Université Bordeaux 1
Mathématiques

Préparation à l'agrégation
Année 2012–2013

Résultant de deux polynômes

Tous les anneaux considérés dans cette note sont commutatifs et unitaires.

1. Rappels sur les anneaux factoriels

Définition 1.1. Un anneau intègre A est dit *factoriel* si les deux conditions suivantes sont réalisées.

(1) Pour tout élément non nul a de A, il existe des éléments irréductibles $p_1, \dots, p_r$ de A et une unité u de A tels que
$$a = u \prod_{i=1}^{r} p_i.$$

(2) Si $up_1 \dots p_r = vq_1 \dots q_r$, où $u, v \in A^*$, et où les éléments $p_1, \dots, p_r, q_1, \dots, q_s \in A$ sont irréductibles, alors $r = s$ et il existe une permutation σ de S_r telle que pour tout i dans $\{1, \dots, r\}$, p_i et $q_{\sigma(i)}$ sont associés (c'est-à-dire qu'il existe $u_i \in A^*$ tel que $p_i = u_i q_{\sigma(i)}$).

Dans un anneau factoriel, la notion de pgcd est bien définie, à multiplication par un élément inversible près. Par contre, il n'y a pas en général d'identité de Bézout. Par exemple, dans $\mathbb{C}[X, Y]$, le pgcd de X et de Y est 1, mais pour tous $P, Q \in \mathbb{C}[X, Y]$, le polynôme $XP + YQ$ est différent de 1.

Si K est un corps, nous connaissons déjà l'algorithme d'Euclide pour calculer le pgcd dans l'anneau de polynômes $K[X]$. Si A est un anneau *intègre*, on peut considérer l'anneau des fractions K de A, et calculer le pgcd dans $K[X]$, mais cela ne donne pas en général le pgcd dans $A[X]$. Par exemple, si l'on considère les polynômes $f = 2X^2 + 2$ et $g = 6X + 2$ de $\mathbb{Z}[X]$, alors $\operatorname{pgcd}(f, g) = 1$ dans $\mathbb{Q}[X]$, mais $\operatorname{pgcd}(f, g) = 2$ dans $\mathbb{Z}[X]$.

Nous alllons maintenant définir les valuations dans un anneau factoriel, et dans son corps des fractions, puis donner un définition du pgcd et du ppcm dans un tel anneau.

Proposition 1.2. *Soient A un anneau factoriel, K son corps des fractions, p un élément irréductible de A. Soit a un élément non nul de K. Alors il existe $u, v \in A$ non divisibles par p, et un entier relatif r tels que*
$$a = p^r \frac{u}{v}.$$
Cet entier r est unique. C'est par définition la valuation en p de a, *notée $v_p(a)$. On convient que $v_p(0) = +\infty$.*

Proposition 1.3. *Pour tous éléments a et b de A, on a*
$$v_p(ab) = v_p(a) + v_p(b),$$
$$v_p(a + b) \geqslant \min(v_p(a), v_p(b)).$$
De plus, cette dernière inégalité est une égalité si $v_p(a) \neq v_p(b)$.

Une partie $\mathcal{P}$ de A est appelée système de représentants des irréductibles de A si pour tout irréductible q de A, il existe p dans $\mathcal{P}$ et u dans A^* uniques tels que $q = up$. C'est en fait un ensemble de représentants de l'ensemble des éléments irréductibles de A, pour la relation d'équivalence : $x \sim y$ s'il existe $u \in A^*$ tel que $x = uy$. (Dans ce cas, on dit que x et y sont associés.)

Si un tel $\mathcal{P}$ est fixé, tout élément a de K^* s'écrit de façon unique sous la forme

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)},$$

où $u \in A^*$. On définit alors le pgcd et le ppcm dans K^* (à multiplication près par un élément de A^*) de la manière suivante.

$$\operatorname{pgcd}(a, b) = \prod_{p \in \mathcal{P}} p^{\min\left(v_p(a), v_p(b)\right)},$$

$$\operatorname{ppcm}(a, b) = \prod_{p \in \mathcal{P}} p^{\max\left(v_p(a), v_p(b)\right)}.$$

La définition du pgcd garde un sens quand $a = 0$ ou $b = 0$ tant qu'ils ne sont pas tous deux nuls ; on pose $\operatorname{pgcd}(0, 0) := 0$.

2. Polynômes à coefficients dans un anneau factoriel

On considère un anneau factoriel A, de corps des fractions K.

Définition 2.1. Soit $f = \sum_{i=0}^{n} f_i X^i$ un polynôme non nul de degré n de $K[X]$. Le *coefficient dominant* de f est son coefficient de plus haut degré, $\operatorname{cd}(f) = f_n \neq 0$. Le *contenu* de f est par définition (à multiplication près par un élément de A^*)

$$\operatorname{cont}(f) = \operatorname{pgcd}(f_0, \ldots, f_n).$$

On définit $\operatorname{cont}(0) := 0$.

Plus généralement, sans hypothèse particulière sur A, on pourrait définir le contenu de $f \in A[X]$ comme l'idéal engendré par ses coefficients. (Noter que définir un élément modulo multiplication par une unité équivaut à se donner l'idéal principal qu'il engendre.)

Le polynôme f est dans $A[X]$ si et seulement si $\operatorname{cont}(f)$ appartient à A.

Définition 2.2. On dit que $f \in K[X]$ est *primitif* si $\operatorname{cont}(f) = 1$ — ce qui implique que $f \in A[X]$.

Définition 2.3. La *partie primitive* $\operatorname{pp}(f)$ d'un polynôme f de $K[X]$ est définie (modulo multiplication par une unité de A) par

$$f = \operatorname{cont}(f) \cdot \operatorname{pp}(f), \quad \text{si } f \neq 0,$$

et $\operatorname{pp}(0) = 0$.

Théorème 2.4. *Le produit de deux polynômes primitifs de $A[X]$ est primitif.*

Preuve. Soient f et g deux éléments primitifs de $A[X]$. Soit p un élément irréductible de A. Comme l'idéal pA est premier, l'anneau $D = A/pA$ est intègre, ainsi donc que $D[X]$. Dans $D[X]$, $[f]_p$ et $[g]_p$ sont non nuls, donc $[fg]_p \neq 0$. Par conséquent, p ne divise pas $\mathrm{cont}(fg)$. Ceci valant pour tout irréductible p de A, on en déduit que $\mathrm{cont}(fg) = 1$. □

Corollaire 2.5. *Soient f et g deux polynômes de $K[X]$. Alors*

$$\mathrm{cont}(fg) = \mathrm{cont}(f)\,\mathrm{cont}(g) \quad \textit{et} \quad \mathrm{pp}(fg) = \mathrm{pp}(f)\,\mathrm{pp}(g).$$

Preuve. Si $fg = 0$, le résultat est évident. Sinon, il suffit de démontrer l'assertion sur les contenus ; en effet on a d'une part

$$fg = \mathrm{cont}(fg)\,\mathrm{pp}(fg),$$

et d'autre part, en décomposant f et g séparément,

$$fg = \mathrm{cont}(g)\,\mathrm{cont}(f)\,\mathrm{pp}(f)\,\mathrm{pp}(g);$$

les contenus étant non nuls, on déduit de $\mathrm{cont}(fg) = \mathrm{cont}(f)\,\mathrm{cont}(g)$ que $\mathrm{pp}(fg) = \mathrm{pp}(f)\,\mathrm{pp}(g)$.

Commençons par un cas particulier : si $g \in K^*$, alors

$$\mathrm{cont}(fg) = \mathrm{pgcd}(f_0 g, \ldots, f_n g) = g\,\mathrm{pgcd}(f_0, \ldots, f_n) = \mathrm{cont}(g)\,\mathrm{cont}(f),$$

et le résultat est démontré dans ce cas.

Soient maintenant f et g dans $K[X]$. On note $h = \mathrm{pp}(fg)$ et $h^* = \mathrm{pp}(f)\,\mathrm{pp}(g)$. On a l'égalité $fg = \mathrm{cont}(f)\,\mathrm{pp}(f)\,\mathrm{cont}(g)\,\mathrm{pp}(g) = \mathrm{cont}(f)\,\mathrm{cont}(g)h^*$. D'où

$$\mathrm{cont}(fg) = \mathrm{cont}\left(\mathrm{cont}(f)\,\mathrm{cont}(g)\,\mathrm{cont}(h^*)\right) = \mathrm{cont}(f)\,\mathrm{cont}(g)\,\mathrm{cont}(h^*),$$

d'après le cas particulier que nous venons de démontrer. Comme h^* est primitif, on peut conclure. □

Proposition 2.6.

(1) *Soit A un anneau intègre. Alors $A[X]^* = A^*$.*
(2) *Soit A un anneau factoriel. Les éléments irréductibles de $A[X]$ sont les irréductibles de A et les polynômes primitifs de $A[X]$ qui sont irréductibles dans $K[X]$.*

Preuve. Pour le (1), l'égalité $fg = 1$ implique que f et g sont non-nuls ; donc $\mathrm{cd}(f)$ et $\mathrm{cd}(g)$ sont bien définis et non-nuls. Leur produit est donc non-nul (A étant intègre) ; on en déduit que $\deg fg = \deg f + \deg g = 0$ ce qui n'est possible que si $\deg f = \deg g = 0$.

Pour le (2), montrons que les polynômes en question sont bien irréductibles dans $A[X]$

- si $p \in A$ est irréductible dans $A[X]$, il est irréductible dans A.
- si $f \in A[X]$ est primitif et irréductible dans $K[X]$, supposons $f = f_1 f_2$, où $f_i \in A[X]$. Alors l'un des f_i, disons f_1, est de degré 0 (irréducibilité dans $K[X]$) et est donc dans K, donc dans A. Donc f_1 est associé à $\mathrm{cont}(f1)$, mais $1 = \mathrm{cont}(f) = \mathrm{cont}(f_1)\,\mathrm{cont}(f_2)$ et donc $f_1 \in A^*$.

Inversement, si p est irréductible dans A, il est irréductible dans $A[X]$, puisque si $p = fg$, alors $\deg f + \deg g = 0$, donc $\deg f = \deg g = 0$. Finalement, soit f dans $A[X] \setminus A$ irréductible dans $A[X]$. Alors il est primitif, sinon $f = \mathrm{cont}(f)pp(f)$ est une factorisation non triviale. On veut démontrer qu'il est irréductible dans $K[X]$. Si $f = f_1 f_2$ dans $K[X]$, alors $f = \mathrm{pp}(f) = \mathrm{pp}(f_1)\,\mathrm{pp}(f_2)$ est une factorisation dans $A[X]$. L'un des f_i est donc une unité de $A[X]$, et donc une unité de $K[X]$. □

Théorème 2.7. *Si A est un anneau factoriel, alors $A[X]$ est un anneau factoriel.*

Preuve. Soit $f \in A[X]$ non nul et non inversible. Montrons que l'on peut décomposer f en un produit d'irréductibles de $A[X]$. Déjà, dans $K[X]$, on peut écrire

$$\mathrm{pp}(f) = \prod_{i=1}^{r} f_i,$$

où les f_i sont des irréductibles de $K[X]$. En prenant la partie principale du produit ci-dessus, on obtient

$$\mathrm{pp}(f) = \prod_{i=1}^{r} \mathrm{pp}(f_i).$$

Chacun de ces $\mathrm{pp}(f_i)$, étant primitif et irréductible dans $K[X]$, est irréductible dans $A[X]$. L'anneau A étant factoriel, on peut aussi décomposer $\mathrm{cont}(f)$ en produit d'irréductibles de A, donc de $A[X]$. Cela montre qu'on peut décomposer f en un produit d'irréductibles de $A[X]$. Il reste à montrer l'unicité de cette écriture. Supposons

$$f = \prod_{i=1}^{r} p_i \prod_{i=1}^{s} f_i = \prod_{i=1}^{t} q_i \prod_{i=1}^{u} g_i$$

où les p_i et les q_i sont des irréductibles de A et où les f_i et les g_i sont des irréductibles de degré $\geqslant 1$ de $A[X]$ (donc primitifs). On en déduit

$$\mathrm{cont}(f) = \prod_{i=1}^{r} p_i = \prod_{i=1}^{t} q_i.$$

Ainsi, $r = t$ et il existe une permutation σ de S_r telle que pour tout i dans $\{1, \ldots, r\}$, p_i est associé à $q_{\sigma(i)}$. De même, on a

$$\mathrm{pp}(f) = \prod_{i=1}^{s} f_i = \prod_{i=1}^{u} g_i.$$

puisque les f_i et g_i sont primitifs. Voyant cette égalité dans $K[X]$, il vient que $s = u$ et qu'il existe une permutation τ dans S_s telle que pour tout i dans $\{1, \ldots, s\}$, f_i et $g_{\tau(i)}$ sont associés. □

Corollaire 2.8. *Soit A un anneau factoriel, alors $A[X_1, \ldots, X_n]$ est un anneau factoriel.*

Corollaire 2.9. *Soit A un anneau factoriel de corps des fractions K. Soient f et g deux éléments de $A[X]$, et h leur pgcd dans $A[X]$. Alors $h/\operatorname{cd}(h)$ est le pgcd unitaire de f et g dans $K[X]$.*

Preuve. Comme $h/\operatorname{cd}(h)$ divise f et g dans $K[X]$, il divise leur pgcd unitaire h^*. D'autre part, il existe un $f^* \in K[X]$ tel que $f = f^*h^*$, donc $\operatorname{pp}(h^*) \mid \operatorname{pp}(f) \mid f$ dans $A[X]$. De même, $\operatorname{pp}(h^*)$ divise g, donc $\operatorname{pp}(h^*)$ divise h ; on en déduit que les deux polynômes unitaires h^* et $h/\operatorname{cd}(h)$ ont même degrés. Ils sont donc égaux. □

Soit A un anneau factoriel. On suppose que l'on sait calculer le pgcd de deux éléments de A. On veut maintenant calculer le pgcd de deux polynômes f et g dans $A[X]$. On a

$$\operatorname{pgcd}(f,g) = \operatorname{pgcd}(\operatorname{cont}(f),\operatorname{cont}(g))\operatorname{pgcd}(\operatorname{pp}(f),\operatorname{pp}(g)).$$

Supposons donc que f et g sont primitifs. Pour calculer $h = \operatorname{pgcd}(f,g))$ dans $A[X]$, on peut calculer $d = \operatorname{pgcd}(f,g)$ dans $K[X]$; alors $h = \operatorname{pp}(d)$.

3. Le résultant de deux polynômes

Le résultant de deux polynômes non nuls à coefficients dans un corps K s'annule si et seulement si leur pgcd dans $K[X]$ est non constant, c'est-à-dire si ces deux polynômes ont des racines communes dans une clôture algébrique de K. Dans la pratique, il est plus simple et plus efficace de calculer le pgcd de ces polynômes.

D'un point de vue algorithmique, le résultant peut être utilisé pour éliminer des variables dans un système d'équations polynomiales à plusieurs variables

$$\begin{cases} P_1(X_1,\ldots,X_k) = 0 \\ \qquad\qquad \vdots \\ P_r(X_1,\ldots,X_k) = 0. \end{cases}$$

Par exemple, on peut l'utiliser pour calculer l'intersection de deux courbes ou deux surfaces algébriques. Si l'on veut faire de l'élimination sur un système d'équations polynomiales assez grand, la taille des polynômes intermédiaires devient vite trop grande, et il vaut mieux utiliser une autre méthode, par exemple les bases de Gröbner.

D'un point de vue théorique, l'utilisation du résultant, et des sous-résultants, donne des résultats sur la croissance des coefficients des polynômes intervenant dans l'algorithme d'Euclide naïf sur $\mathbb{Q}[X]$ (voir [1, Theorem 6.52 & 6.53]).

3.1. Polynômes à coefficients dans un corps.

Soit K un corps.

Lemme 3.1. *Soient f et g deux polynômes non nuls de $K[X]$. Alors* $\operatorname{pgcd}(f,g) \neq 1$ *si et seulement s'il existe s et t non nuls dans $K[X]$ tels que* $\deg(s) < \deg(g)$, $\deg(t) < \deg(f)$ *et $sf + tg = 0$.*

Preuve. Soit $h = \operatorname{pgcd}(f,g)$. Si $\deg(h) \geqslant 1$, alors $s = -g/h$ et $t = f/h$ conviennent. Réciproquement, si f et g sont premiers entre eux, et si $sf+tg = 0$, alors f divise $t \neq 0$, et donc $\deg(t) \geqslant \deg(f)$. □

On peut reformuler ce lemme dans le langage de l'algèbre linéaire. Pour tout entier naturel d, on pose

$$P_d = \{P \in K[X] \colon \deg(P) < d\}\,.$$

C'est un espace vectoriel sur K de dimension d. Soient n et m les degrés respectifs de f et g. On considère l'application K-linéaire

$$\begin{aligned} \varphi \colon P_m \times P_n &\longrightarrow P_{m+n} \\ (s,t) &\longmapsto sf + tg. \end{aligned}$$

Alors le lemme 3.1 se traduit de la façon suivante :

Théorème 3.2.

- $\operatorname{pgcd}(f,g) = 1$ *si et seulement si* φ *est un isomorphisme.*
- *Si* $\operatorname{pgcd}(f,g) = 1$ *et si* $n+m \geqslant 1$*, alors les coefficients de Bézout* s *et* t *calculés par l'algorithme d'Euclide étendu fournissent l'unique solution de* $\varphi(s,t) = 1$*.*

On va représenter φ par une matrice. On écrit pour cela

$$f = \sum_{j=0}^{n} f_j X^j \quad \text{et} \quad g = \sum_{j=0}^{m} g_j X^j,$$

où les f_j et les g_j appartiennent à K. Pour P_{m+n}, on choisit la base $X^{m+n-1}, \dots, 1$; pour $P_m \times P_n$, on prend $(X^{m-1}, 0), \dots, (1,0)$, $(0, X^{n-1}), \dots, (0,1)$. La matrice de φ pour ces bases est alors la matrice carrée de taille $m+n$

$$S = \begin{pmatrix} f_n & & & & g_m & & \\ f_{n-1} & f_n & & & & & \\ & & & & & \ddots & \\ \vdots & & \ddots & & & & g_m \\ & \vdots & & f_n & g_1 & & \\ f_0 & & & f_{n-1} & g_0 & & \\ & f_0 & & & & \ddots & \vdots \\ & & \ddots & \vdots & & & \\ & & & & & & \\ & & & f_0 & & & g_0 \end{pmatrix}$$

où les coefficients de f sont reproduits sur $m = \deg g$ colonnes tandis que ceux de g sont reproduits sur $n = \deg f$ colonnes. Si on pose

$$s = \sum_{j=0}^{m-1} s_j X^j, \quad t = \sum_{j=0}^{n-1} t_j X^j \quad \text{et} \quad sf + tg = \sum_{j=0}^{m+n-1} u_j X^j,$$

où les s_j, t_j et u_j sont dans K, alors

$$S \begin{pmatrix} s_{m-1} \\ \vdots \\ s_0 \\ t_{n-1} \\ \vdots \\ t_0 \end{pmatrix} = \begin{pmatrix} u_{n+m-1} \\ \vdots \\ \\ \\ \vdots \\ u_0 \end{pmatrix}.$$

Corollaire 3.3.

- $\operatorname{pgcd}(f,g) = 1$ *si et seulement si* $\det S \neq 0$.
- *Si* $\operatorname{pgcd}(f,g) = 1$*, si* $m+n \geqslant 1$ *et si* $s_0, \ldots, s_{m-1}, t_0, \ldots, t_{n-1}$ *satisfont*

$$S \begin{pmatrix} s_{m-1} \\ \vdots \\ s_0 \\ t_{n-1} \\ \vdots \\ t_0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

alors $s = \sum_{j=0}^{m-1} s_j X^j$ *et* $t = \sum_{j=0}^{n-1} t_j X^j$ *sont les coefficients de Bézout calculés par l'algorithme d'Euclide étendu.*

La matrice S est appelée *matrice de Sylvester* de f et g et est notée $\operatorname{Sylv}(f,g)$. Son déterminant est appelé résultant de f et g et est noté $\operatorname{Res}_X(f,g)$ ou $\operatorname{Res}(f,g)$.

3.2. **Polynômes à coefficients dans un anneau factoriel.** Les notions de matrice de Sylvester et de résultant se généralisent pour des polynômes de $A[X]$, où A est un anneau commutatif quelconque.

Définition 3.4. Soit A un anneau commutatif, et soient f et g deux polynômes de $A[X]$. Alors la matrice S ci-dessus est appelée matrice de Sylvester de f et g et notée $\operatorname{Sylv}(f,g)$. Son déterminant est appelé resultant de f et g et noté $\operatorname{Res}_X(f,g) = \operatorname{Res}(f,g)$.

Si $\deg f = \deg g = 0$, alors $\operatorname{Sylv}(f,g)$ est la matrice vide de déterminant $\operatorname{Res}(f,g) = 1$. De plus, on note $\operatorname{Res}(f,0) = \operatorname{Res}(0,f) = 0$ si f est nul ou de degré $\geqslant 1$, et $\operatorname{Res}(f,0) = \operatorname{Res}(0,f) = 1$ si f est de degré 0.

Remarque 3.5. Dans certains ouvrages, on appelle matrice de Sylvester la transposée de S.

Théorème 3.6. *Soit A un anneau factoriel. Soient f, g deux polynômes non nuls de $A[X]$, alors* $\operatorname{pgcd}(f,g) \notin A$ *si et seulement si* $\operatorname{Res}(f,g) = 0$.

Preuve. Soit K le corps des fractions de A. Alors $\operatorname{Res}(f,g) = 0$ si et seulement si $\operatorname{pgcd}_{K[X]}(f,g) \neq 1$, si et seulement si $\operatorname{pgcd}_{A[X]}(f,g) \notin A$ (ils ont la même partie principale d'après le corollaire 2.9). □

Proposition 3.7. *Soit A un anneau intègre, et soient f et g deux polynômes non nuls de $A[X]$ tels que $\deg(f)+\deg(g) \geqslant 1$. Alors il existe s et t non nuls dans $A[X]$ tels que $sf+tg = \mathrm{Res}(f,g)$, $\deg(s) < \deg(g)$ et $\deg(t) < \deg(f)$.*

Preuve. Soit K le corps des fractions de A. Si $\mathrm{Res}(f,g) = 0$, alors on sait grâce au corollaire 3.3 et au lemme 3.1 qu'il existe s et t convenables dans $K[X]$. On conclut en multipliant par un dénominateur commun des coefficients.

Si le résultant est non nul, alors f et g sont premiers entre eux dans $K[X]$ et il existe u et v dans $K[X]$ tels que $\deg(u) < \deg(g)$, $\deg(v) < \deg(f)$ et $sf+tg = 1$. Les coefficients de u et v sont la solution unique d'un système de Cramer de matrice $S = \mathrm{Sylv}(f,g)$. Soit $E = {}^t(0,\dots,0,1)$, de taille $m+n$, où $m = \deg(g)$ et $n = \deg(f)$. Chaque coefficient de u et v est le quotient du déterminant d'une sous matrice de taille $m+n$ de la matrice concaténée $(S|E)$ de S et E par $r = \det(S)$. Ainsi, $s = ur$ et $t = vr$ sont dans $A[X]$. □

4. Résultant et racines

On revient maintenant à $K[X]$, où K est un corps commutatif. Du corollaire 3.3, on déduit :

Théorème 4.1. *Si deux polynômes f et g de $K[X]$ admettent une racine commune dans K, alors $\mathrm{Res}(f,g) = 0$. Cette condition est suffisante si l'un des deux polynômes est scindé dans K, en particulier si K est algébriquement clos.*

Comme le résultant est fonction des coefficients des polynômes f et g, on peut aussi l'exprimer en fonction de leurs racines. Rappelons quelques résultats sur les relations entre racines et coefficients. Soient

$$f = \sum_{j=0}^{n} f_j X^j \quad \text{et} \quad g = \sum_{j=0}^{m} g_j X^j$$

deux polynômes de $K[X]$ de degrés respectifs n et m. On note respectivement $a_1,\dots,a_n$ et $b_1,\dots,b_m$ les racines de f et g.

Définition 4.2. Pour k dans $\{1,\dots,n\}$, le k-ème polynôme symétrique élémentaire σ_k des racines de f est défini par

$$\sigma_k = \sum_{i_1<\dots<i_k} a_{i_1}\dots a_{i_k}.$$

Proposition 4.3. *Pour k dans $\{1,\dots,n\}$, on a l'égalité*

$$\sigma_k = (-1)^k \frac{f_{n-k}}{f_n}.$$

Rappelons aussi les formules de Newton, même si l'on ne s'en servira pas ici :

Théorème 4.4. *Pour tout entier naturel k, on note $S_k = \sum_{i=1}^{n} a_i^k$. Alors pour tout k, on a*

$$\sum_{j=1}^{k} (-1)^{j-1} \sigma_{k-j} S_j = k\sigma_k,$$

où on définit $\sigma_k := 0$ pour $k > n$ et $\sigma_0 := 1$.

Venons en maintenant à une relation liant les racines de f et de g avec $\mathrm{Res}(f, g)$. Pour cela, on utilise le lemme suivant :

Lemme 4.5. *Soient $\Sigma_1, \ldots, \Sigma_n$, et $\Sigma'_1, \ldots, \Sigma'_m$ les polynômes symétriques élémentaires associés respectivement aux indéterminées $X_1, \ldots, X_n$ et $Y_1, \ldots, Y_m$. Soient U et V les polynômes de $K[X_1, \ldots, X_n, Y_1, \ldots, Y_m][X]$ donnés par*

$$U = (X - X_1) \ldots (X - X_n) = X^n + \sum_{k=1}^{n} (-1)^k \Sigma_k X^{n-k},$$

$$V = (X - Y_1) \ldots (X - Y_m) = X^m + \sum_{k=1}^{m} (-1)^k \Sigma'_k X^{m-k}.$$

Alors, si $I = \{1, \ldots n\} \times \{1, \ldots, m\}$, on a

$$\mathrm{Res}(U, V) = \prod_{(i,j) \in I} (X_i - Y_j).$$

Preuve. Soit $R = \mathrm{Res}(U, V)$; c'est un polynôme de $K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$. Dans $K[X_1, \ldots, X_n, Y_1, \ldots, Y_m][X]$, les deux polynômes U et V sont scindés. Si on considère R comme un élément de

$$K[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n, Y_1, \ldots, Y_m][X_i],$$

on voit que R s'annule en $X_i = Y_j$. Donc, pour tout (i, j) dans I, $X_i - Y_j$ divise R. C'est donc qu'il existe Q dans $K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ tel que

$$R = Q \prod_{(i,j) \in I} (X_i - Y_j). \tag{1}$$

On considère la matrice de Sylvester

$$\mathrm{Sylv}(U,V) = \begin{pmatrix} 1 & & & & & 1 & & \\ -\Sigma_1 & 1 & & & & -\Sigma'_1 & & \\ & & & & & & \ddots & \\ \vdots & & \ddots & & & & & 1 \\ & \vdots & & 1 & (-1)^{n-1}\Sigma'_{m-1} & & & \\ (-1)^n\Sigma_n & & & -\Sigma_1 & (-1)^m\Sigma'_m & & & \\ & (-1)^n\Sigma_n & & & & & \ddots & \vdots \\ & & \ddots & \vdots & & & & \\ & & & (-1)^n\Sigma_n & & & & (-1)^m\Sigma'_m \end{pmatrix}$$

et on développe son déterminant comme somme sur les permutations de S_{m+n} de produits de coefficients. On constate qu'un seul terme est divisible par

$$(Y_1 \dots Y_m)^n;$$

ce terme provient de la diagonale de la matrice de Sylvester, laquelle donne

$$(1)^m \times ((-1)^m \Sigma'_m)^n = (-1)^{mn}(Y_1 \dots Y_m)^n.$$

En comparant avec (1), on en déduit que $Q = 1$. □

Théorème 4.6. *On a l'égalité*

$$\mathrm{Res}(f,g) = f_n^m g_m^n \prod_{(i,j)\in I} (a_i - b_j).$$

Preuve. On a

$$\mathrm{Res}(f,g) = \mathrm{Res}\left(f_n \frac{f}{f_n}, g_m \frac{g}{g}_m\right) = f_n^m g_m^n \,\mathrm{Res}\left(\frac{f}{f_n}, \frac{g}{g}_m\right) = f_n^m g_m^n \prod_{(i,j)\in I} (a_i - b_j),$$

d'après le lemme 4.5. □

Corollaire 4.7.

$$\mathrm{Res}(f,g) = f_n^m \prod_{i=1}^{n} g(a_i) = (-1)^{mn} g_m^n \prod_{j=1}^{m} f(b_j).$$

Preuve. La première égalité suit de $g(X) = g_m \prod_{j=1}^m (X - b_j)$, la deuxième de $f(X) = (-1)^n f_n \prod_{i=1}^n (a_i - X)$. □

5. Un algorithme d'Euclide pour calculer le résultant

Soit A un anneau intègre. Le calcul du résultant $\operatorname{Res}(f,g)$ par un pivot de Gauss sur $\operatorname{Sylv}(f,g)$, effectué sur $K = \operatorname{Frac} A$, a trois défauts : sa complexité algébrique est cubique en $O(m+n)^3$, il fait apparaître des dénominateurs, et la taille des coefficients intermédiaires peut exploser même si le résultat et les entrées sont petites.

Lemme 5.1. *Soient $f, g \in K[X]$ et $f = qg + r$ la division euclidienne. On a*

$$\operatorname{Res}(f,g) = (-1)^{\deg f \deg g} \operatorname{cd}(g)^{\deg f - \deg r} \operatorname{Res}(g,r)$$

Preuve. On applique successivement les deux égalités du corollaire 4.7, en remarquant que $f = qg + r$ implique $f(b_j) = r(b_j)$ pour tout j :

$$\operatorname{Res}(f,g) = (-1)^{mn} g_m^n \prod_{j=1}^{m} f(b_j) = (-1)^{mn} g_m^n \prod_{j=1}^{m} r(b_j) = (-1)^{mn} g_m^n \frac{\operatorname{Res}(g,r)}{g_m^{\deg r}}.$$

□

Ce lemme produit un algorithme à la Euclide, quadratique comme son prototype, pour le calcul du résultant :

Algorithme 5.2
Entrée : Deux polynômes non nuls $f, g \in A[X]$.
Sortie : $\operatorname{Res}_X(f,g)$.

(1) $c \leftarrow 1$.
(2) Tant que $\deg g > 0$
(3) Effectuer la division Euclidienne $f = qg + r$ dans $K[X]$.
(4) Remplacer $c \leftarrow (-1)^{\deg f \deg g} \operatorname{cd}(g)^{\deg f - \deg r} \times c$.
(5) Remplacer $(f,g) \leftarrow (g,r)$.
(6) Retourner 0 si $g = 0$, et $c \cdot \operatorname{cd}(g)^{\deg f}$ sinon.

L'algorithme suit du lemme, la dernière étape étant justifiée par $\operatorname{Res}(f,g) = \operatorname{cd}(g)^{\deg f}$ si $\deg g = 0$.

Le deuxième défaut — passer dans $K[X]$ au lieu de rester dans $A[X]$— peut être lui aussi supprimé en remarquant que la division euclidienne

$$\operatorname{cd}(g)^{\deg f - \deg g} f = qg + r \quad \text{(pseudo-division)}$$

fournit en fait $q, r \in A[X]$; il suffit ensuite de modifier l'algorithme ci-dessus en remplaçant les divisions euclidienne par des pseudo-divisions et en utilisant $\operatorname{Res}(\lambda f, g) = \lambda^{\deg g} \operatorname{Res}(f,g)$ pour corriger le résultant à chaque étape.

Pour finir, on peut aussi éliminer le dernier défaut — explosion des coefficients — par une méthode modulaire, si l'anneau A est raisonnable, par exemple $A = \mathbb{Z}$. Plus généralement, il faut connaître suffisamment d'idéaux maximaux $\mathfrak{m}$ tels que $A/\mathfrak{m}$ soit *fini*. On utilise le lemme suivant :

Lemme 5.3. *Soit A un anneau intègre, I un idéal de A ; pour a dans A, on note $\overline{a}$ l'image de a dans A/I ; on utilise la même notation pour la projection de $A[X] \to$*

$(A/I)[X]$, *coefficient par coefficient. Soient* f *et* g *deux éléments non nuls de* $A[X]$ *tels que* $\overline{\mathrm{cd}(f)} \neq 0$, $\overline{\mathrm{cd}(g)} \neq 0$. *Alors* $\overline{\mathrm{Res}(f,g)} = \mathrm{Res}(\bar{f},\bar{g})$.

Preuve. Il suffit de remarquer que $\bar{f}, \bar{g}$ ont mêmes degrés que f, g. Le déterminant d'une matrice de Sylvester $\mathrm{Sylv}(f,g)$ s'exprime comme polynôme en les coefficients de f, g ; on conclut en remarquant que la réduction $A \to A/I$ est un morphisme d'anneau. □

On choisit donc $\mathfrak{m}$ maximal tel que $\mathrm{cd}(f), \mathrm{cd}(g) \notin \mathfrak{m}$ et on calcule $\mathrm{Res}(\bar{f},\bar{g})$ par un algorithme d'Euclide sur $(A/\mathfrak{m})[X]$: comme $A/\mathfrak{m}$ est un corps fini, il n'y a pas explosion des coefficients ; de plus on n'a pas besoin d'introduire de pseudo-division puisque travailler sur un corps fini n'introduit pas de dénominateur !

On en déduit $\mathrm{Res}(f,g) \pmod{\mathfrak{m}}$ pour suffisamment de $\mathfrak{m}$ pour pouvoir appliquer le lemme chinois. Par exemple, si $A = \mathbb{Z}$, on peut calculer $\mathrm{Res}(f,g)$ modulo un produit de premiers $N = p_1 \dots p_\ell$, majorer

$$|\mathrm{Res}(f,g)| \leqslant B := \|f\|_2^{\deg g} \, \|g\|_2^{\deg f}$$

par la borne de Hadamard et il suffit que $N > 2B$ pour déterminer $\mathrm{Res}(f,g) \in \mathbb{Z}$. (Exercice : justifier ce point ; pourquoi $N > 2B$ et pas $N > B$?)

Si $A = k[Y]$, on peut de même borner

$$\deg_Y \mathrm{Res}_X(f,g) \leqslant B := \max(\deg_X f \cdot \deg_Y g,\ \deg_X g \cdot \deg_Y f),$$

et calculer $\mathrm{Res}(f,g) \mod (Y-a)$ pour $B+1$ éléments $a \in k$ distincts ; on reconstruit alors $\mathrm{Res}(f,g) \in k[Y]$ par interpolation de Lagrange (qui est une version du lemme chinois).

6. Le discriminant

Dans ce paragraphe, A est un anneau factoriel et $f = \sum_{i=0}^{n} f_i X^i$ est un polynôme de degré $n \geqslant 1$ de $A[X]$.

Définition 6.1. On appelle discriminant de f l'élément $\Delta(f)$ de A

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}} \frac{\mathrm{Res}(f,f')}{f_n}.$$

Remarque 6.2. Si la caractéristique de A ne divise pas n, alors f_n divise $\mathrm{Res}(f,f')$, puisqu'il divise le coefficient dominant de f et de f', on peut donc le mettre en facteur dans la première ligne, dans l'expression du déterminant de $\mathrm{Sylv}(f,f')$. Si la caractéristique de A divise n, alors $\Delta(f)$ peut ne pas se trouver dans A, mais dans le corps des fractions de A.

Exercice. Vérifier les égalités suivantes.

$$\Delta(aX+b) = 1 \qquad (a \neq 0)$$
$$\Delta(aX^2+bX+c) = b^2 - 4ac \qquad (a \neq 0)$$
$$\Delta(X^3+pX+q) = -(4p^3+27q^2)$$

Proposition 6.3. *On suppose que* $\operatorname{Frac} A$ *est un corps parfait, c'est-à-dire de caractéristique* 0 *ou de caractéristique* $p > 0$*, tel que* $a \mapsto a^p$ *soit surjective. Un polynôme* $f \in A[X]$ *admet un facteur carré de degré* $\geqslant 1$ *si et seulement si* $\Delta(f) = 0$*.*

Preuve. Si $f = qg^2$, alors $f' = 2qgg' + q'g^2$, donc g divise $\operatorname{pgcd}(f, f')$. Pour la réciproque, on décompose f en facteurs irréductibles.

$$f = \prod_{i=1}^{r} p_i^{e_i}$$

où, pour tout i, $e_i \geqslant 1$ et p_i est un polynôme irréductible de $A[X]$ de degré $\geqslant 1$. Alors

$$f' = \sum_{i=1}^{r} e_i p_i' p_i^{e_i - 1} \prod_{j \neq i} p_j^{e_j}.$$

Soient $I = \{i \in \{1, \dots, n\} \colon \operatorname{car} A \nmid e_i\}$ et $I' = \{i \in \{1, \dots, n\} : \operatorname{car} A \mid e_i\}$; alors

$$\prod_{i \in I} p_i^{e_i - 1} \prod_{i \in I'} p_i^{e_i} = \operatorname{pgcd}(f, f').$$

On a utilisé que $\operatorname{pgcd}(p_i, p_i') = 1$ pour tout i, qui suit de $\deg p_i' < \deg p_i$ et de $p_i' \neq 0$ (qui suit de l'hypothèse sur $\operatorname{Frac} A$). Ainsi, si le degré du pgcd de f et g est supérieur ou égal à 1, il existe i tel que $e_i \geqslant 2$. □

Remarque 6.4. Dans cette preuve, le calcul effectué pour la réciproque permet aussi de montrer le sens direct.

Proposition 6.5. *Soit* K *le corps des fractions de* A*, et soient* a_i *(*$i = 1, \dots, n$*) les racines de* f *dans une clôture algébrique de* K*. Si* $\operatorname{car}(K)$ *ne divise pas* n*, on a*

$$\Delta(f) = f_n^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (a_i - a_j)^2.$$

Preuve. On utilise le fait que

$$\operatorname{Res}(f, f') = f_n^{n-1} \prod_{i=1}^{n} f'(a_i).$$

Or, si $f = f_n(X - a_1) \dots (X - a_n)$, on a

$$f'(X) = f_n \sum_{i=1}^{n} \prod_{j \neq i} (X - a_j),$$

soit $f'(a_i) = f_n \prod_{j \neq i} (a_i - a_j)$. Donc

$$\begin{aligned} \operatorname{Res}(f, f') &= f_n^{2n-1} \prod_{i=1}^{n} \prod_{j \neq i} (a_i - a_j) \\ &= (-1)^{\frac{n(n-1)}{2}} f_n^{2n-1} \prod_{1 \leqslant i < j \leqslant n} (a_i - a_j)^2. \end{aligned}$$

Dans ce calcul, on utilise que le degré de f' est $n-1$, puisque $\mathrm{car}(K) \nmid n$. □

7. Élimination

7.1. **Intersection de deux courbes planes.** Soit K un corps algébriquement clos, et soient f et g deux polynômes de $K[X,Y]$. On veut pouvoir calculer l'intersection des courbes

$$V(f) = \left\{(a,b) \in K^2 \colon f(a,b) = 0\right\},$$
$$V(g) = \left\{(a,b) \in K^2 \colon g(a,b) = 0\right\}.$$

On peut pour cela éliminer la variable Y en considérant le résultant $r = \mathrm{Res}_Y(f,g) \in K[X]$. Si $f(a,b) = g(a,b) = 0$, alors les polynômes $f(a,Y)$ et $g(a,Y)$ de $K[X]$ ont une racine commune b. Donc $\mathrm{Res}_Y(f(a,Y), g(a,Y)) = 0$, ce qui signifie que $\mathrm{Res}_Y(\bar{f}, \bar{g}) = 0$, où $\bar{f}$ et $\bar{g}$ sont les réductions de f et g modulo $X - a$. Or si les coefficients dominants de f et de g ne s'annulent pas en a, on a d'après le lemme 5.3

$$\mathrm{Res}_Y(\bar{f}, \bar{g}) = \overline{\mathrm{Res}_Y(f,g)}.$$

On trouve donc a en calculant les racines de $\mathrm{Res}_Y(f,g) \in K[X]$. Supposer que les coefficients dominants de f et g ne s'annulent pas en a n'est pas une restriction grave : elle nous oblige simplement à considérer séparément, dans un deuxième temps, les a qui sont racines de $\mathrm{cd}_X(f)$ ou $\mathrm{cd}_X(g)$.

En fait, le lemme suivant montre que pour avoir l'équivalence

$$\mathrm{Res}_Y(\bar{f}, \bar{g}) = 0 \Leftrightarrow \overline{\mathrm{Res}_Y(f,g)} = 0,$$

il suffit que l'un des deux coefficients dominants de f ou de g ne s'annule pas en a et on se contentera donc des a qui sont racines de $\mathrm{pgcd}_{K[Y]}(\mathrm{cd}_X(f), \mathrm{cd}_X(g))$:

Lemme 7.1. *Soit A un anneau intègre. Soient f et g deux éléments non nuls de $A[X]$. Soit I un idéal de A. Pour a dans A, on note $\overline{a}$ l'image de a dans A/I. On suppose que $\overline{\mathrm{cd}(f)} \neq 0$. Soit $r = \mathrm{Res}(f,g)$. Alors $\overline{r} = 0$ si et seulement si $\mathrm{Res}(\bar{f}, \bar{g}) = 0$. Par conséquent, si A/I est un anneau factoriel, $\overline{r} = 0$ si et seulement si $\deg(\mathrm{pgcd}(\bar{f}, \bar{g})) > 0$.*

Preuve. On pose $f = \sum_{j=0}^{n} f_j X^j$ et $g = \sum_{j=0}^{m} g_j X^j$, de degrés respectifs n et m. Si $\deg(f) = 0$, alors $\mathrm{Sylv}(f,g) = fI_m$ et $\mathrm{Sylv}(\bar{f}, \bar{g}) = \bar{f} I_m$. Donc $\overline{r}$ et $\mathrm{Res}(\bar{f}, \bar{g})$ sont non nuls.

On suppose maintenant que $\deg(f) \geqslant 1$. Si $\bar{g} = 0$, alors $\mathrm{Res}(\bar{f}, \bar{g}) = 0$. De plus, les n dernières colonnes de $\mathrm{Sylv}(f,g)$ (celles qui contiennent les g_i) s'annulent modulo I,

donc $\overline{r} = 0$. Si $\bar{g} \neq 0$, soit i le plus petit indice tel que $\bar{g}_{m-i} \neq 0$. Alors

$$\overline{\mathrm{Sylv}(f,g)} = \begin{pmatrix} \bar{f}_n & & & & 0 & & \\ \bar{f}_{n-1} & \bar{f}_n & & & 0 & & \\ & & & & \bar{g}_{m-i} & \ddots & \\ \vdots & & \ddots & & & & 0 \\ & \vdots & & \bar{f}_n & \bar{g}_1 & & \bar{g}_{m-i} \\ \bar{f}_0 & & & \bar{f}_{n-1} & \bar{g}_0 & & \\ & \bar{f}_0 & & & & \ddots & \vdots \\ & & \ddots & \vdots & & & \\ & & & & & & \\ & & & \bar{f}_0 & & & \bar{g}_0 \end{pmatrix},$$

c'est-à-dire de la forme

$$\overline{\mathrm{Sylv}(f,g)} = \begin{pmatrix} T & 0 \\ U & V \end{pmatrix}$$

où T est carrée de taille i et triangulaire inférieure avec des $\bar{f}_n$ sur la diagonale, et V est carrée de taille $m-i$.

$$V = \begin{pmatrix} \bar{f}_n & & & \bar{g}_{m-i} & & \\ & \ddots & & & & \\ & & \bar{f}_n & \bar{g}_1 & & \\ & & \bar{f}_{n-1} & \bar{g}_0 & \bar{g}_{m-i} & \\ & & & & \ddots & \\ \bar{f}_0 & & \vdots & & \vdots & \\ & \ddots & & & & \\ & & \bar{f}_0 & & \bar{g}_0 & \end{pmatrix} = \mathrm{Sylv}(\bar{f}, \bar{g}).$$

On en déduit que $\overline{r} = \bar{f}_n^i \,\mathrm{Res}(\bar{f}, \bar{g})$. □

Remarque 7.2. La conclusion est fausse en général si $\mathrm{cd}(\bar{f}) = \mathrm{cd}(\bar{g}) = 0$. Par exemple, dans $\mathbb{Z}[X]$, si $f = 2X^3 + X$ et $g = 2X + 1$, et si on réduit modulo 2, alors $\mathrm{Res}(f,g) \equiv 0 \mod 2$ alors que $\mathrm{Res}(\bar{f}, \bar{g}) = \mathrm{Res}(X, 1) = 1$.

Autre exemple, dans $\mathbb{Q}[X,Y]$: soient $f = XY + 1$ et $g = XY^3 + Y + 1$. Alors $\mathrm{Res}(f,g) \equiv 0 \pmod X$ alors que dans $\mathbb{Q}[X,Y]/(X)$, on a $\mathrm{Res}(\bar{f}, \bar{g}) = \mathrm{Res}(1, y+1) = 1$.

Pour trouver l'intersection des courbes $V(f)$ et $V(g)$, on peut éliminer Y en considérant $r = \mathrm{Res}_Y(f,g) \in K[X]$. Soit $\pi : K^2 \to K$, $\pi(x,y) = y$ la projection sur l'axe des Y et $Z = \pi(V(f) \cap V(g))$. Si $a \in K$ et si $\mathrm{cd}_Y(f)$ ou $\mathrm{cd}_Y(g)$ ne s'annule pas en $X = a$,

alors

$$\begin{aligned} a \in Z &\Leftrightarrow \exists b \in K \colon f(a,b) = g(a,b) = 0 \\ &\Leftrightarrow \operatorname{pgcd}(f(a,Y), g(a,Y)) \neq 1 \\ &\Leftrightarrow r(a) = \operatorname{Res}_Y(f,g)(a) = 0. \end{aligned}$$

On a donc $r(a) = 0$ si et seulement si $a \in Z$.

7.2. **Intersection de deux hypersurfaces.** Soit K un corps algébriquement clos. Soient f et g dans $K[X_1, \ldots, X_n]$. Soient

$$\begin{aligned} V(f) &= \{(c_1, \ldots, c_n) \in K^n \colon f(c_1, \ldots, c_n) = 0\}, \\ V(g) &= \{(c_1, \ldots, c_n) \in K^n \colon g(c_1, \ldots, c_n) = 0\}. \end{aligned}$$

Soit

$$\begin{aligned} \pi \colon K^n &\longrightarrow K^{n-1} \\ (c_1, \ldots, c_n) &\longmapsto (c_2, \ldots, c_n) \end{aligned}$$

et soit $Z = \pi(V(f) \cap V(g))$. On suppose que $\operatorname{cd}_{X_1}(f)$ ou $\operatorname{cd}_{X_1}(g)$ ne s'annule pas en $(c_2, \ldots, c_n)$. Alors

$$\begin{aligned} (c_2, \ldots, c_n) \in Z &\Leftrightarrow \exists c_1 \in K \colon f(c_1, \ldots, c_n) = g(c_1, \ldots, c_n) = 0 \\ &\Leftrightarrow \operatorname{Res}_{X_1}(c_2, \ldots, c_n) = 0. \end{aligned}$$

Références

[1] J. von zur Gathen & J. Gerhard, *Modern computer algebra*, Cambridge University Press, New York, 1999.