 R = 0$ or ∞ property (i) is obvious. Suppose then $0 < \mathrm{ord}_0 R < \infty$ i.e. $R(0) = 0$ and $R(X) \neq 0$ in $\mathbb{K}[X]$. Let $(0, b_1)$, …, $(0, b_s)$ be a pairwise different solutions of the system $F(0,y) = G(0,y) = 0$. By Hensel's

Lemma we get $F(X,Y) = \prod_{i=1}^{s+1} F_i(X,Y)$, $G(X,Y) = \prod_{i=1}^{s+1} G_i(X,Y)$ where $F_i, G_i \in \mathbb{K}[[X]][Y]$ are such that $F_i(0,Y) = (Y - b_i)^{m_i}$, $G_i(0,Y) = (Y - b_i)^{n_i}$ for $i = 1, \ldots, s$ and $F_{s+1}(0, b_i)G(0, b_i) \neq 0$ for $i = 1, \ldots, s$. Denote by $R_{ij}(X)$ the Y–resultant of $F_i(X,Y)$ $G_j(X,Y)$. Thus $R(X) = \prod i, j R_{ij}(X)$ with $R_{ij}(0) \neq 0$ if $i \neq j$ or $i = j = s+1$ since $R_{ij}(0)$ is the Y–resultant of polynomials $F_i(0,Y)$, $G_j(0,Y)$. $\mathrm{ord}_0 R(X) = \sum_{i=1}^{s} \mathrm{ord}_0 R_{ii}(X)$. We get

$$\begin{aligned}\mathrm{ord}_0 R_{ii}(X) &= \mathrm{ord}_0(Y\text{–resultant } F_i(X,Y), G_i(X,Y)) = \\ &= \mathrm{ord}_0(Y\text{–resultant } F_i(X, Y + b_i), G_i(X, Y + b_i)) = \\ &= i_{(0,0)}(F_i(X, Y + b_i), G_i(X, Y + b_i)) = i_{(0,0)}(F, G).\end{aligned}$$

Thus $\mathrm{ord}_0 R(X) = \sum\limits_{i=1}^{s} i_{(0,b_i)}(F,G)$ and we are done. $\square$

Let F^+ be the leading form of F, i.e. the sum of monomials of degree $\deg F$ which appear in F.

Proposition B.4. *Let $F = F(X,Y)$ and $G = G(X,Y)$ be polynomials of degree $n > 0$ and $m > 0$ such that $\deg_Y F = n$, $\deg_Y G = m$. Let $R(X) = Y$–resultant of $F(X,Y)$ and $G(X,Y)$ and $r = Y$–resultant of $F^+(1,Y)$ and $G^+(1,Y)$. Then*

$$R(X) = rX^{mn} + \ldots + \text{(monomials of degree} < mn)$$

Proof. Without diminishing the generality we may assume $F = Y^n + a_1(X)Y^{n-1} + \ldots + a_n(X)$ and $G = Y^m + b_1(X)Y^{m-1} + \ldots + b_m(X)$ where $a_i(X), b_j(X)$ are polynomials of degree $\leq i$ and $\leq j$. Let $R(A_1, \ldots, A_n, B_1, \ldots, B_m)$ be Y–resultant of polynomials $Y^n + A_1Y^{n-1} + \ldots + A_n$ and $Y^m + B_1Y^{m-1} + \ldots + B_m$ with variable coefficients $A_1, \ldots, A_m$, $B_1, \ldots, B_n$. We have then $R(tA_1, \ldots, t^nA_n, tB_1, \ldots, t^mB_m) = t^{mn}R(A_1, \ldots, A_n, B_1, \ldots, B_m)$ (the resultant is quasi–homogeneous) hence

$$(\star) \qquad \begin{aligned}\frac{R(X)}{X^{mn}} &= \frac{1}{X^{mn}} R(a_1(X), \ldots, a_n(X), b_1(X), \ldots, b_m(X)) = \\ &= R\left(\frac{a_1(X)}{X}, \ldots, \frac{a_n(X)}{X^n}, \frac{b_1(X)}{X}, \ldots, \frac{b_m(X)}{X^m}\right).\end{aligned}$$

Let us consider the place of field of rational functions $\mathbb{K}(X)$ defined be the valuation $v = -\deg$. It is the mapping $F(X) \mapsto F(\infty)$ of the field $\mathbb{K}(X)$ in the set $\hat{\mathbb{K}} = \mathbb{K} \cup \{\infty\}$ defined as follows: if $F(X) = \frac{A(X)}{B(X)}$ where $A(X) = a_0x^p + \ldots$, $B(X) = b_0X^q + \ldots$ are polynomials of degree $p \geq 0$ and $q \geq 0$ then $F(\infty) = \frac{a_0}{b_0}$ if $p = q$, $F(\infty) = 0$ if $p < q$ and $F(\infty) = \infty$ if $p > q$. Let us write $a_i(X) = a_{i0}X^i + \ldots$, $b_j(X) = b_{j0}X^j + \ldots$. Then $\left.\frac{a_i(X)}{X^i}\right|_{X=\infty} = a_{i0}$, $\left.\frac{b_j(X)}{X^j}\right|_{X=\infty} = b_{j0}$ and from equality $(\star)$ it follows

$$(\star\star) \qquad \frac{R(X)}{X^{mn}} = R(a_{10}, \ldots, a_{m0}, b_{10}, \ldots, b_{n0}) = r$$

Hence $R(X) = rX^{mn} + \ldots$ which proves the proposition. $\square$

We may present now the proof of Bezout's Theorem.

Proof of Bezout's Theorem. We keep the notation introduced above. The sum $\sum_{p\in\mathbb{K}^2} i_p(F,G)$ does not depend on the choice of affine coordinates. Thus we may suppose that $\deg_Y F = m$, $\deg_Y G = n$. We get then (Proposition B.3(ii) and Proposition B.4) $\sum_{p\in\mathbb{K}^2} i_p(F,G) = \deg\, R(X) \leq mn$ with equality if and only if $r \neq 0$ i.e. if the system of equations $F^+(1,Y) = G^+(1,Y) = 0$ does not have solution. $\square$

References

[Abh 2006] S.S. Abhyankar, Lectures on Algebra I, Word Scientific 2006

[Apéry–Jouan 2007] F. Apéry, J.P. Jouanolou, Élimination. Le cas d'me variable, Hermann 2007

[Nash 1952] J. Nash, Real Algebraic Manifolds, Annals of Math. vol. 56, No. 3, November 1952, page 412.

[Pł 1980] A. Płoski, Remarque sur le lemme de Hensel, Bull. Acad. Polon. Sci. Sér. Sci. Math. , 28(1980), n^o 3–4, 115–116

[Pł 2013] A. Płoski, Introduction to the local theory of plane algebraic curves, Analytic and Algebraic Geometry, eds. T. Krasiński and St. Spodzieja, Łódź University Press 2013, 115–134

Department of Mathematics and Phycics
Kielce University of Technology
Al. 1000 L PP 7
25-314 Kielce
Poland
e–mail: matap@tu.kielce.pl