ALGÈBRE - LEÇON 125 : EXTENSIONS DE CORPS. EXEMPLES ET APPLICATIONS

SIMON RICHE

1. Commentaires du jury (rapport 2024)

Les extensions de degré fini, le théorème de la base téléscopique et ses applications à l'irréductibilité de certains polynômes, ainsi que les corps finis, sont incontournables. Il est souhaitable d'introduire la notion d'élément algébrique et d'extension algébrique en en donnant des exemples. Il faut savoir calculer le polynôme minimal d'un élément algébrique dans des cas simples, notamment pour quelques racines de l'unité. La leçon peut être illustrée par des exemples d'extensions quadratiques et leurs applications en arithmétique, ainsi que par des extensions cyclotomiques.

Pour aller plus loin, les candidates et candidats peuvent montrer que l'ensemble des nombres algébriques forme un corps algébriquement clos, par exemple en expliquant comment l'utilisation du résultant permet de calculer des polynômes annulateurs de sommes et de produits de nombres algébriques. Il est possible de s'intéresser aux nombres constructibles à la règle et au compas, et éventuellement s'aventurer en théorie de Galois.

2. Plan

Cette leçon est très riche. Le livre de Perrin [Pe] est une bonne référence de base. Ce sujet est subtil, et la seule façon de le dompter est de s'y confronter, et de faire durant la préparation toutes les erreurs stupides classiques, pour éviter de devoir les faire au moment du concours.

2.1. **Ce qui doit apparaître.** Définition d'une extension (tout morphisme de corps est injectif).

Degré d'une extension.

Théorème de la base téléscopique.

Sous-corps engendré par une partie.

Éléments algébriques, éléments transcendants. (Les éléments algébriques forment un sous-corps.)

Polynôme minimal.

Corps de rupture (existence, unicité, exemples).

Corps de décomposition (existence, unicité, exemples).

Corps algébriquement clos.

Exemple des corps finis. (Construction comme corps de rupture et/ou comme corps de décomposition. Groupe multiplicatif cyclique. Tout corps gauche fini est un corps.)

Des exemples, des exemples, et encore des exemples, dont les corps cyclotomiques.

Date: Année 2024–2025.

2.2. **Ce qui peut apparaître.** Extensions séparables. Théorème de l'élément primitif.

Théorie de Galois.

Groupes de Galois [1] des corps finis [2], des corps cyclotomiques [3].

Constructibilité à la règle et au compas.

Invariance ou non de diverses notions par extension de corps [4].

Théorème de Springer [5].

3. Quelques questions bêtes auxquelles il faut absolument savoir répondre rapidement

(1) Que peut-on dire du degré d'un corps de rupture ? D'un corps de décomposition ?

(2) Donner un exemple de polynôme irréductible dont le corps de rupture n'est pas un corps de décomposition.

(3) Donner un exemple d'extension non séparable. (Voir l'Exercice 5 si besoin...)

(4) Le théorème de l'élément primitif assure que toute extension séparable est monogène. La réciproque est-elle vraie ?

(5) Si $\mathbb{K}$ est un corps, quels sont les éléments de $\mathbb{K}[X]$ qui sont les polynômes minimaux d'éléments algébriques dans une extension de $\mathbb{K}$?

(6) On rappelle qu'un polynôme $P \in \mathbb{K}[X]$ est dit séparable s'il est à racines simples dans son corps de décomposition. Montrer que si P est irréductible, P est séparable si et seulement si $P' \neq 0$. En déduire que si $\mathbb{K}$ est de caractéristique nulle, tout polynôme irréductible dans $\mathbb{K}[X]$ est séparable, puis que toute extension algébrique de $\mathbb{K}$ est séparable.

4. Exercices

Le sujet de cette leçon est proche de celui de la leçon 123, et les exercices de la feuille de cette leçon sont également conseillés pour préparer celle-ci.

Exercice 1. On considère une extension de corps $\mathbb{L}/\mathbb{K}$. Partant de données à coefficients dans $\mathbb{K}$, déterminer parmi les problèmes suivants ceux qui ont la même réponse sur $\mathbb{K}$ ou sur $\mathbb{L}$, et ceux pour lesquels la réponse peut être différente.

(1) le déterminant d'une matrice ;

(2) le rang d'une matrice ;

(3) la dimension d'un sous-espace vectoriel de $\mathbb{E}^n$ engendré par une famille de vecteurs donnés ;

(4) l'existence de solutions pour un système linéaire ;

(5) la dimension de l'espace des solutions d'un système linéaire ;

(6) le polynôme caractéristique d'une matrice ;

(7) le polynôme minimal d'une matrice ;

1. Notons qu'on peut calculer des groupes de Galois sans parler explicitement de théorie de Galois si on veut éviter des questions possiblement gênantes du jury.
2. Voir l'Exercice 2 de la feuille de la leçon 123.
3. Voir le §5.2 ci-dessous.
4. Voir l'exercice 1 ci-dessous
5. Voir le §5.1 ci-dessous.

(8) la diagonalisabilité ;
(9) la trigonalisabilité ;
(10) le fait d'être nilpotente (pour une matrice) ;
(11) le nombre de classes de conjugaison de matrices nilpotentes ;
(12) les facteurs invariants d'une matrice ;
(13) le fait, pour 2 matrices, d'être conjuguées ou non [6] ;
(14) l'ensemble des valeurs propres d'une matrice ;
(15) la dimension de l'espace propre d'une matrice associé à une valeur propre donnée ;
(16) l'irréductibilité d'un polynôme ;
(17) le PGCD de 2 polynômes ;
(18) le polynôme minimal d'un élément algébrique.

Pour tous ces exemples, il pourra être utile (quand c'est possible) de traiter le cas de l'extension $\mathbb{C}/\mathbb{R}$ par des méthodes spécifiques.

Référence : pour (12) et (13), voir [CG, Chap. III, Corollaires 5.13 et 5.14].

Exercice 2. (1) Soit $\mathbb{L}/\mathbb{K}$ une extension de corps de degré m, et soit d un entier premier à m. Montrer que si $P \in \mathbb{K}[X]$ est de degré d, alors P est irréductible sur $\mathbb{K}$ si et seulement si il est irréductible sur $\mathbb{L}$. (*Indication* : Supposant que P est irréductible sur $\mathbb{K}$, on pourra considérer un facteur irréductible Q de P dans $\mathbb{L}[X]$, puis appliquer la multiplicativité des degrés en considérant un corps de rupture de Q sur $\mathbb{L}$.)

(2) Application : montrer que le polynôme $X^3 + X + 1$ est irréductible sur $\mathbb{F}_{2^{2^n}}$ pour tout $n \geq 1$.

Référence : Exercice 5 de la feuille de TD7 de C. Demarche mentionnée à la Partie 6.

Exercice 3. (1) Déterminer $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$.

(2) Déterminer un élément α tel que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$.

(3) Déterminer le groupe des automorphismes de corps de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. (Indication : on pourra commencer par montrer que ce groupe est de cardinal au plus 4, puis construire 2 éléments distincts d'ordre 2.)

Exercice 4. (1) Soit $\mathbb{K}$ un corps de caractéristique $\neq 2$, et $a, b \in \mathbb{K}^\times$. Fixons une extension $\mathbb{L}$ de $\mathbb{K}$ dans laquelle a et b admettent des racines carrées $\sqrt{a}$ et $\sqrt{b}$. Montrer qu'on a $\mathbb{K}(\sqrt{a}) = \mathbb{K}(\sqrt{b})$ si et seulement si $\frac{a}{b}$ est un carré de $\mathbb{K}$. (*Indication* : si $\sqrt{b} = x + y\sqrt{a}$ avec $x, y \in \mathbb{K}$, et si a n'est pas un carré de $\mathbb{K}$, on pourra montrer que $x = 0$.)

(2) Montrer que si $p_1, \cdots, p_n$ sont des entiers deux à deux premiers entre eux et sans facteur carré on a $[\mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$. (*Indication* : on pourra raisonner par récurrence sur n.)

(3) Déterminer le groupe des automorphismes de corps de $\mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n})$. (*Indication* : on pourra s'inspirer de l'exercice 3.)

6. Le cas particulier de cette question pour l'extension $\mathbb{C}/\mathbb{R}$ (cf. par exemple [Go, Chap. 3, §6, Problème 11]) est un exercice archi-classique, qu'il faut absolument savoir faire !

Référence : Exercices 2 et 8 de la feuille de TD7 de C. Demarche mentionnée à la Partie 6.

Exercice 5. (1) Soit $\mathbb{K}$ un corps, soit $a \in \mathbb{K}$, et soit $n \geq 2$. Montrer que s'il existe des polynômes unitaires $P, Q \in \mathbb{K}[X]$ tels que $X^n - a = PQ$ avec $\deg(P)$ premier à n, alors a est la puissance n-ième d'un élément de $\mathbb{K}$. (*Indication* : en travaillant dans un corps de décomposition de $X^n - a$, on vérifiera que si $b = (-1)^{\deg(P)}P(0)$, alors on a $b^n = a^{\deg(P)}$, puis on utilisera cette relation pour construire explicitement un élément dont la puissance n-ième est a.)

(2) En déduire que si $\mathbb{K}$ est un corps et p est un nombre premier, le polynôme $X^p - a$ est réductible si et seulement si a est la puissance p-ième d'un élément de $\mathbb{K}$.

(3) *Application 1* : montrer que si p est un nombre premier et $\mathbb{K}$ un corps de caractéristique p, l'extension $\mathbb{K}(T)/\mathbb{K}(T^p)$ est de degré p, et non séparable.

(4) *Application 2* : soient p et ℓ deux nombres premiers tels que $\ell \mid p-1$, et soit n un entier dont la classe modulo p est un générateur de $(\mathbb{F}_p)^\times$. Montrer que le polynôme $x^\ell + pQ(X) - n$ est irréductible dans $\mathbb{Z}[X]$ pour tout $Q \in \mathbb{Z}[X]$. (Indication : on pourra réduire modulo p.)

Exercice 6 (Résultant et nombres algébriques)**.** Soit K un corps. On rappelle que si P et Q sont des polynômes à coefficients dans K, de degrés respectifs m et n tels que $n + m > 0$, en notant

$$P(X) = a_m X^m + \cdots + a_1 X + a_0, \quad Q(X) = b_n X^n + \cdots + b_1 X + b_0,$$

la *matrice de Sylvester* de (P, Q) est la matrice carrée de taille $n + m$ définie par

$$\mathrm{Sylv}(P,Q) = \begin{pmatrix} a_m & a_{m-1} & \cdots & \cdots & a_0 & 0 & \cdots & \cdots \\ 0 & a_m & a_{m-1} & \cdots & \cdots & a_0 & 0 & \cdots \\ \vdots & \ddots & \ddots & & & & \ddots & \\ b_n & b_{m-1} & \cdots & b_0 & 0 & \cdots & \cdots & \\ 0 & b_n & b_{n-1} & \cdots & b_0 & 0 & \cdots & \\ \vdots & \ddots & \ddots & & & & \ddots & \end{pmatrix}$$

où b_n apparait sur la ligne d'indice $n + 1$, et que le *résultant* de (P, Q) est

$$\mathrm{Res}(P,Q) = \det(\mathrm{Sylv}(P,Q)).$$

On rappelle également que les polynômes P et Q sont premiers entre eux (dans $K[X]$) si et seulement si $\mathrm{Res}(P, Q) \neq 0$. (Pour des détails, voir par exemple la feuille sur la leçon 142.)

(1) Soient $P, Q \in A[X]$. Montrer que P et Q admettent une racine commune dans une extension de K si et seulement si $\mathrm{Res}(P, Q) = 0$.

(2) Soit L une extension de K, et soient $x, y \in L$ des nombres algébriques sur K. Fixons des polynômes non nuls $P, Q \in K[X]$ tels que $P(x) = 0$ et $Q(y) = 0$.

  (a) On considère $P(X)$ et $Q(Y - X)$ comme polynômes à coefficients dans $K(Y)$, et on note R leur résultant. Montrer que $R \in K[Y]$ et $R(x+y) = 0$, et en déduire que $x + y$ est algébrique sur K. (*Indication* : pour montrer que R est non nul, on pourra travailler sur le corps $M(Y)$ où M est un corps de décomposition de P.)

(b) On note p le degré de Q. On considère $P(X)$ et $X^pQ(Y/X)$ comme polynômes à coefficients dans $K(Y)$, et on note S leur résultant. Montrer que $S \in K[Y]$ et $S(xy) = 0$, et en déduire que xy est algébrique sur K.

(c) Déterminer les polynômes minimaux de $\sqrt{2} + \sqrt[3]{3}$ et $\sqrt{2} \cdot \sqrt[3]{3}$ sur $\mathbb{Q}$.

Exercice 7. Pour p un nombre premier et $n \geq 1$, on note $\varphi_{n,p} \in \mathbb{F}_p[X]$ l'image du n-ième polynôme cyclotomique φ_n par le morphisme naturel $\mathbb{Z}[X] \to \mathbb{F}_p[X]$. On rappelle [7] que si n est premier à p, alors $\varphi_{n,p} = \prod_{\zeta \in \mu_n^\circ(\mathbb{F})}(X - \zeta)$ où $\mathbb{F}$ est une clôture algébrique de $\mathbb{F}_p$ et $\mu_n^\circ(\mathbb{F})$ est l'ensemble des racines primitives n-ièmes de l'unité dans $\mathbb{F}$. Le but de cet exercice est de démontrer que pour $n \geq 2$ fixé, il existe p premier tel que $\varphi_{n,p}$ soit irréductible (dans $\mathbb{F}_p[X]$) si et seulement si $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

(1) Rappeler pourquoi si $\mathbb{K}$ est un corps, un polynôme $P \in \mathbb{K}[X]$ est réductible si et seulement si il admet une racine dans une extension de $\mathbb{K}$ de degré $< \deg(P)$ [8].

(2) En déduire que si n est premier à p, $\varphi_{n,p}$ est réductible (dans $\mathbb{F}_p[X]$) si et seulement si l'ordre de l'image de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est $< \phi(n)$ (où ϕ est l'indicatrice d'Euler). (On pourra utiliser le fait que le groupe des inversibles d'un corps fini est cyclique.)

(3) On suppose que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique, et on fixe $a \in \mathbb{Z}$ dont la classe dans $\mathbb{Z}/n\mathbb{Z}$ est un générateur de $(\mathbb{Z}/n\mathbb{Z})^\times$. Montrer que si p est un nombre premier [9] tel que $p \equiv a \mod n$, alors $\varphi_{n,p}$ est irréductible.

(4) On suppose maintenant que $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique.

(a) Montrer que si p ne divise pas n, alors $\varphi_{n,p}$ est réductible.

(b) On suppose à partir de maintenant que $p \mid n$, et on écrit $n = p^\alpha m$ avec $\alpha \geq 1$ et $m \geq 1$. On suppose par l'absurde que $\varphi_{n,p}$ est irréductible. Montrer que $\varphi_{n,p}$ divise $X^m - 1$ dans $\mathbb{F}_p[X]$. (*Indication* : on pourra utiliser les propriétés du morphisme de Frobenius.)

(c) En déduire qu'alors il existe un diviseur d de m tel que $\varphi_{n,p}$ divise $\varphi_{d,p}$.

(d) Montrer qu'on a nécessairement $p = 2$, $\alpha = 1$, et $d = m$. (*Indication* : considérer les degrés de polynômes appropriés.)

(e) Montrer qu'alors $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times$, et trouver une absurdité.

Référence : [Pe, Chap. III, Théorème 4.14 et Proposition 4.16].

Exercice 8. L'objectif de cet exercice est de décrire, étant donné un corps $\mathbb{K}$, le groupe $\mathrm{Aut}_{\mathbb{K}}(\mathbb{K}(X))$ des automorphismes de corps $\mathbb{K}$-linéaires de $\mathbb{K}(X)$.

(1) Montrer que les endomorphismes de $\mathbb{K}$-algèbres de $\mathbb{K}(X)$ sont exactement les applications

$$\Phi_Q : \left\{ \begin{array}{ccc} \mathbb{K}(X) & \to & \mathbb{K}(X) \\ P & \mapsto & P \circ Q \end{array} \right.$$

pour $Q \in \mathbb{K}(X)$.

7. Voir par exemple [Pe, Chap. III, Proposition 4.8].

8. On peut raffiner cette condition en disant un degré $\leq \deg(P)/2$, mais cela ne sera pas utile pour les considérations de cet exercice.

9. L'existence d'un tel nombre premier n'est pas évidente. Mais le théorème de la progression arithmétique de Dirichlet (qu'on admettra ici) assure que c'est bien le cas.

(2) Montrer que l'application

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \Phi_{\frac{aX+b}{cX+d}}$$

induit un morphisme de groupes injectif

$$\mathrm{PGL}_2(\mathbb{K}) \to \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}(X)).$$

(3) On veut maintenant montrer que le morphisme précédent est également surjectif. Pour cela on choisit $Q \in \mathbb{K}(X)$ tel que Φ_Q est bijectif, et on note P l'unique élément tel que $\Phi_Q(P) = X$. On écrit $Q = \frac{A}{B}$ et $P = \frac{C}{D}$ avec $A, B, C, D \in \mathbb{K}[X]$, $\mathrm{pgcd}(A, B) = 1 = \mathrm{pgcd}(C, D)$. On écrit également $C = \sum_{j=0}^{r} c_j X^j$ et $D = \sum_{j=0}^{s} d_j X^j$ avec $c_r \neq 0$, $d_s \neq 0$.

(a) Montrer que $(c_0, d_0) \neq (0, 0)$.

(b) Montrer que si $m = \max(r, s)$ alors on a

$$\sum_{j=0}^{r} c_j A^j B^{m-j} = X \sum_{k=0}^{s} d_k A^k B^{m-k}.$$

(c) En déduire que A divise $c_0 - d_0 X$, puis que $\deg(A) \leq 1$.

(d) Montrer de même que $\deg(B) \leq 1$. (*Indication* : on pourra distinguer les cas $r = s$, $r > s$ et $r < s$.)

(e) Conclure.

Référence : [FGN, Ex. 4.86]. Pour une preuve plus sophistiquée, mais aussi plus courte et plus précise, voir `https://perso.univ-rennes1.fr/matthieu.romagny/agreg/dvt/automorphismes_k_de_X.pdf`.

5. Compléments

5.1. **Le théorème de Springer.** Rappelons qu'une forme quadratique sur $\mathbb{K}^n$ peut être vue comme un polynôme homogène de degré 2 en n variables $X_1, \dots, X_n$, à coefficients dans $\mathbb{K}$. De ce point de vue, pour toute extension $\mathbb{L}$ de $\mathbb{K}$, q définit également une forme quadratique sur $\mathbb{L}^n$.

Dans cette partie on explique la démonstration du résultat suivant.

Théorème 1 (Théorème de Springer)**.** Soit $\mathbb{K}$ un corps, soit $n \in \mathbb{Z}_{\geq 1}$, et soit q une forme quadratique sur $\mathbb{K}^n$. Si $\mathbb{L}$ est une extension de $\mathbb{K}$ de degré impair, et si q admet un vecteur non nul isotrope [10] dans $\mathbb{L}^n$, alors q admet également un vecteur non nul isotrope dans $\mathbb{K}^n$.

Cette démonstration est expliquée (sous des formes légèrement différentes) dans [dSP, Chap. XV, Théorème 3.2.1], [DEMN, Théorème III.2.1], ou l'exercice 11 de la feuille de TD7 de C. Demarche mentionnée à la Partie 6. Voir aussi `http://math.univ-lyon1.fr/~caldero/Agregexterne/Theoreme-de-Springer.pdf` [11]

Démonstration. On fixe $\mathbb{K}$ et n, et on raisonne par récurrence sur $m := [\mathbb{L} : \mathbb{K}]$, le cas $m = 1$ étant tautologique. On suppose donc $m \geq 3$ impair, et le résultat connu pour une extension de degré impair inférieur ou égal à $m - 2$. On fixe une extension

10. On rappelle qu'un vecteur isotrope pour une forme quadratique est un vecteur sur lequel cette forme quadratique s'annule.

11. Attention, dans cette référence une subtilité dans la démonstration est omise...

$\mathbb{L}/\mathbb{K}$ de degré m, et une forme quadratique q sur $\mathbb{K}^n$ admettant un vecteur non nul isotrope dans $\mathbb{L}^n$.

Remarquons tout d'abord que s'il existe un sous-corps $\mathbb{K}' \subset \mathbb{L}$ tel que $\mathbb{K} \subsetneq \mathbb{K}' \subsetneq \mathbb{L}$, alors q admet un vecteur non nul isotrope dans $\mathbb{K}^n$. En effet, on a alors

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}'] \cdot [\mathbb{K}' : \mathbb{K}],$$

de sorte que $[\mathbb{L} : \mathbb{K}']$ et $[\mathbb{K}' : \mathbb{K}]$ sont impairs. On peut considérer q comme une forme quadratique sur $(\mathbb{K}')^n$. Puisque $[\mathbb{L} : \mathbb{K}'] < m$, en appliquant l'hypothèse de récurrence on obtient que q admet un vecteur non nul isotrope dans $(\mathbb{K}')^n$. Puis on applique de nouveau l'hypothèse de récurrence, cette fois pour q vue comme forme quadratique sur $\mathbb{K}^n$ et pour l'extension $\mathbb{K}'$ de $\mathbb{K}$.

Dans la suite, on suppose donc qu'il n'existe pas de sous-extension non triviale $\mathbb{K} \subsetneq \mathbb{K}' \subsetneq \mathbb{L}$. Si x est un élément de $\mathbb{L}$ qui n'appartient pas à $\mathbb{K}$, on a alors $\mathbb{L} = \mathbb{K}(x)$ puisque $\mathbb{K}(x)$ est un sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ strictement.

On fixe un tel x, et on note μ son polynôme minimal sur $\mathbb{K}$ (qui est nécessairement de degré m). Par hypothèse il existe un vecteur $(y_1, \dots, y_n) \in \mathbb{L}^n$ tel que

$$q(y_1, \dots, y_n) = 0.$$

Puisque $\mathbb{L} = \mathbb{K}(x)$, il existe des polynômes $g_1, \dots, g_n \in \mathbb{K}[X]$ tels que $y_i = g_i(x)$ pour tout i. De plus, on peut supposer que pour tout i on a $\deg(g_i) < m$ (puisque x est annulé par μ, qui est de degré m). On a alors

$$q(g_1(x), \dots, g_n(x)) = 0.$$

Si on note h le PGCD de $g_1, \dots, g_n$, puisque q est homogène de degré 2 on a

$$q(g_1(x), \dots, g_n(x)) = h(x)^2 \cdot q\left(\frac{g_1}{h}(x), \dots, \frac{g_n}{h}(x)\right).$$

De plus, $h(x) \neq 0$ puisque $\deg(h) < m$, donc on a

$$q\left(\frac{g_1}{h}(x), \dots, \frac{g_n}{h}(x)\right) = 0.$$

Quitte à remplacer g_i par $\frac{g_i}{h}$ pour chaque i, on peut donc supposer (et on supposera) que les g_i sont premiers entre eux dans leur ensemble. Enfin, puisque μ est le polynôme minimal de x sur $\mathbb{K}$, le fait que

$$q(g_1(x), \dots, g_n(x)) = 0$$

équivaut à la condition

$$\mu(X) \mid q(g_1(X), \dots, g_n(X))$$

dans $\mathbb{K}[X]$.

Notons d le maximum des degrés des g_i, et, pour chaque i, notons a_i le coefficient de X^d dans g_i. (Il est possible que certains de ces coefficients valent 0, mais ils ne sont pas tous nuls.) Si $q(a_1, \dots, a_n) = 0$, alors q admet un vecteur isotrope non nul dans $\mathbb{K}^n$, ce qui achève la preuve. Sinon, $q(g_1(X), \dots, g_n(X))$ est de degré $2d$ (et le coefficient de X^{2d} est $q(a_1, \dots, a_n)$). Considérons le polynôme quotient

$$\frac{q(g_1, \dots, g_n)}{\mu}.$$

Ce polynôme est de degré $2d-m$, qui est impair puisque m est impair, et strictement inférieur à m puisque $d < m$. Il admet donc un facteur irréductible f de degré impair, et ce degré est nécessairement strictement inférieur à m.

Notons alors $\mathbb{M}$ un corps de rupture de f. Par définition, cela signifie que $\mathbb{M}$ est une extension de $\mathbb{K}$ qui possède un élément y tel que $f(y) = 0$. On a alors

$$q(g_1(y), \dots, g_n(y)) = 0.$$

De plus, il existe i tel que $g_i(y) \neq 0$. (En effet, sinon f diviserait chacun des g_i, ce qui contredirait l'hypothèse que les g_i sont premiers entre eux dans leur ensemble.) Donc le vecteur $(g_1(y), \dots, g_n(y))$ est un vecteur non nul de $\mathbb{M}^n$, qui est isotrope pour q.

Puisque $[\mathbb{M} : \mathbb{K}] < m$, on peut appliquer l'hypothèse de récurrence une dernière fois pour conclure que q admet un vecteur isotrope dans $\mathbb{K}^n$. □

Remarque 1. Pour tester sa compréhension de la démonstration, le lecteur pourra essayer de l'adapter pour prouver l'énoncé suivant. Soit $\mathbb{K}$ un corps, soit $n \geq 1$, et soit q un polynôme homogène de degré 3 en $X_1, \dots, X_n$ à coefficients dans $\mathbb{K}$. Si $\mathbb{L}$ est une extension de $\mathbb{K}$ de degré 2 et s'il existe $y \in \mathbb{L}^n \smallsetminus \{0\}$ tel que $q(y) = 0$, alors il existe $z \in \mathbb{K}^n \smallsetminus \{0\}$ tel que $q(z) = 0$.

5.2. **Automorphismes des corps cyclotomiques.** On fixe $n \in \mathbb{Z}_{\geq 1}$, et on note φ_n le n-ième polynôme cyclotomique, c'est-à-dire que

$$\varphi_n(X) = \prod_{\zeta \in \mu_n^\circ} (X - \zeta)$$

où μ_n est l'ensemble des racines n-ièmes de l'unité dans $\mathbb{C}$ et $\mu_n^\circ \subset \mu_n$ est le sous-ensemble des racines primitives n-ièmes de l'unité. On rappelle que φ_n est unitaire, de degré $\phi(n)$ (où ϕ est l'indicatrice d'Euler), à coefficients entiers, et irréductible dans $\mathbb{Q}[X]$.

On notera K_n le n-ième corps cyclotomique, c'est-à-dire le sous-corps de $\mathbb{C}$ engendré par les racines n-ièmes de l'unité (ou, de façon équivalente, par une racine primitive n-ième de l'unité fixée). On notera $\mathrm{Aut}(K_n)$ le groupe des automorphismes de corps de K_n.

Proposition 1. Il existe un isomorphisme de groupes

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Aut}(K_n)$$

qui est caractérisé par le fait que pour tout $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ (où k est un entier premier à n), l'image $\xi_{\overline{k}}$ de $\overline{k}$ envoie tout $\zeta \in \mu_n$ sur ζ^k.

Démonstration. Remarquons pour commencer que si $\zeta \in \mu_n$, alors ζ^k ne dépend que de l'image de k dans $\mathbb{Z}/n\mathbb{Z}$, ce qui justifie que l'énoncé a bien un sens.

Fixons maintenant un entier k premier à n, et montrons qu'il existe un unique automorphisme ξ_k de K_n qui vérifie $\xi_k(\zeta) = \zeta^k$ pour tout $\zeta \in \mu_n$. L'unicité est claire, puisque μ_n engendre K_n comme sous-corps de $\mathbb{C}$. Pour démontrer l'existence, on remarque que pour tout $\zeta \in \mu_n^\circ$ il existe un unique morphisme de $\mathbb{Q}$-algèbres

$$\mathrm{ev}_\zeta : \mathbb{Q}[X] \to K_n$$

qui envoie tout polynôme $P(X)$ sur $P(\zeta)$. Puisque $\varphi_n(\zeta) = 0$, ce morphisme se factorise en un morphisme de $\mathbb{Q}$-algèbres

$$\alpha_\zeta : \mathbb{Q}[X]/(\varphi_n) \to K_n.$$

Puisque φ_n est irréductible dans $\mathbb{Q}[X]$, le quotient $\mathbb{Q}[X]/(\varphi_n)$ est un corps, ce qui implique que α_ζ est injectif, et que son image est un sous-corps de K_n. Celui-ci contient ζ, qui engendre K_n ; on en déduit que α_ζ est surjectif, et donc un isomorphisme de corps.

Fixons maintenant $\zeta \in \mu_n^\circ$, et posons

$$\xi_k := \alpha_{\zeta^k} \circ \alpha_\zeta^{-1} : K_n \to K_n.$$

Alors ξ_k est un automorphisme de corps de K_n, et on a $\xi_k(\zeta) = \zeta^k$ par construction. Puisque ζ engendre le groupe μ_n, on en déduit qu'on a en fait $\xi_k(\zeta') = (\zeta')^k$ pour tout $\zeta' \in \mu_n$, ce qui achève la démonstration de l'existence.

Il est clair par construction (ou par unicité) que ξ_k ne dépend que de l'image $\overline{k}$ de k dans $\mathbb{Z}/n\mathbb{Z}$; on le notera donc $\xi_{\overline{k}}$. Par unicité, pour $\overline{k}, \overline{l} \in (\mathbb{Z}/n\mathbb{Z})^\times$ on a

$$\xi_{\overline{k}} \circ \xi_{\overline{l}} = \xi_{\overline{k}\cdot\overline{l}}.$$

On en déduit que l'application $\overline{k} \mapsto \xi_{\overline{k}}$ définit un morphisme de groupes $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(K_n)$. De plus on a $\xi_{\overline{k}} = \mathrm{id}$ si et seulement si $\zeta^k = \zeta$ pour tout $\zeta \in \mu_n$, c'est-à-dire si et seulement si $\overline{k} = \overline{1}$. Donc ce morphisme est injectif.

Pour conclure, il suffit de montrer que tout automorphisme de corps de K_n est de la forme $\xi_{\overline{k}}$ pour un $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Cependant, si $\xi \in \mathrm{Aut}(K_n)$, et si on fixe $\zeta \in \mu_n^\circ$, on doit avoir $\varphi_n(\xi(\zeta)) = \xi(\varphi_n(\zeta)) = 0$, donc $\xi(\zeta) \in \mu_n^\circ$. Il existe ainsi un entier k premier à n tel que $\xi(\zeta) = \zeta^k$. Comme ci-dessus, ceci implique que $\xi(\zeta') = (\zeta')^k$ pour tout $\zeta' \in \mu_n$, et donc que $\xi = \xi_{\overline{k}}$. □

6. Autres ressources sur cette leçon

`http://math.univ-lyon1.fr/~caldero/Agregexterne/Lecon-125-Ext-Corps.pdf`

Pour des exercices utiles et corrigés (dont certains des exercices ci-dessus sont extraits), on pourra consulter les documents suivants :
`https://webusers.imj-prg.fr/~cyril.demarche/enseignements/2012-2013/M1-TDN/MM020-TD2-corrige.pdf`
`https://webusers.imj-prg.fr/~cyril.demarche/enseignements/2012-2013/M1-TDN/MM020-TD7-corrige.pdf`

Références

[CG] P. Caldero et J. Germoni, *Nouvelles histoires hédonistes de groupes et de géométries, Tome I*, Calvage & Mounet, 2017.

[DEMN] A. Debreil, J.-D. Eiden, R. Mneimné, T.-H. Nguyen, *Formes quadratiques et géométrie*, Calvage et Mounet, 2015.

[FGN] S. Francinou, H. Gianella, S. Nicolas, *Oraux X-ENS, Mathématiques 1*, Cassini, 2019.

[Go] X. Gourdon, *Les maths en tête - Algèbre, 2ème édition*, Ellipses, 2009.

[Pe] D. Perrin, *Cours d'algèbre*, Ellipses, 1996.

[dSP] C. de Seguins Pazzis, *Invitation aux formes quadratiques*, Calvage & Mounet, 2010.