ÉNS de Lyon
M2 FEADEP

Cours d'algèbre
2018-2019

Polynômes de plusieurs variables, racines, critères d'irréductibilité

Leçons directement concernées (2019)

(102)* Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.
(122)* Anneaux principaux. Applications.
(141) Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
(144)* Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.

Leçons directement liées, dans lesquelles on peut parler d'extensions de corps (2019)

(105) Groupe des permutations d'un ensemble fini. Applications.
(120) Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
(121) Nombres premiers. Applications.
(123) Corps finis. Applications.
(125)* Extensions de corps. Exemples et applications.
(126) Exemples d'équations en arithmétique.
(142)* PGCD et PPCM, algorithmes de calcul. Applications.
(153) Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.

Leçons où des extensions de corps peuvent également apparaître sporadiquement (2019)

(152) Déterminant. Exemples et applications.
(156) Exponentielle de matrices. Applications.
(170) Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.
(171)* Formes quadratiques réelles. Coniques. Exemples et applications.

Ce qui est dans le programme

(b) Algèbre des polynômes à une ou plusieurs indéterminées sur un anneau commutatif. Racine d'un polynôme, multiplicité. Relations entre les coefficients et les racines d'un polynôme scindé. Sommes de Newton. Polynôme dérivé. Décomposition en somme de polynômes homogènes. Polynômes symétriques.

(d) Factorialité de $A[X]$ quand A est un anneau factoriel. Polynômes irréductibles. Exemples : polynômes cyclotomiques dans $\mathbb{Q}[X]$, critère d'Eisenstein.

(f) Corps des fractions rationnelles à une indéterminée sur un corps. Décomposition en éléments simples. Cas réel et complexe.

Bibliographie

- À suivre...

Ce polycopié a pour objectif de proposer une synthèse d'un certain nombre de techniques liées à la manipulation des polynômes à une ou plusieurs indéterminées sur un anneau factoriel.

Tous les anneaux considérés seront commutatifs, et on désigne toujours par A un anneau commutatif et K un corps.

Avant toute chose, rappelons brièvement la propriété universelle des algèbres de polynômes

Théorème 0.1 (Propriété universelle des algèbres de polynômes (finies))**.** *Soit A un anneau commutatif et B une A-algèbre. Soit $n \in \mathbb{N}^*$. Soient $\mathbf{b} = (b_1, \dots, b_n)$ un n-uplet d'éléments de B qui commutent deux à deux. Alors il existe un unique morphisme de A-algèbres $\varphi = \mathrm{ev}_{\mathbf{b}} : A[X_1, \dots, X_n] \to B$ tel que $\varphi(X_i) = b_i$ pour tout $i \in [\![1, n]\!]$.*

Ceci définit en particulier $P(\mathbf{b}) = \varphi(P)$ et permet de manipuler des formules usuelles. On notera que la condition de commutativité est vide si $n = 1$, ce qui est le cas en général quand on manipule des polynômes d'endomorphisme en algèbre linéaire par exemple.

Corollaire 0.2. *On a un isomorphisme d'algèbres naturel $A[X_1, \dots, X_n][Y] \simeq A[X_1, \dots, X_n, Y]$.*

Corollaire 0.3. *À tout polynôme $P \in A[X_1, \dots, X_n]$, on associe une fonction $f_P : A^n \to A$ dite polynômiale, donnée par $(x_0, \dots, x_n) \mapsto P(x_0, \dots, x_n) = \mathrm{ev}_{x_1,\dots,x_n}(P)$.*

Remarque 0.4. Si B est une R-algèbre et que $\rho : A \to R$ est un morphisme d'anneau, alors B hérite d'une structure de A algèbre via ρ mais il faudra alors remarquer que les coefficients de P via φ sont « modifiés » par ρ.

1 Polynômes à n indéterminées

On se fixe un entier naturel $n \in \mathbb{N}^*$ et on considère l'algèbre $A[X_1, \dots, X_n]$ des polynômes à n indéterminées sur un anneau A.

1.1 Degré, polynômes homogènes

Notation 1.1. Pour tout n-uplet d'entiers naturels $\mathbf{m} = (m_1, \dots, m_n)$ on notera $X^{\mathbf{m}} = X_1^{m_1} \cdots X_n^{m_n}$.

Définition 1.2. Un *monôme* est un polynôme de la forme $aX^{\mathbf{m}} = aX_1^{m_1} \cdots X_n^{m_n}$ avec $a \in A$ et $(m_1, \dots, m_n) \in \mathbb{N}^n$. Il est *non nul* si $a_{\mathbf{m}} \neq 0$.

Son *degré total*, ou plus simplement son *degré*, est $\deg(aX_1^{m_1} \cdots X_n^{m_n}) = \begin{cases} -\infty & \text{si } a = 0 \\ \sum_{i=1}^n m_i & \text{sinon.} \end{cases}$. Son *multidegré* est $\mathrm{mdeg}\,(X_1^{m_1} \cdots X_n^{m_n}) = (m_1, \dots, m_n)$.

Le *degré total* (ou *degré*) d'un polynôme $P = \sum_{\mathbf{m}=(m_1,\dots,m_n)\in\mathbb{N}^n} a_{\mathbf{m}} X_1^{m_1} \cdots X_n^{m_n}$ est le maximum des degrés des monômes qui le constituent, autrement dit, $\deg(P) = \begin{cases} -\infty & \text{si } P = 0 \\ \max\{\sum_{i=1}^n,\ a_{\mathbf{m}} \neq 0\} & \text{sinon.} \end{cases}$.

Le *degré partiel* en X_i d'un polynôme $P \in A[X_1, \dots, X_n]$, noté $\deg_{X_i}(P)$, est le degré du polynôme canoniquement associé à P dans l'anneau $A[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n][X_i]$.

Fait 1.3. *Pour tous $P, Q \in A[X_1, \dots, X_n]$, on a :*
(1) $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$ *avec égalité si* $\deg(P) \neq \deg(Q)$ *;*
(2) $\deg(PQ) \leq \deg(P) + \deg(Q)$ *avec égalité si A est intègre.*

Définition 1.4. Un polynôme est dit *homogène* de degré d si les monômes non nuls qui le constituent sont tous de degré d.

Une *forme algébrique* de degré d à n variables est l'application polynomiale $f_P : K^n \to K$ associée à un polynôme $P \in K[X_1, \dots, X_n]$ homogène de degré d.

Exemple 1.5.

(1) Une forme algébrique de degré 1 est une forme linéaire.

(2) Une forme algébrique de degré 2 est une forme quadratique.

(n) Le déterminant $\det = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \prod_{j=1}^n X_{\sigma(j),j}$ est un polynôme homogène en n^2 variables de degré n. La forme algébrique associée $f_{\det}$ de degré n permet de définir une application n-linéaire alternée f sur le A-module libre A^n, donnée par $f\left(\sum x_{1j}, \dots, \sum x_{nj}\right) = f_{\det}(x_{i,j})$.

Fait 1.6. *L'ensemble des polynômes homogènes de degré d est un A-module libre de rang $\binom{n+d-1}{d}$ et de base $(X_1^{m_1}\cdots X_n^{m_n})_{\mathbf{m}}$ où $\mathbf{m}=(m_1,\dots,m_n)\in\mathbb{N}^n$ vérifie $m_1+\cdots+m_n=d$.*

Exemple 1.7.

(1) L'espace vectoriel des formes linéaires sur K^n est de dimension n.

(2) L'espace vectoriel des formes quadratiques sur K^n est de dimension $\binom{n+2-1}{n}=\frac{n(n+1)}{2}$.

Voici deux liens entre les polynômes à plusieurs variables et les polynômes homogènes :

Lemme 1.8. *Soit $P\in A[X_1,\dots,X_n]$ un polynôme, $Q(T)=P(TX_1,\dots,TX_n)\in A[X_1,\dots,X_n][T]$ et $d\in\mathbb{N}$. S'équivalent :*

(i) le polynôme $P\in A[X_1,\dots,X_n]$ est homogène de degré d ;

(ii) $Q(T)=T^dP(X_1,\dots,X_n)$;

(iii) le polynôme $Q(T)$ est un monôme de degré d.

Démonstration. Soit $P=\sum_{\mathbf{m}} a_{\mathbf{m}}X^{\mathbf{m}}\in A[X_1,\dots,X_n]$. Alors $Q(T)=\sum_{d\in\mathbb{N}}\sum_{\substack{\mathbf{m}\in\mathbb{N}^n\\ m_1+\cdots+m_n=d}} a_{\mathbf{m}}X^{\mathbf{m}}T^d$. $(i)\Rightarrow(ii)$ car tous les monômes non nuls ont degré d donc on peut ôter la somme sur $d\in\mathbb{N}$. $(ii)\Rightarrow(iii)$ est évident. $(iii)\Rightarrow(i)$ car tout monôme de P doit être soit nul, soit de degré d. □

Proposition 1.9 (Échelonnement en degré)**.** *Tout polynôme $P\in A[X_1,\dots,X_n]$ s'écrit de manière unique sous la forme $P=\sum_{d\in\mathbb{N}}P_d$ avec $P_d\in A[X_1,\dots,X_n]$ homogène de degré d.*

Démonstration. **Existence :** Soit $Q(T)=P(TX_1,\dots,TX_n)\in A[X_1,\dots,X_n][T]$. On écrit alors $Q(T)=\sum_{d\in\mathbb{N}}P_dT^d$ avec $P_d=\sum_{\substack{\mathbf{m}\in\mathbb{N}^n\\ m_1+\cdots+m_n=d}} a_{\mathbf{m}}X^{\mathbf{m}}$. Les P_d sont homogènes de degré d par construction.

Unicité : Si $P=\sum_{d\in\mathbb{N}}P'_d$ avec P'_d homogène de degré d. Alors $Q(T)-Q(T)=0=\sum_{d\in\mathbb{N}}P'_d(TX_1,\dots,TX_n)-P(TX_1,\dots,TX_n)=\sum_{d\in\mathbb{N}}T^d\,(P'_d-P_d)$. Donc $P'_d=P_d$. □

Définition 1.10. Si $P\in A[X_1,\dots,X_n]$, on appelle *homogénéisé* de P le polynôme homogène :

$$X_0^dP\left(\frac{X_1}{X_0},\dots,\frac{X_n}{X_0}\right)\in A[X_0,\dots,X_n]\quad\text{où}\quad d=\deg(P).$$

Voici quelques propriétés des polynômes homogènes, laissées en exercice au lecteur :

Proposition 1.11. *1. Si $P\in K[X_0,\dots,X_n]$ est homogène, alors l'application polynomiale f_P est homogène, c'est-à-dire que $f_P(\lambda x)=\lambda^{\deg(P)}f_P(x)$.*

2. Réciproquement si K est infini et f_P est homogène, alors P est homogène.

3. Les facteurs irréductibles d'un polynôme homogène sont homogènes de degré inférieur.

Remarque 1.12. Il existe un lien fort entre les lieux de zéros de polynômes et la géométrie. Par exemple, X^2+Y^2-1 définit un polynôme dans $\mathbb{R}[X,Y]$ dont le lieu des zéros dans $\mathbb{R}$ est un cercle. Plus généralement, une *conique* dans K^2 est, par définition, le lieu d'annulation d'un polynôme de $K[X,Y]$ de degré total 2 ; une *quadrique* dans K^3 est le lieu d'annulation d'un polynôme de $K[X,Y,Z]$ de degré total 2.

Pour un polynôme homogène $P\in K[X_1,\dots,X_n]$, on dispose d'une forme algébrique $f_P:K^n\to K$ qui est une fonction homogène. En particulier, étant donné une droite vectoriel D de K^n, on a la disjonction suivante :

– soit f_P s'annule sur D ;

– soit f_P ne s'annule pas sur $D\setminus\{0\}$.

On ne peut pas définir directement de fonction polynômiale sur l'espace projectif (i.e. l'espace des droites vectorielles), mais on peut donner un sens à l'équation $P[x_0:\dots:x_n]=0$.

Par exemple, le polynôme $X^2+Y^2-Z^2$, qui est l'homogénéisé de X^2+Y^2-1 définit un cône de $\mathbb{R}^3$ et, en fait, une conique dans $\mathbb{P}^2(\mathbb{R})$. Une conique projective est alors, par définition, le lieu d'annulation dans $\mathbb{P}^2(K)$ d'un polynôme homogène de degré 2 de $K[X,Y,Z]$.

On étudiera plus en détails ces propriétés géométriques dans le cours de géométrie et dans le prochain cours sur les formes quadratiques, ainsi que quelques éléments de classifications.

1.2 Polynômes symétriques

Considérons le groupe $G = \mathfrak{S}_n$ et B la A-algèbre $A[X_1, \dots, X_n]$ des polynômes à n indéterminées. La propriété universelle donne l'existence d'un unique automorphisme de A-algèbres $\varphi_\sigma : B \to B$ tel que $X_i \mapsto X_{\sigma(i)}$. On note P^σ le polynôme $\varphi_\sigma(P) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$.

Ceci définit une action de groupes $\mathfrak{S}_n \circlearrowleft A[X_1, \dots, X_n]$.

Définition 1.13. Un polynôme $P \in A[X_1, \dots, X_n]$ est dit *symétrique* s'il est fixé par l'action de $\mathfrak{S}_n$. Le polynôme symétrique $\Sigma_k^n = \sum_{1 \le i_1 < \cdots < i_k \le n} \prod_{j=1}^{k} X_{i_j}$ est appelé *k-ième polynôme symétrique élémentaire.*

Par convention, on posera $\Sigma_0^n = 1$.

Exemple 1.14. $\Sigma_1^n = X_1 + \cdots + X_n$ et $\Sigma_n^n = X_1 \cdots X_n$.

Exercice 1. Écrire Σ_2^4 et Σ_3^4. Combien de monômes non nuls constituent le polynôme Σ_k^n ?

Théorème 1.15. *L'ensemble $A[X_1, \dots, X_n]^{\mathfrak{S}_n}$ des polynômes symétriques est une sous-A-algèbre de $A[X_1, \dots, X_n]$ engendrée par les Σ_k^n.*

Démonstration. La preuve de ce théorème est fondamentale car elle fournit également un algorithme qui permet d'écrire explicitement un polynôme symétrique comme polynôme en les polynômes symétriques élémentaires. On considère l'ordre lexicographique, noté $\succ$, sur $\mathbb{N}^n$ donné par

$$\mathbf{a} = (a_1, \dots, a_n) \succ \mathbf{b} = (b_1, \dots, b_n) \iff \exists k \in [\![0, n-1]\!],\ a_{k+1} > b_{k+1} \text{ et } \forall i \le k,\ a_i = b_i$$

Pour $P = \sum_{\mathbf{m} \in \mathbb{N}^n} a_{\mathbf{m}} X^{\mathbf{m}}$, on définit son multidegré par $\mathrm{mdeg}(P) = \max\{\mathbf{m} \in \mathbb{N}^n,\ a_{\mathbf{m}} \neq 0\}$ où le maximum est pris pour l'ordre lexicographique $\succ$. On dira que $a_{\mathrm{mdeg}(P)}$ est le coefficient dominant de P.

Soit P un polynôme symétrique de multidegré $\mathbf{m} = (m_1, \dots, m_n)$. On cherche alors un polynôme $Q \in A[\Sigma_1^n, \dots, \Sigma_n^n] \subset A[X_1, \dots, X_n]^{\mathfrak{S}_n}$ ayant même coefficient dominant que P et même multidegré.

Lemme 1.16. *Si P est symétrique de multidegré $\mathbf{m}$, alors $m_1 \ge m_2 \ge \cdots \ge m_n$.*

Démonstration. Soit $\sigma \in \mathfrak{S}_n$. Notons $\mathbf{m}^\sigma = \left(m_{\sigma(1)}, \dots, m_{\sigma(n)}\right)$. Le monôme $\sigma \cdot X^{\mathbf{m}} = X^{\mathbf{m}^\sigma}$ apparait dans $P^\sigma = P$. Comme $\mathbf{m} \succ \mathbf{m}^\sigma$, on a $m_1 \ge m_{\sigma(1)}$. Ceci étant valable pour tout $\sigma \in \mathfrak{S}_n$, il vient $\alpha_1 \ge \alpha_i$ pour tout i. Plus généralement, pour tout $k \in [\![1, n-1]\!]$, on montre que $m_k \ge m_{\sigma(k)}$ pour tout σ tel que $\sigma_{|[\![1,k-1]\!]} = \mathrm{id}_{[\![1,k-1]\!]}$. Ainsi, on a bien $m_1 \ge m_2 \ge \cdots \ge m_n$. □

On peut donc définir $Q = (\Sigma_1^n)^{m_1 - m_2} \cdots \left(\Sigma_{n-1}^n\right)^{m_{n-1} - m_n} (\Sigma_n^n)^{m_n} \in A[\Sigma_1^n, \dots, \Sigma_n^n]$. On a :

$$\mathrm{mdeg}(Q) = \sum_{i=1} (m_i - m_{i+1})\, \mathrm{mdeg}\,(\Sigma_i^n)$$

avec $m_{n+1} = 0$. Or $\mathrm{mdeg}\,(\Sigma_i^n) = \mathrm{mdeg}\,(X_1 \cdots X_i) = (\underbrace{1, \dots, 1}_{i \text{ termes}}, 0, \dots, 0)$. D'où :

$$\mathrm{mdeg}(Q) = (m_1 - m_2, 0, \dots, 0) + (m_2 - m_3, m_2 - m_3, 0, \dots, 0) + \cdots + (m_n, \dots, m_n) = \mathbf{m}.$$

Soit $\widetilde{P} = P - a_{\mathbf{m}} Q$. Alors $\mathrm{mdeg}(P) \succ \mathrm{mdeg}(\widetilde{P})$. Comme $\succ$ est un bon ordre sur $\mathbb{N}^n$, on en déduit que la suite définie par $P_0 = P$ et $P_{i+1} = \widetilde{P_i}$ stationne en 0 et, en particulier, que $P \in A[\Sigma_1^n, \dots, \Sigma_n^n]$ car $P = \sum P_i - P_{i+1}$ avec $P_i - P_{i+1} = P_i - \widetilde{P_i} \in A[\Sigma_1^n, \dots, \Sigma_n^n]$. □

Exercice 2. Montrer que $P = X_1^3 + X_2^3 + X_3^3$ est symétrique et l'écrire comme un polynôme en les polynômes symétriques élémentaires.

Puisqu'on s'intéresse à l'action du groupe $\mathfrak{S}_n$, il est naturel de s'intéresser également à l'action du sous-groupe $\mathfrak{A}_n$. On note $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ la signature. Parce qu'on a besoin de distinguer 1 et -1, on suppose que A est un anneau intègre de caractéristique $\mathrm{car}(A) \neq 2$. On est d'abord amené à introduire la notion suivante :

Définition 1.17. Un polynôme $P \in K[X_1, \dots, X_n]$ est dit *antisymétrique* si pour tout $\sigma \in \mathfrak{S}_n$, on a $\sigma \cdot P = \varepsilon(\sigma) P$.

Exemple 1.18. Le polynôme $\Delta = \prod_{1 \le i < j \le n} (X_i - X_j)$ est antisymétrique. En fait, c'est un polynôme antisymétrique non nul de degré minimal et il engendre le module des polynômes antisymétriques sur l'anneau des polynômes symétriques.

Voici quelques propriétés laissées en exercices :

Proposition 1.19.

(1) Pour tout polynôme antisymétrique Q, il existe un unique polynôme symétrique P tel que $Q = \Delta P$.

(2) Les polynômes $P \in A[X_1, \dots, X_n]$ fixés par l'action de $\mathfrak{A}_n$ sont exactement ceux qui s'écrivent sous la forme $P = S + \Delta T$ avec S, T symétriques. De plus, une telle écriture est unique.

1.3 Relations coefficients-racines

Dans la suite, on suppose que l'anneau A est intègre.

Définition 1.20. Soit $P \in A[T]$ un polynôme en une indéterminée. On dit que a est une racine d'ordre m si $(X-a)^m | P$ et $(X-a)^{m+1} \not| P$.

Exemple 1.21. Un élément $\alpha \in A$ est racine d'ordre supérieur à 2 si, et seulement si, $P(\alpha) = 0 = P'(\alpha)$. En revanche, on n'a pas de résultat analogue pour un ordre $m \geq 3$. Par exemple, si A est intègre de caractéristique 2, alors $P = X^2$ vérifie $P^{(k)}(0) = 0$ pour tout k mais 0 n'est pas racine d'ordre 3 car X^3 ne divise pas P.

Exercice 3. Soit A un anneau commutatif intègre et $n \in \mathbb{N}^*$.

1. Soient $P \in A[X]$ et $a_1, \dots, a_n$ des éléments de A deux à deux distincts. Soit $(m_1, \dots, m_n) \in \mathbb{N}^n$.
   (a) Montrer que s'équivalent :
      (i) pour tout $i \in [\![1, n]\!]$, l'élément a_i est racine d'ordre supérieur à m_i de P ;
      (ii) le polynôme $\prod_{i=1}^n (X - a_i)^{m_i}$ divise P.
      Indication : on pourra se ramener à l'anneau euclidien $\mathrm{Frac}(A)[X]$.
   (b) En déduire que sous ces conditions $\deg(P) \geq \sum_{i=1}^n m_i$.
2. Soit $P \in A[X_1, \dots, X_n]$.
   (a) Soient $E_1, \dots, E_n$ des parties infinies de A. Montrer que f_P est nulle sur $E_1 \times \cdots \times E_n$ si, et seulement si, $P = 0$.
   (b) Montrer que si $A = \mathbb{R}$ et f_P est nulle sur un ouvert Ω de $\mathbb{R}^n$, alors $P = 0$.

Lemme 1.22. *Soit A un anneau commutatif. Dans $A[X_1, \dots, X_d][T]$, on a l'égalité :*

$$\prod_{i=1}^{d} (T - X_i) = \sum_{i=0}^{d} (-1)^i \Sigma_i^d T^{d-i}.$$

Démonstration. C'est un calcul qui se fait par récurrence sur d. □

Proposition 1.23 (Relations coefficients-racines)**.** *Soit A un anneau commutatif, $\lambda \in A^\times$ et $P = \lambda \prod_{i=1}^d (X - \alpha_i) \in A[X]$ un polynôme scindé de racines $\alpha_1, \dots, \alpha_d \in A$ comptées avec multiplicité. On écrit $P = \sum_{i=0}^d a_i X^i$. Alors $a_d = \lambda \in A^\times$ et pour tout $i \in [\![0, d-1]\!]$, on a :*

$$a_i = a_d (-1)^{d-i} \Sigma_{d-i}^d (\alpha_1, \dots, \alpha_n).$$

Démonstration. On évalue par la propriété universelle la formule du lemme en $(\alpha_1, \dots, \alpha_n)$, ce qui donne :

$$\lambda \prod_{i=1}^{d} (X - \alpha_i) = \sum_{i=0}^{d} \lambda (-1)^i \Sigma_i^d (\alpha_1, \dots, \alpha_n) X^{d-i} = P.$$

□

Corollaire 1.24. *Soit A est un anneau commutatif intègre et $P = X^d + \sum_{i=0}^{d-1} a_i X^i \in A[X]$ un polynôme unitaire de degré d. Soit $K = \mathrm{Frac}(A)$ et $L = \mathrm{Dec}_K(P)$ le corps de décomposition de P sur K. Soient $\alpha_1, \dots, \alpha_d$ les racines de P dans L comptées avec multiplicité. Alors pour tout polynôme symétrique $Q \in A[X_1, \dots, X_n]$, il existe (un unique) polynôme $R \in A[Y_1, \dots, Y_d]$ tel que $Q(\alpha_1, \dots, \alpha_d) = R(a_0, \dots, a_{d-1})$.*

En particulier, toute relation symétriques en les racines d'un polynôme est un élément de l'anneau qui contient les coefficients de ce polynôme.

Exemple 1.25. Pour tout $n \in \mathbb{N}$, on a $j^n + j^{2n} \in \mathbb{Z}$, où $j = e^{\frac{i2\pi}{3}}$.

De même, $\left(\frac{1-\sqrt{5}}{2}\right)^n + \left(\frac{1+\sqrt{5}}{2}\right)^n \in \mathbb{Z}$.

2 Polynômes à une indéterminée – compléments

Si A est un anneau, il est en général difficile d'en déterminer les éléments irréductibles (penser par exemple aux irréductibles de $\mathbb{Z}/n\mathbb{Z}$). Lorsque A est un anneau factoriel, les irréductibles jouent alors un rôle important, notamment parce qu'on dispose alors d'une unique écriture en produit d'irréductibles, et donc de valuations associées aux irréductibles de A.

2.1 Permanence de la factorialité

Dans toute la suite, on se restreindra donc au cas d'un anneau factoriel A, donc intègre, dont on notera $K = \mathrm{Frac}(A)$ le corps des fractions.

Définition 2.1. Pour tout polynôme $P = \sum_{i=0}^{d} a_i X^i \in A[X] \setminus \{0\}$, on appelle *contenu* de P, noté $c(P) \in A \setminus \{0\}$, le PGCD dans l'anneau factoriel A des coefficients de P (qui est donc déterminé par le choix d'un système d'irréductibles de A).

On dira que P est *primitif* si $c(P) = 1$.

Lemme 2.2 (Lemme de Gauss sur le contenu)**.** *On suppose A factoriel.*

(1) Pour tout polynôme $P \in A[X] \setminus \{0\}$, il existe un unique $\widetilde{P} \in A[X]$ primitif tel que $P = c(P)\widetilde{P}$.

(2) Si $P, Q \in A[X]$, alors $c(PQ) = c(P)c(Q)$.

(3) Pour tout polynôme $P \in \mathrm{Frac}(A)[X] \setminus \{0\}$, il existe $\alpha \in K^\times$ et $\widetilde{P} \in A[X]$ primitif tel que $P = \alpha\widetilde{P}$. De plus, le couple $\left(\alpha, \widetilde{P}\right)$ est unique à un inversible dans A près, c'est-à-dire que si $P = \alpha Q = \beta R$, alors il existe $\lambda \in A^\times$ tel que $Q = \lambda R$ et $\beta = \lambda\alpha$.

Démonstration. (1) On écrit $P = \sum_{i=0}^{d} a_i X^i$. Pour tout $i \in [\![0, d]\!]$, on peut écrire $a_i = c(P)\widetilde{a_i}$ car $c(P)|a_i$. Le polynôme $\widetilde{P} = \sum_{i=0}^{d} \widetilde{a_i} X^i$ convient. En effet, pour tout $p \in \mathcal{P}$ irréductible de A, on a $v_p(c(P)) = \min\{a_i,\ 0 \leq i \leq d\} = v_p(c(P)) + \min\{\widetilde{a_i},\ 0 \leq i \leq d\} = v_p(c(P)) + v_p(c(\widetilde{P}))$. Donc $v_p(c(\widetilde{P})) = 0$ pour tout irréductible, c'est-à-dire $c(\widetilde{P}) = 1$. L'unicité de $\widetilde{P}$ découle de l'intégrité de l'anneau $A[X]$.

(2) On a $PQ = c(P)c(Q)\widetilde{P}\widetilde{Q}$. Donc $c(PQ) = c(P)c(Q)c(\widetilde{P}\widetilde{Q})$. Il suffit de montrer que $\widetilde{P}\widetilde{Q}$ est primitif.

On écrit $\widetilde{P} = \sum_{i=0}^{d} a_i X^i$ et $\widetilde{Q} = \sum_{j=0}^{e} b_j X^j$ et $\widetilde{P}\widetilde{Q} = \sum_{k=0}^{d+e} c_k X^k$ avec $c_k = \sum_{\substack{i+j=k \\ 0\leq i\leq d \\ 0\leq j\leq e}} a_i b_j$.

Soit $p \in A$ un élément irréductible. Il existe un indice minimal i_0 tel que $p \not| a_{i_0}$ et $\forall i < i_0,\ p|a_i$, car sinon, cela signifierait que $p|c(\widetilde{P})$. De même, il existe un indice minimal j_0 tel que $p \not| b_{j_0}$ et $\forall j < j_0,\ p|b_j$. Alors $p|S = \sum_{\substack{i+j=i_0+j_0 \\ i,j\geq 0 \\ i<i_0 \text{ ou } j<j_0}} a_i b_j$ et comme $c_{i_0+j_0} = a_{i_0}b_{j_0} + S$, on en déduit que $p \not| c_{i_0+j_0}$.

Par conséquent $p \not| c(\widetilde{P}\widetilde{Q})$. On a donc bien $c(\widetilde{P}\widetilde{Q}) = 1$ et donc $c(PQ) = c(P)c(Q)$.

(3) Existence : Soit $a \in A$ tel que $aP \in A[X]$. Alors par (1), on a $aP = c(aP)\widetilde{aP}$ avec $a \neq 0$ dans K. Ainsi $\alpha = \frac{c(aP)}{a}$ et $\widetilde{P} = \widetilde{aP}$ conviennent.

Unicité : Si $P = \alpha Q = \beta R$ avec $Q, R \in A[X]$ primitifs. Soit $a \in A \setminus \{0\}$ tel que $a\alpha, a\beta \in A$. Alors $c(aP) = c(a\alpha) = c(a\beta)$, donc il existe $\lambda \in A^\times$ tel que $a\beta = \lambda a\alpha$. Par intégrité de A, on a le résultat. □

Insistons sur le fait qu'un choix différent d'un système d'irréductibles définissant un PGCD dans A définit alors un autre contenu avec des égalités à un inversible près dans l'anneau factoriel A.

Proposition 2.3 (Éléments irréductibles de $A[X]$)**.**
Si A est factoriel, alors les polynômes irréductibles de $A[X]$ sont exactement :
- *les polynômes constants, irréductibles dans A ;*
- *les polynômes primitifs non constants irréductibles dans $K[X]$.*

Démonstration. Soit $P \in A[X]$ qu'on écrit $P = QR$ avec $Q, R \in A[X]$.

Si $P = a \in A$ est constant, alors $\deg(Q) + \deg(R) \leq 0$, donc $Q, R \in A$. Comme $A[X]^\times = A^\times$ par additivité des degrés, on en déduit que $a \in A$ est irréductible dans A si, et seulement si, il l'est dans $A[X]$.

Si $\deg(P) \geq 1$, montrons que P est irréductible dans $A[X]$ si, et seulement si, $c(P) = 1$ et P est irréductible dans $K[X]$.

$\Rightarrow$: D'une part, $c(P) = 1$ car sinon, par (1), on aurait que $P = c(P)\widetilde{P}$ est réductible car $c(P), \widetilde{P} \notin A^\times$. D'autre part, si $P = UV$ avec $U, V \in K[X]$, par l'existence de (3), on écrit $U = u\widetilde{U}$ et $V = v\widetilde{V}$ avec $u, v \in K$ et $\widetilde{U}, \widetilde{V} \in A[X]$ primitifs. Alors $P = uv\widetilde{U}\widetilde{V} \in K[X]$ donc, par l'unicité de (3), on a $uv \in A^\times$. Ainsi $\widetilde{U} \in A^\times$ ou $\widetilde{V} \in A^\times$ par irréductibilité de P dans $A[X]$. Mais alors $U \in K^\times$ ou $V \in K^\times$, ce qui nous dit bien que P est irréductible sur $K[X]$.

$\Leftarrow$: Si P est irréductible dans $K[X]$, alors l'écriture $P = QR$ donne en particulier que $Q \in K^\times \cap A = A\backslash\{0\}$ ou $Q \in A\backslash\{0\}$. Comme $c(P) = 1 = c(Q)c(R)$, on a $c(Q) = c(R) = 1$, donc $Q \in A^\times$ ou $R \in A^\times$. □

Théorème 2.4 (Permanence de la factorialité – Gauss)**.** *Si A est factoriel, alors $A[X]$ est factoriel.*

En particulier, tout anneau de polynômes sur un anneau factoriel est factoriel.

Démonstration. Premièrement, $A[X]$ est intègre car A l'est.

Deuxièmement, montrons l'existence (E) d'une décomposition en produit d'irréductibles de tout élément de $A[X]$. Soit $P \in A[X] \setminus \{0\}$ qu'on écrit $P = v\prod_{i\in I} Q_i^{m_i}$ comme produit d'irréductibles Q_i dans $K[X]$ avec $v \in K[X]^\times = K^*$. Pour chaque $i \in I$, on écrit $Q_i = \alpha_i\widetilde{Q_i}$ avec $\alpha_i \in K^*$ et $\widetilde{Q_i} \in A[X]$ primitif, donc irréductible dans $A[X]$ car Q_i l'est dans $K[X]$. Soit $p = v\prod_{i\in I} \alpha_i^{m_i} \in K^*$ et $Q = \prod_{i\in I} \widetilde{Q_i}^{m_i} \in A[X]$ primitif. On a alors $P = c(P)\widetilde{P} = pQ$ et, par unicité de (3), on a $p = \lambda c(P)$ avec $\lambda \in A^\times$. Ainsi $p \in A\backslash\{0\}$ s'écrit $p = u\prod_{j\in J} q_j^{n_j}$ comme produit d'irréductibles dans A, donc dans $A[X]$. Ceci nous donne bien une écriture en produit d'irréductibles de P.

Troisièmement, montrons l'unicité (U) d'une décomposition en produit d'irréductibles de tout élément de $A[X]$. Soit q_j un système d'irréductibles de A qu'on complète en un système d'irréductibles de $A[X]$ par des polynômes de $A[X]$ irréductibles dans $K[X]$ et primitifs P_i. Si P s'écrit de deux manière dans ce système d'irréductibles $P = u\prod_{j\in J} q_j^{n_j}\prod_{i\in I} P_i^{m_i} = v\prod_{j\in J} q_j^{n'_j}\prod_{i\in I} P_i^{m'_i}$ alors, comme les P_i forment encore un système d'irréductibles de $K[X]$, on a, par unicité dans l'anneau Euclidien $K[X]$, que $m_i = m'_i$. Par intégrité de $A[X]$, on a donc $u\prod_{j\in J} q_j^{n_j} = v\prod_{j\in J} q_j^{n'_j}$ dans A, mais alors, par unicité dans l'anneau factoriel A, on a $n_j = n'_j$. □

2.2 Quelques critères d'irréductibilité

Proposition 2.5 (Sur un corps)**.** *Soit K un corps et $P \in K[X] \setminus \{0\}$. S'équivalent*

(i) P est irréductible ;

(ii) (P) est un idéal premier de $K[X]$;

(iii) (P) est un idéal maximal de $K[X]$;

(iv) $K[X]/(P)$ est un corps.

De plus, si $\deg(P) \leq 3$, ces conditions équivalent à

(v) P est sans racines dans K.

Démonstration. L'anneau $K[X]$ est principal. □

Corollaire 2.6. *Si K est algébriquement clos, les irréductibles de $K[X]$ sont les polynômes de degré 1.*

Voici une généralisation possible de ce corollaire *, qui pourra s'avérer utile dans l'étude des polynômes sur les corps finis :

Proposition 2.7 (Critère par extension)**.** *Soit $P \in K[X]$ tel que $\deg(P) = d \geq 2$. Alors P est irréductible si, et seulement si, dans toute extension de corps L/K de degré $[L : K] \leq \frac{d}{2}$, le polynôme P est sans racines.*

Sur un anneau factoriel, on a déjà vu que :

Proposition 2.8. *$P \in A[X]$ est irréductible si, et seulement si, P est irréductible dans $K[X]$ et $c(P) = 1$.*

Exercice 4.

1. Montrer que $P = X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$ mais qu'il admet une racine sur $\mathbb{F}_{16}$.
2. En déduire une construction de $\mathbb{F}_{16}$ comme corps de rupture sur $\mathbb{F}_2$.

∗. On rappelle que toute extension finie d'un corps algébriquement clos est triviale.

Le plus important des critères d'irréductibilités est le suivant :

Proposition 2.9 (Critère d'Eisenstein)**.** *Soit A un anneau* **factoriel** *et $P = \sum_{i=0}^{d} a_i X^i \in A[X] \setminus \{0\}$. Soit $p \in A$ irréductible. On suppose que :*
- *$p \not| a_d$;*
- *$p | a_i$ pour tout $i \in [\![1, d-1]\!]$;*
- *$p^2 \not| a_0$.*

Alors P est irréductible dans $K[X]$.

En particulier, si $c(P) = 1$, alors P est irréductible dans $A[X]$.

Exercice 5. Soit $p \in \mathbb{N}^*$ un nombre premier. Montrer que $\Phi_p = \frac{X^p - 1}{X - 1}$ est irréductible sur $\mathbb{Z}$.

Voici un autre critère d'irréductibilité par réduction :

Proposition 2.10 (Critère par réduction)**.** *Soit A un anneau* **factoriel** *et $K = \mathrm{Frac}(A)$. Soit $P \in A[X]$ de coefficient dominant a_d. Soit I un idéal premier de A et $L = \mathrm{Frac}(A/I)$. On suppose que :*
- *$a_d \notin I$;*
- *l'image $\overline{P}$ de P dans $L[X]$ est un polynôme irréductible.*

Alors P est irréductible dans $K[X]$.

En particulier, si $c(P) = 1$, alors P est irréductible dans $A[X]$.

Exercice 6. Montrer que le polynôme $X^8Y + XY^2 + Y^2 + Y - 1$ est irréductible dans $\mathbb{Z}[X, Y]$.

Proposition 2.11 (Critère par recherche de racines dans le corps des fractions)**.** *Soit A un anneau factoriel et $K = \mathrm{Frac}(A)$. Soit $P = \sum_{i=0}^{d} a_i X^i \in A[X]$. Si $r = \frac{\alpha}{\beta}$ avec $\alpha, \beta \in A$ tels que $\alpha \wedge \beta = 1$ est une racine de P dans K, alors $\alpha | a_0$ et $\beta | a_d$.*

En particulier, un polynôme P primitif de degré inférieur à 3 est irréductible dans $A[X]$, si et seulement si, il n'admet pas de racines dans $\left\{ \frac{\alpha}{\beta},\ \alpha | a_0 \text{ et } \beta | a_d \right\}$.

Cette dernière condition peut offrir très peu de choses à tester pour vérifier l'irréductibilité d'un polynôme là où le critère d'Eisenstein ne s'applique pas.

Exercice 7. Le polynôme $Q = X^3 - 4X^2 - \frac{9}{2}X - \frac{5}{2}$ est-il irréductible sur $\mathbb{Q}$?

2.3 Polynômes cyclotomiques

On rappelle que $\mu_n^*(K)$ désigne l'ensemble des racines primitives n-ièmes de l'unité sur K, c'est-à-dire l'ensemble des éléments d'ordre exactement n de $K^\times$. On rappelle que le n-ième polynôme cyclotomique est $\Phi_n = \prod_{\zeta \in \mu_n^*(\mathbb{C})} (X - \zeta)$.

En travaillant dans les anneaux $\mathbb{Z}/n\mathbb{Z}$, on a déjà vu que :

Proposition 2.12 (Rappel)**.**
1. $\deg(\Phi_n) = \varphi(n) = \left| (\mathbb{Z}/n\mathbb{Z})^\times \right|$;
2. $X^n - 1 = \prod_{d|n} \Phi_d$;
3. *Φ_n est unitaire à coefficients dans $\mathbb{Z}$.*

Lemme 2.13. *Soit $n \in \mathbb{N}^*$ et K un corps de caractéristique première à n. Alors*
1. *$X^n - 1$ est sans facteur carré dans K.*
2. *L'ensemble des racines de Φ_n dans K est $\mu_n^*(K)$.*

Démonstration.
1. Si $X^n - 1$ a un facteur carré Q, on écrit $X^n - 1 = Q^2 R$ avec $Q, R \in K[X]$. En dérivant, on a $nX^{n-1} = Q(2Q'R + QR')$ donc Q divise $X^n - 1$ et nX^{n-1}. Comme n est inversible dans K par hypothèse sur la caractéristique, on en déduit que $Q | \operatorname{pgcd}(X^n - 1, X^{n-1}) = 1$.

2. Soit $\zeta \in K$ une racine de $X^n - 1$. Comme $X^n - 1 = \prod_{d|n} \Phi_d$, la racine ζ est racine de l'un des Φ_d. Mais ζ si est une racine primitive, alors ζ n'est pas racine de Φ_d pour $d|n,\ d \neq n$, donc est racine de Φ_n. Si ζ n'est pas une racine primitive, alors il existe $e|n,\ e \neq n$ tel que $\zeta^e = 1$, donc ζ est racine de $\Phi_d | X^e - 1$ pour un certain $d|e|n,\ d \neq n$. □

Théorème 2.14 (Irréductibilité des polynômes cyclotomiques)**.** *Pour tout $n \in \mathbb{N}^*$, le polynôme Φ_n est irréductible sur $\mathbb{Z}$.*

Démonstration. **Étape 1 :** Comme $\mathbb{Z}[X]$ est factoriel, on peut écrire $\Phi_n = \prod_{i=1}^{r} Q_i$ avec $Q_i \in \mathbb{Z}[X]$ irréductible. Le produit des coefficients dominants des Q_i est 1 donc les Q_i sont tous de coefficients dominant ± 1 et le nombre de -1 est pair. Quitte à remplacer certains Q_i en $-Q_i$, on peut supposer que les Q_i sont unitaires.

Étape 2 : Soit $\zeta \in \mu_n^*(\mathbb{C})$. Pour tout nombre premier p ne divisant pas n, l'élément ζ^p dans $\mu_n(\mathbb{C}) \simeq \mathbb{Z}/n\mathbb{Z}$ est encore un générateur car de même ordre n que ζ, donc $\zeta^p \in \mu_n^*(\mathbb{C})$.

Étape 3 : Soient $i, j \in [\![1, r]\!]$ tels que $Q_i(\zeta) = 0 = Q_j(\zeta^p)$. Supposons par l'absurde qu'il est possible de choisir $i \neq j$. Considérons le morphisme de $\mathbb{Q}$-algèbres $\begin{array}{rccc} \text{év}_\zeta : & \mathbb{Q}[X] & \to & \mathbb{C} \\ & P & \mapsto & P(\zeta) \end{array}$. Son noyau est (Q_i) car Q_i est irréductible et annule ζ. En particulier $Q_j \circ X^p \in \ker \text{év}_\zeta = (Q_i)$. Par unicité de l'écriture du polynôme primitif, on en déduit que $Q_j \circ X^p = RQ_i$ pour un certain $R \in \mathbb{Z}[X]$ unitaire.

Étape 4 : Notons $\bar{\cdot} : \mathbb{Z} \to \mathbb{F}_p$ la réduction modulo p, qu'on étend canoniquement par propriété universelle en $\bar{\cdot} : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ et $F : \mathbb{F}_p[X] \to \mathbb{F}_p[X]$ le morphisme de Frobenius, qui est un morphisme d'algèbres. Alors $\left(\overline{Q_j}\right)^p = F(\overline{Q_j}) = \overline{Q_j}(F(X)) = \overline{Q_j}(X^p) = \overline{Q_j \circ X^p} = \overline{Q_i R}$. Soit π un facteur irréductible de $\overline{Q_i}$ dans $\mathbb{F}_p[X]$, ce qui existe car $\deg(\overline{Q_i}) = \deg(Q_i) > 0$. Sur $\mathbb{F}_p$, on a $\pi | \overline{Q_i R} = \overline{Q_j}^p$. Par le lemme de Gauss, on a $\pi | \overline{Q_j}$, donc $\pi^2 | \overline{Q_i Q_j} | \overline{\Phi_n} | \overline{X^n - 1}$. On aboutit ainsi à une contradiction avec $i \neq j$ via le lemme (1.).

Étape 5 : Soit $\zeta' \in \mu_n^*(\mathbb{C})$. Comme ζ engendre $\mu_n^*(\mathbb{C})$, il existe $m \in \mathbb{N}$ tel que $\zeta' = \zeta^m$. Comme ζ' est d'ordre n et que $\zeta'^{\frac{n}{\text{pgcd}(m,n)}} = \zeta^{\frac{nm}{\text{pgcd}(m,n)}} = \zeta^{\text{ppcm}(m,n)} = 1$, on en déduit que n, l'ordre de ζ', divise $\frac{n}{\text{pgcd}(m,n)}$, donc que $\text{pgcd}(m, n) = 1$. On montre alors, par récurrence sur le nombre de facteurs irréductibles de ζ', que toute racine de Φ_n est racine de Q_i. Ainsi $\Phi_n | Q_i | \Phi_n$. Donc Q_i est le seul facteur irréductible de Φ_n. □

Exercice 8. Montrer que la plus petite extension de $\mathbb{Q}$ contenant toutes les racines n-ièmes de l'unité est de degré $\varphi(n)$ sur $\mathbb{Q}$.

Les polynômes cyclotomiques donnent alors une famille de polynômes irréductibles de $\mathbb{Z}[X]$. Cependant, comme la démonstration le suggère, ces polynômes ne sont en général pas irréductibles sur un corps fini. Par exemple $\Phi_8 = X^4 - X^2 + 1 = \left(X^2 + X + 1\right)$ sur $\mathbb{F}_2$. et on a le résultat suivant :

Théorème 2.15. *Soit $\kappa = \mathbb{F}_q$ un corps fini à q éléments et $n \in \mathbb{N}^*$ un entier premier à q. Soit r l'ordre de $\overline{q} \in \mathbb{Z}/n\mathbb{Z}$. Alors les facteurs irréductibles de Φ_n dans $\mathbb{F}_q$ sont deux à deux distincts et de degré r.*

Démonstration. Soit P un facteur irréductible de Φ_n de degré s et $K = \mathbb{F}_q[X]/(P)$, corps de rupture de P sur $\mathbb{F}_q$, qui est donc un corps fini de cardinal q^s. Par construction, K contient une racine de Φ_n, disons $\zeta \neq 0$ qui est donc une racine primitive n-ième de l'unité par le lemme (2.), donc d'ordre n. On a $\zeta^{q^s} = \zeta$ donc $n | q^s - 1$. Ainsi $q^s \equiv 1 \mod n$ et donc $s \geq r$.

Inversement, comme $\zeta^n = 1$ et $q^r \equiv 1 \mod n$, on a $\zeta^{q^r} = \zeta$. Soit L le sous-corps de K formé des racines de $X^{q^r} - X$. Alors $\zeta \in L$ mais $K = \mathbb{F}_q[\zeta]$ par construction comme corps de rupture, donc $L = K = \mathbb{F}_q[\zeta]$. Donc $q^s = \text{Card}(K) \leq q^r$ et ainsi $r \geq s$ car $q \geq 2$.

Ainsi, tous les facteurs irréductibles de Φ_n sont de degré r. De plus, ils sont deux à deux distincts car $\Phi_n | X^n - 1$ qui est sans facteur carré sur $\mathbb{F}_q$ par le lemme. □

Corollaire 2.16. *Le polynôme cyclotomique Φ_n est irréductible sur $\mathbb{F}_q$ si, et seulement si, $\overline{q} \in \mathbb{Z}/n\mathbb{Z}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Démonstration. Φ_n est irréductible si, et seulement si, l'ordre de $\overline{q}$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est $r = \deg(\Phi_n) = \varphi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right|$. □

En particulier, les Φ_{2^m} ne sont jamais irréductibles sur $\mathbb{F}_q$, sauf si $m \in \{1, 2\}$.

Corollaire 2.17. *Dans l'anneau $\mathbb{F}_p[X]$, les facteurs irréductibles de Φ_{p^r-1} sont de degré r.*

Un tel facteur est appelé un *polynôme primitif* sur $\mathbb{F}_p$ et ses racines sont des racines primitives $p^r - 1$-ièmes de 1. En particulier, $\mathbb{F}_{p^r} = \mathbb{F}_p[\zeta]$ pour ζ un générateur de $\mathbb{F}_{p^r}^\times$.

Exemple 2.18. Pour construire $\mathbb{F}_{16}$, on doit choisir un facteur irréductible de $\Phi_{15} = \frac{X^{15}-1}{\Phi_1 \Phi_3 \Phi_5}$. On trouve $\Phi_{15} = \left(X^4 + X^3 + 1\right)\left(X^4 + X + 1\right)$. Ainsi $\mathbb{F}_{16} = \mathbb{F}_2[X]/\left(X^4 + X + 1\right) = \mathbb{F}_2[\alpha]$ et l'élément α vérifiant $\alpha^4 = \alpha + 1$ est un générateur de $\mathbb{F}_{16}^\times$.

Ainsi $\mathbb{F}_{16} = \left\{1, \alpha, \alpha^2, \ldots, \alpha^{15}\right\}$ et la table de multiplication est immédiate. La table d'addition se dresse ensuite facilement en exploitant la relation $\alpha^4 = \alpha + 1$. Par exemple $\alpha^5 = \alpha^2 + \alpha$ et $\alpha^8 = \alpha^2 + 1$ donc $\alpha^5 + \alpha^8 = \alpha + 1 = \alpha^4$.