Concours Agrégation, Mathématiques générales

Leçon 25- Extensions de corps. Exemples et applications.

Commentaires du jury 2015 :
Très peu de candidats ont choisi cette leçon. On doit y voir le théorème de la base télescopique et ses applications à l'irréductibilité de certains polynômes, ainsi que les corps finis. Une version dégradée de la théorie de Galois (qui n'est pas au programme) est très naturelle dans cette leçon.
Commentaires du jury 2016 : Le théorème de la base téléscopique et ses applications à l'irréductibilité de certains polynômes, que les corps finis sont incontournables. De même il faut savoir calculer le polynôme minimal élément algébrique dans des cas simples, notamment pour quelques racines de l'unité. La leçon être illustrée par des exemples d'extensions quadratiques et leurs applications en arithmétique, que par des extensions cyclotomiques. S'ils le désirent, les candidats peuvent s'aventurer en théorie de Galois.

Remarque : On doit savoir justifier que la somme de 2 éléments algébriques sur K est encore algébrique et exhiber un polynôme annulateur à l'aide de polynômes annulateurs des éléments (on peut utiliser le résultant, [Fr. F] exercice 7.9.27 p. 289 pour la somme et le produit de 2 entiers algébriques).

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. A.] Fresnel J. *Algèbre des matrices* (Hermann 2011)
[Fr. F.] Fresnel J. *Anneaux* (Hermann 2001)
et
[Du.] Duverney D. *Théorie des nombres* (Dunod 2007)
[La.] Lang S. *Algebra*

Développements conseillés :

(1) Groupe des automorphismes de l'extension $\mathbb{Q}(e^{\frac{2i\pi}{n}})/\mathbb{Q}$, et construction à la règle et au compas du polygone régulier à n côtés, [F. M. 1] $n°104$ et [F. M. 1'] p.282.
(2) Corps intermédiaires: 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
(*) Notez que si $K = \mathbb{F}_q$ alors $L = \mathbb{F}_{q^m}$, puisque que $L^\star$ est un groupe cyclique i) est trivialement satisfait pour a un générateur de $L^\star$. De plus comme L est fini ii) est aussi trivialement satisfait.
Et si c'est trop court on peut compléter avec "le théorème de l'élément primitif", [Fr. F] p. 266.
(3) Constructions à la règle et au compas ; le théorème de Wantzel et applications, [F. M. 1] $n°104$ p. 281.
(4) Si u_n est une suite récurrente linéaire et si $s \in N^\star$ alors pour $0 \leq i < s$, la suite $(u_{i+sn})_n$ est une suite récurrente linéaire, [F. M. 1] p. 319 et exercice ci-dessous.
(5) Le groupe $U(K) := \{z \in K \mid |z| = 1\}$ pour K un sous-corps de $\mathbb{C}$, [F. M. 2] IV.8.1 p.246 à 248 et exercices ci-dessous.
(6) Une extension Galoisienne de $\mathbb{Q}$, [F. M. 1] $n°105$ p. 294.

Exercice 1 Le théorème de Wederburn, [Fr. F] p. 157.

Exercice 2 Degré du corps de décomposition, [F. M. 1] $n°102$ p. 277.

Exercice 3 Sur l'impossibilité de résoudre une équation de degré 3 avec des radicaux réels, [F. M. 2] p. 262.

Exercice 4 Sous-corps de $K(X)$ et K-automorphismes de $K(X)$, [F. M. 2] p. 260 et [F. M. 1] p. 314-315 et une application au corps des invariants de $\mathbb{C}$ par les automorphismes de $\mathbb{C}$, [Fr. F] ex. 9.4.1. p 319.

Exercice 5

(1) Extensions quadratiques isomorphes, [Fr. F] ex. 3.8.9. p. 177.
(2) Les automorphismes de $\mathbb{Q}$ et de $\mathbb{R}$, [Fr. F] ex. 3.8.14 p 179.
(3) Le corps des invariants de $\mathbb{C}$ par les automorphismes de $\mathbb{C}$, [Fr. F] ex. 9.4.1. p 319.

Exercice 6 Une preuve de la transcendance de π (voir [La.] ou [Du.])

Exercice 7 Les corps extensions finies de $\mathbb{R}$ (ils ne sont pas nécessairement commutatifs)? [F. M. 2] p.254.

Exercice 8 Complément au développement : "Si u_n est une suite récurrente linéaire et si $s \in N^\star$ alors pour $0 \leq i < s$, la suite $(u_{i+sn})_n$ est une suite récurrente linéaire "

Dans [F. M. 1] lemme 1 p. 319 on montre que $K(X) = \bigoplus_{0\leq i<s} K(X^s)X^i$. Ainsi (*) $F(X) = \sum_{0\leq i<s} F_i(X^s)X^i$ pour $F(X) \in K(X)$ et avec $F_i(X)$ uniquement déterminée dans $K(X)$.

Dans le cas où s est inversible dans K et K contient les racines s-ièmes de l'unité on peut donner une expression de la i-ième forme linéaire coordonnée. Soit $\zeta_s \in K$ une racine primitive s-ième de 1 et σ le K-automorphisme de $K[X]$ avec $\sigma(X) = \zeta_s X$, on vérifie qu'il se prolonge en un K-automorphisme de $K(X)$. En appliquant σ^j pour $0 \leq j < s$ à (*) on obtient un système de Vandermonde; il suit que $F_0(X^s) = \frac{1}{s}\sum_{0\leq j<s} F(\zeta_s^j X)$ et plus généralement $F_i(X^s) = \frac{1}{s}\sum_{0\leq j<s} F(\zeta_s^j X)(\zeta_s^j X)^{-i}$.

Dans le cas où la caractéristique de K est $p > 0$ et si $s = p$ on vérifie que $D^{p-1}(F(X)) = -F_{p-1}(X^p)$ où $D : K[X] \to K[X]$ est le K-endomorphisme de dérivation i.e. $D(X^i) = iX^{i-1}$ pour $i > 0$ et $D(1) = 0$. et plus généralement $D^{p-1}(X^{p-1-i}F(X)) = -F_i(X^p)$.

Exercice 9 Groupe des nombres complexes de module 1 et sous-corps de $\mathbb{C}$, [F. M. 2] IV.8.1 p.246

Soit $n \geq 1$, on note μ_n le sous-groupe de $\mathbb{C}^\times$ des racines n-ièmes de l'unité, $\zeta_n \in \mathbb{C}$ une racine primitive n-ième de l'unité et $\mu_\infty := \cup_{n>0}\mu_n$. On note σ l'automorphisme de conjugaison. Si $A \subset \mathbb{C}$, on note $U(A) := \{z \in A \mid |z|^2 = z\sigma(z) = 1\}$. On se propose de montrer que :

- Si n est pair, alors $\mu_\infty \cap \mathbb{Q}(\zeta_n) = \mu_n$ et si n est impair, alors $\mu_\infty \cap \mathbb{Q}(\zeta_n) = \mu_{2n} = \mu_n \cup -\mu_n$.
  - Soit $d|n$, montrer que μ_d est l'unique sous-groupe de $\mathbb{C}^\times$ d'ordre d.
  - Soit $\xi \in \mu_\infty \cap \mathbb{Q}(\zeta_n)$ et G le sous-groupe de $\mathbb{Q}(\zeta_n)^\times$ engendré par ζ_n et ξ. Montrer que $G = \mu_m$ avec $m = dn$ et que $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m)$.
  - En déduire que $\varphi(n) = \varphi(nd)$.
  - Conclure.
- Soit K un sous-corps de $\mathbb{C}$. Alors
  - Si $K \cap \sigma(K) \subset \mathbb{R}$, alors $U(K) = \{-1, 1\}$.
  - Si $K \cap \sigma(K) \subsetneq \mathbb{R}$, alors $U(K)$ est infini et par conséquent dense dans $U(\mathbb{C})$. De plus il existe $z \in U(K)$ avec $z \notin \mu_\infty$.
    - On suppose que $K \cap \sigma(K) \subset \mathbb{R}$. Montrer que $U(K) = \{-1, 1\}$.
    - On suppose que $K \cap \sigma(K) \subsetneq \mathbb{R}$.
      - Soit $x \in K \cap \sigma(K)$ avec $x \notin \mathbb{R}$. Soit $a \in \mathbb{Q}$ et $y(a) := \frac{a+x}{a+\sigma(x)}$, montrer que $y(a) \in U(K)$.
      - Montrer que $U(K)$ est infini.

· En déduire que $U(K)$ dense dans $U(\mathbb{C})$.
· On suppose que $U(K)$ est de torsion. Montrer qu'il existe $a \in \mathbb{Q}$ avec $o(y(a)) = n > 2$.
· Soient $b \in \mathbb{Q}$ et $z(b) := \frac{b+y(a)}{b+y(a)^{-1}}$. Montrer que $z(b) \in U(K)$.
· Conclure à l'aide de la première partie de l'exercice à une absurdité.

– Exemples.
∗ Le groupe $U(K)$ avec $K := \mathbb{Q}(j2^{1/3})$ où $j = e^{i\frac{2\pi}{3}}$.
Montrer que $[K : \mathbb{Q}] = 3$ et que $K \neq \sigma(K)$, en déduire que $K \cap \sigma(K) = \mathbb{Q}$ et donc que $U(K) = \{-1, 1\}$.
∗ Le groupe $U(\mathbb{Q}(i))$.
On rappelle que $\mathbb{Z}[i]$ est un anneau principal et que l'on dispose alors de la décomposition en irréductibles dans $\mathbb{Q}(i)^\times$. Un système d'éléments irréductibles de $\mathbb{Z}[i]$ est indexé sur les premiers $\mathcal{P}$ de $\mathbb{N}$. Précisément si $p = 2$, on note $\pi_2 := 1 + i$, c'est l'unique irréductible à associés près avec $2\mathbb{Z} = \pi_2\mathbb{Z}[i] \cap \mathbb{Z}$. Si $p = 1 \mod 4$ alors $p = a^2 + b^2$ avec $0 < a < b$, on note $\pi_p := a + ib$ et $\overline{\pi}_p$ le conjugué, ce sont à associés près les seuls irréductibles π de $\mathbb{Z}[i]$ avec $p\mathbb{Z} = \pi\mathbb{Z}[i] \cap \mathbb{Z}$. Si $p = 3 \mod 4$, alors p est irréductible dans $\mathbb{Z}[i]$. Ainsi $\pi_2 \cup \{\pi_p,\ \overline{\pi}_p \mid p = 1 \mod 4\} \cup \{\pi_p \mid p = 3 \mod 4\}$ est un système d'irréductibles de $\mathbb{Z}[i]$ (voir [F. M. 1] n° 94 p. 260). Soit $z \in \mathbb{Q}(i)^\times$, alors $z = \epsilon\pi_2^{n_2} \prod_{p=1 \mod 4} \pi_p^{n_p}\overline{\pi}_p^{m_p} \prod_{p=3 \mod 4} p^{n_p}$ où $\epsilon \in \mu_4$ et $z \in U(\mathbb{Q}(i))$ ssi $n_2 = 0$, $n_p + m_p = 0$ pour $p = 1 \mod 4$ et $n_p = 0$ pour $p = 3 \mod 4$. En déduire que $U(\mathbb{Q}(i))$ est isomorphe à $\frac{\mathbb{Z}}{4\mathbb{Z}} \times \mathbb{Z}^{(\mathbb{N})}$ où $\mathbb{Z}^{(\mathbb{N})}$ est le sous-groupe des suites nulles à partir d'un certain rang i.e. c'est la somme de copies de $\mathbb{Z}$ indexées par $\mathbb{N}$.
∗ Une application d'une version faible du théorème 90 de Hilbert, [F. M. 2] prop. p. 248.
On suppose que $\sigma(K) = K$ et que $K \subsetneq \mathbb{R}$. On note ρ l'homomorphisme de $\mathbb{C}^\times$ dans lui-même défini par $\sigma(y) = \frac{y}{\sigma(y)}$. Alors ρ induit un homomorphisme surjectif de $K^\times$ dans $U(K)$ dont le noyau est $(K \cap \mathbb{R})^\times$. Montrons cela.
· Soit $x \in K$ avec $x \notin \mathbb{R}$ et $y := x - \sigma(x)$. Montrer que $-1 = \rho(y)$.
· Soit $z \in U(K)$ avec $z \neq -1$. Soit $y := 1 + z$, calculer $\rho(y)$ et conclure.
· Remarque. Si $K = \mathbb{Q}(i)$, alors $U(\mathbb{Q}(i)) \simeq \frac{\mathbb{Q}(i)^\times}{\mathbb{Q}^\times}$. On peut retrouver cela en utilisant la décomposition en irréductibles comme au-dessus. On notera que $\rho(\pi_2) = i$ est d'ordre 4.

Exercice 10 Equations diophantiennes et Hilbert 90 dans les extensions quadratiques d'après N. Elkies.

Lemme. Hilbert 90 dans les extensions quadratiques, [F. M. 2] p.248. Soit $\delta \in \mathbb{Z}$ non carré, $K := \mathbb{Q}(\sqrt{\delta}) \subset \mathbb{C}$. Si $w := a + b\sqrt{\delta} \in K$ on note $\sigma(w) = a - b\sqrt{\delta}$ et $U(K) := \{w \in K \mid w\sigma(w) = 1\}$. Alors $U(K) = \{\frac{x}{\sigma x},\ x \in K^\times\}$.

Preuve. On remarque que K est stable par σ. Alors $-1 = \frac{x}{\sigma x}$ pour $x := \sqrt{\delta}$. Soit maintenant $-1 \neq w \in U(K)$ et $x := w + 1 \neq 0$, alors $w = \frac{x}{\sigma x}$ d'où l'égalité $U(K) = \{\frac{x}{\sigma x},\ x \in K^\times\}$.

Corollaire 1. Le triplet $(x, y, z) \in \mathbb{Z}^3$ est solution de l'équation diophantienne $x^2 + y^2 = z^2$ ssi il existe $(m, n) \in \mathbb{Z}^2$ et $c \in \mathbb{Q}$ avec $(x, y, z) = c(m^2 - n^2, 2mn, m^2 + n^2)$.

Preuve. Supposons que $(x, y, z) \in \mathbb{Z}^3$ satisfait l'équation diophantienne $x^2 + y^2 = z^2$. Si $z = 0$ alors $(m, n) = (0, 0)$. Supposons donc que $z \neq 0$ et soit $w := \frac{x+iy}{z}$, alors $w \in U(\mathbb{Q}(i))$ et ainsi (c'est le lemme et dans ce cas σ est la conjugaison complexe) il existe $a \in \mathbb{Q}(i)^\star$ avec $w = \frac{a}{\overline{a}}$ et quitte à changer a en ra avec $r \in \mathbb{Z}$ on peut supposer que $a = m + in \in \mathbb{Z}[i]^\star$. Alors $w = \frac{(m^2-n^2)+i(2mn)}{m^2+n^2}$,

ce qui montre bien que (x, y, z) est proportionnel à $(m^2 - n^2, 2mn, m^2 + n^2)$. Réciproquement on vérifie que la condition est suffisante.

Remarque. Si $z \neq 0$ alors $xyz \neq 0$ et quitte à diviser (x, y, z) par leur pgcd, on peut supposer que $PGCD(x, y, z) = 1$. On peut dans le corollaire supposer que $PGCD(m, n) = 1$. Si $m \in 1 + 2\mathbb{Z},\ n \in 2\mathbb{Z}$ alors $PGCD(m^2 - n^2, 2mn, m^2 + n^2) = 1$ et alors $c \in \{-1, 1\}$ (on écrit $c = \frac{u}{v}$ avec $PGCD(u, v) = 1$ et alors $v\mathbb{Z} = PGCD(vx, vy, vz)\mathbb{Z} = PGCDu(m^2 - n^2, 2mn, m^2 + n^2)\mathbb{Z} = u\mathbb{Z}$). Si $m \in 1 + 2\mathbb{Z},\ n \in 1 + 2\mathbb{Z}$ alors $PGCD(m^2 - n^2, 2mn, m^2 + n^2) = 2$ et $c \in \{-1/2, 1/2\}$.

Corollaire 2. Soient $A, B \in \mathbb{Z}$ avec $A^2 - 4B = \delta$ non carré dans $\mathbb{Z}$. Soit $K := \mathbb{Q}(\sqrt{\delta}) \subset \mathbb{C}$ et $\theta \in K$ une racine de $P = X^2 + AX + B$. Le triplet $(x, y, z) \in \mathbb{Z}^3$ est solution de l'équation diophantienne $x^2 + Axy + By^2 = z^2$ ssi il existe $(m, n) \in \mathbb{Z}^2$ et $c \in \mathbb{Q}$ avec $(x, y, z) = c(m^2 - Bn^2, 2mn + An^2, m^2 + Amn + Bn^2)$

Preuve. Même chose que précédement avec $\sigma(a + \theta b) = a + (A - \theta)b$. Soit $w := \frac{x+\theta y}{z} \in K$, alors $w \in U(K)$ ssi $x^2 + Axy + By^2 = z^2$ et $z \neq 0$ et on applique le lemme à K.