Contrôle continu 2

Toute réponse doit être justifiée même si l'énoncé ne le demande pas explicitement.

Exercice 1. Dans $\mathbb{R}[x, y]$, soit I l'idéal engendré par $g_1 = xy - 7y^2 + 2$ et $g_2 = x - 2y^3 + y$.

1. Déterminer une base de Gröbner de I relativement à l'ordre lexicographique (avec $x \succ y$).
   Aide : En principe votre base de Gröbner sera constituée de g_1, g_2, g_3.
2. En déduire $V(I) \subset \mathbb{R}^2$.

Exercice 2.

1. Montrer qu'il existe un unique bon ordre monomial sur $\mathbb{N}$. On le note $\preceq$.
2. Soient $P_1, P_2 \in \mathbf{k}[X]$ (avec une seule variable) deux polynômes non nuls. Soit $P_1, P_2, \ldots, P_r$ une base de Gröbner de $\langle P_1, P_2 \rangle$ construite à partir de l'algorithme de Buchberger relativement à $\preceq$.
   Soit $i \in \{1, \ldots, r\}$ tel que pour tout $j \in \{1, \ldots, r\}$, $\deg(P_i) \leq \deg(P_j)$.
   Montrer que P_i est le pgcd de P_1 et P_2.
3. La conclusion est-elle toujours vraie si la base de Gröbner n'est pas nécessairement obtenue via l'algorithme de Buchberger ?

Exercice 3. On fixe un corps $\mathbf{k}$ et on suppose qu'*il n'est pas* algébriquement clos.
On se donne un ensemble algébrique affine $V = V(I) \subset \mathbf{k}^n$ avec $I \subset \mathbf{k}[X_1, \ldots, X_n]$ un idéal. Le but de l'exercice est de montrer qu'il existe un polynôme $P \in \mathbf{k}[X_1, \ldots, X_n]$ tel que $V = V(P)$.

1. Soit $f = \sum_{i=0}^{d} a_i X^i \in \mathbf{k}[X]$ avec $a_d \neq 0$. On définit l'homogénéisé de f dans $\mathbf{k}[X, Y]$: $f^h = \sum_{i=0}^{d} a_i X^i Y^{d-i}$.
   Montrer que f admet une racine dans $\mathbf{k}$ si et s. si il existe $(a, b) \in \mathbf{k}^2$ tel que $(a, b) \neq (0, 0)$ et $f^h(a, b) = 0$.
2. Déduire de la question précédente qu'il existe $g \in \mathbf{k}[X, Y]$ tel que $V(g) = \{(0, 0)\}$.
3. Utiliser une récurrence pour montrer que pour tout entier $s \geq 2$, il existe un polynôme $g \in \mathbf{k}[X_1, \ldots, X_s]$ tel que $V(g) = \{(0, \ldots, 0)\} \subset \mathbf{k}^s$.
   Indication : on pensera à utiliser un polynôme d'une variable qui n'a pas de racines.
4. En utilisant la question précédente, démontrer le résultat annoncé au départ.
   Indication : on pensera à utiliser des générateurs de l'idéal I.

Tournez la page ⟶

Exercice 4.

1. Soit $h \in \mathbf{k}[Y_1, \ldots, Y_m]$ non nul s'écrivant $h = \sum c_\beta Y_1^{\beta_1} \cdots Y_m^{\beta_m}$ (somme finie) avec $\beta = (\beta_1, \ldots, \beta_m) \in \mathbb{N}^m$ et $c_\beta \in \mathbf{k}$. On dit que h est homogène si il existe $d \in \mathbb{N}$ tel pour tout $\beta \in \mathbb{N}^m$, $c_\beta = 0$ si $|\beta| \neq d$ où $|\beta| = \beta_1 + \cdots + \beta_m$. L'entier d est alors appelé degré de h.
   (a) Soient $f, g \in \mathbf{k}[Y_1, \ldots, Y_m]$ deux polynômes homogènes non nuls. Montrer que le produit fg est homogène.
   (b) On dit qu'un idéal $J \subset \mathbf{k}[X_1, \ldots, X_m]$ est homogène s'il admet un système (fini) de générateurs homogènes.
   Soit $J \subset \mathbf{k}[Y_1, \ldots, Y_m]$ un idéal non nul. Montrer qu'il est homogène si et s. si : pour tout $f \in J$, toutes les composantes homogènes de f sont dans J (on appelle composante homogène de f la somme des termes de f ayant tous un même degré donné).

2. On se donne un ordre monomial $\preceq$ sur $\mathbb{N}^n$ et on suppose qu'il n'est pas bon. Soient $f_1, \ldots, f_s \in \mathbf{k}[X_1, \ldots, X_n]$ et I l'idéal engendré par les f_i.
   On cherche à montrer qu'on peut construire une base de Gröbner de I.
   Soit X_0 une nouvelle variable.
   Pour $f \in \mathbb{K}[X_1, \ldots, X_n]$ non nul s'écrivant $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha X^\alpha$ (somme finie) on définit son homogénéïsé $h(f) \in \mathbf{k}[X_0, \ldots, X_n]$ ainsi : $h(f) = \sum c_\alpha X_0^{d-|\alpha|} X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ où d désigne le degré (total) de f et $|\alpha| = \alpha_1 + \cdots + \alpha_n$.
   On définit un ordre monomial $\preceq^h$ sur $\mathbb{N}^{n+1}$:
   $$(\delta_0, \ldots, \delta_n) \prec^h (\gamma_0, \ldots, \gamma_n) \iff \Big[|\delta| < |\gamma| \text{ ou } \Big(|\delta| = |\gamma| \text{ et } (\delta_1, \ldots, \delta_n) \prec (\gamma_1, \ldots, \gamma_n) \Big) \Big].$$
   (a) Montrer que $\preceq^h$ est un ordre total, qu'il est monomial et bon.
   (b) Soient $p, p_1, \ldots, p_s \in \mathbf{k}[X_1, \ldots, X_n]$ tels que $p = p_1 + \cdots + p_s$. Notons $d, d_1, \ldots, d_s$ les degrés respectifs et $\delta = \max\{d, d_1, \ldots, d_s\}$. Montrer que $X_0^{\delta-d} \cdot h(p) = \sum_{i=1}^{s} X_0^{\delta-d_i} \cdot h(p_i)$.
   (c) Montrer que pour $f, g \in \mathbf{k}[X_1, \ldots, X_n]$, $h(fg) = h(f)h(g)$.
   (d) Soit $q(X_0, \ldots, X_n) \in \mathbf{k}[X_0, \ldots, X_n]$ homogène. Soit $(\alpha_0, \ldots, \alpha_n) = \exp_{\preceq^h}(q)$. Montrer que $\exp_{\preceq}(q(1, X_1, \ldots, X_n)) = (\alpha_1, \ldots, \alpha_n)$.
   (e) Soit I^h l'idéal de $\mathbf{k}[X_0, \ldots, X_n]$ engendré par $h(f_1), \ldots, h(f_s)$. Montrer que I^h admet une $\preceq^h$-base de Gröbner constituée d'éléments homogènes.
   (f) Montrer que si $f \in I$ alors il existe $k \in \mathbb{N}$ tel que $X_0^k \cdot h(f) \in I^h$.
   (g) Soit $q(X_0, \cdots, X_n) \in I^h$. Montrer que $q(1, X_1, \ldots, X_n) \in I$.
   (h) Montrer qu'il existe une partie finie $G = \{g_1, \ldots, g_r\}$ de I telle que G engendre I et pour tout $f \in I$, on ait $f = \sum_{i=1}^{r} q_i \cdot g_i$ avec $q_i \in \mathbf{k}[X_1, \ldots, X_n]$ et pour tout i, $\mathrm{lm}_{\preceq}(f) \succeq \mathrm{lm}_{\preceq}(q_i g_i)$ si $q_i \neq 0$.

3. (Question bonus : si vous avez du temps) On définit $h(I)$ comme l'idéal de $\mathbf{k}[X_0, \ldots, X_n]$ engendré par tous les $h(f)$ avec $f \in I$. Remarquons que $I^h \subset h(I)$. Décrire un algorithme permettant de calculer un système de générateurs de $h(I)$ étant donnés les générateurs $f_1, \ldots, f_s$ de I.

Correction de l'exercice 1

1. L'ordre monomial choisi fait que xy est le monôme dominant de g_1 et x est celui de g_2.

   On va adopter une notation classique. On va dire que par division, xy se réduit en $7y^2 - 2$ modulo g_1 et on notera $xy \to 7y^2 - 2$. De même on a la réduction : $x \to 2y^3 - y$.

   En effet, si on a $f = cx^j y^k xy + f'$ alors on peut écrire $f = cx^j y^k(g_1 + 7y^2 - 2) + f' = cx^j y^k g_1 + cx^j y^k(7y^2 - 2) + f'$. On notera simplement

   $$f \to cx^j y^k(7y^2 - 2) + f'.$$

   C'est le reste partiel après une division élémentaire. Nous allons effectuer la division de $S(g_1, g_2)$ par g_1, g_2.

   On a $S(g_1, g_2) = g_1 - y \cdot g_2 = -7y^2 + 2 + 2y^4 - y^2 = 2(y^4 - 4y^2 + 1)$.

   On ne peut pas réduire modulo g_1, g_2. On pose donc

   $$g_3 = y^4 - 4y^2 + 1.$$

   Avec ce nouvel élément (pour lequel y^4 est le monôme dominant), on a la réduction $y^4 \to 4y^2 - 1$.

   On poursuit avec $S(g_1, g_3)$.

   $$\begin{array}{rcl} S(g_1, g_3) & = & y^3 g_1 - x g_3 \\ & = & -7y^5 + 2y^3 + 4xy^2 - x \\ & \to & -7y^5 + 2y^3 + 4y(7y^2 - 2) - (2y^3 - y) \\ & \to & -7y(4y^2 - 1) + 2y^3 + 28y^3 - 8y - 2y^3 + y \\ & = & -28y^3 + 7y + 28y^3 - 8y + y \\ & = & 0. \end{array}$$

   Ainsi le reste de la division de $S(g_1, g_3)$ par g_1, g_2, g_3 est nul. On continue avec la réduction de $S(g_2, g_3)$.

   $$\begin{array}{rcl} S(g_2, g_3) & = & y^4 g_2 - x g_3 \\ & = & -2y^7 + y^5 + 4xy^2 + x \\ & \to & -2y^7 + y^5 + 28y^3 - 8y - 2y^3 + y \\ & \to & -2y^3(4y^2 - 1) + y^5 + 26y^3 - 7y \\ & = & -7y^5 + 2y^3 + 26y^3 - 7y \\ & \to & -7y(4y^2 - 1) + 28y^3 - 7y \\ & = & -28y^3 + 7y + 28y^3 - 7y \\ & = & 0. \end{array}$$

   Le reste est encore nul. Par conséquent g_1, g_2, g_3 est une base de Gröbner de I pour l'odre lexicographique $\preceq$.

   Remarquons que $g_1 = yg_2 + 2g_3$ ce qui entraine $I = \langle g_2, g_3 \rangle$ d'où $V(I) = V(\{g_2, g_3\})$.

   Résolvons d'abord l'équation $g_3 = 0$, i.e. $y^4 - 4y^2 + 1$. On résout d'abord $Y^2 - 4Y + 1$ pour laquelle on trouve deux solutions $Y_1 = 2 - \sqrt{3}$ et $Y_2 = 2 + \sqrt{3}$. L'équation $g_3 = 0$ a donc 4 solutions en

y (avec x quelconque) $y \in \{\sqrt{2-\sqrt{3}}, -\sqrt{2-\sqrt{3}}, \sqrt{2+\sqrt{3}}, -\sqrt{2+\sqrt{3}}\}$. Notons $y_1, \dots, y_4$ ces quatre éléments dans cet ordre.
L'annulation de g_2 nous permet d'avoir x en fonction de y ce qui donne au final (je laisse les détails) $V(I) = \{(2y_i^3 - y_i, y_i) \mid i = 1,2,3,4\}$.

Correction de l'exercice 2

1. L'ordre usuel sur $\mathbb{N}$ est monomial puisque pour $m,n,p \in \mathbb{N}$, si $m \le n$ alors $m+p \le n+p$. De plus il est bon car $1 > 0$.
Soit $\preceq$ un bon ordre monomial et montrons que $\preceq$ est égal à l'ordre usuel de $\mathbb{N}$. Puisque $\preceq$ est bon on a $1 \succ 0$. L'ordre étant monomial, cela entraine $1+1 \succ 1+0$ i.e. $2 \succ 1$. On peut alors montrer par récurrence que pour tout $n \in \mathbb{N}$, $n+1 \succ n$. On a donc bien l'ordre usuel.
2. Quitte à échanger les rôles de P_1 et P_2 on peut supposer que $\deg P_1 \ge \deg P_2$. Effectuons la division euclidienne de P_1 par P_2 et notons P_3 le reste : $P_1 = QP_2 + P_3$.
Notons $d_i = \deg P_i$ pour $i = 1,2$. Alors $S(P_1,P_2) = \frac{1}{\mathrm{lc}(P_1)} P_1 - \frac{1}{\mathrm{lc}(P_2)} X^{d_1-d_2} P_2$. Maintenant, considérons une division de $S(P_1,P_2)$ par P_1, P_2. Par construction, $\deg(S(P_1,P_2)) < \deg(P_1)$. Par conséquent, la réduction ne se fera qu'en utilisant P_2 et cette division consistera donc en la division euclidienne de $S(P_1,P_2)$ par P_2 : $S(P_1,P_2) = AP_2 + R$. Au final on a donc : $\frac{1}{\mathrm{lc}(P_1)} P_1 = \frac{1}{\mathrm{lc}(P_2)} X^{d_1-d_2} P_2 + AP_2 + R$. Ainsi R est le reste de la division de P_1 par P_2 car la condition $\mathrm{lm}(P_2) \nmid \mathrm{lm}(R)$ est équivalente à dire que $\deg(R) < \deg(P_2)$. En conclusion P_3 et R sont égaux à une constante multiplicative près.
Dans l'algorithme d'Euclide (pour la construction du pgcd de P_1, P_2) on continue en considérant la division euclienne de P_2 par P_3 ce qui donne un reste P_4, etc. Les arguments précédents montrent que la division de $S(P_2,P_3)$ par P_1,P_2,P_3 consiste en la division par P_3 car $\deg(S(P_2,P_3))$ est inférieur à celui de P_1 et P_2.
En conclusion, dans la base de Gröbner ainsi construite, on a tous les éléments produits par l'algorithme d'Euclide. En fait, on en a d'autres, par exemple celui provenant de la division de $S(P_1,P_3)$. En particulier si on note D le pgcd de P_1,P_2 (qui est le dernier reste non nul dans l'algorithme d'Euclide) alors D fait partie de notre base de Gröbner (à une constante multiplicative près).
On sait que $\langle P_1,P_2\rangle = \langle D\rangle = \langle P_1,\dots,P_r\rangle$ donc $D|P_j$ pour tout j d'où $\deg(D) \le \deg(P_j)$ pour tout j donc D est dans la base de Gröbner et son degré est minimal.
3. La conclusion est toujours vraie. En effet, on a toujours $\langle D\rangle = \langle P_1,P_2\rangle = \langle P_1,\dots,P_r\rangle$ où D désigne le pgcd de P_1,P_2. Notons P l'un des P_i ayant le degré minimal. Si on divise P_j par P relativement à l'ordre $\preceq$ alors on obtient un reste R nul car sinon $\mathrm{lm}(R)$ ne serait pas divisible par l'un des $\mathrm{lm}(P_j)$. Ainsi P divise tous les P_j. Cela entraine que $\langle P\rangle = \langle P_1,P_2\rangle = \langle D\rangle$. Par conséquent P et D sont égaux à une constante multiplicative près et P est donc le pgcd de P_1,P_2.

Correction de l'exercice 3

1. Remarquons que $f^h(X,1) = f(X)$.
Supposons que f ait une racine α. Alors $0 = f(\alpha) = f^h(\alpha,1)$.

Réciproquement soit $(a,b) \in \mathbf{k}^2$ avec $(a,b) \neq 0$ tel que $f^h(a,b) = 0$. Si $b \neq 0$ alors on a :

$$f^h(a,b) = \sum_{i=0}^{d} a_i a^i b^{d-i} = b^d \sum_{i=0}^{d} a_i (a/b)^i = b^d f(a/b)$$

ce qui entraine que a/b est une racine de f. Si $b = 0$ alors l'égalité $f^h(a,b) = 0$ entraine $a_d a^d = 0$ d'où $(a,b) = (0,0)$ ce qui est absurde.

2. Comme $\mathbf{k}$ n'est pas algébriquement clos, il existe un polynôme non constant $f \in \mathbf{k}[X]$ sans racines (f est de degré ≥ 2). On adopte les notations de la question 1 et on définit $g = f^h \in \mathbf{k}[X,Y]$ On remarque que $g(0,0) = 0$ (car g n'a pas de terme constant). De plus g n'a pas d'autre zéro que $(0,0)$ car sinon f aurait une racine par la question 1. Ainsi $V(g) = \{(0,0)\}$.
3. Par hypothèse de récurrence, il existe $g(X_1,\ldots,X_s) \in \mathbf{k}[X_1,\ldots,X_s]$ tel que $V(g) = \{(0,\ldots,0)\}$. Soit $f \in \mathbf{k}[X]$ un polynôme de degré ≥ 2 sans racines et on garde les notations de la question 1. On définit $h \in \mathbf{k}[X_1,\ldots,X_{s+1}]$ en posant :

$$h = \sum_{i=0}^{d} a_i \cdot (g(X_1,\ldots,X_s))^i \cdot (X_{s+1})^{d-i}.$$

On voit que $h(0,\ldots,0) = 0$. Soit $(a_1,\ldots,a_{s+1})$ un zéro de h.
Si $a_{s+1} \neq 0$ alors $f(\frac{g(a_1,\ldots,a_s)}{a_{s+1}}) = 0$ ce qui est absurde.
Si $a_{s+1} = 0$ alors $a_d \cdot g(a_1,\ldots,a_s)^d = 0$ ce qui entraine $g(a_1,\ldots,a_s) = 0$ et l'hypothèse de récurrence implique que $(a_1,\ldots,a_s,a_{s+1}) = 0$. Ainsi $V(h) = \{(0,\ldots,0)\}$.
4. Soient $g_1,\ldots,g_s$ un système de générateurs de $I \subset \mathbf{k}[X_1,\ldots,X_n]$. Soit $h \in \mathbf{k}[X_1,\ldots,X_s]$ tel que $V(h) = (0,\ldots,0)$. On pose alors

$$P(X_1,\ldots,X_n) = h(g_1(X_1,\ldots,X_n),\ldots,g_s(X_1,\ldots,X_n)).$$

Soit $a \in \mathbf{k}^n$. Alors $a \in V(P) \iff P(a) = 0 \iff \forall i, g_i(a) = 0 \iff a \in V(I)$.

Correction de l'exercice 4

1. (a) Ecrivons $f = \sum c_\beta Y^\beta$ et $g = \sum d_\gamma Y^\gamma$ avec $\beta,\gamma \in \mathbb{N}^m$ et dans ces sommes $|\beta| = d$ et $|\gamma| = d'$. Le produit fg se décompose alors ainsi $fg = \sum c_\beta d_\gamma Y^{\beta+\gamma}$ et dans cette somme $|\beta+\gamma| = |\beta| + |\gamma| = d + d'$. Ainsi fg est homogène de degré $d + d'$.
   (b) Supposons l'idéal homogène. Soit donc $f_1,\ldots,f_r$ des générateurs homogènes de I. Pour un élément quelconque $f \in \mathbf{k}[X_1,\ldots,X_n]$, notons $\sigma(f)$ sa partie homogène de plus haut degré de sorte que $f - \sigma(f)$ soit de degré $< \deg(f)$.
   Soit $f \in I$. Écrivons $f = \sum_i q_i f_i$. En décomposant les q_i en somme de ses composantes homogènes, on se retrouve avec f comme somme finie de qg avec $g \in \{f_1,\ldots,f_r\}$ et q est homogène. Dans ce cas, les qg sont homogènes par la question 1 et de plus appartiennent à I. Ainsi f est une somme d'éléments de I qui sont tous homogènes. Par identification, chaque composante homogène dans f se trouve être égale à une somme d'éléments de la partie droite et donc appartient à I.
   Voyons la réciproque. Soient $f_1,\ldots,f_s$ des générateurs de I. Par hypothèse, chaque composante homogène de chaque f_i est aussi dans I ce qui entraine que I est engendré par des éléments homogènes.

2. (a) Remarquons que la définition de $\preceq^h$ est équivalente à : $\delta \preceq^h \gamma$ si et s. si $\delta = \gamma$ ou $(\star)$; où $(\star)$ est la définition de l'énoncé. Cela montre que $\preceq$ est réflexif par définition. Montrons qu'il est antisymétrique. Par contraposé, soient $\delta \neq \gamma$ et montrons que $\delta \prec^h \gamma$ ou $\gamma \prec^h \delta$. Si $|\delta| \neq |\gamma|$ alors le résultat est acquis. Sinon, si on avait $(\delta_1, \dots, \delta_n) = (\gamma_1, \dots, \gamma_n)$ alors comme $|\delta| = |\gamma|$ alors on aurait $\delta_0 = \gamma_0$ ce qui serait absurde ; par conséquent on a $(\delta_1, \dots, \delta_n) \prec (\gamma_1, \dots, \gamma_n)$ ou $(\gamma_1, \dots, \gamma_n) \prec (\delta_1, \dots, \delta_n)$ et le résultat est démontré.

   Montrons que $\preceq^h$ est transitif. Soient $\gamma \preceq \delta \preceq \epsilon$. On peut supposer qu'on n'a aucune égalité sinon la conclusion est immédiate. On a $|\gamma| \leq |\delta| \leq |\epsilon|$. Si l'une de ces inégalités est stricte alors cela entraine $|\gamma| < |\epsilon|$ et $\gamma \prec^h \epsilon$. On se place donc dans le cas où $|\gamma| = |\delta| = |\epsilon|$. L'hypothèse entraine donc $(\gamma_1, \dots, \gamma_n) \prec (\delta_1, \dots, \delta_n) \prec (\epsilon_1, \dots, \epsilon_n)$ ce qui entraine à son tour la conclusion $\gamma \prec^h \epsilon$.

   Montrons que l'ordre est total. Soient $\gamma \neq \delta$. Si $|\gamma| \neq |\delta|$ alors γ et δ sont comparables. Plaçons nous dans le cas $|\gamma| = |\delta|$. Comme $\gamma \neq \delta$ on a forcément $(\alpha_1, \dots, \gamma_n) \neq (\delta_1, \dots, \delta_n)$; ces deux éléments sont donc comparables pour $\prec$ et la conclusion en découle.

   Montrons que $\preceq^h$ est monomial. Soient $\delta \prec^h \gamma$ et soit ϵ un autre élément. Si $|\delta| < |\gamma|$ alors $|\delta + \epsilon| < |\gamma + \epsilon|$ d'où $\delta + \epsilon \prec^h \gamma + \epsilon$. Sinon alors $(\delta_1, \dots, \delta_n) \prec (\gamma_1, \dots, \gamma_n)$ ce qui entraine $(\delta_1, \dots, \delta_n) + (\epsilon_1, \dots, \epsilon_n) \prec (\gamma_1, \dots, \gamma_n) + (\epsilon_1, \dots, \epsilon_n)$ d'où la conclusion voulue.

   Il reste à voir que $\preceq^h$ est bon mais cela découle du fait que pour tout $\delta \neq (0, \dots, 0)$, $|\delta| > 0 = |(0, \dots, 0)|$.

   (b) Ecrivons $p_i = \sum c_{\alpha,i} X^\alpha$ et $p = \sum c_\alpha X^\alpha$ (avec les notations habituelles). On a alors $f = \sum_\alpha (\sum_i c_{\alpha,i}) X^\alpha$ d'où $X_0^{\delta-d} h(f) = X_0^{\delta-d} \sum_\alpha (\sum_i c_{\alpha,i}) X_0^{d-|\alpha|} X^\alpha = \sum_\alpha (\sum_i c_{\alpha,i}) X_0^{\delta-|\alpha|} X^\alpha = \sum_i (\sum_\alpha c_{\alpha,i} X_0^{\delta-d_i} X_0^{d_i-|\alpha|} X^\alpha) = \sum_i X_0^{\delta-d_i} \sum_\alpha c_{\alpha,i} X_0^{d_i-|\alpha|} X^\alpha = \sum_i X_0^{\delta-d_i} h(p_i)$.

   (c) Soit $f = \sum c_\alpha X^\alpha$ de degré d et $g = \sum d_\alpha X^\alpha$ de degré e. Alors fg est de degré $d+e$ et $h(fg) = \sum_{\alpha,\beta} c_\alpha d_\beta X_0^{d+e-|\alpha|-|\beta|} X^{\alpha+\beta} = \sum_{\alpha,\beta} c_\alpha d_\beta X_0^{d-|\alpha|} X^\alpha X_0^{e-|\beta|} X^\beta = h(f)h(g)$.

   (d) Notons $q' = q(1, X_1, \dots, X_n)$.

   Ecrivons $q = \sum c_\beta X_0^{\beta_0} X_1^{\beta_1} \cdots X_n^{\beta_n}$ avec $\beta \in N^{1+n}$. Comme q est homogène, il existe $\delta \in \mathbb{N}$ tel que $\delta = \beta_0 + \cdots + \beta_n$ pour tout β tel que $c_\beta \neq 0$.

   Par définition de $\preceq$ (puisque tous les monômes de q ont le même degré), on obtient l'exposant dominant en prenant le max (pour $\preceq$) des $(\beta_1, \dots, \beta_n)$.

   Notons d le max des $\beta_1 + \cdots + \beta_n$. On a bien entendu $\delta \geq d$ (l'inégalité pouvant être stricte). On a alors $q = X_0^{\delta-d} h(q'))$. Cela montre que q et q' ont exactement le même nombre de monômes. De plus $q' = \sum c_\beta X_1^{\beta_1} \cdots X_n^{\beta_n}$. Ainsi le max des $(\beta_1, \dots, \beta_n)$ qui apparaissent est $\exp_{\preceq}(q')$ d'ou l'égalité voulue.

   (e) Soit $h_1, \dots, h_r$ une base de Gröbner de I^h pour $\preceq^h$. Pour chaque i, soit h_i' la composante homogène de h_i de plus haut degré. Par définition de $\preceq^h$, h_i' contient le monôme dominant de h_i, autrement dit $\mathrm{lm}(h_i) = \mathrm{lm}(h_i')$. De plus par 1(b), les h_i' sont dans I^h. Ils forment donc une base de Gröbner de I^h.

   (f) Soit $f \in I$, on peut donc l'écrire $f = \sum q_i f_i$. Notons d le degré de f et d_i celui de $q_i f_i$ et δ le maximum de tous ces degrés alors par 2(b), $X_0^{\delta-d} h(f) = \sum X_0^{\delta-d_i} h(q_i f_i)$ or par 2(c), $h(q_i f_i) = h(q_i) h(f_i)$ ce qui entraine que $X_0^{\delta-d} h(f)$ est une combinaison des $h(f_i)$.

   (g) L'élément q est une combinaison de $h(f_1), \dots, h(f_s)$. Or $h(f_i)_{|X_0=1} = f_i$ donc $q(1, X_1, \dots, x_n)$ est une combinaison des f_i.

(h) Par 2(e), soit $H = \{h_1, \dots, h_r\}$ une base de Gröbner de I^h constituée d'éléments homogènes. Notons $g_i = (h_i)_{|X_0=1}$. Par 2(g), on sait que $g_i \in I$. On note G l'ensemble des g_i.

Soit maintenant $f \in I$. Par 2(f), il existe un entier $k \geq 0$ tel que $f' := X_0^k h(f) \in I^h$.

Considérons une division de f' par les h_i relativement à $\preceq^h$: $f' = \sum q_i h_i$ avec $\mathrm{lm}(f) \succeq^h \mathrm{lm}(q_i h_i)$. Notons $(\alpha_0, \dots, \alpha_n)$ l'exposant dominant de f, $(\delta_{i,0}, \dots, \delta_{i,n})$ et $(\gamma_{i,0}, \dots, \gamma_{i,n})$ ceux de q_i et g_i (pour les q_i non nuls).

Par définition de $\preceq^h$, pour avoir le monôme dominant, on regarde les monômes de plus haut degré et parmi eux on "départage" à l'aide de $\preceq$. Cela signifie que $\deg(f) = \sum_0^n \alpha_i$ et idem pour $\deg(q_i)$ et $\deg(h_i)$. L'inégalité entre les monômes dominants entraine donc $\deg(f') \geq \deg(q_i h_i)$. Comme f' est homogène ainsi que les h_i, on peut (par identification) ne garder que les composantes homogènes de plus haut degré des q_i, autrement dit si on note $q_i = q_i' + q_i''$ avec q_i' la composante de plus haut degré de q_i alors $f' = \sum q_i' h_i$. On se retrouve avec une égalité ne faisant intervenir que des éléments homogènes f', les q_i' et les h_i. Par définition de $\preceq^h$, on a donc $(\alpha_1, \dots, \alpha_n) \succeq (\delta_{i,1}, \dots, \delta_{i,n}) + (\gamma_{i,1}, \dots, \gamma_{i,n})$. On fait $X_0 = 1$ et on obtient : $f = \sum t_i g_i$ où $t_i = (q_i')_{|X_0=1}$ et la question 2(d) nous donne l'inégalité voulue.

3. Soit $\preceq$ un ordre monomial sur $\mathbb{N}^n$ adapté au système de poids $w(\alpha_1, \dots, \alpha_n) = \alpha_1 + \cdots + \alpha_n$. On le définit ainsi. On fixe d'abord un bon ordre monomial $\preceq_0$, puis on définit $\preceq$ à l'aide de l'équivalence suivante : $\alpha \preceq \beta \iff |\alpha| < |\beta|$ ou ($|\alpha| = |\beta|$ et $\alpha \prec_0 \beta$).

   Soit alors $G = g_1, \dots, g_r$ une base de Gröbner de I pour cet ordre. Soit $f \in I$. Par division, on écrit $f = \sum q_i g_i$ avec $\mathrm{lm}(f) \succeq \mathrm{lm}(q_i g_i)$. Par définition de $\preceq$ on a $\deg(f) \geq \deg(q_i g_i)$. En utilisant les questions 2(b) et 2(c), on obtient alors $h(f) = \sum X_0^{\deg(f)-d_i} h(q_i) h(g_i)$ où $d_i = \deg(q_i g_i)$. Cela signifie que $h(I)$ est engendré par les $h(g_i)$.