Bases de Gröbner et applications

Chapitre 2 : Algorithme de division

Victor DE NERVO, Matthias HOSTEIN

ENS Rennes

21 Septembre 2022

Ce qu'on a vu

- Définition d'un ordre monomial sur $k[x_1, \ldots, x_n]$,
- Exemples d'ordres monomiaux : $>_{\text{lex}}$, $>_{\text{grlex}}$, $>_{\text{grevlex}}$,
- Représentation matricielle des ordres monomiaux,
- Définition de multideg, LT, LC, LM et leurs propriétés.

Ce qu'on va voir

1. Préliminaires à l'algorithme de division
2. L'algorithme de division dans $k[x_1, \ldots, x_n]$ et quelques mises en garde.

1. Préliminaires à l'algorithme de division
   - Mieux comprendre multideg, LT, LM et LC avec des exemples.
   - Retour sur le cas $k[x]$ et la stratégie de division dans ce cas.

2. L'algorithme de division dans $k[x_1, \dots, x_n]$ et quelques mises en garde.
   - Le théorème et l'algorithme
   - Mises en garde

Quelques exemples

On pose :

- $f = 4x^3y^2z + 2yz + 6x^2$,
- $f_1 = 2x^2y + 6$,
- $f_2 = -3y^2 + 4x - 2$,
- $f_3 = -4x + 2y - 5$

tous dans $\mathbb{Q}[x, y, z]$.

Quelques exemples

On pose :

- $f = 4x^3y^2z + 2yz + 6x^2$,
- $f_1 = 2x^2y + 6$,
- $f_2 = -3y^2 + 4x - 2$,
- $f_3 = -4x + 2y - 5$

tous dans $\mathbb{Q}[x, y, z]$.
Les quantités multideg, LC, LM et LT se "voient" en ordonnant les monômes selon l'ordre monomial chosi.

Quelques exemples : pour l'ordre $>_{\text{lex}}$

En ordonnant les monômes, on a :

- $f = 4x^3y^2z + 6x^2 + 2yz$,
- $f_1 = 2x^2y + 6$,
- $f_2 = 4x - 3y^2 - 2$,
- $f_3 = -4x + 2y - 5$

Le premier terme donne les quatre quantités qui nous intéressent :

P	multideg(P)	LC(P)	LM(P)	LT(P)
f	$(3,2,1)$	4	x^3y^2z	$4x^3y^2z$
f_1	$(2,1,0)$	2	x^2y	$2x^2y$
f_2	$(1,0,0)$	4	x	$4x$
f_3	$(1,0,0)$	-4	x	$-4x$

Quelques exemples : pour l'ordre $>_{\text{grlex}}$

En ordonnant les monômes selon cet ordre, on a :

- $f = 4x^3y^2z + 6x^2 + 2yz$,
- $f_1 = 2x^2y + 6$,
- $f_2 = -3y^2 + 4x - 2$,
- $f_3 = -4x + 2y - 5$.

Le tableau devient donc :

P	multideg(P)	LC(P)	LM(P)	LT(P)
f	$(3,2,1)$	4	x^3y^2z	$4x^3y^2z$
f_1	$(2,1,0)$	2	x^2y	$2x^2y$
f_2	$(0,2,0)$	-3	y^2	$-3y^2$
f_3	$(1,0,0)$	-4	x	$-4x$

Retour sur le cas à une variable : l'importance du degré

Commençons par un petit rappel :

Théorème (Division euclidienne dans $k[x]$)

Pour tous $A, B \in k[x]$, il existe d'uniques polynômes Q et R tels que :

$$A = BQ + R,$$

et

$$deg(R) < deg(B).$$

Retour sur le cas à une variable : l'importance du degré

En pratique, pour effectuer cette division euclidienne, on utilise l'algorithme d'élimination des puissances décroissantes, permettant d'avoir à chaque étape i de l'algorithme :

$$A = BQ^{(i)} + R^{(i)}$$

avec $R^{(0)} = A$ et $\deg(R^{(i+1)}) < \deg(R^{(i)})$: cela justifie la bonne terminaison de l'algorithme.

Retour sur le cas à une variable : mais pourquoi on fait comme ça ?

deg est un cas particulier de multideg en une variable, pour l'ordre $\leq$ sur $\mathbb{N}$. De cet ordre découle également l'ordre de division dans l'algorithme de division euclidienne. Mais pourquoi cet ordre ?

Retour sur le cas à une variable : mais pourquoi on fait comme ça ?

deg est un cas particulier de multideg en une variable, pour l'ordre $\leq$ sur $\mathbb{N}$. De cet ordre découle également l'ordre de division dans l'algorithme de division euclidienne. Mais pourquoi cet ordre ?

Proposition (L'unique ordre monomial sur $k[x]$)

L'unique ordre monomial sur $k[x]$ est l'ordre $\leq$ sur $\mathbb{N}$.

Retour sur le cas à une variable : mais pourquoi on fait comme ça ?

deg est un cas particulier de multideg en une variable, pour l'ordre $\leq$ sur $\mathbb{N}$. De cet ordre découle également l'ordre de division dans l'algorithme de division euclidienne. Mais pourquoi cet ordre ?

Proposition (L'unique ordre monomial sur $k[x]$)

L'unique ordre monomial sur $k[x]$ est l'ordre $\leq$ sur $\mathbb{N}$.

Démonstration

1. Préliminaires à l'algorithme de division
   - Mieux comprendre multideg, LT, LM et LC avec des exemples.
   - Retour sur le cas $k[x]$ et la stratégie de division dans ce cas.

2. L'algorithme de division dans $k[x_1, \dots, x_n]$ et quelques mises en garde.
   - Le théorème et l'algorithme
   - Mises en garde

Le théorème de division dans $k[x_1, \ldots, x_n]$

Théorème

Soient $f \in k[x_1, \ldots, x_n]$ et $F := (f_1, \ldots, f_s) \in k[x_1, \ldots, x_n]^s$ un s-uplet ordonné de polynômes. Alors, il existe $q_1, \ldots, q_s$, $r \in k[x_1, \ldots, x_n]$ tels que :

$$f = \sum_{i=1}^{s} q_i f_i + r$$

avec :

$$\mathit{multideg}(f) \geq \mathit{multideg}(q_i f_i) \quad \forall i \in [\![0, s]\!] \text{ tel que } q_i f_i \neq 0.$$

et où aucun monôme de r n'est divisible par les $LT(f_i)$.

Le théorème de division dans $k[x_1, \ldots, x_n]$

Théorème

Soient $f \in k[x_1, \ldots, x_n]$ *et* $F := (f_1, \ldots, f_s) \in k[x_1, \ldots, x_n]^s$ *un s-uplet ordonné de polynômes. Alors, il existe* $q_1, \ldots, q_s$, $r \in k[x_1, \ldots, x_n]$ *tels que :*

$$f = \sum_{i=1}^{s} q_i f_i + r$$

avec :

$$\text{multideg}(f) \geq \text{multideg}(q_i f_i) \quad \forall i \in [\![0, s]\!] \text{ tel que } q_i f_i \neq 0.$$

et où aucun monôme de r n'est divisible par les $LT(f_i)$.

Remarque : On veut pouvoir diviser par plusieurs polynômes !

Démonstration par l'algorithme de division dans $k[x_1, \dots, x_n]$

```
define division(F, f)
  -- Initialisation
  s := len(F);
  Q := NewList(s);
  r := 0;
  p := f;
  -- Traitement
  while not(IsZero(p)) do
    i := 1;
    divisionAEuLieu := False;
    -- Etape de division
    while i <= s and divisionAEuLieu = False do
      if IsDivisible(LM(p), LM(F[i])) then
        Q[i] := Q[i] + (LM(p)/LM(F[i]));
        p := p - ((LM(p)/LM(F[i]))*F[i]);
        divisionAEuLieu := True;
      else
        i := i+1;
      endif;
    endwhile;
    -- Etape d'élimination de l'excédent
    if divisionAEuLieu = False then
      r := r + LM(p);
      p := p - LM(p);
    endif;
  endwhile;
  -- Fin
  return [Q, r];
enddefine;
```

Exemple de division

Divisons notre f du début par (f_1, f_2, f_3) en considérant l'ordre monomial $>_{\text{grevlex}}$.

Exemple de division

Divisons notre f du début par (f_1, f_2, f_3) en considérant l'ordre monomial $>_{\text{grevlex}}$.
On obtient :

```
Division de
f = 4*x^3*y^2*z +6*x^2 +2*y*z
par
f_1 = 2*x^2*y +6
f_2 = -3*y^2 +4*x -2
f_3 = -4*x +2*y -5

Quotients :
q_1 = 2*x*y*z
q_2 = 2*z -1/2
q_3 = 3*y*z +(-3/2)*x +(-3/4)*y +2*z +11/8
Reste :
r = 13*y*z +(-13/2)*y +14*z +47/8
```

Mises en garde : les propriétés qu'il ne faut pas espérer !

- Le reste dépend de l'ordre de la famille des f_i !

  Si on divise f par (f_2, f_1, f_3) (toujours avec l'ordre $>_{grevlex}$)...

Mises en garde : les propriétés qu'il ne faut pas espérer !

- Le reste dépend de l'ordre de la famille des f_i !
  Si on divise f par (f_2, f_1, f_3) (toujours avec l'ordre $>_{grevlex}$)...

On obtient :

```
Division de
f = 4*x^3*y^2*z +6*x^2 +2*y*z
par
f_2 = -3*y^2 +4*x -2
f_1 = 2*x^2*y +6
f_3 = -4*x +2*y -5

Quotients :
q_2 = (-4/3)*x^3*z +(-35/36)*z -1/2
q_1 = (4/3)*x*z +(-7/3)*z
q_3 = (1/24)*(-32*x^3*z +56*x^2*z -70*x*z -35*y*z -36*x -18*y +(673/6)*z +33)
Reste :
r_rev = (-527/36)*y*z +(-13/2)*y +(5101/144)*z +47/8
```

Mises en garde : les propriétés qu'il ne faut pas espérer !

- Le reste dépend de l'ordre de la famille des f_i !
- Un polynôme de $\langle\{f_i \ ; \ i \in [\![1, s]\!]\}\rangle$ peut avoir un reste non-nul à l'issue de la division !

Mises en garde : les propriétés qu'il ne faut pas espérer !

- Le reste dépend de l'ordre de la famille des f_i !
- Un polynôme de $\langle \{ f_i \ ; \ i \in [\![1, s]\!] \} \rangle$ peut avoir un reste non-nul à l'issue de la division !

  Si on divise $r - r_{rev}$ par (f_1, f_2, f_3)...

Mises en garde : les propriétés qu'il ne faut pas espérer !

- Le reste dépend de l'ordre de la famille des f_i !
- Un polynôme de $\langle\{f_i\ ;\ i \in [\![1, s]\!]\}\rangle$ peut avoir un reste non-nul à l'issue de la division !

  Si on divise $r - r_{rev}$ par (f_1, f_2, f_3)...

  On obtient :

```
Division de
r - r_rev = (995/36)*y*z +(-3085/144)*z
par
f_1 = 2*x^2*y +6
f_2 = -3*y^2 +4*x -2
f_3 = -4*x +2*y -5

Quotients :
q_1 = 0
q_2 = 0
q_3 = 0
Reste :
r_restes = (995/36)*y*z +(-3085/144)*z
```

Mises en garde : les propriétés qu'il ne faut pas espérer !

- Le reste dépend de l'ordre de la famille des f_i !
- Un polynôme de $\langle\{f_i \ ; \ i \in [\![1, s]\!]\}\rangle$ peut avoir un reste non-nul à l'issue de la division !

  Si on divise $r - r_{rev}$ par (f_1, f_2, f_3)...

  On obtient :

```
Division de
r - r_rev = (995/36)*y*z +(-3085/144)*z
par
f_1 = 2*x^2*y +6
f_2 = -3*y^2 +4*x -2
f_3 = -4*x +2*y -5

Quotients :
q_1 = 0
q_2 = 0
q_3 = 0
Reste :
r_restes = (995/36)*y*z +(-3085/144)*z
```

D'où l'intérêt des bases de Gröbner lorsqu'on veut montrer si un polynôme est dans l'idéal... cf. groupes 4 et 5 !

Mises en garde : les propriétés qu'il ne faut pas espérer !

- Le reste dépend de l'ordre de la famille des f_i !
- Un polynôme de $\langle \{f_i \; ; \; i \in [\![1, s]\!]\} \rangle$ peut avoir un reste non-nul à l'issue de la division !
- Tout dépend de l'ordre monomial choisi au départ !

  Si on utilise l'ordre $>_{lex}$...

Mises en garde : les propriétés qu'il ne faut pas espérer !

- Le reste dépend de l'ordre de la famille des f_i !
- Un polynôme de $\langle\{f_i\ ;\ i \in [\![1, s]\!]\}\rangle$ peut avoir un reste non-nul à l'issue de la division !
- Tout dépend de l'ordre monomial choisi au départ !

  Si on utilise l'ordre $>_{lex}$...

On obtient :

```
Division de
f = 4*x^3*y^2*z +6*x^2 +2*y*z
par
f_1 = 2*x^2*y +6
f_2 = 4*x -3*y^2 -2
f_3 = -4*x +2*y -5

Quotients :
q_1 = 2*x*y*z
q_2 = (3/2)*x +(9/8)*y^2 -3*y*z +3/4
q_3 = 0
Reste :
r = (27/8)*y^4 -9*y^3*z +(9/2)*y^2 -4*y*z +3/2
```

Merci de votre attention !

Prochainement : Idéaux monomiaux et bases de Gröbner...