Jean Fresnel, le 02/11/2008

La théorie de l'élimination

1. Le système résultant de plusieurs polynômes à une variable.

Théorème 1 *Soient les variables sur* $\mathbb{Z}$: $X, A_{1,0}, A_{1,1}, \ldots, A_{1,d_1-1}, A_{i,j}$ *pour* $2 \le i \le r$, $0 \le j \le d_i$, $V_2, V_3, \ldots, V_r$. *Soient*
$F_1(X) := A_{1,0} + A_{1,1} X + \ldots + A_{1,d_1-1} X^{d_1-1} + X^{d_1}$,
$F_i(X) := A_{i,0} + A_{i,1} X + \ldots + A_{i,d_i-1} X^{d_i}$ *pour* $2 \le i \le r$,
$F_V(X) := V_2 F_2(X) + V_3 F_3(X) + \ldots + V_r F_r(X)$. *Alors le résultant de* F_1 *et* F_V *considérés comme polynômes en la variable* X *et en degré* d_1 *et* $\max_{2 \le i \le r} d_i$, *s'écrit sous la forme* $\mathrm{Res}(F_1, F_V) = \sum_{|\nu| = d_1} a_\nu(A) V^\nu$ *où* $\nu = (\nu_2, \nu_3, \ldots, \nu_r)$ *et* $|\nu| = \nu_2 + \nu_3 + \ldots + \nu_r$ *et* $a_\nu(A) \in \mathbb{Z}[A_{ij}]_{i,j}$.
Soient K *un corps commutatif,* $(a_{ij})_{i,j}$ *une famille d'éléments de* K ,
$\rho : \mathbb{Z}[A_{i,j}]_{i,j} \to K$ *l'homomorphisme canonique défini par* $\rho(A_{i,j}) = a_{ij}$,
$f_1, f_2, \ldots, f_r$ *les images canoniques induites par* ρ *de* $F_1, F_2, \ldots, F_r$ *dans* $K[X]$.
Alors les propriétés suivantes sont équivalentes.
i) Il existe $\alpha \in K^{alg}$ *avec* $f_1(\alpha) = f_2(\alpha) = \ldots = f_r(\alpha) = 0$,
ii) on a $\rho(a_\nu(A)) = 0$ *pour tout* ν *avec* $|\nu| = d_1$.
La famille $(a_\nu(A))_\nu$ s'appelle *un système résultant de* $F_1, F_2, \ldots, F_r$.

Démonstration
i) implique *ii)* . Soit $f_V(X) := V_2 f_2(X) + V_3 f_3(X) + \ldots + V_r f_r(X)$. Si donc $f_1(\alpha) = f_2(\alpha) = \ldots = f_r(\alpha) = 0$, il suit que $f_1(\alpha) = 0$ et que $f_V(\alpha) = 0$, on sait alors que cela implique que $\mathrm{Res}(f_1(X), f_V(X)) = 0$. Si on note encore $\rho : \mathbb{Z}[A, V] \to K[V]$ l'homomorphisme canonique induit par $\rho(A_{i,j}) = a_{ij}$ et $\rho(V_i) = V_i$. Alors on déduit que $\rho(\mathrm{Res}(F_1(X), F_V(X)) = 0$; i.e.
$\sum_{|\nu| = d_1} a_\nu(\alpha) V^\nu = 0$ et donc que $a_\nu(\alpha) = 0$, pour tout ν avec $|\nu| = d_1$.
ii) implique i) Si $a_\nu(\alpha) = 0$ pour tout ν avec $|\nu| = d_1$, on a donc $\mathrm{Res}(f_1, f_V) = 0$, il suit qu'il existe $\alpha \in K(V)^{alg}$ tel que $f_1(\alpha) = 0$ et $f_V(\alpha) = 0$, où $K(V) := \mathrm{Fr}(K[V_2, V_3, \ldots, V_r])$. Or $f_1(\alpha) = 0$ implique que $\alpha \in K^{alg}$. Ensuite $V_2 f_2(\alpha) + V_3 f_3(\alpha) + \ldots + V_r f_r(\alpha) = 0$ implique
$f_2(\alpha) = f_3(\alpha) = \ldots = f_r(\alpha) = 0$ parce que $(V_2, V_3, \ldots, V_r)$ reste une famille algébriquement libre sur K^{alg} .

2. Existence d'un système résultant pour plusieurs variables

Théorème 2 *Soient* $q \geq 1$ *un entier*
$N_q := \{ \nu := (\nu_0, \nu_1, \ldots, \nu_n) \in \mathbb{N}^{n+1} \mid |\nu| := \nu_\alpha + \nu_1 + \ldots + \nu_n = q \}$,
$n_q := \operatorname{card} N_q = \binom{n-1+q}{n-1}$, $q_1, q_2, \ldots, q_r$ *des éléments de* $\mathbb{N}$, $X_0, X_1, \ldots, X_n$,
$(A_{i,\nu i})_{1 \leq i \leq r, \nu i \in N_{q_i}}$ *des indéterminées sur* $\mathbb{Z}$. *Soit* $F_i(X) := \sum_{|\nu^i| = q_i} A_{i,\nu i} X^\nu$ *avec*
$X^\nu := X_0^{\nu_0} X_1^{\nu_1} \ldots X_n^{\nu_n}$ *si* $\nu := (\nu_0, \nu_1, \ldots, \nu_n)$, i.e. $F_i(X)$ *est un polynôme homogène en les* X_i *homogène de degré* q_i *et à coefficients dans* $\mathbb{Z}[A_{i,\nu i} \mid |\nu_i| = q_i]$. *Alors il existe* $G_1, G_2, \ldots, G_s \in \mathbb{Z}[A_{i,\nu^i} \mid 1 \leq i \leq r, |\nu^i| = q_i]$ *qui sont des polynômes homogènes en les variables* A_{i,ν^i} *pour chaque* i . *Soient* K *un corps commutatif,* (a_{i,ν^i}) *une famille d'éléments de* K, $f_i(X) := \sum_{|\nu^i| = q_i} a_{i,\nu i} X^{\nu i}$, g_j *l'image canonique de* G_j *dans* $K[a_{i,\nu^i} \mid 1 \leq i \leq r, |\nu^i| = q_i]$.
Alors les propriétés suivantes sont équivalentes.
i) La racine de l'idéal $f_1 K[X] + f_2 K[X] + \ldots + f_n K[X]$ *est l'idéal*
$X_0 K[X] + X_1 K[X] + \ldots + X_n K[X]$,
ii) il existe j *avec* $g_j(a_{i,\nu^i}) \neq 0$.
Cet énoncé est équivalent au suivant.
i) Il existe $x_0, x_1, \ldots, x_n \in K^{alg}$ *avec* $(x_0, x_1, \ldots, x_n) \neq (0, 0, \ldots, 0)$ *et qui est un zéro commun de* $f_1, f_2, \ldots, f_r$,
ii) la famille $(a_{i,\nu i})_{1 \leq i \leq r}$, $|\nu^i| = q_i$ *est un zéro commun de* $g_1, g_2, \ldots, g_s$.
La famille $(G_1, G_2, \ldots, G_s)$ s'appelle *un système résultant de* $F_1, F_2, \ldots, F_r$.

Démonstration Il existe q_0 tel que pour $q \geq q_0$ on ait
$n_{q-q_1} + n_{q-q_2} + \ldots + n_{q-q_r} \geq n_q$. Pour ν tel que $|\nu| + q_i = q$, on a
$X^\nu F_i = \sum_{|\nu_i| = q_i} A_{i,\nu^i} X^{\nu + \nu^i}$, cette suite d'égalités pour $1 \leq i \leq r$ définit une matrice $M_q(A_{i,\nu})$ à n_q colonnes et $N := n_{q-q_1} + n_{q-q_2} + \ldots + n_{q-q_r}$ lignes. Ainsi donc les mineurs d'ordre n_q extraits de cette matrice sont des polynômes homogènes en les $A_{i,\nu}$ pour chaque i . Notons $D_{q,j}$ pour $1 \leq j \leq \binom{N}{q}$ ces polynômes. On peut extraire de la famille $(D_{q,j})_{q \geq q_0}$ une famille finie qui engendre l'idéal $\sum_{q,j} D_{q,j} \mathbb{Z}[A_{i,\nu}]$; notons la $(G_1, G_2, \ldots, G_s)$.
Supposons ii) satisfait. Ainsi il existe un mineur $D_{q,j}(a_{i,\nu i}) \neq 0$, on peut alors résoudre le système linéaire associé et cela veut bien dire que
$X^\nu \in f_1 K[X] + f_2 K[X] + \ldots + f_r K[X]$, ce qui est bien *i)* .
Supposons i) satisfait. Il existe $s_i \geq 1$ avec
$X_i^{s_i} \in f_1 K[X] + f_2 K[X] + \ldots + f_r K[X]$. Soit maintenant

$q \geq \max(s_1+s_2+\ldots+s_r+1, q_0)$, on a donc
$X^\nu \in f_1 K[X]+f_2 K[X]+\ldots+f_r K[X]$ avec $|\nu|=q$. Il suit de cela que $(\sum_i \sum_{|\nu^i|=q-q_i} KX^{\nu i} F_i) = \bigoplus_{|\nu|=q} KX^\nu$. Ainsi donc la matrice $M_q(a_{i,\nu i})$ est de rang n_q . En conséquence il existe un mineur d'ordre n_q de $M_q(a_{i,\nu i})$ qui est non nul.

3. Le résultant de n polynômes à n variables

Théorème 3 *Soient les variables suivantes sur* $\mathbb{Z}$: $X_1, X_2, \ldots, X_n$, $A_{i,\nu i}$ *avec* $1 \leq i \leq r$, $\nu^i = (\nu_1^i, \nu_2^i, \ldots, \nu_n^i)$ *et* $|\nu^i| := \nu_1^i+\nu_2^i+\ldots+\nu_n^i = d_i$. *Soient les polynômes* $F_i(X) := \sum_{|\nu^i|=d_i} A_{i,\nu i} X^i$ avec $X^{\nu i} := X_1^{\nu_1^i} X_2^{\nu_2^i} \ldots X_n^{\nu_n^i}$.

Notons $\mathbb{Z}[A, X]$ *l'anneau des polynômes sur* $\mathbb{Z}$ *en les variables précédentes ; enfin soit* $\mathfrak{A} := \sum_i \mathbb{Z}[A,X] F_i$.

1. *Soit* $T \in \mathbb{Z}[A_i, \nu^i]_{1 \leq i \leq r, \nu^i}$. *Alors les propriétés suivantes sont équivalentes.*

i) Il existe $m \geq 0$ *tel que* $X_1^m T \in \mathfrak{A}$,

ii) pour tout j , *il existe* $m_j \geq 0$ *tel que* $X_j^{m_j} T \in \mathfrak{A}$.

Il suit de ii) que si $G_1, G_2, \ldots, G_s$ *engendre* $\mathfrak{T}$, *alors* $(G_1, G_2, \ldots, G_s)$ *est un système résultant de* $(F_1, F_2, \ldots, F_r)$.

2. *Soit* $\mathfrak{T}$ *l'idéal des* $T \in \mathbb{Z}[A_i, \nu^i]_{1 \leq i \leq r, \nu^i}$ *pour lesquels il existe* $m_T \geq 0$ *avec* $X_1^{m_T} T \in \mathfrak{A}$. *Il suit de* 1. *ii) que si* $G_1, G_2, \ldots, G_s$ *engendre* $\mathfrak{T}$, *alors* $(G_1, G_2, \ldots, G_s)$ *est un système résultant de* $(F_1, F_2, \ldots, F_r)$, *selon le* **théorème 2** . *D'autre part* $\mathfrak{T}$ *est un idéal premier.*

3. *Si* $r < n$, *on a* $\mathfrak{T} = \{0\}$. *Si* $r = n$, *on a* $\mathfrak{T} \neq \{0\}$ *et* $\mathfrak{T}$ *est un idéal principal.* On note $R(F_1, F_2, \ldots, F_n)$ un générateur de l'idéal $\mathfrak{T}$.

1) Montrons 1. . Il est immédiat que *ii)* implique *i)* . Montrons maintenant que *i)* implique *ii)* . Notons $A_{i,\alpha}$ le coefficient de $X_j^{d_i}$ dans $F_i(X)$, on a donc $F_i = A_{i,\alpha} X_j^{d_i} - F_i^*$. Ainsi le degré $F_1^*, F_1^*, \ldots, F_r^*$ en les variables $A_{1,\alpha}, A_{2,\alpha}, \ldots, A_{r,\alpha}$ est négatif ou nul. Soit $\rho_j : \mathbb{Z}[A,X] \to \mathbb{Z}[A, X][\frac{1}{X_j}]$ défini par $\rho_j(A_{i,\alpha}) := \frac{F_i^*}{X_j^{d_i}}$, $\rho_j(A_{i,\nu}) = A_{i,\nu}$ pour $\nu \neq \alpha$ et $\rho_j(A_{i,\alpha}) = X_i$ pour $1 \leq i \leq n$.

Facilement $\rho_j(\mathfrak{A}) = \{0\}$. Si $X_1^m T \in \mathfrak{A}$, on a donc $\rho_j(T) = 0$. Soit $B := \mathbb{Z}[A_{i,\nu}, X]_{\nu \neq \alpha}$, on a donc
$\mathbb{Z}[A,X] = B[A_{1,\alpha}, A_{2,\alpha}, \ldots, A_{r,\alpha}]$, ainsi
$T = \sum b_{t_1 t_2 \ldots t_r} (A_{1,\alpha})^{t_1} (A_{2,\alpha})^{t_2} \ldots (A_{r,\alpha})^{t_r}$ avec $b_{t_1 t_2 \ldots t_r} \in B$. Il existe donc $m' \geq 0$ tel que $X_j^{m'} T = \sum b'_{t_1 t_2 \ldots t_r} (X_j^{d_1} A_{1,\alpha})^{t_1} (X_j^{d_2} A_{2,\alpha})^{t_2} \ldots (X_j^{d_r} A_{r,\alpha})^{t_r}$ avec

$b'_{t_1 t_2 \ldots t_r} \in B$. Sachant que $X_j^{d_i} A_{1,\alpha} = F_i + F_i^*$, on déduit que $X_j^{m'} T = U + V$ où $U \in \mathfrak{A}, V \in B$. Comme $\rho_j(T) = 0$, $\rho_j(U) = 0$ et $\rho_j(V) = V$, on déduit que $V = 0$ et donc $X_j^{m'} T \in \mathfrak{A}$.

En considérant de façon analogue un homomorphisme ρ_1 , on déduit que si $X_j^{m'} T \in \mathfrak{A}$, alors il existe $m'' \geq 0$ avec $X_1^{m''} T \in \mathfrak{A}$.

Soit $(G_1, G_2, \ldots, G_s)$ un système générateur de $\mathfrak{T}$, K un corps commutatif, $a_{i,\nu} \in K$ des spécialisations de $A_{i,\nu}, g_1, g_2, \ldots, g_s, f_1, f_2, \ldots, f_r$ les spécialisations induites sur les G_i et les F_i . On suppose que $x = (x_1, x_2, \ldots, x_n)$ est un zéro commun de $f_1, f_2, \ldots, f_r$ avec $x_i \neq 0$. Comme $x_i^m G_j(a) = U_1(x) f_1(x) + U_2(x) f_2(x) + \ldots + U_r(x) f_r(x)$ on a bien $G_j(a) = 0$ pour $1 \leq j \leq s$. Si on suppose qu'il existe j avec $G_j(a) \neq 0$, sachant que $X_i^{m_i} G_j(a) = U_1(X) f_1(X) + U_2(X) f_2(X) + \ldots + U_r(X) f_r(X)$, on a bien $\sqrt{f_1 K[X] + f_2 K[X] + \ldots + f_r K[X]} = X_1 K[X] + X_2 K[X] + \ldots + X_n K[X]$; ce qui montre que $(0, 0, \ldots, 0)$ est le seul zéro commun de $f_1, f_2, \ldots, f_r$.

2) Montrons 2. Il suit facilement de $i)$ de 1. que $\mathfrak{T}$ est un idéal de $\mathbb{Z}[A_{i,\nu^i}] 1 \leq i \leq r, \nu^i$. Soit $\rho_1 : \mathbb{Z}[A_{i,\nu^i}]_{i,\nu^i} \to \mathbb{Z}[A_{i,\nu^i}][\frac{1}{X_1}]$, il suit de 1) que $T \in \mathfrak{T}$ si et seulement si $\rho_1(T) = 0$. Comme $\mathbb{Z}[A_{i,\nu^i}][\frac{1}{X_1}]$ est intègre, on déduit que $\mathfrak{T}$ est un idéal premier.

3) Montrons 3. .

3.1) *On suppose que* $r < n$. Soit $A_{i,\beta}$ le coefficient de $X_n^{d_i}$ dans F_i , on a donc $F_i = A_{i,\beta} X_n^{d_i} - F_i^*$. Soient $B := \mathbb{Z}[A_{i,\nu}]_{i,\nu \neq \beta}$, $\rho : \mathbb{Z}[A, X] \to B[X][\frac{1}{X_n}]$ défini par $\rho(A_{i,\beta}) = \frac{F_i^*}{X_n^{d_i}}$,

$\rho(A_{i,\nu}) = A_{i,\nu}$ pour $\nu \neq \beta$, $\rho(X_i) = X_i$ pour $1 \leq i \leq n$. Si $T \in \mathfrak{T}$, on a donc $\rho(T) = 0$. On spécialise $A_{i,\nu}$ pour $\nu \neq \beta$ de façon que F_i^* ait pour image $X_i^{d_i}$ pour $1 \leq i \leq r$. Comme T est non nul, par le lemme ci-après, cela veut dire que $(\frac{X_1}{X_n})^{d_1}, (\frac{X_2}{X_n})^{d_2} \ldots, (\frac{X_r}{X_n})^{d_r}$ sont algébriquement liées sur K ; ce qui est faux, ainsi $\mathfrak{T} = \{0\}$.

3.2) *On suppose maintenant que* $r = n$ *et qu'il existe* $T \in \mathfrak{T}$ *et* $T \neq 0$, *il s'agit de montrer que* $\deg_{A_{n,\beta}} T \geq 1$. On suppose le contraire, et ρ est toujours l'homomorphisme défini selon le paragraphe précédent 3.1) , on a donc $\rho(T) = 0$. On spécialise $A_{i,\nu}$ pour $(i, \nu) \neq (n, \beta)$ de façon que F_i^* ait pour image $X_i^{d_i}$ pour $1 \leq i \leq n-1$. Par le lemme ci-après, il suit que $(\frac{X_1}{X_n})^{d_1}, (\frac{X_2}{X_n})^{d_2} \ldots, (\frac{X_{n-1}}{X_n})^{d_{n-1}}$ sont algébriquement liés, ce qui est faux, ainsi $\deg_{A_{n,\beta}} T \geq 1$.

3.3) *Si* $r=n$, *il existe* $D_n\in\mathfrak{T}$ *qui est un polynôme homogène en* $(A_{i,\nu})_\nu$ *et qui est de degré* $d_1d_2\dots d_{n-1}$ *en* $(A_{n,\nu})_\nu$. *En particulier si* $\deg F_1=\deg F_2=\dots=\deg F_{n-1}=1$, *alors* $R(F_1,F_2,\dots,F_n)$ *est homogène en* A_{n,ν^n} *de degré* 1.

Soient $d:=1+(d_1-1)+(d_2-1)+\dots+(d_n-1)$,

$\mathcal{H}:=\{\nu=(\nu_1,\nu_2,\dots,\nu_n)\,|\,|\nu|=d\}$,

$\mathcal{H}_1:=\{\nu=(\nu_1,\nu_2,\dots,\nu_n)\,|\,|\nu|=d,\nu_1\geq d_1\}$,

$\mathcal{H}_2:=\{\nu=(\nu_1,\nu_2,\dots,\nu_n)\,|\,|\nu|=d,\nu_1<d_1,\nu_2\geq d_2\}$,

...

$\mathcal{H}_i:=\{\nu=(\nu_1,\nu_2,\dots,\nu_n)\,|\,|\nu|=d,\nu_1<d_1,\dots,\nu_{i-1}<d_{i-1},\nu_i\geq d_i\}$

...

$\mathcal{H}_n:=\{\nu=(\nu_1,\nu_2,\dots,\nu_n)\,|\,|\nu|=d,\nu_1<d_1,\dots,\nu_{n-1}<d_{n-1},\nu_n\geq d_n\}$

On a donc $\mathcal{H}=\mathcal{H}_1\cup\mathcal{H}_2\cup\cup\dots\cup\mathcal{H}_n$.

On considère le système linéaire suivant

$X_1^{-d_1}X^\nu F_1=\sum_{|\mu|=d_1}A_{1,\mu}X^{\mu+\nu}X_1^{-d_1}$, $\nu\in\mathcal{H}_1$

...

$X_i^{-d_i}X^\nu F_i=\sum_{|\mu|=d_i}A_{i,\mu}X^{\mu+\nu}X_i^{-d_i}$, $\nu\in\mathcal{H}_i$

...

$X_i^{-d_i}X^\iota F_i=\sum_{|\mu|=d_i}A_{i,\mu}X^{\mu+\nu}X_n^{-d_n}$, $\nu\in\mathcal{H}_n$.

Si $h:=\operatorname{card}\mathcal{H}$, c'est un système de h équations à h inconnues, notons D_n le déterminant du système qui est bien un polynôme homogène en $A_{i,\mu}$ de degré $\operatorname{card}\mathcal{H}_i$ pour $1\leq i\leq n$; en particulier $\operatorname{card}\mathcal{H}_n=d_1d_2\dots d_{n-1}$. Si on spécialise $A_{i,\mu}$ de façon que F_i donne $X_i^{d_i}$, il suit que la matrice du système est une permutation des colonnes de la matrice I_h , il suit donc de cela que le polynôme D_n n'est pas nul. On peut donc résoudre le système, ce qui veut dire qu'il existe $U_{i,1},U_{i,2}\dots,U_{i,n}\in\mathbb{Z}[A,X]$ avec

$X_i^dD_n=U_{i,1}F_1+U_{i,2}F_2+\dots+U_{i,n}F_n$. Ainsi $D_n\in\mathfrak{T}$.

3.4) *Si* $r=n$, *montrons que l'idéal* $\mathfrak{T}$ *est principal.* Soit donc $R\in\mathfrak{T}-\{0\}$ et de degré minimum en $A_{n,\beta}$, on a donc $R=R_0+R_1A_{n,\beta}+\dots+R_r(A_{n,\beta})^r$ et $\deg_{A_{n,\beta}}R_i\leq 0$. Soit $T\in\mathcal{T}$, alors il existe $m\geq 1$ tel que $(R_r)^nT-QR=T'$ avec $\deg_{A_{n,\beta}}T'<r$; ce qui veut dire que $T'=0$. Le fait que $\mathfrak{T}$ soit premier implique facilement que R est un élément irréductible de $\mathbb{Z}[A_{i,\nu}]_{i,\nu}$. Comme $R_r\notin\mathfrak{T}$ il suit de la relation $(R_r)^nT=QR$ que R divise T et donc que $\mathfrak{T}=\mathbb{Z}[A_{i,v}]_{i,v}R$.

4. Sur le degré de $R(F_1,F_2,\dots,F_n)$

Théorème 3 *Soient* $A_{i,\nu^i}, X_1,X_2,\dots,X_n$ *des variables sur* $\mathbb{Z}$, $F_i(X) := \sum_{|\nu^i|=d_i} A_{i,\nu^i} X^{\nu^i}$ *, notons toujours* $R(F_1,F_2,\dots,F_n)$ *un générateur de l'idéal* $\mathfrak{T}$ *. Soient* $B_{1,\nu}$ *et* $C_{1,\nu}$ *des variables,* $G(X) := \sum_{|\nu|=\alpha} B_{1,\nu} X^{\nu}$, $H(X) := \sum_{|\nu|=\beta} C_{1,\nu} X^{\nu}$ *avec* $\alpha+\beta=d_1$ *, on a donc* $G(X)H(X) = \sum_{|\nu^1|=d_1} \sum_{\nu+\mu=\nu^1} (B_{1,\nu}C_{1\mu}) X^{\nu^1}$ *. Notons* $\rho(R(F_1,F_2,\dots,F_n))$ *le polynôme où l'on a spécialisé* A_{1,ν^1} *en* $\sum_{\nu+\mu=\nu^1} B_{1\nu}C_{1\mu}$ *. Alors* $R(H,F_2,\dots,F_n)R(G,F_2,\dots,F_n$ *est égal à* $\rho(R(F_1,F_2,\dots,F_n))$ *, aux inversibles près. En plus* $R(F_1,F_2,\dots,F_n)$ *est un polynôme en* A_{i,ν^i} de degré $d_1\dots d_{i-1}d_{i+1}\dots d_{n-1}$ *, pour* $1\le i\le n$ *.*

Démonstration Il existe $m\ge 0$ tel que $X_1^m R(F_1,F_2,\dots,F_n) = U_1F_1+U_2F_2+\dots+U_nF_n$.
En spécialisant A_{1,ν^1} en $\sum_{\nu+\mu=\nu^1} B_{1\nu}C_{1\mu}$ on obtient $X_1^m \rho(R(F_1,F_2,\dots,F_n)) = \rho(U_1)GH+\rho(U_2)F_2+\dots+\rho(U_n)F_n$. Cela veut bien dire que $\rho(R(F_1,F_2,\dots,F_n))$ divise $R(G,F_2,\dots,F_n)$ dans $\mathbb{Z}[B_{1,\nu},A_{2,\nu^2},\dots,A_{n,\nu^2}]_{\nu^i}$ et que $\rho(R(F_1,F_2,\dots,F_n))$ divise $R(H,F_2,\dots,F_n)$ dans $\mathbb{Z}[C_{1,\upsilon},A_{2,\nu^2}\dots,A_{n,\nu^n}]$. Facilement $R(G,F_2,\dots,F_n)$ et $R(H,F_2,\dots,F_n)$ sont des irréductibles non associés, ainsi $\rho(R(F_1,F_2,\dots,F_n))$ divise $R(G,F_2,\dots,F_n)R(H,F_2,\dots,F_n)$.
Si on spécialise $F_1,F_2,\dots,F_{n-1}$ en des produits de polynômes homogènes de degré 1 , on déduit de 3.3) et de ce qui précède que $R(F_1,F_2,\dots,F_n)$ est un polynôme en A_{n,ν^n} de degré $d_1d_2\dots d_{n-1}$.
Sachant que de façon analogue à D_n , il existe un élément D_i de $\mathfrak{T}$ qui est homogène en A_{i,ν^i} de degré $d_1\dots d_{i-1}d_{i+1}\dots d_n$, on déduit que $R(F_1,F_2,\dots,F_n)$ est un polynôme en A_{i,ν^i} de degré $d_1d_{i-1}d_{i+1}\dots d_{n-1}$. Il suit de cela que $R(F_1,F_2,\dots,F_n)$ est aux inversibles près un pgcd de $D_1,D_2,\dots,D_n$.
Il suit aussi du calcul des degrés que $\rho(R(F_1,F_2,\dots,F_n))$ est égal aux inversibles près à $R(G,F_2,\dots,F_n)R(H,F_2,\dots,F_n)$.

Lemme *Soient* K *un anneau intègre,* $A_1,A_2,\dots,A_p,X_1,X_2,\dots,X_n$ *des variables sur* $K,F_1,F_2,\dots,F_s\in K[A,X]$ *. On suppose qu'il existe* $P(Z_1,Z_2,\dots,Z_s)\in K[A][Z_1,Z_2,\dots,Z_s]$ avec $P\ne 0$ et $P(F_1,F_2,\dots,F_s)=0$. *Soient* $a_1,a_2,\dots,a_s\in K$, $f_i(X) := F_i(a_1,\dots,a_sX_1,\dots,X_n)$ *, alors il existe* $Q(Z_1,Z_2,\dots,Z_s)\in K[Z_1,Z_2,\dots,Z_s]$ *avec* $Q\ne 0$ *et* $Q(f_1,f_2,\dots,f_s)=0$.

Démonstration Soient B un anneau intègre, $A, X_1, X_2, \ldots, X_n$ des variables sur $B, F_1, F_2, \ldots, F_0 \in B[A][X_1, X_2, \ldots, X_n]$ et $P[Z_1, Z_2, \ldots, Z_s] \in B[A][Z_1, Z_2, \ldots, Z_s]$ avec $P \neq 0$ et $P(F_1, F_2, \ldots, F_s) = 0$. Soit $a \in B$, si $P(a, Z_1, Z_2, \ldots, Z_s) \neq 0$, alors $Q(Z_1, Z_2, \ldots, Z_s) := P(a, Z_1, Z_2, \ldots, Z_s)$ est tel que $Q(F_1(a, X), F_2(a, X), \ldots, F_s(a, X)) = 0$. Si $P(a, Z_1, Z_2, \ldots, Z_0) = 0$, il existe $m \geq 1$ tel que $P(A, Z_1, Z_2, \ldots, Z_0) = (A - a)^n S(A, Z_1, Z_2, \ldots, Z_s)$ avec $S(a, Z_1, Z_2, \ldots, Z_0) \neq 0$. De plus $P(A, F_1, F_2, \ldots, F_s) = 0$ implique $S(A, F_1, F_2, \ldots, F_s) = 0$; il suit que $S(a, F_1(a, X), \ldots, F_s(a, (X))) = 0$. Cela permet de montrer le lemme par récurrence sur p.

Bibliographie

[M] **Macaulay F.S.** *The algebraic theory of modular systems* Cambridge University Press 1994

[W] **van der Waerden B.L.** *Modern algebra* vol. II p. 1 à 17 Frederick Ungar Publishing Co. 1964

Figuier