Géométrie : exercices

Résultant, Bézout, et paramétrisations

D. Kohel

01/12/2020

Rappel qu'on a deux formules (algorithmes) pour le calcule de $Res(f,g)$.

(i) Si $f = a_0 x^l + \cdots + a_l$

$g = b_0 x^m + \cdots + a_m$, on a

$$Res(f,g) = \det \begin{pmatrix} a_0 & & 0 & b_0 & & \\ & \ddots & & & \ddots & \\ & & a_0 & & & b_0 \\ a_l & & & b_m & & \\ & \ddots & & & \ddots & \\ 0 & & a_l & & & b_m \end{pmatrix}, \text{ et}$$

(ii) $Res(f,g) = a_0^m \det(\mu(g))$, où

$\mu(g) =$ mult. par g sur $B = k[x]/(f(x))$.

Ex. 1 Calculer $Res(f,g) =$

$$Res(x^3 + 4x - 1, 2x^2 + 3x + 7).$$

On verifier que $Res(f,g) = 216 \in \mathbb{Z}$.

Rappel: $Res(f,g) \in \mathbb{Z}[a_0, \ldots, a_l, b_0, \ldots, b_m]$.

Remarque $216 = 2^3 3^3$

On a donc (par defn (i)):

$$\mathrm{Res}(f,g) = \det\left(\begin{bmatrix} 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 3 & 2 & 0 \\ 4 & 0 & 7 & 3 & 2 \\ -1 & 4 & 0 & 7 & 3 \\ 0 & -1 & 0 & 0 & 7 \end{bmatrix}\right) = 216$$

$$= \det\left(\begin{bmatrix} 7 & 2 & 3 \\ 3 & -1 & -10 \\ 2 & 3 & -1 \end{bmatrix}\right) = \text{det de } \mu(g)$$

On calcule le déterminant de $\mu(g)$ dans la base $\{1, x, x^2\}$ de $k[x]/(x^3+4x-1)$.

On a: $1 \longmapsto g = 2x^2+3x+7$

$x \longmapsto xg = 2x^3+3x^2+7x$

N.B. $x^3 \equiv -4x+1$ $\quad = 3x^2-x+2$

$x^2 \longmapsto x^2 g = x(3x^2-x+2)$

$= 3x^3-x^2+2x$

$= -x^2-10x+3.$

Dans la base $\{x^2, x, 1\}$ (changeant l'ordre) on échange l'ordre des colonnes et des lignes. Le déterminant est changé par $(-1)^2 = 1$.

Rappel. L'échange des lignes et des colonnes est l'action d'une permutation σ. (Ici $\sigma = (1\,3)$.)
La signature d'une permutation est un homomorphisme de groupe

$$S_n \xrightarrow{\text{sign}} \{\pm 1\}$$

dont le noyau est A_n. On peut définir $\text{sign}(\sigma) = (-1)^r$ où r est le nombre de transpositions dans une express pour σ en tant que produit de transpositions.

Conclusion. $\det(\mu(g))$ est bien défini indép. de l'ordre de la base (et en effet du choix de base).

On a démontrer que le résultat de f et g dans $\mathbb{Z}$ est $216 = (2.3)^3$

N.B. Le coeffs $a_0, \dots, a_3$ et $b_0, \dots, b_2$ de f et g sont dans $\mathbb{Z}$, alors

$$\underbrace{\mathbb{Z}[a_0, \dots, a_3, b_0, \dots, b_2]}_{\text{extension d'anneau par } a_0, \dots, a_3, b_0, \dots, b_2 \text{ sous les ops de } + \text{ et } \cdot} = \mathbb{Z}.$$

Mais, on rappel que

$\mathrm{Res}(f, g) = 0$ dans un corps k ssi f et g ont une racine comme (dans k). On peut intrepreter f, g comme polynômes dans $\mathbb{F}_2[x]$ ou $\mathbb{F}_3[x]$. Comme $216 = 0$ dans ces corps, ça veut dire que f et g ne sont pas premier entre eux.

Par exemple pour $\mathbb{F}_2 = k$:

$f = x^3 + 4x - 1 = x^3 + 1$, et

$g = 2x^2 + 3x + 7 = x + 1$.

En effet, $\text{pgcd}(x^3+1, x+1) = x+1$.

Ils ont la racine $x=1$ en commun.

Pour $\mathbb{F}_3 = k$:

$f = x^3 + x + 2$ et $g = 2x^2 + 1$.

On a alors

$$\text{pgcd}(x^3+x+2,\ 2x^2+1)$$

$$= \text{pgcd}(2x+2,\ 2x^2+1) = \text{pgcd}(f+xg,\ g)$$

$$\begin{array}{r|l} x^3+x+2 & f \\ +\ 2x^3+x & xg \\ \hline 2x+2 & \end{array}$$

$$= \text{pgcd}(x+1, (x+1)(x-1)) = x+1.$$

Ils ont la racine $x=-1$ en commun.

<u>Remarque</u>. Comme le resultat

$\text{Res}(f,g) = 216 \neq 0$ { dans $\mathbb{Q}$; dans $\mathbb{F}_p$, $p \neq 2,3$

on peut conclure que

(i) f et g sont premier entre eux sur $\mathbb{Q}$ et sur $\mathbb{F}_p$,

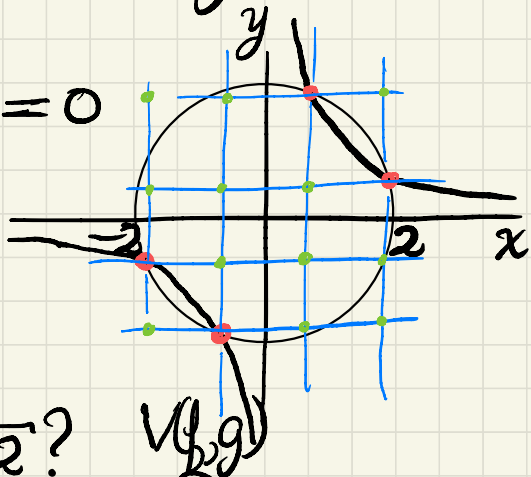
(ii) en particulier ils n'ont pas de racine commune.

Le résultat est à la fois un outil en arithmétique et en géométrie

<u>Ex. 2</u> On considère le système

$$f = xy - 1 = 0$$
$$g = x^2 + y^2 - r^2 = 0$$

dans $\mathbb{A}^2$.



Quels sont les solutions pour $r = 2$? $r = 1$? $r = \sqrt{2}$?

$V(f,g) \subseteq \mathbb{A}^2 \xrightarrow{\pi_i} \mathbb{A}^2$

$\pi_1((x,y)) = x$ et $\pi_2((x,y)) = y$,

qui induisent $\pi_i : V(f,g) \longrightarrow \mathbb{A}^1$.

Le resultant permet de calculer les projections.

$$\mathrm{Res}_x(f,g) = \det\left(\begin{bmatrix} y & 0 & 1 \\ -1 & y & 0 \\ 0 & -1 & y^2-r^2 \end{bmatrix}\right)$$

$$= y^2(y^2-r^2)+1$$

$$= y^4 - r^2y^2 + 1.$$

Par symétrie on a:

$$\mathrm{Res}_y(f,g) = x^4 - r^2x^2 + 1.$$

Racines : $\pm\sqrt{(r^2 \pm \sqrt{r^4-4})/2}$

Alors pour

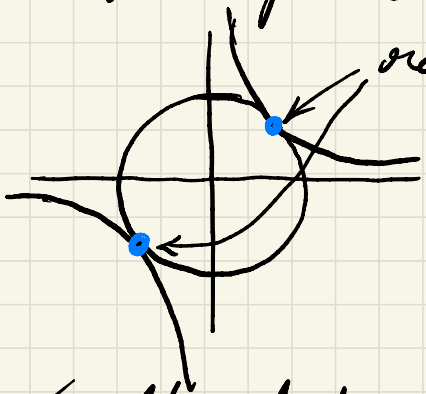
$r=2$: $\pm\sqrt{2\pm\sqrt{3}} \in \mathbb{R}$

$r=1$: $\pm\sqrt{(1\pm\sqrt{-3})/2} \in \mathbb{C}$

$r=\sqrt{2}$: doubles racines ± 1.

N.B. Dans les trois cas on a quatre racines dans $\mathbb{Q}$, comptées

avec multiplicités :



Le résultant permet de conclure que les solutions de $f=g=0$ sont dans (si $r \neq \sqrt{2}$) :

$$\left\{ \pm \sqrt{\frac{r^2 \pm \sqrt{r^4-4}}{2}} \right\}^2 \subseteq \mathbb{A}^2_{\overline{\mathbb{Q}}} = \mathbb{A}^2(\overline{\mathbb{Q}})$$

un ensemble de 16 points.

Pour $r=\sqrt{2}$: Solutions $\{(-1,-1),(1,1)\}$ sont dans $\{\pm 1\} \times \{\pm 1\}$, un ensemble de quatre points.

Autre approche à ce problème :

Paramétrisation d'un conique.

Le parabole $xy=1$ a une paramétrisation : $(x,y)=(t,t^{-1})$.

En prenant l'intersection avec le cercle $x^2+y^2=r^2$ on trouve :

$$t^2+t^{-2}=r^2$$

et donc $t^4-r^2t^2+1=0$.

Les quatre racines donnent les quatre points de l'intersection par la paramétrisation $(x,y)=(t,t^{-1})$.

On peut aussi faire une paramétrisation du cercle. Comment ?

Théorème (Bezout)

Le nombre de solutions de l'intersection de deux courbes ($f=0$ et $g=0$) dans $\mathbb{P}^2$ est le produit de leurs degrés

$$\deg f \cdot \deg g,$$

compté avec multiplicités. (Ou infini s'ils ont une composante en commune).

Remarques. Le degré d'une courbe $V(f)$ est $\deg(f)$, qui est bien-défini car f est homogène. Par exemple $xy=1$ dans $\mathbb{A}^2$ est la partie affine de la courbe projective $XY=Z^2$ dans $\mathbb{P}^2$. Elle est une courbe de degré 2.

Si on calcule

$\mathrm{Res}_Y(f,g)$

pour $f, g \in k[X,Y,Z]$, on a un polynôme homogène de degré $\deg(f)\cdot\deg(g)$ en X et Z.

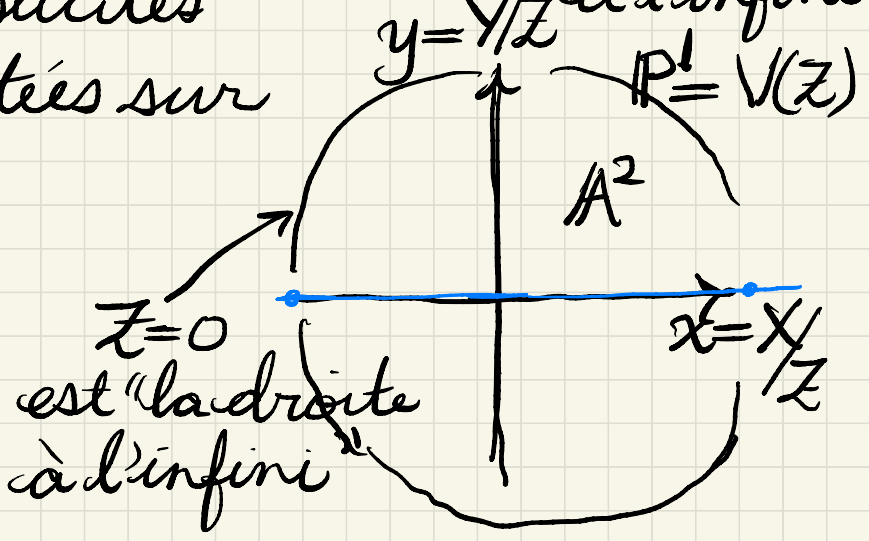
Il a donc une factorisation unique dans $k[X,Z]$:

$$\mathrm{Res}_Y(f,g) = c\left(\prod_{i=1}^{r}(X-\gamma_i Z)^{m_i}\right)\cdot Z^{m_0}$$

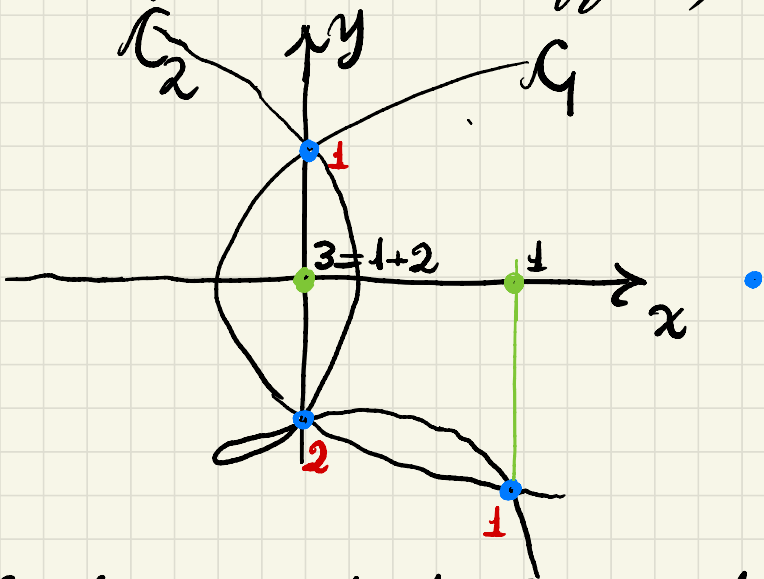
où $\sum_{i=0}^{r} m_i = \deg(f)\cdot\deg(g)$

↑ composante à l'infini

Les m_i sont les multiplicités projectées sur $\mathbb{P}^1_{X,Z}$.



Par exemple (partie affine)

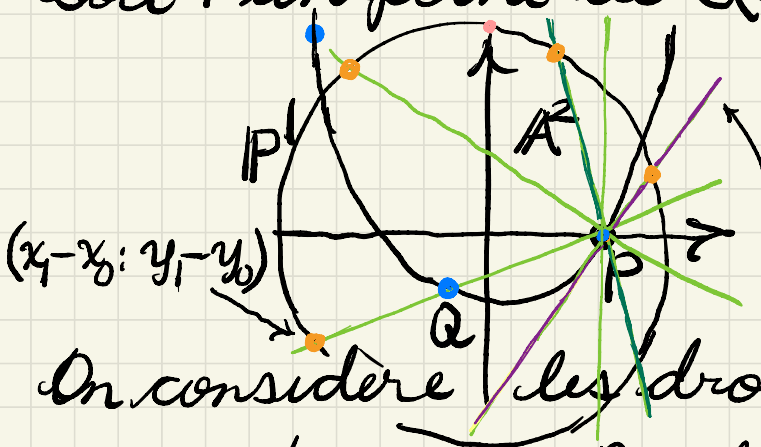


N.B. Si $\deg C_1 = 2$ et $\deg C_2 = 3$, alors il y 4 points d'intersection dans le plan affine. Il y a donc 2 points (ou un point de mult 2) d'intersection à l'infini
La projection vers l'axe x ne permet pas de distinguer un point de mult 3 et 2+1 ou 1+1+1 dans l'intersection, mais la projection à l'axe y "voit" les

bonnes multiplicités 1, 2, 1 des points affines.

Paramétrisation d'un conique C_k projectif du plan $\mathbb{P}^2$

Soit P un point de C(k).



polynôme homogène de degré 2

droite tangente

On considère les droites qui passent par P. Par le théorème de Bezout, chaque droite passe par un unique deuxième point (en bleu), Q. On obtient une proj vers la droite à l'infini, donnée par $Q=(x_1,y_1) \xmapsto{\pi} (x_1-x_0 : y_1-y_0)$, où $P=(x_0,y_0) \in C(k)$, pour $P \neq Q$. Cette projection envoie Q à la

droite $\overline{PQ}$ dans $\mathbb{A}^2$. On identifie $\mathbb{P}^2$ avec des droites en $\mathbb{A}^2$ (en orange) $\leftrightarrow (x_1-x_0 : y_1-y_0) \in \mathbb{P}^1(k)$ passant par P.

$$D(k) = \{(t(x_1-x_0), t(y_1-y_0)) : t \in k\}$$
$$= \{(x,y) \mid (y_1-y_0)(x-x_0) = (x_1-x_0)(y-y_0)\}$$

Remarque. On a utilisé le théorème de Bézout deux fois :

(1) $C \cap D = \{P, Q\}$ est un ensemble de cardinal 2 pour $P \neq Q$,

(2) $D \cap \mathbb{P}^1 = \{\pi(Q)\}$ est un point.
$\mathbb{P}^1 = V(Z)$ = droite à l'infini

En effet par Bézout

$|C \cap D| = 2 = \deg C \cdot \deg D = 2 \cdot 1$,

$|D \cap \mathbb{P}^1| = 1 = \deg D \cdot \deg \mathbb{P}^1 = 1 \cdot 1$.

Exemple classique : le cercle

$$x^2+y^2=1 \quad (X^2+Y^2=Z^2)$$

Soit $P=(1,0)$. On a une paramétrisation :

$$x=\frac{u^2-v^2}{u^2+v^2},\ y=\frac{2uv}{u^2+v^2}$$

ce qui donne $\mathbb{P}^1 \longrightarrow C \subseteq \mathbb{P}^2$:

$$(X:Y:Z)=(u^2-v^2:2uv:u^2+v^2).$$

Si on met $t=u/v$, on a donc

$$x=\frac{t^2-1}{t^2+1},\ y=\frac{2t}{t^2+1},$$

et

$$(X:Y:Z)=(t^2-1:2t:t^2+1).$$

L'inverse de cette paramétrisation est la projection : $\pi : C \to \mathbb{P}^1$

$(1:0:1) \to \infty$

$\|$

$(1,0) \in \mathbb{A}^2$

Décrire cette projection.