Prérequis : on connaît les $\mathbb{F}_p$ mais pas les $\mathbb{F}_{p^n}$

⚠ déf extension dans Perrin. Regarder Gozard.

POLYNÔMES IRRÉDUCTIBLES À UNE INDÉTERMINÉE. CORPS DE RUPTURE. EXEMPLES ET APPLICATIONS

141

[PER] p47

[GOZ] p57

Cadre Soit A un anneau intègre. K un corps (donc factoriel) L/K une extension. $\alpha \in L$.

I. POLYNÔMES IRRÉDUCTIBLES

1. Définitions et premières propriétés.

Déf 1. Soit $P \in A[X]$. P est dit irréductible si
1) $P \notin A^*$
2) $P = QR \Rightarrow Q \in A^*$ ou $R \in A^*$ [PER] p46

Rq on a $A[X]^* = A^*$ en fait

Prop 2. Sur $K[X]$ on a : [GOZ] p9
1) Tout polynôme de degré 1 est irréductible.
2) Tout polynôme irréductible de degré > 1 n'a pas de racine dans K
3) des polynômes irréductibles de degré 2 ou 3 sont exactement ceux qui n'ont pas de racines dans K.

Contre-ex 3 pour 2) $(X^2+1)^2$ n'a pas de racines dans $\mathbb{Q}$ mais est réductible dans $\mathbb{Q}[X]$. [GOZ] p9

Contre-ex 4. Lorsque l'on n'est plus sur un corps :
$2X$ réductible sur $\mathbb{Z}$ mais irréductible sur $\mathbb{Q}$.

Prop 5 $P \in K[X]$ irréductible $\Leftrightarrow (P)$ est maximal (Combes)
⚠ $\Leftrightarrow K[X]/(P)$ est un corps.

Contre-ex dans $\mathbb{Z}[X]$, X^2+1 irréductible mais $\mathbb{Z}[X]/(X^2+1) = \mathbb{Z}[i]$ non corps [GOZ] p57

2. Factorialité.

Déf 6 On dit que A (toujours intègre) est factoriel si :
(E) Tout $a \in A \setminus \{0\}$ s'écrit $a = u p_1 \dots p_r$ avec $u \in A^*$ et $p_1, \dots, p_r$ irréductibles
(U) Cette décomposition est unique, à permutation et inversibles près

Thm 7 (Gauss) A factoriel $\Rightarrow A[X]$ factoriel

Dans toute la suite on considèrera que A est factoriel

App 8 lemme des noyaux. Soit $P \in K[X]$ et $u \in \mathcal{L}(E)$.
On décompose $P = P_1^{\alpha_1} \dots P_r^{\alpha_r}$ avec P_i irréductibles 2à2 distincts
Alors $\ker(P(u)) = \bigoplus_{i=1}^{r} \ker(P_i^{\alpha_i}(u))$ [GA] p64

3. Éléments algébriques et polynôme minimal. [PER]

Déf 9. Soit $\varphi_\alpha : K[X] \to L$ morphisme tq $\varphi_{\alpha|K} = Id_K$ et $\varphi_\alpha(X) = \alpha$
Si φ_α non injective, α est dit algébrique sur K.
↳ ie $\exists P \in K[X] \setminus P(\alpha) = 0$. p66

Plus précisément, si $I_\alpha = \ker \varphi_\alpha$: I_α est de la forme (P_α) où $P_\alpha \neq 0$ qu'on peut supposer unitaire.
On dit que P_α est le polynôme minimal de α sur K.

Ex 10 $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ ($\subset \mathbb{R}$) de polynôme minimal X^2-2

Rappel $K(\alpha)$ est le plus petit sous corps de L contenant K et α.
$K(\alpha) = \{f(\alpha)/g(\alpha),\ f \in K[X], g \in K[X] \text{ et } g(\alpha) \neq 0\}$ [GOZ] p23

Thm/Déf 11 On a :
(α algébrique sur K) $\Leftrightarrow$ ($K[\alpha] = K(\alpha)$) $\Leftrightarrow$ ($\dim_K K[\alpha] < +\infty$)
Plus précisément, P_α irréductible et unitaire sur K et $\dim_K K[\alpha] = [K[\alpha] : K] = \deg P_\alpha$.
On appelle cet entier degré de α. p67

Rq on a $K[X]/(P_\alpha) \simeq K[\alpha]$.

Déf 12. L est dite algébrique si $\forall \alpha \in L$, α algébrique sur K. p67 utile pour après

4. Critères d'irréductibilité : cas général [PER]

Déf 13. Soit $P \in A[X] \setminus \{0\}$ $P(X) = a_n X^n + \dots + a_0$.
Le contenu de P est $c(P) = \text{pgcd}(a_0, \dots, a_n)$ et est défini à multiplication par un inversible près. (modulo A^*) p51

Déf 14 Si $c(P) = 1$ P est dit primitif.

Lem 15 (Gauss) $c(PQ) = c(P)c(Q)$ modulo A^*.

Prop 16. Les polynômes irréductibles de $A[X]$ sont : p51
- les constantes $p \in A$ irréductibles dans A.
- les polynômes de degré ≥ 1, primitifs et irréductibles sur $\text{Frac}A$

Prop 17 Un polynôme est irréductible sur A p76
ssi il l'est sur $\text{Frac}A$ et s'il est primitif.

Ex 18 les polynômes unitaires de degré ≥ 1 sont irréductibles dans $\mathbb{Z}[X]$ ssi ils le sont dans $\mathbb{Q}[X]$

Thm 19 Critère d'Eisenstein.

Soit $P(X) = a_n X^n + \dots + a_0$ avec $a_i \in A$. $p \in A$ irréductible.

p76 **Si:** 1) $p \nmid a_n$ — **Alors** P irréductible dans $\mathrm{Frac}(A)[X]$.

2) $\forall i \in [\![0, n-1]\!]$ $p \mid a_i$

3) $p^2 \nmid a_0$

p77 **Ex 20** • Les irréductibles de $\mathbb{Z}$ sont les entiers premiers.

Si p premier, $X^{p-1} + \dots + X + 1$ est irréductible sur $\mathbb{Z}$.

• $a \in \mathbb{Z}$, $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Si l'un des $\alpha_i = 1$, alors $X^n - a$ irréductible sur $\mathbb{Z}$

p78 • $X^4 + 1$ irréductible sur $\mathbb{Z}$ mais réductible sur $\mathbb{F}_2$.

Thm 21 Critère de réduction

p77 Soit $B = A/I$, avec I idéal premier de A

Soit $P = a_n X^n + \dots + a_0 \in A[X]$ et $\bar{P}$ sa réduction modulo I

On suppose $\bar{a_n} \neq 0$ dans B. $\tilde{K} = \mathrm{Frac}\, A$; $\tilde{L} = \mathrm{Frac}\, B$

Si $\bar{P}$ irréductible sur B ou $\tilde{L}$, alors P irréductible sur $\tilde{K}$.

p77 **Rq** On utilise souvent le Thm 21 avec $A = \mathbb{Z}$, $I = (p)$ où p premier et donc $B = \mathbb{F}_p$ est un corps.

p77 **Ex 22** $X^3 + 2014X^2 + 13X - 21$ est irréductible sur $\mathbb{Z}$.

II ADJONCTION DE RACINES. (dans les corps)

1. Corps de rupture d'un polynôme. [GOZ]

p57 **Def 23** Soit $P \in K[X]$. Un corps de rupture est un corps de la forme $K(\alpha)$, où α est une racine de P.

Ex 24 Si $\deg P = 1$, K est un corps de rupture de P.

Thm 25 Existence et unicité.

Soit P un polynôme irréductible de $K[X]$.

• Il existe un corps de rupture de P.

• Si $L = K(\alpha)$ et $L' = K(\beta)$ sont 2 corps de rupture de P,

p57 alors L et L' sont isomorphes.

Plus précisément, il existe un unique K-isomorphisme

$$\varphi : L \to L'$$
$$\alpha \to \beta.$$

Rq Si α est une racine de P. $[K(\alpha) : K] = \deg P$.

Plus précisément une base de $K(\alpha)$ sur K est formée de la famille $(1, \alpha, \dots, \alpha^{\deg P - 1})$ des classes modulo (P) de $1, X, \dots, X^{\deg P - 1}$ p58

Ex 26 $X^2 + 1$ irréductible sur $\mathbb{R}$.

On construit $\mathbb{C}$ comme étant le corps de rupture de X^2+1 :

$$\mathbb{R}[X]/(X^2+1).$$

Ex 27 $X^2 + X + 1$ irréductible sur $\mathbb{F}_2$

On construit un corps à 4 éléments avec $\mathbb{F}_2[X]/(X^2+X+1)$

Prop 28 $P \in K[X]$ polynôme de degré n.

(P irréductible dans $K[X]$) $\iff$ (P n'a pas de racines dans les extensions L de K tq $[L:K] \leq n/2$) p59

App 29 $X^4 + 1$ est réductible sur $\mathbb{F}_p$, pour tout p premier (DEV) p78

Prop 30 $P \in K[X]$ irréductible de degré n.

Soit L une extension de degré m de K, avec $m \wedge n = 1$.

Alors P irréductible dans $L[X]$. p59

2. Corps de décomposition

Def 31 $P \in K[X]$ de degré $n \in \mathbb{N}^*$. [GOZ] p59

Un corps de décomposition L de P sur K est une extension L de K telle que • $\exists a, \alpha_1, \dots, \alpha_n \in L$ / $P = a(X - \alpha_1) \dots (X - \alpha_n)$ dans $L[X]$

• $L = K(\alpha_1, \dots, \alpha_n)$

↳ L est une extension minimale de K tq P ait $\deg(P)$ racines dans cette extension. [GOZ] p59

Ex 32 K est un corps de décomposition sur K de tout polynôme de degré 1. [GOZ] p66

Rq Un corps de rupture peut être un corps de décomposition

Ex 33 $\mathbb{C} = \mathbb{R}(i)$ est un corps de décomposition sur $\mathbb{R}$ de X^2+1.

⚠ Ça ne l'est pas forcément. (cf ex 35)

Thm 34 Existence et unicité. p60

$P \in K[X]$ de degré ≥ 1.

1) Il existe un corps de décomposition D de P sur K avec $[D:K] \leq n!$

2) Deux corps de décomposition de P sur K sont K-isomorphes

On note alors $D_K(P)$ "le" corps de décomposition de P sur K.

Ex 35 $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de X^3-2 sur $\mathbb{Q}$ mais est strictement inclus dans $D_{\mathbb{Q}}(P) = \mathbb{Q}(\sqrt[3]{2}, j)$.

p65

Thm 36 Théorème de l'élément primitif.

[PER] p87

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

POUR NOUS

(Rq : analogue pour les corps finis. Si $L = \mathbb{F}_{q^n}$ est une extension de $K = \mathbb{F}_q$, $\exists \alpha \in L$ / $L = K(\alpha)$) [PER] p88

Cas des corps finis

[PER] p73

Thm 37 Soit p un nombre premier et $n \in \mathbb{N}^*$.

1) Il existe un corps à p^n éléments : c'est le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$.

2) Ce corps est unique à isomorphisme près, on le note $\mathbb{F}_{p^n}$.

Rq $x \to x^{p^n}$ est un automorphisme (le Frobenius itéré n fois)

[GOZ] p87

Thm 38 p premier, $n \in \mathbb{N}^*$. $q = p^n$.

Alors $\mathbb{F}_q = \mathbb{F}_p[X]/(\Pi)$ où Π irréductible quelconque de degré n sur $\mathbb{F}_p$.

p89

Ex 39 • On a déjà un $\mathbb{F}_4$ (ex 27)

• $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3+X+1)$

[GOZ] p87

Cor 40 Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_p[X]$.

[PER] p77

(Ex 41 $X^p - X - 1$ irréductible sur $\mathbb{F}_p$)

[GOZ] p87

Cor 41 Si P est un polynôme irréductible de degré n sur $\mathbb{F}_p$, son corps de rupture ($\mathbb{F}_{p^n}$) est aussi son corps de décomposition

p89

Def 42 On définit la fonction μ de Möbius par :

$\mu(1) = 1$

$\mu(p_1 \cdots p_k) = (-1)^k$ si les p_i sont premiers distincts.

$\mu(n) = 0$ sinon.

DVPT

[FG] p190

Prop 43 p premier, $r \in \mathbb{N}^*$, $q = p^r$. Si $n \geq 1$, $A(n,q)$ est l'ensemble des polynômes de degré n irréductibles sur $\mathbb{F}_q$.

$I(n,q) = \text{Card } A(d,q)$

1) $X^{q^n} - X = \prod_{d/n} \prod_{P \in A(d,q)} P$

2) $I(n,q) = \frac{1}{n} \sum_{d/n} \mu(n/d)$ 3) $I(n,q) \underset{n \to +\infty}{\sim} q^n/n$

3. Clôture algébrique [GOZ] p62-63

Prop 44 Sont équivalents :

1) Tout polyn. de degré ≥ 1 de $K[X]$ est scindé sur K.

2) " " " " " " admet au moins une racine dans K.

3) Les seuls polynômes irréductibles de $K[X]$ sont ceux de degré 1.

4) La seule extension algébrique de K est K.

Def 45 Un corps est algébriquement clos s'il vérifie l'une des conditions précédentes.

Ex 46 $\mathbb{Q}$ et $\mathbb{R}$ ne sont pas algébriquement clos.

Prop 47 Tout corps algébriquement clos est infini.

Thm 48 D'Alembert-Gauss. $\mathbb{C}$ est algébriquement clos.

Cor 49 • Les polynômes irréductibles de $\mathbb{C}[X]$ sont ceux de degré 1

• Les " " " $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racines réelles (ie de discriminant strictement négatif).

Def 50 L est une clôture algébrique de K si L est une extension algébrique de K et si elle est algébriquement close.

Ex 51 $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Thm 52 (Admis) Steinitz.

1) Tout corps commutatif admet une clôture algébrique.

2) Deux clôtures algébriques de K sont K-isomorphes.

Ex 53 $\bigcup_{n \in \mathbb{N}^*} \mathbb{F}_{p^{n!}}$ est un clôture algébrique de $\mathbb{F}_p$.

III. POLYNÔMES CYCLOTOMIQUES (ou FACTORISATION)

1. Polynômes cyclotomiques [GOZ] p67→69

Def 54 Soit $n \in \mathbb{N}^*$. On appelle n-ième polynôme cyclotomique :

$$\Phi_n(X) = \prod_{\substack{k=1 \\ k \wedge n = 1}}^{n} (X - e^{2ikT/n})$$

C'est un polynôme unitaire de degré $\varphi(n)$, à coefficients dans $\mathbb{C}$.

p76 **Ex 55** $\Phi_1(X) = X - 1$; $\Phi_3(X) = X^2 + X + 1$; $\Phi_8(X) = X^4 + 1$.

Prop 56 $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$

Prop 57 $\forall n \in \mathbb{N}^* \quad \Phi_n(X) \in \mathbb{Z}[X]$.

DVPT [GOU] p91 p92

Prop 58 $\forall n \in \mathbb{N}^* \quad \Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$

App 59 Théorème de Dirichlet, version faible

Il y a une infinité de nombres premiers $p \equiv 1 [n]$ $n \geq 2$

2. Algorithme de Berlekamp [OA] (trop moche)

p244 p248 Thm 5.36

Algo 5.41

Références

[GOZ] Gozard, Théorie de Galois

[PER] Perrin, Cours d'algèbre

[OA] Objectif agrégation

[GOU] Gourdon Algèbre

[FG] Francinou Gianella, Exercices de mathématiques pour l'agrégation, Algèbre 1.

((Combes) Combes, Algèbre & Géométrie)

Notes de fin

- **Prop 5** C'équivalence

A principal. (p est irréductible) $\Leftrightarrow$ (p) maximal $\Leftrightarrow$ $A/(p)$ corps

(cf [GOU] p239 pour plus général)

marche ici pour $A[X]$ principal

or $A[X]$ principal $\Leftrightarrow$ A corps.

- I.3 extension.

Se méfier de la déf de [PER].

Extension L d'un corps K s'il $\exists$ morphisme $\varphi : K \to L$.

cela est équivalent à dire K sous corps de L.

JURY

Poly. irréd. de degré 2, 3 ou 4 sur $\mathbb{F}_2$

[FG] p191

On les liste.

- degré 2 ou 3 : il y en a 6.

ceux qui n'ont pas de racines : $X^2 + X + 1$

$X^3 + X + 1$

$X^3 + X^2 + 1$

- degré 4 : il y en a 8.

ceux qui n'ont pas de racines et qui ne sont pas produit de 2 polynômes de degré 2.

De plus $I(4,2) = \frac{2^2(2^2-1)}{4} = 3$.

Par élimination : $X^4 + X^3 + 1$

$X^4 + X^3 + X^2 + X + 1$

$X^4 + X + 1$