143 Résultant. Applications.

Cadre : $\mathbb{A}$ anneau commutatif unitaire intègre. $\mathbb{A}_d[X]$ le $\mathbb{A}$-module des polynômes de degré $\leq d$.

I- Résultant et racines.

1.1. application de Bézout.

[M] 377

déf. 1 : Soient $p, q \in \mathbb{N}$ et $P = \sum_{i=0}^{p} x_i X^i$ et $Q = \sum_{i=0}^{q} y_i X^i$ dans $\mathbb{A}[X]$ de degré p et q. L'application de Bézout $B(P,Q)$ est le morphisme :

$$B(P,Q) : Fx(\mathbb{A})_q[X] \times Fx(\mathbb{A})_p[X] \longrightarrow Fx(\mathbb{A})_{p+q}[X]$$
$$(U, V) \longmapsto PU + QV$$

- la matrice de Sylvester est la matrice de $B(P,Q)$ dans la base $\{(X^{q-1}, 0), (X^{q-2}, 0) \dots (1,0), (0, X^{p-1}) \dots (0,1)\}$.

$$M(P,Q) = \begin{pmatrix} x_p & 0 & & 0 & y_q & 0 & \\ x_{p-1} & x_p & & & y_{q-1} & y_q & \\ \vdots & & \ddots & 0 & \vdots & & \ddots \\ x_0 & & & x_p & y_0 & & y_q \\ 0 & x_0 & & & 0 & y_0 & \\ & \ddots & & & & & \ddots \\ 0 & & 0 & x_0 & & & y_0 \end{pmatrix}$$

(q colonnes, p colonnes)

- le résultant de P et Q est le déterminant de $B(P,Q)$. On le note $Res_X(P,Q)$ ou $Res(P,Q)$.

(*) rmq : $M(P,Q) \in \mathcal{M}_{p+q}(\mathbb{A}) \subsetneq \mathcal{M}_{p+q}(Fx(\mathbb{A}))$. Le résultant est donc un élément de $\mathbb{A}$.

Exemple $P = X^2 + X + 1$, $Q = X - 1$ dans $\mathbb{Z}[X]$ $M(P,Q) = \begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & 1 \\ 0 & 1 & -1 \end{pmatrix}$
$Res_X(P,Q) = 3 \in \mathbb{Z}$

[SP] 142

prop. 2 : soient $P, Q \in \mathbb{A}[X]$ ($\deg(P) = m$, $\deg(Q) = n > 0$), $\alpha \in \mathbb{A}$. On a :

i) $Res(\alpha, Q) = \alpha^n$
ii) $Res(Q,Q) = 0$
iii) $Res(P,Q) = (-1)^{mn} Res(Q,P)$ (loi de réciprocité)

iv) Si $T \in \mathbb{A}[X]$ alors $Res(PT, Q) = Res(P,Q)\, Res(T,Q)$

1.2. résultant et diviseurs communs.

[SP] 144

Thm 3 : $P, Q \in \mathbb{A}[X]$ de degré m et n. R le reste de la division euclidienne de P par Q dans $Fr(\mathbb{A})[X]$. $r = \deg(R)$

$$Res(P,Q) = (-1)^{mn} b_n^{m-r} Res(Q,R) \qquad (\text{où } Q = \sum_{i=0}^{n} b_i X^i).$$

[M] 378

prop. 4 : Soient P, Q non nuls dans $\mathbb{A}[X]$. On a équivalence entre :
i) $Res(P,Q) = 0$
ii) P et Q ont un multiple commun de degré $< \deg(P) + \deg(Q)$
iii) $B(P,Q)$ n'est pas injectif.

[M] 378

Corollaire 5 : si $\mathbb{A}$ est factoriel alors $Res(P,Q) = 0$ ssi $P \wedge Q$ est de degré non nul.

[M] 379

contre-exemple : $\mathbb{A} = \mathbb{Q}[X_1, X_2, Y_1, Y_2]/(X_1Y_2 - X_2Y_1)$ intègre, non-factoriel. $P = x_1X + x_2$ $Q = y_1X + y_2$ (où $x_i = \overline{X_i}$)
$Res_X(P,Q) = x_1y_2 - x_2y_1 = 0$ mais P et Q n'ont pas de diviseur non constant.

[BZ] 565

Corollaire 6 : Si $\mathbb{A}$ est un corps algébriquement clos, alors $Res(P,Q) = 0$ ssi P et Q ont une racine commune.

[G] 208

Appli : si $\mathcal{D}$ est l'ensemble des matrices diagonalisable de $\mathcal{M}_n(\mathbb{C})$ alors $\mathring{\mathcal{D}}$ est l'ensemble des matrices à valeurs propres distinctes.

1.3. racines multiples et discriminant.

[H]

Thm 7 : Si $P = \prod_{i=1}^{m} (X - \lambda_i)$ et $Q = \prod_{i=1}^{n} (X - \mu_i)$ alors on a :

$$Res_X(P,Q) = \prod_{i=1}^{m} \prod_{j=1}^{n} (\lambda_i - \mu_j)$$
$$= \prod_{i=1}^{m} Q(\lambda_i)$$
$$= (-1)^{mn} P(\mu_j)$$

Corollaire 8 : (Kronecker)
Soit $P \in \mathbb{Z}[X]$ unitaire dont les racines sont de module ≤ 1. Si $P(0) \neq 0$ alors les racines de P sont des racines de l'unité.

[SZ] 568 **déf.9**: Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{A}[X]$. On appelle discriminant de P la quantité : $\Delta(P) = \frac{(-1)^{\frac{n(n-1)}{2}}}{a_n} Res_x(P, P')$

prop.10: Si $P = \alpha \prod_{i=1}^{n} (X - \lambda_i)$ alors $\Delta(P) = \alpha^{2n-2} \prod_{1 \le i < j \le n} (\lambda_i - \lambda_j)^2$

(*) **Exemples**:

$P_2 = aX^2 + bX + c$ $\quad \Delta_2 = b^2 - 4ac$

$P_3 = X^3 + pX + q$ $\quad \Delta_3 = -4p^3 - 27q^2$

[SZ] 568 **prop 11**: Si $\mathbb{A}$ est un corps algébriquement clos, on a : $\Delta(P) = 0$ ssi P possède une racine multiple.

(*) **exemple**:

$P = X^2 + 2X + 1$ $\quad \Delta = 0$

Appli: Théorème de Cayley-Hamilton

II - Résultant et élimination.

2.1. élimination

[SP] 147 **But** résoudre des systèmes polynomiaux.

exemple: dans $\mathbb{C}[x,y]$ $(S) \begin{cases} P = X^2 + 2X - XY + 2Y - 6 \\ Q = 3X^2 - 5X + 5 + XY - 2Y \end{cases}$

Si (α, β) est solution, alors α est une racine commune de $P(X, \beta)$ et $Q(X, \beta)$. Donc β est une racine de $Res_x(P, Q) \in \mathbb{C}[Y]$

$Res_x(P, Q) = (36Y - 108)(Y - 3)$ (variable x éliminée)

donc $\beta \in \{3, \frac{108}{36}\}$

L'élimination consite à faire décroitre le nombre d'inconnue.

(*) **Appli**: Formule de Héron (Cf annexe 1)

$\mathcal{A} = \sqrt{p(p-a)(p-b)(p-c)}$ où p est le demi-périmètre.

il suffit d'éliminer x et y dans le système

$\begin{cases} P = x^2 + y^2 - b^2 \\ Q = (a-x)^2 + y^2 - c^2 \\ R = ay - 2S \end{cases}$

2.2. Équation implicite et paramétrique d'une courbe.

[M] 385 **déf.12**: une courbe C de $\mathbb{R}^2$ admet une équation implicite lorsqu'elle admet une expression : $C = \{(x,y) \in \mathbb{R}^2 / P(x,y) = 0\}$ avec $P \in \mathbb{R}[X,Y]$.

exemple: le cercle " $x^2 + y^2 - 1 = 0$ "

[M] 385 **déf.13**: une courbe C admet une paramétrisation rationnelle lorsqu'elle admet une expression $C = \{(x,y) \in \mathbb{R}^2 / \exists t \in \mathbb{R} \quad x = F(t) \text{ et } y = G(t)\}$ avec $F, G \in \mathbb{R}(X)$.

[A] 305 **prop.14**: les coniques privées d'un point admettent une paramétrisation rationnelle.

exemple: le cercle $C(0,1)$, privé de $(-1, 0)$ est paramétré par

$\begin{cases} x(t) = -\frac{t^2-1}{t^2+1} \\ y(t) = \frac{2t}{t^2+1} \end{cases}$, $t \in \mathbb{R}$. (Cf annexe 2)

Implicitation:

[M] 385 Soit $F = \frac{P_1}{Q_1}$, $G = \frac{P_2}{Q_2} \in \mathbb{R}(T)$ et C une courbe paramétrée par F et G. On cherche une equation implicite de C.

On pose $\tilde{F}(T, X) = Q_1(T)X - P_1(T)$ $\quad \tilde{G}(T, Y) = Q_2(T)Y - P_2(T)$

$R(x,y) = Res_T(\tilde{F}, \tilde{G})$ (élimination de la variable T).

[M] 385 **prop.15**: la courbe $\tilde{C} = \{(x,y) \in \mathbb{R}^2 / R(x,y) = 0\}$ contient C.

- Si Q_1 et Q_2 sont constants, alors $C = \tilde{C}$.

(*) **exemple**: $C = \{(x,y) \in \mathbb{R}^2 / \exists t \in \mathbb{R} \quad x = t^2 - 2t + 1, \ y = t^2\}$

$R(x,y) = X^2 - 2XY + Y^2 - 2X - 2Y + 1$. C'est une parabole.

La différence entre $\mathbb{C}$ et $\bar{\mathbb{C}}$ s'explique grâce au théorème suivant:

[SP] 148 **Thm 16**: (Théorème d'extension) **DEV. 1**

$\mathbb{K}$ corps algébriquement clos. $P, Q \in (\mathbb{K}[Y_1 \cdots Y_{n-1}])[X]$.

$P = \sum_{i=1}^{m} a_i X^i$, $Q = \sum_{i=1}^{m} b_i X^i$ avec $a_i, b_i \in \mathbb{K}[Y_1 \cdots Y_{n-1}]$, $mn \neq 0$.

- Si $P(\alpha_1 \cdots \alpha_{n-1}, \alpha) = 0 = Q(\alpha_1 \cdots \alpha_{n-1}, \alpha)$ alors $\mathrm{Res}_X(P,Q)(\alpha_1 \cdots \alpha_{n-1}) = 0$
- Si $\mathrm{Res}_X(P,Q)(\alpha_1 \cdots \alpha_{n-1}) = 0$, on a l'une des quatre éventualités:
  - i) $\exists \alpha \in \mathbb{K}$ tq $P(\alpha_1 \cdots \alpha_{n-1}, \alpha) = 0 = Q(\alpha_1 \cdots \alpha_{n-1}, \alpha)$
  - ii) $P(\alpha_1 \cdots \alpha_{n-1}, X) = 0$
  - iii) $Q(\alpha_1 \cdots \alpha_{n-1}, X) = 0$
  - iv) $a_m(\alpha_1 \cdots \alpha_{n-1}) = 0 = b_n(\alpha_1 \cdots \alpha_{n-1})$

2.3. intersection de courbes.

[SZ] 588 **déf. 17**: une courbe algébrique plane est le lieu d'annulation d'un polynôme de $\mathbb{C}[X,Y]$.
C'est un sous-ensemble de $\mathbb{C}^2$.
On note $V(P)$ la courbe définie par $P \in \mathbb{C}[X,Y]$.

[SZ] **Thm. 18**: (Borne de Bézout) **DEV. 2**

Soient P et $Q \in \mathbb{C}[X,Y]$ de degrés totaux m et n.
Si $P \wedge Q = 1$, alors $V(P) \cap V(Q)$ est fini et $\#(V(P) \cap V(Q)) \leq mn$

exemple (Cf annexe 3)
L'intersection de deux coniques contient au plus 4 points.

III - Résultant et arithmétique.

3.1. nombres algébriques.

[SZ] 571 **déf. 19**: un complexe est algébrique (sur $\mathbb{Q}$) s'il est racine d'un polynôme à coefficient entier.
- un complexe est un entier algébrique (sur $\mathbb{Q}$) s'il est racine d'un polynôme unitaire à coefficient entier.

exemple: $\sqrt{2}$ est racine de $X^2 - 2$.
i est racine de $X^2 + 1$.

propo: l'ensemble des entiers algébriques est un anneau.
l'ensemble des nombres algébriques est un corps.

en effet, si $P(\alpha) = 0 = Q(\beta)$ alors $\alpha + \beta$ est racine de $\mathrm{Res}_X(P(X), Q(Y-X))$, et $\alpha \cdot \beta$ est racine de $\mathrm{Res}_X(P(X), X^n Q(\frac{Y}{X}))$ avec $n = \deg(Q)$.

3.2. loi de réciprocité quadratique.

[M]

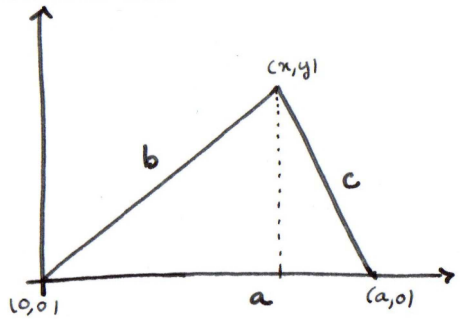
déf 21: symbole de Legendre
soit p premier impair et $a \in \mathbb{Z}$. $\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } p \mid a \\ 1 \text{ si } a \text{ est un carré modulo } p \\ -1 \text{ sinon.} \end{cases}$

Thm 22: (loi de réciprocité quadratique)
p, q premiers, impairs, distincts. On a:

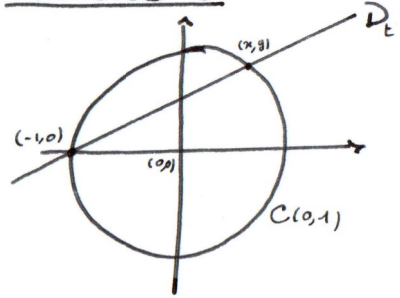
$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

rmq: on utilise la loi de réciprocité du résultant en exprimant le symbole de Legendre comme le résultant de deux polynômes bien choisis.

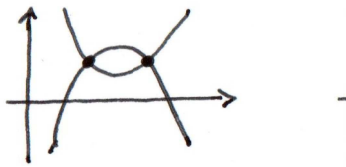
· Annexe 1

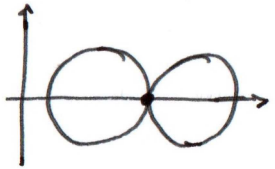


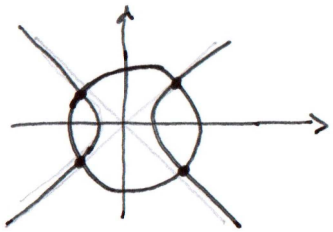
· Annexe 2



· Annexe 3







· Références

[A] M. Audin, Géométrie.

[G] x. Gourdon, Algèbre.

[M] J-y. Mérindol, Nombres et algèbre.

[SP] P. Saux Picart, Cours de calcul formel, Algo. fondamentaux.

[SZ] A. Szpirglas, Algèbre.

[*] sans réf.

Borne de Bézout

Références : Szpirglas, *Mathématiques L3 - Algèbre*, p 592
Mérindol, *Nombres et algèbre*, p 386
Saux Picart, *Cours de calcul formel - Algorithmes fondamentaux*, p 157

Soit k un corps commutatif de cardinal infini. On se propose dans ce développement de majorer le nombre de points d'intersection de deux courbes planes à valeurs dans k.

Théorème.

Soient A et B deux polynômes de $k[X,Y]$ de degrés totaux respectifs m et n. Si A et B sont premiers entre eux et que k est de cardinal infini, alors $\#Z(A)\cap Z(B)\leqslant mn$.

Démonstration. Si A et B n'ont pas de racine commune, le résultat est évident et dans toute la suite, on suppose que $Z(A)\cap Z(B)$ est non vide.

On note $R_Y=\mathrm{Res}_Y(A,B)$ et $R_X=\mathrm{Res}_X(A,B)$. Pour tout $(x,y)\in Z(A)\cap Z(B)$, il vient $R_Y(x)=R_X(y)=0$. Comme A et B sont premiers entre eux, R_Y est un polynôme non nul de $k[X]$ et il a au plus $\deg R_Y$ racines. Ainsi, il y a au plus $\deg R_Y$ possibilités pour l'abscisse d'un point de $Z(A)\cap Z(B)$. De la même façon, il y au plus $\deg R_X$ possibilités pour l'ordonnée de ces points. On en déduit que

$$\#Z(A)\cap Z(B)\leqslant \deg R_X \deg R_Y.$$

Notons à présent

$$A(X,Y)=\sum_{k=0}^{p}a_k(X)Y^k \quad B(X,Y)=\sum_{k=0}^{q}b_k(X)Y^k,$$

où $\deg a_k\leqslant m-k$, $\deg b_k\leqslant n-k$ et a_p,b_q sont deux éléments non nuls de k. Alors

$$R_Y=\det(\mathrm{Syl}_Y(A,B))=\begin{vmatrix} a_p & & & b_q & & & \\ \vdots & \ddots & & \vdots & \ddots & & \\ \vdots & & a_p & b_0 & & \ddots & \\ a_0 & & \vdots & & \ddots & & b_q \\ & \ddots & \vdots & & & \ddots & \vdots \\ & & a_0 & & & & b_0 \end{vmatrix}.$$

On note $\mathrm{Syl}_Y(A,B)=(c_{i,j})$. Alors

$$\forall j\in[\![1,q]\!]: \qquad c_{i,j}=\begin{cases} a_{p-(i-j)} & \text{si } 0\leqslant i-j\leqslant p \\ 0 & \text{sinon}\end{cases} \qquad \leqslant m-p+i-j,$$

$$\forall j\in[\![q+1,q+p]\!]: \quad \deg c_{i,j}=\begin{cases} b_{q-(i-(j-q))} & \text{si } -q\leqslant i-j\leqslant 0 \\ 0 & \text{sinon}\end{cases} \qquad \leqslant n-j+i.$$

On en déduit :

$$\forall\sigma\in\mathcal{S}_{p+q}:\deg\left(\varepsilon(\sigma)\prod_{i=1}^{p+q}c_{i,\sigma(i)}\right)=\sum_{i=1}^{p+q}\deg c_{i,\sigma(i)}\leqslant\sum_{i=1}^{q}(m-p+i-\sigma(i))+\sum_{i=q+1}^{q+p}(n-\sigma(i)+i)$$

$$=mq-pq+np=mn+(m-p)(q-n)\leqslant mn,$$

et avec la formule du déterminant, $\deg R_Y \leqslant mn$. On obtient de même $\deg R_X \leqslant mn$ puis

$$\#Z(A) \cap Z(B) \leqslant (mn)^2.$$

Pour achever la démonstration, il ne reste plus qu'à affiner la majoration précédente. Dans ce but, on numérote les éléments de $Z(A) \cap Z(B) = \{(x_i, y_i) : i \in [\![1, r]\!]\}$ et on pose

$$\mathcal{E} = \left\{ \frac{x_i - x_j}{y_j - y_i} : y_j \neq y_i, i, j \in [\![1, r]\!] \right\}.$$

Alors $\#\mathcal{E} < \#k^*$ car k est de cardinal infini et on peut considérer $u \in k^* \backslash \mathcal{E}$. Remarquons le fait suivant :

$$\forall i, j \in [\![1, r]\!] : x_i - x_j \neq u(y_j - y_i) \Leftrightarrow x_i + uy_i \neq x_j + uy_j.$$

On effectue alors le changement de variables suivant :

$$\begin{cases} X' = X + uY \\ Y' = Y \end{cases} \quad \begin{cases} \tilde{A}(X', Y') = A(X, Y) \\ \tilde{B}(X', Y') = B(X, Y) \end{cases}.$$

Soit alors la fonction φ : $\begin{array}{ccc} Z(A) \cap Z(B) & \to & Z(\mathrm{Res}_{Y'}(\tilde{A}, \tilde{B})) \\ (x, y) & \mapsto & x + uy \end{array}$.

La fonction φ est bien définie car si $(x, y) \in Z(A) \cap Z(B)$, alors $A(x, y) = B(x, y) = 0$ ce qui entraîne $\tilde{A}(x + uy, y) = \tilde{B}(x + uy, y) = 0$ puis $\mathrm{Res}_{Y'}(\tilde{A}(x + uy, y), \tilde{B}(x + uy, y)) = 0$ ce qui se réécrit $\mathrm{Res}_{Y'}(\tilde{A}, \tilde{B})(x + uy) = 0$. De plus, φ est injective puisque u n'est pas un élément de $\mathcal{E}$. Ainsi :

$$\#Z(A) \cap Z(B) \leqslant \#Z(\mathrm{Res}_{Y'}(\tilde{A}, \tilde{B}) \leqslant \deg \mathrm{Res}_{Y'}(\tilde{A}, \tilde{B}) \leqslant mn$$

d'après le point précédent, ce qui achève la démonstration.

□

Remarques : • Ce développement est une simplification du vrai théorème de Bézout. Si on homogénéise A et B en polynômes homogènes de $\overline{k}[X, Y, T]$, alors si on compte la multiplicité des intersections et les points à l'infini, on a $\#Z(A) \cap Z(B) = mn$.
• Pour trouver les points d'intersections en pratique, on fait comme dans la preuve :on calcule les deux résultants (en X et en Y) et on cherche leurs zéros communs. En faisant cela, on obtient des équations seulement en X ou seulement en Y, d'où le nom de théorie de l'élimination.
Si on veut les points d'intersection à l'infini, il suffit d'homogénéiser les résultants, d'évaluer en "$T = 0$", puis de résoudre.
• La condition k infini n'est pas nécessaire. Il suffit de faire la preuve dans $\overline{k}$ qui est infini, puis comme $k \subset \overline{k}$, on a le résultat.

Adapté du travail de Paul Alphonse.

Théorème d'extension

Références : Saux Picart, *Cours de calcul formel - Algorithmes fondamentaux*, p 148

On sait que si P et Q sont deux polynômes admettant une racine commune, alors leur résultant est nul en cette racine. Le calcul du résultant permet donc de trouver toutes les racines possibles.
Néanmoins les racines du résultant ne se remontent pas toutes en racines des polynômes. C'est ce que permet d'étudier le théorème d'extension.

Théorème.

Soit $\mathbb{K}$ un corps algébriquement clos et soient P, Q deux polynômes de $\mathbb{K}[Y,...,Y_k][X]$, on note $P = \sum_{i=0}^{m} a_i X^i$ et $Q = \sum_{i=0}^{n} b_i X^i$ avec m, $n \neq 0$ et a_i, $b_i \in \mathbb{K}[Y,...,Y_k]$.
Si $(\alpha_1, ..., \alpha_k, \alpha)$ est tel que $P(\alpha_1, ..., \alpha_k, \alpha) = Q(\alpha_1, ..., \alpha_k, \alpha) = 0$, alors $\mathrm{Res}_X(P,Q)(\alpha_1, ..., \alpha_k) = 0$.
Réciproquement, si $\mathrm{Res}_X(P,Q)(\alpha_1, ..., \alpha_k) = 0$, alors une des propositions suivantes est vérifiée :

1. $\exists \alpha \in \mathbb{K}$, $P(\alpha_1, ..., \alpha_k, \alpha) = Q(\alpha_1, ..., \alpha_k, \alpha) = 0$,
2. $P(\alpha_1, ..., \alpha_k, X) = 0$,
3. $Q(\alpha_1, ..., \alpha_k, X) = 0$,
4. $a_m(\alpha_1, ..., \alpha_k) = b_n(\alpha_1, ..., \alpha_k) = 0$.

Pour prouver ce théorème, on va utiliser l'application suivante :

$$\Phi : \begin{array}{ccc} \mathbb{K}[Y,...,Y_k][X] & \to & \mathbb{K}[X] \\ U & \mapsto & U(\alpha_1, ..., \alpha_k, X) \end{array}$$

Pour voir sa compatibilité avec le résultant, on a le résultat suivant.

Lemme.

Soient A, B deux anneaux, et Φ un morphisme d'anneau de A dans B, alors si on note p et q les degrés respectifs de P et Q, on a

$$\Phi(\mathrm{Res}_X(P,Q)) = \begin{cases} \Phi(a_m)^{n-q}\,\mathrm{Res}_X(\Phi(P),\Phi(Q)) & \text{si } \Phi(a_m) \neq 0 \text{ ou } \Phi(a_m) = \Phi(b_n) = 0, \\ \Phi(b_n)^{m-p}\,\mathrm{Res}_X(\Phi(P),\Phi(Q)) & \text{si } \Phi(b_n) \neq 0 \text{ ou } \Phi(a_m) = \Phi(b_n) = 0. \end{cases}.$$

Démonstration. Le résultant est défini comme le déterminant de la matrice de Sylvester. On a donc, comme le déterminant est un polynôme :

$$\Phi(\mathrm{Res}_X(P,Q)) = \Phi(\det(Sylv(P,Q))) = \det(\Phi(Sylv(P,Q))).$$

Si on note a'_i et b'_i les images des a_i et b_i par Φ, alors

$$\Phi(Sylv(P,Q)) = \begin{pmatrix} a'_m & & & 0 & & \\ \vdots & \ddots & & b'_q & \ddots & \\ a'_0 & \ddots & & \vdots & \ddots & 0 \\ & \ddots & a'_m & b'_0 & & b'_q \\ & & \ddots & \vdots & \ddots & \vdots \\ & & & a'_0 & & b'_0 \end{pmatrix}.$$

Supposons $a'_m \neq 0$, alors en développant par rapport aux premières lignes, on a

$$\det(\Phi(Sylv(P,Q))) = (a'_m)^{n-q} \det(Sylv(\Phi(P),\Phi(Q))).$$

Il vient

$$\Phi(\mathrm{Res}_X(P,Q)) = (\Phi(a_m))^{n-q} \mathrm{Res}_X(\Phi(P),\Phi(Q)).$$

Si $a'_m = 0$ et $b'_n = 0$, la formule précédente marche encore car $\Phi(\mathrm{Res}_X(P,Q)) = 0$.
Enfin si $a'_m = 0$ et $b'_n \neq 0$, on a par le même raisonnement

$$\Phi(\mathrm{Res}_X(P,Q)) = (\Phi(b_n))^{m-p} \mathrm{Res}_X(\Phi(P),\Phi(Q)).$$

□

Passons à la preuve du théorème !

Démonstration. $\Leftarrow$: Si $P(\alpha_1,...,\alpha_k,\alpha) = Q(\alpha_1,...,\alpha_k,\alpha) = 0$, alors α est racine de $\Phi(P)$ et $\Phi(Q)$, donc $\mathrm{Res}_X(\Phi(P),\Phi(Q)) = 0$. Le lemme donne alors $\Phi(\mathrm{Res}_X(P,Q)) = 0$, donc $\mathrm{Res}_X(P,Q)(\alpha_1,...,\alpha_k) = 0$.

$\Rightarrow$: Supposons que $\mathrm{Res}_X(P,Q)(\alpha_1,...,\alpha_k) = 0$.

• Si $\Phi(a_m) \neq 0$, alors le lemme donne $\Phi(a_m)^{n-q} \mathrm{Res}_X(\Phi(P),\Phi(Q)) = 0$, donc $\mathrm{Res}_X(\Phi(P),\Phi(Q)) = 0$. On en déduit que soit $\Phi(Q) = 0$ (cas 3), soit $\Phi(Q) \neq 0$ et $\Phi(P)$ et $\Phi(Q)$ ont une racine commune α. Alors $(\alpha_1,...,\alpha_k,\alpha)$ est racine commune de P et Q.

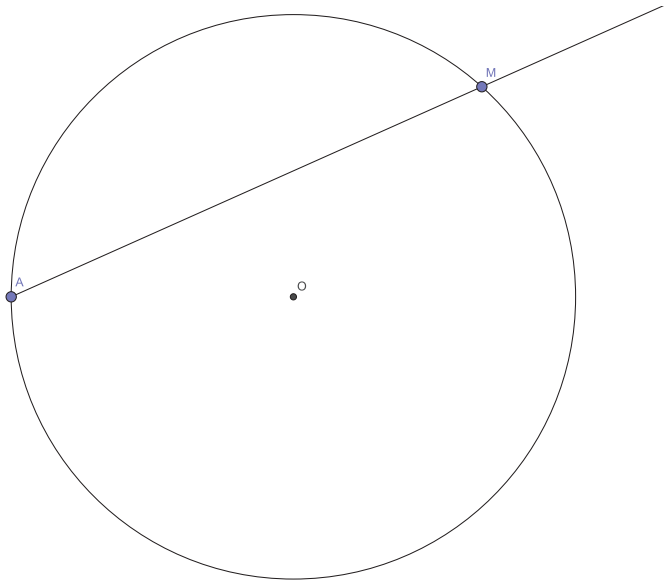
• Si $\Phi(a_m) = 0$ et $\Phi(b_n) \neq 0$, on peut refaire le raisonnement pour tomber sur les cas 1 ou 3.

• Si $\Phi(a_m) = \Phi(b_n) = 0$, on est dans le cas 4. □

Application : Paramétrisation du cercle
On tente de trouver une paramétrisation du cercle centré en 0 et de rayon 1. Pour cela, on choisit un point A sur le cercle (ici $(-1,0)$). L'intersection d'une droite de pente $t \in \mathbb{R}$ passant par A - et non-tangente au cercle - avec le cercle est appelée $M(t)$. $M(t)$ est donc racine de $P = X^2 + Y^2 - 1$ et $Q = Y - t(X+1)$.
Pour trouver une expression en t des coordonnées de $M(t)$, on fait un résultant :

$$\mathrm{Res}_Y(P,Q) = \begin{vmatrix} 1 & 1 & 0 \\ 0 & -t(X+1) & 1 \\ X^2-1 & 0 & -t(X+1) \end{vmatrix} = (1+t^2)X^2 + 2t^2X + t^2 - 1$$

On trouve deux racines : $X = -1$ (qui correspond au point A), et $X = \dfrac{1-t^2}{1+t^2}$. Finalement, la paramétrisation du cercle est donnée ici par $M(t) = \left(\dfrac{1-t^2}{1+t^2}, \dfrac{2t}{1+t^2}\right)$.



Refaisons maintenant le raisonnement à l'envers ! Supposons que j'ai la paramétrisation précédente, et que je veuille trouver une équation de la courbe décrite par cette paramétrisation.
On pose $P = (1+t^2)X + t^2 - 1$ et $Q = (1+t^2)Y - 2t$, alors

$$\mathrm{Res}_t(P,Q) = \begin{vmatrix} X+1 & 0 & Y & 0 \\ 0 & X+1 & -2 & Y \\ X-1 & 0 & Y & -2 \\ 0 & X-1 & 0 & Y \end{vmatrix} = 4(X^2+Y^2-1).$$

Les zéros du résultant décrivent le cercle $\mathcal{C}(0,1)$, or $M(t)$ paramétrise le cercle privé du point A. Le point A représente le cas 4 du théorème, c'est à dire que comme $\Phi(P) = -2$ et $\Phi(Q) = -2t$, le terme dominant a disparu dans les deux polynômes.

Remarques : • Pour illustrer les cas 2 et 3 du théorème, on peut juste prendre $P = (Y_1 - \alpha_1)P'$ car alors $a_i' = 0$ pour tout i et la matrice de Sylvester est de déterminant nul (pareil pour Q pour le cas 3).

Loi de réciprocité quadratique (avec le résultant)

Références : Mérindol, *Nombres et algèbre*, p 389

Théorème (Loi de réciprocité quadratique)**.**

Soit p et q, deux nombres premiers impairs, distincts. On a : $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$.

Le but est d'exprimer le symbole de Legendre $\left(\frac{p}{q}\right)$ sous la forme d'un résultant de deux polynômes. Pour cela, nous avons besoin d'un lemme portant sur les polynômes.

Lemme.

Soit $R \in \mathbb{Z}[X]$ un polynôme palindromique de degré d pair. Alors, il existe un polynôme $S \in \mathbb{Z}[T]$, de degré $\frac{d}{2}$ tel que l'on ait : $R(X) = X^{d/2} S(X + X^{-1})$.

Démonstration. Les polynômes symétriques élémentaires de $\mathbb{Z}[X,Y]$ sont $\sigma = X+Y$ et $\pi = XY$. Tout polynôme symétrique de $\mathbb{Z}[X,Y]$ s'exprime de manière polynomiale en σ et π, *id est*, si $P \in \mathbb{Z}[X,Y]$ est symétrique, on dispose de $Q \in \mathbb{Z}[X,Y]$ tel que $P(X,Y) = Q(X+Y, XY)$. En particulier, ce résultat est valable pour les polynômes homogènes palindromiques qui sont symétriques.

Soit $R \in \mathbb{Z}[X]$ de degré d pair. On pose $\tilde{R} \in \mathbb{Z}[X,Y]$ son polynôme homogénéisé, définit de la manière suivante : si $R(X) = \sum_{k=0}^{d} a_k X^k$, alors $\tilde{R}(X,Y) = \sum_{k=0}^{d} a_k X^k Y^{d-k}$. On dispose de $Q \in \mathbb{Z}[U,V]$ tel que $\tilde{R}(X,Y) = Q(X+Y, XY)$.

Soit $X^a Y^b$ un monôme de $\tilde{R}$, alors $a+b=d$ et est pair. Donc il n'y a pas de puissance impaire de U dans $Q(U,V)$. De plus $(X+Y)^2 = X^2+Y^2+2XY$ donc on dispose de $\hat{Q} \in \mathbb{Z}[U,V]$ tel que $\tilde{R}(X,Y) = \hat{Q}(X^2+Y^2, XY)$. En outre le degré de Q est $\frac{d}{2}$.

On a : $R(x) = \tilde{R}(X,1) = \hat{Q}(X^2+1, 1)$. Donc $R(x) = X^{d/2}\hat{Q}(X + X^{-1}, 1)$. On pose $S \in \mathbb{Z}[T]$ tel que $S(T) = \hat{Q}(T,1)$. S convient. □

Soit n un entier impair, supérieur à 2. On définit le polynôme $P_n \in \mathbb{Z}[X]$ par $P_n(X) = X^{n-1} + \ldots + X + 1$. C'est un polynôme palindromique de degré pair. On dispose donc de $V_n \in \mathbb{Z}[T]$, de degré $\frac{n-1}{2}$ tel que $P_n(X) = X^{\frac{n-1}{2}} V_n(X+X^{-1})$. On définit enfin $K_n \in \mathbb{Z}[Y]$ par $K_n(Y) = V_n(Y+2)$. Nous avons besoin des résultats suivants sur les polynômes K_n.

Proposition.

i) Pour tout $n > 2$ impair, K_n est unitaire de degré $\frac{n-1}{2}$;

ii) Pour tout $n > 2$ impair, $K_n(0) = n$;

iii) Pour tout p premier impair, dans $\mathbb{F}_p[X]$, $K_p(Y) = Y^{\frac{p-1}{2}}$.

Démonstration. i) Cela se vérifie aisément par construction.

ii) On a : $K_n(0) = V_n(2) = V_n(1 + 1/1) = P_n(1) = n$

iii) Pour tout $n > 2$, on a : $P_n(X) = \dfrac{X^n - 1}{X - 1}$. Soit p un nombre premier impair, en se plaçant dans $\mathbb{F}_p[X]$, on a : $X^p - 1 = (X-1)^p$. Ainsi $P_p(X) = (X-1)^{p-1}$.

$$\begin{aligned} V_p(X + X^{-1}) &= X^{-\frac{p-1}{2}}(X-1)^{p-1} \\ &= (X^{-1}(X-1)^2)^{\frac{p-1}{2}} \\ &= (X + X^{-1} - 2)^{\frac{p-1}{2}} \end{aligned}$$

Et ainsi, dans $\mathbb{F}_p[X]$, on a : $K_p(Y) = Y^{\frac{p-1}{2}}$. □

Nous sommes donc à présent à même d'exprimer le symbole de Legendre comme un résultant.

Proposition.

Soient p et q deux nombres premiers impairs. On a alors :

$$\left(\frac{q}{p}\right) = Res(K_p, K_q) \quad .$$

Démonstration. Si p et q sont égaux le résultat est immédiat car le symbole de Legendre et le résultant sont nuls. On peut donc supposer que p et q sont distincts.

Les polynômes K_p et K_q sont à coefficients entiers, leur résultant est donc un entier. Supposons par l'absurde que ce résultant ne soit pas un élément inversible de $\mathbb{Z}$. Dans ce cas on dispose de $r \in \mathbb{Z}$, nombre premier, qui le divise. En tant que polynôme de $\mathbb{F}_r[X]$, les polynômes K_p et K_q ne sont donc pas premiers entre-eux. On dispose donc d'une extension de corps $\mathbb{L}$ de $\mathbb{F}_r[X]$ et d'un élément $y \in \mathbb{L}$ tel que y soit une racine commune de K_p et K_q.

Quitte à faire une nouvelle extension, on peut supposer que le polynôme $X^2 - (y+2)X + 1 \in \mathbb{L}[X]$ admette une racine dans $\mathbb{L}$. On la note x. On remarque que x est inversible car il est non nul. ainsi, il vérifie : $x + x^{-1} - 2 = y$. On a donc :

$$0 = K_p(y) = V_p(y+2) = Vp(x + x^{-1}) = x^{-\frac{p-1}{2}} P_p(x) \quad .$$

Ainsi, x est une racine de $X^p - 1$ dans une extension de $\mathbb{F}_r$. C'est de la même manière une racine de $X^q - 1$. Si x était égal à 1, dans ce cas, y serait nul mais ceci est absurde car dans $\mathbb{Z}$, on a $K_p(0) = p$ et $K_q(0) = q$ et p et q ne peuvent pas être tous les deux congrus à 0 modulo r. Donc x est différent de 1. Ceci conduit à une absurdité car 1 est la seule racine p-ième et q-ième de l'unité.

On a donc montrer que le résultant de K_p et K_q était un inversible de $\mathbb{Z}$, *id est* : $Res(K_p, K_q) \in \{-1, 1\}$. Pour conclure on va calculer ce résultant dans F_p.

$$\begin{aligned} Res(K_p, K_q) &= Res(Y^{\frac{p-1}{2}}, K_q) \\ &= [Res(Y, K_q)]^{\frac{p-1}{2}} \\ &= K_q(0)^{\frac{p-1}{2}} \end{aligned}$$

On a donc montré que $Res(K_p, K_q)$ et $\left(\dfrac{q}{p}\right)$ ont la même réduction modulo p. De plus ils sont tous les deux égaux à 1 ou -1. Comme p est impair alors 1 et -1 ont une réduction différente modulo p. Donc on a bien l'égalité annoncée. □

Pour démontrer la loi de réciprocité quadratique, il suffit juste d'utiliser le défaut de symétrie du résultant :

$$\left(\frac{q}{p}\right) = Res(K_p, K_q) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} Res(K_q, K_p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) \quad .$$

En plus d'apporter une démonstration de cette loi, la méthode utilisée fournit une expression trigonométrique du symbole de Legendre. En effet, on montre que les racines de V_n sont les $\{\omega_k + \omega_k^{-1} / 1 \leqslant k \leqslant \dfrac{n-1}{2}\}$, où $\omega_k = e^{\frac{2ik\pi}{n}}$. On montre alors que $K_n(Y) = \Pi_{k=1}^{\frac{n-1}{2}}(Y + 4\sin^2\left(\dfrac{k\pi}{n}\right))$. En utilisant l'expression du résultant avec les racines on obtient l'expression trigonométrique du symbole de Legendre.

Adapté du travail de Baptiste Huguet.