Leçon 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Soit $\mathbb{K}$ un corps commutatif et soit $P \in \mathbb{K}[X]$.

1 Polynômes irréductible

1.1 Notion d'irréductibilité

Définition 1 (ROM 370, BER 609)**.** Un polynôme $P \in \mathbb{K}[X] \setminus \{0\}$ est dit irréductible s'il est non constant et n'est divisible que par les constantes non nulles ou les polynômes λP avec $\lambda \in \mathbb{K}^*$.

Exemple 2 (ROM 370)**.** $X^2 - 2$ est réductible dans $\mathbb{R}[X]$ avec $-\sqrt{2}$, $\sqrt{2}$ comme racines simples, mais pas dans $\mathbb{Q}[X]$.

Exemple 3 (ROM 370)**.** Tout polynôme de degré 1 est irréductible.

Proposition 4 (BER 612)**.** Si K est un corps et si $P \in K[X]$ est de degré 2 ou 3, alors P est irréductible si et seulement si P n'a pas de racines dans K.

Exemple 5 (ROM 370)**.** Les polynômes réels de degré 2 de discriminant strictement négatifs sont irréductibles.

Théorème 6 (ROM 371)**.** [Euclide] Supposons P irréductible. Si P est un produit $\prod_{k=1}^{r} A_k$ de $r \geq 2$ polynôme non nuls, il divise alors l'un des A_k.

Théorème 7 (ROM 371)**.** Tout polynôme non constant $P \in \mathbb{K}[X]$ est produit de polynômes irréductibles et cette décomposition est unique à l'ordre près des facteurs.

Corollaire 8 (ROM 372, A VOIR)**.** Tout polynôme non constant $P \in \mathbb{K}[X]$ admet au moins un diviseur irréductible.

Corollaire 9 (ROM 372, A VOIR)**.** L'ensemble des polynôme unitaire irréductible de $\mathbb{K}[X]$ est infini

Théorème 10 (ROM 375 + 371)**.** Supposons P unitaire de degré $n \geq 1$. L'algèbre $\mathbb{K}[X]/(P)$ est de dimension n et $(\overline{X^k})_{0 \leq k \leq n-1}$ en est une base.

Théorème 11 (ROM 375 + 371)**.** Supposons P unitaire de degré $n \geq 1$. LASSE :

1. P est irréductible
2. (P) est maximal
3. $\mathbb{K}[X]/(P)$ est un corps
4. $\mathbb{K}[X]/(P)$ est un intègre

Exemple 12 (ROM376)**.** $\mathbb{R}[X]/(X^2+1)$ est un corps. On remarque en notant i la classe de X modulo X^2+1 que $i^2 = -1$. Le corps $\mathbb{R}[X]/(X^2+1)$ est en faite isomorphe à $\mathbb{C}$.

1.2 Critère d'irréductibilité

Théorème 13 (TL1 275ROM 381)**.** [d'Alembert-Gauss] Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine.

Corollaire 14 (No ref)**.** Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Théorème 15 (ROM 381)**.** Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 de discriminant négatif.

Exemple 16 (No ref)**.** $P = X^2+1$ est irréductible sur $\mathbb{R}[X]$ car il n'a pas de racines réelles ; cependant on peut le scinder sur $\mathbb{C}$ par $P = (X-i)(X+i)$.

Définition 17 (ROM 382, mettre K pour suite)**.** Le contenu d'un polynôme $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X] \setminus \{0\}$ est l'entier $c(P) = pgcd(a_0, .., a_n)$.
Si $c(P) = 1$, on dit que P est primitif

Lemme 18 (GOU 62)**.** Soient $P, Q \in \mathbb{Z}[X]$ et p un nombre premier. Si p divise tous les coefficients de PQ, alors p divise tous les coefficients de P ou tous ceux de Q.

Proposition 19 (GOU 62)**.** Si $P, Q \in \mathbb{Z}[X]$ alors $c(PQ) = c(P)c(Q)$.

Proposition 20 (GOU 62)**.** Si $\phi \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$, alors il est irréductible dans $\mathbb{Q}[X]$.

Théorème 21 (GOU 62)**.** [critère d'Eisenstein] Soit $P = a_nX^n + .. + a_1X + a_n \in \mathbb{Z}[X]$ et p un nombre premier. Si on a :

1. p ne divise pas a_n
2. p divide a_i, pour tout $1 \leq i \leq n-1$
3. p^2 ne divise pas a_0

Alors P est irréductible dans $\mathbb{Q}[X]$. PER 76 ; s'étend à un anneau unitaire commutatif intègre et son corps des fractions associé

Exemple 22 (BER 780, pour après)**.** Le polynôme $X^4 - 3 \in \mathbb{Z}[X]$ vérifie les conditions du critère d'Eisenstein avec $p = 3$. Ainsi il est irréductible dans $\mathbb{Q}[X]$.

Théorème 23 (PER 77)**.** [critère de réduction] Soit A un anneau factoriel et $\mathbb{K} = Fr(A)$. Soit I un idéal premier de A et $B = A/I$ qui est un anneau intègre de corps de fractions $\mathbb{L}$. Soit $P(X) = a_nX. + ... + a_0$ un polynôme de $A[X]$ et $\overline{P}$ sa réduction modulo I.
On suppose $\overline{a_n} \neq 0$ dans B. Alors, si $\overline{P}$ est irréductible sur B ou $\mathbb{L}$, le polynôme P est irréductible sur $\mathbb{K}$.

Exemple 24 (PER 77, REvoir partie admise)**.** Soit p un nombre premier. En admettant que $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$, on trouve grâce au théorème précédent, que $X^p - X - 1$ est irréductible qur $\mathbb{Q}$.

2 Extensions de corps et nombre algébrique

2.1 Notion d'extension de corps

Définition 25 (BER 767)**.** Une extension de $\mathbb{K}$ est un corps $\mathbb{L}$ contenant $\mathbb{K}$ comme sous-corps. On le note $\mathbb{L}/\mathbb{K}$.

Exemple 26 (No ref)**.** $\mathbb{C}$ est une extension de corps de $\mathbb{R}$

Définition 27 (BER 767)**.** On appelle degré de $\mathbb{L}/\mathbb{K}$ la dimension de $\mathbb{L}$ comme $\mathbb{K}$-espace vectoriel. On le note $[\mathbb{L} : \mathbb{K}]$.

Définition 28 (BER 768)**.** Une sous-extension de $\mathbb{L}/\mathbb{K}$ est une extension $\mathbb{L}'/\mathbb{K}$ tel que $\mathbb{L}'$ soit un sous-coprs de $\mathbb{L}$.

Théorème 29 (BER 769)**.** [base télescopique] Soient $\mathbb{M}/\mathbb{K}$ et $\mathbb{L}/\mathbb{M}$ des extension de corps. Alors $\mathbb{L}/\mathbb{K}$ est de degré fini si et seulement si $\mathbb{L}/\mathbb{M}$ et $\mathbb{M}/\mathbb{K}$ le sont.

Dans ce cas, $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{M}][\mathbb{M} : \mathbb{K}]$.

2.2 Nombre algébrique et transcendant

On considère désormais $\mathbb{L}/\mathbb{K}$ une extension de corps et $\alpha \in \mathbb{L}$

Définition 30 (BER 778)**.** On dit que α est algébrique sur $\mathbb{K}$ s'il existe un polynôme $P \in \mathbb{K}[X]$ non nul tel que $P(\alpha) = 0$.

On dit que α est transcendant sinon .

Exemple 31 (BER 778)**.** [admis] e et π sont des nombres transcendant sur $\mathbb{Q}$.

$i \in \mathbb{C}$ est algébrique sur $\mathbb{Q}$ puisqu'il est racine du polynôme $X^2 + 1$.

Proposition 32 (BER 778)**.** Si $\mathbb{L}/\mathbb{K}$ est une extension de degré fini, alors tout élément $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$.

Proposition 33 (BER 779)**.** L'ensemble $I_\alpha = \{P \in \mathbb{K}[X] | P(\alpha) = 0\}$ est un idéal de $\mathbb{K}[X]$. Il est non nul si et seulement si α est algébrique sur $\mathbb{K}$.
Dans ce cas, il existe un unique polynôme unitaire irréductible $\mu_{\alpha,\mathbb{K}}$ de $\mathbb{K}[X]$ tel que $\mu_{\alpha,\mathbb{K}}(\alpha) = 0$. Ce polynôme est l'unique générateur unitaire de I_α.

Définition 34 (BER 779)**.** Le polynôme $\mu_{\alpha,\mathbb{K}}$ du théorème précédent est appelé le polynôme minimal de α sur $\mathbb{K}$.

Exemple 35 (BER 780)**.**
1. Soit $\mathbb{K} = \mathbb{R}$ et $\alpha = i$. $X^2 + 1 \in \mathbb{R}[X]$ annule i et est unitaire et irréductible. Ainsi $\mu_{i,\mathbb{R}} = X^2 + 1$
2. Soit $\mathbb{K} = \mathbb{Q}$ et $\alpha = \sqrt[4]{3}$. $X^4 - 3 \in \mathbb{Q}[X]$ annule α. Il est unitaire et irréductible (cf exemple 22). Ainsi $\mu_{\alpha,\mathbb{Q}} = X^4 - 3$.

Définition 36 (BER 770)**.** Soit I une partie de $\mathbb{L}$. On note $\mathbb{K}(I)$ l'intersection des sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et I. C'est donc la plus petite sous-extension de $\mathbb{L}/\mathbb{K}$ contenant I.
L'extension $\mathbb{K}(I)/\mathbb{K}$ s'appelle la sous-extension de $\mathbb{L}/\mathbb{K}$ engendré par I.

Notation 37 (BER 770)**.** Si $I = \{s_1, .., s_n\}$, on note $\mathbb{K}(s_1, ..., s_r)/\mathbb{K}$

Théorème 38 (BER 780)**.** α est algébrique sur $\mathbb{K} \iff [\mathbb{K}(\alpha):\mathbb{K}] < +\infty$. Dans ce cas, $(1, \alpha, ..., \alpha^{d-1})$ est une $\mathbb{K}-$base de $\mathbb{K}(\alpha)$, où $d = deg(\mu_{\alpha,\mathbb{K}})$. En particulier $\mathbb{K}(\alpha) = \mathbb{K}[\alpha]$ et $[K(\alpha):\mathbb{K}] = d$.

Exemple 39. En reprenant les résultats de l'exemple 35 on a $[\mathbb{R}(i):\mathbb{R}] = 2$ et $[\mathbb{Q}(\sqrt[4]{3}):\mathbb{Q}] = 4$.

3 Extensions remarquables

3.1 Corps de rupture

Définition 40 (PER 70, ROM 418, BER 816)**.** On dit qu'une extension $\mathbb{L}$ de $\mathbb{K}$ est un corps de rupture d'un polynôme non constant $P \in \mathbb{K}[X]$ si le polynôme P a une racine ω dans $\mathbb{L}$ telle que $\mathbb{L} = \mathbb{K}(\omega)$.

Théorème 41 (PER 70)**.** Soit $P \in \mathbb{K}[X]$ irréductible. Il existe un corps de rupture de P sur K, unique à isomorphisme près.

Exemple 42 (BER 818)**.** Prenons $P = X(X^2+1) \in \mathbb{Q}[X]$. $\mathbb{Q}/\mathbb{Q}$ et $\mathbb{Q}(i)/\mathbb{Q}$ sont deux corps de rupture de P. Ceci montre qu'il n'y a pas unicité. De plus ces extension ne sont pas isomorphe car elles n'ont pas le même degré A voir la derniere rem!!!

Exemple 43 (BER 818, PER 71)**.** Considérons $P = X^3 - 2 \in \mathbb{Q}[X]$. Un corps de rupture de P est par exemple $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Notons que ce corps n'admet pas d'éléments complexes alors que P admet 2 autres racines complexes. On constate donc qu'un polynôme n'a pas forcément toutes ses racines dans un même coprs de rupture. Ceci emmène à la définition suivante.

3.2 Corps de décomposition

Définition 44 (BER 819, 71)**.** Soit $P \in \mathbb{K}[X]$ non constant. Un corps de décomposition de P est une extension $\mathbb{L}/\mathbb{K}$ vérifiant :

1. P se décompose en facteurs de degré 1 dans $\mathbb{L}[X]$
2. $\mathbb{L} = \mathbb{K}(\alpha_1, .., \alpha_n)$, où $\alpha_1, ..., \alpha_n \in \mathbb{L}$ sont les recines de P dans $\mathbb{L}$.

Théorème 45 (PER 71)**.** Pour tout $P \in \mathbb{K}[X]$, il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près. On le note $D_{\mathbb{K}}(P)$.

Application 46. Dans BER application à F_q, à voir soit là soit parite app

Exemple 47 (PER 72)**.** Si on reprend le polynôme $P = X^3 - 2$, on a $D_{\mathbb{Q}}(P)$.

3.3 Clotûre algébrique

Définition 48 (ROM 364)**.** On dit que $\mathbb{K}$ est algébriquement clos si tout polynôme $P \in \mathbb{K}[X]$ est scindé sur $\mathbb{K}$.

Définition 49 (PER 72, BER 823)**.** On dit que $\mathbb{L}$ est une clôture algébrique de $\mathbb{K}$ si $\mathbb{L}/\mathbb{K}$ est une extension algébrique et $\mathbb{L}$ est algébriquement clos.

Exemple 50 (BER 823)**.** $\mathbb{C}$ est le clôture algébrique de $\mathbb{R}$, d'après le théorème de D'Alembert Gauss.

Application 51 (ROM 676, TL2 313)**.** Si $\mathbb{K}$ est algébriquement clos, tout endomorphisme de $\mathcal{L}(E)$ est trigonalisable.

4 Applications

4.1 Polynômes cyclotomiques

Définition 52 (TL1 260, ou PER 80)**.** Une racine primitive $n$ème de l'unité est un générateur de $\mathbb{U}_n$

Notation 53. On note $\mathbb{U}_n^*$ l'ensemble des racines primitives $n-$ème de l'unité.

Exemple 54 (No ref)**.** $-1 \in \mathbb{U}_4$ mais ce n'est pas une racine primitive 4ème car $< -1 >= \{1, -1\}$. C'est cependant une racine 2ème de l'unité

Proposition 55 (TL1 260, un peu)**.** Les générateur de $\mathbb{U}_n$ sont les $e^{i2k\pi/n}$ où $k \in [\![1, n-1]\!]$ et $k \wedge n = 1$. Ainsi, $|\mathbb{U}_n^*| = \varphi(n)$, où φ est l'indicatrice d'Euler

Définition 56 (TL1 309)**.** Le $n-$ème polynôme cyclotomique est le polynôme unitaire ϕ_n dont les racines sont les racines primitives $n-$ème de l'unité : $\phi_n(X) = \prod_{\xi \in \mathbb{U}_n^*} (X - \xi)$

Proposition 57 (TL1 309, PER 80)**.** $deg(\phi_n) = \varphi(n)$

Exemple 58 (TL1 309)**.**

1. $\phi_1(X) = X - 1$
2. Si p est premier, $\varphi_p(X) = \frac{X^p-1}{X-1} = X^{p-1} + ... + X + 1$
3. $\phi_4(X) = X^2 + 1$

Proposition 59 (TL1 309)**.** Soit $n \geq 1$. Alors : $X^n - 1 = \prod_{d|n} \phi_d$

Théorème 60 (PER 82, DEV 1)**.** Pour $n \geq 1$, $\varphi_n(X) \in \mathbb{Z}[X]$ est un polynôme irréductible et unitaire, donc irréductible dans $\mathbb{Q}[X]$ également.

4.2 Construction des corps finis

Soit $p \leq 2$ un nombre premier et $n \in \mathbb{N}^*$. On pose $q = p^n$.

Proposition 61 (BER 651)**.** Soit $P \in \mathbb{F}_p$ un polynôme irréductible de degré $n \geq 1$. Alors $\mathbb{F}_p[X]/(P)$ est un corps. De plus, c'est aussi un $\mathbb{F}_p-$espace vectoriel de base $(\overline{1}, \overline{X}, ..., \overline{X}^{n-1})$. En particulier, il a p^n éléments.

Méthode 62 (BER 651)**.** Si l'on dispose d'un polynôme irréductible $P \in \mathbb{F}_p$ de degré $n \geq 1$, on peut donc construire un corps à p^n éléments facilement.

question qui vient : étant donné un nombre premier p, existe t-il des polynômes irréductibles à coefficients dans $\mathbb{F}_p$ de tout degré ?

Notation 63 (ROM 422)**.** Dans la suite, on considère P_n le polynôme $X^{p^n} - X$ où $n \in \mathbb{N}$ et $p \geq 2$ est un nombre premier.
On note également $U_n(p)$ l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_p[X]$ de degré n ; et $I_n(p)$ le cardinal de cet ensemble.

Lemme 64 (ROM 422, DEV2)**.** 1. Soit $P \in \mathbb{F}_p[X]$. $P|P_n \implies deg(P)|n$

2. Soit $d|n$. Tout $P \in U_d(p)$ divise P_n.

Proposition 65 (ROM 422,DEV2)**.** $\forall n \in \mathbb{N}^*$, $nI_n(p) = \sum\limits_{d|n} \mu(\frac{n}{d})p^d$ où μ est la fonction de Möbius

2 suivants à voir si time / compris

Corollaire 66 (BER 656)**.** Il existe un polynôme irréductible unitaire de degré n dans $\mathbb{F}_p[X]$.

Théorème 67 (BER 656, A voir)**.** Soit $q = p^n$, où p est un nombre premier et $n \geq 1$. Alors il existe un corps fini à q éléments, unique à isomorphisme près. De plus, tout morphisme entre deux corps finis à q éléments est un isomorphisme de $\mathbb{F}_q-$algèbres.