DM d'Algorithmique 2

Younesse Kaddar

- Version PDF
- http://younesse.net/Algorithmique/DM_Algo2/

I. Ordre bien fondé

1.

Soient $F \subseteq E$ où E est doté d'un ordre $\preccurlyeq$ bien fondé, $f \in F$.

Montrons qu'il existe f^* minimal tel que

$$f^* \preccurlyeq f$$

Par l'absurde : supposons que pour tout $f' \in F$ tel que $f' \preccurlyeq f$, il existe $f'' \in F$ tel que $f'' \prec f'$.

Comme $f \preccurlyeq f$ (par réflexivité), il existe donc $f_0 \in F$ tel que $f_0 \prec f$.

Et de même, comme $f_0 \preccurlyeq f$, il existe $f_1 \in F$ tel que $f_1 \prec f_0 \prec f$.

Par une récurrence immédiate, on construit donc une suite $(f_n)_{n\in\mathbb{N}} \in F^{\mathbb{N}}$ telle que : $\forall n \in \mathbb{N}$,

$$f_n \prec f_{n-1} \prec \cdots \prec f_0 \prec f$$

En particulier : $(f_n)_{n\in\mathbb{N}}$ est strictement décroissante, ce qui contredit le fait que $\preccurlyeq$ soit bien fondé.

On a donc montré que

> Si $F \subseteq E$ où E est doté d'un ordre $\preccurlyeq$ bien fondé, et $f \in F$: il existe $f^* \in F$ minimal tel que
>
> $$f^* \preccurlyeq f$$

2.

Soit $\prec$ un ordre monomial sur $\mathbb{N}^n$, c'est-à-dire que :

1. $\prec$ est *total*
2. pour tous $\alpha, \beta, \gamma \in \mathbb{N}^n$,
$$\alpha \prec \beta \Longrightarrow \alpha + \gamma \prec \beta + \gamma$$
3. $\prec$ est *bien fondé*

Montrons que pour tout $\alpha \neq \mathbf{0} \in \mathbb{N}^n$,

$$\mathbf{0} \prec \alpha$$

Remarquons que comme $\prec$ est **total**, cela revient à montrer que $\mathbf{0}$ est minimal.

- *en effet* :

$$\begin{aligned} \nexists \alpha \in \mathbb{N}^n;\ \alpha \prec \mathbf{0} &\iff \nexists \alpha \in \mathbb{N}^n;\ \mathbf{0} \not\preccurlyeq \alpha && (\text{ car l'ordre est total}) \\ &\iff \forall \alpha \in \mathbb{N}^n,\ \mathbf{0} \preccurlyeq \alpha \\ &\iff \forall \alpha \in \mathbb{N}^n \backslash \{\mathbf{0}\},\ \mathbf{0} \prec \alpha && (\text{ par réflexivité}) \end{aligned}$$

Par l'absurde : supposons que $\mathbf{0}$ n'est pas minimal.

Alors il existe $\alpha \in \mathbb{N}^n$ tel que

$$\underbrace{\alpha}_{\text{noté } \alpha_1} \prec \mathbf{0}$$

Par suite, comme $\prec$ est monomial : $\forall m \in \mathbb{N}^*$,

$$\underbrace{(m+1)\alpha}_{\text{noté } \alpha_{m+1}} = \alpha + m\alpha \prec \mathbf{0} + m\alpha = \underbrace{m\alpha}_{\text{noté } \alpha_m}$$

On a donc construit une suite $(\alpha_m)_{m\in\mathbb{N}^*}$ strictement décroissante, ce qui contredit le caractère bien fondé de $\prec$.

On a donc montré que :

> Si $\prec$ est un ordre monomial, pour tout $\alpha \neq \mathbf{0} \in \mathbb{N}^n$:

$$\mathbf{0} \prec \alpha$$

3.

NB : On supposera qu'on dénote, par convention :

- $\prec_{lex}$ et $\prec_{grlex}$ les ordres stricts (qui ne sont pas des ordres, puisque non réflexifs)
- $\preccurlyeq_{lex}$ et $\preccurlyeq_{grlex}$ les ordres larges

---

$$\preccurlyeq_{lex} \text{ est monomial.}$$

1. $\preccurlyeq_{lex}$ est clairement *total*, puisque $\leq$ l'est.
2. Soient $\alpha, \beta, \gamma \in \mathbb{N}^n$ tels que $\alpha \preccurlyeq_{lex} \beta$. Montrons que

   $$\alpha + \gamma \preccurlyeq_{lex} \beta + \gamma$$

   Comme $\alpha \preccurlyeq_{lex} \beta$:
   - *soit* $\alpha = \beta$, auquel cas le résultat est acquis par réflexivité.
   - *soit* il existe i tel que
     - $\alpha_i < \beta_i$
     - $\forall j < i, \alpha_j = \beta_j$

     auquel cas, pour ce même i :
     - $\alpha_i + \gamma_i < \beta_i + \gamma_i$
     - $\forall j < i, \alpha_j + \gamma_j = \beta_j + \gamma_j$

     ce qui conclut.
3. $\preccurlyeq_{lex}$ est *bien fondé* :
   Par l'absurde, supposons qu'il existe une suite $(\alpha^{(i)})_{i\in\mathbb{N}}$ strictement décroissante pour $\preccurlyeq_{lex}$.
   Alors pour tout $i \in \mathbb{N}$, il existe $k_i \in [\![1, n]\!]$ tel que

   $$\alpha^{(i+1)}_{k_i} < \alpha^{(i)}_{k_i}$$

   c'est-à-dire (comme $(\alpha^{(i)})_{i\in\mathbb{N}}$ est décroissante) :

   $$\forall i' > i, \quad \alpha^{(i')}_{k_i} < \alpha^{(i)}_{k_i}$$

   Donc comme $(k_i)_{i\in\mathbb{N}}$ est à valeurs dans l'ensemble **fini** $[\![1, n]\!]$, il existe (par le principe des tiroirs) $j \in [\![1, n]\!]$ tel que :

   $$K_j \overset{\text{def}}{=} \{i \in \mathbb{N} \mid k_i = j\}$$

   est infini.
   La suite $(\alpha^{(i)}_j)_{i\in K_j}$ est donc strictement décroissante, car :

   $$\forall i < i' \in K_j, \ \ \alpha^{(i')}_j \leq \alpha^{(i+1)}_j = \alpha^{(i+1)}_{k_i} < \alpha^{(i)}_{k_i} = \alpha^{(i)}_j$$

   ce qui est impossible, puisque $<$ est bien fondé.

$$\preccurlyeq_{grlex} \text{ est monomial.}$$

Montrons déjà que $\preccurlyeq_{grlex}$ est un ordre :

- la réflexivité de $\preccurlyeq_{grlex}$ est héritée de celles de $=$ et de $\preccurlyeq_{lex}$.

- $\preccurlyeq_{grlex}$ *est antisymétrique* :
  si $\alpha, \beta \in \mathbb{N}^n$ sont tels que $\alpha \preccurlyeq_{grlex} \beta$ et $\beta \preccurlyeq_{grlex} \alpha$:
  - alors $\sum_{i\leq n} \alpha_i < \sum_{i\leq n} \beta_i$ est impossible
    - *car sinon*, de $\beta \preccurlyeq_{grlex} \alpha$, on tire $\sum_{i\leq n} \alpha_i = \sum_{i\leq n} \beta_i$

    d'où, comme $\alpha \preccurlyeq_{grlex} \beta$:

    $$\sum_{i\leq n} \alpha_i = \sum_{i\leq n} \beta_i \text{ et } \beta \preccurlyeq_{lex} \alpha$$

  - de même, de $\beta \preccurlyeq_{grlex} \alpha$, on tire :

    $$\sum_{i\leq n} \beta_i = \sum_{i\leq n} \alpha_i \text{ et } \alpha \preccurlyeq_{lex} \beta$$

  donc $\alpha = \beta$, par antisymétrie de $\preccurlyeq_{lex}$.

- $\preccurlyeq_{grlex}$ *est transitive* :
  si $\alpha, \beta, \gamma \in \mathbb{N}^n$ sont tels que $\alpha \preccurlyeq_{grlex} \beta$ et $\beta \preccurlyeq_{grlex} \gamma$:

- alors *si* $\sum_{i\leq n}\alpha_i < \sum_{i\leq n}\beta_i$, dans tous les cas :

$$\sum_{i\leq n}\alpha_i < \sum_{i\leq n}\gamma_i, \text{ d'où } \alpha \preccurlyeq_{grlex} \gamma$$

- *sinon si* $\sum_{i\leq n}\alpha_i = \sum_{i\leq n}\beta_i$ *et* $\alpha \preccurlyeq_{lex} \beta$:
  - et si $\sum_{i\leq n}\beta_i < \sum_{i\leq n}\gamma_i$: *alors* $\sum_{i\leq n}\alpha_i < \sum_{i\leq n}\gamma_i$, d'où $\alpha \preccurlyeq_{grlex} \gamma$
  - et si $\sum_{i\leq n}\beta_i = \sum_{i\leq n}\gamma_i$ et $\beta \preccurlyeq_{lex} \gamma$: *alors* $\sum_{i\leq n}\alpha_i = \sum_{i\leq n}\gamma_i$ et $\alpha \preccurlyeq_{lex} \gamma$ (par transitivité de $\preccurlyeq_{lex}$), d'où $\alpha \preccurlyeq_{grlex} \gamma$

il vient que $\alpha \preccurlyeq_{grlex} \gamma$.

Montrons que $\preccurlyeq_{grlex}$ est monomial :

1. $\preccurlyeq_{grlex}$ est *total* :
   Pour tous $\alpha, \beta \in \mathbb{N}^n$:
   - *Cas 1* : $\sum_{i\leq n}\alpha_i < \sum_{i\leq n}\beta_i$
     alors
     $$\alpha \preccurlyeq_{grlex} \beta$$
   - *Cas 2* : $\sum_{i\leq n}\beta_i < \sum_{i\leq n}\alpha_i$
     alors
     $$\beta \preccurlyeq_{grlex} \alpha$$
   - *Cas 3* : $\sum_{i\leq n}\alpha_i = \sum_{i\leq n}\beta_i$
     alors comme $\preccurlyeq_{lex}$ est total :
     $$\alpha \preccurlyeq_{lex} \beta, \text{ d'où } \alpha \preccurlyeq_{grlex} \beta \qquad \text{OU} \qquad \beta \preccurlyeq_{lex} \alpha, \text{ d'où } \beta \preccurlyeq_{grlex} \alpha$$
2. Soient $\alpha, \beta, \gamma \in \mathbb{N}^n$ tels que $\alpha \preccurlyeq_{grlex} \beta$. Montrons que
   $$\alpha + \gamma \preccurlyeq_{grlex} \beta + \gamma$$
   - *Si* $\sum_{i\leq n}\alpha_i < \sum_{i\leq n}\beta_i$:
     alors $\sum_{i\leq n}\alpha_i + \gamma_i < \sum_{i\leq n}\beta_i + \gamma_i$, et
     $$\alpha + \gamma \preccurlyeq_{grlex} \beta + \gamma$$
   - *Si* $\sum_{i\leq n}\alpha_i = \sum_{i\leq n}\beta_i$ et $\alpha \preccurlyeq_{lex} \beta$:
     alors $\sum_{i\leq n}\alpha_i + \gamma_i = \sum_{i\leq n}\beta_i + \gamma_i$ et $\alpha + \gamma \preccurlyeq_{lex} \beta + \gamma$ (par monomialité de $\preccurlyeq_{lex}$), d'où
     $$\alpha + \gamma \preccurlyeq_{grlex} \beta + \gamma$$
3. $\preccurlyeq_{grlex}$ est *bien fondé* :
   Par l'absurde, supposons qu'il existe une suite $(\alpha^{(i)})_{i\in\mathbb{N}}$ strictement décroissante pour $\preccurlyeq_{grlex}$.
   Alors pour tout $i \in \mathbb{N}$:
   - $\sum_{i\leq n}\alpha_j^{(i+1)} < \sum_{i\leq n}\alpha_j^{(i)}$

   ou
   - $\sum_{i\leq n}\alpha_j^{(i+1)} = \sum_{i\leq n}\alpha_j^{(i)}$ et $\alpha^{(i+1)} \preccurlyeq_{lex} \alpha^{(i)}$

   Donc par le principe des tiroirs :
   - $$E \overset{\text{def}}{=} \left\{ i \in \mathbb{N} \;\middle|\; \sum_{i\leq n}\alpha_j^{(i+1)} < \sum_{i\leq n}\alpha_j^{(i)} \right\} \text{ est infini}$$

   ou
   - $$F \overset{\text{def}}{=} \left\{ i \in \mathbb{N} \;\middle|\; \sum_{i\leq n}\alpha_j^{(i+1)} = \sum_{i\leq n}\alpha_j^{(i)} \text{ et } \alpha^{(i+1)} \preccurlyeq_{lex} \alpha^{(i)} \right\} \text{ est infini}$$

   $\longrightarrow$ Si E (resp. F) est infini, alors la stricte décroissance pour $<$ (resp. $\preccurlyeq_{lex}$) de la suite $\left(\sum_{i\leq n}\alpha_j^{(i)}\right)_{i\in E} \in \mathbb{N}^E$ (resp. $(\alpha^{(i)})_{i\in F} \in (\mathbb{N}^n)^F$)
   contredit le caractère bien fondé de $<$ (resp. $\preccurlyeq_{lex}$).
   Dans tous les cas, on obtient une contradiction.

4.

Soit $(\alpha^{(k)})_{k\in\mathbb{N}} \in (\mathbb{N}^n)^{\mathbb{N}}$ une suite infinie.

Montrons par récurrence sur $n \in \mathbb{N}$ qu'on peut extraire une sous-suite infinie $(\alpha^{(m_k)})_{k\in\mathbb{N}} \in (\mathbb{N}^n)^{\mathbb{N}}$ telle que pour tout $k \in \mathbb{N}$,

$$\alpha^{(m_k)} \leq \alpha^{(m_{k+1})}$$

- *Initialisation* : Pour $n = 1$:
  Par l'absurde : supposons que ce ne soit pas le cas : aucune sous-suite de $(\alpha^{(k)})_{k\in\mathbb{N}}$ n'est croissante.
  On pose alors :
  - $m_0 \stackrel{\text{def}}{=} 0$
  - pour tout $i \in \mathbb{N}$, l'ensemble

    $$E_{m_i} \stackrel{\text{def}}{=} \{k > m_i \mid \alpha^{(k)} < \alpha^{(m_i)}\}$$

    est non vide, car sinon la sous-suite $(\alpha^{(k)})_{k>m_i}$ est croissante.
    On note alors m_{i+1} l'un de ses éléments (on utilise ici l'axiome du choix).
    Il vient que $\alpha^{(m_{i+1})} < \alpha^{(m_i)}$.

  On a construit une suite infinie strictement décroissante, ce qui contredit le caractère bien fondé de $\leq$ sur $\mathbb{N}$.
- *Hérédité* : Pour $n > 1$:
  De la même manière que dans l'initialisation, on montre qu'on peut extraire une suite croissante infinie $(\alpha_n^{(\varphi(k))})_{k\in\mathbb{N}}$ de $(\alpha_n^{(k)})_{k\in\mathbb{N}} \in \mathbb{N}^{\mathbb{N}}$.
  De plus, l'hypothèse de récurrence fournit une sous-suite infinie

  $$\left((\alpha_1^{(\psi(k))}, \ldots, \alpha_{n-1}^{(\psi(k))})\right)_{k\in\mathbb{N}}$$

  de $\left((\alpha_1^{(k)}, \ldots, \alpha_{n-1}^{(k)})\right)_{k\in\mathbb{N}} \in (\mathbb{N}^{(n-1)})^{\mathbb{N}}$.
  On vérifie alors aisément que la sous-suite infinie

  $$\left((\alpha_1^{((\varphi\circ\psi)(k))}, \ldots, \alpha_n^{((\varphi\circ\psi)(k))})\right)_{k\in\mathbb{N}} \in (\mathbb{N}^n)^{\mathbb{N}}$$

  de $(\alpha^{(k)})_{k\in\mathbb{N}}$ est croissante (par stricte croissance des extractrices φ et ψ), ce qui conclut.

On a montré que :

> Si $(\alpha^{(k)})_{k\in\mathbb{N}} \in (\mathbb{N}^n)^{\mathbb{N}}$ est une suite infinie, on peut en extraire une sous-suite infinie croissante.

5.

a). $<$ est bien fondé sur $\mathbb{N}^n$

Montrons que $<$ est bien fondé sur $\mathbb{N}^n$.

Par l'absurde : supposons qu'il existe une suite $(\alpha^{(i)})_{i\in\mathbb{N}} \in (\mathbb{N}^n)^{\mathbb{N}}$ strictement décroissante.

Alors comme pour tout $i \in \mathbb{N}$,

$$\alpha^{(i+1)} \leq \alpha^{(i)} \text{ et } \alpha^{(i+1)} \neq \alpha^{(i)}$$

i.e

$$\begin{cases} \forall k \in [\![1, n]\!],\ \alpha_k^{(i+1)} \leq \alpha_k^{(i)} \\ \exists k \in [\![1, n]\!];\ \alpha_k^{(i+1)} \neq \alpha_k^{(i)} \end{cases}$$

il existe $k_i \in [\![1, n]\!]$ tel que

$$\alpha_{k_i}^{(i+1)} < \alpha_{k_i}^{(i)}$$

c'est-à-dire (comme $(\alpha^{(i)})_{i\in\mathbb{N}}$ est décroissante) :

$$\forall i' > i, \quad \alpha_{k_i}^{(i')} < \alpha_{k_i}^{(i)}$$

Donc comme $(k_i)_{i\in\mathbb{N}}$ est à valeurs dans l'ensemble **fini** $[\![1, n]\!]$, il existe (par le principe des tiroirs) $j \in [\![1, n]\!]$ tel que :

$$K_j \stackrel{\text{def}}{=} \{i \in \mathbb{N} \mid k_i = j\}$$

est infini.

La suite infinie $(\alpha_j^{(i)})_{i\in K_j}$ à valeurs dans $\mathbb{N}$ est alors strictement décroissante, puisque :

$$\forall i < i' \in K_j,\ \alpha_j^{(i')} \leq \alpha_j^{(i+1)} = \alpha_{k_i}^{(i+1)} < \alpha_{k_i}^{(i)} = \alpha_j^{(i)}$$

ce qui contredit le caractère bien fondé de $<$ dans $\mathbb{N}$.

b). Si $F \subseteq \mathbb{N}^n$, l'ensemble des éléments minimaux de F est fini

Par l'absurde : supposons qu'il existe une suite infinie $(f^{(i)})_{i\in\mathbb{N}} \in F^{\mathbb{N}}$ d'éléments minimaux distincts de $F \subseteq \mathbb{N}^n$.

On va construire une suite $(g^{(i)})_{i\in\mathbb{N}^*} \in (\mathbb{N}^n)^{\mathbb{N}}$ strictement décroissante.

On pose

- $$g^{(0)} \stackrel{\text{def}}{=} f^{(0)}$$

- pour tout $i \in \mathbb{N}$,

$$f^{(i+1)} \text{ est minimal } \implies g^{(i)} \not< f^{(i+1)} \implies \begin{cases} \exists k \in [\![1,n]\!],\ g_k^{(i)} > f_k^{(i+1)} \\ \text{ ou} \\ \forall k \in [\![1,n]\!];\ g_k^{(i)} = f_k^{(i+1)} \end{cases} \qquad (\text{i.e } g^{(i)} = f^{(i+1)})$$

  d'où :
  - *Si* $g^{(i)} \neq f^{(i+1)}$:
    alors

$$\exists k \in [\![1,n]\!],\ f_k^{(i+1)} < g_k^{(i)}$$

    et en posant :

$$\mathbb{N}^n \ni g^{(i+1)} \overset{\text{def}}{=} \left(f_k^{(i+1)}, \dots, f_k^{(i+1)}\right)$$

    il vient, si $i \geq 1$, que :

$$g^{(i+1)} < g^{(i)}$$

  - *Sinon si* $g^{(i)} = f^{(i+1)}$:
    alors comme $f^{(i+2)} \neq f^{(i+1)} = g^{(i)}$ et $f^{(i+2)}$ est minimal :

$$g^{(i)} \not< f^{(i+2)} \implies \exists k \in [\![1,n]\!],\ f_k^{(i+2)} < g_k^{(i)}$$

    et en posant :

$$\mathbb{N}^n \ni g^{(i+1)} \overset{\text{def}}{=} \left(f_k^{(i+2)}, \dots, f_k^{(i+2)}\right)$$

    il vient, si $i \geq 1$, que :

$$g^{(i+1)} < g^{(i)}$$

Donc on construit une suite

$$(g^{(i)})_{i \in \mathbb{N}^*} \in (\mathbb{N}^n)^{\mathbb{N}}$$

strictement décroissante, ce qui contredit le caractère bien fondé de $\mathbb{N}^n$.

c). Tout suite $(F_k)_{k \in \mathbb{N}}$ croissante d'ensembles clos supérieurement stationne.

Soit $(F_k)_{k \in \mathbb{N}}$ une suite croissante d'ensembles clos supérieurement.

Si tous les F_k sont vides, le résultat est immédiat.

Sinon : on supposera dans la suite que les F_k sont non vides, sans perte de généralité (quitte à considérer $(F_k)_{k > k_0}$ pour le plus petit indice k_0 tel que $F_{k_0} \neq \emptyset$).

Pour tout $k \in \mathbb{N}$: l'ensemble des éléments minimaux de F_k est fini (d'après le point **b)**) et non vide (d'après la **question 1**, puisque les F_k sont non vides) : on le note : $\min F_k$.

D'après la **question 1** :

$$\bigcup_{f^* \in \min F_k} \{f \mid f \geq f^*\} = F_k \qquad \circledast$$

- *en effet* :
  - $\bigcup_{f^* \in \min F_k} \{f \mid f \geq f^*\} \subseteq F_k$ car F_k est clos supérieurement
  - pour tout $f \in F_k$, il existe, d'après la **question 1**, un $f_0^* \in \min F_k$ tel que

$$f \in \{f' \mid f' \geq f_0^*\} \subseteq \bigcup_{f^* \in \min F_k} \{f \mid f \geq f^*\}$$

Par l'absurde : supposons que la suite croissante $(F_k)_{k \in \mathbb{N}}$ ne soit pas stationnaire, c'est-à-dire qu'il existe une sous-suite infinie $(F_{k_i})_{i \in \mathbb{N}}$ strictement croissante.

On va construire une suite $(f_i^*)_{i \in \mathbb{N}} \in (\mathbb{N}^n)^{\mathbb{N}}$ dont on ne peut pas extraire de sous-suite infinie croissante (ce qui contredira la **question 4**).

- On note f_0^* un élément de $\min F_{k_0} \neq \emptyset$.
- Soit $i \in \mathbb{N}$, et supposons qu'on ait défini $f_0^*, \dots, f_i^*$.
  Comme $F_{k_i} \subsetneq F_{k_{i+1}}$, $\min F_{k_{i+1}} \setminus \min F_{k_i}$ est *non vide*
  - *en effet* : d'après $\circledast$, si $\min F_{k_{i+1}} \subseteq \min F_{k_i}$, alors on aurait $F_{k_{i+1}} \subseteq F_{k_i}$

  : on note f_{i+1}^* un de ses éléments.

On vérifie ainsi que pour tout $i \in \mathbb{N}$,

$$\forall j > i, f_i^* \not\leq f_j^*$$

- *en effet* : s'il existait $j > i$ tel que $f_i^* \leq f_j^*$ alors on aurait

$$f_j^* \in \{f \mid f \geq f_i^*\} \subseteq \bigcup_{f^* \in \min F_{k_i}} \{f \mid f \geq f^*\} = F_{k_i}$$

ce qui est impossible puisque $f_j^* \in F_{k_j} \setminus \underbrace{F_{k_{j-1}}}_{\supseteq F_{k_i} \text{ car } j-1 \geq i} \subseteq F_{k_j} \setminus F_{k_i}$

On ne peut donc extraire de sous-suite croissante infinie de $(f_i^*)_{i \in \mathbb{N}}$, ce qui contredit la **question 4**.

> On a donc montré que la suite croissante $(F_k)_{k \in \mathbb{N}}$ stationne, c'est-à-dire qu'il existe $k_0 \in \mathbb{N}$ tel que
>
> $$F_{k_0} = \bigcup_{k \in \mathbb{N}} F_k$$

II. Division de polynômes multivariables

6.

> $$x_1 + x_2 = x_2(x_1x_2 + 1) - x_1(x_2^2 - 1) \in \langle x_1x_2 + 1, x_2^2 - 1 \rangle$$

7.

Supposons que $x^\alpha | x^\beta$, et montrons que $\alpha \preccurlyeq \beta$.

Si $\alpha = \beta$: le résultat est immédiat, par réflexivité.

Sinon :

- $\forall i \in [\![1, n]\!], \alpha_i \leq \beta_i$ (car $x^\alpha \mid x^\beta$)
- et $\exists j \in [\![1, n]\!], \alpha_j < \beta_j$ (car $\alpha \neq \beta$)

d'où le fait qu'il existe $\gamma \overset{\text{def}}{=} (\beta_i - \alpha_i)_{i \in [\![1,n]\!]} \in \mathbb{N}^n \setminus \mathbf{0}$ tel que :

$$\beta = \alpha + \gamma$$

Or, d'après la **question 2** :

$$\mathbf{0} \prec \gamma$$

et comme l'ordre est monomial :

$$\alpha = \mathbf{0} + \alpha \prec \gamma + \alpha = \beta$$

ce qui conclut.

On a montré que :

> Si $x^\alpha | x^\beta$, alors $\alpha \prec \beta$.

8.

Terminaison

Montrons qu'à chaque tour de boucle, $mdeg(h)$ diminue strictement pour l'ordre monomial $\preccurlyeq$.

En effet :

- $mdeg(h - lt(h)) \prec mdeg(h)$ par définition de $lt(h)$
- $mdeg\left(h - \frac{lt(h)}{lt(f_i)} f_i\right) \prec mdeg(h)$ car la partie entière de la fraction rationnelle $\frac{f_i}{lt(f_i)}$ vaut 1 (par définition de $lt(f_i)$), d'où $lt\left(\frac{lt(h)}{lt(f_i)} f_i\right) = lt(h)$, et les monômes de $h - \frac{lt(h)}{lt(f_i)} f_i$ sont d'exposant strictement inférieur (pour $\preccurlyeq$) à l'exposant de $lt(h)$ (qui vaut $mdeg(h)$).

Or, l'ordre $\preccurlyeq$ est bien fondé (en tant qu'ordre monomial), donc la boucle ne peut pas être infinie, et

> l'algorithme termine.

Correction

Montrons que

> 1. le résultat de l'algorithme vérifie $g = \sum_{i \leq k} q_i f_i + r$ et pour tout $i \leq k$ et tout monôme x^α de r, $mdeg(f_i) \not\leq \alpha$
>
> 2. $\max_{i \leq k}(mdeg(f_i q_i)) = mdeg(g - r)$ pour l'ordre $\prec$

1.

Montrons l'invariant :

> I_j : après la j-ème itération de la boucle principale (`while h≠0 do ⋯ end`) :
>
> - $$g - h = \sum_{i \leq k} q_i f_i + r \quad \circledast$$
> - pour tout $i \leq k$ et tout monôme x^α de r, $mdeg(f_i) \not\leq \alpha \quad \circledast\circledast$

Par récurrence sur $j \in \mathbb{N}$:

- Pour $j = 0$: au début de l'algorithme, $h = g$, $r = 0$, et tous les q_i sont égaux à 0, donc $I_0\circledast$ est bien vérifié, et $I_0 \circledast\circledast$ aussi (puisque r ne contient pas de monôme).
- Pour $j > 0$: supposons que l'invariant est vérifié au début du j-ième tour de boucle, et montrons qu'il le reste à la sortie.
  - *Cas 1* : $\forall i \in [\![1, n]\!],\ lm(f_i) \nmid lm(h)$:
    donc $encore$ vaut encore $true$ à l'issue de la boucle interne `while i ≤ n and encore do ⋯ end` et à la fin de la j-ième boucle, on a effectué :

    $$r \leftarrow r + lt(h);\ h \leftarrow h - lt(h)$$

    les autres polynômes étant restés inchangés.
    Alors en posant $h' \overset{\text{def}}{=} h - lt(h)$ et $r' \overset{\text{def}}{=} r + lt(h)$:

    $$\begin{aligned} g - h' &= g - h + lt(h) \\ &= \sum_{i \leq k} q_i f_i + r + lt(h) \qquad (\text{par } I_j\ ) \\ &= \sum_{i \leq k} q_i f_i + r' \end{aligned}$$

    et $I_{j+1}\circledast$ reste vérifié.
    Par ailleurs, comme $I_j \circledast\circledast$ est vrai, il suffit de montrer que :

    $$\forall i \leq k, mdeg(f_i) \not\leq mdeg(h)$$

    pour vérifier $I_{j+1} \circledast\circledast$, puisque $x^{mdeg(h)}$ est le seul nouveau monôme ajouté à r.
    Or :

    $$x^\alpha | x^\beta \iff \alpha \leq \beta$$

    (les deux implications sont immédiates)
    Pour vérifier $I_{j+1} \circledast\circledast$, il suffit donc montrer que :

    $$\forall i \leq k, lm(f_i) = x^{mdeg(f_i)} \nmid x^{mdeg(h)} = lm(h)$$

    ce qui est exactement l'hypothèse faite : le résultat est donc acquis.
  - *Cas 2* : $\exists i \in [\![1, n]\!],\ lm(f_i) \mid lm(h)$:
    donc $encore$ se voit attribuer la valeur $false$ après la boucle interne `while i ≤ n and encore do ⋯ end` et à la fin de la j-ième boucle, on a effectué :

    $$q_i \leftarrow q_i + \frac{lt(h)}{lt(f_i)};\ h \leftarrow h - \frac{lt(h)}{lt(f_i)} f_i$$

    les autres polynômes étant restés inchangés.
    Alors en posant $h' \overset{\text{def}}{=} h - \frac{lt(h)}{lt(f_i)} f_i$ et $q_i' \overset{\text{def}}{=} q_i + \frac{lt(h)}{lt(f_i)}$:

    $$\begin{aligned} g - h' &= g - h + \frac{lt(h)}{lt(f_i)} f_i \\ &= \sum_{l \leq k} q_l f_l + r + \frac{lt(h)}{lt(f_i)} f_i \qquad (\text{par } I_j\ ) \\ &= \sum_{\substack{l \leq k \\ l \neq i}} q_l f_l + r + q_i f_i + \frac{lt(h)}{lt(f_i)} f_i \\ &= \sum_{\substack{l \leq k \\ l \neq i}} q_l f_l + r + q_i' f_i \end{aligned}$$

    Donc $I_{j+1}\circledast$ est vrai.
    Par ailleurs, comme aucun monôme n'est ajouté à r, $I_{j+1} \circledast\circledast$ reste vérfié.

  Dans tous les cas, le résultat est acquis.

À la sortie de la dernière boucle, $h = 0$, donc l'invariant fournit le résultat escompté.

2.

Pour tout j, on notera $r^{(j)}, h^{(j)}, q_i^{(j)}$ (pour $i \in [\![1, k]\!]$) la valeur des variables correspondantes à la fin de la j-ème itération ($r^{(0)}, h^{(0)}, q_i^{(0)}$ étant leur valeur initiale).

Comme l'algorithme termine, les suites $(r^{(j)})_j, (h^{(j)})_j, (q_i^{(j)})_j$ (pour $i \in [\![1,k]\!]$) sont de même cardinal fini : en notant N le numéro de la dernière itération ($N=0$ si on n'entre pas la boucle principale), elles sont de cardinal $N+1$.

Dans la preuve de terminaison, on a montré que

> $(mdeg(h^{(j)}))_{0\leq j\leq N}$ est strictement décroissante pour l'ordre bien fondé $\preccurlyeq$.

On note j_0 le nombre d'itérations de la boucle principale `while h≠0 do ⋯ end` avant que $encore$ se voie attribuer la valeur $false$ pour la première fois ($j_0=0$ si $encore$ est mis à $false$ dès la première itération).

Alors :

- au début de la (j_0+1)-ème itération,

$$h^{(j_0)} = g - r^{(j_0)} \text{ et } \forall i \in [\![1,k]\!], q_i^{(j_0)} = 0$$

  - *en effet* : au cours des j_0 premières itérations, comme $encore$ vaut $true$, on n'effectue que :

$$r \leftarrow r + lt(h);\ h \leftarrow h - lt(h)$$

    à chaque tour de boucle (les autres polynômes, donc en particulier les q_i, restant inchangés).
    Par conséquent, les invariants $g = h + r$ et $\forall i, q_i = 0$ sont vérifiés (les q_i sont initialisés à 0) au cours des j_0 premières itérations (même si $j_0 = 0$, puisqu'alors $h = g, r = 0$ et $\forall i, q_i = 0$).

- à la fin de la (j_0+1)-ème itération : comme $encore$ s'est vu attribuer la valeur $false$, on a effectué :

$$q_{i_0} \leftarrow q_{i_0} + \frac{lt(h)}{lt(f_{i_0})};\ h \leftarrow h - \frac{lt(h)}{lt(f_{i_0})} f_{i_0}$$

  les autres polynômes étant restés inchangés.
  Il vient, d'après le point précédent, que :

$$\begin{cases} h^{(j_0+1)} & = \overbrace{g - r^{(j_0)}}^{h^{(j_0)}} - \frac{lt(h^{(j_0)})}{lt(f_{i_0})} f_{i_0} \\ q_{i_0}^{(j_0+1)} & = q_{i_0}^{(j_0)} + \frac{lt(h^{(j_0)})}{lt(f_{i_0})} \\ & = \frac{lt(h^{(j_0)})}{lt(f_{i_0})} \\ \forall i \in [\![1,k]\!] \setminus \{i_0\}, q_i^{(j_0+1)} & = q_i^{(j_0)} \\ & = 0 \end{cases}$$

  De plus :

$$lt\left(q_{i_0}^{(j_0+1)} f_{i_0}\right) = lt\left(\frac{lt(h^{(j_0)})}{lt(f_{i_0})} f_{i_0}\right) \overset{\circledast}{=} lt(h^{(j_0)}) = lt\left(g - r^{(j_0)}\right) \quad \circledast\circledast$$

  (on a montré l'égalité $\circledast$ dans la preuve de terminaison)

Montrons que

> *Lemme* : $\forall j > j_0$,
>
> $$\begin{cases} \max_{1\leq i\leq k} mdeg\left(q_i^{(j)} f_i\right) = mdeg\left(lt\left(q_{i_0}^{(j_0+1)} f_{i_0}\right)\right) \\ lt\left(g - r^{(j)}\right) = lt\left(g - r^{(j_0)}\right) \end{cases}$$

Il suffit de montrer que les seuls termes que l'on peut ajouter (ou soustraire : au sens algébrique), à chaque itération, aux $q_i^{(j)} f_i$ (resp. $g - r^{(j)}$) sont d'exposants strictement inférieurs (pour $\preccurlyeq$) à celui de $lt\left(q_{i_0}^{(j_0+1)} f_{i_0}\right)$ (resp. $lt\left(g - r^{(j_0)}\right)$).

Or, l'exposant de $lt\left(q_{i_0}^{(j_0+1)} f_{i_0}\right) = lt\left(g - r^{(j_0)}\right) = lt(h^{(j_0)})$ vaut $mdeg(h^{(j_0)})$, et pour $j > j_0$, le seul terme possiblement ajouté (ou soustrait) aux polynômes précédents au cours de la j-ième itération est

$$lt(h^{(j)}) = lt\left(\frac{lt(h^{(j)})}{lt(f_j)} f_j\right)$$

(on a montré cette égalité dans la preuve de terminaison)

dont l'exposant est

$$mdeg(h^{(j)}) \prec mdeg(h^{(j_0)})$$

par stricte décroissance de $(mdeg(h^{(j')}))_{j'}$.

Le résultat est donc acquis.

Par conséquent, à la fin de l'algorithme :

- Si $N = j_0$:
  Le résultat s'ensuit immédiatement puisqu'on a montré dans le premier point que :

$$h = h^{(N)} = g - r^{(N)} = g - r = 0$$

  puisque $g = \sum_{i \leq k} q_i f_i + r = r$, et

$$\forall i \in [\![1, k]\!],\ q_i = q_i^{(N)} = 0$$

- Si $N > j_0$:

$$\begin{aligned}
\max_{i \leq k}(mdeg(f_i q_i)) &= \max_{i \leq k}(mdeg(f_i^{(N)} q_i^{(N)})) \\
&= mdeg\Big(lt\big(q_{i_0}^{(j_0+1)} f_{i_0}\big)\Big) && \text{(lemme)} \\
&= mdeg\Big(lt\big(g - r^{(j_0)}\big)\Big) && \text{(par } \circledast\circledast\text{)} \\
&= mdeg\Big(lt\big(g - r^{(N)}\big)\Big) && \text{(lemme)} \\
&= mdeg\Big(lt\big(g - r\big)\Big) \\
&= mdeg(g - r)
\end{aligned}$$

  ce qui conclut.

9.

On pose

- $g \overset{\text{def}}{=} x_1 x_2 + x_2 x_3$
- $f_1 \overset{\text{def}}{=} x_1 + x_3$
- $f_2 \overset{\text{def}}{=} x_1$

Division de g par (f_1, f_2) :

	$encore$	h	q_1	q_2	r
Initialisation		$x_1 x_2 + x_2 x_3$	0	0	0
Fin de la 1ère itération	$\underbrace{lm(f_1)}_{=x_1} \mid \underbrace{lm(h)}_{=x_1 x_2}$ $\longrightarrow false$	$x_1 x_2 + x_2 x_3 - x_1 x_2(1 + \frac{x_3}{x_1})$ $= 0$	$0 + \frac{x_1 x_2}{x_1} = x_2$	0	$\boxed{0}$

Division de g par (f_2, f_1) :

	$encore$	h	q_1	q_2	r
Initialisation		$x_1 x_2 + x_2 x_3$	0	0	0
Fin de la 1ère itération	$\underbrace{lm(f_2)}_{=x_1} \mid \underbrace{lm(h)}_{=x_1 x_2}$ $\longrightarrow false$	$x_1 x_2 + x_2 x_3 - x_1 x_2$ $= x_2 x_3$	$0 + \frac{x_1 x_2}{x_1} = x_2$	0	0
Fin de la 2ème itération	$\underbrace{lm(f_2) = lm(f_1)}_{=x_1} \nmid \underbrace{lm(h)}_{=x_2 x_3}$ $\longrightarrow true$	$x_2 x_3 - x_2 x_3 = 0$	x_2	0	$0 + x_2 x_3$ $= \boxed{x_2 x_3}$

Donc

> le reste de la division de g par (f_1, f_2) (qui vaut 0) est différent du reste de la division de g par (f_2, f_1) (qui vaut $x_2 x_3$).

10.

Si le reste de la division de g par $(f_1, \ldots, f_k)$ est nul, alors d'après la **question 8** :

$$\begin{aligned}
g &= \sum_{i \leq k} q_i f_i + \underbrace{r}_{=0} \\
&= \sum_{i \leq k} q_i f_i \in \langle f_1, \ldots, f_k \rangle
\end{aligned}$$

Mais la réciproque n'est pas vraie : en reprenant l'exemple de la **question 9** :

$$g = x_2(x_1 + x_3) \in \langle f_2, f_2 \rangle$$

mais le reste de la division de g par (f_2, f_1) n'est pas nul (il vaut $x_2 x_3$).

On a donc montré que :

> Si le reste de la division de g par $(f_1, \dots, f_k)$ est nul, alors $g \in \langle f_1, \dots, f_k \rangle$ mais que l'inverse n'est pas nécessairement vrai.

11.

On suppose que $f_1, \dots, f_k$ sont des monômes, et que $g \overset{\text{def}}{=} \sum_{i \leq k} q'_i f_i \in \langle f_1, \dots, f_k \rangle$.

Par l'absurde : supposons que le reste r de la division de g par $(f_1, \dots, f_k)$ n'est pas nul.

Avec les notations de la **question 8** :

$$\begin{aligned} g &= \sum_{i \leq k} q_i f_i + r \\ \implies r &= \sum_{i \leq k} (q'_i - q_i) f_i \end{aligned}$$

Soit $c\, x^\alpha$ un terme non nul ($c \neq 0$) de r (il en existe un puisque $r \neq 0$).

Comme $c\, x^\alpha$ apparaît dans la some de droite, il existe $i \leq k$ tel que l'un des termes $c'\, x^\beta f_i$ de $(q'_i - q_i) f_i$ vaut $c\, x^\alpha$.

Donc comme $c \neq 0$ et $\mathbb{Q}$ est un corps (donc c y est inversible):

$$f_i \mid \underbrace{x^\alpha}_{= \frac{c'}{c} x^\beta f_i}$$

donc l'exposant de f_i est inférieur (dans $\mathbb{N}^n$, pour $\leq$) à α, ce qui contredit le fait que :

pour tout $j \leq k$ et tout monôme $x^{\alpha'}$ de r, $mdeg(f_j) \not\leq \alpha'$ (démontré à la **question 8**).

On a donc montré que

> Si $f_1, \dots, f_k$ sont des monômes, et $g \in \langle f_1, \dots, f_k \rangle$, le reste de la division de g par $(f_1, \dots, f_k)$ est nul.

III. Une première caractérisation d'une base

12.

Supposons que $\mathcal{F}$ est une base.

Montrons que $\langle lm(\mathcal{F}) \rangle = \langle lm(\langle \mathcal{F} \rangle) \rangle$.

L'inclusion $\langle lm(\mathcal{F}) \rangle \subseteq \langle lm(\langle \mathcal{F} \rangle) \rangle$ est toujours vraie, puisque

$$\begin{aligned} & \mathcal{F} \subseteq \langle \mathcal{F} \rangle \\ \implies & lm(\mathcal{F}) \subseteq lm(\langle \mathcal{F} \rangle) \subseteq \langle lm(\langle \mathcal{F} \rangle) \rangle \\ \implies & lm(\mathcal{F}) \subseteq \langle lm(\langle \mathcal{F} \rangle) \rangle \\ \implies & \langle lm(\mathcal{F}) \rangle \subseteq \langle lm(\langle \mathcal{F} \rangle) \rangle \end{aligned}$$

la dernière implication venant du fait que $\langle lm(\mathcal{F}) \rangle$ est le plus petit idéal contenant $lm(\mathcal{F})$ et $\langle lm(\langle \mathcal{F} \rangle) \rangle$ est un idéal.

Montrons que $\langle lm(\langle \mathcal{F} \rangle) \rangle \subseteq \langle lm(\mathcal{F}) \rangle$.

Il suffira de montrer que $lm(\langle \mathcal{F} \rangle) \subseteq \langle lm(\mathcal{F}) \rangle$, par minimalité de $\langle lm(\langle \mathcal{F} \rangle) \rangle$.

Soit $x^\alpha \overset{\text{def}}{=} lm(g) \in lm(\langle \mathcal{F} \rangle)$, où $g \in \langle \mathcal{F} \rangle$. Montrons que $x^\alpha \in \langle lm(\mathcal{F}) \rangle$.

Comme $g \in \langle \mathcal{F} \rangle$, en divisant g par la **base** $\mathcal{F}$, g s'écrit, d'après la **question 8** :

$$g = \sum_{i \leq k} q_i f_i + \underbrace{0}_{\mathcal{F} \text{ est une base}}$$

et

$$\alpha = mdeg(g) = \max_{i \leq k}(mdeg(f_i q_i))$$

Donc il existe $i_0 \in [\![1, k]\!]$ tel que

$$\alpha = mdeg(f_{i_0} q_{i_0})$$

Or, par monomialité de $\prec$, $lm(f_{i_0} q_{i_0}) = lm(f_{i_0}) lm(q_{i_0})$, où x^γ est un monôme de q_{i_0}.

- *en effet* : en posant $\alpha_0 \overset{\text{def}}{=} mdeg(f_{i_0})$: pour tout monôme

$$\underbrace{x^\beta}_{\text{monôme de } f_{i_0}} \overbrace{x^\gamma}^{\text{monôme de } q_{i_0}}$$

de $f_{i_0}q_{i_0}$, l'exposant de $x^\beta x^\gamma$ est inférieur à celui de $lm(f_{i_0})x^\gamma$, puisque :

$$\beta \prec \alpha_0 \implies \underbrace{\beta+\gamma}_{\text{exposant de } x^\beta x^\gamma} \prec \overbrace{\alpha_0+\gamma}^{\text{exposant de } lm(f_{i_0})x^\gamma}$$

Donc le monôme de tête de $f_{i_0}q_{i_0}$ est nécessairement de la forme $lm(f_{i_0})x^\gamma$, où x^γ est un monôme de q_{i_0}.
Puis, par symétrie, on montre que $\gamma = mdeg(q_{i_0})$.

Par suite, en posant $\gamma \overset{\text{def}}{=} mdeg(q_{i_0}$:

$$\alpha = mdeg(lm(f_{i_0})x^\gamma) = mdeg(f_{i_0}) + \gamma$$

et

$$mdeg(f_{i_0}) \leq \alpha$$

d'où

$$lm(f_{i_0}) = x^{mdeg(f_{i_0})} \mid x^\alpha$$

et

$$x^\alpha \in \langle lm(f_{i_0})\rangle \subseteq \langle lm(\mathcal{F})\rangle$$

ce qui conclut.

On a donc montré que

> Si $\mathcal{F}$ est une base, alors
>
> $$\langle lm(\mathcal{F})\rangle = \langle lm(\langle \mathcal{F}\rangle)\rangle$$

13.

Supposons que $\langle lm(F)\rangle = \langle lm(\langle F\rangle)\rangle$.

Par l'absurde : Soit $g \overset{\text{def}}{=} \sum_{i\leq k} q'_i f_i \in \langle F\rangle$ tel que r le reste de la division par $\mathcal{F}$ soit non nul.

En divisant g par $\mathcal{F}$, g s'écrit, d'après la **question 8** :

$$g = \sum_{i\leq k} q_i f_i + r$$
$$\implies r = \sum_{i\leq k} (q'_i - q_i) f_i \quad \circledast$$

et pour tout monôme x^α de r :

- $\forall i \in [\![1,k]\!], \quad mdeg(f_i) \not\leq \alpha$
- *i.e* $\forall i \in [\![1,k]\!], \quad lm(f_i) \nmid x^\alpha$
- *i.e* le reste de la division de x^α par $(lm(f_i))_{1\leq i\leq k}$ vaut x^α et n'est donc pas nul (l'algorithme de division finit après une itération de la boucle principale).
- *i.e* $x^\alpha \notin \langle (lm(f_i))_{1\leq i\leq k}\rangle = \langle lm(\mathcal{F})\rangle$ (d'après la contraposée de la **question 11**)

Par suite, en appliquant ce qui précède au monôme $lm(r)$ (qui existe puisque r est **non nul**) :

$$lm(r) \notin \langle lm(\mathcal{F})\rangle$$

Mais comme $r \in \langle \mathcal{F}\rangle$ (par $\circledast$) :

$$lm(r) \in lm(\langle \mathcal{F}\rangle) \subseteq \langle lm(\langle \mathcal{F}\rangle)\rangle$$

Donc

$$\emptyset \neq \langle lm(\langle \mathcal{F}\rangle)\rangle \setminus \langle lm(\mathcal{F})\rangle \ni lm(r)$$

ce qui est absurde, du fait de l'hypothèse $\langle lm(F)\rangle = \langle lm(\langle F\rangle)\rangle$.

On a donc montré que

> Si $\langle lm(F)\rangle = \langle lm(\langle F\rangle)\rangle$, alors $\mathcal{F}$ est une base.

IV. Une caractérisation plus effective

14.

$$S(x_1x_2+1, x_2^2-1) = x_1x_2^2\left(1+\frac{1}{x_1x_2} - \left(1-\frac{1}{x_2^2}\right)\right) = x_2 + x_1$$

15.

Si $\mathcal{F}$ est une base : alors pour tous $f_i, f_j \in \mathcal{F}$,

$$S(f_i, f_j) \overset{\text{def}}{=} x^{lcm(mdeg(f_i), mdeg(f_j))} \left(\frac{f_i}{lt(f_i)} - \frac{f_j}{lt(f_j)} \right) \in \langle f_i, f_j \rangle \subseteq \langle \mathcal{F} \rangle$$

en vérifiant aisément que $\frac{x^{lcm(mdeg(f_i), mdeg(f_j))}}{lt(f_i)}$ (resp. $\frac{x^{lcm(mdeg(f_i), mdeg(f_j))}}{lt(f_j)}$) est un polynôme, car l'exposant $mdeg(f_i)$ (resp. $mdeg(f_j)$) de $lt(f_i)$ (resp. $lt(f_j)$) est inférieur (pour $\leq$) à l'exposant $lcm(mdeg(f_i), mdeg(f_j))$ de $x^{lcm(mdeg(f_i), mdeg(f_j))}$.

Et comme $S(f_i, f_j) \in \langle \mathcal{F} \rangle$, le reste de la division de $S(f_i, f_j)$ par $\mathcal{F}$ est nul (car $\mathcal{F}$ est une base, par définition).

On a montré que :

> Si $\mathcal{F}$ est une base, alors pour tous $f_i, f_j \in \mathcal{F}$, le reste de la division de $S(f_i, f_j)$ par $\mathcal{F}$ est nul.

16.

Supposons, *par l'absurde*, qu'il existe au plus un indice i tel que $mdeg(f_i q_i) = \max_{l \leq k}(mdeg(f_l q_l))$.

Comme il en existe au moins un (puisque la famille sur lequel le $\max$ est pris est $(mdeg(f_l q_l))_{l \leq k}$, et l'ordre $\prec$ est total (en tant qu'ordre monomial)), il existe exactement un indice i tel que $mdeg(f_i q_i) = \max_{l \leq k}(mdeg(f_l q_l))$.

Mais alors

$$mdeg\left(\sum_{\substack{l \leq k \\ l \neq i}} f_l q_l \right) \preceq \max_{\substack{l \leq k \\ l \neq i}}(mdeg(f_l q_l)) \prec mdeg(f_i q_i)$$

d'où :

$$lm\left(\sum_{l \leq k} f_l q_l \right) = lm(f_i q_i)$$

et

$$mdeg(g) = mdeg\left(\sum_{l \leq k} f_l q_l \right) = mdeg(f_i q_i) = \max_{l \leq k}(mdeg(f_l q_l))$$

ce qui contredit l'hypothèse

$$mdeg(g) \prec \max_{l \leq k}(mdeg(f_l q_l))$$

On a donc montré que :

> il existe au moins deux indices i, j tels que
>
> $$mdeg(f_j q_j) = mdeg(f_i q_i) = \max_{l \leq k}(mdeg(f_l q_l))$$

17.

En divisant $S(f_i, f_j)$ par $\mathcal{F}$, $S(f_i, f_j)$ s'écrit, d'après la **question 8** :

$$S(f_i, f_j) = \sum_{l \leq k} f_l h_l + \underbrace{0}_{\text{le reste est nul par hypothèse}}$$

avec

$$\max_{l \leq k}(mdeg(f_l h_l)) = mdeg(S(f_i, f_j)) \quad \circledast$$

Par suite :

$$\begin{aligned} S(f_i, f_j) &\overset{\text{def}}{=} x^{lcm(mdeg(f_i), mdeg(f_j))} \left(\frac{f_i}{lt(f_i)} - \frac{f_j}{lt(f_j)} \right) \\ &= x^{lcm(mdeg(f_i), mdeg(f_j))} \left(\frac{f_i}{lm(f_i)} - \frac{f_j}{lm(f_j)} \right) \qquad (\text{puisque } lc(f_j) = lc(f_i) = 1) \end{aligned}$$

Or : les parties entières des fractions rationnelles $\frac{f_i}{lm(f_i)}$ et $\frac{f_j}{lm(f_j)}$ sont égales (elles valent 1), donc la fraction rationnelle $\frac{f_i}{lm(f_i)} - \frac{f_j}{lm(f_j)}$ n'est somme que de parties polaires de **degrés strictement négatifs**.

Par conséquent, $S(f_i, f_j)$ est une somme (algébrique) de termes dont les exposants des monômes sont strictement inférieurs (pour $\prec$) à l'exposant $lcm(mdeg(f_i), mdeg(f_j))$ du terme $x^{lcm(mdeg(f_i), mdeg(f_j))}$ en facteur de $\frac{f_i}{lm(f_i)} - \frac{f_j}{lm(f_j)}$.

De fait,

$$mdeg(S(f_i,f_j)) = mdeg\Big(\frac{f_i}{lc(f_i)} - \frac{f_j}{lc(f_j)}\Big) \prec lcm(mdeg(f_i), mdeg(f_j))$$

et par ⊛ :

$$\forall l \in [\![1,k]\!], \quad mdeg(f_l h_l) \preceq mdeg(S(f_i,f_j)) \prec lcm(mdeg(f_i), mdeg(f_j))$$

d'où, finalement :

$$\forall l \in [\![1,k]\!], \quad mdeg(f_l h_l) \prec lcm(mdeg(f_i), mdeg(f_j))$$

On a montré que

> $S(f_i,f_j) = \sum_{l\leq k} f_l h_l$ avec pour tout l, $mdeg(f_l h_l) \prec lcm(mdeg(f_i), mdeg(f_j))$

18.

Soit $t = \frac{lt(f_i q_i)}{x^{lcm(mdeg(f_i),mdeg(f_j))}}$

- $q_i' = q_i - lt(q_i) + th_i$
- $q_j' = q_j + lc(q_i)lm(q_j) + th_j$
- $q_l' = q_l + th_l$ pour tout $l \notin \{i,j\}$

Montrons que $g = \sum f_l q_l'$

$$\begin{aligned}
\sum_{l\leq k} f_l q_l' &= f_i\big(q_i - lt(q_i) + th_i\big) + f_j\big(q_j + lc(q_i)lm(q_j) + th_j\big) + \sum_{\substack{l\leq k\\ l\notin\{i,j\}}} f_l(q_l + th_l) \\
&= -f_i lt(q_i) + f_i th_i + f_j lc(q_i)lm(q_j) + f_j th_j + \underbrace{\sum_{l\leq k} f_l q_l}_{=g} + \sum_{\substack{l\leq k\\ l\notin\{i,j\}}} f_l th_l \\
&= g - f_i lt(q_i) + f_j lc(q_i)lm(q_j) + t\overbrace{\sum_{l\leq k} f_l h_l}^{=S(f_i,f_j)} \\
&= g - f_i lt(q_i) + f_j lc(q_i)lm(q_j) + tx^{lcm(mdeg(f_i),mdeg(f_j))}\Big(\frac{f_i}{lt(f_i)} - \frac{f_j}{lt(f_j)}\Big) \\
&= g - f_i lt(q_i) + f_j lc(q_i)lm(q_j) + lt(f_i q_i)\Big(\frac{f_i}{lt(f_i)} - \frac{f_j}{lt(f_j)}\Big) \quad \circledast
\end{aligned}$$

Or, on montre, de la même manière qu'à la **question 12** (au milieu de la démonstration) que, comme l'ordre $\prec$ est monomial : le monôme de tête de $f_i q_i$ est le produit des monômes de tête de f_i et de q_i, et partant :

$$lt(f_i q_i) = lt(f_i)lt(q_i)$$

Donc

$$-f_i lt(q_i) + lt(f_i q_i)\frac{f_i}{lt(f_i)} = -f_i lt(q_i) + lt(q_i) f_i = 0 \quad \circledast\circledast$$

Par ailleurs,

$$\begin{aligned}
& f_j lc(q_i)lm(q_j) - lt(f_i q_i)\frac{f_j}{lt(f_j)} = 0 \\
\Longleftarrow\quad & lt(f_i q_i) = lc(q_i)lm(q_j)lt(f_j) \\
\Longleftrightarrow\quad & lc(f_i)lm(f_i)lc(q_i)lm(q_i) = lc(q_i)lm(q_j)lc(f_j)lm(f_j) \\
\Longleftarrow\quad & lc(f_i)\underbrace{lm(f_i)lm(q_i)}_{=lm(f_i q_i)=lm(f_j q_j)} = lc(f_j)\underbrace{lm(q_j)lm(f_j)}_{=lm(f_j q_j)=lm(f_i q_i)} \\
\Longleftarrow\quad & lc(f_i) = lc(f_j)
\end{aligned}$$

la dernière égalité étant vérifiée, puisque $lc(f_i) = lc(f_j) = 1$.

Donc

$$f_j lc(q_i)lm(q_j) - lt(f_i q_i)\frac{f_j}{lt(f_j)} = 0 \quad \circledast\circledast\circledast$$

D'après ⊛, ⊛⊛ et ⊛ ⊛ ⊛, il vient que :

$$g = \sum_{l\leq k} f_l q_l'$$

Cette représentation contredit la minimalité de la représentation originelle

Montrons que le multi-ensemble associé à cette représentation est strictement inférieur au multi-ensemble associé à la représentation originelle.

En effet :

Pour tout l,

$$\begin{aligned}
mdeg(tf_lh_l) &= mdeg(t) + mdeg(f_lh_l) && \text{(puisque le monôme de tête du produit est le produit des monômes de tête)}\\
&= \underbrace{mdeg(f_iq_i)}_{=\max_{l\leq k}(lm(f_lq_l))} - lcm(mdeg(f_i), mdeg(f_j)) + mdeg(f_lh_l)\\
&\prec \max_{l\leq k}(mdeg(f_lq_l)) - lcm(mdeg(f_i), mdeg(f_j)) + lcm(mdeg(f_i), mdeg(f_j)) && \text{(question 17)}\\
&= \max_{l\leq k}(mdeg(f_lq_l))
\end{aligned}$$

Donc, comme $mdeg(tf_lh_l) \prec \max_{l\leq k}(lm(f_lq_l))$, l'ajout des th_l ne fait pas augmenter le multidegré des q'_lf_l dans cette représentation.

De plus,

$$q_j + lc(q_i)lm(q_j)$$

a un multidegré inférieur ou égal à celui de q_j, donc

$$mdeg(q'_jf_j) \preceq mdeg(q_jf_j) = \max_{l\leq k}(mdeg(f_lq_l))$$

Enfin :

$$q_i - lt(q_i)$$

a un multidegré **strictement inférieur** à celui de q_i, donc

$$mdeg(q'_if_i) \prec mdeg(q_if_i) = \max_{l\leq k}(mdeg(f_lq_l))$$

et la multiplicité du degré maximal $\max_{l\leq k}(mdeg(f_lq_l)) = mdeg(q_if_i) = mdeg(q_if_i)$ des q'_lf_l dans le multi-ensemble associé à cette représentation a diminué strictement par rapport à celle de la représentation originelle, ce qui, d'après la définition de l'ordre sur les multi-ensembles rappelée dans l'énoncé, implique que

> le multi-ensemble associé à cette représentation est strictement inférieur au multi-ensemble associé à la représentation originelle

ce qui est absurde, par minimalité de la représentation originelle.

Conclusion :

Il vient donc que

$$mdeg(g) = max_{i\leq k}(mdeg(f_iq_i))$$

comme cette propriété est vérifiée pour tous les $g \in \langle\mathcal{F}\rangle$, on peut montrer avec la même démonstration que celle de la **question 12** que :

$$\langle lm(\mathcal{F})\rangle = \langle lm(\langle\mathcal{F}\rangle)\rangle$$

ce qui, d'après la **question 13**, est suffisant pour établir que tous les polynômes de $\langle\mathcal{F}\rangle$ ont un reste nul dans la division par $\mathcal{F}$, c'est-à-dire que $\mathcal{F}$ **(qui est fini) est une base**.

On a donc montré que :

> Si, pour tous $f_i, f_j \in \mathcal{F}$ (fini), le reste de la division de $S(f_i, f_j)$ par $\mathcal{F}$ est nul, alors $\mathcal{F}$ est une base.

V. Calcul d'une base

19.

Terminaison

Méthode 1 :

À chaque itération de la boucle principale, l'idéal engendré par les monômes de tête de G croît strictement (hormis à la dernière itération de la boucle principale, lorsque $new = \emptyset$), puisque new est constitué de restes non nuls r_j de divisions par G : ce qui implique, d'après la **question 8**, que pour tout j, aucun monôme de tête d'un polynôme de G ne divise r_j.

Donc $lm(r_j) \notin \langle lm(G)\rangle$ (comme on l'a rappelé à la **question 13** (d'après la contraposée de la **question 11**)), et l'idéal engendré par $lm(G \cup \underbrace{new}_{=\{r_j\}_j})$ est strictement plus grand que l'idéal engendré par $lm(G)$ dans $\mathbb{Q}[x_1, \ldots, x_n]$.

Or, comme on l'a vu dans le cours d'algèbre : $\mathbb{Q}[x_1, \ldots, x_n]$ est un anneau **noethérien** : toute suite croissante d'idéaux y stationne.

Donc la suite précédente ne peut pas croître strictement indéfiniment, et **l'algorithme termine** (puisque $\langle lm(G \cup new)\rangle = \langle lm(G)\rangle$ n'est possible que si $new = \emptyset$ (l'algorithme s'arrête alors), car si $new \neq \emptyset$, les éléments de $lm(new)$ n'appartiennent pas à $\langle lm(G)\rangle$).

Méthode 2 (trouvée après) :

Si on appelle "partie engendrée par $\alpha \in \mathbb{N}^n$" la partie $\langle \alpha \rangle \overset{\text{def}}{=} \{\beta \in \mathbb{N}^n \mid \beta \geq \alpha\}$, on peut reprendre l'argument précédent en considérant **les parties engendrées par les exposants des monômes de tête** de G à chaque itération : elles sont closes supérieurement (par définition), et elles ne peuvent pas croître indéfiniment par la **question 5**.

L'argument est analogue à la méthode précédente, en utilisant l'équivalence

$$x^\alpha \mid x^\beta \iff \alpha \leq \beta$$

À chaque itération de la boucle principale, la partie engendrée par les exposants des monômes de tête de G croît strictement (hormis à la dernière itération de la boucle principale, lorsque $new = \emptyset$), puisque new est constitué de restes non nuls r_j de divisions par G vérifiant $lm(r_j) \notin \langle lm(G) \rangle$, donc $exposant(lm(r_j)) \notin \langle exposant(lm(G)) \rangle$.

Correction

À la dernière itération de la boucle principale, $new = \emptyset$, ce qui signifie qu'on n'a trouvé aucune paire $\{f, g\} \subseteq G$ telle que le reste de la division de $S(f, g)$ par G ne soit pas nul.

En d'autres termes : à la fin de l'algorithme, pour tous $f, g \in G$, le reste de la division de $S(f, g)$ par G est nul, ce qui implique, d'après la conclusion de la **question 18**, que

> G est une base de $\langle G \rangle$.

Or, G est initialisé à $\{f_1, \ldots, f_k\}$, et à chaque itération de la boucle principale, l'invariant

$$\langle G \rangle = \langle f_1, \ldots, f_k \rangle$$

est conservé.

- *en effet*, chaque reste r d'une division `Divise(S(f, g), G)` appartient à l'idéal engendré par G, puisque, $S(f, g) \in \langle G \rangle$ (montré à la **question 15**) et d'après la **question 8** :

  $$r = \underbrace{S(f, g)}_{\in \langle G \rangle} - \underbrace{\sum_{g'_l \in G} q'_l g'_l}_{\in \langle G \rangle} \in \langle G \rangle$$

  donc à la fin de chaque boucle :

  $$\langle G \rangle = \langle G \cup new \rangle$$

On en conclut donc qu'à la fin de l'algorithme :

> $\langle G \rangle = \langle f_1, \ldots, f_k \rangle$

En récapitulant tout :

> À la fin de l'algorithme, G est une base de $\langle G \rangle = \langle f_1, \ldots, f_k \rangle$.

20.

Construction d'une base de $\langle x_1 x_2 + 1, x_2^2 - 1 \rangle$:

	new	G	**paires de polynômes de G**	$S(f, g)$	$Divise(S(f, g), G)$
Initialisation		$\{x_1 x_2 + 1, x_2^2 - 1\}$	$\{x_1 x_2 + 1, x_2^2 - 1\}$		
Fin de la 1ère itération	$\{x_1 + x_2\}$	$\{x_1 + x_2, x_1 x_2 + 1, x_2^2 - 1\}$	$\{x_1 x_2 + 1, x_2^2 - 1\}$ $\{x_1 + x_2, x_1 x_2 + 1\}$ $\{x_1 + x_2, x_2^2 - 1\}$	$S(x_1 x_2 + 1, x_2^2 - 1) = x_1 + x_2$	$x_1 + x_2$
Fin de la 2ème itération	$\emptyset$	$\{x_1 + x_2, x_1 x_2 + 1, x_2^2 - 1\}$	$\{x_1 x_2 + 1, x_2^2 - 1\}$ $\{x_1 x_2 + 1, x_1 + x_2\}$ $\{x_2^2 - 1, x_1 + x_2\}$	$S(x_1 x_2 + 1, x_2^2 - 1) = x_1 + x_2$ $S(x_1 + x_2, x_1 x_2 + 1) = x_2^2 - 1$ $S(x_1 + x_2, x_2^2 - 1,) = x_1 + x_2^3$	0 0 0

> **Sortie** :
>
> $$G = \{x_1 + x_2, x_1 x_2 + 1, x_2^2 - 1\}$$