1 Généralités

On se place dans l'ensemble $\mathbb{Q}[X_n]$ des polynômes en l'alphabet $X_n = x_1, x_2, \ldots, x_n$. Pour $\mathbf{p} = (p_1, p_2, \ldots, p_n) \in \mathbb{N}^n$, on note

$$X_n^{\mathbf{p}} = x_1^{p_1}\, x_2^{p_2} \cdots x_n^{p_n}\,.$$

Définition 1 $f_1, \ldots, f_k \in \mathbb{Q}[X_n]$. L'*idéal* engendré par $f_1, \ldots, f_k$, noté $(f_1, \ldots, f_k)$ est l'ensemble des polynômes pouvant s'écrire sous la forme :

$$P = \sum_{i=1}^{k} A_i\, f_i \qquad A_i \in \mathbb{Q}[X_n].$$

Exemple 2 Soient :

$$\begin{aligned} f_1 &= x_1 + x_2 \\ f_2 &= x_1^2 + x_1\, x_2 + x_2^2 \\ f_3 &= x_1^3 + x_1^2\, x_2 + x_1\, x_2^2 + x_2^3. \end{aligned}$$

$I = (f_1, f_2, f_3)$,

$$x_1^2 = f_2 - x_2\, f_1 \ \in I\,.$$

Définition 3 $P,\ Q \in \mathbb{Q}[X_n]$ sont *équivalents* modulo I si $P - Q \in I$; on note $P \equiv Q\ [I]$.

Le *quotient* de $\mathbb{Q}[X_n]$ par I, noté $Q[X_n]/I$ est l'ensemble des classes modulo I.

Exemple 4

$$\begin{aligned} x_1\, x_2 &= x_1\, x_2 + x_1^2 - x_1^2 \\ &\equiv x_1\,(x_1 + x_2) \\ &\equiv 0. \end{aligned}$$

Proposition 5 *$\mathbb{Q}[X_n]/I$ est un espace vectoriel.*

Exemple 6

$$I = (f_1, f_2, f_3)$$

$\{1, x_1\}$ est une base de $\mathbb{Q}[X_2]/I$.

$$\dim \mathbb{Q}[X_2]/I = 2$$

Définition 7 On définit un *produit scalaire* sur $\mathbb{Q}[X_n]$ par

$$\langle P, Q\rangle = L_0(P(\partial)Q).$$

Exemple 8

$$P = x_1^2 + 3\,x_1\,x_2 + x_2\ ,\quad Q = x_1^3 + x_1\,x_2$$

$$\begin{aligned} P(\partial)Q &= (\partial x_1^2 + 3\partial x_1 x_2 + \partial x_2)(x_1^3 + x_1\,x_2) \\ &= 6x_1 + 0 + 0 + 3 + 0 + x_1 \\ \langle P, Q\rangle &= 3 \end{aligned}$$

Remarque 9

$$\langle X_n^{\mathbf{p}}, X_n^{\mathbf{q}}\rangle = \begin{cases} 0 & \text{si } \mathbf{p} \neq \mathbf{q}, \\ \mathbf{p}! = p_1!\,p_2!\cdots p_n! & \text{si } \mathbf{p} = \mathbf{q}. \end{cases}$$

Définition 10

$$I^{\perp} = \{P \in \mathbb{Q}[X_n] \ /\ \forall Q \in I,\ \langle P, Q\rangle = 0\}$$

$$\begin{aligned}\pi_m \quad : \quad & \mathbb{Q}[X_n] \longrightarrow \mathbb{Q}[X_n] \\ & X_n^{\mathbf{p}} \longmapsto \begin{cases} 0 & \text{si } |\mathbf{p}| \neq m, \\ X_n^{\mathbf{p}} & \text{si } |\mathbf{p}| = m. \end{cases}\end{aligned}$$

Pour $\mathbf{V}$ un sous-espace de $\mathbb{Q}[X_n]$,

$$\mathcal{H}_m(\mathbf{V}) = \pi_m(\mathbf{V}).$$

Définition 11 $\mathbf{V}$ est dit *homogène* si

$$\forall m \geq 0 \ , \quad \mathcal{H}_m(\mathbf{V}) \subseteq \mathbf{V}.$$

Remarque 12 Si $\mathbf{V}$ est homogène,

$$\mathbf{V} = \mathcal{H}_0(\mathbf{V}) \oplus \mathcal{H}_1(\mathbf{V}) \oplus \mathcal{H}_2(\mathbf{V}) \oplus \cdots$$

$$\dim \mathcal{H}_m(\mathbf{V}) \leq \dim \mathcal{H}_m(\mathbb{Q}[X_n]) = \binom{n+m-1}{n-1}$$

Définition 13 La *série de Hilbert* de $\mathbf{V}$ est :

$$F_{\mathbf{V}}(q) = \sum_m \dim \mathcal{H}_m(\mathbf{V})\, q^m.$$

Exemple 14

$$\begin{aligned} F_{\mathbb{Q}[X_n]}(q) &= \sum_{\mathbf{p}\in\mathbb{N}^n} q^{\deg X_n^{\mathbf{p}}} \\ &= \sum_{p_1\geq 0,\ldots,p_n\geq 0} q^{p_1+\cdots+p_n} \\ &= \frac{1}{(1-q)^n} \end{aligned}$$

Proposition 15 *Si* $\mathbf{V}$ *est homogène alors* $\mathbf{V}^\perp$ *l'est aussi et*

1. $\mathbf{V}^{\perp\perp} = \mathbf{V}$
2. $\mathbf{V} \oplus \mathbf{V}^\perp = \mathbb{Q}[X_n]$.

Proposition 16 *Si* $f_1, f_2, \ldots, f_k$ *sont homogènes, alors* $(f_1, f_2, \ldots, f_k)$ *est homogène et :*

$$\begin{aligned}(f_1, f_2, \ldots, f_k)^\perp &= \{P \in \mathbb{Q}[X_n] \ / \ \forall i,\ f_i(\partial)P = 0\} \\ &= K(f_1, \ldots, f_k).\end{aligned}$$

$$\Big((f_1, f_2, \ldots, f_k)^\perp = \{P \in \mathbb{Q}[X_n] \,/\, \forall i,\ f_i(\partial)P = 0\}\Big)$$

Preuve.
Il est clair que $K(f_1, \ldots, f_k) \subseteq (f_1, \ldots, f_k)^\perp$.

Inversement, soit $P \in (f_1, \ldots, f_k)^\perp$. Comme $X_n^{\mathbf{q}}\, f_i \in (f_1, \ldots, f_k)$,

$$\langle X_n^{\mathbf{q}}\, f_i, P\rangle = L_0(\partial X_n^{\mathbf{q}}\, f_i(\partial)P) = 0.$$

Le polynôme $f_i(\partial)P$ a ainsi toutes ses dérivées nulles en 0. D'après le théorème de Taylor, il est nul.

∎

Proposition 17 *Soit I un idéal homogène.*

$\mathbf{H}_I = I^\perp$ *et* $R_I = \mathbb{Q}[X_n]/I$ *sont isomorphes.*

Plus précisément, si $\{P_1, \ldots, P_m\}$ *est une base de* $\mathbf{H}_I$*, c'est aussi une base de* R_I*.*

$\Big($ toute base de $\mathbf{H}_I$ est une base de R_I $\Big)$

Preuve.

- $\mathbb{Q}[X_n] = I \oplus \mathbf{H}_I$

donc tout $P \in \mathbb{Q}[X_n]$ s'écrit de façon unique

$$P = \sum_{i=1}^{m} c_i \, P_i + E \ , \quad E \in I.$$

Donc $\{P_1, \ldots, P_m\}$ engendre R_I.

- $\mathbb{Q}[X_n] = I \oplus \mathbf{H}_I$

donc si

$$\sum_{i=1}^{m} c_i \, P_i = E \ , \quad E \in I$$

alors $E = 0$.

Donc $\{P_1, \ldots, P_m\}$ est linéairement indépendante dans R_I.

∎

Bases de Gröbner.

Définition 18 On ordonne les monômes de $\mathbb{Q}[X_n]$ à l'aide de l'*ordre lexicographique (gradué)* :

$$X_n^{\mathbf{p}} > X_n^{\mathbf{q}} \iff |\mathbf{p}| > |\mathbf{q}| \text{ ou } \exists k \,/$$

$$p_1 = q_1,\ \ldots,\ p_{k-1} = q_{k-1},\ p_k > q_k.$$

C'est un ordre total.

Le *monôme dominant* d'un polynôme P, noté $LM(P)$ est son plus grand monôme pour cet ordre.

Exemple 19

$$P = 2x_1^3\, x_2 - x_1\, x_2\, x_3^2 + x_2^4 - 3x_2\, x_3^2\ ,\ \ LM(P) = x_1^3\, x_2$$

Définition 20 Une *base de Gröbner* d'un idéal I est un ensemble fini de polynômes $\mathcal{G} = \{g_1, \ldots, g_m\}$ tel que :

$$\forall P \in I \ , \quad \exists g_i \in \mathcal{G} \ / \ LM(g_i) \,|\, LM(P).$$

On note $LM(I) = \{LM(P), \ P \in I\}$.

Théorème 21 *Tout idéal I possède une unique base de Gröbner réduite.*

Proposition 22 *Soit $\{g_1, \ldots, g_m\}$ base de Gröbner de I. Alors*

$$\mathcal{B} = \{X_n^{\mathbf{p}} \ / \ \forall i, \ LM(g_i) \not| \ X_n^{\mathbf{p}}\}$$

est une base de $\mathbb{Q}[X_n]/I$.

Preuve.

• **famille génératrice :**

On montre que tout monôme $X_n^{\mathbf{q}} \notin \mathcal{B}$ peut être réécrit (modulo I) à l'aide de monômes plus petits.

$$\begin{aligned} \exists i,\ X_n^{\mathbf{q}} &= X_n^{\alpha}\, LM(g_i) \\ X_n^{\mathbf{q}} &= X_n^{\alpha}\,(LM(g_i) - g_i) + X_n^{\alpha}\, g_i \\ &\equiv X_n^{\alpha}\,(LM(g_i) - g_i) \quad [I] \end{aligned}$$

• **famille linéairement indépendante :**

Si $\exists(\alpha_{\mathbf{p}})$ tels que

$$\begin{aligned} \sum \alpha_{\mathbf{p}}\, X_n^{\mathbf{p}} &\equiv 0 \quad [I] \\ \sum \alpha_{\mathbf{p}}\, X_n^{\mathbf{p}} &\in I \\ LM(\sum \alpha_{\mathbf{p}}\, X_n^{\mathbf{p}}) &\in LM(I) \end{aligned}$$

∎

Exemple 23

I idéal, $\mathcal{G} = \{x_1 + x_2 + x_3,\ x_2^2 + x_2x_3 + x_3^2,\ x_3^3\}$

$\mathcal{B} = \{1,\ x_2,\ x_3,\ x_2x_3,\ x_3^2,\ x_2x_3^2\}$

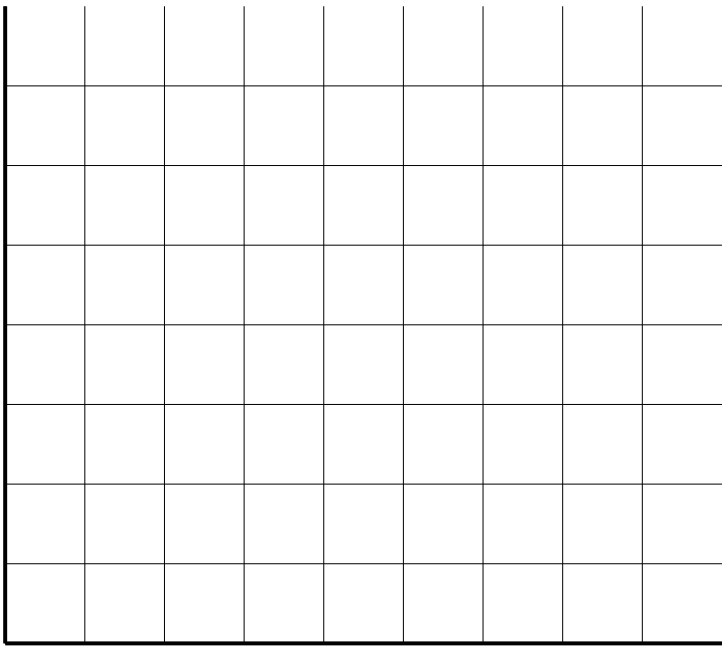
$x_1x_2 \equiv$

Remarque 24

$$\mathbb{Q}[X_n]/I \simeq \mathbb{Q}[X_n]/LM(I)$$

Exemple 25 Visualisation pour $n = 2$:

I idéal de $\mathbb{Q}[X_2]$, $LM(\mathcal{G}) = \{x_2^6,\ x_1\,x_2^4,\ x_1^4,\ x_1^3\,x_2\}$



Critère de Buchberger

$F = \{f_1, f_2\}$ avec
$f_1 = x_1^3 + 2x_1x_2^2 + x_2^3 \quad$ et $\quad f_2 = x_1x_2 - x_2^2$

$$
\begin{aligned}
S(f_1, f_2) &= x_2\, f_1 - x_1^2\, f_2 \\
&= x_2(x_1^3 + 2x_1x_2^2 + x_2^3) \\
&\quad -x_1^2(x_1x_2 - x_2^2) \\
&= 2x_1x_2^3 + x_2^4 - x_1^2x_2^2 \\
&= -x_1^2x_2^2 + 2x_1x_2^3 + x_2^4 \\
&\equiv -x_1^2x_2^2 + 2x_1x_2^3 + x_2^4 \\
&\quad +x_1x_2(x_1x_2 - x_2^2) \\
&= x_1x_2^3 + x_2^4 \\
&\equiv x_1x_2^3 + x_2^4 - x_2^2(x_1x_2 - x_2^2) \\
&= 2x_2^4 \\
&= \overline{S(f_1, f_2)}^F
\end{aligned}
$$

Critère 26 *Un ensemble fini* $\mathcal{G} = \{g_1, \ldots, g_m\}$ *est une base de Gröbner si et seulement si*

$$\forall i \neq j, \quad \overline{S(g_i, g_j)}^{\mathcal{G}} = 0.$$

Proposition 27 *Si* f *et* g *ont des monômes dominants* disjoints *alors*

$$\overline{S(f, g)}^{\{f,g\}} = 0.$$

Exemple 28 Soit I engendré par :

$$x_1 + x_2 + x_3 \qquad x_1x_4 \qquad x_4 + x_5 + x_6$$

$$x_1x_2 \qquad x_2x_5 \qquad x_4x_5$$

$$x_1x_3 \qquad x_3x_6 \qquad x_4x_6$$

$$x_2x_3 \qquad x_5x_6$$

Représentations.
Cas du groupe symétrique.

$\mathbf{V}$: $\mathbb{C}$-espace vectoriel de dimension finie
$GL(\mathbf{V})$: groupe des isomorphismes de $\mathbf{V}$.

Définition 29 G un groupe fini. Une *représentation* de G est un morphisme ρ de G dans $GL(\mathbf{V})$, *i.e.* ρ tel que

$$\forall s, t \in G \ , \quad \rho(st) = \rho(s)\rho(t).$$

Remarque 30 On a immédiatement :

- $\rho(1_G) = Id$,
- $\rho(s^{-1}) = \rho(s)^{-1}$,

On notera souvent $s.v$ pour $\rho(s)(v)$.

Exemple 31 $\mathbf{V} = \mathbb{Q}[X_n]$

$\forall \sigma \in \mathcal{S}_n \ , \ \sigma.P(x_1, \ldots, x_n) = P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$

Action de S_n sur $\mathbb{Q}[X_n]$ car :

$$\begin{aligned} \tau.(\sigma.P(X_n)) &= \tau.(P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})) \\ &= P((x_{\tau(\sigma(1))}, \ldots, x_{\tau(\sigma(n))})) \\ &= P((x_{(\tau\sigma)(1)}, \ldots, x_{(\tau\sigma)(n)})) \\ &= (\tau\sigma).P(X_n) \end{aligned}$$

$Sym_n \subset \mathbb{Q}[X_n]$ est stable car

$$\forall \sigma \in \mathcal{S}_n \ , \quad \sigma.P = P \in Sym_n$$

$\forall P \in Sym_n \ , \quad \mathcal{L}[P]$ est stable : représentation triviale.

$\mathbf{W} \subseteq \mathbf{V}$ est *stable* si

$$\forall s \in G,\ x \in \mathbf{W} \Longrightarrow \rho(s)(x) \in \mathbf{W}.$$

Somme directe : $\mathbf{V} = \mathbf{W} \oplus \mathbf{W}'$

Définition 32 La représentation $\mathbf{V}$ est *irréductible* si elle n'admet pas de sous-espace stable autre que $\{0\}$ et $\mathbf{V}$.

Théorème 33 *Toute représentation est somme directe de représentations irréductibles.*

Définition 34 Le *degré* de la représentation ρ est $\dim \mathbf{V}$.

Exemple 35 La représentation de degré 1

$$\forall s \in G \ , \quad \rho(s) = Id$$

est appelée *représentation triviale*.

Exemple 36 Soit $\mathbf{V}$ ayant une base indexée par les éléments t de G, ie : $(e_t)_{t \in G}$.

La représentation

$$s.e_t = \rho(s)(e_t) = e_{st}$$

est appelée *représentation régulière (à gauche)* de G. En particulier, son degré est égal à l'ordre $|G|$ de G.

Exemple 37 $G = S_3$

$\mathbf{V} = \mathcal{L}[e_{Id}, e_{(1,2)}, e_{(1,3)}, e_{(2,3)}, e_{(1,2,3)}, e_{(1,3,2)}]$

Représentation régulière : $\tau.e_\sigma = e_{\tau\sigma}$

$$\mathrm{Mat}_B \rho((1,2)) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Théorème 38 *Le nombre de représentations irréductibles de G est égal au nombre de classes de conjugaison de G.*

Théorème 39 *Chaque représentation irréductible est contenue dans la régulière un nombre de fois égal à son degré n_i. En particulier*

$$\sum n_i^2 = |G|.$$

Cas du groupe symétrique

T tableau injectif de forme $\lambda \vdash n$:

$$T = \begin{array}{|c|c|c|}\hline 3 & 1 & \\ \hline 5 & 7 & \\ \hline 2 & 4 & 6 \\ \hline \end{array}$$

$$\begin{aligned} \Delta_T(X_n) &= \Delta_3(x_2, x_5, x_3)\Delta_3(x_4, x_7, x_1)\Delta_1(x_6) \\ &= \begin{vmatrix} 1 & x_2 & x_2^2 \\ 1 & x_5 & x_5^2 \\ 1 & x_3 & x_3^2 \end{vmatrix} \times \begin{vmatrix} 1 & x_4 & x_4^2 \\ 1 & x_7 & x_7^2 \\ 1 & x_1 & x_1^2 \end{vmatrix} \times 1 \end{aligned}$$

Action du groupe symétrique $\mathcal{S}_n$:

$$\sigma.\Delta_T(X_n) = \Delta_T(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

$$S^\lambda = \mathcal{L}[\Delta_T(X_n)\ ,\ T \text{ injectif de forme } \lambda]$$

Théorème 40
Les S^λ forment un système complet de représentations irréductibles et

$$\dim S^\lambda = f_\lambda\ .$$

Remarque 41 Ceci est compatible avec

$$\sum_{\lambda \vdash n} f_\lambda^2 = n!$$

Exemple 42 Représentations de S_3 :

• $\lambda = \ydiagram{3}$, $T = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline \end{array}$

$$\Delta_T(X_3) = 1$$

Représentation *triviale*.

• $\lambda = \ydiagram{1,1,1}$, $T = \begin{array}{|c|}\hline 3 \\ \hline 2 \\ \hline 1 \\ \hline \end{array}$

$$\Delta_T(X_3) = \Delta_3(X_3) = \begin{vmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{vmatrix}$$

Représentation *alternante* :

$$\sigma.\Delta_3(X_3) = \epsilon(\sigma)\Delta_3(X_3)$$

• $\lambda = \ydiagram{2,1}$ $\qquad T_1 = \begin{array}{|c|c|}\hline 3 & \\ \hline 1 & 2 \\ \hline \end{array}$ $\Delta_{T_1} = x_3 - x_1$

$T_2 = \begin{array}{|c|c|}\hline 2 & \\ \hline 1 & 3 \\ \hline \end{array}$ $\Delta_{T_2} = x_2 - x_1$

On vérifie que $\Delta_{\begin{array}{|c|c|}\hline 3 & \\ \hline 2 & 1 \\ \hline \end{array}} = x_3 - x_2 = \Delta_{T_1} - \Delta_{T_2}$.

$$\rho(Id) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \rho((12)) = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$$

$$\rho((13)) = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \qquad \rho((23)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\rho((123)) = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \qquad \rho((132)) = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$

On vérifie que :

$$\rho((12))\,\rho((23)) = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \rho((123))$$