

# Mathématiques assistées par ordinateur

## Chapitre 3 : Arithmétique des polynômes

Michael Eisermann

Mat249, DLST L2S4, Année 2008-2009  
www-fourier.ujf-grenoble.fr/~eiserm/cours # no  
Document mis à jour le 6 juillet 2009



1/55

## Objectifs de ce chapitre

Nous allons discuter et approfondir l'arithmétique des polynômes sur un corps, notamment à coefficients rationnels, réels, complexes.

Afin de procéder systématiquement et efficacement, nous introduisons d'abord le vocabulaire adéquat (corps et anneaux).

Ensuite on établira quelques outils fondamentaux, notamment

- la division euclidienne :  $S = PQ + R$  où  $\deg R < \deg P$ ,
- l'algorithme d'Euclide pour calculer  $\text{pgcd}(A, B)$ ,
- l'algorithme d'Euclide-Bézout :  $\text{pgcd}(A, B) = AU + BV$ .

Les applications sont nombreuses !

- Décomposition des polynômes et des fractions rationnelles.
- Localisation des racines réelles d'un polynôme réel (Sturm).
- Localisation des racines complexes d'un polynôme complexe.

2/55

## Sommaire

- 1 Arithmétique des polynômes sur un corps, Euclide, Bézout
  - Polynômes sur un corps
  - La division euclidienne
  - Les algorithmes d'Euclide et de Bézout
- 2 Évaluation, racines, décomposition en facteurs irréductibles
  - Fonctions polynomiales, méthode de Horner, Horner-Taylor
  - Multiplicité d'une racine, réduction aux racines simples
  - Décomposition de polynômes en facteurs irréductibles
- 3 Fractions rationnelles, éléments simples, intégration symbolique
  - Le corps des fractions rationnelles
  - Décomposition d'une fraction en fractions simples
  - Primitive d'une fraction rationnelle

3/55 11.1

## Corps

Les nombres rationnels  $(\mathbb{Q}, +, \cdot)$ , les nombres réels  $(\mathbb{R}, +, \cdot)$ , et les nombres complexes  $(\mathbb{C}, +, \cdot)$  jouissent des propriétés suivantes :

$$(A1 : \text{associativité}) \quad \forall a, b, c : (a + b) + c = a + (b + c)$$

$$(A2 : \text{commutativité}) \quad \forall a, b : a + b = b + a$$

$$(A3 : \text{élément neutre}) \quad \exists 0 \forall a : 0 + a = a$$

$$(A4 : \text{élément opposé}) \quad \forall a \exists b : a + b = 0$$

$$(M1 : \text{associativité}) \quad \forall a, b, c : (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

$$(M2 : \text{commutativité}) \quad \forall a, b : a \cdot b = b \cdot a$$

$$(M3 : \text{élément neutre}) \quad \exists 1 \neq 0 \forall a : 1 \cdot a = a$$

$$(M4 : \text{élément inverse}) \quad \forall a \neq 0 \exists b : a \cdot b = 1$$

$$(D : \text{distributivité}) \quad \forall a, b, c : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

### Définition (corps)

Un **corps**  $(\mathbb{K}, +, \cdot)$  est un ensemble  $\mathbb{K}$  muni de deux opérations, appelées addition  $+$  :  $\mathbb{K} \times \mathbb{K} \rightarrow \mathbb{K}$  et multiplication  $\cdot$  :  $\mathbb{K} \times \mathbb{K} \rightarrow \mathbb{K}$ , vérifiant tous les axiomes (A1-4), (M1-4), (D) ci-dessus.

4/55

## Corps finis

Outre les corps  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  il existe beaucoup d'autres exemples !  
Sur l'ensemble  $\mathbb{F}_2 = \{0, 1\}$  à deux éléments on n'a qu'un seul choix :

$$\begin{array}{c|c|c} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ \hline 1 & 1 & 0 \end{array} \quad \text{et} \quad \begin{array}{c|c|c} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ \hline 1 & 0 & 1 \end{array}.$$

### Proposition (le corps à deux éléments)

$(\mathbb{F}_2, +, \cdot)$  est un corps.

**Démonstration.** Les axiomes se vérifient en énumérant tous les cas.  
Alternative : Si l'on interprète 0 et 1 comme « vrai » et « faux » alors la multiplication  $\cdot$  est la conjonction « et » tandis que l'addition  $+$  est la disjonction « ou exclusif ». Sous cette forme vous avez déjà établi la véracité des axiomes lors de votre introduction à la logique.  
Alternative : On peut reconnaître  $\mathbb{F}_2$  comme le quotient  $\mathbb{Z}/2\mathbb{Z}$ .  $\square$

### Remarque

Les corps finis sont fortement utilisés en algèbre et en cryptographie.  
Tout corps fini est de cardinal  $p^k$  pour un premier  $p$ . Réciproquement, pour tout premier  $p$  et  $k \geq 1$  il existe un unique corps de cardinal  $p^k$ .

§1.1

§1.1

§55

## Les quatre opérations dans un corps

On abrège  $a \cdot b$  par  $ab$ . Au lieu de  $a + (b \cdot c)$  on écrit aussi  $a + bc$ .

Les éléments 0 et 1 ainsi que les applications  $a \mapsto -a$  et  $a \mapsto a^{-1}$  ne figurent pas explicitement dans  $(\mathbb{K}, +, \cdot)$ , ils s'en déduisent :

L'élément neutre de l'addition est unique : si  $0 + a = a$  et  $0' + a = a$  pour tout  $a \in \mathbb{K}$ , alors  $0' = 0 + 0' = 0' + 0 = 0$ .

Pour tout  $a \in \mathbb{K}$  l'opposé est unique : Si  $a + b = 0$  et  $a + b' = 0$  alors  $b = 0 + b = b + 0 = b + (a + b') = (b + a) + b' = (a + b) + b' = 0 + b' = b'$ .  
On notera donc sans ambiguïté l'opposé de  $a$  par  $-a$ .

De même l'élément neutre 1 de la multiplication est unique.

Pour tout  $a \in \mathbb{K} \setminus \{0\}$  l'inverse est unique, et sera noté par  $a^{-1}$ .

On a  $ab = 0$  ssi  $a = 0$  ou  $b = 0$  : si  $a \neq 0$  alors  $b = a^{-1}ab = 0$ .

## Anneaux

Les entiers  $(\mathbb{Z}, +, \cdot)$  ne forment pas un corps mais un anneau :

### Définition (anneau)

Un **anneau**  $(\mathbb{A}, +, \cdot)$  est un ensemble muni de deux opérations dont on exige les axiomes ci-dessus à l'exception de M4 (élément inverse).

Ici tout anneau sera donc supposé commutatif (M2) et unitaire (M3).

### Définition (éléments inversibles)

Soit  $a \in \mathbb{A}$ . On dit que  $b \in \mathbb{A}$  est un **inverse** de  $a$  si  $a \cdot b = 1$ .  
Dans ce cas l'inverse de  $a$  est unique et sera noté par  $a^{-1}$ .  
On appelle  $a \in \mathbb{A}$  **inversible** s'il admet un inverse dans  $\mathbb{A}$ .

Dans  $\mathbb{Z}$ , par exemple, les seuls éléments inversibles sont 1 et  $-1$ .  
L'élément 0 n'est jamais inversible : on a toujours  $0 \cdot b = 0 \neq 1$ .  
Un anneau  $\mathbb{A}$  est un corps ssi tout élément  $a \in \mathbb{A}$ ,  $a \neq 0$  est inversible.

On note  $\mathbb{A}^* = \mathbb{A} \setminus \{0\}$  l'ensemble des éléments non nuls,  
et  $\mathbb{A}^\times \subset \mathbb{A}^*$  l'ensemble des éléments inversibles dans  $\mathbb{A}$ .

§1.1

§1.1

§55

## Polynômes

Soit  $\mathbb{K}$  un corps (par exemple  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ ).

Un **polynôme** sur  $\mathbb{K}$  est une expression formelle

$$P = p_0 + p_1X^1 + p_2X^2 + \dots + p_nX^n \quad \text{où } p_0, p_1, p_2, \dots, p_n \in \mathbb{K}.$$

**⚠** Ici  $X$  n'est qu'une variable formelle (et non un élément de  $\mathbb{K}$ ).  
De même,  $P$  n'est qu'une expression formelle (et non une fonction).

**◆** Ce qui compte est la suite des coefficients dans  $\mathbb{K}$  :

$$\sum_{k=0}^n a_k X^k = \sum_{k=0}^n b_k X^k \quad \iff \quad a_k = b_k \text{ pour tout } k = 0, \dots, n$$

**⚠** On peut rajouter ou supprimer des termes nuls,  $0 \cdot X^{n+1}$ .  
Ainsi  $P = \sum_{k=0}^m p_k X^k$  en prolongeant par  $p_{n+1} = \dots = p_m = 0$ ,  
voire  $P = \sum_{k=0}^m p_k X^k$  en prolongeant par  $p_k = 0$  pour tout  $k > n$ .

**◆** Pour l'implémentation il suffit de stocker les coefficients non nuls.  
Typiquement on stocke la suite  $(p_0, p_1, p_2, \dots, p_n)$  telle que  $p_n \neq 0$ .

## L'anneau des polynômes

On note par  $\mathbb{K}[X]$  l'ensemble des polynômes sur l'anneau  $\mathbb{K}$ .

On définit l'addition terme par terme :

$$\left(\sum_{k=0}^n a_k X^k\right) + \left(\sum_{k=0}^n b_k X^k\right) := \sum_{k=0}^n (a_k + b_k) X^k$$

Pour obtenir  $X^i \cdot X^j = X^{i+j}$  on définit la multiplication par

$$\left(\sum_{i=0}^m a_i X^i\right) \cdot \left(\sum_{j=0}^n b_j X^j\right) := \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j\right) X^k$$

◆ Ces définitions se traduisent directement en algorithme de calcul.

### Proposition (l'anneau des polynômes sur $\mathbb{K}$ )

L'ensemble  $\mathbb{K}[X]$  des polynômes sur  $\mathbb{K}$  muni de l'addition + et de la multiplication · définies ci-dessus est un anneau.

On remarque que  $aX^0 + bX^0 = (a+b)X^0$  et  $aX^0 \cdot bX^0 = (ab)X^0$ .

Ainsi on obtient  $\mathbb{K} \subset \mathbb{K}[X]$  en identifiant  $a \in \mathbb{K}$  avec  $aX^0 \in \mathbb{K}[X]$ .

§1.1

§5.1

## L'anneau des polynômes : vérification des axiomes

Pour prouver le théorème il faut vérifier les axiomes un par un.

L'associativité de  $(\mathbb{K}[X], +)$  découle de celle de  $(\mathbb{K}, +)$  :

$$\begin{aligned} [(\sum a_k X^k) + (\sum b_k X^k)] + (\sum c_k X^k) &= [\sum (a_k + b_k) X^k] + (\sum c_k X^k) \\ &= \sum [(a_k + b_k) + c_k] X^k = \sum [a_k + (b_k + c_k)] X^k \\ &= (\sum a_k X^k) + [\sum (b_k + c_k) X^k] = (\sum a_k X^k) + [(\sum b_k X^k) + (\sum c_k X^k)] \end{aligned}$$

La commutativité de  $(\mathbb{K}[X], +)$  découle de celle de  $(\mathbb{K}, +)$  :

$$\begin{aligned} (\sum a_k X^k) + (\sum b_k X^k) &= \sum (a_k + b_k) X^k \\ &= \sum (b_k + a_k) X^k = (\sum b_k X^k) + (\sum a_k X^k) \end{aligned}$$

L'élément neutre de  $(\mathbb{K}[X], +)$  est le polynôme nul :

$$(\sum 0 X^k) + (\sum a_k X^k) = \sum (0 + a_k) X^k = \sum a_k X^k.$$

L'élément opposé de  $\sum a_k X^k$  est  $\sum (-a_k) X^k$  :

$$(\sum a_k X^k) + (\sum (-a_k) X^k) = \sum (a_k + (-a_k)) X^k = \sum 0 X^k.$$

§5.5

## L'anneau des polynômes : vérification des axiomes

L'associativité de  $(\mathbb{K}[X], \cdot)$  repose sur celle de  $(\mathbb{K}, \cdot)$  :

$$\begin{aligned} \left[\left(\sum_i a_i X^i\right) \cdot \left(\sum_j b_j X^j\right)\right] \cdot \left(\sum_k c_k X^k\right) &= \left[\sum_s \left(\sum_{i+j=s} a_i b_j\right) X^s\right] \cdot \left(\sum_k c_k X^k\right) = \sum_t \left(\sum_{i+j+k=t} (a_i b_j) c_k\right) X^t \\ &= \sum_t \left(\sum_{i+j+k=t} a_i (b_j c_k)\right) X^t = \left(\sum_i a_i X^i\right) \cdot \left[\sum_s \left(\sum_{j+k=s} b_j c_k\right) X^s\right] \\ &= \left(\sum_i a_i X^i\right) \cdot \left[\left(\sum_j b_j X^j\right) \cdot \left(\sum_k c_k X^k\right)\right] \end{aligned}$$

La commutativité de  $(\mathbb{K}[X], \cdot)$  repose sur de celle de  $(\mathbb{K}, \cdot)$  :

$$\begin{aligned} \left(\sum_i a_i X^i\right) \cdot \left(\sum_j b_j X^j\right) &= \sum_s \left(\sum_{i+j=s} a_i b_j\right) X^s \\ &= \sum_s \left(\sum_{j+i=s} b_j a_i\right) X^s = \left(\sum_j b_j X^j\right) \cdot \left(\sum_i a_i X^i\right) \end{aligned}$$

L'élément neutre est  $1 \cdot X^0$ . La distributivité est laissée en exercice.

§1.1

§5.1

## L'anneau des polynômes : algorithmes

### Algorithme 1 addition de deux polynômes

**Entrée :** les coefficients de  $A = \sum_{k=0}^n a_k X^k$  et  $B = \sum_{k=0}^n b_k X^k$  sur  $\mathbb{K}$ .

**Sortie :** les coefficients de la somme  $C = A + B$ ,  $C = \sum_{k=0}^n c_k X^k$

```
pour k de 0 à n faire c_k ← a_k + b_k fin pour
retourner (c_0, ..., c_n)
```

### Algorithme 2 multiplication de deux polynômes

**Entrée :** les coefficients de  $A = \sum_{i=0}^m a_i X^i$  et  $B = \sum_{j=0}^n b_j X^j$  sur  $\mathbb{K}$ .

**Sortie :** les coefficients du produit  $C = A \cdot B$ ,  $C = \sum_{k=0}^{m+n} c_k X^k$

```
pour k de 0 à m+n faire c_k ← 0 fin pour
pour i de 0 à m faire
  pour j de 0 à n faire
    c_{i+j} ← c_{i+j} + a_i b_j
  fin pour
fin pour
retourner (c_0, ..., c_{m+n})
```

⚠ Cette méthode de multiplication est de complexité quadratique : elle effectue  $(m+1)(n+1)$  additions et multiplications dans  $\mathbb{K}$ .

§2.55

## Le degré des polynômes

Tout polynôme non nul s'écrit comme  $P = \sum_{k=0}^n p_k X^k$  où  $p_n \neq 0$ .

Cette écriture est unique. On appelle  $\deg P := n$  le **degré** de  $P$ , et  $\text{dom } P := p_n$  le **coefficient dominant** de  $P$ .

Le polynôme nul est particulier ; on pose  $\deg 0 := -\infty$  et  $\text{dom } 0 := 0$ .

### Proposition (propriétés du degré sur un corps)

On a  $\deg(P + Q) \leq \sup\{\deg P, \deg Q\}$ , avec égalité si  $\deg P \neq \deg Q$ .

On a  $\deg(PQ) = \deg P + \deg Q$  et  $\text{dom}(PQ) = \text{dom } P \cdot \text{dom } Q$ .  
Soulignons en particulier que  $P \neq 0$  et  $Q \neq 0$  implique  $PQ \neq 0$ .

**Démonstration.** Supposons  $P = p_0 + p_1 X^1 + \dots + p_n X^n$  avec  $p_n \neq 0$  et  $Q = q_0 + q_1 X^1 + \dots + q_m X^m$  avec  $q_m \neq 0$ . Alors

$$PQ = p_0 q_0 + (p_0 q_1 + p_1 q_0) X^1 + \dots + (p_n q_m) X^{m+n}.$$

Dans un corps  $p_n \neq 0$  et  $q_m \neq 0$  implique  $p_n q_m \neq 0$ .

On conclut que  $\deg(PQ) = n + m$  et  $\text{dom}(PQ) = \text{dom } P \cdot \text{dom } Q$ .

Si  $P = 0$  ou  $Q = 0$ , on a  $PQ = 0$  et  $\deg(PQ) = \deg P + \deg Q$  selon la convention  $(-\infty) + \deg Q = -\infty$  et  $\deg P + (-\infty) = -\infty$ .  $\square$

§1.1

15.55

14.55

## La division euclidienne : existence et unicité

Soit  $\mathbb{K}$  un corps (par exemple  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ ).

### Proposition (division euclidienne de polynômes)

Soit  $P \in \mathbb{K}[X]$  un polynôme non nul. Alors pour tout  $S \in \mathbb{K}[X]$  il existe une unique paire  $Q, R \in \mathbb{K}[X]$  telle que  $S = PQ + R$  et  $\deg R < \deg P$ .

### Définition (quotient et reste)

Si  $S = PQ + R$  et  $\deg R < \deg P$ , on appelle  $S$  quo  $P := Q$  le **quotient** et  $S \text{ rem } P := R$  le **reste** de la division euclidienne de  $S$  par  $P$ .

$$\begin{array}{r} (X^5 + 1) \\ - (X^5 - 3X^4) \\ \hline (3X^4 + 1) \\ - (3X^4 - 9X^3) \\ \hline (9X^3 + 1) \\ - (9X^3 - 27X^2) \\ \hline (27X^2 + 1) \end{array} = (X^3 - 3X^2)(X^2 + 3X + 9) + (27X^2 + 1)$$

## La division euclidienne : démonstration

**Unicité.** Si l'on avait  $PQ + R = P'Q' + R'$  avec  $\deg R < \deg P$  et  $\deg R' < \deg P$ , alors on aurait  $P(Q - Q') = R' - R$ , donc  $\deg P + \deg(Q - Q') = \deg(R' - R) < \deg P$ .

Ceci n'est possible que pour  $\deg(Q - Q') < 0$ , d'où  $Q - Q' = 0$ . On conclut que  $Q = Q'$  puis  $R = R'$ .

**Existence.** Si  $\deg S < \deg P$  alors  $Q = 0$  et  $R = S$  conviennent.

Pour  $\deg S \geq \deg P$  on procède par récurrence sur  $n = \deg S$ . On suppose le résultat vrai pour tout polynôme  $\tilde{S}$  avec  $\deg \tilde{S} < n$ .

On pose  $M = \text{dom}(P)^{-1} \text{dom}(S) \cdot X^{\deg S - \deg P}$  et  $\tilde{S} = S - PM$ . Ainsi  $\deg(PM) = \deg S$  et  $\text{dom}(PM) = \text{dom } S$ , donc  $\deg \tilde{S} < \deg S$ .

Il existe  $\tilde{Q}, R \in A[X]$  tels que  $\tilde{S} = P\tilde{Q} + R$  et  $\deg R < \deg P$ . Ainsi  $S = \tilde{S} + PM = P\tilde{Q} + R + PM$  en posant  $Q = \tilde{Q} + M$ .

◆ Cette construction se traduit en l'algorithme bien connu.

§1.2

15.55

## La division euclidienne : algorithme

### Algorithme 3 division euclidienne de deux polynômes

**Entrée:** deux polynômes  $S, P \in \mathbb{K}[X]$ ,  $P \neq 0$ , sur un corps  $\mathbb{K}$ .

**Sortie:** les polynômes  $Q, R \in \mathbb{K}[X]$  vérifiant  $S = PQ + R$  et  $\deg R < \deg P$ .

```
Q ← 0; R ← S // invariant S = PQ + R
tant que deg R ≥ deg P faire
    M ← dom(P)-1 dom(R) · Xdeg R - deg P // R = PM en degré dominant
    Q ← Q + M; R ← R - PM // préserve S = PQ + R
fin tant que
retourner (Q, R)
```

### Proposition

L'algorithme 3 ci-dessus est correct.

**Terminaison.** Le monôme  $M$  est choisi de sorte que  $R$  et  $PM$  aient le même degré et coefficient dominant. Ainsi  $\deg(R - PM) < \deg R$ . L'algorithme se termine après au plus  $1 + \deg S - \deg P$  itérations.

**Validité.** L'initialisation  $Q \leftarrow 0, R \leftarrow S$  assure que  $S = PQ + R$ , et chaque itération  $Q \leftarrow Q + M, R \leftarrow R - PM$  conserve cette égalité.

15.55

## Divisibilité

### Définition

Soient  $A, B \in \mathbb{K}[X]$  deux polynômes sur  $\mathbb{K}$ . On dit que  $A$  **divise**  $B$  dans  $\mathbb{K}[X]$ , noté  $A \mid B$ , s'il existe  $Q \in \mathbb{K}[X]$  de sorte que  $AQ = B$ .

Par exemple,  $X + 1$  divise  $X^2 - 1$  car  $(X + 1)(X - 1) = X^2 - 1$ .

### Notation

On écrit  $P_1 \sim P_2$  si  $P_1 = cP_2$  pour un facteur constant  $c \in \mathbb{K}^\times$ . Dans ce cas on dit que  $P_1$  et  $P_2$  sont **proportionnels**.

Si  $P_1 \sim P_2$ , alors  $A \mid P_1 \Leftrightarrow A \mid P_2$  et  $P_1 \mid B \Leftrightarrow P_2 \mid B$ .

### Observation

On a toujours  $A \mid A$  (réflexivité),  
 $A \mid B$  et  $B \mid C$  implique  $A \mid C$  (transitivité),  
 $A \mid B$  et  $B \mid A$  implique  $A \sim B$  (antisymétrie).

Dans ce sens la divisibilité définit un ordre partiel sur les polynômes. Dans cet ordre, 1 est minimal car  $1 \mid P$  pour tout  $P \in \mathbb{K}[X]$ . De même, 0 est maximal car  $P \mid 0$  pour tout  $P \in \mathbb{K}[X]$ .

§1.2

17/55

## Divisibilité : vérification des propriétés

**Rappel.** On a  $A \mid B$  s'il existe  $Q$  de sorte que  $AQ = B$ .

**Réflexivité :**  $A \mid A$ .

C'est clair car  $A \cdot 1 = A$ .

**Transitivité :**  $A \mid B$  et  $B \mid C$  implique  $A \mid C$ .

Si  $AU = B$  et  $BV = C$  alors  $A(UV) = C$ .

**Antisymétrie :**  $A \mid B$  et  $B \mid A$  implique  $A \sim B$ .

Si  $A = 0$  alors  $B = AU = 0$ , et on a  $A \sim B$ . Supposons donc  $A \neq 0$ .

Par hypothèse on a  $AU = B$  et  $BV = A$ , donc  $AUV = A$ , soit encore  $A(UV - 1) = 0$ . Puisque  $A \neq 0$  ceci implique  $UV = 1$ . Ensuite  $UV = 1$  implique  $\deg U = \deg V = 0$  et donc  $U, V \in \mathbb{K}^\times$ . On conclut que  $A \sim B$ .

**Observation.** Si  $A \mid B$  et  $A \mid C$  alors  $A \mid (B + C)$ .

Par distributivité  $AU = B$  et  $AV = C$  implique  $A(U + V) = B + C$ .

§1/55

## Définition du pgcd

### Définition

On dit que  $C$  est un **diviseur commun** de  $A_1, \dots, A_n$  si  $C \mid A_k$  pour tout  $k$ . On note  $\mathcal{D}(A_1, \dots, A_n)$  l'ensemble des diviseurs communs.

On dit que  $D \in \mathcal{D}(A_1, \dots, A_n)$  est un **plus grand commun diviseur** (pgcd) si tout autre diviseur commun  $C \in \mathcal{D}(A_1, \dots, A_n)$  divise  $D$ .

On note  $\text{pgcd}(A_1, \dots, A_n)$  le **pgcd unitaire** de  $A_1, \dots, A_n$ , si non nul.

**Exemple :**  $A_1 = 3X^2 - 6X - 9 = (3X - 9)(X + 1)$   
 et  $A_2 = 6X^2 - 10X - 24 = (2X - 6)(3X + 4)$  dans  $\mathbb{Q}[X]$ .  
 Ici  $X - 3$  ou  $2X - 6$  ou  $3X - 9$  sont des diviseurs communs, voire des pgcd de  $A_1$  et  $A_2$ . À noter qu'ils sont proportionnels entre eux.

⚠ Cette ambiguïté nous oblige à dire **un** pgcd et non **le** pgcd. Pour nos implémentations ceci pose un problème de spécification.

📍 On privilégiera le pgcd unitaire, à coefficient dominant 1. Sur un corps on peut toujours passer de  $P$  à  $P/\text{dom}(P)$ .

§1.3

19/55

## Existence du pgcd : algorithme préliminaire

Soit  $A, B \in \mathbb{K}[X]$  deux polynômes. On itère la division euclidienne :

$$\begin{aligned} R_0 &= A \\ R_1 &= B \\ R_2 &= R_0 \text{ rem } R_1 &= R_0 - R_1 Q_1 \\ &\vdots &\vdots \\ R_n &= R_{n-2} \text{ rem } R_{n-1} &= R_{n-2} - R_{n-1} Q_{n-1} \\ 0 &= R_{n-1} \text{ rem } R_n &= R_{n-1} - R_n Q_n \end{aligned}$$

La terminaison est assurée car  $\deg R_1 > \deg R_2 > \dots > \deg R_n$ . Après un nombre fini d'itération on tombe donc sur  $R_{n+1} = 0$ .

### Proposition

Le dernier reste  $R_n$  non nul est un pgcd de  $A$  et  $B$ .

### Démonstration.

Par hypothèse  $R_n$  divise  $R_{n-1}, R_{n-2}, \dots, R_2$  puis  $R_1 = B, R_0 = A$ . C'est donc un diviseur commun de  $A$  et  $B$ . Réciproquement, si  $P$  divise  $R_0 = A$  et  $R_1 = B$  alors il divise aussi  $R_2, \dots, R_n$ .  $\square$

20/55

## Propriétés du pgcd

On a défini le pgcd unitaire de sorte qu'il soit **unique**.  
On vient de prouver qu'il **existe**. Il reste à le **calculer** efficacement.

### Observation

On a  $\mathcal{D}(A_1, \dots, A_n) = \mathcal{D}(\text{pgcd}(A_1, \dots, A_{n-1}), A_n)$ .  
Ainsi  $\text{pgcd}(A_1, \dots, A_n) = \text{pgcd}(\text{pgcd}(A_1, \dots, A_{n-1}), A_n)$ .  $\square$

Il suffit donc de savoir calculer le pgcd de deux polynômes.

### Observation

On a  $\mathcal{D}(A, B) = \mathcal{D}(B, A) = \mathcal{D}(B, A - QB)$ ,  
d'où  $\text{pgcd}(A, B) = \text{pgcd}(B, A) = \text{pgcd}(B, A - QB)$ .  $\square$

C'est l'observation clé pour l'algorithme d'Euclide.

### Observation

On a finalement le cas trivial  $\text{pgcd}(A, 0) = A / \text{dom}(A)$ .  $\square$

C'est la condition d'arrêt dans l'algorithme d'Euclide.

§1.3

21.55

## L'algorithme d'Euclide, version prête à programmer

### Algorithme 4 calcul du pgcd selon Euclide

**Entrée:** deux polynômes  $A_0, B_0 \in \mathbb{K}[X]$  sur un corps  $\mathbb{K}$

**Sortie:** le pgcd de  $A_0$  et  $B_0$  dans  $\mathbb{K}[X]$ , unitaire si non nul

```
A ← A0, B ← B0 // pgcd(A, B) = pgcd(A0, B0)
tant que B ≠ 0 faire
  R ← A rem B // A = QB + R et deg R < deg B
  A ← B, B ← R // pgcd(A, B) = pgcd(B, R)
fin tant que
si A = 0 alors retourner 0 sinon retourner A / dom(A)
```

### Théorème

L'algorithme 4 ci-dessus est correct :

- Il se termine [après au plus  $\deg(B_0) + 1$  itérations].
- Il renvoie le pgcd unitaire de  $A_0$  et  $B_0$ .

22/55

## L'algorithme d'Euclide : démonstration

**Terminaison.** Dans chaque itération  $\deg(B)$  diminue. Après au plus  $\deg(B_0) + 1$  itérations on arrive à  $B = 0$  et l'algorithme s'arrête.

**Correction.** On cherche à calculer  $\text{pgcd}(A_0, B_0)$ .  
Initialement  $A = A_0$  et  $B = B_0$  donc  $\text{pgcd}(A, B) = \text{pgcd}(A_0, B_0)$ .

Cas exceptionnel : pour  $A_0 = B_0 = 0$  l'algorithme s'arrête tout de suite avec  $A = 0$  et on renvoie  $\text{pgcd}(0, 0) = 0$ , ce qui est correct.

Les polynômes  $A$  et  $B$  changent, mais  $\text{pgcd}(A, B)$  est invariant :  
chaque itération le conserve car  $\text{pgcd}(A, B) = \text{pgcd}(B, A - BQ)$ .

À la fin on a  $A \neq 0$  et  $B = 0$ , et on renvoie  $\text{pgcd}(A, B) = A / \text{dom}(A)$ .  
Par l'invariance on a toujours  $\text{pgcd}(A, B) = \text{pgcd}(A_0, B_0)$ .  $\square$

§1.3

23.55

## L'algorithme d'Euclide-Bézout

### Théorème (identité de Bézout)

Pour tout  $A, B \in \mathbb{K}[X]$  il existe  $U, V \in \mathbb{K}[X]$  tels que  
 $\text{pgcd}(A, B) = AU + BV$ . L'algorithme 5 les calcule.

### Algorithme 5 Euclide-Bézout

**Entrée:** deux polynômes  $A_0, B_0 \in \mathbb{K}[X]$  sur un corps  $\mathbb{K}$

**Sortie:** trois polynômes  $D, U, V$  tels que  $D = A_0U + B_0V = \text{pgcd}(A_0, B_0)$

```
( A U V ) ← ( A0 1 0 ) // invariant { A = A0U + B0V
( B S T ) ← ( B0 0 1 ) { B = A0S + B0T
tant que B ≠ 0 faire
  Q ← A quo B // A = QB + R, deg R < deg B
  ( A U V ) ← ( B S T )
  ( B S T ) ← ( A - QB U - QS V - QT )
fin tant que
si A = 0 alors retourner le triplet [0, 0, 0] sinon
retourner le triplet [A / dom(A), U / dom(A), V / dom(A)]
```

⚠ Les coefficients  $U, V$  ne sont pas uniques : Pour tout  $Q \in \mathbb{K}[X]$   
les coefficients  $U' = U + QB/D$  et  $V' = V - QA/D$  marchent aussi.

24/55

## L'algorithme d'Euclide-Bézout : démonstration

Il existe plusieurs façon de démontrer ce théorème. Comme il s'agit d'un énoncé d'existence pour  $U$  et  $V$  nous devons construire deux polynômes  $U$  et  $V$  qui conviennent. Ici nous prouvons ce théorème en montrant que l'algorithme ci-dessus est correct.

**Terminaison.** Dans chaque itération  $\deg(B)$  diminue. Après au plus  $\deg(B_0) + 1$  itérations on arrive à  $B = 0$  et l'algorithme s'arrête.

**Correction.** On cherche à calculer  $\text{pgcd}(A_0, B_0) = A_0U + B_0V$ .

Cas exceptionnel : pour  $A_0 = B_0 = 0$  l'algorithme s'arrête tout de suite et on renvoie  $(0, 0, 0)$ , ce qui est correct.

Initialement  $A = A_0$  et  $B = B_0$  donc  $\text{pgcd}(A, B) = \text{pgcd}(A_0, B_0)$ . Le polynôme  $\text{pgcd}(A, B)$  est invariant pendant l'algorithme. À la fin on a  $B = 0$  donc  $\text{pgcd}(A, B) = A / \text{dom}(A)$ .

L'initialisation assure que  $A = A_0U + B_0V$  et  $B = A_0S + B_0T$ . Chaque itération conserve précieusement ces égalités. À la fin on a  $\text{pgcd}(A_0, B_0) = A / \text{dom}(A)$  ainsi que  $A / \text{dom}(A) = A_0 \cdot U / \text{dom}(A) + B_0 \cdot V / \text{dom}(A)$ . □

§1.3

25/55

## Non-unicité des coefficients de Bézout

### Lemme (de Gauss)

Si  $\text{pgcd}(A, B) = 1$  alors  $A \mid BC$  implique  $A \mid C$ .

**Démonstration.** Supposons que  $AU + BV = 1$  ainsi que  $AQ = BC$ . Alors  $C = (AU + BV)C = AUC + BVC = A(UC + QV)$ . □

### Proposition

Soit  $D = \text{pgcd}(A, B)$  et  $AU_0 + BV_0 = D$ . Alors  $AU_1 + BV_1 = D$  implique  $U_1 = U_0 + QB/D$  et  $V_1 = V_0 - QA/D$  pour un  $Q \in \mathbb{K}[X]$ .

### Démonstration.

Quitte à passer à  $A/D$  et  $B/D$  on peut supposer que  $D = 1$ . Pour  $U = U_0 - U_1$  et  $V = V_0 - V_1$  on trouve  $AU + BV = 0$ . Or,  $A \mid BV$  implique  $A \mid V$ . Donc  $V = QA$ , puis  $U = -QB$ . □

### Corollaire

S'il existe une **solution minimale** vérifiant  $\deg U_0 < \deg(B/D)$  et  $\deg V_0 < \deg(A/D)$  alors elle est nécessairement unique. □

§1.3

## L'algorithme d'Euclide-Bézout : minimalité

### Proposition

Supposons que  $A_0, B_0 \in \mathbb{K}[X]^*$  ne sont pas proportionnels,  $A_0 \not\sim B_0$ . Alors les coefficients de Bézout  $U, V$  calculés par l'algorithme 5 sont minimaux : on a  $\deg U < \deg(B_0/D)$  et  $\deg V < \deg(A_0/D)$ .

**Esquisse de démonstration** (à détailler en exercice)

Si  $\deg A_0 > \deg B_0 \geq 0$ , alors on trouve après une itération

$$\deg A > \deg B, \quad \deg A + \deg U < \deg B_0, \quad \deg A + \deg V < \deg A_0, \\ \deg A + \deg S = \deg B_0, \quad \deg A + \deg T = \deg A_0.$$

Si  $\deg A_0 \leq \deg B_0$ , il faut deux itérations initiales pour y arriver.

Les itérations suivantes préservent ces relations. On s'arrête avec  $B = 0$  et  $A \sim D$ , donc  $\deg U < \deg(B/D)$  et  $\deg V < \deg(A/D)$ . □

**Remarque.** Ces inégalités ne tiennent plus dans les cas dégénérés :

- Si  $A_0 = 0$  on a  $D \sim B_0$  donc  $\deg D = \deg B_0 \geq \deg A_0$ .
- Si  $B_0 = 0$  on a  $D \sim A_0$  donc  $\deg D = \deg A_0 \geq \deg B_0$ .
- Si  $A_0 \sim B_0$  on a  $D \sim A_0 \sim B_0$  donc  $\deg D = \deg A_0 = \deg B_0$ .

Dans tout autre cas la proposition s'applique comme esquisé.

§1.3

27/55

## Fonctions polynomiales

### Définition

Soit  $P = \sum_{k=0}^n a_k X^k$  un polynôme dans  $\mathbb{K}[X]$ . On définit l'**évaluation** de  $P$  en  $x \in \mathbb{K}$  par  $P(x) := \sum_{k=0}^n a_k x^k$ .

Autrement dit, on substitue la variable  $X$  par un élément  $x \in \mathbb{K}$ .

Pour tout  $P, Q \in \mathbb{K}[X]$  l'évaluation en  $x \in \mathbb{K}$  vérifie  $(P + Q)(x) = P(x) + Q(x)$  et  $(P \cdot Q)(x) = P(x) \cdot Q(x)$ .

### Définition

Tout polynôme  $P = \sum_{k=0}^n a_k X^k$  dans  $\mathbb{K}[X]$  induit une **fonction polynomiale**  $f_P: \mathbb{K} \rightarrow \mathbb{K}$  par  $x \mapsto P(x) = \sum_{k=0}^n a_k x^k$ .

⚠ *Expression  $\neq$  fonction !* Ne pas confondre le polynôme  $P \in \mathbb{K}[X]$  et la fonction polynomiale  $f_P: \mathbb{K} \rightarrow \mathbb{K}$  associée.

### Exemple

Le polynôme  $P = X^2 + X$  dans  $\mathbb{F}_2[X]$  est non nul mais induit la fonction nulle :  $f_P(0) = 0^2 + 0 = 0$  et  $f_P(1) = 1^2 + 1 = 0$ .

28/55

## La méthode de Horner : calcul de $P(x_0)$

Soit  $P = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$  un polynôme dans  $\mathbb{K}[X]$ .  
Comment calculer efficacement  $P(x)$  pour  $x \in \mathbb{K}$  ?

**Méthode naïve** : On calcule  $a_k x^k$  en effectuant  $k$  multiplications.  
Implémenté ainsi, le calcul de  $P(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$  nécessite  $n$  additions et  $1 + 2 + \dots + n = \frac{n(n+1)}{2}$  multiplications.

**Méthode de Horner** : En profitant de la distributivité on évalue  $P(x) = ((\dots((a_nx + a_{n-1})x + a_{n-2}) \dots (a_2)x + a_1)x + a_0$ .  
Ceci ne nécessite que  $n$  additions et  $n$  multiplications !

Exemples : Pour  $n = 100$  on passe de 5050 à 100 multiplications.  
Pour  $n = 1000$  on passe de 500500 à 1000 multiplications.

---

### Algorithme 6 évaluation d'un polynôme selon Horner

---

**Entrée** : des coefficients  $a_0, a_1, a_2, \dots, a_n \in \mathbb{K}$  et un élément  $x_0 \in \mathbb{K}$ .

**Sortie** : la valeur  $y = a_0 + a_1x_0 + a_2x_0^2 + \dots + a_nx_0^n$ .

---

$y \leftarrow a_n$

**pour**  $k$  de  $n-1$  à 0 **faire**  $y \leftarrow y \cdot x_0 + a_k$  **fin pour**  
**retourner**  $y$

---

## Transformer $P(X)$ en $P(X + x_0)$

Soit  $P = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$  un polynôme et  $x_0 \in \mathbb{K}$ .  
Comment calculer les coefficients  $b_0, b_1, b_2, \dots, b_n$  tels que  $P = b_0 + b_1(X - x_0) + b_2(X - x_0)^2 + \dots + b_n(X - x_0)^n$  ?

**Première méthode** : Par la formule binomiale on trouve

$$\begin{aligned} \sum_{k=0}^n b_k X^k &= P(X + x_0) = \sum_{\ell=0}^n a_\ell (X + x_0)^\ell = \sum_{\ell=0}^n a_\ell \sum_{k=0}^{\ell} \binom{\ell}{k} X^k x_0^{\ell-k} \\ &= \sum_{k=0}^n \sum_{\ell=0}^n a_\ell \binom{\ell}{k} X^k x_0^{\ell-k} = \sum_{k=0}^n \left( \sum_{\ell=0}^n a_\ell \binom{\ell}{k} x_0^{\ell-k} \right) X^k. \end{aligned}$$

Ainsi on obtient la formule  $b_k = \sum_{\ell=k}^n \binom{\ell}{k} a_\ell x_0^{\ell-k}$ .

**Seconde méthode** : Par la formule de Taylor on trouve d'une part  $P^{(k)}(x_0) = \sum_{\ell=k}^n \frac{\ell!}{(\ell-k)!} a_\ell x_0^{\ell-k}$  et d'autre part  $P^{(k)}(x_0) = k! b_k$ .

On obtient la même formule  $b_k = \sum_{\ell=k}^n \binom{\ell}{k} a_\ell x_0^{\ell-k}$ .

⚠ Cette formule est belle et explicite, mais pas encore optimale :  
La méthode de Horner calcule  $b_0, b_1, \dots, b_n$  avec moins d'opérations.

## La méthode de Horner-Taylor : calcul de $P(X + x_0)$

### Objectif.

Étant donné  $P = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$  et  $x_0 \in \mathbb{K}$   
on cherche  $P = b_0 + \underbrace{b_1(X - x_0) + b_2(X - x_0)^2 + \dots + b_n(X - x_0)^n}_{(X - x_0)Q}$ .

### Méthode de Horner :

On effectue une division euclidienne  $P = q_0 + (X - x_0)Q$ .

---

### Algorithme 7 division euclidienne par $(X - x_0)$

---

**Entrée** : des coefficients  $a_0, a_1, a_2, \dots, a_n \in \mathbb{K}$  et un élément  $x_0 \in \mathbb{K}$ .

**Sortie** : des coefficients  $q_0, q_1, q_2, \dots, q_n \in \mathbb{K}$  tels que  $P = q_0 + (X - x_0)Q$  où  $P = \sum_{k=0}^n a_k X^k$  et  $Q = \sum_{k=0}^{n-1} q_{k+1} X^k$ .

---

$q_n \leftarrow a_n$

**pour**  $k$  de  $n-1$  à 0 **faire**  $q_k \leftarrow q_{k+1} \cdot x_0 + a_k$  **fin pour**  
**retourner**  $q_0, q_1, q_2, \dots, q_n$

---

Ainsi  $b_0 = q_0$  et  $b_1 + b_2(X - x_0) + \dots + b_n(X - x_0)^{n-1} = Q$ .

On calcule ensuite les coefficients  $b_1, b_2, \dots, b_n$  par récurrence.

## La méthode de Horner-Taylor, prête à programmer

L'algorithme 8 résume la méthode issue de notre discussion :

---

### Algorithme 8 la méthode de Horner-Taylor

---

**Entrée** :  $a_0, a_1, \dots, a_n \in \mathbb{K}$  et  $x_0 \in \mathbb{K}$ .

**Sortie** :  $b_0, b_1, \dots, b_n \in \mathbb{K}$  tels que  $\sum_{k=0}^n b_k (X - x_0)^k = \sum_{k=0}^n a_k X^k$ .

---

**pour**  $j$  de 0 à  $n$  **faire**  $b_j \leftarrow a_j$  **fin pour**

**pour**  $\ell$  de 0 à  $n-1$  **faire**

**pour**  $k$  de  $n-1$  à  $\ell$  **faire**  $b_k \leftarrow b_{k+1} \cdot x_0 + b_k$  **fin pour**

**fin pour**

**retourner**  $b_0, b_1, \dots, b_n$

---

### Conclusion

Étant donné  $P = \sum a_k X^k$ , les coefficients de  $P = \sum b_k (X - x_0)^k$  peuvent être calculés avec  $\frac{n(n+1)}{2}$  multiplications et  $\frac{n(n+1)}{2}$  additions.

## Multiplicité d'une racine

On dit que  $r \in \mathbb{K}$  est une **racine** de  $P \in \mathbb{K}[X]$  si  $P(r) = 0$ .

### Proposition

Un élément  $r \in \mathbb{K}$  est une racine de  $P$  ssi  $P = (X - r)Q$  où  $Q \in \mathbb{K}[X]$ .

**Démonstration.** Il existe des polynômes  $Q, R \in \mathbb{K}[X]$  tels que  $P = (X - r)Q + R$  et  $\deg R < \deg(X - r) = 1$ , donc  $R \in \mathbb{K}$ . Ainsi  $P(r) = R$  s'annule si et seulement si  $R = 0$ .  $\square$

### Corollaire

Pour tout  $P \in \mathbb{K}[X]^*$  et tout  $r \in \mathbb{K}$  il existe un unique entier  $m \geq 0$  tel que  $P = (X - r)^m Q$  et  $Q(r) \neq 0$ .  $\square$

Si  $m \geq 1$  on dit que  $r$  est une racine de  $P$  de **multiplicité**  $m$ . La racine est **simple** si  $m = 1$ , et **multiple** si  $m \geq 2$ .

§2.2

33/55

## Factorisation et racines

### Corollaire

Tout  $P \in \mathbb{K}[X]^*$  s'écrit comme  $P = (X - r_1)^{m_1} \cdots (X - r_k)^{m_k} Q$  où  $r_1, \dots, r_k \in \mathbb{K}$  sont des racines distinctes, de multiplicité  $m_1, \dots, m_k \geq 1$ , et  $Q \in \mathbb{K}[X]$  n'a pas de racine dans  $\mathbb{K}$ .

Ainsi un polynôme de degré  $n$  sur  $\mathbb{K}$  admet au plus  $n$  racines dans  $\mathbb{K}$ .

**Démonstration.** On suppose  $P \neq 0$  donc  $\deg(P) \geq 0$ .

On procède par récurrence sur  $\deg P$  :

■ Si  $\deg(P) = 0$  alors  $P$  n'a pas de racines et  $P = Q$  convient.

■ Si  $\deg(P) \geq 1$  on distingue deux cas :

Si  $P$  n'a pas de racines, alors  $P = Q$  convient.

Si  $P$  admet une racine  $r_1 \in \mathbb{K}$ , alors il existe  $P^* \in \mathbb{K}[X]$

tel que  $P = (X - r_1)^{m_1} P^*$  avec  $m_1 \geq 1$  et  $P^*(r_1) \neq 0$ .

Par récurrence on sait que  $P^* = (X - r_2)^{m_2} \cdots (X - r_k)^{m_k} Q$ , où  $r_2, \dots, r_k \in \mathbb{K}$  sont des racines distinctes, de multiplicité  $m_2, \dots, m_k \geq 1$ , et  $Q \in \mathbb{K}[X]$  n'a pas de racine dans  $\mathbb{K}$ .

On a  $\deg P = m_1 + \cdots + m_k + \deg Q$ , donc  $m_1 + \cdots + m_k \leq \deg P$ . Si  $P(r) = 0$ , alors  $r \in \{r_1, \dots, r_k\}$ , car un des facteurs s'annule.  $\square$

§4/55

## Interpolation de Lagrange

### Théorème

Étant donnés des points distincts  $x_0, \dots, x_n \in \mathbb{K}$  et des valeurs arbitraires  $y_0, \dots, y_n \in \mathbb{K}$ , il existe un unique polynôme  $P \in \mathbb{K}[X]$  de degré  $\leq n$  vérifiant  $P(x_k) = y_k$  pour tout  $k = 0, \dots, n$ .

On appelle  $P$  le **polynôme interpolateur de Lagrange**.

**Unicité :** Supposons que  $P, Q \in \mathbb{K}[X]$  sont de degré  $\leq n$  et vérifient  $P(x_k) = Q(x_k)$  pour tout  $k = 0, \dots, n$ . Alors  $R = P - Q$  est de degré  $\leq n$  et s'annule dans les  $n + 1$  points distincts  $x_0, \dots, x_n$ .

Ceci n'est possible que pour  $R = 0$ , donc  $P = Q$ .

**Existence :** Pour tout  $k = 0, \dots, n$  le polynôme

$$P_k = \prod_{j \neq k} \frac{X - x_j}{x_k - x_j}$$

est de degré  $n$  et vérifie  $P_k(x_k) = 1$  ainsi que  $P_k(x_j) = 0$  pour  $j \neq k$ . Ainsi  $P = \sum_{k=0}^n y_k P_k$  vérifie  $P(x_j) = y_j$  pour tout  $j = 0, \dots, n$ .  $\square$

§2.2

35/55

## Dérivation des polynômes

### Proposition

On définit la **dérivation**  $\partial: \mathbb{K}[X] \rightarrow \mathbb{K}[X]$  par

$$\partial \left( \sum_{k=0}^n p_k X^k \right) := \sum_{k=1}^n k p_k X^{k-1}.$$

Cette application est  $\mathbb{K}$ -linéaire et vérifie la règle de Leibniz :

$$\partial(PQ) = (\partial P) \cdot Q + P \cdot (\partial Q).$$

### Démonstration.

Évidemment  $\partial(P + Q) = \partial P + \partial Q$  et  $\partial(aP) = a(\partial P)$  pour tout  $a \in \mathbb{K}$ . La règle de Leibniz est vérifiée pour  $P = X^m$  et  $Q = X^n$  car

$$\begin{aligned} \partial(PQ) &= \partial X^{m+n} = (m+n)X^{m+n-1} \\ &= mX^{m-1} \cdot X^n + X^m \cdot nX^{n-1} = (\partial P) \cdot Q + P \cdot (\partial Q). \end{aligned}$$

Cette formule est  $\mathbb{K}$ -linéaire en  $P$  et en  $Q$ .

Elle s'étend donc à tout couple de polynômes  $P, Q \in \mathbb{K}[X]$ .  $\square$

§6/55

## Racines multiples et dérivée

### Proposition

Un élément  $r \in \mathbb{K}$  est une racine multiple de  $P \in \mathbb{K}[X]^*$  si et seulement si  $r$  est une racine commune de  $P$  et de sa dérivée  $P'$ .

**Démonstration.** Supposons  $P = (X - r)^m Q$  avec  $m \geq 1$  et  $Q(r) \neq 0$ . En appliquant la règle de Leibniz on obtient la dérivée

$$P' = m(X - r)^{m-1}Q + (X - r)^m Q'.$$

Si  $m = 1$ , alors  $P(r) = 0$  mais  $P'(r) = Q(r) \neq 0$ .

Si  $m \geq 2$ , alors  $P(r) = 0$  et  $P'(r) = 0$ . □

### Corollaire

Si  $\text{pgcd}(P, P') = 1$  alors toute racine de  $P$  est simple.

**Démonstration.** Supposons  $P(r) = 0$  et  $P'(r) = 0$ .

Dans ce cas on aurait  $P = (X - r)Q_0$  et  $P' = (X - r)Q_1$ ,

donc  $\text{pgcd}(P, P') = (X - r) \text{pgcd}(Q_0, Q_1)$  serait de degré  $\geq 1$ . □

§2.2

37/55

## Réduction aux racines simples

En général il est difficile de trouver des racines !

Par contre, il est facile de réduire leur multiplicité à 1 :

### Corollaire (sur $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ )

Pour tout polynôme  $P \in \mathbb{K}[X]^*$  le quotient  $P / \text{pgcd}(P, P')$  a les mêmes racines que  $P$ , mais chacune est de multiplicité 1.

### Démonstration.

Supposons  $P = (X - r)^m Q$  où  $m \geq 1$  et  $Q(r) \neq 0$ . Alors

$$P' = m(X - r)^{m-1}Q + (X - r)^m Q' = (X - r)^{m-1}R$$

où  $R = mQ + (X - r)Q'$  et ainsi  $R(r) = mQ(r) \neq 0$ .

Autrement dit,  $r$  est une racine de  $P'$  de multiplicité  $m - 1$ .

Donc  $r$  est une racine de  $\text{pgcd}(P, P')$  de multiplicité  $m - 1$ .

On conclut que  $r$  est une racine simple de  $P / \text{pgcd}(P, P')$ . □

**Avertissement :** La situation est plus compliquée sur des corps finis :

pour  $P = (X + 1)^2$  dans  $\mathbb{F}_2[X]$  on trouve  $P' = 0$  car  $1 + 1 = 0$ .

Ici  $P / \text{pgcd}(P, P') = 1$  n'a pas les mêmes racines que  $P$ .

§2.2

38/55

## C Factorisation « squarefree »

L'astuce de passer de  $P$  à  $P / \text{pgcd}(P, P')$  peut être perfectionnée :

On peut trier les racines du polynôme  $P$  par leur multiplicité.

### Algorithme 9 factorisation « squarefree » selon Yun (1976)

**Entrée :** un polynôme  $P \in \mathbb{Q}[X]$  tel que  $\text{dom } P = 1$ .

**Sortie :** des polynômes  $P_1, P_2, \dots, P_n \in \mathbb{Q}[X]$  vérifiant  $P = P_1 P_2^2 \cdots P_n^n$  et  $\text{pgcd}(P_i, P_i') = \text{pgcd}(P_2, P_2') = \dots = \text{pgcd}(P_n, P_n') = 1$ .

$n \leftarrow 0$ ;  $U \leftarrow \text{pgcd}(P, P')$ ;  $V \leftarrow P/U$ ;  $W \leftarrow P'/U$ ;

**tant que**  $\deg(V) > 0$  **faire**

$n \leftarrow n + 1$ ;  $W \leftarrow W - V'$

$P_n \leftarrow \text{pgcd}(V, W)$ ;  $V \leftarrow V/P_n$ ;  $W \leftarrow W/P_n$

**fin tant que**

**retourner**  $P_1, \dots, P_n$

□ Pour une preuve et une discussion détaillée voir Gathen & Gerhard, *Modern Computer Algebra*, §14.6

§2.2

39/55

## Décomposable vs irréductible

### Définition

Un polynôme  $P \in \mathbb{K}[X]$  est **réductible** (ou décomposable) dans  $\mathbb{K}[X]$  s'il existe  $A, B \in \mathbb{K}[X]$  tels que  $P = AB$  où  $\deg A \geq 1$  et  $\deg B \geq 1$ .

Un polynôme  $P \in \mathbb{K}[X]$  est **irréductible** (ou indécomposable) dans  $\mathbb{K}[X]$  si  $P = AB$  où  $A, B \in \mathbb{K}[X]$  implique soit  $A \in \mathbb{K}^\times$  soit  $B \in \mathbb{K}^\times$ .

Dans  $\mathbb{K}[X]$  il y a donc quatre types de polynômes :

- L'élément nul :  $P = 0 \Leftrightarrow \deg(P) = -\infty$ .
- Les éléments inversibles :  $P \in \mathbb{K}[X]^\times = \mathbb{K}^\times \Leftrightarrow \deg(P) = 0$ .
- Les éléments irréductibles, nécessairement de degré  $\geq 1$ .
- Les éléments décomposables, nécessairement de degré  $\geq 2$ .

⚠ Étant donné  $P \in \mathbb{K}[X]$  de degré élevé, il peut être difficile d'effectivement déterminer s'il est décomposable ou irréductible.

⚠ Même si l'on sait d'avance que  $P \in \mathbb{K}[X]$  est décomposable, il peut être difficile d'effectivement trouver une décomposition.

Il existe quelques critères d'irréductibilité. Les algorithmes de factorisation sont un domaine de recherche toujours très actif.

§2.2

39/55

40/55

## Décomposable vs irréductible : exemples

### Observation

Tout polynôme  $P = aX + b$  de degré 1 est irréductible.

Si  $\deg P \geq 2$  et  $P(r) = 0$  alors  $P = (X - r)Q$  est décomposable.

Un polynôme  $P \in \mathbb{K}[X]$  de degré 2 ou 3 est irréductible si et seulement s'il n'admet pas de racine dans  $\mathbb{K}$ .

**Démonstration.** Si  $P = AB$  alors  $\deg P = \deg A + \deg B$ .

Dans le cas  $\deg P = 1$  on ne peut avoir  $\deg A \geq 1$  et  $\deg B \geq 1$ .

Si  $\deg P \in \{2, 3\}$ , alors  $\deg A \geq 1$  et  $\deg B \geq 1$  implique  $\deg A = 1$  ou  $\deg B = 1$ . Or  $P = (aX + b)B$  entraîne que  $P(-\frac{b}{a}) = 0$ .  $\square$

**Exemple.** Dans  $\mathbb{R}[X]$  sont irréductibles les polynômes linéaires  $aX - b$  où  $a \neq 0$ , et quadratiques  $aX^2 + bX + c$  où  $b^2 - 4ac < 0$ .

**Exemple.**  $X^2 - 2$  et  $X^3 - 2$  n'admettent pas de racine dans  $\mathbb{Q}$  et sont donc irréductibles dans  $\mathbb{Q}[X]$ . Ils sont décomposables dans  $\mathbb{R}[X]$  :  $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$  et  $X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$ . Sur  $\mathbb{C}$  on a  $X^3 - 2 = (X - \sqrt[3]{2})(X - j\sqrt[3]{2})(X - j^2\sqrt[3]{2})$  où  $j = e^{2\pi i/3}$ .

**⚠** Le polynôme  $X^4 - 9$  n'admet pas de racine dans  $\mathbb{Q}$ . Néanmoins il est décomposable :  $X^4 - 9 = (X^2 - 3)(X^2 + 3)$ .

3.23

41.55

## Décomposition en facteurs irréductibles : existence

### Lemme (existence d'une décomposition)

Pour tout  $P \in \mathbb{K}[X]^*$  il existe  $u \in \mathbb{K}^*$  et  $P_1, \dots, P_k \in \mathbb{K}[X]$  unitaires et irréductibles dans  $\mathbb{K}[X]$  de sorte que  $P = uP_1 \cdots P_k$ .

**Démonstration.** Par récurrence sur  $\deg P$ .

Pour  $\deg P = 0$  on a  $P = u \in \mathbb{K}^*$ . Supposons alors  $\deg P \geq 1$  :

- Si  $P$  est irréductible, alors  $P = uP_1$  où  $u = \text{dom}(P)$  et  $P_1 = P/u$ .
- Si  $P = AB$  avec  $\deg A, \deg B \geq 1$  alors  $\deg A, \deg B < \deg P$ . Par hypothèse on a  $A = vQ_1 \cdots Q_i$  et  $B = wR_1 \cdots R_j$  où  $v, w \in \mathbb{K}^*$  et  $Q_1, \dots, Q_i, R_1, \dots, R_j \in \mathbb{K}[X]$  sont unitaires et irréductibles dans  $\mathbb{K}[X]$ . Ainsi  $P = (vw)Q_1 \cdots Q_i R_1 \cdots R_j$ .  $\square$

### Lemme (d'Euclide)

Soit  $P$  irréductible dans  $\mathbb{K}[X]$ . Si  $P \mid AB$  alors  $P \mid A$  ou  $P \mid B$ .

**Démonstration.**  $C = \text{pgcd}(P, A)$  divise  $P$ , supposé irréductible. On a donc ou  $C = 1$  ou  $C \sim P$ . Si  $C \sim P$  alors  $P \mid A$ .

Si  $C = 1$ , alors il existe  $U, V \in \mathbb{K}[X]$  tels que  $AU + PV = 1$ .

Ainsi  $PQ = AB$  entraîne  $B = (AU + PV)B = P(QU + BV)$ .  $\square$

3.23

41.55

42.55

## Décomposition en facteurs irréductibles : unicité

### Théorème (factorisation unique de polynômes)

Tout polynôme  $P \in \mathbb{K}[X]^*$  s'écrit comme  $P = uP_1 \cdots P_k$  où  $u \in \mathbb{K}^*$  et  $P_1, \dots, P_k \in \mathbb{K}[X]$  sont unitaires et irréductibles dans  $\mathbb{K}[X]$ . Cette décomposition est unique à l'ordre des facteurs près.

**Unicité.** Supposons  $P = uP_1 \cdots P_k = vQ_1 \cdots Q_\ell$ .

Récurrence sur  $k$  : si  $k = 0$  alors  $\deg P = 0$ , donc  $\ell = 0$  et  $P = u = v$ .

Supposons  $k \geq 1$ . Puisque  $P_k$  est irréductible, il divise un des facteurs  $Q_1, \dots, Q_\ell$ . Après permutation on peut supposer que  $P_k \mid Q_\ell$ .

Puisque  $Q_\ell$  est irréductible, on a  $P_k \sim Q_\ell$ .

On suppose  $P_k$  et  $Q_\ell$  unitaires, donc  $P_k = Q_\ell$ .

Par récurrence,  $P/P_k = uP_1 \cdots P_{k-1} = vQ_1 \cdots Q_{\ell-1}$  implique  $k = \ell$  ainsi que  $u = v$  et  $P_1 = Q_1, \dots, P_{k-1} = Q_{k-1}$ , après permutation.  $\square$

### Théorème (factorisation unique d'entiers, rappel)

Tout nombre entier  $n \in \mathbb{Z}^*$  s'écrit comme  $n = up_1 \cdots p_k$  où  $u \in \{\pm 1\}$  et  $p_1, \dots, p_k \in \mathbb{Z}$  sont des entiers positifs irréductibles (= premiers). Cette décomposition est unique à l'ordre des facteurs près.  $\square$

3.23

43.55

## Le théorème de Gauss-d'Alembert

Un polynôme  $P \in \mathbb{K}[X]$  de degré  $n$  admet au plus  $n$  racines dans  $\mathbb{K}$ . S'il admet  $n$  racines  $r_1, \dots, r_n \in \mathbb{K}$ , éventuellement avec répétitions, alors il factorise dans  $\mathbb{K}[X]$  comme  $P = u(X - r_1) \cdots (X - r_n)$ .

### Théorème (de Gauss-d'Alembert, version complexe)

Pour tout  $P \in \mathbb{C}[X]$  de degré  $n$  il existe  $r_1, r_2, \dots, r_n \in \mathbb{C}$  et  $u \in \mathbb{C}^*$  tels que  $P = u(X - r_1)(X - r_2) \cdots (X - r_n)$ . Autrement dit, les seuls polynômes irréductibles dans  $\mathbb{C}[X]$  sont ceux de degré 1.  $\square$

Si  $P \in \mathbb{R}[X]$ , alors  $P(z) = 0$  implique  $P(\bar{z}) = \overline{P(z)} = 0$  : les racines non réelles forment des paires conjuguées. En les regroupant on obtient des facteurs  $(X - z)(X - \bar{z})$  qui sont irréductibles dans  $\mathbb{R}[X]$  :

### Théorème (de Gauss-d'Alembert, version réelle)

Tout polynôme réel  $P \in \mathbb{R}[X]$  factorise comme  $P = uP_1 P_2 \cdots P_k$  où  $u \in \mathbb{R}^*$  et pour tout  $j$  on a ou bien  $P_j = X - r_j$  avec  $r_j \in \mathbb{R}$  ou bien  $P_j = X^2 + p_j X + q_j$  avec  $p_j, q_j \in \mathbb{R}$  et  $p_j^2 - 4q_j < 0$ .  $\square$

Par exemple, le polynôme  $X^2 + 1$  est irréductible dans  $\mathbb{R}[X]$ , mais se décompose comme  $X^2 + 1 = (X + i)(X - i)$  dans  $\mathbb{C}[X]$ .

3.23

43.55

44.55

## Le corps des fractions rationnelles

On note  $\mathbb{K}(X)$  l'ensemble des fractions  $\frac{A}{B}$  où  $A, B \in \mathbb{K}[X]$ ,  $B \neq 0$ , avec l'identification  $\frac{A}{B} = \frac{C}{D}$  dans  $\mathbb{K}(X)$  ssi  $AD = CB$  dans  $\mathbb{K}[X]$ .

Pour ces fractions on définit l'addition et la multiplication par

$$\frac{A}{B} + \frac{C}{D} := \frac{AD + CB}{BD}, \quad \frac{A}{B} \cdot \frac{C}{D} := \frac{AC}{BD}.$$

### Proposition

L'ensemble  $\mathbb{K}(X)$  des fractions rationnelles sur  $\mathbb{K}$  muni de l'addition + et de la multiplication  $\cdot$  définit un corps.

On remarque que  $\frac{A}{1} + \frac{B}{1} = \frac{A+B}{1}$  et  $\frac{A}{1} \cdot \frac{B}{1} = \frac{AB}{1}$ .

Ainsi  $\mathbb{K}[X] \subset \mathbb{K}(X)$  en identifiant  $A \in \mathbb{K}[X]$  avec  $\frac{A}{1} \in \mathbb{K}(X)$ .

### Exercice (long mais bénéfique)

Vérifier la construction de  $(\mathbb{K}(X), +, \cdot)$  et les axiomes de corps.

§3.1

47:55

## Construction du corps des fractions

On construit l'ensemble  $\mathbb{K}(X)$  comme un ensemble quotient.

On considère d'abord l'ensemble  $\mathcal{F} = \mathbb{K}[X] \times \mathbb{K}[X]^*$  formé de toutes les paires  $(A, B)$  où  $A, B \in \mathbb{K}[X]$  et  $B \neq 0$ .

On introduit la relation  $(A, B) \sim (C, D) \iff AD = CB$ .

C'est une relation d'équivalence :

Réflexivité :  $(A, B) \sim (A, B)$ .

Symétrie :  $(A, B) \sim (C, D) \implies (C, D) \sim (A, B)$ .

Transitivité :  $(A, B) \sim (C, D) \wedge (C, D) \sim (E, F) \implies (A, D) \sim (E, F)$ .

Le dernier point mérite une attention particulière :

$(A, B) \sim (C, D)$  veut dire que  $AD = CB$ , donc  $ADF = CBF$ .

$(C, D) \sim (E, F)$  veut dire que  $CF = ED$ , donc  $CBF = EBD$ .

On en déduit que  $ADF = EBD$  ou encore  $(AF - EB)D = 0$ .

Puisque  $D \neq 0$  on conclut que  $AF - EB = 0$ , donc  $(A, B) \sim (E, F)$ .

Maintenant on peut définir l'ensemble  $\mathbb{K}(X)$  comme le quotient  $\mathcal{F}/\sim$ .

La classe d'équivalence de  $(A, B)$  dans  $\mathbb{K}(X)$  sera notée  $\frac{A}{B}$ .

Par construction on a  $\frac{A}{B} = \frac{C}{D} \iff AD = CB$ .

§3.1

48:55

48:55

## Construction de l'addition et de la multiplication

Sur  $\mathcal{F} = \mathbb{K}[X] \times \mathbb{K}[X]^*$  l'addition  $(A, B) + (C, D) := (AD + CB, BD)$  est associative, commutative, et admet  $(0, 1)$  pour élément neutre.

De même, la multiplication  $(A, B) \cdot (C, D) := (AC, BD)$  est associative, commutative, et admet  $(1, 1)$  pour élément neutre.

$(\mathcal{F}, +, \cdot)$  n'est pas un corps : les axiomes (A4), (M4), et (D) ne sont pas vérifiés. Il faut encore passer à l'ensemble quotient  $\mathbb{K}(X) = \mathcal{F}/\sim$ .

L'addition et la multiplication passent-elles au quotient ?

Si  $(A_1, B_1) \sim (A_2, B_2)$  et  $(C_1, D_1) \sim (C_2, D_2)$

alors  $(A_1, B_1) + (C_1, D_1) \sim (A_2, B_2) + (C_2, D_2)$

ainsi que  $(A_1, B_1) \cdot (C_1, D_1) \sim (A_2, B_2) \cdot (C_2, D_2)$ .

L'addition  $\frac{A}{B} + \frac{C}{D} := \frac{AD + CB}{BD}$  et la multiplication  $\frac{A}{B} \cdot \frac{C}{D} := \frac{AC}{BD}$  sont donc bien définies sur  $\mathbb{K}(X)$ , i.e. indépendantes des représentants.

### Exercice (maintenant facile)

Vérifier les axiomes de corps pour  $(\mathbb{K}(X), +, \cdot)$ .

Indications : L'élément opposé de  $\frac{A}{B}$  est  $-\frac{A}{B}$ .

On a  $\frac{A}{B} \neq \frac{0}{1}$  ssi  $A \neq 0$ . Dans ce cas l'élément inverse est  $\frac{B}{A}$ .

§3.1

47:55

## Implémentation des fractions rationnelles

♦ On stocke  $\frac{A}{B} \in \mathbb{K}(X)$  comme une paire  $(A, B) \in \mathbb{K}[X] \times \mathbb{K}[X]^*$ . Il est naturel de passer systématiquement à la forme réduite :

### Proposition

Toute fraction dans  $\mathbb{K}(X)$  s'écrit de manière unique comme  $\frac{A}{B}$  de sorte que  $\text{pgcd}(A, B) = 1$  et  $\text{dom}(B) = 1$ .

**Existence** : Évidemment toute fraction  $\frac{A}{B} \in \mathbb{K}(X)$  peut être représentée par la paire  $(A, B) \in \mathbb{K}[X] \times \mathbb{K}[X]^*$ .

Si  $D = \text{pgcd}(A, B) \neq 1$ , alors on passe à  $(A/D, B/D)$ .

Si  $c = \text{dom}(B) \neq 1$ , alors on passe à  $(A/c, B/c)$ .

**Unicité** : Considérons une fraction  $\frac{A}{B} = \frac{C}{D}$  telle que  $\text{pgcd}(A, B) = \text{pgcd}(C, D) = 1$  et  $\text{dom } B = \text{dom } D = 1$ .

On a  $AD = CB$ . On applique deux fois le lemme de Gauss :

$B \mid AD$  et  $\text{pgcd}(B, A) = 1$  implique  $B \mid D$ .

$D \mid CB$  et  $\text{pgcd}(D, C) = 1$  implique  $D \mid B$ .

Or,  $B \mid D$  et  $D \mid B$  implique  $B \sim D$ .

Comme  $\text{dom } B = \text{dom } D = 1$  on conclut que  $B = D$ , puis  $A = C$ .  $\square$

§3.1

47:55

48:55

## Décomposition en fractions simples

**Objectif.** On cherche à décomposer  $\frac{Q}{P}$  en « fractions simples ».

**Factorisation (partielle) du dénominateur.**

Si  $P = AB$  avec  $\text{pgcd}(A, B) = 1$ , alors il existe  $U, V \in \mathbb{K}[X]$  tels que  $AU + BV = 1$ . Ainsi notre fraction se décompose en une somme :

$$\frac{Q}{P} = \frac{Q(AU + BV)}{AB} = \frac{QU}{B} + \frac{QV}{A}.$$

♦ Étant donné  $A$  et  $B$ , c'est juste un calcul d'Euclide-Bézout.

**Factorisation complète du dénominateur.**

Tout polynôme unitaire  $P \in \mathbb{K}[X]$  factorise comme  $P = P_1^{m_1} \dots P_k^{m_k}$  où tout  $P_i$  est irréductible unitaire,  $m_i \geq 1$ , et  $P_i \neq P_j$  pour  $i \neq j$ .

⚠ Dans la pratique cette décomposition peut être difficile à trouver.

**Finalement, réduction d'une fraction  $\frac{Q}{P^m}$ .**

On développe  $Q = Q_m + Q_{m-1}P + \dots + Q_1P^{m-1} + Q_0P^m$  tel que  $\deg Q_k < \deg P$  pour  $k = 1, \dots, m$ . Ainsi on obtient

$$\frac{Q}{P^m} = Q_0 + \frac{Q_1}{P} + \dots + \frac{Q_{m-1}}{P^{m-1}} + \frac{Q_m}{P^m}.$$

♦ Étant donné  $Q$  et  $P$ , c'est juste une division euclidienne itérée.

3.2

48.55

## Décomposition en fractions simples

**Théorème (décomposition en fractions simples)**

Tout polynôme unitaire  $P \in \mathbb{K}[X]$  factorise comme

$$(1) \quad P = P_1^{m_1} \dots P_k^{m_k}$$

où tout  $P_i$  est irréductible unitaire,  $m_i \geq 1$ , et  $P_i \neq P_j$  pour  $i \neq j$ .

Par conséquent, toute fraction  $\frac{Q}{P}$  se décompose comme

$$(2) \quad \frac{Q}{P} = Q_0 + \frac{Q_{11}}{P_1} + \frac{Q_{12}}{P_1^2} + \dots + \frac{Q_{1m_1}}{P_1^{m_1}} \\ + \dots \\ + \frac{Q_{k1}}{P_k} + \frac{Q_{k2}}{P_k^2} + \dots + \frac{Q_{km_k}}{P_k^{m_k}}.$$

pour certains polynômes  $Q_0, Q_{ij} \in \mathbb{K}[X]$  vérifiant  $\deg Q_{ij} < \deg P_i$ .

⚠ Dans la pratique la factorisation (1) peut être difficile à expliciter.

♦ Étant donnée (1), l'étape (2) est facile avec Euclide-Bézout.

51.55

## Décomposition en fractions très simples

**Corollaire (décomposition en fractions très simples)**

Supposons que  $P = (X - a_1)^{m_1} \dots (X - a_k)^{m_k}$  où  $m_1, \dots, m_k \geq 1$  et  $a_1, \dots, a_k \in \mathbb{K}$  tels que  $a_i \neq a_j$  pour  $i \neq j$ . Alors pour tout  $Q \in \mathbb{K}[X]$  il existe un polynôme  $Q_0 \in \mathbb{K}[X]$  et des coefficients  $\alpha_{ij} \in \mathbb{K}$  tels que

$$\frac{Q}{P} = Q_0 + \frac{\alpha_{11}}{X - a_1} + \frac{\alpha_{12}}{(X - a_1)^2} + \dots + \frac{\alpha_{1m_1}}{(X - a_1)^{m_1}} \\ + \dots \\ + \frac{\alpha_{k1}}{X - a_k} + \frac{\alpha_{k2}}{(X - a_k)^2} + \dots + \frac{\alpha_{km_k}}{(X - a_k)^{m_k}}.$$

⚠ Attention à l'hypothèse !

Sur  $\mathbb{C}$  tout polynôme unitaire  $P$  factorise comme souhaité.

Sur  $\mathbb{R}$  il peut y avoir des facteurs irréductibles de degré 2.

(Dans ce cas on revient au théorème précédent.)

3.2

51.55

## Primitive d'une fraction rationnelle

Dériver un polynôme

$$P = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$$

dans  $\mathbb{R}[X]$  est facile car

$$P' = a_1 + 2a_2X + \dots + na_nX^{n-1}.$$

Intégrer est aussi facile : le polynôme

$$S = a_0X + \frac{1}{2}a_1X^2 + \frac{1}{3}a_2X^3 + \dots + \frac{1}{n+1}a_nX^{n+1}$$

est une primitive de  $P$  car  $S' = P$ .

Dériver une fraction rationnelle dans  $\mathbb{R}(X)$  est facile car

$$\left(\frac{Q}{P}\right)' = \frac{Q'P - QP'}{P^2}.$$

Mais comment intégrer ? Le résultat sera-t-il à nouveau dans  $\mathbb{R}(X)$  ?

En général, non ! Apparaissent deux primitives transcendentes :

$$\int \frac{dx}{x} = \ln|x| \quad \text{et} \quad \int \frac{dx}{x^2 + 1} = \arctan x.$$

51.55

## Primitive d'une fraction rationnelle

Rappelons que dans  $\mathbb{R}[X]$  sont irréductibles les polynômes linéaires  $aX - b$  où  $a \neq 0$  et quadratiques  $aX^2 + bX + c$  vérifiant  $b^2 - 4ac < 0$  :

### Théorème (de Gauss-d'Alembert, version réelle)

Tout polynôme réel  $P \in \mathbb{R}[X]$  factorise comme  $P = u P_1^{m_1} \dots P_k^{m_k}$  où  $u \in \mathbb{R}^\times$  et pour tout  $j$  on a ou bien  $P_j = X - r_j$  avec  $r_j \in \mathbb{R}$  ou bien  $P_j = X^2 + p_j X + q_j$  avec  $p_j, q_j \in \mathbb{R}$  et  $p_j^2 - 4q_j < 0$ .  $\square$

Ici on peut et on va supposer que  $P_i \neq P_j$  pour tout  $i \neq j$ .  
Par conséquent, toute fraction  $\frac{Q}{P}$  se décompose comme

$$\begin{aligned} \frac{Q}{P} &= Q_0 + \frac{Q_{11}}{P_1} + \frac{Q_{12}}{P_1^2} + \dots + \frac{Q_{1m_1}}{P_1^{m_1}} \\ &+ \dots \\ &+ \frac{Q_{k1}}{P_k} + \frac{Q_{k2}}{P_k^2} + \dots + \frac{Q_{km_k}}{P_k^{m_k}}. \end{aligned}$$

pour certains polynômes  $Q_0, Q_{ij} \in \mathbb{K}[X]$  vérifiant  $\deg Q_{ij} < \deg P_i$ .

§3.3

§3.3

## Primitive d'une fraction rationnelle

Comment intégrer  $\frac{Q}{P} \in \mathbb{R}(X)$  ? Voici quelques intégrales faciles :

$$\begin{aligned} \int \frac{1}{x-a} dx &= \ln|x-a| \\ \int \frac{1}{(x-a)^n} dx &= \frac{1}{(n-1)(x-a)^{n-1}} \end{aligned}$$

Ceci règle le cas où  $P$  se décompose en facteurs linéaires.

Regardons ensuite les dénominateurs irréductibles de degré 2 :

$$\begin{aligned} \int \frac{2x+p}{x^2+px+q} dx &= \ln|x^2+px+q| \\ \int \frac{1}{x^2+px+q} dx &= \frac{2}{\sqrt{4q-p^2}} \arctan \frac{2x+p}{\sqrt{4q-p^2}} \end{aligned}$$

**Démonstration.** Une fois la formule trouvée, il suffit de dériver.  $\square$

§4.55

## Primitive d'une fraction rationnelle

On établit finalement deux intégrales plus compliquées pour les dénominateurs irréductibles de degré 2 et de multiplicité  $n \geq 2$  :

$$\begin{aligned} \int \frac{2x+p}{(x^2+px+q)^n} dx &= -\frac{1}{(n-1)(x^2+px+q)^{n-1}} \\ \int \frac{1}{(x^2+px+q)^n} dx &= \frac{2x+p}{(n-1)(4q-p^2)(x^2+px+q)^{n-1}} \\ &+ \frac{2(2n-3)}{(n-1)(4q-p^2)} \int \frac{1}{(x^2+px+q)^{n-1}} dx \end{aligned}$$

### Théorème

Toute fraction rationnelle  $\frac{Q}{P} \in \mathbb{R}(X)$  admet une primitive dans

$$\mathbb{R}(X) \{ \ln|x-a|, \ln|x^2+px+q|, \arctan|ax+b| \}.$$

Étant donnée la décomposition de  $P$  en facteurs irréductibles, la primitive peut être explicitée comme indiqué ci-dessus.

Cette méthode d'intégration symbolique est implémentée par tout logiciel de calcul formel. Algorithmiquement le seul point délicat est la factorisation du polynôme  $P \in \mathbb{R}[X]$ . Nous y reviendrons plus loin.

§3.3

§5.55