Soient A un anneau unitaire intègre commutatif, et L/K une extension de corps commutatif. Soit $P \in A[X]$.

I - Polynômes irréductibles

A - Notion d'irréductibilité pour les polynômes

[Rb] 370 **Def 1** : On dit que P est irréductible sur A si $P \notin A[X]^\times = A^\times$, si $P \neq 0$ et si :
$$\forall (P_1, P_2) \in A[X]^2, \quad P = P_1 P_2 \Rightarrow P_1 \in A^\times \text{ ou } P_2 \in A^\times$$

[Rb] 370 **Ex 2** :
- Tout polynôme de degré 1 est irréductible ;
- Les polynômes réels de degré 2 de discriminant < 0 sont irréductibles

[Rb] 371 **Prop 3** :
- Si $P \in K[X]$ est irréductible et si $\deg(P) > 1$, alors P n'a pas de racine dans K.
- Si $P \in K[X]$ n'a pas de racine dans K et si $\deg(P) \leq 3$, alors P est irréductible sur K.

Ex 4 :
- $(X^2+1)^2$ est réductible sur $\mathbb{R}$ et sans racine dans $\mathbb{R}$.
- Les polynômes irréductibles de petit degré de $\mathbb{F}_2[X]$ sont X, $X+1$, X^2+X+1, X^3+X^2+1, X^3+X+1.

B - Propriétés de $A[X]$

[Rb] 374 **Prop 5** : $A[X]$ euclidien $\Leftrightarrow$ $A[X]$ principal $\Leftrightarrow$ A est un corps.

[Rb] ~375 **Prop 6** : Si $P \in K[X]$ est irréductible, alors $\frac{K[X]}{\langle P \rangle}$ est un corps.

On suppose A factoriel.

[S] 547-548 ou [P] 51 **Def 7** :
- Le contenu de $P \in A[X] \setminus \{0\}$, noté $c(P)$, est un PGCD des coefficients de P.
- On dit que P est primitif si $c(P) \in A^\times$.

Thm 8 : Soit $P \in A[X]$ primitif non constant. [P] 51 [S] 548

P est irréductible dans $A[X]$ $\Leftrightarrow$ A est irréductible dans $K[X]$

Ex 9 : Soient $a_1, \dots, a_n$ des entiers distincts. Le polynôme $(X-a_1)\cdots(X-a_n)-1$ est irréductible sur $\mathbb{Q}$.

Lemme 10 : Un produit de polynômes primitifs est primitif.

$\boxed{\textbf{Lemme 11} \text{ (de Gauss) : } c(PQ) = c(P)c(Q) \qquad \text{DEV 1.a}}$ [S] 548 [P] 51

Thm 12 : $A[X]$ est factoriel $\Leftrightarrow$ A est factoriel [Rb] 358 [S] 548 [P] 51

C - Critères d'irréductibilité

Thm 13 (critère d'Eisenstein) : Écrivons $P = \sum_{k=0}^{n} a_k X^k$, $a_n \neq 0$. [S] 549 [P] 76

S'il existe $p \in A$ premier non nul tel que $\forall k \in [\![1, n-1]\!]$, $p \mid a_k$, $p^2 \nmid a_0$ et $p \nmid a_n$, alors P est irréductible dans $\mathrm{Frac}(A)[X]$.

Ex 14 : $\forall n \geq 2$, $\forall d \in \mathbb{N}^*$ sans facteur carré, $X^n - d$ est irréductible dans $\mathbb{Z}[X]$.

Thm 15 : Soit I un idéal de A. Écrivons $P = \sum_{k=0}^{n} a_k X^k$, $a_n \neq 0$. [P] 77

Si $a_n \not\equiv 0 \bmod I$ et si $P \bmod I$ est irréductible dans $A/I[X]$ alors P est irréductible dans $A[X]$.

Ex 16 : Pour tout p premier, $X^p - X - 1$ est irréductible sur $\mathbb{Q}$. [P] 77

II - Polynômes et extensions de corps

Soient L et K deux corps commutatifs. Soit $P \in K[X]$.

A - Extensions de corps, éléments algébriques

[P] 65 Def 17 : On dit que L est une *extension* de K, et on note L/K, si $L \subseteq K$.

[P] 65 Prop/Def 18 : L est un K-espace vectoriel dont on note $[L:K]$ la dimension, que l'on appelle *degré de l'extension* L/K.

On dit que L/K est *finie* si $[L:K]$ est fini.

[P] 65 Thm 19 (de la base téléscopique) : Si $(e_i)_{i \in I}$ est une K-base de M et si $(f_j)_{j \in J}$ est une M-base de L, alors $(e_i f_j)_{(i,j) \in I \times J}$ est une K-base de L.

[P] 65 Cor 20 (multiplicativité des degrés) : $[L:K] = [L:M] \cdot [M:K]$

[P] 66 Def 21 : On dit que $\alpha \in L$ est *algébrique* sur K s'il existe $P \in K[X]$ tel que $P(\alpha) = 0$. Sinon, on dit que α est *transcendant*.

[P] 66 Thm/Def 22 : Si $\alpha \in L$ est algébrique sur K, alors $\{P \in K[X] \mid P(\alpha) = 0\}$ est un idéal non nul, qui donc admet un unique générateur unitaire $P_{\alpha,K}$, appelé *polynôme minimal de α sur K*.

Notation : $K[\alpha] = \{P(\alpha) : P \in K[X]\}$.

[P] 66 Thm 23 : Soit $\alpha \in L$. Sont équivalentes :

1. α est algébrique sur K
2. $K[\alpha] = K(\alpha)$
3. $K[\alpha]$ est un K-espace vectoriel de dimension finie.

Le cas échéant, $\deg(P_{\alpha,K}) = [K(\alpha) : K]$.

B - Corps de rupture et de décomposition

[P] 70 Def 24 : Supposons P irréductible. On dit que L est un *corps de rupture* de P sur K s'il existe $\alpha \in L$ tel que $P(\alpha) = 0$ et $L = K(\alpha)$.

Thm 25 : Supposons P irréductible. Le corps $\frac{K[X]}{\langle P \rangle}$ est un corps de rupture de P sur K, et c'est le seul à isomorphisme près. [P] 70

Ex 26 : $\mathbb{C}$ peut être défini comme $\frac{\mathbb{R}[X]}{\langle X^2+1 \rangle}$.

Appli 27 : Si P est irréductible et si $\deg(P) \wedge [L:K]$, alors P est irréductible sur L.

Def 28 : On dit que L est un *corps de décomposition* de P sur K si P est scindé sur L et si $L = K(\alpha_1, \dots, \alpha_n)$ avec $\alpha_1, \dots, \alpha_n$ les racines de P. [P] 71

Thm 29 : Il existe un corps de décomposition de P sur K, unique à isomorphisme près. [P] 71

Ex 30 : $\mathbb{Q}(j, \sqrt[3]{2})$ est un corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$. [P] 72

Thm 31 (de l'élément primitif) : Toute extension finie d'un corps de caractéristique nulle est monogène. [P] 87

C - Clôture algébrique

Def 32 : On dit que K est *algébriquement clos* si tout polynôme non nul de $K[X]$ est scindé, et si K n'admet pas d'extension algébrique non triviale. [P] 67

Def 33 : On dit que L est une *clôture algébrique* de K si c'est une extension de K algébrique et algébriquement close. [P] 72

Ex 34 : [P] 68 72
- $\mathbb{C}$ est algébriquement clos (d'Alembert, Gauss)
- $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Ex 35 : Si L est algébriquement clos, alors l'ensemble des éléments de L algébriques sur K est un corps algébriquement clos. [Go] 94

Thm 36 : K admet une unique clôture algébrique à isomorphisme près.

III - Polynômes cyclotomiques

On note $\mathbb{U}_n := \{z \in \mathbb{C} \mid z^n = 1\}$ le groupe des racines complexes n-ièmes de l'unité, et μ_n^* l'ensemble de ses générateurs (que l'on appelle racines primitives n-ièmes de l'unité).

[P] 80 [Rb] 385 **Def 37** : Pour $n \in \mathbb{N}^*$, on définit le n-ième polynôme cyclotomique :

$$\Phi_n = \prod_{\zeta \in \mu_n^*} X - \zeta$$

[P] 80-83 [Rb] ~386 **Prop 38** :
- $\Phi_n = \prod_{\substack{k=1 \\ k \wedge n = 1}}^{n} X - \zeta_n^k$ avec $\zeta_n \in \mu_n^*$.
- $X^n - 1 = \prod_{d \mid n} \Phi_d$
- $\Phi_n \in \mathbb{Z}[X]$

[P] 81 **Ex 39** :
- Pour p premier, $\Phi_p = X^{p-1} + \cdots + X + 1$
- $\Phi_1 = X - 1$, $\Phi_4 = X^2 + 1$, $\Phi_6 = X^2 - X + 1$, $\Phi_8 = X^4 + 1$

[Rb] 392 [P] 82-83 **Thm 40** : Soit $\zeta_n \in \mu_n^*$. Le polynôme minimal de ζ_n sur $\mathbb{Q}$ est Φ_n.

Cor 41 : Φ_n est irréductible sur $\mathbb{Q}$ et $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ DEV 1.b

IV - Polynômes irréductibles des corps finis

[Rb] 331 **Def 42** : La fonction de Moëbius est :

$$\mu : \mathbb{N}^* \longrightarrow \{-1, 0, 1\}$$
$$n \longmapsto \begin{cases} 1 & \text{si } n = 1 \\ (-1)^r & \text{si } n \text{ est le produit de } r \text{ facteurs premiers distincts} \\ 0 & \text{sinon} \end{cases}$$

Thm 43 (formule d'inversion de Moebius) : Soient $(u_n)_{n \in \mathbb{N}^*} \in \mathbb{R}^{\mathbb{N}^*}$ et $(v_n)_{n \in \mathbb{N}^*} \in \mathbb{R}^{\mathbb{N}^*}$. [Rb] 333
Si $\forall n \in \mathbb{N}^*$, $u_n = \sum_{d \mid n} v_d$, alors $\forall n \in \mathbb{N}^*$, $v_n = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) u_d$.

Thm 44 : $P_n := X^{p^n} - X = \prod_{d \mid n} \prod_{P \in \mathcal{U}_d(p)} P$ où $\mathcal{U}_d(p)$ est l'ensemble des polynômes irréductibles unitaires de degré d de $\mathbb{F}_p[X]$. [Rb] 423

Cor 45 : $\# \mathcal{U}_n(p) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d$ DEV 2 [Rb] 424

Références

[P] Perrin

[Rb] Rombaldi

[S] Szpirglas

[Go] Gourdon