Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Mohamed NASSIRI

Les polynômes sont un excellent outil formel avec lequel on peut faire des calculs. Comme pour les nombres premiers, l'idée va être de donner une décomposition "atomique" des polynômes. La tâche va être compliquée par la dépendance du corps où l'on étudie les polynômes ... Par exemple, X^2+X+1 est irréductible sur $\mathbb{F}_2$ (il n'a pas de racine dans ce corps donc on ne peut pas le factoriser en produit de deux polyômes de degré 1 ...) et pourtant sur $\mathbb{C}$, $X^2+X+1=(X-j)(X-\bar{j})$ ...

Deux critères intéressants méritent d'être mis en avant : le critère d'Eisenstein et le critère de "réduction modulo". Par de la simple arithmétique, ils permettent de dire si un polynôme est irréductible.

Une autre approche va être de regarder, pour un polynôme $P \in K[X]$, les extensions du corps K où P admet une racine. De là va émerger la notion de *corps de rupture*. Par exemple, pour $P(X)=X^3-2 \in \mathbb{Q}[X]$, on va se placer dans l'extension $\mathbb{Q}(\sqrt[3]{2})$ et constater que P a bien une racine dans cette extenstion (c'est $\sqrt[3]{2}$ ...) Mais manque de bol, il manque des racines ... : $j\sqrt[3]{2}$ et $\bar{j}\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$

Précedemment, on a "cassé" notre polynôme mais pas "totalement décomposé". L'autre idée est de regarder, pour un polynôme $P \in K[X]$, une ou des extensions du corps K où P sera totalement scindé. On parle alors de *corps de décomposition*. Pour notre précédent exemple, le corps de décomposition de X^3-2 est $\mathbb{Q}(j, \sqrt[3]{2})$.

Dernière petite remarque, un corps de décomposition est a priori différent d'un corps de rupture comme on a pu le voir par l'exemple précédent. Cependant, pour les corps finis, cette notion coïncide ...

Références

[GOZ] Théorie de Galois, Ivan Gozard ♠
[GOUag] Les maths en tête : Algèbre, Xavier Gourdon
[ROU] Petit guide de calcul différentiel, François Rouvière
[FGNag1] Algèbre 1 Oraux X-ENS, Serge Francinou, Hervé Gianella et Serge Nicolas ♠

Développements

Existence et unicité des corps finis
Critère d'Eisenstein

1 Irréductibilité [GOZ] p.8 → 12

Définition 1 *Soit A un anneau. Un polynôme $P \in A[X]$ est dit irréductible dans $A[X]$ si et seulement si son dégré est supérieur ou égal à 1 et ses seuls diviseurs dans $A[X]$ sont les polynômes uP où $u \in A^*$ et les élements de A^**

Définition 2 *Soit k un sous-corps d'un corps K et $P \in k[X]$. Une racine (ou un zéro) de P dans K est un élément $\alpha \in K$ tel que $P(\alpha)=0$.*
La multiplicité de α comme racine de P est le plus grand $n \in \mathbb{N}$ tel que $(X-a)^n$ divise $P(X)$ dans $K[X]$.

Proposition 3 *(i) Tout polynôme de degré 1 est irréductible.*
(ii) Tout polynôme irréductible de degré >1 n'a pas de racine dans K.
(iii) La réciproque de (ii) est fausse.
(iv) Toutefois la réciproque de (ii) est vraie pour les polynômes de degré 2 ou 3.

Proposition 4 *Soit $P(X)=a_nX^n+...+a_1X+a_0 \in \mathbb{Z}[X]$ avec $a_n \neq 0$ et $a_0 \neq 0$. Si le rationnel α est zéro de $P(X)$, en notant $\alpha=p/q$ (avec $(p,q) \in \mathbb{Z}^* \times \mathbb{N}^*$ et $pgcd(p,q)=1$), alors $p|a_0$ et $q|a_n$.*

Définition 5 *Soit A un anneau factoriel. Pour tout polynôme non nul $P \in A[X]$, on appelle contenu de P et on note $c(P)$, le pgcd des coefficients de P.*
P est dit primitif si et seulement si $c(P)=1$.

Proposition 6 *(i) Le produit de deux polynômes primitifs est primitif.*
(ii) $\forall (P,Q) \in (A[X]\backslash\{0\})^2,\ c(PQ)=c(P)c(Q)$.

Théorème 7 *Soient A un anneau factoriel, K=Frac(A) le corps des fractions de A et $P \in A[X]$*

de degré supérieur ou égal à 1.
P est irréductible dans A[X] si et seulement si P est irréductible dans K[X] et c(P) = 1.

Théorème 8 *Critère d'Eisenstein : Soient A un anneau factoriel, K=Frac(A) le corps des fractions de A et* $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ *de degré* $n \geq 1$.
On suppose qu'il existe un élément p irréductible de A tel que :

$$(i)\ p \nmid a_n \quad , \quad (ii)\ p \mid a_0, ..., a_{n-1} \quad , \text{et} \quad (iii)\ p^2 \nmid a_0$$

Alors P est irréductible dans K[X].

Application 9 *Pour tout p premier, le polynôme* $\Phi_{p,\mathbb{Q}}(X) = \sum_{i=0}^{p-1} X^i$ *est irréductible dans* $\mathbb{Z}[X]$.

Théorème 10 *Soient A un anneau factoriel, K=Frac(A) le corps des fractions de A et* $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ *de degré* $n \geq 1$.
Soient I un idéal premier de A, $B = A/I$ *l'anneau quotient (qui est donc intègre) et L=Frac(B) le corps des fractions de B. On suppose que* $a_n \notin I$.
Si le réduit $\overline{P}$ *de P modulo I est irréductible dans L[X], alors P est irréductible dans K[X].*

Exemple 11 *Avec* $A = \mathbb{Z}$, $I = (p)$ *où p est un nombre premier, alors* $K = \mathbb{Q}$ *et* $B = \mathbb{F}_p = L$, *on a, par exemple, que* $P(X) = X^3 - 127X^2 + 3608X + 19$ *est irréductible dans* $\mathbb{Z}[X]$ *(*$p = 2$*).*

2 Extensions algébriques et polynôme minimal [GOZ] p.30 → 33

Définition 12 *Soit K un corps, et L une extension de K. Pour* $a \in L$, *on considère le morphisme de K-algèbres suivant :*

$$\begin{aligned} ev_a : K[X] &\to L \\ P(X) &\mapsto P(a) \end{aligned}$$

- Si ev_a *est injective, a est dit algébrique sur K,*
- Sinon, a est dit transcendant sur K

Théorème 13 *Si a est transcendant :*
(i) L'application

$$\begin{aligned} \widetilde{ev_a} : K(X) &\to K(a) \\ f(X) = \frac{P(X)}{Q(X)} &\mapsto f(a) = P(a)Q(a)^{-1} \end{aligned}$$

est un ismorphisme de K-algèbres.
(ii) $[K(a) : K] = +\infty$

Remarque 14 *Pour le reste de cette partie, on suppose que a est algébrique.*

Définition 15 *K[X] étant principal,* $\mathrm{Ker}(ev_a)$ *est un idéal principal de K[X] engendré par un unique polynôme* $\pi_{a,K}(X) \in K[X]$ *appelé polynôme minimal de a sur K.*

Proposition 16 *(i) Soit* $P(X) \in K[X]$. *(P est le polynôme minimal de a)* $\Leftrightarrow$ *(P(X) est unitaire, P(a)=0 et pour tout polynôme* $R(X) \in K[X]\backslash\{0\}$ *vérifiant R(a)=0, on a* $\deg(P) \leq \deg(R)$*).*
(ii) Soit $P(X) \in K[X]$. *(P est le polynôme minimal de a)* $\Leftrightarrow$ *(P(X) est unitaire, P(a)=0 et le polynôme P(X) est irréductible dans* $K[X]$*).*

Exemple 17 *Soient* $n \in \mathbb{N}^*$ *et* $\alpha = 2^{1/n}$. *On a* $\pi_{\alpha,\mathbb{Q}}(X) = X^n - 2$.

Proposition 18 *En notant* $m = \deg(\pi_{a,K}(X))$, *alors la famille* $(a^i)_{i \in [\![0,m-1]\!]}$ *est une base de K[a] en tant que K-e.v.*

Proposition 19 *(i) K(a)=K[a]*
(ii) Soit L une extension de K. Si $a \in L^*$ *est algébrique sur K, alors* $a^{-1} \in K[a]$
(iii) L'application

$$\begin{aligned} K(X)/(\pi_{a,K}(X)) &\to K(a) \\ \overline{P(X)} &\mapsto P(a) \end{aligned}$$

est un ismorphisme de K-algèbres.

3 Adjonction de racines

3.1 Corps de rupture [GOZ] p.57→ 59

Définition 20 *Soient K un corps et* $P \in K[X]$ *un polynôme irréductible dans K[X]. On dit que le corps L est un corps de rupture de P si et seulement si L est une extension simple de K engendré par K et une racine, notée* α, *de P.*

Exemple 21 $\mathbb{Q}(\sqrt[3]{2})$ *est un corps de rupture de* $P(X) = X^3 - 2$.

Théorème 22 *Soient K un corps et* $P \in K[X]$ *un polynôme irréductible dans K[X].*
(i) Il existe un corps de rupture de P.
(ii) Si $L = K(\alpha)$ *et* $L' = K(\beta)$ *sont deux corps de rupture de P, alors L et L' sont K-isomorphes*

Corollaire 23 *Soient K un corps et* $P \in K[X]$ *un polynôme de degré* $n \geq 1$. *Il existe une extension algébrique simple L de K dans laquelle P possède (au moins) une racine.*

Proposition 24 *Soit* $P \in K[X]$ *un polynôme de degré* $n \geq 1$. *P(X) est irréductible dans K[X] si et seulement si P(X) n'a pas de racine dans les extensions L de K telles que* $[L : K] \leq n/2$.

Exemple 25 *X^4+X+1 est irréductible sur $\mathbb{F}_2$ car il n'a pas de racines dans $\mathbb{F}_2$, ni $\mathbb{F}_4$.*

Proposition 26 *Soient $P \in K[X]$ un polynôme irréductible de degré $n \geq 1$ et L une extension de degré m de K avec pgcd(m,n)=1. Alors P(X) est irréductible dans L[X].*

Exemple 27 *$X^3 + X + 1$ est irréductible sur $\mathbb{Q}(i)$ comme sur $\mathbb{Q}$.*

3.2 Corps de décomposition [GOZ] p.59-60

Théorème 28 *Soient K un corps, E une extension de K et $P \in K[X]$ un polynôme de degré $n \geq 1$. On dit que E est un corps de décomposition de P sur K si et seulement si :*
(i) $\exists a \in E$ et $(\alpha_1, ..., \alpha_n) \in E^n$ tel que, dans E[X], $P(X) = a(X - \alpha_1)...(X - \alpha_n)$
(ii) $E = K(\alpha_1, ..., \alpha_n)$

Exemple 29 • *$\mathbb{C} = \mathbb{R}(i)$ est le corps de décomposition sur $\mathbb{R}$ de $X^2 + 1$*
• *$\mathbb{Q}(\sqrt{2})$ est le corps de décomposition sur $\mathbb{R}$ de $X^2 - 2$*

Théorème 30 (admis) *Soient K un corps et $P \in K[X]$ un polynôme de degré $n \geq 1$.*
(i) Il existe un corps de décomposition Σ de P sur K, avec $[\Sigma : K] \leq n!$
(ii) Si Σ et Σ' sont deux corps de décomposition de P sur K, alors ils sont K-isomorphes

3.3 Corps algébriquement clos [GOZ] p.62-63

Proposition-Définition 31 *Soit K un corps. Les conditions suivantes sont équivalentes :*
(i) Tout polynôme de degré ≥ 1 de K[X] est scindé sur K ;
(ii) Tout polynôme de degré ≥ 1 de K[X] admet au moins une racine dans K ;
(iii) Les seuls polynômes irréductibles de K[X] sont ceux de degré 1 ;
(iv) Toute extension algébrique de K est identique à K lui-même.
On dit alors que K est algébriquement clos.

Exemple 32 *$\mathbb{Q}$ et $\mathbb{R}$ ne sont pas algébriquement clos*

Proposition 33 *Tout corps algébriquement clos est infini.*

Théorème 34 *Théorème de D'Alembert-Gauss :* *$\mathbb{C}$ est algébriquement clos.*

Corollaire 35 • *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*
• *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 qui n'ont pas de racine réelle.*

4 Applications

4.1 Polynômes cyclotomiques [GOZ] p.67 → 69

Proposition-Définition 36 *Soit $m \in \mathbb{N}^*$. L'ensemble $\mathbb{U}_m = \{z \in \mathbb{C} \mid z^m = 1\}$ des racines m-ièmes de l'unité dans $\mathbb{C}$.*
$\mathbb{U}_m$ est un groupe cyclique d'ordre m.
On appelle racine primitive m-ièmes de l'unité tout générateur de $\mathbb{U}_m$. On notera $\mathcal{P}_m(\mathbb{C})$ l'ensemble des racines primitives m-ièmes de l'unité.

Proposition 37 *$\mathcal{P}_m(\mathbb{C}) = \{\exp(2ik\pi/m),\ 1 \leq k \leq m,\ pgcd(k, m) = 1\}$ a pour cardinal $\varphi(m)$.*

Proposition 38 *Soient $m \in \mathbb{N}^*$ et ξ une racine primitive m-ièmes de l'unité dans $\mathbb{C}$. Alors les (autres) racines primitives m-ièmes de l'unité sont les ξ^k, où $1 \leq k \leq m,\ pgcd(k, m) = 1$.*

Définition 39 *Le sous-corps $\mathbb{Q}(\mathbb{U}_m) de \mathbb{C}$ engendré par les racines m-ièmes de l'unité, qui est $\mathbb{Q}(\xi)$ où ξ une racine primitive m-ièmes de l'unité quelconque, est appelé corps cyclotomique d'indice m.*

Définition 40 *Soit $m \in \mathbb{N}^*$. On appelle m-ième polynôme cyclotomique le polynôme*

$$\Phi_{m,\mathbb{Q}}(X) = \prod_{\xi \in \mathcal{P}_m(\mathbb{C})} (X - \xi)$$

$\Phi_{m,\mathbb{Q}}(X)$ est un polynôme unitaire de degré $\varphi(m)$ et à coefficients dans $\mathbb{C}$.

Proposition 41

$$X^m - 1 = \prod_{d|m} \Phi_{d,\mathbb{Q}}(X)$$

Proposition 42 *$\forall n \in \mathbb{N}^*$, $\Phi_{n,\mathbb{Q}}(X) \in \mathbb{Z}[X]$*

Proposition 43 *$\forall n \in \mathbb{N}^*$, $\Phi_{n,\mathbb{Q}}(X)$ est irréductible dans $\mathbb{Q}[X]$*

Corollaire 44 *Soit $n \in \mathbb{N}^*$, le polynôme minimal sur $\mathbb{Q}$ de toute racine primitive n-ième de l'unité est $\Phi_{n,\mathbb{Q}}(X)$. Donc $[\mathbb{Q}(\mathbb{U}_m) : \mathbb{Q}] = \varphi(n)$*

4.2 Corps finis [GOZ] p.85 → 89

Théorème 45 ♠ *Existence et unicité des corps finis* ♠
Soit p un nombre premier et $n \in \mathbb{N}^*$. On note $q = p^n$.
(1) *Il existe un unique corps fini à q éléments. Il est le corps de décomposition sur $\mathbb{F}_p$ de $X^q - X$. On le note $\mathbb{F}_q$*
(2) *$\mathbb{F}_q = \mathbb{F}_p[X]/(\pi)$, où π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$.*
(3) *Si π est un polynôme irréductible de degré n sur $\mathbb{F}_p$, alors $\pi(x) \mid X^q - X$ dans $\mathbb{F}_p[X]$, donc est scindé sur $\mathbb{F}_q$.*

Remarque 46 *L'assertion* (3) *se traduit par le fait que, dans les corps finis, le corps de rupture est égal au corps de décomposition.*

Exemple 47 $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$.
Comme j est racine de $X^2 + X + 1$, on a

$$\mathbb{F}_4 = \mathbb{F}_2(j) = \{0, 1, j, j^2 = 1 + j\}$$

Questions

Exercice : 1) Pour tout p premier, montrer que le polynôme $\Phi_{p,\mathbb{Q}}(X) = \sum_{i=0}^{p-1} X^i$ est irréductible dans $\mathbb{Z}[X]$.
2) Montrer que l'ensemble $\mathcal{I}$ des polynômes annulateurs de $\zeta = e^{\frac{2i\pi}{p}}$ dans $\mathbb{Q}[X]$ est $\Phi_{p,\mathbb{Q}}(X)\mathbb{Q}[X]$

Solution : 1) Posons le polynôme

$$P(X) = \Phi_{p,\mathbb{Q}}(X+1) = \sum_{i=0}^{p-1}(X+1)^i$$

On a donc

$$\begin{aligned} P(X) = \frac{1-(X+1)^p}{1-(X+1)} &= \frac{(X+1)^p - 1}{X} \\ &= X^{p-1} + \binom{p}{p-1}X^{p-2} + ... + \binom{p}{2}X + \binom{p}{1} \in \mathbb{Z}[X] \\ &:= a_p X^{p-1} + a_{p-1}X^{p-2} + ... + a_1 X + a_0 \end{aligned}$$

Pour montrer que P est irréductible, on va utiliser le critère d'Eisenstein avec le nombre premier p. On a bien $p \nmid a_p = 1$ et que $p^2 \nmid a_0 = \binom{p}{1} = p$. Il reste donc à vérifier que $p \mid a_0, ..., a_{p-1}$ (*i.e.*) $p \mid \binom{p}{k}$ pour tout $1 \leq k \leq p-1$.
Or, pour tout $1 \leq k \leq p-1$, on a

$$k!\binom{p}{k} = p(p-1)...(p-k+1)$$

Donc $p \mid k!\binom{p}{k}$, mais comme $k < p$, p est premier avec $k!$ et donc $p \mid \binom{p}{k}$.
Ainsi par le critère d'Eisenstein, P est irréductible dans $\mathbb{Q}[X]$, et dans $\mathbb{Z}[X]$ car il est unitaire.

Revenons à $\Phi_{p,\mathbb{Q}}$! Supposons, par l'absurde, que $\Phi_{p,\mathbb{Q}}$ soit composé. Il existe donc deux polynômes $U, V \in \mathbb{Q}[X]$ tels que

$$\Phi_{p,\mathbb{Q}}(X) = U(X)V(X)$$

vérifiant $\deg U < \Phi_{p,\mathbb{Q}}$ et $\deg V < \Phi_{p,\mathbb{Q}}$. Mais alors,

$$P(X) = \Phi_{p,\mathbb{Q}}(X+1) = U(X+1)V(X+1)$$

Comme $\deg U(X+1) = \deg U < \Phi_{p,\mathbb{Q}}$ et $\deg V(X+1) = \deg V < \Phi_{p,\mathbb{Q}}$. On en déduit donc que P n'est pas irréductible. Contradiction !

Par conséquent, $\Phi_{p,\mathbb{Q}}$ est irréductible dans $\mathbb{Q}[X]$, et dans $\mathbb{Z}[X]$ car il est unitaire.

2) Soit $\mathcal{I} = \{P \in \mathbb{Q}[X] \mid Q(\zeta) = 0\}$. Considérons

$$\begin{aligned} \varphi \ : \ \mathbb{Q}[X] &\to \mathbb{C} \\ Q &\mapsto Q(\zeta) \end{aligned}$$

On remarque que $\mathcal{I} = \text{Ker}\varphi$, et ainsi $\mathcal{I}$ est un idéal de $\mathbb{Q}[X]$. $\mathbb{Q}[X]$ étant un anneau principal, $\mathcal{I}$ est engendré par un unique polynôme unitaire Q (*i.e.*) $\mathcal{I} = Q\mathbb{Q}[X]$.
Or

$$\Phi_{p,\mathbb{Q}}(\zeta) = \sum_{i=0}^{p-1}\zeta^i = \frac{1-\overbrace{\zeta^p}^{=1}}{1-\zeta} = 0 \quad \Rightarrow \quad \Phi_{p,\mathbb{Q}} \in \mathcal{I}$$

Par suite, $Q \mid \Phi_{p,\mathbb{Q}}$, mais comme $Q \neq 1$ et que $\Phi_{p,\mathbb{Q}}$ est irréductible, on a donc $Q = \Phi_{p,\mathbb{Q}}$. Ainsi

$$\mathcal{I} = \Phi_{p,\mathbb{Q}}(X)\mathbb{Q}[X]$$

Exercice : 1) Montrer que $\mathbb{Q}$ possède des extensions de tout degré.
2) Montrer que le corps $\overline{\mathbb{Q}}$ (l'ensemble des éléments algébriques sur $\mathbb{Q}$) est dénombrable.

Solution : 1) Soit $n \in \mathbb{N}$. $\sqrt[n]{2} \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$ car racine du polynôme $X^n - 2 \in \mathbb{Q}[X]$. De plus, ce dernier vérifie le critère d'Eisenstein (avec $p = 2$), donc est irréductible. Par conséquent, $\sqrt[n]{2}$ est donc algébrique sur $\mathbb{Q}$ de degré n et $\mathbb{Q}[\sqrt[n]{2}]\backslash\mathbb{Q}$ est une extension de degré n.

2) Soit $P \in \mathbb{Q}[X]\backslash\{0\}$. On note

$$\mathcal{Z}(P) = \{\alpha \in \mathbb{C} \mid P(\alpha) = 0\}$$

Alors, on a

$$\overline{\mathbb{Q}} = \bigcup_{P \in \mathbb{Q}[X]\backslash\{0\}} \mathcal{Z}(P)$$

Ainsi, $\overline{\mathbb{Q}}$ est donc décrit comme une union dénombrable d'ensembles finis. Par conséquent, $\overline{\mathbb{Q}}$ est dénombrable.

Exercice : Soit $\alpha = j\sqrt[3]{2} \in \mathbb{C}$ (avec $j = e^{2i\pi/3}$). Montrer que -1 n'est pas une somme de carrés dans $\mathbb{Q}[j\sqrt[3]{2}]$.

Solution : $X^3 - 2 \in \mathbb{Q}[X]$ est le polynôme minimal sur $\mathbb{Q}$ de α car :
- $X^3 - 2$ est unitaire,
- $\alpha^3 - 2 = 0$, et
- $X^3 - 2$ est irréductible sur $\mathbb{Q}$ par le critère d'Eisenstein (avec $p = 2$).

$\mathbb{Q}[j\sqrt[3]{2}]$ est donc un corps de rupture de $X^3 - 2$, et on a l'isomorphisme suivant :

$$\mathbb{Q}[j\sqrt[3]{2}] \sim \mathbb{Q}[X]/(X^3 - 2), \qquad \text{avec } \mathbb{Q}[j\sqrt[3]{2}] \subset \mathbb{C}$$

Par ailleurs, le corps de rupture $\mathbb{Q}[\sqrt[3]{2}]$ vérifie également (par le même raisonnement) :

$$\mathbb{Q}[\sqrt[3]{2}] \sim \mathbb{Q}[X]/(X^3 - 2), \qquad \text{avec } \mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{R}$$

De plus, en posant $\beta = \sqrt[3]{2}$, on sait qu'il existe un isomorphisme entre $\mathbb{Q}[\alpha]$ et $\mathbb{Q}[\beta]$ (*i.e.*)

$$\varphi \ : \ \mathbb{Q}[\alpha] \to \mathbb{Q}[\beta]$$

Ainsi, s'il existait des éléments $x_1, ..., x_n$ de $\mathbb{Q}[\alpha]$ tels que $x_1^2 + ... + x_n^2 = -1$, alors on aurait

$$\begin{aligned} &\varphi(x_1^2 + ... + x_n^2) = \varphi(-1) \\ \Leftrightarrow\ &\varphi(x_1)^2 + ... + \varphi(x_n)^2 = -1 \end{aligned}$$

Or, pour $i = 1, ..., n$, $\varphi(x_i)^2 \in \mathbb{R}_+$. Absurde !