Jean Fresnel, le 27 juin 2001

Le théorème de Bézout sur l'intersection des courbes planes

0. Introduction

Le théorème de **Bézout** sur l'intersection des courbes planes (théorème 2.1. , 2.2.) dit qu'une courbe plane de degré n et une courbe plane de degré m se coupent en exactement $n\,m$ points modulo une notion de multiplicité d'intersection. Ce résultat est bien démontré dans l'ouvrage de 1969 de **William Fulton** (*Fu*, p. 112), nous reprenons ici sa démonstration en simplifiant peu de choses.

Sachant que les zéros communs de deux polynômes à deux variables peuvent être décrits par élimination d'une variable, i.e. en considérant le résultant des deux polynômes considérés comme polynômes en l'une des variables, il était normal de savoir si l'on pouvait lire la multiplicité d'intersection en un point à partir du résultant. Cela est décrit par le théorème 3. Si l'essentiel se trouve dans [*W*] , page 109, en revanche la liaison avec la multiplicité d'intersection définie par **Fulton** n'est pas claire.

Enfin pour être le plus "self-contained" possible nous avons ajouté un paragraphe 4. concernant quelques résultats dits classiques.

Le paragraphe 5. traite le cas d'une famille linéaire de coniques et le paragraphe 6. décrit une série d'exemples traités par MAPLE et aimablement communiqués par **Christian Batut**. Le paragraphe 7. essaie de décrire le processus algorithmique qui permettra de calculer la multiplicité d'intersection de 2 courbes en point.

Pour terminer, je dois dire que ce petit exercice est un travail de commande de **Michel Matignon**

1. La multiplicité d'intersection de deux courbes planes

1.1. **Définition de la multiplicité d'intersection** Soient k un corps commutatif, algébriquement clos, $F,G\in k[X,Y]$, sans facteur irréductible commun dans $k[X,Y]$, $p=(\alpha,\beta)\in k^2$, $\mathfrak{M}_{\alpha,\beta}:=(X-\alpha)\,k[X,Y]+(Y-\beta)\,k[X,Y]$. Alors on appelle *multiplicité d'intersection de* F *et* G *en* p, le nombre $i(p;F,G):=\dim_k\frac{k[X,Y]_{\mathfrak{M}_{\alpha,\beta}}}{(F,G)}$. Ce nombre est fini (théorème 2.1. partie 1.). De plus $i(p;F,G)\geq 1$ si et seulement si $F(\alpha,\beta)=G(\alpha,\beta)=0$, i.e. si p est un point commun aux deux courbes planes définies par F et G.

1.2. **Proposition** *Soient* k *un corps commutatif algébriquement clos.*
1.2.1. *Soient* $F,G\in k[X,Y]$, $p\in k^2,\lambda\in k$. *Alors on a*
$i(p;F,G)=i(p;F,G+\lambda F)$.
1.2.2. *Soient* $F,G,H\in k[X,Y]$ *avec* F *et* G (resp. F *et* H) *sans facteur irréductible commun dans* $k[X,Y]$, $p\in k^2$. *Alors on a*
$i(p;F,GH)=i(p;F,G)+i(p;F,H)$.
1.2.3. *Soient* σ *un* k*-automorphisme de* $k[X,Y]$, $P(X,Y):=\sigma(X)$, $Q(X,Y):=\sigma(Y)$, $p=(\alpha,\beta)$, $\sigma(p)=(P(\alpha,\beta),Q(\alpha,\beta))$. *Alors on a*
$i(\sigma(p);\sigma(F),\sigma(G))=i(p;F,G)$.

Démonstration 1) La démonstration de 1. est immédiate.
2) Montrons 2. .Soient $p=(\alpha,\beta)$, $\mathfrak{M}=(X-\alpha)\,k[X,Y]+(Y-\beta)\,k[X,Y]$, $S:=k[X,Y]_{\mathfrak{M}}$. Considérons la suite
(1) $\quad\{0\}\to\frac{S}{(F,H)}\xrightarrow{\alpha}\frac{S}{(F,GH)}\xrightarrow{\beta}\frac{S}{(F,G)}\to 0$,
où β est la surjection canonique et α est l'application induite par $z\mapsto Gz$ de S dans S. Il faut montrer que cette suite est exacte. Il suffit de vérifier que α est injectif, le reste est immédiat. Si $zG=AF+BGH$, on a $G\mid AF$. Or F et G n'ont pas de facteur irréductible en commun dans $k[X,Y]$, donc aussi dans S (Fr. F.7.5.1.), ainsi $G\mid A$, i.e. $A=A_1G$. Il suit de cela que $z=A_1F+BH$, ce qui prouve que α est injectif. Sachant que (1) est exacte, on a la formule $0=\dim_k\frac{S}{(F,H)}-\dim_k\frac{S}{(F,GH)}+\dim_k\frac{S}{(F,G)}$, ce qui n'est autre chose que $i(p;F,GH)=i(p;F,G)+i(p;F,H)$.
3) La démonstration de 3. est immédiate.

1.3. **Définition de la multiplicité d'intersection pour les courbes planes projectives**

Soient k un corps commutatif, algébriquement clos, $F, G \in k[X_0, X_1, X_2]$ des polynômes homogènes avec $\deg F = n, \deg G = m$ et sans facteur irréductible commun dans $k[X_0, X_1, X_2]$. Soit V la variété projective définie par $V := \mathrm{Proj}(\frac{k[X_0, X_1, X_2]}{(F, G)})$. Alors les points fermés de V s'identifient à l'ensemble des $p = (x_0 : x_1 : x_2) \in \mathbb{P}^2(k)$ tels que $F(p) = G(p) = 0$.

1.3.1. Si donc p est un tel point, on appelle *multiplicité d'intersection de F et G en p* le nombre $i(p; F, G) := \dim_k \frac{\mathcal{O}_{V,p}}{(F, G)}$. Ce nombre est fini. Si p ne satisfait pas $F(p) = G(p) = 0$, alors par définition $i(p; F, G) = 0$.

1.3.2. *Soient σ un k-automorphisme de $k[X_0, X_1, X_2]$,* $P_i(X_0, X_1, X_2) := \sigma(X_i)$ *pour* $0 \le i \le 2$, $p = (x_0 : x_1 : x_2)$, $\sigma(p) := (P_0(x_0, x_1, x_2) : P_1(x_0, x_1, x_2) : P_2(x_0, x_1, x_2))$. *Alors on a* $i(\sigma(p); \sigma(F), \sigma(G)) = i(p; F, G)$.

1.3.3. *Soient* $p = (x_0 : x_1 : x_2)$, supposons $x_0 \neq 0$, $\alpha := \frac{x_1}{x_0}$, $\beta = \frac{x_2}{x_0}$, $q = (\alpha, \beta)$, $F^\sharp(X, Y) := F(1, X, Y)$, $G^\sharp(X, Y) := G(1, X, Y)$. Alors on a $i(p; F, G) = i(q; F^\sharp, G^\sharp)$ *(on a un résultat analogue si $x_1 \neq 0$, ou $x_2 \neq 0$).*

2. Le théorème de Bézout pour l'intersection des courbes planes (ou un résultat global)

2.1. **Théorème de Bézout affine** *Soient k un corps commutatif, algébriquement clos, $F, G \in k[X, Y]$, $\deg F = n$, $\deg G = m$, $F = F_0 + F_1 + \ldots + F_n$, $G = G_0 + G_1 + \ldots + G_m$ où F_i* (resp. G_i) *est la composante homogène de degré i de F* (resp. G).

1. *On suppose que F et G n'ont pas de facteur irréductible en commun dans $k[X, Y]$. Alors $\frac{k[X, Y]}{(F, G)}$ est un k-espace vectoriel de dimension finie. En particulier les $(\alpha, \beta) \in k^2$ tels que $F(\alpha, \beta) = G(\alpha, \beta) = 0$ sont en nombre fini.*

2. *On suppose que F et G* (resp. F_n *et* G_m) *n'ont pas de facteur irréductible en commun dans $k[X, Y]$. Alors on a* $\dim_k \frac{k[X, Y]}{(F, G)} = n\,m$.

3. *On suppose que F et G* (resp. F_n *et* G_m) *n'ont pas de facteur irréductible en commun dans $k[X, Y]$. Alors on a* $\sum_{p \in k^2} i(p; F, G) = \deg F \deg G$.

Démonstration

1) *La dimension du k-espace vectoriel $\frac{k[X,Y]}{(F,G)}$ est finie.*

1.α) *On peut supposer que F est unitaire en Y.* Soient $\lambda\in k$, σ_λ le k-automorphisme de $k[X,Y]$ défini par $\sigma_\lambda(X)=X+\lambda Y$ et $\sigma_\lambda(Y)=Y$. Facilement il existe $\lambda\in k$ tel que $F_n(\lambda,1)\neq 0$. Soit $\sigma:=\sigma_\lambda$, alors $\deg_Y\sigma(F)=n$, $\sigma(F)$ et $\sigma(G)$ sont sans facteur irréductible commun dans $k[X,Y]$. En plus $\frac{k[X,Y]}{(F,G)}$ est isomorphe à $\frac{k[X,Y]}{(\sigma(F),\sigma(G))}$.

Si donc le théorème est vrai pour $(\sigma(F),\sigma(G))$, il sera vrai pour (F,G).

1.β) *On a* $(Fk[X,Y]+Gk[X,Y])\cap k[X]\neq\{0\}$. La méthode la plus rapide consiste à utiliser le résultant $R(X)$ de $F(X,Y)$ et $G(X,Y)$ considérés comme polynômes en Y, par Fr. F.7.9.22., il est non nul.

La seconde méthode consiste à remarquer que F et G comme élément de $k(X)[Y]$ sont premiers entre eux. En effet si $D\mid F$ et $D\mid G$ avec $\deg_Y D\geq 1$ et $D\in k(X)[Y]$, on déduit les relations $\Delta F_1=FS$ et $\Delta G_1=GS$ avec $\Delta,F_1,G_1\in k[X,Y]$, $\deg_Y\Delta\geq 1$ et $S\in k[X]-\{0\}$. Sachant que $k[X,Y]$ est factoriel, il existe un facteur irréductible Δ_1 de Δ avec $\deg_Y\Delta_1\geq 1$, et ainsi $\Delta_1\mid F$, $\Delta_1\mid G$. C'est donc impossible. Ainsi F,G sont premiers entre eux dans $k(X)[Y]$ et par **Bézout** il existe $A,B\in k[X,Y]$, $C(X)\in k[X]-\{0\}$ tels que $AF+BG=C$.

Il existe donc $R(X)\in(Fk[X,Y]+Gk[X,Y])$ avec $R\neq 0$.

1.γ) *On a* $\dim_k\frac{k[X,Y]}{(F,G)}\leq rn$, *avec* $r:=\deg R$. Soit $\pi:k[X,Y]\to\frac{k[X,Y]}{(R,F)}$ la surjection canonique, alors sachant que $\deg_Y F=n$, on a $\pi(\sum_{i=0}^{r-1}\sum_{j=0}^{n-1}kX^iY^j)=\frac{k[X,Y]}{(R,F)}$. Cela montre que la dimension de $\frac{k[X,Y]}{(R,F)}$ est majorée par rn. Comme $(R,F)\subset(F,G)$, on a aussi $\dim_k\frac{k[X,Y]}{(F,G)}\leq rn$.

1.δ) *Les $(\alpha,\beta)\in k^2$ tels que $F(\alpha,\beta)=G(\alpha,\beta)=0$ sont en nombre fini.*

Soient $S:=k[X,Y]$, $T:=\frac{k[X,Y]}{(F,G)}$, $\rho:S\to T$ la surjection canonique, $\mathfrak{Z}$ l'ensemble des maximaux $\mathfrak{M}$ de S tels que $(F,G)\subset\mathfrak{M}$. Alors ρ induit une bijection de $\mathfrak{Z}$ sur les maximaux de T. Par 1.γ) et 4.2. ces maximaux sont en nombre fini ; disons $\rho(\mathfrak{M}_1),\rho(\mathfrak{M}_2),\ldots,\rho(\mathfrak{M}_r)$. Par ailleurs $\mathfrak{Z}$ est en bijection avec les éléments $(\alpha_i,\beta_i)\in k^2$ tels que $F(\alpha_i,\beta_i)=G(\alpha_i,\beta_i)=0$ par $\mathfrak{M}_i=(X-\alpha_i)S+(Y-\beta_i)S$.

2) *On a* $\dim_k\frac{k[X,Y]}{(F,G)}=nm$. Soient $S:=k[X,Y]$, $t\geq 0$, $S_t:=\{P\in S\mid\deg P\leq t\}$. Soit la suite

(1) $\quad 0\to S_d\xrightarrow{\alpha}S_{d+m}\times S_{d+m}\xrightarrow{\beta}S_{d+m+n}\xrightarrow{\gamma}\frac{k[X,Y]}{(F,G)}$

où γ est la restriction à S_{d+m+n} de la surjection canonique de S sur $\frac{k[X,Y]}{(F,G)}$; de plus α est défini par $\alpha(P)=(PG,-PF)$ et β par

$\beta(A,B)=AF+BG$. Il s'agit de montrer que $\ker\beta=\operatorname{im}\alpha$ et $\ker\gamma=\operatorname{im}\beta$. Facilement $\beta\alpha=0$ et $\gamma\beta=0$. Si $AF+BG=0$, comme F et G n'ont pas de facteur irréductible commun dans l'anneau factoriel $k[X,Y]$, on a $B=-FP$ et $A=GP$ avec $\deg P=d$; ainsi $\ker\beta\subset\operatorname{im}\alpha$. Soit $U\in\ker\gamma$, on a donc $U=AF+BG$, il s'agit de montrer qu'il existe une telle écriture avec $\deg A\leq d+m$, et $\deg B\leq d+n$. Soit $U=AF+BG$ avec $\deg A$ minimum. Si $\deg A\leq d+m$, alors on a $\deg B\leq d+n$. Si $\deg A=d'+n>d+n$, alors $\deg B=d'+n$. En décomposant A et B en composantes homogènes, on a $A=A_0+A_1+\ldots+A_{d'+m}$, $B=B_0+B_1+\ldots+B_{d'+n}$. Il suit que $0=A_{d'+m}F_n+B_{d'+m}G_m$, comme F_n et G_m n'ont pas de facteurs irréductibles en commun, on a $A_{d'+n}=G_mP$, $B_{d'+m}=-F_nP$. Soient $A_1:=A-PG$, $B_1=B-PF$, on a $U=A_1F+B_1G$ et $\deg A_1<\deg A$. Cela contredit la minimalité du degré de A , ainsi l'hypothèse $\deg A>d+m$ est à rejeter. Sachant que $\frac{k[X,Y]}{(F,G)}$ est de dimension finie, il suit que pour d assez grand, on a $\gamma(S_{d+m+n})=\frac{k[X,Y]}{(F,G)}$

De la suite exacte à "gauche" (1) on déduit que

(2) $0=\dim_k S_d-\dim_k(S_{d+m}\times S_{d+n})+\dim_k S_{d+m+n}-\dim_k\gamma(S_{d+m+n})$.

Sachant que $\dim_k S_t=\frac{(t+1)(t+2)}{2}$, on déduit de (2) que $\dim_k\gamma(S_{d+m+n})=nm$. Comme $\frac{k[X,Y]}{(F,G)}=\gamma(S_{d+m+n})$, on a bien $\dim_k(\frac{k[X,Y]}{(F,G)})=nm$.

3) *On a* $\sum_{p\in k^2} i(p;F,G)=\deg F\deg G$. Soient $S:=k[X,Y]$, $T:=\frac{k[X,Y]}{(F,G)}$, $\rho:S\to T$ la surjection canonique, $\mathfrak{L}$ l'ensemble des maximaux $\mathfrak{M}$ de S tels que $(F,G)\subset\mathfrak{M}$. Alors ρ induit une bijection de $\mathfrak{L}$ sur les maximaux de T . Par 2.1. partie 1. et 4.2. ces maximaux sont en nombre fini ; disons $\rho(\mathfrak{M}_1),\rho(\mathfrak{M}_2),\ldots,\rho(\mathfrak{M}_r)$. Par ailleurs $\mathfrak{L}$ est en bijection avec les éléments $(\alpha_i,\beta_i)\in k^2$ tels que $F(\alpha_i,\beta_i)=G((\alpha_i,\beta_i)=0$ par $\mathfrak{M}_i=(X-\alpha_i)S+(Y-\beta_i)S$. Toujours par 4.2. , T est isomorphe à $\prod_{i=1}^{r}T_{\rho(\mathfrak{M}_i)}$ et comme $T_{\rho(\mathfrak{M}_i)}\simeq\frac{S_{(\mathfrak{M}_i)}}{(F,G)}$, on a $\dim_k T=\prod_{i=1}^{r}\dim_k\frac{S_{\mathfrak{M}_i}}{(F,G)}$. Compte tenu de 1.1. et de 2.1. partie 2. , on a bien $\sum_{p\in k^2} i(p;F,G)=\deg F\deg G$.

2.2. **Théorème de Bézout projectif** *Soient k un corps commutatif, algébriquement clos, $F,G\in k[X_0,X_1,X_2]$, homogènes avec* $\deg F=n$, $\deg G=m$. *On suppose que F et G n'ont pas de facteur irréductible en commun dans $k[X_0,X_1,X_2]$. Alors on a* $\sum_{p\in\mathbb{P}^2(k)} i(p;F,G)=\deg F\deg G$.

Démonstration Facilement $F(1,X_1,X_2)$ et $G(1,X_1,X_2)$ (resp. $F(X_0,1,X_2)$ et $G(X_0,1,X_2)$, $F(X_0,X_1,1)$ et $G(X_0,X_1,1)$) sont sans facteur commun dans $k[X_1,X_2]$ (resp. $k[X_0,X_2]$, $k[X_0,X_1]$). Il suit de 2.1. partie 1. que les $(x_0:x_1:x_2)\in\mathbb{P}^2(k)$ tels que $F(x_0,x_1,x_2)=G(x_0,x_1,x_2)=0$ sont en nombre fini. En conséquence, il existe $\lambda,\mu\in k$ tels que $x_0+\lambda x_1+\mu x_2\neq 0$ pour tout $(x_0:x_1:x_2)$, zéro commun de F et G . Soient σ l'automorphisme de $k[X_0,X_1,X_2]$ défini par $\sigma(X_0)=X_0-\lambda X_1-\mu X_2$, $\sigma(X_1)=X_1$, $\sigma(X_2)=X_2$ et $F^\natural(X_0,X_1,X_2)=\sigma(F)$, $G^\natural(X_0,X_1,X_2)=\sigma(G)$. Il suit que si $(x_0:x_1:x_2)$ est un zéro commun de $F^\natural$ et $G^\natural$, on a $x_0\neq 0$. Il suit de cela que $\deg F^\natural(1,X_1,X_2)=n$, $\deg G^\natural(1,X_1,X_2)=m$, que $F^\natural(1,X_1,X_2)$ et $G^\natural(1,X_1,X_2)$ sont sans facteur commun dans $k[X_1,X_2]$. Posons $F^\sharp(X_1,X_2):=F^\natural(1,X_1,X_2)$, $G^\sharp(X_1,X_2):=G^\natural(1,X_1,X_2)$, on a donc $F^\sharp=F_0^\sharp+F_1^\sharp+\ldots+F_n^\sharp$, $G^\sharp=G_0^\sharp+G_1^\sharp+\ldots+G_m^\sharp$. Il suit de ce que F et G n'ont pas de zéro commun de la forme $(0:x_1:x_2)$, que $F_n^\sharp$ et $G_m^\sharp$ sont sans zéro commun et donc sans facteur irréductible en commun. alors le théorème 2.2. est une conséquence de 2.1. partie 3. .

3. Interprétation de la multiplicité d'intersection de deux courbes planes en termes de résultant (ou un résultat local)

3.0. **Rappels sur le résultant de deux polynômes** Soient A un anneau commutatif, $f,g\in A[X]$, $n=\deg f$, $m=\deg g$, $f(X)=a_0X^n+a_1X^{n-1}+\ldots+a_n$, $g(X)=b_0X^m+b_1X^{m-1}+\ldots+b_m$, alors on appelle résultant de f et g et on le note $\mathrm{res}(f,g)$, l'élément $\mathrm{res}_{n,m}(\boldsymbol{a},\boldsymbol{b})$ avec $\boldsymbol{a}:=(a_0,a_1,\ldots,a_n)$, $\boldsymbol{b}:=(b_0,b_1,\ldots,b_m)$ et défini selon Fr. , F.7.7.1.1. . En particulier si f se factorise sous la forme $f(X)=a_0(X-\xi_1)(X-\xi_2)\ldots(X-\xi_n)$, on a $\mathrm{res}(f,g)=a_0^m\prod_{i=1}^n g(\xi_i)$ (Fr. , F..7.7.2.1.). De plus, si $h\in A[X]$, on a $\mathrm{res}(f,g+fh)=a_0^{t-m}\,\mathrm{res}(f,g)$ où $t=\deg(g+fh)$. Enfin on a $\mathrm{res}(ff_1,g)=\mathrm{res}(f,g)\,\mathrm{res}(f_1,g)$ et $\mathrm{res}(f,gg_1)=\mathrm{res}(f,g)\,\mathrm{res}(f,g_1)$ (Fr. , F.7.7.2.3.).

3.1. Théorème (multiplicité d'intersection et résultant) *Soient* k *un corps algébriquement clos,* $F,G\in k[X,Y]$ *, avec* $\deg F=n$, $\deg G=m$ *et* $\deg_Y F=n$ *; en plus on suppose que* F *et* G *n'ont pas de facteur irrréductible en commun. Soit* $R(X):=\mathrm{res}(F,G)$ *où* F *et* G *sont considérés comme polynômes de la variable* Y *. Enfin on note toujours* $i(p;F,G)$ *la multiplicité d'intersection de* F *et* G *en* p *, et* $\mathrm{val}_{(X-\alpha)}(R(X))$ *l'entier* ν *tel que* $(X-\alpha)^{\nu}\mid R(X)$ *et* $(X-\alpha)^{\nu+1}\nmid R(X)$.

1. *Soient* $\alpha\in k$ *et* $p_1=(\alpha,\beta_1),p_2=(\alpha,\beta_2),\ldots,p_r:=(\alpha,\beta_r)$ *l'ensemble des zéros communs à* F *et* G *dont la première coordonnée est* α , $k[X,Y]_{(\alpha,\beta_i)}$ *la localisation de* $k[X,Y]$ *en l'idéal maximal* $(X-\alpha)k[X,Y]+(Y-\beta_i)k[X,Y]$. *Alors on a*
$\sum_{i=1}^{r}\dim_k\left(\frac{k[X,Y]_{(\alpha,\beta_i)}}{(F,G)}\right)=\mathrm{val}_{(X-\alpha)}(R(X))$, i.e.
$\sum_{j=1}^{r} i(p_j;F,G)=\mathrm{val}_{(X-\alpha)}(R(X))$.

2. *En particulier si* $p:=(\alpha,\beta)$, $F(\alpha,\beta)=G(\alpha,\beta)=0$ *et si* $F(\alpha,\gamma)=G(\alpha,\gamma)=0$ *impliquent* $\beta=\gamma$, i.e. F *et* G *ont un seul zéro en commun dont la première coordonnée est* α *. Alors on a*
$i((\alpha,\beta);F,G):=\dim_k\left(\frac{k[X,Y]_{(\alpha,\beta)}}{(F,G)}\right)=\mathrm{val}_{(X-\alpha)}(R(X))$, i.e.
$i(p;F,G)=\mathrm{val}_{(X-\alpha)}(R(X))$.

3. *En particulier on a* $\deg R(X)\le nm$ *; si* $R(X)$ *a toutes ses racines simples,* i.e. $R(X)=\prod_{i=1}^{nm}(X-\alpha_i)$ *avec* $\alpha_i\neq\alpha_j$ *pour* $i\neq j$ *, alors pour chaque* i *il existe un unique* β_i *tel que* $F(\alpha_i,\beta_i)=G(\alpha_i,\beta_i)=0$ *. En particulier* $i(\alpha_j,\beta_j);F,G)=1$ *pour* $1\le j\le nm$.

Démonstration 1) *On suppose que* $F(X,Y)$ *est un irréductible de* $k[X,Y]$.
Soient $y\in K(X)^{alg}$ tel que $F(X,y)=0$, $A:=k[X][y]$, C la clôture intégrale de A (ou de $k[X]$) dans $k(X)[y]$.
1.α) *(le* k*-espace vectoriel* $\frac{S^{-1}C}{S^{-1}A}$ *est de dimension finie)* En utilisant Fr, F.9.4.19. , il existe $d\in k[X]-\{0\}$ tel que $dC\subset A$. Soit $S:=k[X]-Xk[X]$, alors $d(S^{-1}C)\subset S^{-1}A$. Facilement $\frac{(S^{-1}C)}{(S^{-1}A)}$ est isomorphe à $\frac{dS^{-1}C}{dS^{-1}A}$ et ce dernier s'injecte dans $\frac{S^{-1}A}{d(S^{-1}A)}$. Enfin, comme espace vectoriel, $\frac{S^{-1}A}{d(S^{-1}A)}$ est isomorphe à $\left(\frac{S^{-1}k[X]}{dS^{-1}k[X]}\right)^n$ qui est un k-espace vectoriel de dimension majorée par $n\deg(d)$.

1.β) *(le k-espace vectoriel $\frac{S^{-1}A}{g(S^{-1}A)}$ est de dimension finie)* Soit $g:=G(X,y)$, comme $G(X,y)$ est entier sur $k[X]$, il existe $b\in k[X]-\{0\}$ tel que $g\mid d$ dans A. D'une part la surjection $\frac{S^{-1}A}{d(S^{-1}A)}\to\frac{S^{-1}A}{g(S^{-1}A)}$ et d'autre part l'isomorphisme de k-espace vectoriel $\frac{S^{-1}A}{d(S^{-1}A)}\simeq(\frac{S^{-1}k[X]}{d(S^{-1}k[X])})^n$ montrent que $\frac{S^{-1}A}{g(S^{-1}A)}$ est de dimension finie.

1.γ) *(on a $\dim_k(\frac{S^{-1}A}{g(S^{-1}A)})=\dim_k(\frac{S^{-1}C}{g(S^{-1}C)})$)* C'est en effet une conséquence de 1.α), 1.β) et du lemme 4.1..

1.δ) *(on a $\sum_{i=1}^{r}\dim_k(\frac{k[X,Y]_{(\alpha,\beta_i)}}{(F,G)})=\mathrm{val}_{(X-\alpha)}(R(X))$)* Soient $\mathfrak{N}_1,\mathfrak{N}_2,\dots,\mathfrak{N}_{r_2}$ (resp. $\mathfrak{N}_1,\mathfrak{N}_2,\dots,\mathfrak{N}_{r_1}$) les maximaux de $S^{-1}A$ (resp. les maximaux de $S^{-1}A$ qui contiennent $G(X,y)$). Soient $\mathfrak{M}_1,\mathfrak{M}_2,\dots,\mathfrak{M}_s$ (resp. $\mathfrak{M}_1,\mathfrak{M}_2,\dots,\mathfrak{M}_{s'}$) les maximaux de $S^{-1}C$ (resp. les maximaux de $S^{-1}C$ qui contiennent $G(X,y)$). Il suit du lemme 4.2. que l'application diagonale $\frac{S^{-1}A}{(G(X,y))}\xrightarrow{\sim}\prod_{i=1}^{r_1}\frac{(S^{-1}A)_{\mathfrak{N}_i}}{(G(X,y))}$ (resp. $\frac{S^{-1}C}{(G(X,y))}\xrightarrow{\sim}\prod_{i=1}^{s'}\frac{(S^{-1}C)_{\mathfrak{M}_i}}{(G(X,y))}$) est un isomorphisme. En utilisant 1.γ), on a donc

(1) $\sum_{i=1}^{r_1}\dim_k\frac{(S^{-1}A)_{\mathfrak{N}_i}}{(G(X,y))}=\sum_{i=1}^{s'}\dim_k\frac{(S^{-1}C)_{\mathfrak{M}_i}}{(G(X,y))}$.

Soit $\rho:k[X,Y]\to A$ la surjection canonique, alors les $\rho^{-1}(\mathfrak{N}_i\cap A)$ pour $1\le i\le r_1$ sont exactement les maximaux $\mathfrak{A}_i:=(X-\alpha)k[X,Y]+(Y-\beta_i)k[X,Y]$ pour $1\le i\le r$. On a donc $r_1=r$ et $\mathfrak{N}_i=S^{-1}\rho(\mathfrak{A}_i)$ (quitte à permuter les indices). De plus ρ induit un isomorphisme $\tilde{\rho}:\frac{k[X,Y]_{\mathfrak{A}_i}}{(F,G)}\to\frac{(S^{-1}A)_{\mathfrak{N}_i}}{(G(X,y))}$. Enfin si $s<i\le s'$, on a $\dim_k\frac{S^{-1}C_{\mathfrak{M}_i}}{(G(X,y))}=0$. Ainsi la formule (1) devient

(2) $\sum_{i=1}^{r}\dim_k\frac{k[X,Y]_{\mathfrak{A}_i}}{(F,G)}=\sum_{i=1}^{s}\dim_k\frac{(S^{-1}C)_{\mathfrak{M}_i}}{(G(X,y))}$.

Facilement les $\mathfrak{M}_i\cap C$ pour $1\le i\le s$ sont exactement les maximaux de C au-dessus de $(X-\alpha)k[X]$. Il suit alors de 4.5. partie 4. que les $C_{(\mathfrak{M}_i\cap C)}\simeq(S^{-1}C)_{\mathfrak{M}_i}$ sont les anneaux des valuations normalisées de $k(X)[y]$ au-dessus de la valuation $\mathrm{val}_{(X-\alpha)}$ de $k(X)$ définie par $\mathrm{val}_{(X-\alpha)}(X-\alpha)=1$ et triviale sur k. Par 4.5., partie 3., on a

(3) $\mathrm{val}_{(X-\alpha)}(\prod_{i=1}^{n}G(X,\xi_i))=\sum_{i=1}^{r}w_i(G(X,y))$ où $F(X,Y)=(Y-\xi_1)(Y-\xi_2)\dots(Y-\xi_n)$ avec $\xi_i\in k(X)^{alg}$. Sachant que

$\dim_k \frac{(S^{-1}C)_{\mathfrak{M}_i}}{(G(X,y))} = w_i(G(X,y))$ et $R(X) = a_0^t \prod_{i=1}^{n} G(X,\xi_i)$, où $t := \deg_Y G(X,Y)$ et a_0 est l'élément de k, coefficient de Y^n dans $F(X,Y)$ (Fr, F.7.7.2.1., ou 3.0.), la relation (3) donne bien le résultat.

2) *Le cas général* On a $F(X,Y) = A_1(X,Y)A_2(X,Y)\ldots A_r(X,Y)$ avec A_i irréductible de $k[X,Y]$ et $\deg_Y A_i = \deg A_i$. Sachant que

$i(p;F,G) = \prod_{j=1}^{r} i(p;F,A_j)$ (proposition 1.2.) et que

$\operatorname{res}(F,G) = \prod_{j=1}^{r} \operatorname{res}(A_j,G)$ (Fr, F.7.7.2.3., ou 3.0.) on a bien le résultat cherché.

3) La démonstration de 2. est immédiate. Pour 3., il suit de Fr, F.7.7.2.5. que $\deg R(X) \leq n\,m$. Par Fr, F.7.7.1.9. il suit que $F(\alpha,\beta) = G(\alpha,\beta) = 0$ implique $R(X) = 0$; de plus si $R(X) = 0$, par Fr, F.7.7.1.9. il existe $\gamma \in k$ tel que $F(\alpha,\gamma) = G(\alpha,\gamma) = 0$. Il suit alors de 2.2. que les (α_j,β_j) pour $1 \leq j \leq n\,m$ sont les seuls zéros communs et que $i(\alpha_j,\beta_j;F,G) = 1$.

3.2. Remarque *Soient k un corps algébriquement clos, $F, G \in k[X,Y]$, avec* $\deg F = n$, $\deg G = m$ *et F* (resp. G) *unitaire en Y de degré n* (resp. m) *; en plus on suppose que F et G n'ont pas de facteur irrréductible en commun. Soit $R(X) := \operatorname{res}(F,G)$ où F et G sont considérés comme polynômes de la variable Y. Soit $\lambda \in k$, alors on a $R(X) := \operatorname{res}(F, G+\lambda F)$.*

4. Appendice ou rappel de quelques résultats classiques

4.1. Un lemme sur la dimension dans les extensions d'anneaux

Lemme ([L] 7.1.38.) *Soient k un corps commutatif, A et B deux k-algèbres commutatives intègres avec $A \subset B$ et $\frac{B}{A}$ qui est un k-espace vectoriel de dimension finie. Soit $a \in A$ tel que $\frac{A}{aA}$ soit un k-espace vectoriel de dimension finie. Alors $\frac{B}{aB}$ est un k-espace vectoriel de dimension finie et on a* $\dim_k \frac{A}{aA} = \dim_k \frac{B}{aB}$.

Démonstration On a les suites exactes de k-espaces vectoriels

(1) $0 \to \frac{A}{aA} \to \frac{B}{aA} \to \frac{B}{A} \to 0$, $0 \to \frac{aB}{aA} \to \frac{B}{aA} \to \frac{B}{aB} \to 0$.

De la première, on déduit que $\frac{B}{aA}$ est de dimension finie et de la seconde que $\frac{B}{aB}$ l'est aussi. Enfin elles se traduisent en termes de dimension par les relations

(2) $\dim\frac{B}{aA}=\dim\frac{A}{aA}+\dim\frac{B}{A}$, $\dim\frac{B}{aA}=\dim\frac{aB}{aA}+\dim\frac{B}{aB}$.

Sachant que $x\mapsto ax$ est un isomorphisme de B sur aB, on a $\dim\frac{B}{A}=\dim\frac{aB}{aA}$ et donc $\dim\frac{A}{aA}=\dim\frac{B}{aB}$.

4.2. Les algèbres commutatives de dimension de Krull nulle.

Lemme. *Soient k un corps commutatif, C une k-algèbre commutative qui est un k-espace vectoriel de dimension finie. Alors les idéaux premiers de C sont maximaux, ils sont en nombre fini : $\mathfrak{M}_1,\mathfrak{M}_2,\dots,\mathfrak{M}_s$. De plus l'application diagonale $\rho:C\to\prod_{i=1}^{s}C_{\mathfrak{M}_i}$ est un isomorphisme.*

Démonstration

α) *(les maximaux sont localement nilpotents)* L'anneau C est nœthérien puisque tout idéal est un k-espace vectoriel de dimension finie. Soit $\mathfrak{M}$ un idéal maximal de C, comme $(\dim_k\mathfrak{M}^i)_i$ est une suite décroissante, il existe N tel que $\mathfrak{M}^N=\mathfrak{M}^{N+1}$ et par **Nakayama** (Fr. F.8.2.1.) on a $\mathfrak{M}^N C_{\mathfrak{M}}=\{0\}$.

β) *(tout premier est maximal)* Soit $\mathfrak{P}$ un idéal premier de C, il existe un maximal $\mathfrak{M}$ de C avec $\mathfrak{P}\subset\mathfrak{M}$. Par α) il existe $s\in C-\mathfrak{M}$ tel que $s\mathfrak{M}^N=\{0\}$, i.e. $s\mathfrak{M}^N\subset\mathfrak{P}$, comme $s\notin\mathfrak{P}$, on a $\mathfrak{M}\subset\mathfrak{P}$. Ainsi, tout premier est maximal.

γ) *(les maximaux sont en nombre fini)* Soient $\mathfrak{M}_1,\mathfrak{M}_2,\dots,\mathfrak{M}_t$ des idéaux maximaux de C, par le théorème des chinois (Fr, F.1.9.14.), l'application diagonale $\alpha:C\to\prod_{i=1}^{t}\frac{C}{\mathfrak{M}_i}$ est surjective. Comme $\dim_k\frac{C}{\mathfrak{M}_i}\geq 1$, on a donc $t\leq\dim_k C$.

δ) *(l'application $\rho:C\to\prod_{i=1}^{s}C_{\mathfrak{M}_i}$ est injective)* Soit $x\in\ker\rho$, on a donc $s_i\in C-\mathfrak{M}_i$ tel que $s_i x=0$. Soit $\mathfrak{A}:=\{d\in C\mid dx=0\}$; il suit que $\mathfrak{A}\not\subset\mathfrak{M}_i$ pour $1\leq i\leq s$. Donc $\mathfrak{A}=C$, ce qui implique $x=0$.

ε) *(l'application $\rho:C\to\prod_{i=1}^{s}C_{\mathfrak{M}_i}$ est surjective)* Par α) il existe $N\geq 1$ tel que $\mathfrak{M}_i^N=\{0\}$ dans $C_{\mathfrak{M}_i}$ pour $1\leq i\leq s$.

$\varepsilon.1)$ *Il existe* $t_i \in (\mathfrak{M}_1 \dots \mathfrak{M}_{i-1} \mathfrak{M}_{i+1} \dots \mathfrak{M}_s)^N$, $t_i \notin \mathfrak{M}_i$.
Il suffit de le montrer pour $i=1$. En effet il existe $x_2 \in \mathfrak{M}_2$ et $x_2 \notin \mathfrak{M}_1$, $x_3 \in \mathfrak{M}\mathfrak{M}_3$ et $x_3 \notin \mathfrak{M}_1$, ..., $x_s \in \mathfrak{M}_s$ et $x_s \notin \mathfrak{M}_1$.
Soit $t_1 := (x_2 x_3 \dots x_s)^N$, alors t_1 convient.
$\varepsilon.2)$ Alors on a $C = C t_1 + C t_2 + \dots + C t_s$. Sinon, il existerait i avec $C t_1 + C t_2 + \dots + C t_s \subset \mathfrak{M}_i$. Comme $t_1, t_2, \dots, t_{i-1}, t_{i+1}, \dots, t_s \in \mathfrak{M}_i$, il en résulterait que $t_i \in \mathfrak{M}_i$, ce qui est impossible. Ainsi il existe $\lambda_1, \lambda_2, \dots, \lambda_s \in C$ avec

(1) $$1 = t_1 \lambda_1 + t_2 \lambda_2 + \dots + t_s \lambda_s$$

$\varepsilon.3)$ Soit $\frac{a_i}{s_i} \in C_{\mathfrak{M}_i}$, $1 \le i \le s$, $a_i \in C$, $s_i \in C - \mathfrak{M}_i$. Il s'agit de montrer qu'il existe $x \in C$ avec $x = \frac{a_i}{s_i}$ dans $C_{\mathfrak{M}_i}$ pour $1 \le i \le s$.
Montrons qu'il existe $\mu \in C$, $m \in \mathfrak{M}_1$ avec $1 = s_1 \mu + m^N$.
Comme $s_1 \notin \mathfrak{M}_1$, on a $s_1 C + \mathfrak{M}_1 = C$, ainsi, il existe $\lambda \in C$ et $m \in \mathfrak{M}_1$ avec $1 = s_1 \lambda + m$, donc $1 = s_1 \lambda + m\ (s_1 \lambda + m) = s_1(\lambda + s_1 m) + m^2$; par récurrence on montre facilement qu'il existe $\mu \in C$ avec $1 = s_1 \mu + m^N$.
$\varepsilon.4)$ Il suit de la relation précédente que $a_1 = s_1(\mu a_1) + m^N a_1$, cela veut dire que $\frac{a_1}{s_1} = (\mu a_1) + \frac{a_1}{s_1} m^N$. Cela veut dire qu'il existe $b_1 \in C$ tel que $\frac{a_1}{s_1} = b_1$ dans $C_{\mathfrak{M}_1}$. De façon analogue il existe $b_i \in C$ tel que

(2) $$\frac{a_i}{s_i} = b_i \text{ dans } C_{\mathfrak{M}_i}.$$

$\varepsilon.5)$ Soit

(3) $$x := t_1 \lambda_1 b_1 + t_2 \lambda_2 b_2 + \dots + t_s \lambda_s b_s.$$

On sait que $t_1 = 0$ dans $C_{\mathfrak{M}_i}$ pour $i \ge 2$, ce qui veut dire que $x = t_1 \lambda_1 b_1$ dans $C_{\mathfrak{M}_1}$. Or par (1), on a $1 = t_1 \lambda_1$ dans $C_{\mathfrak{M}_1}$, et par (2) on a $\frac{a_1}{s_{i1}} = b_1$ dans $C_{\mathfrak{M}_1}$ Il suit de cela que $x = \frac{a_1}{s_1}$ dans $C_{\mathfrak{M}_1}$.
De la même façon $x = \frac{a_i}{s_i}$ dans $C_{\mathfrak{M}_i}$.

4.3. Sur la séparabilité pour les corps valués

Lemme *Soient* k *un corps commutatif, algébriquement clos,* w *la valuation de* $K = k(T)$ *avec* $w(T) = 1$ *et triviale sur* k, $\hat{K}$ *le complété de* K *pour cette valuation. Alors l'extension* $\hat{K}$ *de* K *est séparable. En particulier si* L/K *est une extension de corps commutatifs, l'algèbre* $L \otimes_K \hat{K}$ *est réduite.*

Démonstration Si $\mathrm{car}\, k=0$, par **Bourbaki** A.V.117 théorème 1 , toute extension de K est séparable, donc $\hat{K}/K$ est séparable.

On suppose maintenant que $\mathrm{car}\, k=p\geq 2$. Tout d'abord $\hat{K}$ est le corps des fractions de l'algèbre des séries formelles $k[\![T]\!]$. Par **Bourbaki** A.V. 117 théorème 2, il suffit de montrer que $K^{\frac{1}{p}}\otimes_K \hat{K}$ est une algèbre réduite. Comme k est algébriquement clos, on a $K^{\frac{1}{p}}=k(T^{\frac{1}{p}})=K1\oplus KT^{\frac{1}{p}}\oplus\ldots\oplus KT^{\frac{p-1}{p}}$. Soit $x\in K^{\frac{1}{p}}\otimes_K\hat{K}$, un élément nilpotent, alors $x=1\otimes\lambda_0+T^{\frac{1}{p}}\otimes\lambda_1+\ldots+T^{\frac{p-1}{p}}\otimes\lambda_{p-1}$. Ainsi x^p est nilpotent et c'est un élément de $\hat{K}$ donc nul, et de la forme $x^p=\lambda_0^p+T\lambda_1^p+\ldots+T^{p-1}\lambda_{p-1}^p$. Soit $d\in k[\![T]\!]$ tel que $d\lambda_i\in k[\![T]\!]$ pour $0\leq i<p$; ainsi $(d\lambda_i)^p=f_i(T^p)$ où $f_i(T)\in k[\![T]\!]$. On a donc la relation $0=f_0(T^p)+Tf_1(T^p)+\ldots+T^{p-1}f_{p-1}(T^p)$; il suit de cela que $f_0=f_1=\ldots=f_{p-1}=0$, donc $\lambda_0=\lambda_1=\ldots=\lambda_{p-1}=0$. Ainsi $x=0$, ce qui veut dire que $K^{\frac{1}{p}}\otimes_K\hat{K}$ est réduit.

4.4. Un anneau de valuation discrète

Lemme *Soient k un corps commutatif, $K=k(X)$, $F(X,Y)\in k[X,Y]$ un polynôme irréductible, unitaire en Y , de degré n en Y , $y\in K(X)^{alg}$ tel que $F(X,y)=0$. Soient C la clôture intégrale de $k[X]$ dans $k(X)[y]$, $\mathfrak{M}$ un idéal maximal de C au-dessus de $Xk[X]$. Alors il existe une valuation v de $K[y]$ tel que la restriction de v à k soit triviale, que $v(K[y]-\{0\})=\mathbb{Z}$, que $C_{\mathfrak{M}}=\{z\in K[y]\mid v(z)\geq 0\}$, et que $\mathfrak{M}C_{\mathfrak{M}}=\{z\in K[y]\mid v(z)>0\}$.*

Démonstration Si on montre que $\{0\}$ et $\mathfrak{M}C_{\mathfrak{M}}$ sont exactement les idéaux premiers de $C_{\mathfrak{M}}$ alors l'équivalence *iii)* et *i)* de Fr, F.8.3.8. dit que $\mathfrak{M}C_{\mathfrak{M}}$ est de la forme $xC_{\mathfrak{M}}$, avec $x\neq 0$, et que les idéaux de $C_{\mathfrak{M}}$ sont exactement les $x^\alpha C_{\mathfrak{M}}$. Il suit de cela que tout élément de $K[y]$ s'écrit de façon unique sous la forme $x^\alpha u$, avec $\alpha\in\mathbb{Z}$ et $u\in(C_{\mathfrak{M}})^\times$. Alors l'application $x^\alpha u\mapsto\alpha$ est bien une valuation avec les propriétés indiquées.

Soit $\mathfrak{P}$ un idéal premier de $C_{\mathfrak{M}}$ avec $\mathfrak{P}\neq\{0\}$ et donc $\mathfrak{P}\subset\mathfrak{M}C_{\mathfrak{M}}$; il s'agit de montrer que $\mathfrak{P}=\mathfrak{M}C_{\mathfrak{M}}$. Soit $\mathfrak{P}_1:=\mathfrak{P}\cap C$, facilement $\mathfrak{P}_1$ est un idéal premier non nul de C . Il faut d'abord montrer que $\mathfrak{P}_1\cap k[X]\neq\{0\}$. Soit $x\in\mathfrak{P}_1-\{0\}$, comme x est entier sur $k[X]$, on a une relation $a_0(X)+a_1(X)x+\ldots+x^m=0$ avec $a_i(X)\in k[X]$ et $a_0(X)\neq 0$. Ainsi $a_0(X)\in\mathfrak{P}_1\cap k[X]$, ce qui veut dire que $\mathfrak{P}_1\cap k[X]\neq\{0\}$. Comme $\mathfrak{P}_1\subset\mathfrak{M}$ et que $\mathfrak{M}$ est au-dessus de $Xk[X]$, on a

$\{0\} \neq \mathfrak{P}_1 \cap k[X] \subset Xk[X]$; cela veut dire que l'idéal premier $\mathfrak{P}_1 \cap k[X]$ est $Xk[X]$. Donc $\mathfrak{P}_1 \cap k[X]$ est maximal, par Fr, F.8.2.4. il suit que $\mathfrak{P}_1$ est maximal et donc aussi $\mathfrak{P}$. On a donc $\mathfrak{P} = \mathfrak{M} C_{\mathfrak{M}}$.

4.5. La description des valuations des corps de fonctions d'une variable

Soient k *un corps commutatif, algébriquement clos,* $K = k(X)$, w *la valuation triviale sur* k *avec* $w(X) = 1$, $\hat{K}$ *le complété de* K *relativement à* w , $\hat{K}^{alg}$ *la clôture algébrique de* $\hat{K}$ *et on note aussi* w *un prolongement de* w *à* $\hat{K}^{alg}$ *qui est fixé une fois pour toutes. Soient* $F(X,Y) \in k[X,Y]$, *unitaire en* Y *de degré* n .

1. *Alors la factorisation de* F *en polynômes, unitaires, irréductibles de* $\hat{K}[Y]$, *est de la forme* $F(X,Y) = S_1(Y) S_2(Y) \dots S_r(Y)$ *avec* $S_i \neq S_j$ *pour* $i \neq j$.

2. *Soient* $y \in \hat{K}^{alg}$ *tel que* $F(X,y) = 0$, $y_i \in \hat{K}^{alg}$ *tel que* $S_i(y_i) = 0$, $\sigma_i : K[y] \to \hat{K}^{alg}$ *le* K*-homomorphisme tel que* $\sigma_i(y) = y_i$. *Soit* $v_i : K[y] \to \mathbb{Q}$ *défini par* $v_i(z) := w(\sigma_i(z))$. *Alors* $(v_1, v_2, \dots, v_r)$ *sont exactement les valuations de* $K[y]$ *qui prolongent la valuation* $w_{|K}$. *De plus* $\hat{K}[y_i]$ *est le complété de* $K[y]$ *relativement à* v_i .

Soient $S_i(Y) = \prod_{j=1}^{\alpha_i} (Y - y_{ij})$ *avec* $y_{ij} \in \hat{K}^{alg}$, $y_{i1} := y_i$ *pour* $1 \leq i \leq r$. *Soit* $H(X,y) \in K[y]$, *alors* $v_i(H(X,y)) = w(H(X,y_{ij}))$ *pour* $1 \leq j \leq \alpha_i$, *ainsi* $v_i(H(X,y)) = \frac{1}{\deg S_i} w(\prod_{j=1}^{\alpha_i} H(X,y_{ij}))$.

Enfin si π_i *est une uniformisante relativement à* v_i , i.e. *un générateur de l'idéal de valuation, on a* $v_i(\pi_i) = \frac{1}{\deg S_i}$ *ou encore* $v_i(K[Y] - \{0\}) = \frac{1}{e_i}\mathbb{Z}$ *avec* $e_i = \deg S_i$. *Si donc* w_i *est la valuation normalisée de* $K[Y]$ *équivalente à* v_i (i.e. $w_i(K[Y]) = \mathbb{Z} \cup \{\infty\}$) *on a* $w_i(z) = (\deg S_i) v_i(z)$ *et aussi* $w_i(H(X,y)) = w(\prod_{j=1}^{\alpha_i} H(X,y_{ij}))$.

3. *Soit* $F(X,Y) = (Y - \xi_1)(Y - \xi_2) \dots (Y - \xi_n)$ *avec* $\xi_i \in K^{alg}$. *Alors on a* $w_1(H(X,y)) + w_2(H(X,y)) + \dots + w_r(H(X,y)) = w(\prod_{i=1}^{n} H(X,\xi_i))$.

4. *Soient* $A_w := \{ z \in \hat{K}^{alg} \mid w(z) \geq 0 \}$, $\mathfrak{M}_w := \{ z \in \hat{K}^{alg} \mid w(z) > 0 \}$, C *la clôture intégrale de* $k[X]$ *dans* $K[y]$, $\mathfrak{M}_i := \sigma_i^{-1}(\mathfrak{M}_w) \cap C$. *Alors* $\mathfrak{M}_i$ *est un idéal maximal de* C , $C_{\mathfrak{M}_i}$ *est l'anneau de valuation de* v_i *(ou de* w_i*) et* $\mathfrak{M}_i C_{\mathfrak{M}_i}$ *est l'idéal de valuation de* v_i *(ou de* w_i*). De plus,* $\mathfrak{M}_1, \mathfrak{M}_2, \dots, \mathfrak{M}_r$ *sont exactement les idéaux maximaux de* C *au-dessus de* $Xk[X]$.

Démonstration

1) Soit $F(X,Y)=S_1(Y)^{u_1}S_2(Y)^{u_2}\dots S_r(Y)^{u_r}$ la factorisation de F en irréductibles, distincts, unitaires de $\hat{K}[Y]$. On a alors $K[y]\otimes_K\hat{K}\simeq\frac{K[Y]}{(F(X,Y))}\otimes_K\hat{K}\simeq\frac{\hat{K}[Y]}{(F(X,Y))}\simeq\prod_{i=1}^{r}\frac{\hat{K}[Y]}{(S_i(Y)^{u_i})}$. Par 4.3., $K[y]\otimes_K\hat{K}$ est réduit, ainsi $u_1=u_2=\dots=u_r=1$. Ce qui montre 1..

2) Clairement les v_i sont des valuations sur $K[y]$ qui prolongent w. Soient v une valuation sur $K[y]$ qui prolonge w, $K\widehat{[y]}$ le complété de $K[y]$ pour v et $\rho:K[y]\to K\widehat{[y]}$ l'injection canonique. On a $\hat{K}\subset\hat{K}[\rho(y)]\subset K\widehat{[y]}$. Comme y est algébrique sur K, $\rho(y)$ est algébrique sur $\hat{K}$; donc $K[\rho(y)]$ est un $\hat{K}$-espace vectoriel de dimension finie, donc complet. Ainsi $\hat{K}[\rho(y)]=K\widehat{[y]}$. Comme $F(X,\rho(y))=0$, $\mathrm{irr}(\rho(y),\hat{K},Y)$ divise $F(X,Y)$, ainsi il existe i tel que $\mathrm{irr}(\rho(y),\hat{K},Y)=S_i(Y)$. Il existe donc un $\hat{K}$-isomorphisme $\theta:\hat{K}[\rho(y)]\to\hat{K}[y_i]\subset\hat{K}^{alg}$ avec $\theta(\rho(y))=y_i$. Il suit que $v\theta^{-1}$ et w sont deux valuations de $\hat{K}[y_i]$ qui prolongent $w_{|\hat{K}}$. Sachant qu'il y a unicité on a $v\theta^{-1}=w$, i.e. $v=w\theta$ et $v(z)=w(\theta\rho(z))$ pour tout $z\in K[y]$. Comme $\theta\rho=\sigma_i$, on a bien $v=v_i$. En plus on a montré au passage que $\hat{K}[y_i]$ est le complété de $K[y]$ pour v_i et aussi que pour toute racine y_{ij} de S_i on a $v_i((H(X,y))=w(H(X,y_{ij}))$. En particulier on en déduit la formule $v_i(H(X,y))=\frac{1}{\deg S_i}w\left(\prod_{j=1}^{\alpha_i}H(X,y_{ij})\right)$.

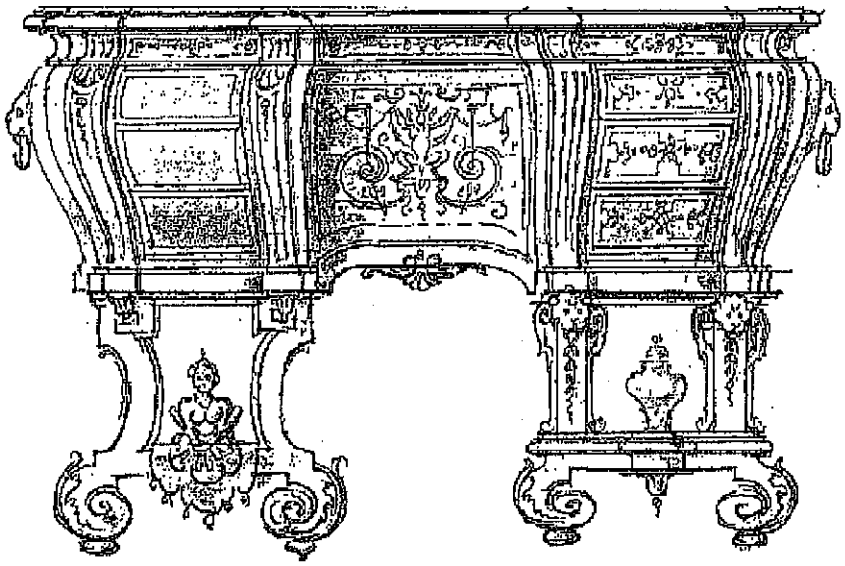
Si on considère $\hat{K}[y_i]\simeq K\widehat{[y]}^{\,i}$, complété pour v_i de $K[y]$, c'est une extension du corps valué complet $\hat{K}$, avec $\deg S_i=[\hat{K}[y_i]:\hat{K}]=e_i f_i$ où e_i (resp. f_i) est l'indice de ramification (resp. le degré de l'extension résiduelle). Comme le corps résiduel de $\hat{K}$ est k, algébriquement clos, on a $f_i=1$. Par ailleurs e_i est défini par $v_i(\hat{K}[y_i]-\{0\})=\frac{1}{e_i}\mathbb{Z}$, ce qui veut dire aussi que si π_i est un générateur de l'idéal de valuation, on a $v_i(\pi_i)=\frac{1}{e_i}$.

3) C'est immédiat.

4) Comme C est entier sur $k[X]$, $\sigma_i(C)$ est entier sur $k[X]$, et $w(k[X])\geq 0$ implique $w(\sigma_i(C))\geq 0$. L'application canonique $C\xrightarrow{\sigma_i}A_w\to\frac{A_w}{\mathfrak{M}_w}=k$ est surjective ; comme $\mathfrak{M}_i$ est le noyau de cette application, on a $\mathfrak{M}_i$ qui est maximal. Il est facile de vérifier que $C_{\mathfrak{M}_i}=\{z\in K[y]\mid v_i(z)\geq 0\}$ et que $\mathfrak{M}_i C_{\mathfrak{M}_i}=\{z\in K[y]\mid v_i(z)>0\}$.

Réciproquement, soit $\mathfrak{M}$ un idéal maximal de C avec

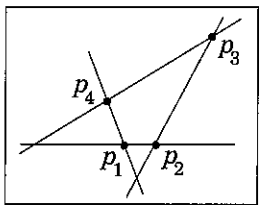
$\mathfrak{M} \cap k[X] = X k[X]$, alors on sait qu'il existe une valuation discrète v sur $K[y]$ telle que $C_{\mathfrak{M}} = \{ z \in K[y] \mid v_i(z) \geq 0 \}$, que $\mathfrak{M} C_{\mathfrak{M}} = \{ z \in K[y] \mid v(z) \geq 1 \}$ et $v(K[Y] - \{0\}) = \mathbb{Z}$ (4.4.) . Si $v(X) = e$, alors $\frac{1}{e} v$ est une valuation de $K[y]$ qui prolonge $w_{|K}$. Par 3. il existe i tel que $v_i = \frac{1}{e} v$; on en déduit que $\mathfrak{M} = \mathfrak{M}_i$.



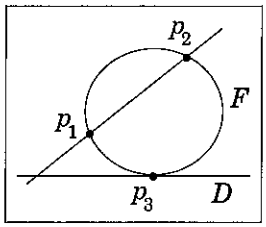
5. Famille linéaire de coniques.

Soient k un corps algébriquement clos, F et G deux polynômes de degré 2 tels F, G (resp. F_2, G_2) n'ont pas de facteur irréductible en commun. Si donc $p_1, p_2, \ldots, p_s$ sont les points communs de $F=G=0$, alors pour $\lambda \in k$, $p_1, p_2, \ldots, p_s$ sont les points communs de $F=\lambda F+G=0$ et on a $i(p_j; F, G) = i(p_j; F, G+\lambda F)$ pour $1 \leq j \leq s$. On peut donc dire que les points p_j et les nombres $i(p_j; F, G)$ sont associés à la famille linéaire de coniques $\mathcal{F} := \{ \mu F + (1-\mu) G \mid \mu \in k \}$; c'est pourquoi on notera $i(p_j; F, G)$ par $i(p_j; \mathcal{F})$.

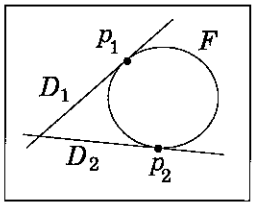
5.1. **Quatre points d'intersection** p_1, p_2, p_3, p_4. C'est la famille engendrée par la conique dégénérée $F = V(p_1, p_2) \cup V(p_3, p_4)$ et $G = V(p_1, p_4) \cup V(p_2, p_3)$. Si H est la conique dégénérée $V(p_1, p_2) \cup V(p_3, p_4)$, la famille est aussi engendrée par F et H et aussi par G et H. Bien entendu $i(p_j; \mathcal{F}) = 1$ pour $1 \leq j \leq 4$.



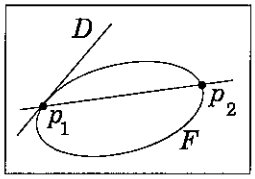
5.2. **Trois points d'intersection** p_1, p_2, p_3 **avec** $i(p_1; \mathcal{F}) = i(p_2; \mathcal{F}) = 1$, $i(p_3; \mathcal{F}) = 2$. La famille est engendrée par une conique propre F passant par p_1, p_2 et tangente à D en p_3 et la conique dégénérée $V(p_1, p_2) \cup D$.



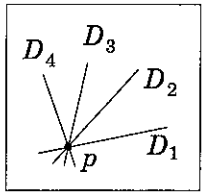
5.3. **Deux points d'intersection** p_1, p_2 **avec** $i(p_1; \mathcal{F}) = i(p_2; \mathcal{F}) = 2$. Il existe une droite D_1 (resp. D_2) passant par p_1 (resp. p_2). Aussi la famille est engendrée par $G = D_1 \cup D_2$ et une conique propre F tangente à D_i en p_i.



5.4. **Deux points d'intersection** p_1, p_2 **avec** $i(p_1; \mathcal{F}) = 3$, $i(p_2; \mathcal{F}) = 1$. La famille est engendrée par $G = V(p_1, p_2) \cup D$ où D est une droite passant par p_1, $D \neq V(p_1, p_2)$ et une conique propre F, pasant par p_1, p_2 et tangente à D en p_1.

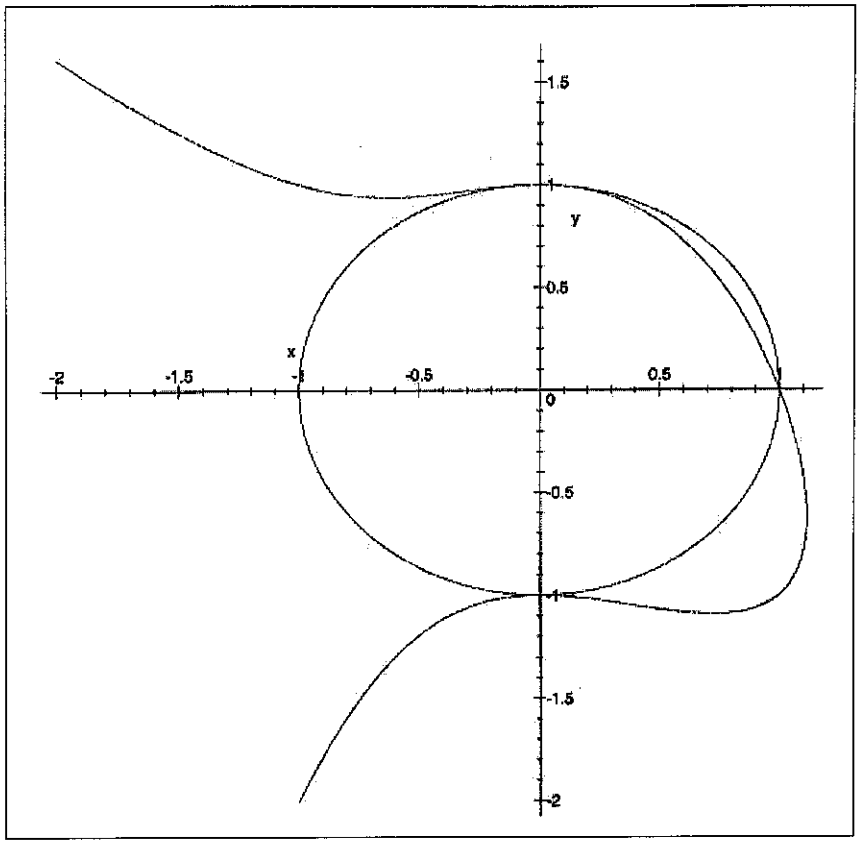


5.5. **Un point** p **d'intersection avec** $i(p; \mathcal{F}) = 4$. Il existe quatre droites distinctes D_1, D_2, D_3, D_4 passant par p et la famille est engendrée par $F = D_1 \cup D_2$ et $G = D_3 \cup D_4$. Ce qui veut dire aussi que $F = F_2$, $G = G_2$.



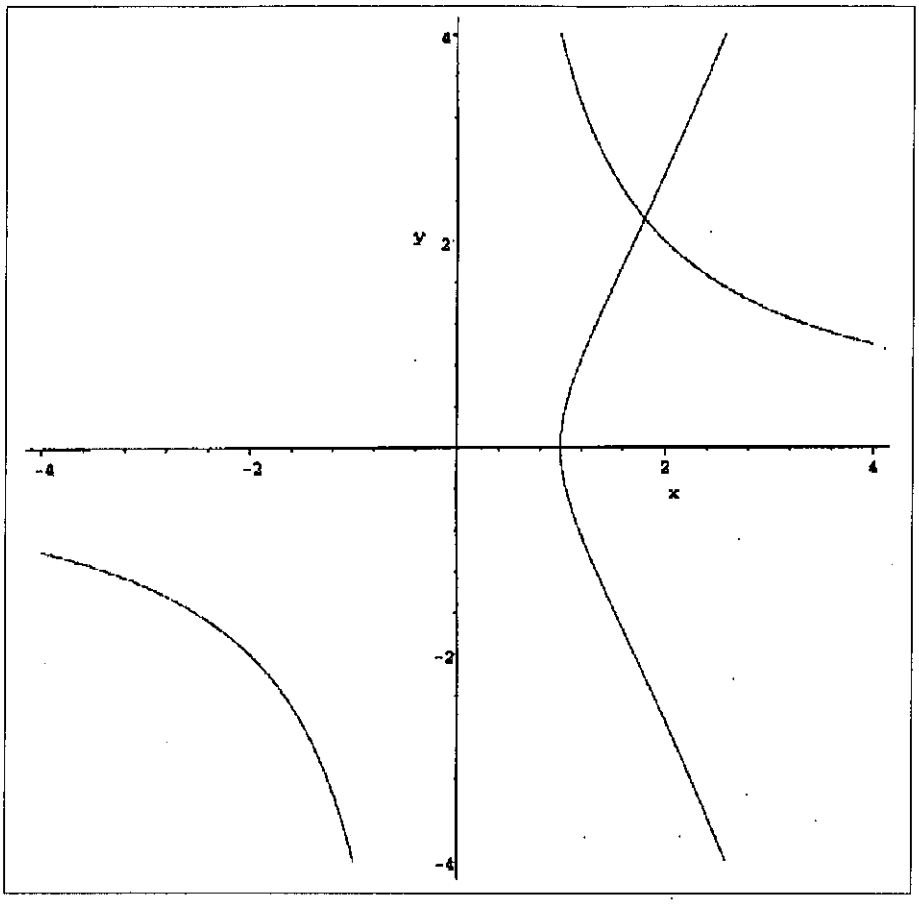
6. Des exemples

6.1. Exemple



$F=X^2+Y^2-1$, $G=X^3+X^2Y+Y^2-1$
$R(X)=2X^5(X-1)$ (F,G, comme polynômes de la variable Y)
$R(Y)=2Y(Y+1)^2(Y-1)^3$ (F,G , comme polynôme de la variable X)
$i((1,0);F,G)=1$, $i((0,1);F,G)=3$, $i(0,-1);F,G))=2$

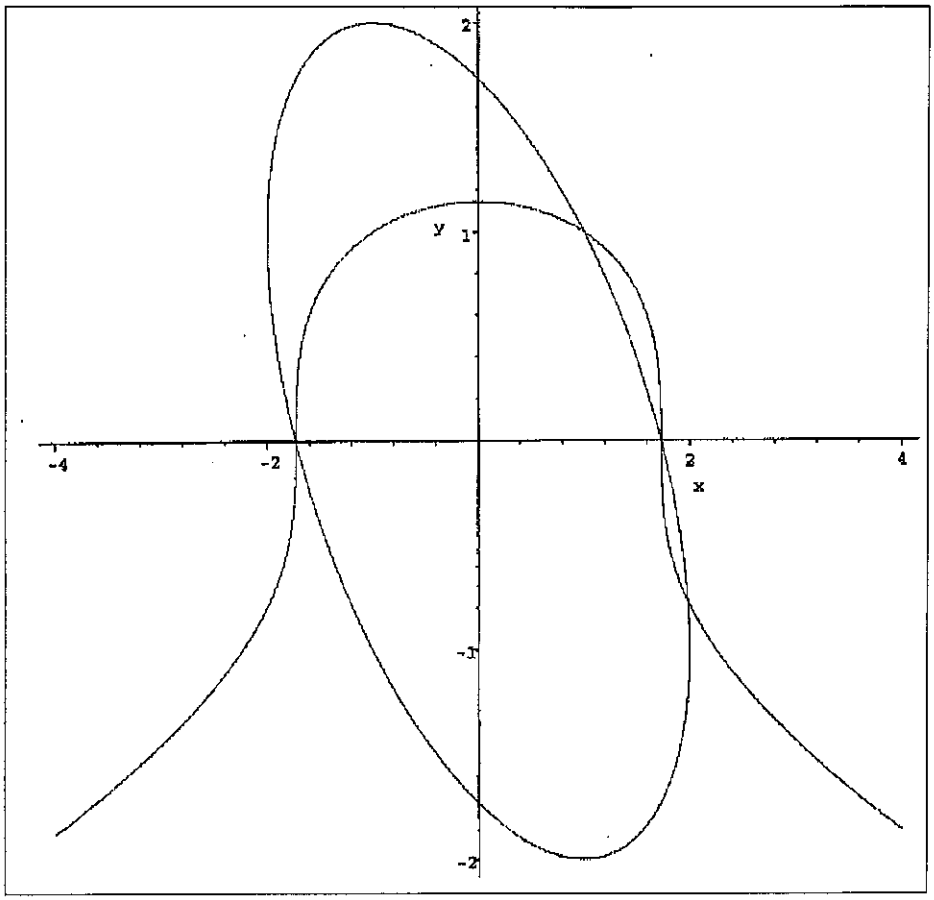
6.2. Exemple



$F=XY-4$, $G=Y^2-X^3+1$ (attention F_2 et G_3 ont un facteur en commun)
$R(X)=-X^5+X^2+16$ $R(Y)=Y^5+Y^3-64$

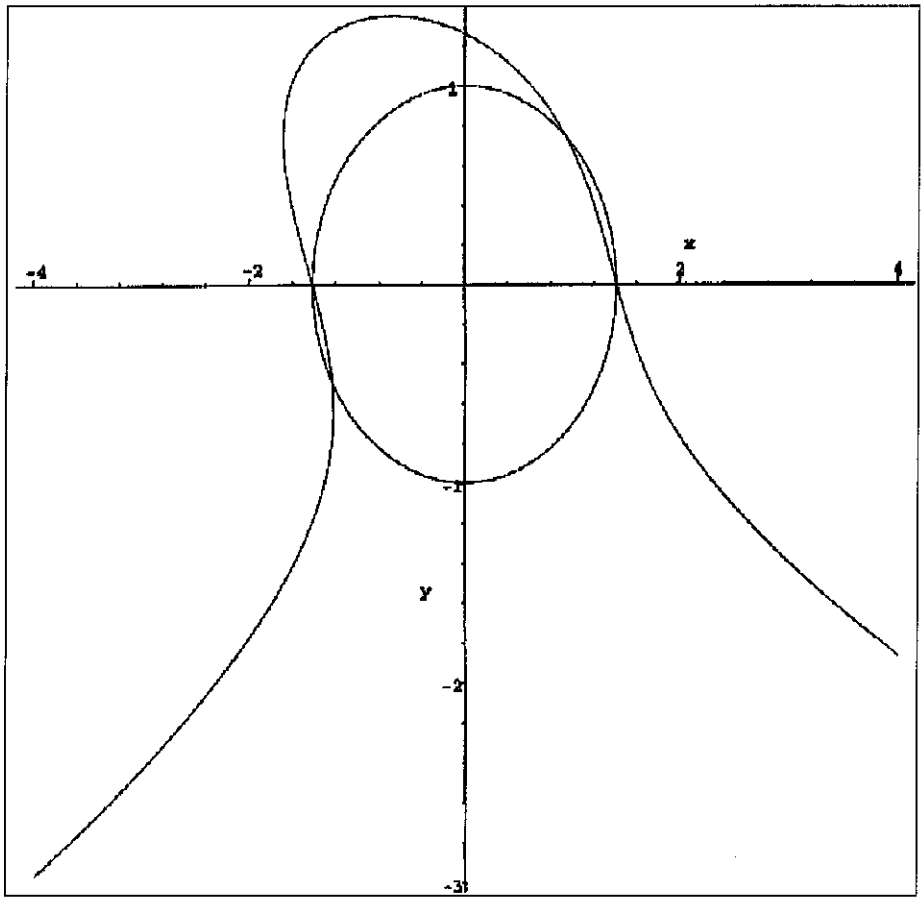
Par l'algorithme d'Euclide $1=\text{pgcd}(R(X),R'(X))$. Ce qui veut dire que $R(X) = (X-x_1)(X-x_2)(X-x_3)(X-x_4)(X-x_5)$. Sachant qu'il existe un point à l'infini qui en coordonnée homogène est $p_6:=(0:0:1)$, il existe un unique y_i tel que $F(x_i,y_i)=G(x_i,y_i)=0$. Si donc $F^\natural(Z,X,Y)=XY-4Z^2$, $G^\natural(Z,X,Y)=Y^2Z^{-3}X^3+Z^3$ avec $p_i:=(1:x_i:y_i)$, on a six points d'intersection et donc $i(p_i;F^\natural,G^\natural)=1$. (Il y a un point réel $x_1=1.80698....$, $y_1=2.2136...$).

6.3. Exemple



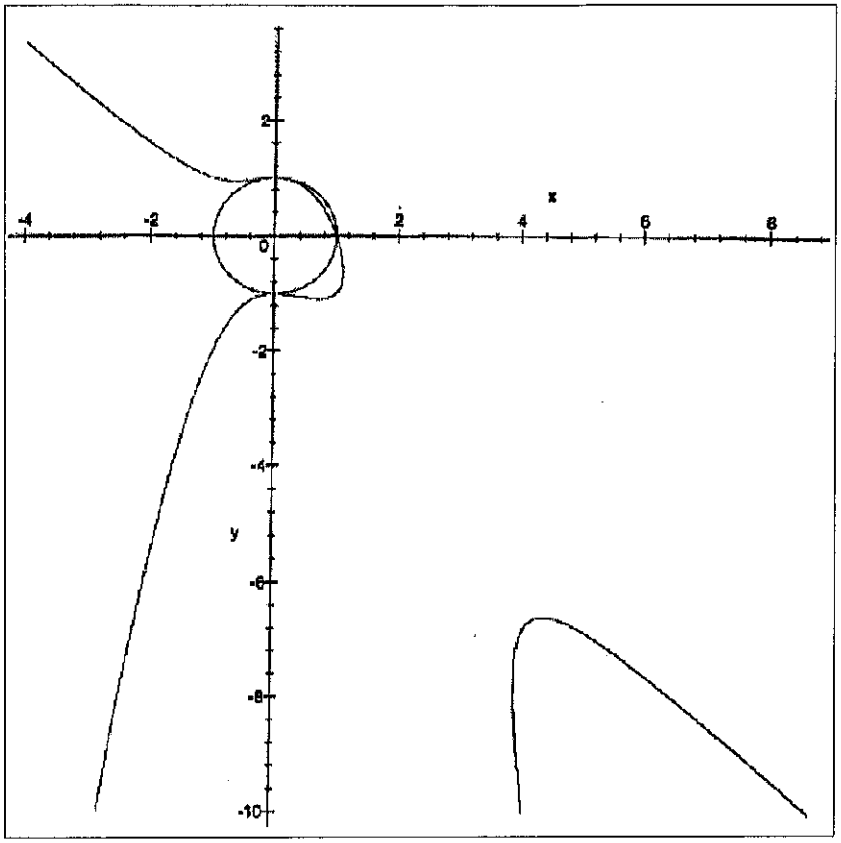
$F=X^2+2Y^3-3$, $G=X^2+XY+Y^2-3$,
$R(X)=(X-1)(X^2-3)(4X^3+8X^2-15X-33)$,
$R(Y)=Y^2(Y-1)(4Y^3+3Y^2+3Y+3)$.
Comme $R(X)$ a 6 racines simples, il y a donc 6 points d'intersection, chacun ayant un nombre d'intersection 1. On a 3 racines réelles x_1, x_2, x_3 avec $x_1=-1.732..., x_2=1.732..., x_3=1.984...$

6.4. Exemple



$F=X^2+2Y^2-2$, $G=X^2+XY+Y^3-2$
$R(X)=(X^2-2)(X^4-4X^3+8X^2+8X-12)$
$R(Y)=Y^2(6Y^2-2+Y^4-4Y^3)$
Facilement les racines y_1,y_2,y_3,y_4 de $6Y^2-2+Y^4-4Y^3$ sont distinctes. Par ailleurs pour $y=0$, on a $x=\pm\sqrt{2}$. Ainsi les points d'intersection sont (x_i,y_i) pour $1\leq i\leq 4$ et $(\sqrt{2},0),(-\sqrt{2},0)$. Encore une fois chaque point est de nombre d'intersection 1. Les points réels en dehors des 2 derniers sont $(x_1,y_1)=(-1.23...,-0.49),(x_2,y_2)=(0.937...,0.749...)$.

6.5. Exemple



$F=X^3+Y^3-2XY$, $G=2X^3-4YX^2+3XY^2+Y^3-2Y^2$.
$R(X)=8X^5(-4+7X)(X-1)^3$, $R(Y)=8Y^5(7Y+8)(Y-1)^3$.
Les points d'intersection sont les suivants $(1,1),(1,\alpha),(1,\alpha')$ de nombre d'intersection 1 avec α,α' racines de Y^2+Y-1, i.e. $\frac{-1\pm\sqrt{5}}{2}$, ensuite $(\frac{4}{7},y_4)$ de nombre d'intersection 1. Enfin $(0,0)$ de nombre d'intersection 5.

7. Méthode pratique de calcul de la multiplicité d'intersection de 2 courbes planes en un point

7.0. Les outils de base

7.0.1. *Si P est un polynôme non nul, on peut trouver un point où il ne s'annule pas.* Soient k un corps commutatif infini, $P(X_1,X_2,\dots,X_n)\in k[X_1,X_2,\dots,X_n]$ avec $\deg P\le s$, $\mathcal{A}$ une partie finie de k avec $\operatorname{card}\mathcal{A}=s+1$. Alors il existe $(x_1,x_2,\dots,x_n)\in\mathcal{A}^n$ tel que $P(x_1,x_2,\dots,x_n)\neq 0$. (Fr., F.2.5.12.).

7.0.2. *Soit $P(X)\in\mathbb{C}[X]$ qui se factorise sous la forme* $P(X)=(X-a_1)^{\alpha_1}(X-a_2)^{\alpha_2}\dots(X-a_k)^{\alpha_k}$, *avec* $a_i\in\mathbb{C}$, $a_i\neq a_j$ *pour* $i\neq j$ *et* $\alpha_i\ge 1$. *Alors pour chaque i, on peut construire de façon algorithmique une suite $(a_{i,\ell})_\ell$ telle que* $\lim_{\ell\to\infty} a_{i,\ell}=a_i$. *En d'autres termes, on peut approcher aussi près que l'on veut les a_i.*

Cette approximation nous permettra de résoudre un problème essentiel de "non-annulation". Il se présente comme il suit. Soient $a_1,a_2,\dots,a_k$ (resp. $b_1,b_2,\dots,b_k$) des racines de polynômes, ce qui veut dire que $(a_i)_i$ (resp. $(b_i)_i$) est connu par approximation ; on suppose en plus que $(a_i,b_i)\neq(0,0)$ pour tout i. Alors on souhaite trouver $v\in k$ de façon que $a_i+v\,b_i\neq 0$ pour tout i. On considère donc le polynôme $S(X):=\prod_{i=1}^{k}(a_i+X\,b_i)$, il est non nul. Soient $\mathcal{A}:=\{x_1,x_2,\dots,x_{k+1}\}$ une partie de $\mathbb{C}$ avec $k+1$ éléments distincts, on sait qu'il existe $x_m\in\mathcal{A}$ tel que $S(x_m)\neq 0$; i.e. $a_i+x_m\,b_i\neq 0$ pour tout i. Ainsi, parmi les $k+1$ suites $(a_i+x_t\,b_i)_i$ pour $1\le t\le k+1$, il en est au moins une qui ne converge pas vers zéro. Cela doit donc se lire avec les approximations.

Le second problème se présente comme il suit. Soient $a_1,a_2,\dots,a_k$ (resp. $b_1,b_2,\dots,b_k$) des racines de polynômes, ce qui veut dire que $(a_i)_i$ (resp. $(b_i)_i$) est connu par approximation ; on suppose en plus que $(a_i,b_i)\neq(a_j,b_j)$ pour $i\neq j$. Là, on souhaite trouver v de façon que $(a_i-v\,b_i)\neq(a_j-v\,b_j)$ pour tout $i\neq j$. On a donc $((a_i-a_j),(b_i-b_j))\neq(0,0)$ pour tout $i<j$; ce qui est le problème précédent

7.0.3. *Soit $P(X)\in\mathbb{C}[X]$ qui se factorise sous la forme* $P(X)=(X-a_1)^{\alpha_1}(X-a_2)^{\alpha_2}\dots(X-a_k)^{\alpha_k}$, *avec* $a_i\in\mathbb{C}$, $a_i\neq a_j$ *pour* $i\neq j$ *et* $\alpha_i\ge 1$. *On souhaite calculer* α_1, i.e. $\operatorname{val}_{(X-a_1)}(P(X))$.

Facilement on a
$P_1(X) := \mathrm{pgcd}(P, P') = (X-a_1)^{\alpha_1-1}(X-a_2)^{\alpha_2-1}\ldots(X-a_k)^{\alpha_k-1}$. On pose
$P_2(X) := \mathrm{pgcd}(P_1(X), P_1'(X)$... On aura donc
$P_1(a_1) = P_2(a_1) = \ldots = P_{\alpha_1-1}(a_1) = 0$ et $P_{\alpha_1}(a_1) \neq 0$. Si
$P(X) = X^n + u_1 X^{n-1} + \ldots + u_n$, on a $|a_i| \leq \max(1, |u_1| + \ldots + |u_n|) =: M$. Si donc $X - a_1 \mid P_i(X)$, on a $|P_k(a_{1,\ell})| \leq |a_{1\ell} - a_1|\,(2M)^{(\deg P_k)-1}$. Si $\delta = \min_{2\leq i\leq k} |a_1 - a_i|$ et si $(X-a_1) \nmid P_k$, on a $|P_k(a_{1,\ell})| \geq \delta^{\deg P_k}$. Ainsi donc ces deux inégalités doivent permettre de calculer α_1 (et idem pour $\alpha_2, \alpha_3, \ldots \alpha_n$) .

7.1. Les racines communes de 2 polynômes à 2 variables sans facteurs irréductibes communs

Soient F , $G \in k[X,Y]$, $\deg F = n$, $\deg G = m$. Soient $\lambda \in k$ tel que $F_n(\lambda, 1) \neq 0$, $F^\sharp(X,Y) := F(X + \lambda Y, Y)$, alors $\deg_Y F^\sharp = n$. Soient $R(X)$ le résultant de $F^\sharp$ et $G^\sharp$ comme polynômes de la variable Y, $\alpha_1, \alpha_2, \ldots \alpha_t$ les racines de R . Soient $\beta_{i\ell}$ les racines communes de $F^\sharp(\alpha_i, Y)$ et $G^\sharp(\alpha_i, Y)$ (il existe au moins une, Fr , F.7.7.1.9.). Alors les $(\alpha_i, \beta_{i\ell})$ sont exactement les racines communes de $F^\sharp$ et $G^\sharp$. Bien entendu, de là on trouve les racines communes de F et G .

7.2. Les racines communes de 2 polynômes homogènes à 3 variables

Soient $F(Z,X,Y)$ (resp. $G(Z,X,Y)$) un polynôme homogène de degré n (resp. m) ; on suppose F et G sans facteur irréductible en commun. Alors les éléments de $\mathbb{P}^2(k)$, racines de F et G sont les $(1:x:y)$ avec (x,y) racines de $F(1,X,Y)$ et $G(1,X,Y)$ et les $(0:x:y)$ avec (x,y) racines de $F(0,X,Y)$ et $G(0,X,Y)$. Cela est résolu par 7.1. .

7.3. Calcul de la multiplicité d'intersection de deux courbes planes projectives en un point

Soient $F(Z,X,Y)$ (resp. $G(Z,X,Y)$) un polynôme homogène de degré n (resp. m) ; on suppose F et G sans facteur irréductible en commun. Par 7.2. , on sait déterminer les éléments $p_i := (z_i : x_i : y_i) \in \mathbb{P}^2(k)$ qui sont zéros communs de F et G , et on a $1 \leq i \leq nm$. Il existe $\lambda, \mu \in k$ tels que $z_i + \lambda x_i + \mu y_i \neq 0$ pour tout i (il suffit de considérer le polynôme $S(\lambda,\mu) = \prod_{i<j} ((z_i - z_j) + \lambda(x_i - x_j) + \mu(y_i - y_j))$. Soit
$F^\natural(Z,X,Y) := F(Z - \lambda X - \mu Y, X, Y)$, $G^\natural(Z,X,Y) := G(Z - \lambda X - \mu Y, X, Y)$; alors les zéros communs de $F^\natural$ et $G^\natural$ sont les $q_i := (z_i + \lambda x_i + \mu y_i : x_i : y_i)$, $\deg F^\natural = n$, $\deg G^\natural = m$ et $F^\natural$ et $G^\natural$ sont sans facteur irréductible en

commun. Ainsi les éléments de $\mathbb{P}^2(k)$ racines communes de $F^\natural$ et $G^\natural$ sont de la forme $(1:x_i':y_i')$; cela s'identifie aux racines communes de $F^\natural(1,X,Y)$ et $G^\natural(1,X,Y)$ qui sont les $r_i:=(x_i':y_i')$. Soit $F_n^\natural$ la composante homogène de degré n de $F^\natural(1,X,Y)$. Alors il existe $v\in k$ tel que $F_n^\natural(v,1)\neq 0$ et $x_i'-vy_j'\neq x_j'-vy_j'$ si $i\neq j$ (il suffit de considérer le polynôme $F_n^\natural(v,1)\prod_{i<j}((x_i'-y_j')-v(y_i'-y_j'))$. Soient $F^\sharp(X,Y):=F^\natural(1,X,Y)$, $G^\sharp(X,Y):=G^\natural(1,X,Y)$ alors les zéros communs de $F^\sharp$ et $G^\sharp$ sont les $t_i:=(x_i'-vy_j',x_j')$.

D'abord il suit que 1.2. et 1.3. que $i(p_i;F,G)=i(q_i;F^\natural,G^\natural)=i(r_i;F^\natural(1,X,Y),G^\natural(1,X,Y))=i(t_i;F^\sharp,G^\sharp)$. Si donc $\alpha:=x_i'-vy_i'$, $\beta:=y_i'$, il suit de la définition de v que $F^\sharp(\alpha,\gamma)=G^\sharp(\alpha,\gamma)=0$ implique $\beta=\gamma$. Par conséquent 3.1 partie 2. dit que $i(t_i;F^\sharp,G^\sharp)=\mathrm{val}_{(X-\alpha)}R(X)$ où $R(X)=\mathrm{res}(F^\sharp,G^\sharp)$.

Bibliographie

[*Bki*] **Nicolas Bourbaki** *Algèbre Algèbre ch. 4 à 7* (Masson 1981)

[*C. L. O.*] **David Cox, John Little, Donald O'Shea** *Using algebraic geometry* (Springer Verlag, graduate texts in mathematics (edition 1998)

[*Fr*] **Jean Fresnel** *Anneaux* Hermann 2001

[*Fu*] **William Fulton** *Algebraic curves* Benjamin Cummings publ. Company 1969

[*L*] **Qing Liu** *Introduction to algebraic curves over Dedekind domains* Oxford Graduate texts in Mathematics 2002

[*P. R.*] **Bernadette Perrin-Riou** *Algèbre, arithmétique et Maple* Cassini 2000

[*W*] **Robert G. Walker** *Algebraic curves,* Springer Verlag (édition 1978)