Projet de Calcul Formel

Nombres algébriques et résultant

A l'attention de :
NOM PROFS ? ?

Rédigé par :
CARVAILLO Thomas

Table des matières

Introduction

Intro

1 Un peu de théorie

1.1 Rappels

Définition 1. On appelle corps tout anneau A abélien unitaire dans lequel tout élément non nul est inversible, i.e. $A^\times = A\backslash\{0\}$.

Notation 1. Dans ce qui suit, le corps de base sera noté $\mathbb{K}$ et désignera indifféremment, sauf indication contraire, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

Définition 2. On appelle extension de $\mathbb{K}$ tout corps $\mathbb{L}$ contenant un sous-corps isomorphe à $\mathbb{K}$. On notera $\mathbb{L}/\mathbb{K}$ une telle extension.

Définition 3. On appelle degré de l'extension $\mathbb{L}/\mathbb{K}$ la dimension de $\mathbb{L}$ en tant que $\mathbb{K}$-espace vectoriel. On le notera $[\mathbb{L} : \mathbb{K}]$.

Proposition 1. *multiplicativité du degré.*

Définition 4. On dit que $\mathbb{L}/\mathbb{K}$ est finie si elle est de degré finie.

Proposition 2. *L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ en l'indéterminée X est muni d'une structure d'anneau Euclidien.*

1.2 Eléments algébriques

Définition 5. Soient $\mathbb{L}/\mathbb{K}$ une extension de corps et $P(X) = \sum_{i=0}^{n} a_i X^i$ un polynôme de degré n à coefficients dans $\mathbb{K}$. On considère le morphisme d'évaluation

$$ev_\alpha : \left| \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{L} \\ P(X) & \longmapsto & P(\alpha) \end{array} \right.$$

Soit $I(\alpha) := ker(ev_\alpha) = \{P \in \mathbb{K}[X] \text{ tels que } P(\alpha) = 0\}$; on a deux possibilites :

- Soit $I(\alpha) \neq \{0\}$, i.e. ev_a n'est pas injective et donc $\exists P \in \mathbb{K}[X]\backslash\{0\}$ tel que $P(\alpha) = 0$.
  Dans ce cas α est dit algébrique sur $\mathbb{K}$.
- Soit $I(\alpha) = \{0\}$ i.e. ev_a est injective et donc $\nexists P \in \mathbb{K}[X]\backslash\{0\}$ tel que $P(\alpha) = 0$.
  Dans ce cas, α est dit transcendant sur $\mathbb{K}$.

Théorème 1. *Soit $\mathbb{L}/\mathbb{K}$ une extension de corps et α un élément algébrique sur $\mathbb{L}$, alors il existe un unique polynôme $P(X)$ unitaire irréductible dans $\mathbb{K}[X]$ vérifiant*

$$(Q(X) \in \mathbb{K}[X]\backslash\{0\} \text{ et } Q(\alpha) = 0) \text{ ssi } P(X) \mid Q(X)$$

Démonstration. $\mathbb{K}[X]$ est euclidien, donc en particulier principal. Il s'ensuit qu'il existe $P(X) \in \mathbb{K}[X]\backslash\{0\}$ unitaire tel que $I(a) = (P(X))$, $I(a)$ étant un idéal propre non nul. Par le premier théorème d'isomorphisme, on obtient que $Im(ev_\alpha) \simeq \frac{\mathbb{K}[X]}{(P(X))}$. Ce dernier étant intègre, on obtient que $P(X)$ est premier donc irréductible dans $\mathbb{K}[X]$ factoriel.
Il s'ensuit naturellement que $Q(X) \in I(a)\backslash\{0\} = (P(X))\backslash\{0\}$ ssi $P(X) \mid Q(X)$. □

Proposition 3 (Admise)**.** *On a de plus* $deg(P) = [\mathbb{L} : \mathbb{K}]$.

Définition 6. Le polynôme $P(X)$ comme décrit ci-dessus est appellé le polynôme minimal de α sur $\mathbb{K}$ et est noté $Irr(\alpha, X, \mathbb{K})$.

Proposition 4 (Critère d'Eiseinstein - Admis)**.** *Soit* $P(X) = \sum_{i=0}^{n} a_i X^i$ *un polynôme de* $\mathbb{Z}[X]$*, supposons de plus qu'il existe* p *premier tel que* $\forall i \in [\![0, n-1]\!]$

- $p \mid a_i$,
- $p \nmid a_n$
- $p^2 \nmid a_0$

alors $P(X)$ *est irréductible dans* $\mathbb{Q}[X]$.

Exemple 1. racine de 2

Définition 7. Soit $\mathbb{L}/\mathbb{K}$ une extension. On appelle fermeture algébrique de $\mathbb{K}$ dans $\mathbb{L}$ l'ensemble des éléments de $\mathbb{L}$ algébriques sur $\mathbb{K}$.

Définition 8. On dit que $\mathbb{L}/\mathbb{K}$ est algébrique si tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.

Proposition 5 (Admise)**.** *Une extension finie est algébrique.*

Notation 2. On notera $\mathbb{K}(\alpha_1, ..., \alpha_n)$ le plus petit corps, au sens de l'inclusion, contenant $\mathbb{K}$, α_1, ..., α_n.

Théorème 2. *Soit* $\mathbb{L}/\mathbb{K}$ *une extension de corps et soient* α *et* β *deux éléments de* $\mathbb{L}$ *non nuls algébriques sur* $\mathbb{K}$*. Alors,* $\alpha + \beta$*,* $\alpha.\beta$ *et* α^{-1} *sont algébriques sur* $\mathbb{K}$*. En d'autres termes, la fermeture algébrique de* $\mathbb{K}$ *est une extension de* $\mathbb{K}$*.*

Démonstration. Nous allons donner ici une première preuve non constructive. $\mathbb{K}(\alpha)/\mathbb{K}$ et $\mathbb{K}(\beta)/\mathbb{K}$ sont finies et $[\mathbb{K}(\alpha, \beta) : \mathbb{K}] = [\mathbb{K}(\alpha, \beta) : \mathbb{K}(\alpha)].[\mathbb{K}(\alpha) : \mathbb{K}]$
De plus, on a $K \subseteq \mathbb{K}(\alpha) \subseteq \mathbb{K}(\alpha, \beta)$ et $\mathbb{K} \subseteq \mathbb{K}(\beta) \subseteq \mathbb{K}(\alpha, \beta)$ donc

$$deg(Irr(\beta, X, \mathbb{K}(\alpha))) \leq deg(Irr(\beta, X, \mathbb{K}))$$

d'où

$$[\mathbb{K}(\alpha, \beta) : \mathbb{K}] \leq [\mathbb{K}(\beta) : \mathbb{K}].[\mathbb{K}(\alpha) : \mathbb{K}] < \infty$$

Donc $[\mathbb{K}(\alpha, \beta) : \mathbb{K}]$ est fini et l'extension est algébrique. Il s'ensuit naturellement que $\alpha + \beta$, $\alpha.\beta$ et α^{-1} sont algébriques, car contenus dans $\mathbb{K}(\alpha, \beta)$. □

1.3 Résultants

Introduisons maintenant une notion fondamentale, celle de *résultant*, qui va nous permettre de donner une seconde démonstration - cette fois ci constructrice - du dernier théorème.

Définition 9. Soient $A = \sum_{i=0}^{n} a_i X^i$ et $B = \sum_{i=0}^{m} b_i X^i$ deux polynômes de $\mathbb{K}[X]$. On appelle matrice de Sylvester de P et Q la matrice de taille $(m+n)\times(m+n)$ définit par :

$$Syl(A,B) := \begin{pmatrix} a_n & a_{n-1} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ 0 & a_n & \cdots & a_2 & a_1 & a_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n & a_{n-1} & a_{n-2} & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ 0 & b_m & \cdots & b_2 & b_1 & b_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_m & b_{m-1} & b_{m-2} & \cdots & b_0 \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} \text{m} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} \text{n} \end{matrix}$$

Définition 10. On appelle résultant de A et B le déterminant de la matrice de Sylvester de A et B :

$$Res(A,B) := det(Syl(A,B))$$

Théorème 3 (Admis)**.** *Soient A et $B \in \mathbb{K}[X]$, alors $Res(A,B) = 0$ ssi P et Q ont un facteur commun non constant dans $\mathbb{K}[X]$.*

Notation 3. On notera $Res_X(A,B)$ le résultant de deux polynôme en la variable X à coefficient dans $\mathbb{K}[Y]$.

Nous allons maintenant considérer α et β deux éléments de $\mathbb{L}$ algébriques sur $\mathbb{K}$. On notera respectivement leur polynômes minimaux $A(X)$ et $B(X) \in \mathbb{K}[X]$, avec $deg(A) = n$ et $deg(B) = m$. L'objectif est de constuire un polynôme annulateur (et non forcément minimal !) de $\alpha+\beta$, $\alpha.\beta$ et α^{-1} afin de donner une preuve constructive du *Théorème 2.*

Proposition 6. *La fermeture algébrique de $\mathbb{K}$ dans $\mathbb{L}$ est munie d'une structure d'anneau ; en effet*

i) Le polynôme $S(X) := Res_Y(A(Y), B(Y-X))$ est un polynôme annulateur de $\alpha+\beta$.

ii) Le polynôme $P(X) := Res_Y(A(Y), X^m.B(\frac{X}{Y}))$ est un polynôme annulateur de $\alpha.\beta$.

Démonstration. De simples calculs suffisent, remarquons que

i) $S(\alpha+\beta) = Res_Y(A(Y), B(Y-\alpha+\beta))$. Or, $A(\alpha) = 0$ et $B(\alpha-\alpha+\beta) = B(\beta) = 0$. Donc les polynômes $A(Y)$ et $B(Y-\alpha+\beta) \in \mathbb{K}[Y]$ admettent α comme racine commune. De part le théorème précédent, on obtient que $S(\alpha+\beta) = Res_Y(A(Y), B(Y-\alpha+\beta)) = 0$, la conclusion s'ensuit.

ii) De manière similaire, $P(\alpha.\beta) = Res_Y(A(Y), (\alpha.\beta)^m.B(\frac{\alpha.\beta}{Y}))$. Or, $A(\alpha) = 0$ et $(\alpha.\beta)^m.B(\frac{\alpha.\beta}{\alpha}) = (\alpha.\beta)^m.B(\beta) = 0$ Le terme $(\alpha.\beta)^m$ est nécessaire lorsque $\alpha = 0$. La conclusion s'ensuit.

□

Et finalement :

Proposition 7. *La fermeture algébrique de* $\mathbb{K}$ *dans* $\mathbb{L}$ *est munie d'une structure de corps ; en effet le polynôme* $I(X) := X^n.A(1/X)$ *est un polynôme annulateur de* α^{-1}.

Démonstration. $I(\alpha^{-1}) = ((\alpha^{-1})^n).A(\alpha^{-1}) = \alpha^{-n}.\sum a_i(\alpha^{-1})^i$ □

2 Du code

3 Des exemples