

Une version vectorielle des bases standard(Octobre 2017)

PAR PATRICK TELLER

Version révisée Octobre 2017

L'Algèbre commutative a développé les bases de Grobner qui permettent d'étendre la notion de division polynomiale aux anneaux de polynômes en plusieurs indéterminées, de sorte que soit défini le reste d'un polynôme modulo un idéal; R. Thomas a introduit une interprétation géométrique du cas des binômes dans l'étude des applications à la programmation linéaire en entiers [1] mais il nous semble que la piste ouverte à cette occasion mérite d'être explorée plus avant.

L'idée de base consiste à représenter les binômes sans facteurs communs par des vecteurs, comme dans l'exemple suivant:

$$x_1^{n_1} x_2^{n_2} x_4^{n_4} - x_3^{n_3} x_5^{n_5} \text{ sera représenté par le vecteur } \begin{pmatrix} n_1 \\ n_2 \\ -n_3 \\ n_4 \\ -n_5 \end{pmatrix}.$$

Comme les exposants des x_i sont nécessairement positifs il n'y a aucune ambiguïté.

Reste à mettre en place les outils nécessaires à la réduction d'un vecteur par un autre (l'analogie de la division) et la réduction d'un vecteur par (modulo) une famille finie.

Dans tout ce qui suit « combinaison linéaire » s'entendra comme combinaison linéaire à coefficients dans \mathbb{Z} ; de même on utilisera indistinctement les expressions p-uplet et vecteur pour des éléments de \mathbb{Z}^p .

1. Les outils (inspirés des bases de Grobner)

Nous désignerons par \preceq la relation d'ordre (partiel) sur \mathbb{N}^p définie comme suit $U = \begin{pmatrix} u_1 \\ \dots \\ u_p \end{pmatrix} \preceq V = \begin{pmatrix} v_1 \\ \dots \\ v_p \end{pmatrix} \iff \forall i \in \{1, \dots, p\}, u_i \leq v_i$, on dira alors que U précède V; lorsque 0 précède U on dira que U est positif.

On désignera par α l'ordre lexicographique qui, lui, est un ordre total; lorsque $\begin{pmatrix} 0 \\ \cdot \\ 0 \end{pmatrix} \alpha \begin{pmatrix} v_1 \\ \dots \\ v_p \end{pmatrix}$ on dira que $\begin{pmatrix} v_1 \\ \dots \\ v_p \end{pmatrix}$ est lex-positif, de même on dira lex-strictement-positif pour lex-positif et non nul.

Définition 1. Soit un p-uplet $U = \begin{pmatrix} u_1 \\ \dots \\ u_p \end{pmatrix}$ on notera, pour chaque i , $u_i^+ = \max\{u_i, 0\}$ et $u_i^- = \max\{0, -u_i\}$, $U^+ = \begin{pmatrix} u_1^+ \\ \dots \\ u_p^+ \end{pmatrix}$ et $U^- = \begin{pmatrix} u_1^- \\ \dots \\ u_p^- \end{pmatrix}$, d'où $U = U^+ - U^-$; lorsque $U \neq 0$ on notera $s(U) = \min\{i \in \llbracket 1, \dots, p \rrbracket, u_i \neq 0\}$ et $U^* = U$ lorsque $u_{s(U)} > 0$ et $U^* = -U$ lorsque $u_{s(U)} < 0$; si U est un p-uplet non nul U^* sera donc lex-strictement-positif.

On appellera support de U l'ensemble $\text{supp}(U) = \{i, u_i \neq 0\}$ et de même on pourra s'intéresser à $\text{supp}(U^+)$ et $\text{supp}(U^-)$.

Par ailleurs on remarquera que si U est non nul alors U^* est nécessairement lex-strictement positif.

Définition 2. Réduction d'un p uplet U par un p uplet V lex-strictement positif.

Soit U et V deux p uplets tels que $V^+ \preceq U^{*+}$, soit $\beta = \max \{k \in \mathbb{N}, 0 \preceq U^{*+} - kV^+\}$, d'où on posera $U = \varepsilon \beta V + W$ (où $\varepsilon = 1$ si $U^* = U$, $\varepsilon = -1$ si $U^* = -U$). on remarquera (proposition 3) que V^+ ne précède plus ni W^+ , ni W^- .

W sera appelé le reste (ou la réduction) de U modulo (par) V .

Dans le cas $U = 0V + W$ on dira que U est irréductible par V .

Proposition 3.

Soit la réduction de U par V $U = \gamma V + W$ alors V^+ ne précède ni W^+ , ni W^-

Démonstration.

Comme $\beta = \max \{k \in \mathbb{N}, 0 \preceq U^{*+} - kV^+\}$ l'une au moins des coordonnées de W qui appartiennent au support de V^+ est nulle, donc V^+ ne peut précéder ni W^+ ni W^- . \square

Exemple 4.

$$U = \begin{pmatrix} 4 \\ 3 \\ -3 \\ -2 \end{pmatrix}, V = \begin{pmatrix} 1 \\ 3 \\ -1 \\ -4 \end{pmatrix}, U = 1V + W = \begin{pmatrix} 3 \\ 0 \\ -2 \\ 2 \end{pmatrix}, \text{ donc } U \xrightarrow{V} \begin{pmatrix} 3 \\ 0 \\ -2 \\ 2 \end{pmatrix}$$

$$U = \begin{pmatrix} -4 \\ -3 \\ 3 \\ 2 \end{pmatrix}, V = \begin{pmatrix} 1 \\ 3 \\ -1 \\ -4 \end{pmatrix}, U = (-1)V + W = \begin{pmatrix} -3 \\ 0 \\ 2 \\ -2 \end{pmatrix}, \text{ donc } U \xrightarrow{V} \begin{pmatrix} -3 \\ 0 \\ 2 \\ -2 \end{pmatrix}$$

$$U = \begin{pmatrix} 0 \\ -3 \\ 3 \\ 2 \end{pmatrix}, V = \begin{pmatrix} 1 \\ 3 \\ -1 \\ -4 \end{pmatrix}, U^* = \begin{pmatrix} 0 \\ 3 \\ -3 \\ -2 \end{pmatrix} \text{ n'est pas précédé par } V \text{ donc } U \xrightarrow{V} U$$

Proposition 5. Le processus de réduction et les premières coordonnées

Démonstration.

1) Soit $U = \begin{pmatrix} a \\ \dots \\ \dots \\ \dots \end{pmatrix}$, où $a > 0$; il ne peut être réduit que par un vecteur lex-strictement positif $V = \begin{pmatrix} b \\ \dots \\ \dots \\ \dots \end{pmatrix}$, où $0 \leq b \leq a$ et alors $U \xrightarrow{V} \begin{pmatrix} c \\ \dots \\ \dots \\ \dots \end{pmatrix}$, où $0 \leq c \leq a$.

2) Soit $U = \begin{pmatrix} 0 \\ a \\ \dots \\ \dots \end{pmatrix}$, où $a > 0$; il ne peut être réduit que par un vecteur lex-strictement positif $V = \begin{pmatrix} 0 \\ b \\ \dots \\ \dots \end{pmatrix}$, où $0 \leq b \leq a$ et alors $U \xrightarrow{V} \begin{pmatrix} 0 \\ c \\ \dots \\ \dots \end{pmatrix}$, où $0 \leq c \leq a$.

3) Soit $U = \begin{pmatrix} 0 \\ a \\ \dots \\ \dots \end{pmatrix}$, où $a < 0$; alors $U^* = \begin{pmatrix} 0 \\ -a \\ \dots \\ \dots \end{pmatrix}$ il ne peut être réduit que par un vecteur lex-strictement positif $V = \begin{pmatrix} 0 \\ b \\ \dots \\ \dots \end{pmatrix}$, où $0 \leq b \leq -a$ et alors $U \xrightarrow{V} \begin{pmatrix} 0 \\ c \\ \dots \\ \dots \end{pmatrix}$. \square

Proposition 6.

Le reste d'un vecteur positif modulo un vecteur lex-strictement positif est positif

Démonstration.

Soit $U = \begin{pmatrix} u_1 \\ \dots \\ u_p \end{pmatrix} \succcurlyeq 0$ et $V = \begin{pmatrix} v_1 \\ \dots \\ v_p \end{pmatrix}$, lex - strictement positif; si U n'est pas irréductible alors $\forall i, v_i > 0, u_i \geq v_i$ et le reste de U par V sera $U - \min\{u_i/v_i, v_i > 0\}V$, donc à coordonnées positives. \square

Définition 7. Réduction d'un p -uplet U par un ensemble de p -uplets lex-strictement positifs S

Soit le $n+m$ -uplet U et un ensemble de p -uplets $S = \{V_i, i \in I\}$ on dira que U est réduit à W modulo S lorsqu'il existe un ensemble d'indices (i_1, \dots, i_q) à valeurs dans I tel que $U \xrightarrow{V_{i_1}} \xrightarrow{V_{i_2}} \dots \xrightarrow{V_{i_q}} W$, où W est irréductible par les différents V_i ; W pourra être appelé « un reste » de U modulo S .

Avertissement 8.

Dans le cas general le reste modulo un ensemble de p -uplets n'est pas unique, comme le prouve l'exemple suivant

$$U = \begin{pmatrix} 1 \\ 2 \\ -1 \\ 0 \end{pmatrix}, V_1 = \begin{pmatrix} 1 \\ 1 \\ -1 \\ 0 \end{pmatrix}, V_2 = \begin{pmatrix} 0 \\ 2 \\ 0 \\ 0 \end{pmatrix}$$

$$U \xrightarrow{V_1} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \xrightarrow{V_2} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \text{ tandis que } U \xrightarrow{V_2} \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} \xrightarrow{V_1} \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}$$

Rappelons le

Lemme 9. Gordon-Dickson

Toute partie non vide de N^p possède un nombre fini d'éléments minimaux (pour la relation \preccurlyeq)

(généralise le classique minimum d'une partie non vide de \mathcal{N} ; pour les algébristes: ce résultat nous épargne les recours Noetheriens)

Théorème 10. (d'après le théorème de Buchberger)

On suppose donné un ensemble fini de p -uplets lex-strictement positifs $S = \{V_i, i \in I\}$.

On pose $S := \{V_i, i \in I\}$, $G := \{\{V_i, V_j\}, V_i \neq V_j\}$

tant que $G \neq \emptyset$

on prend $\{V_i, V_j\} \in G$, on pose $G := G - \{V_i, V_j\}, W :=$ une réduction de $(V_i - V_j)$ modulo S

si $W \neq 0$ on pose $G := G \cup \{\{V, W^*\}, V \in G\}, S := S \cup \{W^*\}$

L'algorithme de Buchberger s'arrête en un temps fini.

Remarquons au passage que, suite à l'hypothèse sur les V_i et la définition des W^* , les éléments de S sont tous lex-positifs.

Démonstration.

Désignons par (S_k) la suite des ensembles S créés par l'algorithme et, pour chaque k , par S_k° l'ensemble $\{V^+, V^-\}_{V \in S_k}$; tant qu'on obtient un p uplet W^* avec W^{*+} et/ou W^{*-} non nul $S_k^\circ \subsetneq S_{k+1}^\circ$; $S_\infty^\circ = \cup_{k \in \mathbb{N}} S_k^\circ$ est une partie non vide de \mathbb{N}^n et possède donc un ensemble fini d'éléments minimaux pour \preceq , par suite il existe un indice k tel que S_k^+ contient tous ces éléments minimaux; or pour tout élément W^* créé par l'algorithme ni W^{*+} ni W^{*-} n'est précédé par aucun élément préexistant (proposition 3), par suite à partir d'un certain moment les W^{*+} et les W^{*-} sont nuls, par suite $W^*=0$ et l'algorithme de Buchberger s'arrête donc $S_\infty = S_k$ et sera appelé (une) base standard associée à S .

On retiendra que les éléments de la base standard sont lex-strictement positifs, que S_∞ contient S et que les ensembles S et S_∞ engendrent le même sous-groupe additif. □

Exemple 11.

On considère les trois uplets $\begin{pmatrix} 1 \\ 2 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 5 \\ 0 \\ 0 \\ -1 \end{pmatrix}$, l'application de l'algorithme produit les six uplets: $\begin{pmatrix} 1 \\ 0 \\ 2 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ -3 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 7 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -5 \\ 1 \\ 1 \end{pmatrix}$.

Lemme 12.

Soit la base standard $S_\infty = \{V_i, i \in I\}$.

1) 1) Soit $V = \sum_{i \in I} m_i V_i$ (où les m_i sont dans \mathbb{Z}), alors il existe un sous-ensemble $\mathcal{G} = \{W_i, i \in I'\} \subset S_\infty$ tel que $V = \sum_{i \in I'} n_i W_i$ et $\forall i \in I', s(W_i) \geq s(V)$.

2) Soit $V = \sum_{i \in I} m_i V_i$ (où les m_i sont dans \mathbb{Z}) et $s(V) = t$, alors il existe un élément W de S_∞ tel que $s(W) = t$ et le reste de V modulo W est une combinaison linéaire d'éléments de S_∞ dont les t premières coordonnées sont nulles.

Démonstration. □

1) Montrons d'abord que si $s(V) > 1$ alors il existe un sous-ensemble $\mathcal{G} = \{W_i, i \in I'\} \subset S_\infty$ tel que $V = \sum_{i \in I'} n_i W_i$ et $\forall i \in I', s(W_i) > 1$.

Soit $V = \sum_{i \in I} m_i V_i$ tel que $\forall i \in I, V_i = \begin{pmatrix} v_i \\ \dots \\ \dots \end{pmatrix}$ et $\sum_{i \in I} m_i v_i = 0$ et $K = \{i, s(V_i) = 1\}$ n'est pas vide.

Pour chacun des $i \in K$ nous savons que v_i est strictement positif, les coefficients m_i sont des entiers relatifs et la somme $\sum_{i \in K} m_i v_i = 0$.

Montrons qu'il est possible pas à pas de diminuer le cardinal de K .

Soit $K^- = \{k \in K, m_k < 0\}$ et $K^+ = \{k \in K, m_k > 0\}$, comme $\sum_{i \in K} m_i v_i = 0$ ni K^- ni K^+ ne peuvent être vides.

On pourra tout au long de la procédure suivante, quitte à introduire des différences $(V_i - V_j)^*$ dont la première coordonnée serait alors nulle, toujours supposer que $\forall (i, j) \in K^- \times K^+, v_i \neq v_j$

Soit $v_t = \max\{v_k, k \in K\}$

i) si c'est $v_j \in K^+$ on considère $v_s = \max\{v_i, i \in K^-\}$, alors $v_j - v_s > 0$

$m_s V_s + m_j V_j = m_j (V_j - V_s) + (m_s - m_j) V_s$; la proposition 5 permet de conclure que le $\max\{v_k, k \in K\}$ diminue strictement

ii) si c'est $v_i \in K^-$ on considère $v_t = \max\{v_j, j \in K^+0\}$, alors $v_i - v_t > 0$

$m_i V_i + m_t V_t = m_i (V_i - V_t) + (m_i + m_t) V_t$ d'où, de même le $\max\{v_k, k \in K\}$ diminue strictement

comme les v_k sont des entiers naturels ce processus sera fini.

Comme nous avons remarqué que, si K n'est pas vide, ni K^- ni K^+ ne peuvent l'être, nous aboutissons en fin de compte à $K = \emptyset$, ce qui démontre le résultat annoncé: nous avons obtenu une écriture de V comme combinaison linéaire d'éléments de la base standard tels que $s > 1$.

On montrerait de même que, quel que soit $s(V)$, il existe un sous-ensemble $\mathcal{G} = \{W_i, i \in I'\} \subset S_\infty$ tel que $V = \sum_{i \in I'} n_i W_i$ et $\forall i \in I', s(W_i) \geq s(V)$

2) Soit $V = \sum_{i \in I} m_i V_i$ où $s(V) = t, \forall i \in I, s(V_i) \geq t, V_i = \begin{pmatrix} 0 \\ \dots \\ 0 \\ v_i \\ \dots \\ \dots \end{pmatrix}$ et $s(V) = t, \sum_{i \in I} m_i v_i = v > 0$.

Soit $J = \{k \in I, v_k > 0\}$

En appliquant la démarche du 1) on peut supposer que les coefficients m_i sont tous strictement positifs et, quitte à introduire des différences $(V_i - V_j)^*$ dont la t -ième coordonnée serait alors nulle, toujours supposer que $\forall (i, j) \in I^2, i \neq j \implies v_i \neq v_j$.

Si $\text{card}(J) = 1$ V est la somme de $m_1 V_1$ et de T , somme d'éléments de S_∞ dont les t premières coordonnées sont nulles.

Si $\text{card}(J) > 1$ considérons les deux indices i, j qui correspondent aux deux plus grandes valeurs de $\{v_k\}$:

supposons $v_j < v_i$ $m_i V_i + m_j V_j = m_i (V_i - V_j) + (m_i + m_j) V_j$, où $V_i - V_j$ est une combinaison linéaire de termes lex-positifs de la base standard dont la t -ième coordonnée est strictement inférieure à v_i . En itérant on obtient en fin de compte $V = mW + T$, où W est un élément de S_∞ tel que $s(W) = t$ et T une combinaison linéaire d'éléments de S_∞ dont les t premières coordonnées sont nulles.

Théorème 13.

Soit un ensemble fini de p -uplets $S = \{V_i, i \in I\}$ et une base standard $S_\infty = \{W_j, j \in J\}$ associée à S ; un p -uplet V appartient au sous-groupe engendré par S si et seulement il est réduit modulo S_∞ .

Démonstration.

Soit $V = \sum a_j W_j$

1) Le lemme 12 implique que V s'écrit $V = m_1 W_1 + T$, où $s(W_1) = s(V)$ et T est une combinaison linéaire d'éléments de S_∞ dont les $s(V)$ premières coordonnées sont nulles, donc c'est le reste de la réduction de V par W_1 .

En itérant on obtient une suite de réductions par des éléments W_i de S_∞ et des entiers m_i telle que $\forall i, s(V - \sum_{k=1}^i m_k W_k)$ croît strictement dans $[1, \dots, p]$, donc il existe un entier r tel que $V = \sum_{k=1}^r m_k W_k$, donc V est réduit modulo S_∞

2) La réciproque est triviale. □

Théorème 14. *Unicité du reste d'un p -uplet modulo S_∞*

Soit V un p -uplet positif, le reste de V dans une réduction modulo S_∞ est unique (indépendant de la procédure utilisée).

Démonstration.

Soit V un $n+m$ -uplet positif, supposons que $\begin{cases} V = \sum_{j \in J} m_j W_j + R_1 \\ V = \sum_{j \in J} \mu_j W_j + R_2 \end{cases}$ deux réductions de V modulo S_∞ , alors $(R_1 - R_2)^$ appartient au sous-groupe engendré par les W_j et donc (Théorème 13) son reste est nul; par ailleurs comme R_1 et R_2 sont positifs $(R_1 - R_2)^*$ n'est précédé par aucun des W_j donc il est égal à son reste.*

Donc le reste de V modulo S_∞ est indépendant de la réduction opérée. □

Comparaison avec les bases standard « classiques »

Dans le cas des binômes il semble que la forme proposée est plus légère:

Au lieu d'un binôme $a^2x^3y - b^0z^3t^2$ nous écrivons $\begin{pmatrix} 2 \\ 0 \\ 3 \\ 1 \\ -3 \\ -2 \end{pmatrix}$ et au lieu de $ay^2z - b^2x^2t^3$ nous écrivons $\begin{pmatrix} 1 \\ -2 \\ -2 \\ 2 \\ 1 \\ -3 \end{pmatrix}$ (avec l'ordre $a > b > x > y > z > t$).

Le calcul du S-polynome associé passe par le ppcm des monômes a^2x^3y et ay^2z qui est $a^2x^3y^2z$, puis $yz(a^2x^3y - b^0z^3t^2) - ax^3(ay^2z - b^2x^2t^3) = -a^0b^0yz^4t^2 + ab^2x^5t^3 = t^2(-a^0b^0yz^4t^0 + ab^2x^5z^0t)$, où l'on simplifie par le facteur commun en invoquant les propriétés de l'idéal d'un treillis, d'où le vecteur

$$\begin{pmatrix} 1 \\ 2 \\ 5 \\ -1 \\ -4 \\ 1 \end{pmatrix}.$$

Tandis qu'en soustrayant simplement les vecteurs on obtient directement $\begin{pmatrix} 2 \\ 0 \\ 3 \\ 1 \\ -3 \\ -2 \end{pmatrix} - \begin{pmatrix} 1 \\ -2 \\ -2 \\ 2 \\ 1 \\ -3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 5 \\ -1 \\ -4 \\ 1 \end{pmatrix}.$

La présentation proposée évite l'usage de polynômes en plusieurs indéterminées et des connaissances algébriques associées, permettant un emploi par un public d'étudiants beaucoup plus large.

Bibliographie : [1] R.R. Thomas (1995), A geometric Buchberger Algorithm for integer programming, Math.Operations Research 20, pp.864-884

Paris, Octobre 2017