KUGLER Benoit. Références : Perrin

141 — Polynomes irréductibles à une indeterminée. Corps de rupture. App.

A désigne un anneau commutatif, unitaire, intègre, et K un corps.

I - Polynôme et corps. Irréductibilité

1) Irréductibilité, introduction

Def 1 : $P \in A[X]$ est dit <u>irréductible</u> si $P \notin A[X]^\times$ et si $P = QR$, $Q, R \in A[X] \Rightarrow Q \in A[X]^\times$ ou $R \in A[X]^\times$

Rem 2 : Les polynômes irréductibles et constants sont les irréductibles de A.

Rem 3 : Si $A = K$, si $\deg P \geq 1$, alors P irréductible ssi $P = QR \Rightarrow \deg P$ or $\deg Q = 0$

Ex 4 : $(X+1)^2$ n'est pas irréductible dans $\mathbb{Q}[X]$.

Prop 5 : Si P est irréductible dans $A[X]$, alors P n'a pas de racine dans A.

Rem 6 : Réciproque fausse : $(X^2+1)^2$ est réductible sur $\mathbb{R}$ mais n'y a pas de racines.

Prop 7 : Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 sans racines. Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

2) Structure de $A[X]$

Def 8 : Si A est factoriel, si $P \in A[X] \setminus \{0\}$ on note $c(P) = \text{pgcd}\{\text{coefficients de } P\}$, unique à $A^\times$ près.

Prop 9 : (Lemme de Gauss) $c(PQ) = c(P)\,c(Q)$

Th 10 : (Gauss) Si A est factoriel, $A[X]$ l'est.
(Hilbert) Si A est noethérien, $A[X]$ l'est.

Prop 11 : $A[X]$ principal $\Leftrightarrow$ A corps

App 12 : Si $u \in \mathcal{L}(E)$, E K-ev de dim finie, $\{P \in K[X] \,/\, P(u) = 0\}$ est un idéal de $K[X]$ non réduit à $\{0\}$. On note Π_u son unique générateur unitaire, appelé <u>polynome minimal</u> de u.

Def 13 : u est <u>semi-simple</u> si tout sev de E stable par u admet un supplémentaire stable.

Prop 14 : u est semi-simple $\Leftrightarrow \Pi_u = \prod_{i=1}^{r} P_i$, P_i irr. sur K, distincts.

Prop 15 : P premier $\Leftrightarrow$ (P) premier $\Leftrightarrow A[X]/(P)$ intègre
P irréductible $\Leftrightarrow$ (P) maximal parmi les idéaux principaux

Prop 16 : (Résultat fondamental) Si $A = K$, si $P \in K[X]$, $\boxed{P \text{ irréductible} \Leftrightarrow A[X]/(P) \text{ corps}}$

3) Critères d'irréductibilité

On suppose A factoriel, et on note ici $K = \text{Frac}(A)$

Prop 17 : Si $P \in A[X]$, $\deg P \geq 1$, on a
P irr. sur A $\Leftrightarrow$ P irr. sur K et $c(P) = 1$

App 18 : Si P unitaire sur $\mathbb{Z}$, P irr sur $\mathbb{Z} \Leftrightarrow$ P irr sur $\mathbb{Q}$

Prop 19 : Soit I idéal premier de A, $P = \sum_{k=0}^{d} p_k X^k \in A[X]$. On note $\bar{P} = \sum_{k=0}^{d} \bar{p}_k X^k \in A/_I[X]$. On suppose que $\bar{p}_d \neq 0$ et $c(P) = 1$. Alors

$$\bar{P} \text{ irr. dans } A/_I[X] \Rightarrow P \text{ irr dans } A[X]$$

Rem 20 : Réciproque fausse : X^2+1 irr sur $\mathbb{Z}$ mais pas sur $\mathbb{F}_2$

App 21 : $X^p - X - 1$ est irréductible sur $\mathbb{Z}$, si p premier

Prop 22 : (Critère d'Eisenstein) Soit $p \in A$, irréductible, $P \in A[X]$. On suppose que $p_d = 1$, $p \mid p_k$ pour $k \in [\![0, d-1]\!]$, et $p^2 \nmid p_0$. Alors P est irréductible sur A.

App 23 : Si p premier, $X^{p-1} + \dots + X + 1$ est irr. sur $\mathbb{Z}$.

II - Extensions de corps, corps de rupture

1) Généralités

Def 24 : Si K est un corps, une <u>extension</u> de K est un corps L dans lequel K se plonge. On confond souvent K avec son plongement et on note $K \subset L$.

Prop 25 : Si $K \subset L$, L est un K-ev. On note $[L:K]$ sa dimension (éventuellement infinie)

Prop 26 : (Base télescopique) Si $K \subset L \subset M$, on a

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

Prop-Def 27 : Si $K \subset L$, $\alpha \in L$ on note $I = \{P \in K[X] / P(\alpha) = 0\}$ idéal de $K[X]$.

- Si $I = \{0\}$ on dit que α est <u>transcendant</u> et on a $K[X] \simeq K[\alpha]$
- Sinon, α est dit <u>algébrique</u>. On note Π_α le générateur unitaire de I, appelé polynôme minimal de α sur K, et on a $K[\alpha] \simeq K[X]/_{(\Pi_\alpha)}$

Prop 28 : On a α algébrique $\Leftrightarrow K[\alpha] = K(\alpha) \Leftrightarrow [K[\alpha]:K] < +\infty$

Dans ce cas, Π_α est irréductible sur K et $[K(\alpha):K] = \deg \Pi_\alpha$

Prop 29 : L'ensemble des nombres algébriques sur K est un sous-corps de L.

2) Corps de rupture et de décomposition.

Th-Def 30 : Si $P \in K[X]$ est irréductible, alors il existe L ext. de K, $\alpha \in L$ tels que $P(\alpha) = 0$ et $L \simeq K[\alpha]$.
L est unique à isomorphisme près, on l'appelle <u>corps de rupture</u> de P sur K.

Ex 31 : $P = X^2+1 \in \mathbb{R}[X]$, corps de rupture : $\mathbb{R}[X]/_{(X^2+1)} \simeq \mathbb{C}$

Th-Def 32 : Si $P \in K[X]$, $\deg P = n \geq 1$, alors il existe L ext de K, $\alpha_1, \dots, \alpha_n \in L$, $\lambda \in K$ tels que $P = \lambda \prod_{i=1}^{n} X - \alpha_i$ et $L \simeq K[\alpha_1, \dots, \alpha_n]$

Un tel corps est unique à isomorphisme près, on l'appelle <u>corps de décomposition</u> de P sur K, noté $D_K(P)$

III – Corps finis

Ici, $q=p^n$, p premier, $n \geq 1$.

1) Définition

Rappel 33 : $\mathbb{Z}/p\mathbb{Z}$ corps $\Leftrightarrow$ $\mathbb{Z}/p\mathbb{Z}$ intègre $\Leftrightarrow$ p premier

Dans ce cas on note $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Prop 34 : (Caractéristique) Si K corps fini, il existe un unique couple $(p,r) \in \mathbb{N}^{*2}$, p premier, tel que $|K| = p^r$. On dit que p est la caractéristique de K. On a de plus $p \cdot 1_K = 0_K$.

Rem 35 : Il n'y a donc, par exemple, pas de corps à 6 éléments.

Th 36 : On note $\mathbb{F}_q = D_{\mathbb{F}_p}(X^q - X)$. Alors

- Tout corps de cardinal q est isomorphe à $\mathbb{F}_q$
- $\mathbb{F}_q$ est bien un corps de cardinal q.

Ex 37 : $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2+X+1)$

Prop 38 : Tout sous-groupe fini du groupe des inversibles d'un corps est cyclique. En particulier, $\mathbb{F}_q^*$ est cyclique.

Coro 39 : Si $L = \mathbb{F}_q$, $K = \mathbb{F}_p$, il existe $\alpha \in L$ tel que $L = K(\alpha)$.

Coro 40 : On a $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \Leftrightarrow n \mid m$.

2) Dénombrement dans les corps finis

Prop 41 : $|GL_m(\mathbb{F}_q)| = (q^m - q^{m-1}) \dots (q^m - 1)$

$|\{M \in GL_m(\mathbb{F}_q) / M = \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}\}| = q^{\frac{m(m-1)}{2}}$

App 42 : Tout groupe fini, de cardinal $p^n \alpha$, $p \nmid \alpha$, admet un p-sg de Sylow

Def 43 : On pose pour $n \in \mathbb{N}^*$, $\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \text{ a un facteur carré} \\ (-1)^r & \text{si } n = \prod_{i=1}^{r} p_i, \ p_i \text{ premiers distincts} \end{cases}$

Prop 44 : Si $\forall n \geq 1$ $a_n = \sum_{d \mid n} b_d$, alors $b_n = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) a_d$

App 45 : Le nombre $I(n,q)$ de poly. irr. unitaires sur $\mathbb{F}_q$ de degré n vaut $\frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d \underset{n \to +\infty}{\sim} \frac{q^n}{n}$ DVP 1

IV – Polynômes cyclotomiques

Def 46 : . Si K corps, on note $U_{n,K} = \{x \in D_K(X^n - 1) / x^n = 1\}$

. Si $car(K) \nmid n$, on pose

$$\phi_{n,K} = \prod_{\xi \in \tilde{U}_{n,K}} (X - \xi)$$

, où $\tilde{U}_{n,K}$ est l'ensemble des générateurs de $U_{n,K}$.

Prop 47 : $\phi_{n,K}$ est unitaire, de degré $\varphi(n)$.

Prop 48 : $X^n - 1 = \prod_{d \mid n} \phi_{d,K}$

Prop 49 : $\phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$ et $\phi_{n,\mathbb{F}_p} = \overline{\phi_{n,\mathbb{Q}}}^p$

Prop 50 : $\phi_{n,\mathbb{Q}}$ est irréductible sur $\mathbb{Q}$, et donc sur $\mathbb{Z}$. DVP 2

Corollaire 51 : Si $\xi \in \tilde{U}_{n,\mathbb{Q}}$, $\mathbb{Q}(\xi)$ est une extension de $\mathbb{Q}$ de degré $\varphi(n)$.