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.

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.

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 $\alpha - \beta = \Big($ $\alpha_1 - \beta_1$, ..., $\alpha_{i-1} - \beta_{i-1}, \underbrace{\alpha_i - \beta_i}_{<0}, 0, ..., 0\Big)$.

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 :* $\text{Lt}_<(p) = \text{Lc}_<(p)\,\text{Lm}_<(p)$

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 $\text{Reduction}_>(f, [f_1, ..., f_s])$ 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

- $f = q_1 f_1 + ... + q_s f_s + \text{r}$
- 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 $\text{Lt}_<(f_i), i = 1...s$
- si $q_i f_i \neq 0$ alors $\text{multideg}(f) \geqslant \text{multideg}(f_i q_i)$

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 $>_{\text{lex}}$ tel que $x >_{\text{lex}} y$, puis refaire le calcul en posant $F = [f_2, f_1]$.

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.

2) Soit I un idéal de monômes de $\mathbb{K}[X_1, ..., X_n]$. 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

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

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

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

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

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

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

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 $\delta = \max(\text{multideg}_>(h_i\, g_i), h_i g_i \neq 0)$ soit minimal. En déduire que si $\text{multideg}_>(f) = \delta$, alors $\text{Lt}_>(f) \in \langle \text{Lt}_>(g_1), ..., \text{Lt}_>(g_s) \rangle$.

5)b) Montrer que $\text{multideg}_>(f) < \delta$ si et seulement si $\text{multideg}_>\big(f_\delta = \sum_{\text{multideg}(h_i g_i) = \delta} \text{Lt}_>(h_i)\, g_i\big) < \delta$ 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 $X^{\gamma_{i,j}} = \text{ppcm}(\text{Lm}_>(g_i), \text{Lm}_>(g_j))$.

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

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

3 Bases de Gröbner

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

Algorithme de Buchberger

Entrée : $F = (f_1, ..., f_s)$
Sortie : $G = (g_1, ..., g_t)$
$G := F$
Répéter
    $G' := G$
    Pour toute paire $\{p, q\}, p \neq q$ de G'
        r:=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.

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

3) Montrer que $r =$ 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 Reduction$_>(f,$ $\{g_1, ..., g_t\}) = 0$ si et seulement si $f \in \langle f_1, ..., f_s \rangle$.