

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	2
1 Un peu de théorie	3
1.1 Rappels	3
1.2 Eléments algébriques	3
1.3 Résultants	5
2 Digression sur les corps finis	8

Introduction

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec et eleifend erat, eu aliquam elit. Etiam eu viverra est. Proin sed diam vel orci vehicula egestas. In facilisis scelerisque elit. Integer et hendrerit quam, sed pellentesque velit. Nullam pellentesque dui ac luctus rhoncus. Duis fringilla dapibus lorem in hendrerit. Duis efficitur fringilla consequat. Quisque viverra purus ac nibh tristique iaculis. Donec euismod diam sem, quis sagittis lacus volutpat sit amet. Sed nec ultricies eros. Suspendisse ullamcorper est ut sapien ultrices, in sodales massa tempus. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi dignissim dapibus ultrices.

Nunc hendrerit, erat bibendum pharetra pellentesque, risus nulla congue lorem, et lobortis libero magna quis ligula. Praesent et elementum nulla. In hac habitasse platea dictumst. Nulla dignissim nibh sodales nulla tristique condimentum. Nam luctus urna ac ligula scelerisque, non euismod ante pulvinar. Vivamus luctus tellus quis viverra laoreet. Proin vel iaculis libero. Sed tempor massa urna, non rhoncus urna pulvinar nec. Sed ut condimentum sem. Maecenas ac dolor metus. Sed eu luctus arcu.

Mauris tempor mauris diam, et porttitor tortor mollis sit amet. Maecenas dui neque, imperdiet egestas posuere at, ornare vitae ligula. Fusce scelerisque dictum consequat. Etiam nec tempus nisi. Morbi scelerisque sapien augue, nec placerat ex mollis id. Donec sit amet nibh ut mi condimentum malesuada. Donec sit amet felis varius, lobortis lacus vitae, bibendum justo. Curabitur lacinia lectus ac lacinia porta. Donec elit ante, pulvinar aliquam dolor ac, ullamcorper suscipit erat. Curabitur dignissim, tortor a mollis cursus, risus sapien aliquam risus, at lobortis urna tellus at lectus. Etiam in luctus nibh. Praesent maximus orci turpis, sed tincidunt mauris aliquam id. Duis eu interdum tellus. Pellentesque nibh tellus, varius eget diam ac, viverra faucibus tellus.

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. $A^\times = A - \{0\}$.

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.

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

$$ev_\alpha : \begin{cases} \mathbb{K}[X] & \longrightarrow \mathbb{L} \\ P(X) & \longmapsto P(\alpha) \end{cases}$$

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_α 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_α 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 $I(\alpha) = (P(X))$, $I(\alpha)$ 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 $Q(X) \in I(a) - \{0\} = (P(X)) - \{0\}$ ssi $P(X) \mid Q(X)$. \square

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

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

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'Eisenstein - 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 $\forall i \in \llbracket 0, n-1 \rrbracket$*

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

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 $\mathbb{K}(\alpha_1, \dots, \alpha_n)$ le plus petit corps, au sens de l'inclusion, contenant \mathbb{K} , $\alpha_1, \dots, \alpha_n$.

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 $[\mathbb{K}(\alpha, \beta) : \mathbb{K}] = [\mathbb{K}(\alpha, \beta) : \mathbb{K}(\alpha)] \cdot [\mathbb{K}(\alpha) : \mathbb{K}]$. 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

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

d'où

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

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

1.3 Résultants

Introduisons maintenant une notion fondamentale, celle de *résultant*, qui va nous permettre de donner une seconde démonstration - cette fois ci constructive - 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 :

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

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

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

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

Notation 3. On notera $\text{Res}_Y(A, B)$ 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 $\alpha + \beta$, $\alpha \cdot \beta$ 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 $S(X) := \text{Res}_Y(A(Y), B(X - Y))$ est un polynôme annulateur de $\alpha + \beta$.*
- ii) *Le polynôme $P(X) := \text{Res}_Y(A(Y), X^m \cdot B(\frac{X}{Y}))$ est un polynôme annulateur de $\alpha \cdot \beta$.*

Démonstration. De simples calculs suffisent, remarquons que

- i) $S(\alpha + \beta) = \text{Res}_Y(A(Y), B(\alpha + \beta - Y))$. 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 $S(\alpha + \beta) = \text{Res}_Y(A(Y), B(\alpha + \beta - Y)) = 0$, la conclusion s'ensuit.
- ii) De manière similaire, $P(\alpha \cdot \beta) = \text{Res}_Y(A(Y), (\alpha \cdot \beta)^m \cdot B(\frac{\alpha \cdot \beta}{Y}))$. Or, $A(\alpha) = 0$ et $(\alpha \cdot \beta)^m \cdot B(\frac{\alpha \cdot \beta}{\alpha}) = (\alpha \cdot \beta)^m \cdot B(\beta) = 0$. Le terme $(\alpha \cdot \beta)^m$ est nécessaire lorsque $\alpha = 0$. La conclusion s'ensuit.

□

```

1  # Fonction qui permet le calcul d'un polynôme annulateur
2  # de la somme de nombres algébriques
3
4  annulSomme := proc(u, v)
5  local f, g, A, B, syl, res;
6  A := PolynomialTools:-MinimalPolynomial(u, X);
7  B := PolynomialTools:-MinimalPolynomial(v, X);
8  f := Y -> subs(X = Y, A);
9  g := Y -> subs(X = Y, B);
10 syl := SylvesterMatrix(f(Y), g(Y - X), Y);
11 res := Determinant(syl);
12 return res;
13 end proc;
14
15 # Fonction qui permet le calcul d'un polynôme annulateur
16 # du produit de nombres algébriques
17
18 annulProduit := proc(u, v) \
19 local f, g, A, B, res, m;
20 A := PolynomialTools:-MinimalPolynomial(u, X);
21 B := PolynomialTools:-MinimalPolynomial(v, X);
22 f := Y -> subs(X = Y, A);
23 g := Y -> subs(X = Y, B);
24 m := degree(g(Y));
25 res := resultant(f(Y), X^m*g(Y/X), Y);
26 return res;
27 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 :

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

```

1  # Fonction qui permet le calcul d'un polynôme annulateur
2  # de l'inverse d'un nombre algébrique
3
4  annulInverse := proc(u)
5  local A, n, G, v;
6  v := 1/u;
7  A := PolynomialTools:-MinimalPolynomial(v, X);
8  n := degree(A(X));
9  G := X -> X^n*A(X);
10 return G(v);
11 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 $Syl(A(Y), B(Y - X))$. On a $B(Y - X) = (Y - X)^2 - 3 = Y^2 + (-2X)Y + (X^2 + 3)$ d'où

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

et donc,

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

En utilisant la fonction Maple codée précédemment on obtient alors

> annulSomme(a, b)

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

D'où $Res_Y((A(Y), B(Y - X))) = X^4 - 10X^2 + 1$.

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.

2 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 placher 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 $\{1, \dots, n-1\}$.*

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 $\{1, \dots, n-1\}$.

Il nous est maintenant facile de construire 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

$$\text{Irr}(\alpha, \mathbb{F}_q, X) = \prod_{i=0}^{m-1} (X - \alpha^{q^i}).$$