THE RESULTANT OF TWO POLYNOMIALS

PIERRE-LOÏC MÉLIOT

Abstract. We introduce the notion of resultant of two polynomials, and we explain its use for the computation of the intersection of two algebraic curves.

Case of two polynomials in one variable. Consider an algebraically closed field k (say, $k = \mathbb{C}$), and let P and Q be two polynomials in $k[X]$:

$$P(X) = a_r X^r + a_{r-1} X^{r-1} + \cdots + a_1 X + a_0;$$
$$Q(X) = b_s X^s + b_{s-1} X^{s-1} + \cdots + b_1 X + b_0.$$

We want a simple criterion to decide whether P and Q have a common root α. Note that if this is the case, then

$$P(X) = (X - \alpha)\, P_1(X);$$
$$Q(X) = (X - \alpha)\, Q_1(X)$$

and $P_1 Q - Q_1 P = 0$. Therefore, there is a linear relation between the polynomials

$$P(X), XP(X), \ldots, X^{s-1}P(X), Q(X), XQ(X), \ldots, X^{r-1}Q(X).$$

Conversely, such a relation yields a common multiple $P_1 Q = Q_1 P$ of P and Q with degree strictly smaller than $\deg P + \deg Q$, so P and Q are not coprime and they have a common root.

If one writes in the basis $1, X, \ldots, X^{r+s-1}$ the coefficients of the non-independent family of polynomials, then the existence of a linear relation is equivalent to the vanishing of the following determinant of size $(r + s) \times (r + s)$:

$$\operatorname{Res}(P, Q) = \begin{vmatrix} a_r & a_{r-1} & \cdots & a_0 & & & \\ & a_r & a_{r-1} & \cdots & a_0 & & \\ & & \ddots & \ddots & & \ddots & \\ & & & a_r & a_{r-1} & \cdots & a_0 \\ b_s & b_{s-1} & \cdots & b_0 & & & \\ & b_s & b_{s-1} & \cdots & b_0 & & \\ & & \ddots & \ddots & & \ddots & \\ & & & b_s & b_{s-1} & \cdots & b_0 \end{vmatrix},$$

with s lines with coefficients a_i and r lines with coefficients b_j. This determinant is called the **resultant** of P and Q, and the previous discussion shows that P and Q share a common root in k if and only if $\operatorname{Res}(P, Q) = 0$. On the other hand, the resultant is a polynomial function of the coefficients:

$$\operatorname{Res}(P, Q) \in k[a_r, \ldots, a_0, b_s, \ldots, b_0],$$

and it is homogeneous with total degree $r + s$. This property and the vanishing condition can be used to prove the following formula:

$$\operatorname{Res}(P, Q) = (a_r)^s (b_s)^r \prod_{\substack{x \text{ root of } P \\ y \text{ root of } Q}} (x - y),$$

Date: March 17, 2020.

where the enumeration of the roots of P and Q takes into account their possible multiplicities.

If $P, Q \in k[X]$ with k arbitrary field (not supposed anymore algebraically closed), then the factorisation of the resultant presented above still holds, but with the enumeration of roots in an algebraic closure $\overline{k}$ of k. On the other hand, note that the following conditions are equivalent:

(1) The polynomials P and Q have a common factor in $k[X]$.

(2) The polynomials P and Q have a common root in $\overline{k}$, an algebraic closure of k.

(3) The polynomials $P(X), XP(X), \dots, X^{s-1}P(X), Q(X), XQ(X), \dots, X^{r-1}Q(X)$ are linearly dependent in $k_{r+s-1}[X]$, the space of polynomials with degree smaller than $r+s-1$.

(4) The resultant $\mathrm{Res}(P, Q)$ vanishes.

Example 1. Consider a polynomial $P(X) = aX^2 + bX + c$ and its derivative $Q(X) = 2aX + b$ (the base field k is supposed with characteristic not equal to 2). Their resultant is $\mathrm{Res}(P, Q) = -a(b^2 - 4ac)$; we recognise the discriminant $b^2 - 4ac$ whose vanishing corresponds to the existence of a double root for P.

Example 2. Consider a polynomial $P(X) = X^3 + pX + q$ and its derivative $Q(X) = 3X^2 + p$, with a base field with characteristic 0. Their resultant is $\mathrm{Res}(P, Q) = 27q^2 + 4p^3$; we recognise again the discriminant of polynomials of degree 3.

The equation $\mathrm{Res}(P, Q) = 0$ is an explicit equation in terms of the polynomials P and Q, and it has many uses; in the sequel we investigate two of those.

Intersection of two algebraic curves. Consider two polynomials $P(x, y)$ and $Q(x, y)$ in two variables and with coefficients in some field k. We are interested in the intersection of the two algebraic curves $\mathscr{C}_P$ and $\mathscr{C}_Q$ determined by the two equations

$$\begin{aligned} P(x, y) &= 0; \\ Q(x, y) &= 0. \end{aligned}$$

To make things concrete, we can for instance consider the two equations in real numbers:

$$\begin{aligned} y^4 - y^3 + y^2 - 2x^2y + x^4 &= 0; \\ y - 2x^2 &= 0. \end{aligned}$$

This particular example can be solved by replacing y by $2x^2$ in the first equation, and then solving in terms of x; but it is clear that this technique would not work if the second equation was a bit more complicated. However, the resultants of polynomials allow one to perform the **elimination** of a variable in any case. Let us fix $y = y_0$, and let us consider the set of solutions x for this particular value of y. We now have two polynomials P_{y_0} and Q_{y_0} in $k[X]$:

$$P_{y_0}(x) = P(x, y_0) = 0 \qquad ; \qquad Q_{y_0}(x) = Q(x, y_0) = 0.$$

The set of equations above says that P_{y_0} and Q_{y_0} have a common root x; therefore, $\mathrm{Res}(P_{y_0}, Q_{y_0}) = 0$. To make clear that we are considering polynomials in x, we add an index to the notation Res_x. Thus:

Proposition 3. *If $y_0 \in k$ is the ordinate of a pair (x_0, y_0) in the intersecion of the algebraic curves $\mathscr{C}_P$ and $\mathscr{C}_Q$, then y_0 is solution of the polynomial equation*

$$\mathrm{Res}_x(P_{y_0}, Q_{y_0}) = 0.$$

Note that the equation is indeed polynomial in y_0, because the resultant is a homogeneous polynomial of the coefficients of the two polynomials. Thus, we can use the following method in order to find all the intersection points of the two curves:

(1) Solve the polynomial equation $\mathrm{Res}_x(P_{y_0}, Q_{y_0}) = 0$; it has a finite number of solutions y_0.

(2) For each of these solutions y_0, replace y by y_0 in $P(x, y) = Q(x, y) = 0$, and find the corresponding x's; again there are only a finite number of solutions.

We have thus transformed a system of two polynomial equations in two variables into a finite family of polynomial equations in one variable, which in general are much easier to solve.

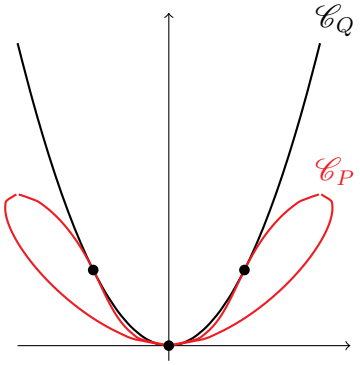
Example 4. Let us solve the previous example over $\mathbb{R}^2$. The resultant of the two polynomials with $y = y_0$ fixed can be computed:

$$\mathrm{Res}_x(P_{y_0}, Q_{y_0}) = 16 \left(y_0 - \frac{1}{2} \right)^4 (y_0)^4.$$

Therefore, if there exists an intersection point (x_0, y_0), then y_0 belongs to the set $\{0, \frac{1}{2}\}$. We now replace y by one of these values, and we solve the corresponding system:

- $y_0 = 0$: the equations become $x^4 = 0$ and $x^2 = 0$, so one has the solution $(x_0, y_0) = (0, 0)$.
- $y_0 = \frac{1}{2}$: the equations become $x^4 - x^2 + \frac{3}{16} = 0$ and $x^2 = \frac{1}{4}$, and there are two solutions: $x_0 = \pm\frac{1}{2}$.

Therefore, the intersections of the two real curves $\mathscr{C}_P$ and $\mathscr{C}_Q$ are the three points $(0, 0)$, $(\frac{1}{2}, \frac{1}{2})$ and $(-\frac{1}{2}, \frac{1}{2})$; see the figure below.



In the elimination technique, it is sometimes easier to fix x_0 and to compute $\mathrm{Res}_y(P_{x_0}, Q_{x_0})$; we leave the reader try to perform this alternative technique for the previous example. On the other hand, the reasoning above could be used in order to compute the number of intersection points in terms of the degrees of P and Q; however, in order to have a satisfying result (the so-called Bezout intersection theorem for algebraic curves), it is required to consider the case where k is an algebraically closed field, and where the two algebraic curves are replaced by their projective versions (homogeneous polynomial equations in three variables).

The field of algebraic numbers. An algebraic number is a complex number z which is the root of a polynomial with rational coefficients; for instance, $\sqrt{2}$ and $\frac{1+\mathrm{i}\sqrt{3}}{2}$ are algebraic numbers, but this is not the case of π or e. Denote $\overline{\mathbb{Q}}$ the set of all algebraic numbers; it is a strict subset of $\mathbb{C}$. It turns out that the theory of resultants allows one to prove:

Proposition 5. *The set of algebraic numbers $\overline{\mathbb{Q}}$ is a field.*

This result is not at all trivial: although

$$X^2 - 2 \quad \text{and} \quad X^6 - 1$$

clearly vanish on the two aforementioned algebraic numbers, it seems at first sight much more complicated to find a polynomial with rational coefficients vanishing on their sum $\sqrt{2} + \frac{1+\mathrm{i}\sqrt{3}}{2}$. We give hereafter the arguments which prove the stability of $\overline{\mathbb{Q}}$ by sum and by product: the stability by inversion or by taking the opposite is much easier.

- *stability by sum*. Consider two algebraic numbers z_1 and z_2 which are roots of polynomials P and Q in $\mathbb{Q}[X]$. We consider the polynomial in Y

  $$R(Y) = \mathrm{Res}_X(P(X), Q(Y - X)).$$

  This is a polynomial in $\mathbb{Q}[Y]$, with total degree $\deg P \times \deg Q$. Notice then that $z_1 + z_2$ is a root of R, because the two polynomials $P(X)$ and $Q(z_1 + z_2 - X)$ vanish simultaneously at $X = z_1$. Thus, $z_1 + z_2$ is algebraic, as a root of the polynomial R.
- *stability by product*. In the same setting as above, let us consider the polynomial in Y

  $$S(Y) = \mathrm{Res}_X\left(P(X), X^{\deg Q} Q\left(\frac{Y}{X}\right)\right).$$

  This polynomial in $\mathbb{Q}[Y]$ has again for total degree $\deg P \times \deg Q$, and it vanishes on $z_1 z_2$: indeed, the two polynomials $P(X)$ and $X^{\deg Q} Q(\frac{z_1 z_2}{Y})$ vanish simultaneously at $X = x_1$. So, the product $z_1 z_2$ is algebraic.

Let us close this note by two remarks. First, the exact same arguments can be used in order to prove that $\mathcal{O}$, the set of algebraic integers (roots of monic polynomials with coefficients in $\mathbb{Z}$), is a ring in $\mathbb{C}$. On the other hand, the proof above of the fact that $\overline{\mathbb{Q}}$ is a field has the advantage of providing explicit vanishing polynomials; however there exists also an abstract proof of the same fact. Let us remark that the following facts are equivalent:

- The complex number z is algebraic.
- The $\mathbb{Q}$-vector space $\mathbb{Q}_z$ spanned in $\mathbb{C}$ by the image of

  $$\begin{aligned} \phi_z : \mathbb{Q}[X] &\to \mathbb{C} \\ P &\mapsto P(z) \end{aligned}$$

  is finite-dimensional.

Consider now two algebraic numbers z_1 and z_2, and denote $\mathbb{Q}_{z_1,z_2}$ the set of complex numbers which are rational polynomials in z_1 and z_2; it is also a $\mathbb{Q}$-vector space. There is a natural surjective linear map

$$\begin{aligned} \mathbb{Q}_{z_1} \otimes_{\mathbb{Q}} \mathbb{Q}_{z_2} &\to \mathbb{Q}_{z_1,z_2} \\ a \otimes b &\mapsto ab. \end{aligned}$$

If P and Q are minimal rational polynomials for z_1 and z_2, then the tensor product on the left-hand side is a finite-dimensional space over $\mathbb{Q}$ with dimension $\deg P \times \deg Q$. Therefore, $\mathbb{Q}_{z_1,z_2}$ is also finite dimensional, and it contains the two $\mathbb{Q}$-vector spaces $\mathbb{Q}_{z_1+z_2}$ and $\mathbb{Q}_{z_1 z_2}$. This proves that $z_1 + z_2$ and $z_1 z_2$ are algebraic, and also that there exists rational polynomials of degree at most $\deg P \times \deg Q$ that vanish on these elements; the theory of resultants provides *explicit* vanishing polynomials.