MMA: sūgaku tokuron I. Lecture VI
Resultant and applications (Part II)

Xavier Dahan, 2010, June 17th & 24th

1 Intersection of 2 curves

R is a commutative ring, that is an integral domain (like $R = \mathbb{Z}$, $R = k[X]$ etc.).

We have seen (Slide 2) that the Sylvester matrix of 2 polynomials A and B in $R[X]$ represents the linear map $(f, g) \mapsto Af + Bg$ (in a relevant basis...). Actually the resultant of A and B is in the *image* of this linear map. Precisely, there is the following proposition:

Proposition 2 *There exists $U \in R[X]_{<n}$ and $V \in R[X]_{<m}$ such that*

$$AU + BV = \mathsf{Res}(A, B)$$

Moreover U and V are polynomials in $\mathbb{Z}[\text{coefficients of } A \text{ and coefficients of } B]$.

Proof: By construction, $\mathsf{Syl}(A, B) \in \mathrm{Mat}_{n+m}(R)$. Let us *extend the scalars* from R to $R[X]$, so that $\mathsf{Syl}(A, B) \in \mathrm{Mat}_{n+m}(R[X])$.

Let us write $\mathsf{Syl}(A, B) = \left(C_1 \mid C_2 \mid \cdots \mid C_{n+m} \right)$, where C_i represents the i-th column in $R[X]^{n+m}$ of $\mathsf{Syl}(A, B)$.

Recall that the determinant of a matrix *does not* change if we add to a column a linear combination of the others.

Hence we perform this replacement: $C'_{m+n} \leftrightarrow C_1 X^{n+m-1} + C_2 X^{n+m-2} + \cdots + C_{n+m-1} X + C_{n+m}$, to obtain:

$$M = \left(\begin{array}{cccccc|l}
a_m & a_{m-1} & & a_1 & a_0 & & a_m X^{n+m-1} + \cdots + a_1 X^n + a_0 X^{n-1} \\
 & a_m & & & & a_0 & a_m X^{n+m-2} + \cdots + a_0 X^{n-2} \\
 & & \ddots & & & \ddots & \\
 & & & a_m & & a_1 & a_m X^m + \cdots + a_1 X + a_0 \\
b_n & b_{n-1} & & & b_0 & & b_n X^{n+m-1} + \cdots + b_0 X^{m-1} \\
 & b_n & & & & b_0 & b_n X^{n+m-2} + \cdots + b_0 X^{m-2} \\
 & & \ddots & & & \ddots & \\
 & & & b_n & & b_1 & b_n X^n + \cdots + b_1 X + b_0
\end{array} \right)$$

We can see that: $C'_{m+n} = {}^t(\underbrace{X^{n-1}A, X^{n-1}A, \ldots, XA, A}_{n}, \underbrace{X^{m-1}B, \ldots, XB, B}_{m})$.

Moreover, the determinant of M is unchanged equal to $\det \mathsf{Syl}(A,B) = \mathsf{Res}(A,B)$. We compute it by developing along the column C'_{m+n}. Let M_i be the $(i, n+m)$ cofactor matrix of M, obtained by removing the i-th line and the $m+n$-th column of M:

$$\mathsf{Res}(A,B) = \sum_{\ell=1}^{n} (-1)^{m+n+\ell} X^{m-\ell} A \det M_\ell + \sum_{\ell=1}^{m} (-1)^{m+n+\ell} X^{n-\ell} B \det M_{n+\ell}.$$

Let $U = \sum_{\ell=1}^{n} (-1)^{m+n+\ell} X^{m-\ell} \det M_\ell$ and let $V = \sum_{\ell=1}^{m} (-1)^{m+n+\ell} X^{n-\ell} \det M_{n+\ell}$, so that $\mathsf{Res}(A,B) = AU + BV$. This proves the fist part of the theorem. Next, since X does not appear in each cofactor matrix M_i, we have $\det M_i \in R$ and $\deg(U) < m$ and $\deg(V) < n$, as required.

Finally since $\det M_\ell \in \mathbb{Z}$[coefficients of A and B] we also have $U, V \in \mathbb{Z}$[coefficients of A and B]. □

We consider two plane curves $\mathcal{C}_A$ and $\mathcal{C}_B$ defined by polynomials A and B in $\Bbbk[X.Y]$. Let us write $\left| \begin{array}{lcl} A & = & a_0(X) + a_1(X)Y + \cdots + a_{m-1}(X)Y^{m-1} + a_m(X)Y^m \\ B & = & b_0(X) + b_1(X)Y + \cdots + b_n(X)Y^n \end{array} \right.$. The following proposition 3 gives information about the coordinates of the projection on the X-axis of the intersection points $\mathcal{C}_A \cap \mathcal{C}_B$. Before, one remark and a lemma:

Remark: $\mathsf{Res}_X(A,B)$ or $\mathsf{Res}_Y(A,B)$? If we see A and B as univariate polynomial in $R[Y]$ with coefficients in $R = \Bbbk[X]$ then the Sylvester matrix is constructed with its entries in $R = \Bbbk[X]$, and the resultant is an element of $R = \Bbbk[X]$. We have eliminated Y, and we write $\mathsf{Res}_Y(A,B) \in \Bbbk[X]$.

If we see A and B as *univariate* polynomials $R[X]$ with coefficients in $R = \Bbbk[Y]$, then the Sylvester matrix has its entries in $R = \Bbbk[Y]$, and the resultant is in $R = \Bbbk[Y]$.

Lemma 5 *Let $A, B \in \Bbbk[X,Y]$. The polynomials A and B have a common factor in $\Bbbk[X,Y]$ if and only if $\mathsf{Res}_Y(A,B) = 0$.*

Proof: Corollary 1 says that A and B have certainly a common factor with coefficients in $\Bbbk(X) = \mathrm{Frac}(\Bbbk[X])$, if $\mathsf{Res}_Y(A,B) = 0$. Let $\tilde{D} \in \Bbbk(X)$ be a such a factor, and let us write:

$$A = \tilde{D}\tilde{A}_0 \qquad B = \tilde{D}\tilde{B}_0, \quad \text{with } \tilde{D}, \tilde{A}_0, \tilde{B}_0 \in \Bbbk(X)[Y].$$

The theorem of Gauss permits to conclude:

> **Gauss theorem:** Let $\mathbb{A}$ be an unique factorization domain. This means that factorization into prime is possible (like in $\mathbb{Z}$, $k[X_1, \ldots, X_n]$). Let $\mathbb{K} = \mathrm{Frac}(\mathbb{A})$ be the field of fractions of $\mathbb{A}$. Assume that $P \in \mathbb{A}[X]$ with $\deg(P) \geq 2$, admits the factorization $P = \tilde{Q}\tilde{R}$ over $\mathbb{K}$, i.e. $\tilde{Q} \in \mathbb{K}[X]$ and $\tilde{R} \in \mathbb{K}[X]$.
>
> Then P admits a factorization over $\mathbb{A}$; more precisely there exists, $Q \in \mathbb{A}[X]$ and $R \in \mathbb{A}[X]$ such that $P = QR$. Moreover R and Q are uniquely determined by $\tilde{R}$ and $\tilde{Q}$, and have the same degree.

We apply it with $\mathbb{A} = \Bbbk[X]$ and $\mathbb{K} = \Bbbk(X)$. There exists D, A_0 and B_0 in $\Bbbk[X,Y]$ uniquely determined by $\tilde{D}$, $\tilde{A}_0$ and $\tilde{B}_0$ and of the same degree, such that $A = DA_0$ and $B = DB_0$. □

The main result concerning the intersection points of the two curves is:

Proposition 3 *Let* $r(X) = \mathsf{Res}_Y(A,B) \in \mathbb{k}[X]$. *Let* $x \in \overline{\mathbb{k}}$ *be a root of* r. *Then, one of the two facts is true:*
(i) $a_m(x) = 0 = b_n(x)$ *or*
(ii) $\exists\, y \in \overline{\mathbb{k}}$ *such that* $(x,y) \in \mathcal{C}_A \cap \mathcal{C}_B$.

PROOF: Let $\phi_x : \overline{\mathbb{k}}[X] \to \overline{\mathbb{k}},\ P \mapsto P(x)$, be the evaluation map at x.

If $\phi_x(a_m) = 0$ and $\phi_x(b_n) = 0$, so that x is a common root of a_m and b_n and we are in case (i); then:

$$\begin{array}{rcl}\text{the first column of the matrix } \phi_x(\mathsf{Syl}(A,B)) \text{ is null} & \Longleftrightarrow & \det \phi_x(\mathsf{Syl}(A,B)) = 0 \\ & \Longleftrightarrow & \phi_x(\det(\mathsf{Syl}(A,B))) = 0 \\ & \Longleftrightarrow & \phi_x(\mathsf{Res}_Y(A,B)) = 0 = r(x)\end{array}$$

If $a_m(x) \neq 0$ or $b_n(x) \neq 0$ (not case (i)) say $a_m(x) \neq 0$, for example. Then by the specialization of the resultant (Proposition 1, second point) we have

$$\begin{array}{rcl} r(x) = \phi_x(\mathsf{Res}_Y(A,B)) & = & \phi_x(a_m)^{m-\deg_Y(\phi_x(A))}\mathsf{Res}(\phi_x(A), \phi_x(B)) \\ & = & a_m(x)^{\ell}\mathsf{Res}(A(x,Y), B(x,Y)). \end{array}$$

with $\ell = m - \deg_Y(A(x,Y))$. Because $a_m(x) \neq 0$,

$$\begin{array}{rrcl} & r(x) = 0 & \Longleftrightarrow & \mathsf{Res}(A(x,Y), B(x,Y)) = 0 \\ \text{by Lemma 5,} & & \Longleftrightarrow & A(x,Y) \text{ and } B(x,Y) \text{ have a common factor in } \overline{\mathbb{k}}[Y] \\ & & \Longleftrightarrow & \exists\, y \in \overline{\mathbb{k}} \text{ such that } A(x,y) = 0 = B(x,y), \end{array}$$

which proves that any root x of r not verifying Case (i), verifies Case (ii). □

REMARK: Cf Mathematica file "`Syl-2.nb`" for examples of intersections of 2 plane curves.

2 Vanishing polynomial of an algebraic number

(Cf. Mathematica file "`VanishPolyOnAlgNbr.nb`").

→ Algebraic numbers... review Lecture II !

Problem: Given an algebraic number $\alpha \in \overline{\mathbb{Q}}$, how to find a vanishing polynomial of α ? (i.e. a polynomial $P \in \mathbb{Q}[X]$ such that $P(\alpha) = 0$).

For $\alpha = \sqrt{2}$, then it is $X^2 - 2$. For $\alpha = \sqrt{2} + \sqrt{3}$, then $\alpha^2 = 2 + 2\sqrt{6} + 3$, so $(\alpha^2 - 5)^2 = 24$, and α is a root of $X^4 - 10X^2 + 1$.

What about $\alpha = 2^{2/3} + 2^{1/3} + 1$? It can be more difficult... There are *automated* ways to find a vanishing polynomial (not necessary the minimal polynomial).

Consider α and β two algebraic numbers with f and g for vanishing polynomials (i.e. $f(\alpha) = 0$ and $g(\beta) = 0$).

We write $(\alpha_i)_i$ and $(\beta_j)_j$ the *conjugate* roots of α and β (note that there is an i such that $\alpha_i = \alpha$ and a j such that $\beta_j = \beta$):

$$f = \prod_i X - \alpha_i, \qquad g = \prod_j X - \beta_j, \tag{1}$$

- Addition: $\alpha+\beta$? Let $\tilde{f}(X)=f(Y-X)$. By Equation (1) above, $\tilde{f}=\prod_i Y-(X+\alpha_i)$. Eq (1) of Slide 9 gives: $r(Y):=\mathsf{Res}_X(\tilde{f},g)=\prod_{i,j} Y-\alpha_i-\beta_j$. In particular $r(\alpha+\beta)=0$.

  Application (Cf. Mathematica file "`VanishPolyOnAlgNbr.nb`"): take $\alpha=\sqrt{2}$ and $\beta=\sqrt{3}$, then $f=X^2-2$ and $g=X^2-3$: $\mathsf{Res}_X((Y-X)^2-3,X^2-2)=Y^4-10Y^2+1$.

- Multiplication $\alpha\beta$? Let $\tilde{f}(X)=f(\frac{Y}{X})$. By Equation (1), it arrives $\tilde{f}(X)=\prod_i \frac{Y}{X}-\alpha_i$ and $X^{\deg(f)}\tilde{f}(X)\overset{(\bullet)}{=}\prod_i Y-\alpha_i X$. Recall that the sum of the roots $\sum_i \alpha_i$ and the product $\prod_i \alpha_i$ verify

$$f(X)=X^{\deg(f)}-(\alpha_1+\cdots+\alpha_{\deg(f)})X^{\deg(f)-1}+\cdots+(-1)^{\deg(f)}(\prod_i \alpha_i),$$

$$\Rightarrow \quad X^{\deg(f)}\tilde{f}=Y^{\deg(f)}-\big(\sum_i \alpha_i\big)Y^{\deg(f)-1}X+\cdots+(-1)^{\deg(f)}\big(\prod_i \alpha_i\big)X^{\deg(f)}.$$

  If we use the equality (4) of the main theorem 1 (Slide 9), we have:

$$r(Y)=\mathsf{Res}_x(X^{\deg(f)}f\left(\frac{Y}{X}\right),g(X))=(-1)^{\deg(g)\deg(f)}(\prod_i \alpha_i)^{\deg(g)}\prod_j \beta_j^{\deg(f)}\tilde{f}(\beta_j).$$

  Equality ($\bullet$) gives: $\beta_j^{\deg(f)}\tilde{f}(\beta_j)=\prod_i Y-\alpha_i\beta_j$, we get: $r(Y)=\pm\prod_{i,j} Y-\alpha_i\beta_j$. In particular $r(\alpha\beta)=0$.

  Application: $\alpha=\sqrt{2}+\sqrt{3}$ (so $f=X^4-10X^2+1$) and $\beta=19^{\frac{1}{7}}$ (so $g=X^7-19$). Then $\mathsf{Res}_X(Y^7-19X^7,\ X^4-10X^2+1)=Y^{28}-3362329730Y^{14}+130321$.

- Composition by a polynomial $h\in\mathbb{Q}[X]$. What is a vanishing polynomial of $h(\alpha)$? By the equality (3) of the main theorem (Slide 9) we have:

$$r(Y)=\mathsf{Res}_X(Y-h(X),f(X))=(-1)^{\deg(f)}\prod_{1\le i\le\deg(f)} Y-h(\alpha_i).$$

  In particular $r(h(\alpha))=0$.

  Application: $h(X)=X^2+X+1$, and $\alpha=2^{\frac{1}{3}}$. Then $\mathsf{Res}_X(Y-h(X),X^3-1)$ is a vanishing polynomial of $h(\alpha)=2^{2/3}+2^{1/3}+1$.

3 Computation of the resultant

We focus on resultants of bivariate polynomials in X,Y over a field $\mathbb{K}$. Often, a similar reasoning holds for resultants of polynomials in $\mathbb{Z}[X]$.

Determinant of the Sylvester matrix. Not a good idea, the matrix is too large, and computing the determinant is too costly in general.

Euclidean algorithm for resultant A better method consists in using the Euclidean algorithm, that is authorized by the following Corollary of the main theorem 1.

Corollary 3 *Let $A, B \in \Bbbk[X]$, $\Bbbk$ being a field, with $\deg A > \deg B$. Let $A = BQ + R$ be the Euclidean division of A by B, $\deg R < \deg B$. We have:*

$$\mathsf{Res}(A, B) = (-1)^{\deg(A)\deg(B)}\textsc{lc}(B)^{\deg(A)-\deg(R)}\mathsf{Res}(B, R).$$

Proof: This follows from the formulas of the main theorem Slide 9:

$$\begin{aligned}
\mathsf{Res}(A, B) &\overset{eq.\ (2)}{=} (-1)^{\deg(A)\deg(B)}\textsc{lc}(B)^{\deg(A)}\prod_j A(\beta_j) \\
&= (-1)^{\deg(A)\deg(B)}\textsc{lc}(B)^{\deg(A)}\prod_j B(\beta_j)Q(\beta_j) + R(\beta_j) \\
\text{but } B(\beta_j) = 0, \quad &= (-1)^{\deg(A)\deg(B)}\textsc{lc}(B)^{\deg(A)}\prod_j R(\beta_j)
\end{aligned}$$

On the other hand, $\mathsf{Res}(B, R) \overset{eq.\ (3)}{=} \textsc{lc}(B)^{\deg(B)}\prod_j R(\beta_j)$. We replace this formula in the equation above, and obtain the required formula. □

This formula permits to compute the resultant in an Euclidean style, like hereunder (Cf. Mathematica file "`Syl-2.nb`" and the function `ResEucl` at the end).

In the left-hand side below, d_i means the degree of A_i.

Standard Euclidean algorithm	Euclidean algorithm for the resultant

$A_1 \leftarrow A$
$A_2 \leftarrow B$
$i \leftarrow 2$
while($A_i \neq 0$){
  $A_{i-1} = bA_i + r$ //*Euclidean division*
  $A_{i+1} \leftarrow r$
  $i \leftarrow i + 1$
}
return A_i
	$A_1 \leftarrow A$
	$A_2 \leftarrow B$
	$R_1 \leftarrow 1$
	$i \leftarrow 2$
	while($\deg A_i > 0$){
	  $A_{i-1} = bA_i + r$ //*Euclidean division*
	  $A_{i+1} \leftarrow r$
	  $R_i \leftarrow (-1)^{d_i d_{i-1}}\textsc{lc}(A_i)^{d_{i-1}-d_{i+1}}R_{i-1}$
	  $i \leftarrow i + 1$
	}
	if ($A_i \neq 0$) then return $R_{i-1}\textsc{lc}(A_i)^{d_{i-1}}$
	else return 0

Correctness: While $\deg A_i > 0$ we have $\mathsf{Res}(A, B) \overset{(\star)}{=} R_i\mathsf{Res}(A_i, A_{i-1})$ (exercise: proof by induction on $i \geq 2$, using Corollary 4).

If $\deg A_i = 0$, we exit the while loop and if $A_i = 0$, then $\mathsf{Res}(A_i, A_{i-1}) = 0$, hence $\mathsf{Res}(A, B) = 0$ by Equality ($\star$). If $A_i \neq 0$, then $\deg(A_i) = 0$ says that A_i is a constant and the Sylvester matrix of A_{i-1} and A_i is diagonal with $A_i = \textsc{lc}(A_i)$ on the diagonal, and $\mathsf{Syl}(A_i, A_{i-1})$ has size $d_{i-1} = \deg(A_{i-1})$.