

# Mercredi : Polynômes

Cours de remise à niveau MPRI 2006–2007

David A. Madore

david.madore@ens.fr

13 septembre 2006

# Programme du cours

- ▶ Lundi : Entiers ( $\mathbb{Z}$ )
- ▶ Mardi : Entiers modulaires ( $\mathbb{Z}/n\mathbb{Z}$ )
- ▶ Mercredi : Polynômes ( $k[t]$ )
- ▶ Jeudi : Corps finis ( $\mathbb{F}_q$ )
- ▶ Vendredi : Corps finis, suite ( $\mathbb{F}_q[t]$ )

9h30 à 12h00 ; salle 0D4

Mercredi :  
Polynômes

David Madore

Programme du  
cours

Table des matières

L'anneau des  
polynômes

Arithmétique

Généralités  
Algorithmique

Divers

Résultant  
Plusieurs variables  
Polynômes cyclotomiques

# Table des matières

## L'anneau des polynômes

### Arithmétique

Généralités

Algorithmique

### Divers

Résultant

Plusieurs variables

Polynômes cyclotomiques

Mercredi :  
Polynômes

David Madore

Programme du  
cours

Table des matières

L'anneau des  
polynômes

Arithmétique

Généralités  
Algorithmique

Divers

Résultant  
Plusieurs variables  
Polynômes cyclotomiques

## Définition

Pour l'instant,  $k$  est un **anneau** quelconque (mais souvent ce sera un **corps**).

Un **polynôme** en  $t$  à coefficients dans  $k$  est une somme formelle  $f = a_0 + a_1t + a_2t^2 + \dots$  avec  $a_i \in k$  où *seul un nombre fini* des  $a_i$  est non nul (sinon on parle de **série formelle**).

**Degré** d'un polynôme :  $\deg f =$  le plus grand  $i$  tel que  $a_i \neq 0$  (le degré du polynôme nul est question de convention). On peut donc écrire un polynôme de degré  $\leq N$  comme  $a_0 + \dots + a_N t^N$  ; si  $a_N = 1$  on dit que  $f$  est **unitaire**.

### Opérations :

- ▶ Addition : terme à terme ( $c_i = a_i + b_i$ ).
- ▶ Multiplication : « produit de Cauchy » en développant formellement ( $c_i = \sum_{j=0}^{j=i} a_j b_{i-j}$ ).

## Propriétés du degré :

- ▶  $\deg(f + g) \leq \max(\deg f, \deg g)$  (avec égalité si  $\deg f \neq \deg g$ )
- ▶  $\deg(fg) = \deg f + \deg g$  (dès que  $k$  est intègre)

Si  $k$  est intègre alors  $k[t]$  aussi.

**Complexité** : (sur  $k$  « raisonnable ») essentiellement comme les opérations sur les grands entiers : si  $d = \deg$ ,

- ▶ Addition en  $O(d)$ .
- ▶ Multiplication :
  - ▶ Algorithme naïf en  $O(d^2)$ .
  - ▶ Karatsuba en  $O(d^{\frac{\log 3}{\log 2}})$ .
  - ▶ Schönhage-Strassen en  $O(d \log d \log \log d)$ .

Algorithmes « sophistiqués » beaucoup plus vite intéressants que dans le cas de  $\mathbb{Z}$ .

**Évaluation** de polynômes : si  $f = a_0 + \cdots + a_N t^N$  et  $x \in A$  (une  $k$ -algèbre, par exemple  $k$  ou  $k[t]$ ), on définit  $f(x) = a_0 + \cdots + a_N x^N$ .

Cas particulier : **composition** : si  $g \in k[t]$ , on note  $f \circ g$  plutôt que  $f(g)$ .

**Dérivée** : si  $f = a_0 + a_1 t + \cdots + a_N t^N$  alors  $f' = a_1 + 2a_2 t + \cdots + N a_N t^{N-1}$ .

**Attention** : On peut avoir  $f' = 0$  sans avoir  $f$  constant (e.g.,  $f = t^p$  dans  $\mathbb{F}_p[t]$ ).

**Dérivées successives** :  $f^{(i+1)} = (f^{(i)})'$  pour  $i \in \mathbb{N}$ .

# Formule de Taylor

Mercredi :  
Polynômes

David Madore

Programme du  
cours

Table des matières

L'anneau des  
polynômes

Arithmétique

Généralités  
Algorithmique

Divers

Résultant  
Plusieurs variables  
Polynômes cyclotomiques

Soit  $k$  un corps et  $f \in k[t]$ .

Si  $k$  est de caractéristique zéro, pour tout  $a \in k$  et pour  $N \geq \deg f$  :

$$f = f(a) + (t - a) f'(a) + \frac{(t-a)^2}{2} f''(a) + \dots + \frac{(t-a)^N}{N!} f^{(N)}(a)$$

Permet de reconstruire un polynôme à partir de ses dérivées successives en un point.

**Exercice** : Si  $f \in \mathbb{R}[t]$  vérifie  $f^{(i)}(a) \geq 0$  pour tout  $i \geq 0$  (avec  $a \in \mathbb{R}$  fixé) alors  $f(x) \geq 0$  pour tout  $x \geq a$ .  
(La réciproque est-elle vraie ?)

# Polynôme interpolateur de Lagrange

Mercredi :  
Polynômes

David Madore

Programme du  
cours

Table des matières

L'anneau des  
polynômes

Arithmétique

Généralités  
Algorithmique

Divers

Résultant  
Plusieurs variables  
Polynômes cyclotomiques

Soit  $k$  un corps et  $f \in k[t]$ .

Soient  $a_0, \dots, a_N \in k$  deux à deux distincts, où  $N \geq \deg f$ ,  
et  $b_i = f(a_i)$ , alors

$$f = \sum_{i=0}^N b_i \frac{\prod_{j \neq i} (t - a_j)}{\prod_{j \neq i} (a_i - a_j)}$$

Permet de reconstruire un polynôme à partir de ses valeurs  
en suffisamment de points.

**Exercice** : Quel polynôme  $f \in \mathbb{R}[t]$  de degré  $N$  prend les  
valeurs  $0, 0, \dots, 0, 1$  en  $0, 1, 2, \dots, N$  ?

Sauf mention du contraire,  $k$  est maintenant un **corps**.

**Division euclidienne** analogue à celle des entiers :

Si  $f \in k[t]$  et  $g \in k[t]$  est *non nul*, il existe un unique couple  $(q, r)$  tel que :

- ▶  $q \in k[t]$ ,
- ▶  $r \in k[t]$  est (nul ou) de degré  $\deg r < \deg g$  et
- ▶  $f = gq + r$ .

Comme  $\mathbb{Z}$ , l'anneau  $k[t]$  est **euclidien**.

**Complexité** : comme pour les entiers, algorithme « naïf » en  $O(d^2)$ , algorithme « sophistiqué » en  $O(d \log d \log \log d)$  (très difficile à implémenter!).

**Algorithme « naïf »** de division euclidienne : procéder par puissances *décroissantes* :

Soit  $f = a_N t^N + \cdots + a_0$  et  $g = b_D t^D + \cdots + b_0$  où  $b_D \neq 0$  (donc  $\deg g = D$ ) :

- ▶ si  $N < D$  on renvoie  $q = 0$  et  $r = f$  ;
- ▶ sinon, on pose  $c = a_N/b_D$ , on définit  $f^* = f - ct^{N-D}g$ , donc  $\deg(f^*) < N$ , on applique l'algorithme pour diviser  $f^*$  par  $g$ , soit  $f^* = gq^* + r$  et on a  $f = gq + r$  où  $q = ct^{N-D} + q^*$ .

Relation de **divisibilité** : exactement analogue aux entiers.  
Les **unités** de  $k[t]$  sont les éléments de  $k^\times$  (polynômes constants non nuls).

Polynômes **irréductibles** : définition analogue aux nombres premiers. On les choisira normalement *unitaires*; par convention, 0 et les constantes ne sont pas irréductibles. Les polynômes  $t - a$  (unitaires de degré 1) sont *toujours* irréductibles. Ce sont les seuls ssi le corps  $k$  est algébriquement clos.

Division euclidienne de  $f$  par  $t - a$  : le reste est  $f(a)$  (pourquoi ?).

Sur  $\mathbb{R}$ , les polynômes irréductibles sont les  $t - a$  et les  $t^2 - 2bt + c$  où  $b^2 - c < 0$ .

# Décomposition en facteurs irréductibles

Mercredi :  
Polynômes

David Madore

Programme du  
cours

Table des matières

L'anneau des  
polynômes

Arithmétique

Généralités  
Algorithmique

Divers

Résultant  
Plusieurs variables  
Polynômes cyclotomiques

**Cas général :** écriture unique de tout  $f \in k[t]$  non nul comme  $c \prod_P P^{v_P(f)}$  où  $c \in k^\times$  est le coefficient dominant de  $f$  et  $v_P(f) \in \mathbb{N}$  pour tout  $P$  irréductible.

**Cas de  $k$  algébriquement clos :** tout  $f \in k[t]$  non nul s'écrit de façon unique comme  $c \prod_{a \in k} (t - a)^{v_a(f)}$  où  $c \in k^\times$  est le coefficient dominant de  $f$  et  $v_a(f) \in \mathbb{N}$  est l'ordre du zéro de  $f$  en  $a$ .

# Quotients de $k[t]$

Si  $f \in k[t]$  non nul, on appelle  $(f) = f k[t] = \{fq : q \in k[t]\}$  l'idéal des multiples de  $f$ . On note  $k[t]/(f)$  l'anneau quotient.

C'est un  $k$ -espace vectoriel de dimension  $\deg f$  : si  $\bar{t}$  est l'image (la classe) de  $t \in k[t]$  dans  $k[t]/(f)$ , alors  $k[t]/(f)$  a pour  $k$ -base  $\bar{1}, \bar{t}, \bar{t}^2, \dots, \bar{t}^{\deg f - 1}$ .

- ▶ Si  $f$  (rendu unitaire) est irréductible, alors  $k[t]/(f)$  est un *corps*.
- ▶ Le théorème chinois s'applique : si  $f$  et  $g$  sont premiers entre eux ( $\text{pgcd}(f, g) = 1$ ) alors  $k[t]/(fg)$  est isomorphe au produit de  $k[t]/(f)$  et  $k[t]/(g)$ .

**Exercice** : Décrire précisément la structure de  $\mathbb{R}[t]/(t^2 + 1)$  et  $\mathbb{R}[t]/(t^2 - 1)$ .

# Polynômes à coefficients entiers

Mercredi :  
Polynômes

David Madore

L'anneau  $\mathbb{Z}[t]$  est encore *factoriel*, même s'il n'est pas *euclidien* (ou *principal*).

Si  $f = a_0 + a_1t + \dots + a_Nt^N \in \mathbb{Z}[t]$ , on appelle **contenu** de  $f$ , noté  $\text{cnt}(f)$ , le pgcd de  $a_1, \dots, a_N$ . Lorsque  $\text{cnt}(f) = 1$ , on dit que  $f$  est **primitif**.

Les polynômes irréductibles dans  $\mathbb{Z}[t]$  sont :

- ▶ les nombres premiers (vus comme polynômes constants), et
- ▶ les polynômes primitifs de coefficient dominant positif qui, vus dans  $\mathbb{Q}[t]$  et rendus unitaires, y sont irréductibles.

Les décompositions dans  $\mathbb{Q}[t]$  et dans  $\mathbb{Z}[t]$  sont immédiatement reliées.

Programme du  
cours

Table des matières

L'anneau des  
polynômes

Arithmétique

Généralités  
Algorithmique

Divers

Résultant

Plusieurs variables

Polynômes cyclotomiques

**Exercice :** Soit  $f = a_0 + a_1 t + \cdots + a_N t^N \in \mathbb{Z}[t]$  et  $p$  premier tel que  $p|a_i$  pour  $i < N$ , que  $p^2 \nmid a_0$  (autrement dit  $v_p(a_0) = 1$ ) et que  $p \nmid a_N$ . (Polynôme d'**Eisenstein**.)  
Montrer que  $f$  est irréductible dans  $\mathbb{Q}[t]$  (si on le rend unitaire) ou  $\mathbb{Z}[t]$  (si on le rend de contenu 1 et de coefficient dominant positif). (Indication : étudier les décompositions possibles de  $\bar{f}$  dans  $\mathbb{F}_p[t]$ .)

**Exercice :** Si  $a_1, \dots, a_n$  sont des entiers distincts, montrer que  $\prod_i (t - a_i) - 1$  et  $\prod_i (t - a_i)^2 + 1$  sont irréductibles (dans  $\mathbb{Z}[t]$  ou  $\mathbb{Q}[t]$ ). (Indication : donnée une factorisation  $pq$ , étudier les valeurs possibles de  $p$  et  $q$  en les  $a_i$ , et utiliser des considérations sur le degré.)

# Pseudo-division dans $\mathbb{Z}[t]$

L'anneau  $\mathbb{Z}[t]$  n'est pas euclidien : il n'est même pas *principal* (exemple : idéal des polynômes de coefficient constant pair). On a cependant une **pseudo-division euclidienne** apparentée à celle dans  $\mathbb{Q}[t]$  mais qui évite les divisions d'entiers, en observant que la division dans  $\mathbb{Q}[t]$  de deux polynômes de  $\mathbb{Z}[t]$  ne fait intervenir au dénominateur que le *coefficient dominant* du diviseur :

Si  $f \in \mathbb{Z}[t]$  et  $g \in \mathbb{Z}[t]$  est *non nul* de coefficient dominant  $d$ , il existe un unique couple  $(q, r)$  tel que :

- ▶  $q \in \mathbb{Z}[t]$ ,
- ▶  $r \in \mathbb{Z}[t]$  est (nul ou) de degré  $\deg r < \deg g$  et
- ▶  $d^{\deg f - \deg g + 1} f = gq + r$ .

Exemple :  $f = t^3$  et  $g = 2t + 1$  donnent  $8t^3 = (2t + 1)(4t^2 - 2t + 1) - 1$

L'algorithme d'Euclide est applicable comme dans tout anneau euclidien.

- ▶ Dans  $\mathbb{F}_q[t]$  (sur un corps fini, donc), l'algorithme d'Euclide fonctionne bien.
- ▶ Dans  $\mathbb{Q}[t]$ , l'algorithme d'Euclide fonctionne en théorie, mais *les dénominateurs explosent*. On préfère un algorithme à base de *pseudo-division* qui calcule leur pgcd dans  $\mathbb{Z}[t]$ . Autre possibilité : utilise une *approche modulaire* modulo un premier bien choisi ou beaucoup de petits nombres premiers (et une borne sur les coefficients, p.e. la **borne de Mignotte**).
- ▶ Dans  $\mathbb{R}[t]$  ou  $\mathbb{C}[t]$  (ou  $\mathbb{Q}_p[t]$ ), on ne peut faire que des calculs *approximatifs* : les calculs de pgcd n'ont en général pas de sens (le pgcd n'est pas continu dans les coefficients).

# Comment factoriser dans $\mathbb{F}_q[t]$

Mercredi :  
Polynômes

David Madore

On dispose d'algorithmes *beaucoup plus efficaces* (au moins dans le cas moyen, et pour  $q$  assez petit) que dans  $\mathbb{Z}$ .

**Idée générale** : Pour factoriser  $f \in \mathbb{F}_q[t]$ , on cherche à construire  $h \in \mathbb{F}_q[t]$  de degré  $0 < \deg h < \deg f$  tel que  $h^q \equiv h \pmod{f}$ , autrement dit, tel que  $f$  divise  $h^q - h$ . Or  $h^q - h = \prod_{i \in \mathbb{F}_q} (h - i) \in \mathbb{F}_q[t]$  (pourquoi?). On calcule alors  $\text{pgcd}(f, h - i)$  pour chaque  $i \dots$

Pour trouver  $h$ , diverses méthodes existent : **Berlekamp** (algèbre linéaire sur  $\mathbb{F}_q$ , consiste à construire une matrice  $(\deg f) \times (\deg f)$  et de trouver son noyau),

**Cantor-Zassenhaus** ou **Gathen-Shoup** (calculer  $h = g^{(p^{\deg f} - 1)/(p-1)}$  modulo  $f \dots$ ).

En pratique, on arrive à factoriser des polynômes dans  $\mathbb{F}_2[t]$  dont le degré est dans les dizaines ou centaines de milliers.

Programme du  
cours

Table des matières

L'anneau des  
polynômes

Arithmétique

Généralités

Algorithmique

Divers

Résultant

Plusieurs variables

Polynômes cyclotomiques

# Comment factoriser dans $\mathbb{Z}[t]$

Mercredi :  
Polynômes

David Madore

Programme du  
cours

Table des matières

L'anneau des  
polynômes

Arithmétique

Généralités  
Algorithmique

Divers

Résultant

Plusieurs variables

Polynômes cyclotomiques

Pour factoriser dans  $\mathbb{Z}[t]$  (ou  $\mathbb{Q}[t]$ ), l'algorithme de **Berlekamp-Zassenhaus** a pour principe de

- ▶ factoriser dans  $\mathbb{F}_p[t]$  (pour  $p$  bien choisi),
- ▶ relever la factorisation modulo  $p^2$ ,  $p^4$ ,  $p^8$ , etc., jusqu'à une certaine borne,
- ▶ trouver quels produits de facteurs donnent des polynômes à coefficients entiers.

La dernière étape est problématique si le polynôme a beaucoup de facteurs modulo chaque  $p$  ; des techniques pour l'améliorer sont connues.

## Et dans $\mathbb{C}[t]$ , $\mathbb{R}[t]$ ... ?

Essentiellement de problèmes d'**analyse numérique** : il s'agit essentiellement de

- ▶ isoler les racines,
- ▶ les approcher.

Pour la seconde partie, la méthode de Newton convient bien.

Sur  $\mathbb{R}$ , on utilise le **théorème de Sturm** : si on pose  $f_0 = f$  et  $f_1 = f'$  (dérivée de  $f$ ) et par récurrence  $f_{n+2}$  le reste de la division de  $f_n$  par  $f_{n+1}$ , et  $V_f(x)$  (pour  $x \in \mathbb{R}$  assez général) le nombre de *changements de signe* de la suite  $f_i(x)$  alors le nombre de racines entre deux réels  $a$  et  $b$  est  $V_f(b) - V_f(a)$ .

Sur  $\mathbb{Q}_p$  on se ramène essentiellement au cas de  $\mathbb{F}_p$  par le **lemme de Hensel**.

Soient  $f$  et  $g$  dans  $k[t]$  ( $k$  un corps) non nuls, de degrés respectifs  $m$  et  $n$ . Les  $k$ -espaces vectoriels  $k[t]/(f)$  et  $k[t]/(g)$  ont dimension  $m$  et  $n$  respectivement, et  $k[t]/(fg)$  a pour dimension  $m + n$ . On introduit l'application linéaire

$$\begin{aligned}\varphi: k[t]/(g) \times k[t]/(f) &\rightarrow k[t]/(fg) \\ (y, x) &\mapsto fy + gx\end{aligned}$$

elle est une bijection si et seulement si  $\text{pgcd}(f, g) = 1$ .

On a des bases  $\bar{1}, \bar{t}, \dots, \bar{t}^{m-1}$  et  $\bar{1}, \bar{t}, \dots, \bar{t}^{n-1}$  de  $k[t]/(f)$  et  $k[t]/(g)$ . Le déterminant de  $\varphi$  dans ces bases au départ et dans la base  $\bar{1}, \bar{t}, \dots, \bar{t}^{m+n-1}$  à l'arrivée s'appelle **résultant** ou **déterminant de Sylvester** de  $f$  et  $g$ , noté  $\text{Res}(f, g)$ .

Ainsi,  $\text{Res}(f, g) \neq 0 \iff \text{pgcd}(f, g) = 1$ .

# Résultant (suite)

**Propriété :** Si  $f = a \prod_{i=1}^m (t - \alpha_i)$  alors

$$\text{Res}(f, g) = a^n \prod_{i=1}^m g(\alpha_i)$$

Notamment, si  $g = b \prod_{j=1}^n (t - \beta_j)$  alors

$$\text{Res}(f, g) = a^n b^m \prod_{i,j} (\alpha_i - \beta_j)$$

**Moralité :** Deux polynômes de  $k[t]$  sont premiers entre eux lorsqu'ils n'ont aucune racine commune dans un corps algébriquement clos contenant  $k$ .

**Exercice :** Que vaut  $\text{Res}(f, qf + r)$  en fonction de  $\text{Res}(f, r)$  ?

**Utilité :** Calcul du résultant et calcul du pgcd intimement liés. Le résultant se comporte parfois mieux (il est continu en ses arguments).

**Discriminant** d'un polynôme  $f \in k[t]$  : c'est

$$\text{Disc}(f) = \text{Res}(f, f')$$

**Propriété** : Si  $f = a \prod_{i=1}^m (t - \alpha_i)$  alors

$$\text{Disc}(f) = (-1)^{m(m-1)/2} a^{2m-1} \prod_{i < j} (\alpha_i - \alpha_j)^2$$

**Moralité** :  $\text{Disc}(f) \neq 0$  ssi  $f$  est sans facteur carré.

**Exercice** : Que vaut  $\text{Disc}(fg)$  en fonction de  $\text{Disc}(f)$ ,  $\text{Disc}(g)$  et  $\text{Res}(f, g)$  ?

**Remarque** : On ne connaît pas de méthode algorithmiquement efficace pour déterminer si un entier est sans facteur carré.

On définit par récurrence  $k[t_1, \dots, t_n] = k[t_1] \cdots [t_n]$ .

Propriétés *analogues* à  $\mathbb{Z}[t]$  : c'est un anneau *factoriel* mais non *principal*. Calcul de pgcd « par interpolation de Lagrange ».

Différence importante : pour  $n \geq 2$ , l'élément « générique » de  $k[t_1, \dots, t_n]$  est *irréductible*.

L'étude des idéaux de  $k[t_1, \dots, t_n]$  est l'objet de la **géométrie algébrique**.

Outil très général pour manipuler les idéaux de  $k[t_1, \dots, t_n]$  : cet anneau n'est *pas principal* mais les bases de Gröbner « pallient » en quelque sorte ce fait.

Essentielles pour de nombreux calculs en géométrie algébrique.

Exemple de problème (« théorie de l'élimination ») : trouver une équation polynomiale implicite de la courbe plane réelle décrite paramétriquement par  $x(t) = \frac{t^2-1}{t^2+1}$  et  $y(t) = \frac{2t}{t^2+1}$  (il s'agit d'« éliminer » la variable  $t$ ) ; comment ferait-on avec le déterminant de Sylvester ?

Un polynôme  $f \in k[t_1, \dots, t_n]$  est dit **symétrique** lorsque pour tout  $\sigma \in \mathfrak{S}_n$  on a  $f(t_{\sigma(1)}, \dots, t_{\sigma(n)}) = f(t_1, \dots, t_n)$ .

**Polynômes symétriques élémentaires** : ce sont les  $\Sigma_1, \dots, \Sigma_n$  définis par

$$(u - t_1) \cdots (u - t_n) = u^n - \Sigma_1 u^{n-1} + \cdots + (-1)^n \Sigma_n$$

soit  $\Sigma_1 = t_1 + \cdots + t_n$ ,  $\Sigma_2 = \sum_{i < j} t_i t_j$ , etc.,  $\Sigma_n = t_1 \cdots t_n$ .

**Théorème** : Tout polynôme symétrique est un polynôme (uniquement défini) des  $\Sigma_1, \dots, \Sigma_n$ .

Exemple :  $t_1^2 + \cdots + t_n^2 = \Sigma_1^2 - 2\Sigma_2$

Exercice : exprimer  $t_1^3 + \cdots + t_n^3$  de même.

**Exercice :** (1) Montrer qu'il existe une suite  $\Phi_n \in \mathbb{Z}[t]$

(pour  $n \in \mathbb{N}^*$ ) telle que pour tout  $n$  on ait

$t^n - 1 = \prod_{d|n} \Phi_d$ ; quelles sont les racines de  $\Phi_n$  dans  $\mathbb{C}$ ?

(2) Soit  $p$  premier ne divisant pas  $n$  et  $\bar{\Phi}_n \in \mathbb{F}_p[t]$  la réduction de  $\Phi_n$  modulo  $p$  : montrer que  $\bar{\Phi}_n$  est sans facteur carré.

(3) On veut montrer que  $\Phi_n$  est irréductible dans  $\mathbb{Z}[t]$ . Soit  $f$  un facteur irréductible de  $\Phi_n$  et  $\xi$  une racine de  $f$  : montrer que pour tout  $p$  premier ne divisant pas  $n$ , le complexe  $\xi^p$  est encore racine de  $f$  (indication : sinon,  $f$  divise  $g(t^p)$  pour un autre facteur irréductible  $g$ , et réduire modulo  $p$ ). Conclure.