NOM : UMBER Prénom : Pierre Jury :

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi : Résultant. Applications. Ref : Apery, Elimination, le cas d'une variable ; Gozard, Théorie de Galois

Autre sujet : /

*1) Définitions et premières propriétés

Ici, A est un anneau commutatif unifère

I. Résultant sur un anneau

Soit $m,n \geq 0$, $f = \sum a_i X^i \in A_m[X]$, $g = \sum b_i X^i \in A_n[X]$

Def 1 : On pose $\Phi_{f,g} : A_{n-1}[X] \times A_{m-1}[X] \to A_{m+n-1}[X]$
$(u, v) \mapsto uf + vg$

Def 2 : On pose $Syl_{m,n}(f,g) := \begin{pmatrix} a_m & \cdots & a_0 & & \\ & \ddots & & \ddots & \\ & & a_m & \cdots & a_0 \\ b_n & \cdots & b_0 & & \\ & \ddots & & \ddots & \\ & & b_n & \cdots & b_0 \end{pmatrix}$ (bloc de n lignes, bloc de m lignes)

dite matrice de Sylvester

Def 3 : On pose $Res_{m,n}(f,g) := \det(Syl_{m,n}(f,g))$ dit résultant d'ordre (m,n) de f et g

Def 4 : On pose $Res(f,g) := \begin{cases} Res_{\deg f, \deg g}(f,g) & \text{si } f \text{ et } g \neq 0 \\ 0 & \text{sinon} \end{cases}$

Prop 5 : On munit $A_{n-1}[X] \times A_{m-1}[X]$ et $A_{m+n-1}[X]$ des bases $((X^{n-1},0),\dots,(1,0),(0,X^{m-1}),\dots,(0,1))$ et $(X^{m+n-1},\dots,1)$. Alors la matrice de $\Phi_{f,g}$ dans ces bases est $Syl_{m,n}(f,g)^t$.

Prop 6 : On a :
- $Res_{n,m}(g,f) = (-1)^{mn} Res_{m,n}(f,g)$
- $Res(a_0, g) = a_0^{\deg g}$ (où $f,g \neq 0$)
- $Res(f, b_0) = b_0^{\deg f}$
- $Res_{m,n}(af, bg) = a^n b^m Res_{m,n}(f,g)$
- $Res_{m,m}(f,f) = 0$
- $\forall a \in A$, $Res_{m,n}(f(X+a), g(X+a)) = Res_{m,n}(f,g)$ (invariance par translation)

Prop 7 : On suppose $m' \geq m$ et $n' \geq n$.

alors $Res_{m',n'}(f,g) = \begin{cases} 0 \text{ si } m' > m, n' > n \\ a_m^{n'-n} Res_{m,n}(f,g) \text{ si } m' = m \\ b_n^{m'-m} Res_{m,n}(f,g) \text{ si } n' = n \end{cases}$

Prop 8 : On a $Res_{m,n}(f,g) \in \operatorname{Im} \Phi_{f,g}$

Cor 9 : Si $Res_{m,n}(f,g) \in A^\times$, $(f)+(g) = A[X]$

Rem. 10 : $Res_{m,n}$ est un polynôme à coefficients entiers en $a_0,\dots,a_m, b_0,\dots,b_n$

2) Calcul pratique du résultant

Lemme 11 : Si $a_m \in A^\times$, $A[X]/(f)$ est un A-module libre de rang m, de base $\{1,\dots,X^{m-1}\}$

Def 12 : On pose $\Psi_g : A[X]/(f) \to A[X]/(f)$
$u \longmapsto gu$

Prop 13 : (formule de Poisson) : On suppose $a_m \in A^\times$ alors $Res_{m,n}(f,g) = a_m^n \det \Psi_g$

Cor 14 : Soit $g_1 \in A_{n_1}[X]$, $g_2 \in A_{n_2}[X]$, $n_1 + n_2 = n$ et $a_m \in A^\times$. Alors $Res_{m,n}(f, g_1 g_2) = Res_{m,n_1}(f,g_1) \times Res_{m,n_2}(f,g_2)$

Cor 15 : (formule de Laplace) : Soit $a_m \in A^\times$, $q \in A[X]$ tel que $g + fq \in A_m[X]$. Alors $\mathrm{Res}_{m,m}(f,g) = \mathrm{Res}_{m,m}(f, g+fq)$

Prop 16 (rappel) : si $a_m \in A^\times$, alors il existe un couple (q,r), avec $g = fq + r$ et $\deg(r) < \deg(f)$. On a alors $\deg r \leqslant \deg g$. On parle de division euclidienne. De plus, si A est intègre, cette division est unique.

Cor 17 : Si $a_m \in A^\times$ et $g = fq + r$ est une division euclidienne de g par f, alors $\mathrm{Res}(f,g) = a_m^{\deg g - \deg r}\, \mathrm{Res}(f,r)$

Rem. 18 : Si le calcul d'une division euclidienne est effectif, comme sur un corps fini, le calcul du résultant peut être programmé.

Prop 19 : $\mathrm{Res}_{1,m}(X-\alpha, g) = g(\alpha)$

Cor. 20 : On a $\mathrm{Res}\left(\prod_{i=1}^m (X-\alpha_i), g\right) = \prod_{i=1}^m g(\alpha_i)$

Prop 21 (formule de covariance) : On suppose $m = m, a,b,c,d \in A$, alors $\mathrm{Res}_{m,m}(af+bg, cf+dg) = (ad-bc)^m \mathrm{Res}_{m,m}(f,g)$.

3) Spécialisation du résultant

Prop 22 : Soit $\varphi : A \to B$ morphisme d'anneaux unitaires. Alors $\varphi\left(\mathrm{Res}_{m,m}(f,g)\right) = \mathrm{Res}_{m,m}(\varphi(f), \varphi(g))$.

Rem. 23 : Ici, m et m en indice est important.

Def. 24 : On suppose ici $f,g \in A[X_1,\dots,X_n,X]$. On note $\mathrm{Res}_{m,m,X}(f,g)$ le résultant de f et g vu comme élément de $A[X_1,\dots,X_n][X]$

Prop 25 : (formule de spécialisation) : soit $f,g \in A[X_1,\dots,X_n,X]$ et $a_1,\dots,a_n \in A$. Alors $\mathrm{Res}_{m,m,X}(f,g)(a_1,\dots,a_n) = \mathrm{Res}_{m,m}(f(a_1,\dots,a_n,X), g(a_1,\dots,a_n,X))$

II. Résultant sur un corps.

Soit $\mathbb{K}$ un corps, $A = \mathbb{K}$.

1) Lien résultant - racine.

On pose $d := f \wedge g$, et $\delta := \deg d$

Prop. 26 : si $(a_m, b_m) \neq (0,0)$, $\dim(\Phi_{f,g}) = m+m-\delta$

Cor. 27 :

$\Updownarrow$

- $\Phi_{f,g}$ est bijective
- $\mathrm{Res}_{m,m}(f,g) \neq 0$
- $d = 1$ et $(a_m, b_m) \neq (0,0)$

Cor 28 : $\left\{ f \text{ et } g \text{ ont une racine commune dans } \overline{\mathbb{K}} \right\} \Leftrightarrow \mathrm{Res}(f,g) = 0$

2) Théorie de l'élimination

On suppose $f,g \in \mathbb{K}[X_1,\dots,X_n][X]$

Prop 29 : $\left\{ \begin{array}{l} \mathrm{Res}_{m,m,X}(f,g) = 0 \\ (a_m, b_m) \neq 0 \end{array} \right. \Rightarrow \left\{ f \text{ et } g \text{ ont un facteur commun dans } \mathbb{K}[X_1,\dots,X_n,X] \right\}$

Prop 30 : Si $(\alpha_1,\dots,\alpha_n,\alpha)$ est une racine commune de f et g, alors $\mathrm{Res}_{m,m,X}(f,g)(\alpha_1,\dots,\alpha_n) = 0$

Cor 31 : Soit $\alpha_1,\dots,\alpha_n \in \mathbb{K}$

$\mathrm{Res}_{m,m,X}(f,g)(\alpha_1,\dots,\alpha_n) = 0 \Leftrightarrow \left\{ \begin{array}{l} f(\alpha_1,\dots,\alpha_n,X) \text{ et } g(\alpha_1,\dots,\alpha_n,X) \text{ ont une racine commune dans } \overline{\mathbb{K}} \\ \text{ou } a_m(\alpha_1,\dots,\alpha_n) = b_m(\alpha_1,\dots,\alpha_n) = 0 \end{array} \right\}$

III. Applications

1) Intersection de courbes algébriques

Soit $f, g \in \mathbb{K}[X,Y]$, on pose $V_f := \{(x,y), f(x,y) = 0\}$

Prop 32 : Si $f \wedge g = 1$ dans $\mathbb{K}[X,Y]$, $V_f \cap V_g$ est fini

Prop 33 : On suppose $f = Y^p + \sum_{i=1}^{p} f_i(X) Y^{p-i}$ et $g = Y^q + \sum_{j=1}^{q} g_j(X) Y^{q-j}$, $\deg f_i \leq i$ et $\deg g_j \leq j$. On pose $h := Res_{p,q,Y}(f,g)$ et $\pi : (x,y) \mapsto x$
alors $\pi(V_f \cap V_g) \subset \mathbb{Z}(h)$ (avec égalité si $\mathbb{K}$ alg. clos) et $|\pi(V_f \cap V_g)| \leq pq$

Th 34 (Bezout) : Si $\mathbb{K}$ est infini et $V_f \cap V_g$ est fini, $|V_f \cap V_g| \leq pq$

Ex 35 : Si $f = Y^2 - XY + (X^2 - 1)$ et $g = Y^2 - Y + (2X^2 - 2)$, alors
$h = 3(X-1)^2 X(X+1)$ et $V_f \cap V_g = \{(0,-1), (1,0), (1,1), (-1,0)\}$

2) Paramétrage d'une courbe dans le plan

On suppose $\mathbb{K}$ algébriquement clos

Def 36 : On appelle courbe paramétrée sur $\mathbb{K}^2$ l'image de
$f : t \in \mathbb{K} \mapsto \left(\frac{P(t)}{Q(t)}, \frac{R(t)}{S(t)}\right)$, $P, Q, R, S \in \mathbb{K}[X]$. f est dit paramétrage.

Prop 37 : Soit $(x,y) \in \mathbb{K}^2$. On écarte le cas où $x = -\frac{P_{\deg Q}}{Q_{\deg Q}}$ et
$y = -\frac{R_{\deg S}}{S_{\deg S}}$ si $\deg Q \geq \deg P$ et $\deg S \geq \deg R$

Alors (x,y) est un point de la courbe si et seulement si
$$Res_T(Q(T)X - P(T), S(T)Y - R(T))(x,y) = 0$$

Ex 38 : la courbe $\{(t^2, t^3 - t), t \in \mathbb{K}\}$ est l'ensemble des zéros du polynôme $X(-X+1)^2 - Y^2$

3) Le Nullstellensatz : $\mathbb{K}$ algébriquement clos

Th 39 (Nullstellensatz) : Soit $f_1, \dots, f_m \in \mathbb{K}[X_1, \dots, X_n]$. On suppose que $f_1, \dots, f_m$ n'ont pas de racines communes. Alors $(f_1, \dots, f_m) = \mathbb{K}[X_1, \dots, X_n]$

App 40 : Les idéaux maximaux de $\mathbb{K}[X_1, \dots, X_n]$ sont les $(X_1 - x_1, \dots, X_n - x_n)$, $x_1, \dots, x_n \in \mathbb{K}$.

4) Application en théorie des corps

Soit $\mathbb{L}/\mathbb{K}$ extension de corps, $P, Q \in \mathbb{K}[X]$, $\alpha, \beta \in \mathbb{L}$, $P(\alpha) = 0$, $Q(\beta) = 0$, $R \in \mathbb{K}[X]$

Prop 41 :
- $Res_X(P(X), Q(T - X))$ annule $\alpha + \beta$
- $Res_X(P(X), X^{\deg Q} Q\left(\frac{T}{X}\right))$ annule $\alpha\beta$
- $Res_X(P(X), T - R(X))$ annule $R(\alpha)$

Ex. 42 : Le polynôme minimal de $\sqrt{2} + \sqrt{3}$ sur $\mathbb{Q}$ est $T^4 - 10T^2 + 1$

5) Le discriminant d'un polynôme

Soit $P \in \mathbb{K}[X]$, $\deg P = n \geq 1$, $\mathbb{L}$ le corps de décomposition de P sur $\mathbb{K}$
On note $P = \lambda \prod_{i=1}^{n} (X - x_i)$ dans $\mathbb{L}$

Def 43 : On pose $\Delta(P) := (-1)^{\frac{n(n-1)}{2}} Res(P, P')$: discriminant de P
on pose $\delta(P) := \prod_{i<j} (x_i - x_j)$

Prop 44 : $\Delta(P) = \lambda^{2n-1} \delta(P)^2$

Prop 45 : P a une racine double dans $\mathbb{L}$ si et seulement si $\Delta(P) = 0$

Ex 46 : $\Delta(aX^2 + bX + c) = b^2 - 4ac$

Prop 47 : On suppose $\mathrm{car}\, \mathbb{K} \neq 2$. Alors, si $P = aX^2 + bX + c$, P a une racine dans $\mathbb{K}$ si et seulement si $\sqrt{\Delta} \in \mathbb{K}$. Alors les racines sont $\frac{-b \pm \sqrt{\Delta}}{2a}$.

Ex 48 : $\Delta(X^3 + pX + q) = -4p^3 - 27q^2$

6) La loi de réciprocité quadratique.

Def 49 : Soit p nombre premier impair, $a \wedge p = 1$.
On pose $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \bmod p \text{ est un carré} \\ -1 & \text{sinon} \end{cases}$

Prop 50 : Si $a \wedge p = 1$, p premier impair, $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} [p]$

Th 51 (réciprocité quadratique) : Soit p, q nombres premiers impairs, avec $p \wedge q = 1$. Alors $\left(\frac{p}{q}\right)\left(\frac{1}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

DEV 1

DEV 2

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

III) Commentaires

① Défense de plan

- bien,
- partie II : on part des corps, on descend à A factoriel puis on remonte à K

② Plan

- bien complet
- ambitieux
- il y a certaines choses on sait pas à quoi ça sert (eg. forme de covariance)
- c'est bien de préciser les cas génants (cf. appli)

③ Dvt

- bien clair
- ⚠ $\mathbb{Z}[X]$ pas un anneau
- ⚠ $(-1)^{(\ )\times(\ )}$ est pas $(-1)^{(\ )} \times (-1)^{(\ )}$

II) Exercices

(1) Calculer un poly annulateur de $\sqrt{3}+\sqrt[3]{5}$

$P(X) = X^2 - 3 \quad Q(X) = X^3 - 5$.

$\mathrm{Res}_X(X^2-3, (T-X)^3-5) = \mathrm{Res}_X(X^2-3, -X^3+3TX^2-3T^2X+T^3-5)$

$= \mathrm{Res}_X(X^2-3, 3TX^2-3(T^2+1)X+T^3-5)$

$= \mathrm{Res}_Y(X^2-3, -3(T^2+1)X+T^3+9T-5)$

$$= \begin{vmatrix} 1 & 0 & -3 \\ -3(T^2+1) & T^3+9T-5 & 0 \\ 0 & -3(T^2+1) & T^3+9T-5 \end{vmatrix}$$

$= (T^3+9T-5)^2 - 27(T^2+1)^2$

(2)

$\mathrm{Res}_X(X^r-a, X^s-b) \quad r \leq s$

$\mathrm{Res}_X(X^r-a, aX^{s-r}-b) \quad a \neq 0.$

$= a^r \mathrm{Res}_X(X^r-a, X^{s-r}-b_1) \quad b_1 = b/a$

$= a^{rq} \mathrm{Res}_X(X^r-a, X^t - b/a^q) \quad s = qr+t, \ t<r$

$= a^{rq}(-1)^{rt} \mathrm{Res}_X(X^t - b/a^q, X^r - a)$

$= \lambda \, \mathrm{Res}_X(X-\alpha, X^n-\beta) = \lambda(\alpha^n-\beta) \quad \alpha, \beta \in \mathbb{K}, \ \lambda \in \mathbb{K}^*$

$\Rightarrow \begin{cases} \alpha = a^\ell b^k \\ \beta = a^{\ell'} b^{k'} \end{cases} : \ell, k, \ell', k' \in \mathbb{N}$

On voit rapidement que pr que le résultant soit nul il faut une relation entre a et b. ($\sqrt[r]{\ }$ = $\sqrt[r]{\ }$ r-ième de a = $\sqrt[s]{\ }$ s-ième de b)

Se retrouve ici

I / Questions plan

- Prop 6 Cmt on dém l'invariance par transla° ?
- Prop 8 Dém ?
- Cor 9 Dém ?
- Cmt est-ce qu'on obtient la prop 29 ?
  ↳ ⚠ Qd on passe à plusieurs var $K[X_1, \dots X_n] = A[X_n]$ avec
  $A = K[X_1, \dots X_{n-1}]$ pas un corps.
  ⇝ il vaut mieux passer par A factoriel que d'aller directement
  ds un corps.
- En quoi l'applica° 40 est une appli du thm 39 ?
  ↳ Ω idéal maximal. Alors $\Omega \subset (X_1 - x_1, \dots, X_n - x_n)$
- Prop 41 Degrés attendus ? ⟵ (pour se mettre ds le plan)
- Montrer exple 48
  ↳ $\Delta(X^3+pX+q) = -\mathrm{Res}(X^3+pX+q, 3X^2+p) = -\mathrm{Res}(3X^2+p, X^3+pX+q)$
  $= -3^2 \mathrm{Res}(3X^2+p, \frac{2p}{3}X+q)$
  $= -3^2 \begin{vmatrix} 3 & 0 & p \\ 2p/3 & q & 0 \\ 0 & 2p/3 & q \end{vmatrix} = \dots$
- Applica° du discriminant & de la réciprocité quadratique
  Recherche des $\sqrt{}$ en deg 2 et 3. Matrice ar desp. distincte ? → équa diff
  ↳ Discriminant Prop 15 et 17 + théorie de Galois ($\Delta \in K$?)
  + continuité rpi (cf TD)
  Réciprocité quadr. Permet de déterminer si un nbre de $\mathbb{F}_q$ est un carré
  ↳ théorie des nbres
  (pour déterminer si a est un carré de $\mathbb{F}_q$: on factorise $X^2 - a$ ds $\mathbb{F}_q$ (on a un algo déterministe et rapide pour factoriser ds $\mathbb{F}_q$)
  → Utilité calculatoire majoritairement

Loi de réciprocité quadratique par le résultant

□ **Théorème :** Soit p, q nombres premiers impairs distincts alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

démonstration : Soit n nombre premier impair, alors :

$$\exists ! \psi_n \in \mathbb{Z}[X],\ \psi_n\left(X + \frac{1}{X}\right) = \frac{H_n(X)}{X^{\frac{n-1}{2}}}$$

où $H_n(X) = \sum_{k=0}^{n-1} X^k = \frac{X^n - 1}{X - 1} = \phi_n(X)$.

□ **lemme :** $\psi_n(X) = (X-2)^{\frac{n-1}{2}} \bmod n$

En effet :

$$\psi_n(X + X^{-1}) \bmod n = \frac{1}{X^{\frac{n-1}{2}}} \times \frac{(X-1)^n}{X-1} \bmod n$$

$$= \left(\frac{(X-1)^2}{X}\right)^{\frac{n-1}{2}} \bmod n$$

$$= (X + X^{-1} - 2)^{\frac{n-1}{2}} \bmod n.$$

Par unicité de ψ_n dans $\mathbb{F}_n[X]$, on a $\psi_n(X) = (X-2)^{\frac{n-1}{2}} \bmod p$

□ **lemme :** $\operatorname{Res}(\psi_p, \psi_q) = \left(\frac{q}{p}\right)$

En effet : Comme ψ_p et ψ_q sont unitaires, on a :

$$\operatorname{Res}(\psi_p, \psi_q) \bmod p = \operatorname{Res}(\psi_p \bmod p, \psi_q \bmod p)$$

$$= \operatorname{Res}\left((X-2)^{\frac{p-1}{2}} \bmod p, \psi_q \bmod p\right) *$$

$$= \operatorname{Res}(X - 2 \bmod p, \psi_q \bmod p)^{\frac{p-1}{2}} \text{ car } \psi_q \text{ unitaire}$$

$$* = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \operatorname{Res}(\psi_q \bmod p, (X-2)^{\frac{p-1}{2}} \bmod p) = \psi_q(2)^{\frac{p-1}{2}} \bmod p$$

$$= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \operatorname{Res}(\psi_q \bmod p, X - 2 \bmod p)^{\frac{p-1}{2}} = \psi_q(1+1^{-1})^{\frac{p-1}{2}} \bmod p$$

$$= \operatorname{Res}(X - 2 \bmod p, \psi_q \bmod p)^{\frac{p-1}{2}} = q^{\frac{p-1}{2}} \bmod p \quad \text{par définition de } \psi_q$$

$$= \left(\frac{q}{p}\right) \bmod p \quad (\text{car } p \neq q)$$

Pour conclure, il suffit de montrer que, si n est un nombre premier, alors $n \mid \operatorname{Res}(\psi_p, \psi_q)$, donc, comme ψ_p et ψ_q sont unitaires, de montrer que $\operatorname{Res}(\psi_p \bmod n, \psi_q \bmod n) \neq 0 \bmod n$.

donc, comme $\mathbb{F}_n$ est un corps, ψ_p annule x et ψ_q annule x n'ont pas de racine commune dans $\overline{\mathbb{F}_n}$. On suppose par l'absurde que $\overline{\psi_p}(y) = \overline{\psi_q}(y) = 0$, où $y \in \mathbb{F}_n$. Soit $x \in \overline{\mathbb{F}_n}$ solution de $X^2 - yX + 1$, alors $x \neq 0$ et $x + x^{-1} = y$, alors $\overline{H_p}(x) = \overline{H_q}(x) = 0$, donc $x^p = 1$ et $x^q = 1$. Comme $p \wedge q = 1$, (car $p \neq q$), on a $x = 1$. Or : $0 = \overline{H_p}(1) = p$ modulo n et $0 = \overline{H_q}(1) = q$ modulo n, ce qui est absurde car $p \neq q$.

Ainsi, $\mathrm{Res}(\psi_p, \psi_q) = \left(\frac{q}{p}\right)$.

Conclusion : $\left(\frac{q}{p}\right) = \mathrm{Res}(\psi_p, \psi_q) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \mathrm{Res}(\psi_q, \psi_p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)$.

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

Leçons : 121 : nombres premiers
125 : extension de corps.
143 : Resultant
144 : Racines d'un polynôme.

□ **lemme** : Soit A anneau unifère, on pose $A_{[m]}[X] := \left\{ \sum_{k=-m}^{m} a_k X^k, \forall k, a_k = a_{-k} \right\}$
Soit $P \in A_{[m]}[X]$, $P = \sum_{k=-m}^{m} a_k X^k$. Alors : $\boxed{\exists ! Q \in A_m[X], P(X) = Q\left(X + \frac{1}{X}\right)}$

démonstration : Il suffit de vérifier que $\left\{ \left(X - \frac{1}{X}\right)^k \right\}_{0 \leq k \leq m}$ est une A-base de $A_{[m]}[X]$. Cette famille est clairement libre.
Pour l'existence : . si $P = a_0$, alors $Q = a_0$ convient
. Sinon, on note $n := \deg P \leq m$, $n \geq 1$, alors, comme X et $-\frac{1}{X}$ commutent, on a $P - a_n \left(X - \frac{1}{X}\right)^n \in A_{[n-1]}[X]$, et l'on procède par récurrence.

(?) : est-ce que la preuve s'adapte pour $\left(\frac{2}{p}\right)$

Le Nullstellensatz via le résultant

Théorème : Soit $\mathbb{K}$ un corps algébriquement clos, $f_1, \dots, f_m \in \mathbb{K}[X_1, \dots, X_n]$. On suppose que $V(f_1, \dots, f_m) = \emptyset$. Alors : $\exists h_1, \dots, h_m \in \mathbb{K}[X_1, \dots, X_n]$, $\sum_{i=1}^m h_i f_i = 1$

Démonstration : Comme $\mathbb{K}$ est alg. clos, $\mathbb{K}$ est infini.

lemme : Soit $\mathbb{L}$ un corps infini, $f \in \mathbb{L}[X_1, \dots, X_n]$, $f \neq 0$, $\deg f = d$

alors : $\exists a_1, \dots, a_{n-1} \in \mathbb{L}$, $f(a_1 X_n + X_1, \dots, a_{n-1} X_n + X_{n-1}, X_n)$ est de la forme $c X_n^d + g$, où $\deg_{X_n} g < d$ et $c \neq 0$

En effet : on note h la partie homogène de degré d de f.

Comme $\deg f = d$, $h \neq 0$. Soit $a_1, \dots, a_{n-1} \in \mathbb{L}$

alors $f(a_1 X_n + X_1, \dots, a_{n-1} X_n + X_{n-1}, X_n) = h(a_1, \dots, a_{n-1}, 1) X_n^d + g_{a_1, \dots, a_{n-1}}$

où $\deg_{X_n} g_{a_1, \dots, a_{n-1}} < d$

Comme h est homogène et $h \neq 0$, $h(X_1, \dots, X_{n-1}, 1) \neq 0$

(sinon : $\exists k \in \mathbb{L}[X_1, \dots, X_n]$, $h = (X_n - 1)k$, donc $k = 0$ car h homogène)

et comme $\mathbb{L}$ est infini, il existe $a_1, \dots, a_{n-1} \in \mathbb{L}$, $h(a_1, \dots, a_{n-1}, 1) \neq 0$

d'où le résultat. ∎ lemme

On procède alors par récurrence sur n :

- Si $n = 1$, comme $\mathbb{K}[X]$ est principal, $(f_1, \dots, f_m) = (g)$. Par ailleurs, si $g(\alpha) = 0$, alors $f_i(\alpha) = 0$, $\forall i$. Comme $\mathbb{K}$ est algébriquement clos, et $V(f_1, \dots, f_m) = \emptyset$, on a $g = 1$, d'où le résultat
- On suppose le résultat vrai au rang $n-1$, avec $n > 1$.
- Via le lemme, on peut supposer $f_1 = X_n^d + q$, $\deg_{X_n} q < d$ (car $\mathbb{K}$ est infini)

On pose $g(T, X_1, \dots, X_n) = f_2 + f_3 T + \dots + f_m T^{m-2} \in \mathbb{K}[X_1, \dots, X_n, T]$

et $h := \mathrm{Res}_{X_n}(f_1, g) \in \mathbb{K}[X_1, \dots, X_{n-1}, T]$

On écrit $h = \sum_{i=0}^{k} l_i(X_1, \dots, X_{n-1}) T^{k-i}$

Par ailleurs, il existe $A, B \in \mathbb{K}[X_1, \dots, X_n, T]$ tel que $h = A f_1 + B g$ (car h est un résultant de ces deux polynômes)

En particulier, $h \in (f_1, \dots, f_m) \subset \mathbb{K}[X_1, \dots, X_n, T]$

donc : $\forall i \in [\![0, k]\!]$, $l_i \in (f_1, \dots, f_m) \subset \mathbb{K}[X_1, \dots, X_n]$

lemme : (les l_i n'ont pas de zéros communs)

En effet : on suppose par l'absurde que les l_i ont un zéro

commun $x = (x_1, \dots, x_{n-1}) \in \mathbb{K}^{n-1}$. Soit $a \in \mathbb{K}$
alors $h(x_1, \dots, x_{n-1}, a) = 0$
Par ailleurs, le coefficient dominant de $f_1 \in \mathbb{K}[X_1, \dots, X_{n-1}, T][X_n]$ en X_n est 1, qui ne s'annule pas en $(x_1, \dots, x_{n-1}, a)$, donc d'après la théorie de l'élimination, $f_1(x_1, \dots, x_{n-1}, X_n)$ et $g(x_1, \dots, x_{n-1}, X_n, a)$ ont une racine commune dans $\mathbb{K}$ car $\mathbb{K}$ est algébriquement clos. Par ailleurs, comme $\mathbb{K}$ est intègre, $f_1(x_1, \dots, x_{n-1}, X_n)$ a un nombre fini de racines, donc, comme $\mathbb{K}$ est infini, il existe $x_n \in \mathbb{K}$ tel que $f_1(x_1, \dots, x_n) = 0$ et $g(x_1, \dots, x_{n-1}, x_n, T)$ a une infinité de racines donc $g(x_1, \dots, x_n, T) = 0$ (car $\mathbb{K}$ intègre infini)
donc $(x_1, \dots, x_n) \in V(f_1, \dots, f_m)$, ce qui est absurde.
Ainsi, par hypothèse de récurrence, $1 \in (l_0, \dots, l_k) \subset \mathbb{K}[X_1, \dots, X_{n-1}]$,
donc $1 \in (f_1, \dots, f_m) \subset \mathbb{K}[X_1, \dots, X_n]$.

Leçons : 142 : algèbre de polynômes à plusieurs indéterminées
143 : Résultant.