1 Reduction d'un polynôme modulo un ideal

1.1 Ordonner les monômes - Réduction d'un polynôme

Définition 1. *$\mathbb{K}$ est un corps commutatif. Un ordre monomial sur $\mathbb{K}[X_1, ..., X_n]$ est une relation $>$ sur $\mathbb{Z}^n_{\geqslant 0}$ ou, de façon équivalente sur l'ensemble des monômes $X^\alpha, \alpha \in \mathbb{Z}^n_{\geqslant 0}$, tel que:*

i. $>$ est un ordre total sur $\mathbb{Z}^n_{\geqslant 0}$

ii. Si $\alpha > \beta$ et $\gamma \in \mathbb{Z}^n_{\geqslant 0}$, alors $\alpha + \gamma > \beta + \gamma$

iii. $>$ est un bel ordre *: si $A \subset \mathbb{Z}^n_{\geqslant 0}$, $A \neq \emptyset \Rightarrow$ A admet un plus petit élément pour $>$ c'est à dire $\exists \alpha_A \in A$ tq $\forall \alpha \in A$, $\alpha \neq \alpha_A \Rightarrow \alpha > \alpha_a$*

1) Monter qu'une relation $>$ sur $\mathbb{Z}^n_{\geqslant 0}$ est un bel ordre si et seulement si toute suite strictement décroissante $\alpha_1 > \alpha_2 > ...$ est finie.

1) Si $>$ n'est pas un bel ordre, alors on peut construire une suite infinie $\alpha(1) > \alpha(2) > ....$ On prend un sous-ensemble de cardinal infini $S \subset \mathbb{Z}^n_{\geqslant 0}$ et on choisit arbitrairement $\alpha(1)$. Comme S n'a pas de plus petit élément, on peut alors trouver $\alpha(2)$ tel que $\alpha(1) > \alpha(2)$. Par le même procédé on construit une suite infinie $\alpha(1) > \alpha(2) > ....\alpha(i) > ....$

Inversement Si on se donne une suite infinie strictement décroissante, elle n'a fatalement pas de plus petit élément.

2) On considère l'ordre suivant : $\alpha = (\alpha_1, ..., \alpha_n) >_{\text{lex}} \beta = (\beta_1, ..., \beta_n)$ (ou $X^\alpha = X_1^{\alpha_1} ... X_n^{\alpha_n} >_{\text{lex}} X^\beta = X_1^{\beta_1} ... X_n^{\beta_n}$) si et seulement si la coordonnée non nulle de plus petit indice de $\alpha - \beta \in \mathbb{Z}^n$ est positive, c'est à dire $\alpha - \beta = \left(0, ..., 0, \underbrace{\alpha_i - \beta_i}_{>0}, \alpha_{i+1} - \beta_{i+1}, ..., \alpha_n - \beta_n\right)$.

Montrer que $>_{\text{lex}}$ est un ordre monomial.

2) Les points i) et ii) sont évidents.

Pour le point iii) on prend un élément $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{Z}^n_{\geqslant 0}$ et on remarque que $\beta < \alpha$ est forcément pris dans le sous ensemble de $\mathbb{Z}^n_{\geqslant 0}$ des points $\beta = (\beta_1, ..., \beta_n)$ avec $\beta_1 \leqslant \alpha_1$. Comme $\mathbb{Z}_{\geqslant 0}$ est un bel ordre, l'ensemble des premières coordonnées d'un ensemble $S \subset \mathbb{Z}^n_{\geqslant 0}$ admet une plus petit élément que nous noterons α_1^0. On ne garde alors dans S que les éléments dont la première corrdonnée est α_1^0 (il y en a forcément car $>$ est un bel ordre sur $\mathbb{Z}_{\geqslant 0}$) puis on définit alors de la même manière α_2^0 et ainsi de suite jusqu'à α_n^0. On vérifie alors simplement que $(a_1^0, ..., a_n^0)$ est le plus petit élément de S pour $<_{\text{lex}}$.

Remarque 2. Un autre ordre monomial très utilisé est l'ordre du degré lexicographique renversé : : $\alpha = (\alpha_1, ..., \alpha_n) >_{\text{drl}} \beta = (\beta_1, ..., \beta_n)$ si $\sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i$ ou si $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ et la coordonnée non nulle de plus grand indice de $\alpha - \beta \in \mathbb{Z}^n$ est négative, c'est à dire $\alpha - \beta = \left(\alpha_1 - \beta_1, ..., \alpha_{i-1} - \beta_{i-1}, \underbrace{\alpha_i - \beta_i}_{<0}, 0, ..., 0\right)$.

Définition 3. *$\mathbb{K}$ est un corps commutatif. On se donne un ordre monomial $>$ sur $\mathbb{K}[X_1, ..., X_n]$. Pour tout $p = \sum_\alpha a_\alpha X^\alpha \in \mathbb{K}[X_1, ..., X_n]$:*

- *Le multidegré de p :* $\text{multideg}_<(p) = \max(\alpha \in \mathbb{Z}^n_{\geqslant 0}, a_\alpha \neq 0)$
- *Le coefficient de tête de p :* $\text{Lc}_<(p) = a_{\text{multideg}_<(p)} \in \mathbb{K}$
- *Le monôme de tête de p :* $\text{Lm}_<(p) = X^{\text{multideg}_<(p)}$

- *Le terme de tête de p :* $\mathrm{Lt}_<(p) = \mathrm{Lc}_<(p)\,\mathrm{Lm}_<(p)$

3) Montrer qu'en fixant un ordre monomial $>$, on peut adapter l'algorithme de division Euclidienne dans $\mathbb{K}[X]$ pour réaliser la réduction d'un polynôme par un autre dans $\mathbb{K}[X_1, ..., X_n]$ pour $>$, puis d'un polynôme par une famille de polynômes.

Plus précisément, montrer que l'on peut proposer un agorithme $\mathrm{Reduction}_>(f, [f_1, ..., f_s])$ qui, pour un ordre monomial fixé $>$, étant donnés $f, f_1, ..., f_s \in \mathbb{K}[X_1, ..., X_n]$, permet de calculer explicitement $r, q_1, ..., q_s$ tels que

- $f = q_1 f_1 + ... + q_s f_s + \mathrm{r}$
- soit $r = 0$ soit $r = \sum_{\alpha \in \mathbb{Z}^n_{\geqslant 0}} r_\alpha X^\alpha$ ou aucun des X^α n'est divisible par l'un des $\mathrm{Lt}_<(f_i), i = 1...s$
- si $q_i f_i \neq 0$ alors $\mathrm{multideg}(f) \geqslant \mathrm{multideg}(f_i q_i)$

Algorithme de Reduction Totale

Entrée : $f, \{f_1, ..., f_s\}, >$
Sortie : $q_1, ..., q_s, r$

$q_1 := 0; ..., q_s := 0; r := 0;$
$p := f;$

Tant que p$\neq$0
  $i := 1$
  simplifié:=faux
  Tant que ($i \leqslant s$) et (simplifié=faux)
    Si $\mathrm{Lt}_>(f_i)$ divise $\mathrm{Lt}_>(p)$ alors
      $q_i := q_i + \frac{\mathrm{Lt}_>(p)}{\mathrm{Lt}_>(f_i)}$
      $p := p - \left(\frac{\mathrm{Lt}_>(p)}{\mathrm{Lt}_>(f_i)}\right) f_i$
      simplifié:=vrai
    Sinon
      $i := i + 1$
  Si Simplifié=faux alors
    $r := r + \mathrm{Lt}_>(p)$
    $p := p - \mathrm{Lt}_>(p)$
Renvoyer $q_1, ..., q_s, r$

4) Appliquer l'algorithme de la question précédente avec $f = x\,y^2 - x$, la famille $F = [f_1, f_2]$ ou $f_1 = x\,y - 1$, $f_2 = y^2 - 1$ pour lordre lexicographique $>_{\mathrm{lex}}$ tel que $x >_{\mathrm{lex}} y$, puis refaire le calcul en posant $F = [f_2, f_1]$.

4) $x\,y^2 - x = y(x\,y - 1) + 0\,(y^2 - 1) + (-x + y)$

$x\,y^2 - x = x\,(y^2 - 1) + 0\,(x\,y - 1) + 0$

2 Idéaux de Monômes

Définition 4. *On dit qu'un idéal est un idéal de monômes si il est engendré par des monômes ou, autrement dit, il existe $A \subset \mathbb{Z}^n_{\geqslant 0}$ tel que $f \in I \Rightarrow f = \sum_{\alpha \in A} h_\alpha X^\alpha$ avec $h_\alpha \in \mathbb{K}[X_1, ..., X_n]$.*

1) Soit $I = \langle X^\alpha, \alpha \in A \rangle$ un idéal de monômes. Montrer que $X^\beta \in I$ si et seulement si il existe $\alpha \in A$ tel que X^α divise X^β.

1)si X^α divise X^β alors $X^\beta \in I$ par définition de I

Supposons $X^\beta \in I$. Alors, $X^\beta = \sum_{i=1}^s h_i\, X^{\alpha_i}$ avec $h_i \in \mathbb{K}[X_1, \ldots, X_n]$ et $\alpha_i \in A$. En posant $h_i = \sum_j c_{i,j} X^{\beta_{i,j}}$, il vient que $X^\beta = \sum_{i=1}^s \sum_j c_{i,j} X^{\beta_{i,j}} X^{\alpha_i}$. En regroupant les termes de la somme de droite de même multi-degré, tous divisibles par un α_i et en identifiant les parties droites et gauche de l'équation, on obtient que X^β est divisible par au moins 1 $\alpha_i \in A$.

2) Soit I un idéal de monômes de $\mathbb{K}[X_1, \ldots, X_n]$. Montrer que les 3 points suivants sont équivalents

i. $f \in I$

ii. tous les termes de f sont dans I

iii. f est une combinaison $\mathbb{K}$-linaire de monômes de I

2) on a clairement iii $\Rightarrow$ ii $\Rightarrow i$. Supposons que $f \in I$.

Alors, par définition, $f = \sum_{\alpha \in A} h_\alpha X^\alpha = \sum_{\alpha \in A} (\sum_\beta a_{\alpha,\beta}\, X^\beta) X^\alpha = \sum_{\alpha \in A} \sum_\beta a_{\alpha,\beta}\, X^\beta\, X^\alpha$ avec $X^\beta X^\alpha \in I$ d'après 1).

3) En déduire que 2 idéaux de monômes sont identiques si et seulement si ils contiennent les mêmes monômes.

3) Conséquence directe du 2)

Définition 5. *Soient $f, g \in \mathbb{K}[X_1, \ldots, X_n]$ deux polynômes et $>$ un ordre monomial sur $\mathbb{K}[X_1, \ldots, X_n]$.*

i. Supposant $\mathrm{multideg}(f) = \alpha = (\alpha_1, \ldots, \alpha_n)$ *et* $\mathrm{multideg}(g) = \beta = (\beta_1, \ldots, \beta_n)$*, on définit le plus petit comun multiple de* $\mathrm{Lm}_>(f)$ *et* $\mathrm{Lm}_>(g)$ *par* X^γ *avec* $\gamma = (\max(\alpha_1, \beta_1), \ldots, \max(\alpha_n, \beta_n))$

ii. $S_>(f, g) = \frac{X^\gamma}{\mathrm{Lt}_>(f)} f - \frac{X^\gamma}{\mathrm{Lt}_>(g)} g$ *, le S-polynôme de f et g.*

4) Soient $p_1, \ldots, p_m \in \mathbb{K}[X_1, \ldots, X_n]$ tels que $\mathrm{multideg}_>(p_i) = \delta \in \mathbb{N}^\star$ et $h = \sum_{i=1}^m p_i$. Alors $\mathrm{multideg}_>(h) < \delta \Rightarrow$ h est une combinaison K-linéaire des polynômes $S_>(p_i, p_j)$. De plus, $\mathrm{multideg}_>(S_>(p_i, p_j)) < \delta$.

4)Comme $\mathrm{multideg}_>(p_i) = \delta$, $S_>(p_1, p_2) = \frac{1}{\mathrm{Lc}_>(p_1)} p_1 - \frac{1}{\mathrm{Lt}_>(p_2)} p_2$ et donc $p_1 = \mathrm{Lc}_>(p_1)\Big(S_>(p_1, p_2) + \frac{1}{\mathrm{Lc}_>(p_2)} p_2\Big)$. Ainsi $p_1 + p_2 = \mathrm{Lc}_>(p_1) S_>(p_1, p_2) + (\mathrm{Lc}_>(p_1) + \mathrm{Lc}_>(p_2)) \frac{p_2}{\mathrm{lc}_>(p_2)}$.

De proche en proche, $\sum_{i=1}^{m-1} p_i = \sum_{i=1}^{m-1} (\sum_{j=1}^i \mathrm{Lc}_>(p_j))\, S(p_i, p_{i+1}) + (\sum_{i=1}^{m-1} \mathrm{Lc}_>(p_i)) \frac{p_m}{\mathrm{Lc}_>(P_m)}$.

Or si $\mathrm{multideg}_>(h) < \delta$, necessairement $\sum_{i=1}^m \mathrm{Lc}_>(p_i) = 0$ et en particulier $(\sum_{i=1}^{m-1} \mathrm{Lc}_>(p_i)) = -\mathrm{Lc}_>(p_m)$ et donc $\sum_{i=1}^{m-1} p_i = \sum_{i=1}^{m-1} (\sum_{j=1}^i \mathrm{Lc}_>(p_j))\, S(p_i, p_{i+1}) - p_m$ ce qui donne $\sum_{i=1}^m p_i = \sum_{i=1}^{m-1} (\sum_{j=1}^i \mathrm{Lc}_>(p_j))\, S(p_i, p_{i+1})$ car $S_>(p_1, p_2) = \frac{1}{\mathrm{Lc}_>(p_1)} p_1 - \frac{1}{\mathrm{Lt}_>(p_2)} p_2$.

5) Soient $G = \{g_1, \ldots, g_s\} \subset \mathbb{K}[X_1, \ldots, X_n]$ et $>$ un ordre monomial. Posons $I = \langle G \rangle$. Supposons que $\forall i = 1 \ldots s, \forall j = 1 \ldots s$, $\mathrm{Reduction}_>(S_>(g_i, g_j), G) = 0$.

5)a) Soit $f \in I$. Justifier que l'on peut choisir une décomposition $f = \sum_{i=1}^s h_i\, g_i$ de sorte à ce que $\delta = \max(\mathrm{multideg}_>(h_i\, g_i), h_i g_i \neq 0)$ soit minimal. En déduire que si $\mathrm{multideg}_>(f) = \delta$, alors $\mathrm{Lt}_>(f) \in \langle \mathrm{Lt}_>(g_1), \ldots, \mathrm{Lt}_>(g_s) \rangle$.

5)a) le δ minimal existe par définition d'un ordre monomial. Si $\mathrm{multideg}_>(f) = \delta$, alors $\exists i$, $\mathrm{multideg}_>(f) = \mathrm{multideg}(h_i g_i)$

5)b) Montrer que $\mathrm{multideg}_>(f) < \delta$ si et seulement si $\mathrm{multideg}_>\big(f_\delta = \sum_{\mathrm{multideg}(h_i g_i) = \delta} \mathrm{Lt}_>(h_i)\, g_i\big) < \delta$ et que dans ce cas f_δ une combinaison $\mathbb{K}$-linéaire de polynômes de la forme $X^{\delta - \gamma_{i,j}} S(g_i, g_j)$ avec $X^{\gamma_{i,j}} = \mathrm{ppcm}(\mathrm{Lm}_>(g_i), \mathrm{Lm}_>(g_j))$.

5)b) $f = \underbrace{\sum_{\text{multideg}_>(h_i g_i)=\delta} \text{Lt}_>(h_i)\, g_i}_{f_\delta} + \underbrace{\sum_{\text{multideg}_>(h_i g_i)=\delta} (h_i - \text{Lt}_>(h_i))\, g_i}_{\text{multideg}_<\delta} + \underbrace{\sum_{\text{multideg}_>(h_i g_i)<\delta} h_i\, g_i}_{\text{multideg}_<\delta}$

D'après 4) $f_\delta = \sum_{i,j} c_{i,j} S(\text{Lt}_>(h_i)\, g_i, \text{Lt}_>(h_j)\, g_j) = \sum_{i,j} c_{i,j} X^{\delta-\gamma_{i,j}} S(g_i, g_j)$. On remarque alors que $\text{lcm}\,(\text{Lm}(\text{Lt}_>(h_i)\, g_i), \text{lm}(\text{Lt}_>(h_j)\, g_j)) = X^\delta$ si bien que $S(\text{Lt}_>(h_i)\, g_i, \text{Lt}_>(h_j)\, g_j) = \frac{X^\delta}{X^{\gamma_{i,j}}} S(g_i, g_j)$.

5)c) En déduire que l'on ne peut pas avoir $\text{multideg}_>(f) < \delta$.

5)c) En utilisant l'algorithme de réduction, il vient que $S(g_i,\ g_j) = \sum_{l=1}^{s} A_l\ g_l$ avec $\text{multideg}_>(A_l\ g_l) \leqslant \text{multideg}_>(S(g_i,\ g_j))$. En multipliant par $X^{\delta-\gamma_{i,j}}$, on a alors $S(\text{Lt}_>(h_i)\ g_i, \text{Lt}_>(h_j)\ g_j) = \sum_{l=1}^{s} X^{\delta-\gamma_{i,j}} A_l\, g_l$ et en particulier $\text{multideg}_>(f_\delta) \leqslant \text{multideg}(X^{\delta-\gamma_{i,j}}\, S(g_i, g_j)) < \delta$ puisque $\text{Lt}_>(S(g_i, g_j)) < \text{lcm}\,(\text{Lm}_>(g_i), \text{Lm}_>(g_j))$.

Ainsi, $f_\delta = \sum_{l=1}^{s} B_l\ g_l$ avec $\text{multideg}_>(B_l\ g_l) < \delta$ et par la même occasion $f = \sum_{l=1}^{u} C_l\ g_l$ avec $\text{multideg}_>(C_l\, g_l) < \delta$, ce qui contredit le choix de δ.

5)d) Soient $G = \{g_1, \ldots, g_s\} \subset \mathbb{K}[X_1, \ldots, X_n]$ et $>$ un ordre monomial. Posons $I = \langle G \rangle$. Alors $\langle \text{Lt}_>(I) \rangle = \langle \text{Lt}_>(g_1), \ldots, \text{Lt}_>(g_s) \rangle$ si et seulement si $\forall i = 1 \ldots s, \forall j = 1 \ldots s$, $\text{Reduction}_>(S_>(g_i, g_j), G) = 0$.

5)d) Supposons que $\langle \text{Lt}_>(I) \rangle = \langle \text{Lt}_>(g_1), \ldots, \text{Lt}_>(g_s) \rangle$. Comme $r_{i,j} = \text{Reduction}_>(S_>(g_i, g_j), G) \in I$, alors $\text{Lt}_>(r_{i,j}) \in \langle \text{Lt}_>(g_1), \ldots, \text{Lt}_>(g_s) \rangle$ et donc soit $r_{i,j} = 0$, soit $\exists i, \text{Lt}_>(g_i)$ divise $\text{Lt}_>(r_{i,j})$ ce qui est impossible puisque $r_{i,j}$ est réduit.

Supposons maintenant que $\forall i = 1 \ldots s, \forall j = 1 \ldots s$, $\text{Reduction}_>(S_>(g_i, g_j), G) = 0$. Alors d'après le 5)d) si $f \in I$, $\text{Lt}_>(f) \in \langle \text{Lt}_>(g_1), \ldots, \text{Lt}_>(g_s) \rangle$ ce qui montre que $\langle \text{Lt}_>(I) \rangle \subset \langle \text{Lt}_>(g_1), \ldots, \text{Lt}_>(g_s) \rangle$ et donc que $\langle \text{Lt}_>(I) \rangle = \langle \text{Lt}_>(g_1), \ldots, \text{Lt}_>(g_s) \rangle$ puisque $g_1, \ldots, g_s \in I$.

3 Bases de Gröbner

Définition 6. *Soit $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{K}[X_1, \ldots, X_n]$ et $>$ un ordre monomial. On dit que $G = \{g_1, \ldots, g_t\} \subset I \neq \{0\}$ est une base de Gröbner de I pour $>$ si $\langle \text{Lt}_>(I) \rangle = \langle \text{Lt}_>(g_1), \ldots, \text{Lt}_>(g_t) \rangle$.*

Algorithme de Buchberger

Entrée : $F = (f_1, \ldots, f_s)$
Sortie : $G = (g_1, \ldots, g_t)$
$G := F$
Répéter
  $G' := G$
  Pour toute paire $\{p, q\}, p \neq q$ de G'
    r:=$\text{Reduction}_>(S_>(p, q), G')$
    Si $r \neq 0$ $G = G \cup \{r\}$
Jusqu'à ce que $G = G'$
Renvoyer G

1) Montrer que le programme ci dessus termine en un nombre fini d'étapes.

1) Après 1 tour de boucle, soit $G' = G$ et l'algorithme s'arrête, soit $G' \subsetneq G = G' \cup \{r\}$. Comme r n'est réductible par aucun des éléments de G', $\text{Lt}_>(r)$ n'est divisible par aucun élément de $\text{Lt}_>(G')$ et donc, d'après la question 1) $\text{Lt}_>(r) \notin \langle \text{Lt}_>(G') \rangle$ ce qui montre que $\langle \text{Lt}_>(G') \rangle \subsetneq \langle \text{Lt}_>(G) \rangle$.

Ainsi, chaque passage dans la boucle augmente une suite croissante d'idéaux $\langle \text{Lt}_>(G) \rangle$ qui sera donc stationnaire au bout d'un certain temps par Noetherianité de $\mathbb{K}[X_1, \ldots, X_n]$, impliquant la sortie de la boucle et donc la terminaison de l'algorithme.

2) Montrer que $\langle f_1, ..., f_s \rangle = \langle g_1, ..., g_t \rangle$

2) Par construction, on a $(f_1, ..., f_s) \subset (g_1, ..., g_t)$ ce qui implique $\langle f_1, ..., f_s \rangle \subset \langle g_1, ..., g_t \rangle$. D'autre part si $p, q \in G$, alors $S_>(p, q) \in \langle G \rangle$ et $\text{Reduction}_>(S_>(p, q), G) \in \langle G \rangle$ si bien que $\langle G \rangle \subset \langle f_1, ..., f_s \rangle$ à tout moment. Ainsi $\langle g_1, ..., g_t \rangle \subset \langle f_1, ..., f_s \rangle$.

3) Montrer que $r = \text{Reduction}_>(f, [g_1, ..., g_t])$ est unique, c'est à dire qu'il est indépendant de l'ordre dans lequel les g_i sont considérés dans l'algorithme de réduction. En déduire que $\text{Reduction}_>(f, \{g_1, ..., g_t\}) = 0$ si et seulement si $f \in \langle f_1, ..., f_s \rangle$.

3) Par construction, aucun des termes de r n'est divisible plar l'un des $\text{Lt}_>(g_i)$ et $\exists g = \sum_{i=1}^{s} q_i\, g_i \in I$, $f = g + r$. Supposons $f = g' + r' = g + r$. Alors comme $g - g' \in I$, $r - r' \in I$. Ainsi, si $r - r' \neq 0$, alors $\text{Lt}_>(r - r') \in \langle \text{Lt}_>(I) \rangle = \langle \text{Lt}_>(g_1), ..., \text{Lt}_>(g_t) \rangle$ ce qui implique que $r - r'$ est réductible par l'un des g_i, ce qui est impossible puisque $r - r'$ est constitué de termes irréductibles. La dernière assertion est une conséquence directe.