Polygones constructibles à la règle et au compas (← Idée Fourquaux) (1)

Algebra (Lang) ⇝ Extensions cycliques

Tests d'irréductibilité de polynômes à coefs dans $\mathbb{F}_p$ (Colvel)

141

Polynômes irréductibles à une indéterminée - Corps de rupture. Exemples et Applications

Refs: Perrin, Goblot, Lang, Colvel

I Polynômes irréductibles

① Définitions

On considère A un anneau intègre

Def: Soit $a \in A$. a est irréductible si :

$a \notin A^*$

et $\forall b,c \in A \quad a=bc \Rightarrow b \in A^*$ ou $c \in A^*$

Dans le cas de $P \in A[X]$, on dit que P est irréductible sur A.

exemple:

- Dans $\mathbb{C}[X]$ les irréductibles sont les polynômes de degré 1
- Dans $\mathbb{R}[X]$ il y a en plus les polynômes de degré 2 à discriminant négatif.

Def: A est factoriel si :

- A est intègre
- Tout élément $a \in A$ non nul s'écrit $a = u p_1 \cdots p_r$ avec $u \in A^*$ $p_1, \dots, p_r$ irréductible.
- cette décomposition est unique à permutation près des p_i et à inverse u près.

Def: Soit $P = a_n X^n + \dots + a_0 \in A[X]$ avec A factoriel.

On note $c(P) = \text{pgcd}(a_0, \dots, a_n)$ le contenu de P

On dit que P est primitif si $c(P) = 1$

② Critère d'irréductibilité

Prop: Si A est factoriel

Alors $A[X]$ est factoriel

et pour tout $P \in A[X]$ non nul :

Si P est constant, P irréd. sur $A \Leftrightarrow P \in A \setminus A^*$

Sinon, P irréd. sur $A \Leftrightarrow P$ est primitif et P irréd. sur $\text{Frac}(A)$.

Csq: Si A factoriel, $P \in A[X]$ se décompose de façon unique en produit d'irréductibles

On supposera maintenant A factoriel.

Prop [Eisenstein]: Soit $P = a_n X^n + \dots + a_0 \in A[X]$

$a \in A$ irréductible

Si $a \nmid a_n$ et $a^2 \nmid a_0$ et $a \mid a_i$ pour tout $i \in \{0, \dots, n-1\}$

Alors P est irréductible.

exemple: $X^n - p$ est irréd sur $\mathbb{Z}$ $\forall n \geq 1$ $\forall p \in \mathbb{N}$ premier.

II Adjonction des racines

Les corps sont commutatifs.

Def: Soit k un corps. On appelle extension de corps de k tout corps L tel que $k \subset L$.

Remarque: L est un k-ev, on note $[L:k]$ sa dimension.

exemple: $[\mathbb{C}:\mathbb{R}] = 2$ $\quad [\mathbb{R}(X):\mathbb{R}] = +\infty$

III Factorisation

① Polynômes cyclotomiques

Def: On définit le n-ième polynôme cyclotomique par:

$$\Phi_n = \prod_{\substack{k=1 \\ k\wedge n=1}}^{n} \left(X - e^{\frac{2ik\pi}{n}}\right)$$

Prop: $X^n - 1 = \prod_{d|n} \Phi_d$

Prop: Pour tout $n \in \mathbb{N}^*$: $\Phi_n \in \mathbb{Z}[X]$

- Φ_n est unitaire
- Φ_n est scindé à racine simple dans $\mathbb{C}$ et dans $\mathbb{F}_q$ pour $q \wedge n = 1$.

DVP **Thm:** Φ_n est irréductible sur $\mathbb{Z}$ $\forall n \in \mathbb{N}^*$

Application: Théorème de Wedderburn

Tout corps fini est commutatif.

↳ Quaternions : corps infini non-commutatif.

↑ mieux vaut dire algèbre à division aujourd'hui.

② Algorithme de Berlekamp

Soit p premier, $n \in \mathbb{N}^*$ et $q = p^n$.

Prop: Soit $R \in \mathbb{F}_q[X]$.

$$S_R : \frac{\mathbb{F}_q[X]}{\langle R \rangle} \longrightarrow \frac{\mathbb{F}_q[X]}{\langle R \rangle} \quad Q \longmapsto Q(X^r) = Q^p$$

est une application linéaire.

Algorithme:

Entrée: $P \in \mathbb{F}_q[X]$

Sortie : décomposition en facteurs irréductibles de P sur $\mathbb{F}_q[X]$

Si P est constant
retourner P

Sinon
Calculer $P \wedge P'$.

(i) Si $P \wedge P' = P$ alors $\exists R \in \mathbb{F}_q[X]$ tq $P = R^p$
Appliquer l'algo à R

(ii) si $P \wedge P' = 1$ alors calculer la matrice $S_p - id$ dans la base $\{1, X, \dots, X^{\deg P - 1}\}$
calculer $d = \dim(\ker(S_p - id))$
Si $d = 1$ retourner P
calculer un $Q \in \ker(S_p - id)$ non constant
on a $P = \prod_{\alpha \in \mathbb{F}_q} (P \wedge (Q - \alpha))$.
Appliquer (i) à $Q - \alpha$. ← Sûrement faux.

(iii) Sinon $P = P_1 P_2$ avec $P_1 = P \wedge P'$.
Appliquer l'algo à P_1 et P_2.

Thm (de la base télescopique):

Soit $K \subset L \subset M$ des corps, $(e_i)_{i\in I}$ une base de L sur K et $(f_j)_{j\in J}$ une base de M sur L.

$(e_i f_j)_{(i,j)\in I\times J}$ est une base de M sur K.

Corollaire: $[M:K] = [M:L][L:K]$

Notation: On note $K(A)$ le plus petit corps contenant K et A. Si $A=\{a_1,\dots,a_n\}$ on note aussi $K(a_1,\dots,a_n)$.

Def: Soit K un corps et $P\in K[X]$ irréductible sur K. Un corps de rupture de P sur K est une extension L de K de la forme $K(\alpha)$; où α est une racine de P

exemple:

- $\mathbb{C}$ est un corps de rupture de X^2+1 sur $\mathbb{R}$
- $\mathbb{Q}(\sqrt{2})$ est un corps de rupture de X^2-2 sur $\mathbb{Q}$.

Application: Critère d'irréductibilité.

Soit $P\in K[X]$ de degré $n\in\mathbb{N}^*$

1. P irréductible sur $K \Leftrightarrow$ P n'a pas de racine dans les extensions L de K tq $[L:K]\leq \frac{n}{2}$

2. Soit L une extension de K tq $[L:K] \wedge n = 1$

P irréductible sur $K \Leftrightarrow P$ irréductible sur L

Thm: Soit K un corps et $P\in K[X]$ irréd. sur K. Il existe un unique corps de rupture de P sur K, (à isomorphisme près) c'est $K[X]/P$.

Def: Soit K un corps et $P\in K[X]$ irréd sur K. Un corps de décomposition de P sur K est une extension L de K de la forme $K(\alpha_1,\dots,\alpha_n)$ où $\alpha_1,\dots\alpha_n$ sont les racines de $P = \hat{\prod_{i=1}}(X-\alpha_i)$

Thm: Soit K un corps et $P\in K[X]$ irréd sur K. Il existe un unique corps de décomposition de P sur K (à isomorphisme près).

Théorème de l'élément primitif

Si L est une extension de K de dimension finie et de caractéristique nulle. Alors il existe $\alpha\in L$ tel que $L=K(\alpha)$. — D/P

exemple: $K=\mathbb{Q}$ et $L=\mathbb{Q}(\sqrt{2},\sqrt{3})$.

on a $L=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Corollaire:

Le corps de décomposition d'un polynôme sur un corps K est engendré par un élément.

Irréductibilité des polynômes cyclotomiques dans $\mathbb{Z}$

Mathias Millet

30 novembre 2014

Racine primitive de l'unité Soit $n \in \mathbb{N}$, ξ est une racine primitive $n^{\text{ème}}$ de l'unité si ξ engendre $\mathbb{U}_n$. On note $\mathbb{U}_n^*$ l'ensemble des racines primitives $n^{\text{ème}}$ de l'unité.

De manière équivalente, si $p \in \mathbb{Z}$ est tel que $p \wedge n = 1$, alors $e^{\frac{2i\pi p}{n}}$ est racine primitive $n^{\text{ème}}$ de l'unité.

Définition Le $n^{\text{ème}}$ polynôme cyclotomique est défini, pour $w = e^{\frac{2i\pi}{n}}$, par

$$\Phi_n(X) = \prod_{\xi \in \mathbb{U}_n^*} (X - \xi)$$

Lemme 1 $X^n - 1 = \prod_{d|n} \Phi_d(X)$

Idée de la preuve du Lemme 1 Si ξ est une racine $n^{\text{ème}}$ de l'unité, il existe un unique $d \mid n$ tel que ξ est racine primitive $d^{\text{ème}}$ de l'unité.

Lemme 2 Soit $n \in \mathbb{N}$, p premier ne divisant pas n. Alors $P_n = X^n - 1$ est à racines simples dans $\mathbb{F}_p$.

Preuve du Lemme 2 $P \in \mathbb{F}_p$ est à racines simples si et seulement si P et P' n'ont pas de racine commune. Or si p ne divisa pas n, la seule racine de $\bar{P_n}' = \bar{n}X^{n-1}$ est 0, qui n'est pas racine de $\bar{P_n}$.

Lemme 3

1. Φ_n est unitaire dans $\mathbb{Z}[X]$
2. Φ_n est à racines simples dans $\mathbb{Z}[X]$, et dans tout $\mathbb{F}_p[X]$ tel que p ne divise pas n.

Preuve du Lemme 3

1. Immédiat grâce au lemme 1 par récurrence.
2. Immédiat grâce aux lemmes 1 et 2.

Lemme de Gauss Soit $P \in Z[X]$, on a

P unitaire et irréductible dans $\mathbb{Z}[X] \Leftrightarrow$ P irréductible dans $\mathbb{Q}[X]$.

Théorème Pour tout $n \in \mathbb{N}$, Φ_n est irreductible dans $\mathbb{Z}[X]$

Preuve du théorème

1. Soit $\xi \in \mathbb{U}_n^*$, soit f le polynôme minimal de ξ dans $\mathbb{Q}[X]$ (défini à un inversible de $\mathbb{Q}$ près). Montrons tout d'abord que l'on peut choisir f unitaire dans $Z[X]$.
   $\mathbb{Z}[X]$ étant factoriel, et Φ_n unitaire à racines simples, il existe $f_1, ..., f_r \in \mathbb{Z}[X]$, unitaires tels que $\Phi_n = \prod_{i=1}^{r} f_i$. Comme ξ est racine de Φ_n, il existe i tel que $f \mid f_i$. f_i étant unitaire et irréductible dans $\mathbb{Z}[X]$, il l'est aussi dans $\mathbb{Q}[X]$, donc f et f_i sont égaux à un inversible de $\mathbb{Q}$ près.
2. Soit maintenant p premier, et premier avec n. ξ^p est dans $\mathbb{U}_n^*$, soit g sont polynôme minimal (qui est donc dans $\mathbb{Z}[X]$ et unitaire d'après 1.). Montrons que l'on a : $f = g$.
   Remarquons que ξ est alors racine de $f(X)$ et de $g(X^p)$. Plongeons nous dans $\mathbb{F}_p$: par le morphisme de Frobenius, nous avons $\bar{g}(X^p) = \bar{g}(X)^p$, ξ est alors racine de $\bar{g}^p$, donc de $\bar{g}$. Ainsi, $\bar{f}$ et $\bar{g}$ ont un facteur commun de degré non nul Φ dans $\mathbb{F}_p[X]$. Mais alors, si f et g sont distincts, $\bar{f}g$ divise $\bar{\Phi}_n$, qui est à racine simple d'après le lemme 3, ce qui est absurde. On a donc : $f = g$.
3. Soit maintenant ξ' une autre racine $n^{\text{ème}}$ primitive de l'unité, il existe m premier avec n tel que $\xi' = \xi^m$. Soit $m = p_1...p_s$ la décomposition de m en facteurs premiers, alors, pour tout i, p_i est premier avec n. Montrons par récurrence sur s que f est aussi le polynôme minimal de ξ'.
   — Le cas $s = 1$ a été traité au point précédent.
   — Soit $s \geq 1$, supposons que pour tous $p_1, ..., p_s$ premiers et premiers avec n. Soit p premier, premier avec n. $\xi^{p_1 \cdots p_s}$ est une racine primitive $n^{\text{ème}}$ de l'unité, donc, par le point précédent, $\xi^{p_1 \cdots p_s}$ et $\xi^{p_1 \cdots p_s p}$ ont même polynôme minimal, qui est f par l'hypothèse de récurrence.
4. Ainsi, toutes les racines de Φ_n dans $\mathbb{C}$ sont racines de f, et Φ_n divise f dans $\mathbb{Q}[X]$. Comme f est irréductible, et tous deux sont unitaires et dans $\mathbb{Z}[X]$, on a $\Phi_n = f$, et Φ_n est irréductible dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$.

Références

[1] Gourdon, *Algèbre.*

[2] Perrin, *Cours d'algèbre*

[3] Hernandez, Laszlo, *Introduction à la théorie de Galois*

Théorème de l'élément primitif

Trop court

2 décembre 2014

Théorème Soit L/K une extension finie de caractéristique nulle. Alors, il existe $\alpha \in L$ tel que $L = K(\alpha)$.

Preuve L est de caractéristique nulle, commençons par supposer que $L = K(x, y)$. On note π_x et π_y les polynômes minimaux de x et y. Soit enfin M un corps de décomposition de $\pi_x \pi_y$ dans $K[X]$. Dans M, on peut écrire

$$\pi_x = (X - x) \prod_{i=2}^{m} (X - x_i) \quad \text{et} \quad \pi_y = (X - y) \prod_{j=2}^{n} (X - x_j).$$

Puisque π_x et π_y sont irréductibles dans L de caractéristique nulle, leurs racines dans M sont simples donc les x_i et les y_j sont deux à deux distincts (et respectivement distincts de x et de y). On considère alors l'ensemble (bien défini)

$$\mathcal{E} = \left\{ \frac{x - x_i}{y - y_j} \right\}.$$

$\mathcal{E}$ a au plus $(m-1)(n-1)$ éléments. Comme K est infini, il existe $t \in K \setminus \{0\}$ tel que $t \notin \mathcal{E}$, c'est-à-dire tel que $\forall i, j \; z = x + ty \neq x_i + ty_j$.

On se place alors dans $K(z)$ et on note $F(X) = \pi_x(z - tX) \in K(z)[X]$.

Dans M, F est scindé (car π_x l'est) donc on peut écrire

$$F(X) = (z - tX - x) \prod_{i=2}^{m} (z - tX - x_i) = t(y - X) \prod_{i=1}^{m} (x - x_i + t(y - X)).$$

De par la définition de t, pour tout $j \geq 2$, $F(y_j) \neq 0$ donc $F \wedge \pi_y = (X - y)$ dans $M[X]$. Par unicité du pgcd, $(X - y)$ est aussi pgcd de F et π_y dans $K(z)[X]$. En particulier, $X - y \in K'[X]$ donc $y \in K(z)$.

De plus, $x = z - ty \in K(z)$, et l'on a bien : $K(z) = K(x, y)$.

On va maintenant montrer le cas général par récurrence. On a vu le cas $n = 2$. On suppose le résultat vrai pour une extension de degré $n - 1$. Soit L/K une extension finie de degré n : $L = K(x_1, \cdots, x_n)$. On écrit alors $L = K(x_1, \cdots, x_{n-1})(x_n)$. Par hypothèse de récurrence, il existe $\alpha \in L$ tel que $K(x_1, \cdots, x_{n-1}) = K(\alpha)$. Le cas $n = 2$ permet alors de conclure.

Références Gourdon (algèbre), Francinou et Gianella (Exercices de mathématiques pour l'agrégation).