141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples d'applications.

Refs : [Perr] Perrin, Cours d'algèbre [Goz] Gozard. Théorie de Galois

Dev : [Perr], [Tau Gal], [FGN1]
(17, 18) Polynômes cyclotomiques
(58, 60) Polynômes irréductibles sur $\mathbb{F}_q$
(06) Dirichlet faible.

Cadre : A est un anneau commutatif unitaire intègre, et k un corps.

I. Polynômes irréductibles

1) Définitions et premières propriétés

[Perr] 66

Def 1 : Soit $p \in A$, on dit que p est irréductible si $p \notin A^\times$ et si, pour tout produit $ab = p$, on a $a \in A^\times$ ou $b \in A^\times$. On dit que $P \in A[X]$ est irréductible si irréductible dans l'anneau $A[X]$.

Rq 2 : On a $A[X]^\times = A^\times$.

[Goz] 9

Prop 3 : Dans $k[X]$
(a) Tout polynôme de degré 1 est irréductible
(b) Tout polynôme irréductible de degré >1 n'a pas de racine dans k
(c) La réciproque de b est fausse (Ex : $(X^2+1)^2$ sur $\mathbb{R}$).
(d) La réciproque de b est vraie pour les polynômes de degré 2 ou 3.

Ex 4 : Si l'irréductibilité est conservée (quand cela a un sens) par passage à un sous-anneau, ce n'est pas du tout le cas pour une extension : X^2+1 est irréductible sur $\mathbb{R}$ et pas sur $\mathbb{C}$.

Prop 5 : L'anneau $A[X]$ est principal si et seulement si il est euclidien si et seulement si A est un corps.

Cor 6 : Pour $P \in k[X]$, P est irréductible si et seulement si (P) est maximal (donc ssi $k[X]/(P)$ est un corps).

Ex 7 : Dans $\mathbb{Z}[X]$, X^2+1 est irréductible, mais $\mathbb{Z}[X]/(X^2+1) \simeq \mathbb{Z}[i]$ n'est pas un corps.

2) Factorialité

[Perr] 47, 51

Def 8 : Soit A un anneau intègre. On dit que A est factoriel si :
(E) Tout élément a non nul s'écrit $a = u p_1 \dots p_r$ avec $u \in A^*$ et $p_1 \dots p_r$ des irréductibles,
(U) Si $a = u p_1 \dots p_r = v q_1 \dots q_s$ sont deux décompositions, alors $s = r$ et $\exists \sigma \in \mathfrak{S}_r$ telle que $p_{\sigma(i)} = q_i$ pour $i \in [\![1, r]\!]$.

61

Ex 9 : $\mathbb{Z}$ est factoriel, $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.

Rq 10 : Un anneau principal est factoriel.

Théo 11 (Gauss) Si A est factoriel, alors $A[X]$ également

À partir d'ici, A est supposé factoriel.

Appl 12 (Lemme des noyaux)
Soit E un k-ev de dimension n, $u \in \mathcal{L}(E)$, $P = P_1^{\alpha_1} \dots P_r^{\alpha_r} \in k[X]$ décomposé en produit de facteurs irréductibles. On a
$\mathrm{Ker}\, P(u) = \bigoplus_{i=1}^{r} \mathrm{Ker}(P_i^{\alpha_i}(u))$.

3) Critères d'irréductibilité

[Goz] 10, 11

Prop 13 : Soit $P \in K[X] \setminus 0$ où $K = \mathrm{Frac}\, A$. Il existe $a \in A^*$ tel que $aP \in A[X]$. Or le polynôme aP est irréductible dans $K[X]$ si et seulement si P l'est dans $K[X]$. On peut donc se concentrer sur l'irréductibilité dans $K[X]$ des éléments de $A[X]$.

Def 14 : Soit $P \in A[X]$, on appelle contenu de P, noté $c(P)$, le pgcd des coefficients de P. Il est bien défini dans A/A^*. Si $c(P) = 1$, on dit que P est primitif.

Lemme 15 : On a $c(PQ) = c(P)c(Q)$ pour $P, Q \in A[X]$.

Théo 16 : Si $K = \mathrm{Frac}(A)$, $P \in A[X]$ non constant. Alors P est irréductible dans $A[X]$ si et seulement si il est primitif, et irréductible dans $K[X]$

déplacer dans III

[Perrin] 82

Ex 17 : Pour $n \geq 1$, le polynôme $\Phi_n(X)$ est irréductible sur $\mathbb{Q}$ et à valeurs dans $\mathbb{Z}$.

DEV

Ex 18 : Soit $n \in \mathbb{N}^*$, p premier, $q = p^\alpha$, alors les facteurs irréductibles de Φ_n dans $\mathbb{F}_q[X]$ ont tous pour degré l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

[Goz] 11, 12

Théo 19 (Critère d'Eisenstein). Soit $K = \mathrm{Frac}\, A$. $P(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ de degré ≥ 1. On suppose qu'il existe $p \in A$ irréductible divisant tous les a_i sauf a_n, et tel que p^2 ne divise pas a_0. Alors P est irréductible dans $K[X]$.

Théo 20 : Soit $K = \mathrm{Frac}\, A$, $P = \sum_{i=0}^{n} a_i X^i \in A[X]$, $I \subseteq A$ un idéal premier. $B = A/I$ l'anneau quotient, $L = \mathrm{Frac}\, B$ son corps des fractions. On suppose $a_n \notin I$. Si le réduit $\bar{P}$ de P modulo I est irréductible dans $L[X]$, alors P est irréductible dans $K[X]$

Ex 21 : En pratique, ce sera appliqué à $A = \mathbb{Z}$ et $I = (p)$. Par exemple $X^3 - 127X^2 + 3608X + 19$ est irréductible dans $\mathbb{Z}[X]$ en réduisant modulo 2.

4) Éléments algébriques, polynôme minimal.

On considère pour cette section $K-k$ une extension de k.

Pour $\alpha \in L$, on a un morphisme $k[X] \to K$ associant $P(\alpha)$ à P. On note φ_α ce morphisme et $k[\alpha]$ son image. On peut de même considérer $k(\alpha)$ le plus petit sous corps de K contenant α et k.

[Per22] 66 67

Def 22: Si le morphisme φ_α est injectif, alors $k[\alpha] \simeq k[X]$, on dit que α est transcendant sur k. On a alors $k[\alpha] \subsetneq k(\alpha)$. Ces conditions sont équivalentes.

Def 23: On a équivalence entre $k[\alpha]=k(\alpha)$, φ_α non injectif et $k[\alpha] \not\simeq k[X]$; on dit alors que α est algébrique sur k.

Ex 24: $\sqrt{2}$ est algébrique sur $\mathbb{Q}$, mais pas π ou e.

Def 25: Si $\alpha \in K$ est algébrique sur k, il existe un unique polynôme irréductible unitaire dans $k[X]$ qui soit annulateur de α. On l'appelle polynôme minimal de α sur k, noté $\mu_{\alpha,k}$ ou μ_α quand le contexte est clair.

Ex 26: X^2+1 est le polynôme minimal de i sur $\mathbb{R}$, et sur $\mathbb{Q}$.

Prop 27: $\alpha \in K$ est algébrique sur k si et seulement si $[k(\alpha):k]$ est fini, on a alors $[k(\alpha):k] = d^\circ \mu_{\alpha,k}$.

II Extension de corps par adjonction de racines.

1) Corps de rupture.

Def 28: Soit $P \in k[X]$ irréductible. On dit que L est un corps de rupture de P si L est une extension monogène de k engendrée par k et une racine de P, notée α.

[Go3] 56 58

Rq 29: L est alors une extension de k de degré $d^\circ P$.

Ex 30: Si $\deg P = 1$, k est un corps de rupture de P.

Théo 31: Soit $P \in k[X]$ irréductible.
(1) Il existe un corps de rupture pour P sur k
(2) Deux corps de rupture pour P sont k-isomorphes.

Ex 32: $\mathbb{C}$ est défini ainsi à partir de $\mathbb{R}$ pour X^2+1.

Ex 33: Le corps de rupture de X^2+X+1 sur $\mathbb{F}_2$ donne un corps à 4 éléments.

Co 34: Soit $P \in k[X]$, il existe une extension de k dans laquelle P admet au moins une racine, et cette extension est finie.

Prop 35: Soit $P \in k[X]$ de degré $n \geq 1$. P est irréductible dans $k[X]$ si et seulement s'il n'admet pas de racine dans toute extension de k de degré $\leq \frac{n}{2}$. [Go3] 59.

Rq 36: On retrouve le critère d'irréductibilité des polynômes de degré 2 ou 3.

Prop 37: Soit $P \in k[X]$ irréductible de degré $n \geq 1$. Si $K-k$ est une extension de degré m avec $m \wedge n = 1$. Alors P est irréductible sur L.

2) Corps de décomposition.

Def 38: Soit $L-k$ une extension et $P \in k[X]$ de degré n. On dit que L est un corps de décomposition si P est scindé sur L et si L est minimal avec cette propriété parmi les extensions intermédiaires. [Go3] 59 61

Rq 39: Un corps de décomposition est une extension de degré fini.

Ex 40: k est corps de décomposition de tout polynôme de degré 1.
$\mathbb{C}$ est corps de décomposition de tout polynôme réel irréductible de degré 2.

Théo 41: Soit $P \in k[X]$ de degré ≥ 1. Alors P admet un corps de décomposition sur k. Et deux corps de décomposition pour P sont k-isomorphes. De plus, le degré d'une telle extension est inférieur à $(d^\circ P)!$

Ex 42: $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de X^3-2 sur $\mathbb{Q}$, mais pas de décomposition.

Théo 43: (Élément primitif) Si $L-k$ est une extension finie, et $\mathrm{car}(k)=0$, alors il existe $\alpha \in L$ tel que $k(\alpha)=L$. [Per22]

Cas des corps finis:

Théo 44: Soit p premier et $n \in \mathbb{N}$. On pose $q=p^n$.
(a) Il existe un corps de cardinal q défini comme corps de décomposition de X^q-X.
(b) Ce corps est unique à isomorphisme près, on le note $\mathbb{F}_q$.

3) Corps algébriquement clos, clôture algébrique.

Prop 45: Soit k un corps, on a équivalence entre:
(a) Tout $P \in k[X]$ admet une racine s'il est non constant
(b) Tout $P \in k[X]$ est scindé
(c) Si $P \in k[X]$ est irréductible, il est de degré 1.
(d) Si $L-k$ est une extension algébrique, alors $L=k$.

On dit alors, si ces conditions sont remplies, que k est algébriquement clos. [Go3] 62

[Goz] 62 63

Ex46 : $\mathbb{R}$ et $\mathbb{Q}$ ne sont pas algébriquement clos.

Prop47 : Un corps fini n'est pas algébriquement clos.

Théo48 (D'Alembert-Gauss) $\mathbb{C}$ est algébriquement clos.

Cor49 : Les polynômes irréductibles de $\mathbb{R}$ sont les polynômes de degré 1 et ceux de degré 2 de discriminant négatif (strictement).

Def50 : Soit $K-k$ une extension. On dit que K est une clôture algébrique de k si l'extension est algébrique et K est algébriquement clos.

Prop51 : Soit $K-k$ une extension où K est algébriquement clos, l'ensemble M des éléments de K algébriques sur k est une clôture algébrique de k.

Ex52 $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$, mais pas de $\mathbb{Q}$, sa clôture algébrique est $\overline{\mathbb{Q}}$ l'ensemble des nombres complexes algébriques sur $\mathbb{Q}$.

Théo53 (Steinitz) Tout corps k admet une clôture algébrique, de plus, deux clôtures algébriques d'un même corps sont k-isomorphes.

Ex54 : Dans le cas d'un corps fini $\mathbb{F}_p$, la clôture algébrique $\overline{\mathbb{F}_p}$ est définie comme $\bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^{n!}}$; c'est une limite inductive des $\mathbb{F}_{p^{n!}}$.

III Etudes de certaines familles de polynômes irréductibles.

1) Polynômes irréductibles sur un corps finis.

[Goz] 87,89

Prop55 : Soit $P\in\mathbb{F}_q[X]$ irréductible, $\mathbb{F}_q[X]/(P)\simeq\mathbb{F}_{q^n}$ si $d^\circ P=n$.

Cor56 : $\mathbb{F}_{q^n}$ est corps de rupture et de décomposition de tout polynôme irred de degré n sur $\mathbb{F}_q$. Ainsi $P \mid X^{q^n}-X$.

[Tauvel]

Def57 : On définit la fonction de Möbius $\mu : \mathbb{N}^*\to\mathbb{C}$ par $\mu(1)=1$, et pour $n\geq 2$

$\mu(n)=0$ si n est divisible par un carré parfait

$\mu(n)=(-1)^r$ si n est le produit de r nombres premiers distincts.

Prop58 (Inversion de Möbius) Si $g:\mathbb{N}^*\to\mathbb{C}$ et $G : n\mapsto\sum_{d|n} g(d)$, alors

$$g(n)=\sum_{d|n}G(d)\,\mu\left(\frac{n}{d}\right).$$

DVP

Def59 On pose $P_q(d)$ l'ensemble des polynômes irréductibles de degré d sur $\mathbb{F}_q$ et $I(q,d)$ son cardinal.

[Tauvel]

Prop60 Pour $n\in\mathbb{N}$ et $q=p^\alpha$, on a $X^{q^n}-X=\prod_{d|n}\prod_{P\in P_q(d)} P(X)$ DVP

Par conséquent $I(q,n)=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d \sim \frac{q^n}{n}$ quand $n\to\infty$

Cor61 : Il existe sur $\mathbb{F}_q$ des polynômes irréductibles de tout degré.

2) Cyclotomie.

[Perrin]

Def62 : Pour $n\in\mathbb{N}$, on pose μ_n (resp μ_n^*) les racines (primitives) n-ème de l'unité dans $\mathbb{C}$.

Ex63 : $\mu_4=\{\pm1,\pm i\}$ $\mu_4^*=\{\pm i\}$.

Def64 : Pour $n\in\mathbb{N}^*$, on pose $\phi_n(X):=\prod_{\xi\in\mu_n^*}(X-\xi)$.

Prop65 : Pour $n\in\mathbb{N}^*$, on a $X^n-1=\prod_{d|n}\phi_d(X)$.

Mettre ici dvt polycyclo.

[FGN]

Appl66 : (Dirichlet, version faible) Si $n\geq 2$, il existe une infinité de nombres premiers congrus à 1 modulo n. DVP