

Applications des bases de Gröbner (notes de cours)

Frédéric Chyzak

Le 15 octobre 2003

1 Lemme de Dickson

Lemme. Toute partie stable S du monoïde $[X_1, \dots, X_n]$ est finiment engendrée.

Démonstration. On fait une preuve par récurrence sur n .

Le cas $n = 1$ est immédiat : prendre l'élément de S de degré minimal ; celui-ci engendre S .

Supposons démontré le cas de $[X_1, \dots, X_n]$ et soit S une partie stable de $M = [X_1, \dots, X_n, Y]$. Considérons S' , obtenue en faisant $Y = 1$ dans S . C'est une partie stable de $M' = [X_1, \dots, X_n]$; elle est donc finiment engendrée par des éléments $X^{\alpha_1}, \dots, X^{\alpha_s}$. Il en est de même pour chaque partie stable S'_j de M' donnée par $S'_j = \{m \in M' \mid mY^j \in S\}$: S'_j est finiment engendrée par des éléments $X^{\alpha_{1,j}}, \dots, X^{\alpha_{s_j,j}}$. Sans perte de généralité, on peut se donner un entier m tel que tous les $X^{\alpha_i}Y^m$ sont dans S' . On vérifie aisément que la partie stable (finiment) engendrée par les $X^{\alpha_{i,j}}Y^j$ pour $j < m$ et par les $X^{\alpha_i}Y^m$, tels que définis ci-dessus, n'est autre que S . □

2 Théorème définissant les bases de Gröbner

Définition. Soit I un idéal de $A = \mathbb{C}[X_1, \dots, X_n]$ et \prec un ordre monomial. Un ensemble fini $G \subseteq I$ est une base de Gröbner de I pour l'ordre \prec si l'une quelconque des propriétés équivalentes est vérifiée :

1. la partie stable de M engendrée par $\text{mt}(G)$ est $\text{mt}(I)$;
2. $\text{mt}(G)$ et $\text{mt}(I)$ engendrent le même idéal ;
3. tout $f \in I$ non nul est réductible par G ;
4. pour tout $f \in A$, il existe un unique $r \in A$ tel que $f - r \in I$ et dont aucun monôme n'est divisible par un monôme de $\text{mt}(G)$;
5. pour tout $f \in I$, le reste de la division de f par G est nul.

Démonstration. Faisons une preuve (presque) circulaire.

1 \Rightarrow 2. Supposons que

$$\bigcup_{g \in G} M\text{mt}(g) = \text{mt}(I).$$

Passons alors aux idéaux :

$$(\text{mt}(I)) = \sum_{g \in G} (M\text{mt}(g)) = \sum_{g \in G} (\text{mt}(g)) = (\text{mt}(G)).$$

On a prouvé que $\text{mt}(G)$ et $\text{mt}(I)$ engendrent le même idéal.

2 \Rightarrow 3. Supposons $(\text{mt}(G)) = (\text{mt}(I))$. Soit $f \in I \setminus \{0\}$. On a d'abord que

$$\text{mt}(f) = \sum_{g \in G} q_g \text{mt}(g)$$

pour des polynômes q_g , puis, en scindant en monômes, que

$$\text{mt}(f) = \sum_j c_j m_j \text{mt}(g_j)$$

pour des c_j de \mathbb{C} , des monômes m_j et des g_j de G . Comme cette somme sur j est en fait une somme de terme, les termes en les monômes autres que $\text{mt}(f)$ doivent s'annuler, et on peut sans perte de généralité supposer que pour chaque j , $m_j \text{mt}(g_j) = \text{mt}(f)$. On a alors, pour j_0 l'un de ces j ,

$$\text{mt}(f) = m_{j_0} \text{mt}(g_{j_0}).$$

Donc f est réductible par G .

3 \Rightarrow 4. Soit $f \in A$. On a l'existence en prenant pour r le reste de la division de f par g : alors, $f - r \in I$. Supposons que nous ayons deux écritures $f = h_i + r_i$, pour $i = 1, 2$, avec $h_i \in I$ et des r_i dont aucun des monômes n'est divisible par un monôme de $\text{mt}(G)$. Alors

$$r_1 - r_2 = h_2 - h_1 \in I$$

est soit nul, soit réductible. Supposons cette différence non nulle ; alors $\text{mt}(r_1 - r_2)$ est forcément un monôme parmi ceux de r_1 et r_2 . Ce monôme de tête est à la fois non divisible par un monôme de $\text{mt}(G)$, par définition des r_i , et divisible par l'un d'entre eux, par l'hypothèse faite du point (3). C'est une contradiction, et on a l'unicité de r .

4 \Rightarrow 5. Soit $f \in I$. En application du point (4), on trouve un r , qui par la preuve d'existence et d'unicité précédente ne peut être que le reste de la division de f par G . Comme $r = (r - f) + f \in I$ mais n'est pas réductible, c'est que r est nul.

5 \Rightarrow 2. Soit f divisible par G . Alors $\text{mt}(f)$ est dans la partie stable engendrée par $\text{mt}(G)$, donc dans l'idéal engendré par $\text{mt}(G)$. Comme tout élément non nul de I est divisible par G , on a obtenu

$$(\text{mt}(I)) \subset (\text{mt}(G)) ;$$

l'autre inclusion est évidente.

2 \Rightarrow 1. L'inclusion de la partie stable S engendrée par $\text{mt}(G)$ dans $\text{mt}(I)$ découle de ce que $G \subset I$. Pour l'autre inclusion, soit $m \in \text{mt}(I) \subset (\text{mt}(I)) = (\text{mt}(G))$. Par le même raisonnement que pour l'implication 2 \Rightarrow 3, on écrit m sous la forme $m_{j_0} \text{mt}(g_{j_0})$, qui est un élément de S . La partie stable $\text{mt}(I)$ est donc incluse dans S .

□