Projet de Calcul Formel.
2020-2021

Faculté des Sciences et Techniques
Master 1 - Maths. CRYPTIS

Nombres algébriques et résultant

A l'attention de :
NALDI S.

Rédigé par :
PIARD A.
JACQUET R.
CARVAILLO T.

Table des matières

Introduction

L'étude de ce projet porte sur les nombres algébrique et le résultant. Dans ce projet, nous rappellerons ce que sont les nombres algébriques, résultant, polynômes minimaux, extensions de corps et nous implémenterons des algorithmes permettant le calcul de polynômes minimaux pour la somme, le produit... de nombres algébriques à l'aide de la théorie des résultants. Ces algorithmes seront développés, en Maple, comme suggéré.

1 Préambule

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

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. *Soit $E \subseteq F \subseteq G$ une tour d'extension de corps. On a alors,*

$$[G : E] = [G : F] \cdot [F : E].$$

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.*

2 Éléments algébriques et résultant

2.1 Éléments 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 possibilités :

- Soit $I(\alpha) \neq \{0\}$, i.e. ev_a n'est pas injective et donc $\exists P \in \mathbb{K}[X] - \{0\}$ 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 $\nexists P \in \mathbb{K}[X] - \{0\}$ 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*

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

Démonstration. $\mathbb{K}[X]$ est euclidien, donc en particulier principal. Il s'ensuit qu'il existe $P(X) \in \mathbb{K}[X] - \{0\}$ 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 $Q(X) \in I(a) - \{0\} = (P(X)) - \{0\}$ si et seulement si $P(X) \mid Q(X)$. □

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 $Irr(\alpha, X, \mathbb{K})$.

Remarque 1. Soit $\alpha \in \mathbb{Q}$, il peut être intéressant de remarquer qu'un polynôme irréductible dans $\mathbb{Q}[X]$ annulant α sera son toujours son polynôme minimal sur $\mathbb{Q}$. Cela découle de ce qui a été vu plus haut.

Proposition 4 (Critère d'Eiseinstein - Admis)**.** *Soit* $P(X) = \sum_{i=0}^{n} a_i X^i$ *un polynôme de* $\mathbb{Z}[X]$*. S'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. Voyons quelques cas triviaux :

- i est algébrique sur $\mathbb{Q}$, en effet $X^2 - 1$ est son polynôme minimal sur $\mathbb{Q}$.
- $\sqrt{2}$ et $\sqrt{3}$ sont algébrique sur $\mathbb{Q}$, de polynôme minimaux respectif $X^2 - 2$ et $X^2 - 3$, dont l'irréductibilité découle du critère d'Eisenstein.
- $\alpha = \sqrt{2} + \sqrt{3}$ est également algébrique sur $\mathbb{Q}$. En effet,

$$\begin{aligned} \alpha = \sqrt{2} + \sqrt{3} &\Leftrightarrow (\alpha - \sqrt{2})^2 = 3 \\ &\Leftrightarrow \alpha^2 + 2\alpha\sqrt{2} + 2 = 3 \\ &\Leftrightarrow \alpha^2 - 1 = -2\alpha\sqrt{2} \\ &\Leftrightarrow \alpha^4 - 2\alpha^2 + 1 = 8\alpha^2 \\ &\Leftrightarrow \alpha^4 - 10\alpha^2 + 1 = 0 \end{aligned}$$

  α admet donc pour polynôme minimal $X^4 - 10X^2 + 1$. L'irréductibilité découle de Eisenstein pour $p = 2$.

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 $\mathbb{K}(\alpha,\beta)$. □

2.2 Résultant

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 :

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

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

$$Res(A,B) := det(\mathsf{Syl}(A,B))$$

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

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

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 construire un polynôme annulateur 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 $S(X) := \mathsf{Res}_Y(A(Y), B(X-Y))$ *est un polynôme annulateur de* $\alpha+\beta$*.*

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

Démonstration. De simples calculs suffisent, remarquons que

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

ii) De manière similaire, $P(\alpha.\beta) = \mathsf{Res}_Y(A(Y), (\alpha.\beta)^m.B(\frac{\alpha.\beta}{Y}))$. 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.

□

```
# Fonction qui permet le calcul d'un polynôme annulateur
# de la somme de nombres algébriques

annulSomme := proc(u, v)
local f, g, A, B, syl, res;
A := PolynomialTools:-MinimalPolynomial(u, X);
B := PolynomialTools:-MinimalPolynomial(v, X);
f := Y -> subs(X = Y, A);
g := Y -> subs(X = Y, B);
syl := SylvesterMatrix(f(Y), g(Y - X), Y);
res := Determinant(syl);
return res;
end proc:

# Fonction qui permet le calcul d'un polynôme annulateur
# du produit de nombres algébriques

annulProduit := proc(u, v)
local f, g, A, B, res, m;
A := PolynomialTools:-MinimalPolynomial(u, X);
B := PolynomialTools:-MinimalPolynomial(v, X);
f := Y -> subs(X = Y, A);
g := Y -> subs(X = Y, B);
m := degree(g(Y));
res := resultant(f(Y), X^m*g(Y/X), Y);
return res;
end proc
```

Il vient alors la proposition suivante,

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

Démonstration. Une fois de plus, un simple calcul suffit :

$$P(\alpha^{-1}) = ((\alpha^{-1})^n).A(\alpha^{-1}) = \alpha^{-n}.\sum_{i=0}^{n}(\frac{a_i}{\alpha^{-1}})^i = \alpha^{-n}.\sum_{i=0}^{n}\alpha^i.a_i = \alpha^{-n}.P(\alpha) = 0 \qquad \square$$

```
# Fonction qui permet le calcul d'un polynôme annulateur
# de l'inverse d'un nombre algébrique

annulInverse := proc(u)
local A, n, G, v;
v := 1/u;
A := PolynomialTools:-MinimalPolynomial(v, X);
n := degree(A(X));
G := X -> X^n*A(X);
return G(v);
end proc
```

Exemple 2. Nous avons précédemment vu que le polynôme minimal de $\alpha = \sqrt{2}+\sqrt{3}$ est $X^4 - 10X^2 + 1$. Retrouvons ce résultat grâce à la théorie des résultants. Soient A et B les polynômes minimaux de $\sqrt{2}$ et $\sqrt{3}$. Construisons $\mathsf{Syl}(A(Y), B(Y-X))$. On a $B(Y-X) = (Y-X)^2 - 3 = Y^2 + (-2X)Y + (X^2+3)$ d'où

$$\mathsf{Syl}(A(Y), B(Y-X)) = \begin{pmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & -2 \\ 1 & -2X & X^2+3 & 0 \\ 0 & 1 & -2X & X^2+3 \end{pmatrix}$$

et donc,

$$\mathsf{Res}_Y((A(Y), B(Y-X)) = \begin{vmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & -2 \\ 1 & -2X & X^2-3 & 0 \\ 0 & 1 & -2X & X^2-3 \end{vmatrix}$$

En utilisant la fonction Maple codée précédemment on obtient alors

```
> annulSomme(a, b)
```

$$X^4 - 10X^2 + 1$$

D'où $\mathsf{Res}_Y((A(Y), B(Y-X)) = X^4 - 10X^2 + 1$.

Ce qui correspond au polynôme minimal trouvé lors du précédent exemple. Nous avons ici obtenu un polynôme annulateur qui est *le* polynôme minimal, mais ce ne sera pas le cas.

3 Digression sur les corps finis

On va ici s'intéresser au cas particulier des corps finis.

Notation 4. On dénotera par $q := p^n$ la puissance n-ième d'un nombre premier p.

Proposition 8. *Pour tout p premier, il existe un corps fini à p^n éléments, unique à isomorphisme près, qui sera noté $\mathbb{F}_q$.*

Contrairement au cas où le corps plancher est $\mathbb{Q}$, nous disposons d'algorithmes de construction de polynômes minimaux efficace.

Proposition 9. *Soient P un polynôme de degré n à coefficients dans $\mathbb{F}_q$, et α une racine de P dans $\mathbb{F}_{q^n}$. Alors P admet n racines (distinctes !) dans $\mathbb{F}_{q^n}$, qui ne sont autre que les α^{q^i}, où i décrit $\{1, ..., n-1\}$.*

Définition 11. Soit α un élément algébrique de degré n sur $\mathbb{F}_q$. On appelle conjugués de α sur $\mathbb{F}_{q^n}$ les racines de son polynôme minimal, i.e. les α^{q^i}, où i décrit $\{1, ..., n-1\}$.

Il nous est maintenant facile de constuire le polynôme minimal (dans $\mathbb{F}_{q^n}$!) de $\alpha \in \mathbb{F}_q$.

Algorithme 1 (Méthode des conjugués)**.** Soit $\alpha \in \mathbb{F}_{q^n}$, on calcule les puissances successive de α^q jusqu'à trouver le plus petit entier m tel que $\alpha^{q^m} = \alpha$. On obtient ainsi que α est algébrique de degré m et

$$Irr(\alpha, \mathbb{F}_q, X) = \prod_{i=0}^{m} (X - \alpha^{q^i}).$$

Références

[1] Leçon 143 - RIFFAUT Antonin - http://perso.eleves.ens-rennes.fr/~ariffaut/Agregation/memoire_agregation.pdf

[2] Chapitre 12 - "Mathématiques L3 algèbre" - Aviva Szpirglas.