Concours Agrégation, Mathématiques générales

Leçon 41- Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Commentaires du jury 2015 : Le jury attend dans cette leçon un bagage théorique permettant de définir corps de rupture, corps de décomposition (la preuve de l'unicité de ce dernier n'est pas exigée), ainsi que des illustrations dans différents types de corps (réel, rationnel, corps finis). Attention à ne pas croire qu'un polynôme réductible admet forcément des racines (même en dehors du cadre de cette leçon !). Bien entendu, les corps finis ont une place de choix et il sera instructif de chercher des polynômes irréductibles de degré 2, 3, 4 sur $\mathbb{F}_2$. Il faut savoir qu'il existe des corps algébriquement clos de caractéristique nulle autres que $\mathbb{C}$. Il est bon de savoir montrer que l'ensemble des nombres algébriques sur le corps $\mathbb{Q}$ des rationnels est un corps algébriquement clos. Il faut connaître le théorème de la base téléscopique ainsi que les utilisations artithmétiques (utilisation de la divisibilité) que l'on peut en faire dans l'étude de l'irréductibilité des polynômes.
Commentaires du jury 2016 : La présentation du bagage théorique permettant de définir corps de rupture, corps de décomposition, ainsi que des illustrations dans différents types de corps (réel, rationnel, corps finis) sont inévitables. Les corps finis peuvent être illustrés par des exemples de polynômes irréductibles de degré 2, 3, 4 sur $\mathbb{F}_2$ ou $\mathbb{F}_3$. Il est nécessaire de présenter des critères d'irréductibilité de polynômes et des polynômes minimaux de quelques nombres algébriques. Il faut savoir qu'il existe des corps algébriquement clos de caractéristique nulle autres que $\mathbb{C}$; il est bon de savoir montrer que l'ensemble des nombres algébriques sur le corps $\mathbb{Q}$ des rationnels est un corps algébriquement clos. Le théorème de la base téléscopique, ainsi que les utilisations arithmétiques (utilisation de la divisibilité) que l'on peut en faire dans l'étude de l'irréductibilité des polynômes, est incontournable.

Bibliographie

[F. M. 1] Fresnel J., Matignon M. *Algèbre et Géométrie* (Hermann 2011)
[F. M. 1'] Errata, https ://www.math.u-bordeaux.fr/∼mmatigno/Errata-Alg-Géom.pdf
[F. M. 2] Fresnel J., Matignon M. *Algèbre et Géométrie-81 thèmes pour l'agrégation* (ellipses 2017)
[F. M. 2'] Compléments et errata, https ://www.math.u-bordeaux.fr/∼mmatigno/Errata-FM2.pdf
[Fr. F.] Fresnel J. *Anneaux* (Hermann 2001)
et
[Sa.] Samuel P. *Théorie algébrique des nombres* (Hermann 1997)

Développements conseillés :

(1) Irréductibilité du polynôme cyclotomique, [Fr. F] p. 280 et exercice ci-dessous.
(2) L'anneau A est factoriel ssi $A[X]$ est factoriel, [Fr. F] Th. 7.3.1. p 262.
(3) Il n'existe pas d'anneau unitaire avec 5 unités, [F. M. 1] $n°107$ p. 296 question 4 p. 297 et exercice ci-dessous.
(4) Sous-corps de $K(X)$ et K-automorphismes de $K(X)$, [F. M. 2] p. 260. Voir en complément une application au corps des invariants de $\mathbb{C}$ par les automorphismes de $\mathbb{C}$, [Fr. F] ex. 9.4.1. p 319.

Exercice 1 Critère d'Eisenstein et irréductibilité des polynômes cyclotomiques Φ_{p^n}.

(1) *Le critère d'irréductibilité d'Eisenstein.*

Si ℓ est un nombre premier et $x \in \mathbb{Q}-\{0\}$, on note $v_\ell(x)$ la valuation ℓ-adique de x (i.e. $x = \pm\ell^{v_\ell(x)}\frac{n}{d}$ où $(n,d) \in \mathbb{N}\times\mathbb{N}^\star$ sont premiers à ℓ).

Soit $A(X) := a_nX^n + ... + a_0 \in \mathbb{Q}[X]$. On suppose qu'il existe p premier tel que $v_p(a_n) = 0$, $v_p(a_0) = 1$ et pour $i < n$, $v_p(a_i) \geq 1$. On suppose que $A(X) = B(X)C(X)$ avec $B, C \in \mathbb{Q}[X]$. On note P les premiers dans $\mathbb{N}$ et si $T(X) = \sum_i t_iX^i \in \mathbb{Q}[X] - \{0\}$ on note $Cont(T) := \prod_{\ell\in P}\ell^{\inf_i v_p(t_i)}$ le contenu de T.

(a) Soit $A' := \frac{A}{Cont(A)} = \sum_{0\leq i\leq n} a'_i X^i$. Montrer que $A' \in \mathbb{Z}[X]$ et que $v_p(a'_n) = 0$, $v_p(a'_0) = 1$ et pour $i < n$, $v_p(a'_i) \geq 1$. Soit $B' := \frac{B}{Cont(B)}$, $C' := \frac{C}{Cont(C)}$.

Preuve. Le contenu de A' vaut 1. Ainsi pour tout $\ell \in P$, on a $v_\ell(a'_i) \geq 0$; ainsi $a'_i \in \mathbb{Z}$. Enfin puisque $v_p(a_n) = 0$ et $v_p(a_i) \geq 0$, il suit que $v_p(ContA) = 0$; ainsi $v_p(a'_i) = v_p(a_i)$ pour $0 \leq i \leq n$.///

(b) Montrer qu'il existe un unique homomorphisme d'anneaux $\pi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ qui induit la réduction modulo p sur $\mathbb{Z}$ et tel que $\pi(X) = X$. Montrer que $\deg \pi(T(X)) \leq \deg(T(X))$.

Preuve. C'est la propriété universelle des anneaux de polynômes. L'inégalité sur les degrés est immédiate.///

(c) Montrer que $\pi(A') = \pi(a'_n)X^n$ et en déduire que $\pi(B') = \pi(b'_t)X^t$, $\pi(C') = \pi(c'_s)X^s$ où t resp. s est le degré de B' resp. C'.

Preuve. Puisque $ContA = ContBContC$ par le lemme de Gauss, il suit que $A' = B'C'$ et donc $\pi(A') = \pi(a'_n)X^n = \pi(B')\pi(C')$. Puisque X est irréductible dans $\mathbb{F}_p[X]$, ils suit que $\pi(B') = \beta X^{t'}$, $\pi(C') = \gamma X^{s'}$ avec $t' + s' = n$. Or $t + s = n$ et puisque $t' \leq t$, $s' \leq s$ on a $t' = t$, $s' = s$.///

(d) En déduire que A est irréductible dans $\mathbb{Q}[X]$.

Preuve. L'évaluation en $X = 0$ de l'égalité $A' = B'C'$ donne $a_0 = B'(0)C'(0)$. Si $s > 0$, $t > 0$ il suit de la question précédente que $p|B'(0)$ et $p|C'(0)$; ainsi $p^2|a_0$ ce qui est une contradiction.///

(2) *L'irréductibilité de $\Phi_p(X)$, le p-ième polynôme cyclotomique.*

(a) Montrer que $\Phi_p(X) \in \mathbb{Z}[X]$

Preuve. On a $X^p - 1 = \Phi_1(X)\Phi_p(X)$; ainsi $\Phi_p(X) = \frac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + ... + 1 \in Z[X]$.///

(b) Montrer que $\Phi_p(1) = p$ et que $\Phi_p(X + 1) = X^{p-1} \mod p\mathbb{Z}[X]$.

Preuve. L'égalité $\Phi_p(1) = p$ suit de la formule précédente. Enfin $\Phi_p(X+1) = \frac{(X+1)^p-1}{X}$ et puisque $\binom{p,i}{=}0 \mod p$ pour $0 < i < p$ il suit que $(X + 1)^p = 1 + X^p + pXR(X) \in \mathbb{Z}[X]$ où $R \in \mathbb{Z}[X]$.///

(c) En déduire que $\Phi_p(X)$ est irréductible dans $\mathbb{Z}[X]$.

Preuve. Le critère d'Eisenstein montre l'irréductibilité dans $\mathbb{Q}[X]$ et puisque le contenu vaut 1 il est de plus irréductible dans $\mathbb{Z}[X]$.///

(3) *L'irréductibilité de $\Phi_{p^r}(X)$ pour $r > 1$.*

(a) Montrer que $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$.

Preuve. On remarque que $X^{p^r} - 1 = \Phi_{p^r}\Phi_{p^{r-1}}...\Phi_p\Phi_1 = \Phi_{p^r}(X^{p^{r-1}} - 1)$. Ainsi $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$.///

(b) Montrer que $\Phi_{p^r}(X + 1) = X^{p^{r-1}(p-1)} \mod p\mathbb{Z}[X]$.

Preuve. Ainsi $\Phi_{p^r}(X+1) = \Phi_p((X+1)^{p^{r-1}}) = \Phi_p((X)^{p^{r-1}}+1) \mod p = X^{p^{r-1}(p-1)} \mod p\mathbb{Z}[X]$ par 2.b).///

(c) En déduire que $\Phi_{p^r}(X)$ est irréductible dans $\mathbb{Z}[X]$.

Preuve. Le critère d'Eisenstein montre l'irréductibilité dans $\mathbb{Q}[X]$ et puisque le contenu vaut 1 il est de plus irréductible dans $\mathbb{Z}[X]$.///

Exercice 2 Montrer que la somme des racines primitives n-ièmes de l'unité vaut $\mu(n)$ la fonction de Moebius en n. On pourra utiliser l'identité $X^n - 1 = \prod_{d|n} \Phi_d(X)$ et l'identité $\sum_{d|n} \mu(d) = 0$, [F. M. 2] théorème partie 2. p. 249.

On trouvera un complément dans [F. M. 2'] à la page 249.

Exercice 3 Polynômes irréductibles dans $\mathbb{Z}[X]$ et irréductibilité modulo p, [Fr. F] p. 281.

Exercice 4 Le lemme de Gauss dans $\mathbb{Z}[X]$, [F. M. 1] $n°88$ p. 250.

Exercice 5 Le polynôme $f(X) := \frac{(X+1)^{2p}-(X^{2p}+1)}{X}$ avec p premier > 2 est irréductible dans $\mathbb{Z}[X]$, [F. M. 2] p. 195.

Exercice 6 Un théorème de Kronecker et une application aux matrices $\in \mathrm{GL}_n(\mathbb{Z})$: les polynômes unitaires de $\mathbb{Z}[X]$ dont les racines complexes vérifient $0 < |z| \leq 1$ sont les produits de polynômes cyclotomiques, [Fr. F] p. 201.

Soit $P(X) \in \mathbb{Z}[X]$ un polynôme unitaire à coefficients entiers, de degré $n \geq 1$. On suppose que les racines complexes de $P(X)$ sont de module ≤ 1.

(1) Notons $s_1, ..., s_n \in \mathbb{Z}[X_1, ..., X_n]$ les polynémes symétriques élémentaires. Soit $r \geq 1$, on note $\rho : \mathbb{Z}[X_1, ..., X_n] \to \mathbb{Z}[X_1, ..., X_n]$ l'unique homomorphisme tel que $\rho(a) = a$ pour $a \in \mathbb{Z}$ et $\rho(X_i) = X_i^r$ pour tout $1 \leq i \leq n$ (c'est la propriété universelle des anneaux de polynômes). Montrer en utilisant ρ que $\forall \sigma \in S_n$ on a $s_k(X^r_{\sigma(1)}, ..., X^r_{\sigma(n)}) = s_k(X_1^r, ..., X_n^r)$, en déduire que pour tout $k \leq n$, il existe $P_{r,k}(S_1, ..., S_n) \in \mathbb{Z}[S_1, ..., S_n]$ tel que $s_k(X_1^r, ..., X_n^r) = P_{r,k}(s_1, ..., s_n)$.

(2) Calculer $s_k(1, ..., 1)$.

(3) Notons $\theta_1, ..., \theta_n$ les racines complexes (éventuellement répétées) de $F(X)$. Montrer que pour tout $r \geq 1$ et tout $k \leq n$, on a

$$s_k(\theta_1^r, ..., \theta_n^r) \in \mathbb{Z}, \quad |s_k(\theta_1^r, ..., \theta_n^r)| \leq \binom{n}{k}.$$

(4) Montrer que l'ensemble $\{\theta_i^r \mid 1 \leq i \leq n, r \geq 1\}$ est fini.

(5) En déduire que pour toute racine θ de $P(X)$, il existe $r \geq 2$ tel que $\theta^r = \theta$. Conclure.

(6) En déduire la décomposition en irréductible de P dans $\mathbb{Z}[X]$.

(7) Une application du théorème de Kronecker.

Soit $M \in \mathrm{GL}_n(\mathbb{Z})$, on suppose que la suite $M^k, k \in \mathbb{N}$ est bornée. Montrer que M est d'ordre fini.

Preuve. Si $\lambda \in \mathbb{C}$ est racine de χ_M alors la suite λ^k est bornée ainsi $|\lambda| \leq 1$. Le théorème de Kronecker, [Fr. F] exercice 4.4.2 p. 201, appliqué au polynôme χ_M implique que les racines de χ_M sont des racines de l'unité ; ainsi il existe $m > 0$ avec $\chi_{M^m} = (X-1)^n$ alors $M^m = Id + N$ où N est nilpotente. Montrons que $N = 0$. Pour cela nous allons montrer que si $m_N(X) = X^d$ avec $d \geq 2$ alors la suite M^{mk} est non bornée pour $k \to \infty$. La somme $\mathbb{C}N^0 + \mathbb{C}N + ... + \mathbb{C}N^{d-1} \subset M_n(\mathbb{C})$ est directe ainsi par l'équivalence des normes en dimension finie il existe $c > 0$ avec $\| \sum_{0 \leq i \leq d-1} a_i N^i \| \geq c \max_{0 \leq i \leq d-1} |a_i|$. Puisque $M^{mk} = (Id+N)^k = Id + \binom{k}{1} N + ... + \binom{k}{d-1} N^{d-1}$ et que $d \geq 2$, le résultat suit. ///

A propos des ordres des éléments de $\mathrm{GL}_n(\mathbb{Z})$ voir [F. M. 1] $n°26$ p. 46.

Exercice 7 Autour de Berlekamp [F. M. 1] $n°108$ p. 299 partie A. Appliquer l'algorithme au polynôme $X^p - X - 1 \in \mathbb{F}_p[X]$

Exercice 8 Les racines d'un polynôme irréductible, [F. M. 2] lemme 1 p. 57.

Soit $P \in \mathbb{F}_p[X]$ un polynôme irréductible. Soit $z \in \Omega$ une racine de P dans une clôture algébrique Ω. Soit φ le $\mathbb{F}_p$-automorphisme de Ω défini par $\varphi(x) = x^p$. Montrer que les racines de P sont simples et coincident avec l'orbite de z sous $< \varphi >$.

Exercice 9 Comptage des polynômes irréductibles $\in \mathbb{F}_p[X]$ de degré n, [F. M. 2] 3.2) p. 82.

Soit L un corps fini à $q = p^n$ éléments.

(1) Soit $P \in \mathbb{F}_p[X]$ unitaire, irréductible de degré d. On suppose que $P|(X^q - X)$. Montrer que $d|n$.

Preuve. Puisque L est l'ensemble des racines dans L de $X^q - X$, il suit que P est un produit de polynômes de degré 1 à coefficients dans L, ainsi il existe $x \in L$ avec $P(x) = 0$. On a $\mathbb{F}_p[x] \subset L$ et donc par le théorème de la base télescopique $d = \dim_{\mathbb{F}_p} \mathbb{F}_p[x] \mid \dim_{\mathbb{F}_p} L = n$. ///

(2) Soit $P \in \mathbb{F}_p[X]$ unitaire, irréductible de degré $d|n$. Montrer que $P|(X^q - X)$.

Preuve. Soit $K \supset L$ un corps de décomposition de $P \in K[X]$ et $x \in L$ une racine de P, alors $\mathbb{F}_p[x] \simeq \frac{\mathbb{F}_p[X]}{P\mathbb{F}_p[X]}$ est un corps fini de cardinal p^d. Ainsi $x^{p^d} = x$ et donc $P|(X^{p^d} - X)$ dans $\mathbb{F}_p[X]$. Montrons que $(X^{p^d-1} - X)|(X^{p^n-1} - X)$. Il suffit de montrer que $p^d - 1 \mid p^n - 1$ ce qui est bien le cas puisque $d \mid n$. Ainsi $P|(X^{p^d} - X)|(X^{p^n} - X)$. ///

(3) Pour $d|n$, on note I_d le cardinal de l'ensemble des $P \in \mathbb{F}_p[X]$ unitaires, irréductibles de degré d avec $P|(X^q - X)$. Montrer que $p^n = \sum_{d|n} dI_d$.

Preuve. On écrit la décomposition en irréductible de $X^q - X$ dans $\mathbb{F}_p[X]$ et on en déduit une partition des racines de $X^q - X$ par leur polynôme irréductible. ///

(4) En déduire que $nI_n \leq p^n$.

Preuve. Conséquence immédiate de l'égalité précédente. ///

(5) Montrer que $nI_n \geq p^n - \sum_{1 \leq d \leq n-1} p^d$

Preuve. On a $nI_n = p^n - \sum_{d|n,\ d \neq n} dI_d \geq p^n - \sum_{d|n,\ d \neq n} p^d \geq p^n - \sum_{1 \leq d \leq n-1} p^d$. ///

(6) En déduire que $nI_n \geq 2 + (p-2)\frac{p^n-1}{p-1}$.

Preuve. On a donc $nI_n \geq p^n - p\frac{p^{n-1}-1}{p-1} = 2 + (p-2)\frac{p^n-1}{p-1}$. En particulier $I_n \geq 1$. ///

Remarque. Dans [F. M. 1] $n°86$ on trouve la formule $\sum_{d|n} dI(d) = p^n$. Il suit que $I(n) = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d})p^d$, où $\mu(.)$ est la fonction de Möbius. On en déduit facilement que $I(n) > 0$.

Exercice 10 Une application de l'existence de polynômes irréductibles de degré n dans $K[X]$ si $K = \mathbb{Q}$ ou si $K = \mathbb{F}_q$.

Il existe des sous K-espaces vectoriels $M_n(K)$ de dimension n tels que $V - \{0\} \subset \mathrm{GL}_n(K)$, [F. M. 2] p. 81 questions 1. et 3.

Exercice 11 Il n'existe pas d'anneaux A dont le groupe des inversibles $A^\times$ est d'ordre 5, [F. M. 1] $n°107$ p. 296 question 4 p 297.

On suppose que A est un anneau unitaire dont le groupe des inversibles $A^\times$ est d'ordre 5.

(1) Montrer que $1 = -1$ dans A. En déduire que A contient un sous-corps isomorphe à $\mathbb{F}_2$ (on le notera encore $\mathbb{F}_2$).

Preuve. On remarque que $(-1)^2 = 1$, ainsi $-1 \in A^\times$ et son ordre est 1 ou 2. Par le théorème de Lagrange il n'est pas 2 c'est donc que $1 = -1$ dans A. Ainsi $2.1_A = 0$ et donc l'homomorphisme canonique $\mathbb{Z} \to A$ qui envoie $1 \in \mathbb{Z}$ sur 1_A est de noyau $\subset 2\mathbb{Z}$ et puisque cet homomorphisme n'est pas l'homomorphisme nul le noyau est égal à $2\mathbb{Z}$. Il suit du théorème de factorisation que $\mathbb{F}_2$ s'injecte dans A et son image $\{0, 1_A\}$ est un sous-corps de A isomorphe à $\mathbb{F}_2$. ///

(2) Soit B le sous-anneau de A engendré par $A^\times$, montrer que $A^\times = B^\times$.

Preuve. Par construction $B \subset A$ et donc $B^\times \subset A^\times$ et puisque $A^\times \subset B$ on a l'égalité $A^\times = B^\times$. ///

(3) Soit ζ un générateur de $A^\times$, justifier l'existence d'un homomorphisme de $\mathbb{F}_2$-algèbre $\rho : \mathbb{F}_2[X] \to A$ vérifiant $\rho(P(X)) = P(\zeta)$.

Preuve. C'est la propriété universelle des anneaux de polynômes. ///

(4) Montrer que $B = \operatorname{Im}\rho$ et que $\ker\rho = S(X)\mathbb{F}_2[X]$ avec $S(X)$ unitaire divisant $X^5 - 1$.

Preuve. Par construction $\operatorname{Im}\rho = \mathbb{F}_2[\zeta]$ *et c'est le plus petit sous-anneau de* A *contenant* ζ *et donc* $A^\times$ *; c'est donc* B*. Le noyau est un idéal monogène (*$\mathbb{F}_2[X]$ *est un anneau principal) non nul et puisque* $\rho(X^5 - 1) = 0$*, le résultat suit. ///*

(5) Montrer que $\frac{X^5-1}{X-1}$ est irréductible sur $\mathbb{F}_2$. En déduire la liste des diviseurs de $X^5 - 1$ dans $\mathbb{F}_2[X]$.

Preuve. On a $X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1)$*. Le polynôme* $X^4 + X^3 + X^2 + X + 1$ *n'a pas de racine dans* $\mathbb{F}_2$ *et il n'est pas égal à* $(X^2 + X + 1)^2 = X^4 + X^2 + 1$ *et puisque* $X^2 + X + 1$ *est le seul irréductible de degré* 2 *dans* $\mathbb{F}_2[X]$*, il suit que* $X^4 + X^3 + X^2 + X + 1$ *est irréductible dans* $\mathbb{F}_2[X]$*. Ainsi* $\{1, X - 1, X^4 + X^3 + X^2 + X + 1, X^5 - 1$ *sont les diviseurs de* $X^5 - 1$ *dans* $\mathbb{F}_2[X]$*. ///*

(6) En remarquant que $B \simeq \frac{\mathbb{F}_2[X]}{S(X)\mathbb{F}_2[X]}$, conclure à une contradiction.

Preuve. Puisque $S(X) \neq 1$ *il suit que l'anneau* B *est soit isomorphe à* $B_1 := \frac{\mathbb{F}_2[X]}{(X-1)} = \mathbb{F}_2$*, soit isomorphe à* $B_2 := \frac{\mathbb{F}_2[X]}{(X^4+X^3+X^2+X+1)} \simeq \mathbb{F}_{2^4}$ *ou soit isomorphe à* $B_3 := \frac{\mathbb{F}_2[X]}{(X^5-1)} \simeq B_1 \times B_2$ *par le théorème des restes chinois. On a dans tous les cas une contradiction avec* $|B^\times| = 5$*. ///*

Exercice 12 Le théorème de D'Alembert Gauss, [Fr. F] p. 173 et [Sa] (appendice).

Exercice 13 Montrer qu'un polynôme $P \in \mathbb{R}[X]$ vérifie $P(\mathbb{R}) \subset \mathbb{R}^+$ si et seulement si P est somme de deux carrés dans $\mathbb{R}[X]$.

Exercice 14 Cet exercice pourrait être un développement pour la leçon 25 Extensions de corps. Exemples et applications. Soit K un corps infini et L une extension finie sur K.

Les propriétés suivantes sont équivalentes :

i) $L = K(a)$

ii) L'ensemble des sous-corps de L contenant K est fini, [F. M. 1] $n°103$ p. 280.

Exercice 15 Degré du corps de décomposition, [F. M. 1] $n°102$ p. 277.