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

SIMON RICHE

## 1. Commentaires du jury (rapport 2022)

Le théorème de la base téléscopique et ses applications à l'irréductibilité de certains polynômes, ainsi que les corps finis, sont incontournables. De même 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.

S'ils le désirent, les candidats peuvent montrer que l'ensemble des nombres algébriques forme un corps algébriquement clos et expliquer comment l'utilisation du résultant permet de calculer des polynômes annulateurs de sommes et de produits de nombres algébriques. Pour aller plus loin, les candidats peuvent parler des 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.)

Extensions séparables. Théorème de l'élément primitif.

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

---

*Date*: Année 2022–2023.

2.2. **Ce qui peut apparaître.** 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 (cf. Exercice 1 ci-dessous).

Application du groupe de Galois des corps cyclotomiques au critère pour que la table de caractères soit à valeurs dans $\mathbb{Z}$ ; cf. Partie 5 ci-dessous.

## 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 ;

(8) la diagonalisabilité ;

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 Lemme 1 dans la Partie 5.

(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 [4] ;
(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 fait, pour une représentation $\rho : G \to \mathrm{GL}_n(\mathbb{E})$, d'être irréductible ;
(19) 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 [CG1, 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 $\alpha$ 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 $a, b \in K^\times$. 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 $K$. (*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 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.)

4. 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 $p$ est un nombre premier, le polynôme $X^p - a$ est irréductible 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 $\ell$ 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.** Le but de cet exercice est de démontrer le théorème de Springer, qui affirme que si $\mathbb{K}$ est un corps et $q$ une forme quadratique sur $\mathbb{K}^n$ (par ceci on entend un polynôme homogène de degré 2 en $n$ variables $X_1, \cdots, X_n$), si $\mathbb{L}$ est une extension de degré impair de $\mathbb{K}$, et si $q$ admet un vecteur non nul isotrope (c'est-à-dire tel que $q(x) = 0$) dans $\mathbb{L}^n$, alors $q$ admet également un vecteur non nul isotrope dans $\mathbb{K}^n$. On raisonnera 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 $\leq m-2$. On fixe une extension $\mathbb{L}/\mathbb{K}$ de degré $m$, et une forme quadratique $q$ sur $\mathbb{K}^n$ admettant un vecteur non nul isotrope dans $\mathbb{L}^n$.

(1) Montrer 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 $\mathbb{K}^n$.

(2) On suppose donc qu'il n'existe pas de sous-extension non triviale $\mathbb{K} \subsetneq \mathbb{K}' \subsetneq \mathbb{L}$. Montrer qu'il existe $x \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(x)$.

(3) On fixe $x$ comme dans la question précédente, et on note $\mu$ son polynôme minimal. Montrer qu'il existe $g_1, \cdots, g_n \in \mathbb{K}[X]$, premiers entre eux dans leur ensemble, tels que $\deg(g_i) < m$ pour tout $i$, et tels que $\mu \mid q(g_1, \cdots, g_n)$.

(4) Montrer qu'il existe une extension $\mathbb{L}'/\mathbb{K}$ de degré impair $< m$ telle que $q$ admet un vecteur isotrope non nul dans $(\mathbb{L}')^n$. (*Indication* : on remarquera que si $d = \max(\deg(g_i))$ et si $a_1, \cdots, a_n$ sont les coefficients de degré $d$ des $g_i$, alors soit $q(a_1, \cdots, a_n) = 0$, soit $q(g_1, \cdots, g_n)$ est de degré $2d$. Dans le deuxième cas, on remarquera que $q(g_1, \cdots, g_n)/\mu$ admet un facteur irréductible de degré impair $< m$.)

(5) Conclure

Référence : [DEMN, Théorème III.2.1], ou `http://math.univ-lyon1.fr/~caldero/Agregexterne/Theoreme-de-Springer.pdf` [5], ou l'exercice 11 de la feuille de TD7 de C. Demarche mentionnée à la Partie 6.

5. Attention, dans cette référence une subtilité concernant la question (4) est omise...

**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 $\varphi_n$ par le morphisme naturel $\mathbb{Z}[X] \to \mathbb{F}_p[X]$. On rappelle [6] 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 $< \deg(P)$ [7].

(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 $\phi$ 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 [8] 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
$$\Phi_Q : \left\{ \begin{array}{ccc} \mathbb{K}(X) & \to & \mathbb{K}(X) \\ Q & \mapsto & Q \circ P \end{array} \right. .$$

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

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

7. 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.

8. 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.

(3) On veut maintenant montrer que le morphisme précédent est également surjectif. Pour cela on choisit $Q \in \mathbb{K}(X)$ tel que $\Phi_Q$ 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. 5.46]. 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. Complément : les caractères irréductibles du groupe $\mathfrak{S}_n$ sont à valeurs entières

Dans cette partie on explique (en suivant [CG2, Chap. XIII, Ex. E.33, Ex. E.40, Ex. E.41]) comment l'étude des polynômes cyclotomiques permet de démontrer que certains groupes (et notamment les groupes symétriques) ont leur table des caractères à valeurs entières. Pour une autre application des polynômes cyclotomiques à la théorie des groupes, voir l'exercice 17 de la fiche sur la leçon 108.

5.1. **Préliminaire sur les corps cyclotomiques.** On fixe $n \in \mathbb{Z}_{\geq 1}$, et on note $\varphi_n$ le $n$-ième polynôme cyclotomique, c'est-à-dire que

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

où $\mu_n$ 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 $\varphi_n$ est unitaire, de degré $\phi(n)$ (où $\phi$ 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 $K_n$.

**Lemme 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 $\zeta^k$.

*Démonstration.* Remarquons pour commencer que si $\zeta \in \mu_n$, alors $\zeta^k$ 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 $\xi_k$ de $K_n$ qui vérifie $\xi_k(\zeta) = \zeta^k$ pour tout $\zeta \in \mu_n$. L'unicité est claire, puisque $\mu_n$ 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 $\varphi_n$ est irréductible dans $\mathbb{Q}[X]$, le quotient $\mathbb{Q}[X]/(\varphi_n)$ est un corps, ce qui implique que $\alpha_\zeta$ est injectif, et que son image est un sous-corps de $K_n$. Celui-ci contient $\zeta$, qui engendre $K_n$ ; on en déduit que $\alpha_\zeta$ 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 $\xi_k$ est un automorphisme de corps de $K_n$, et on a $\xi_k(\zeta) = \zeta^k$ par construction. Puisque $\zeta$ engendre le groupe $\mu_n$, 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 $\xi_k$ 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 $\xi = \xi_{\overline{k}}$. □

On note $A_n \subset K_n$ le sous-anneau engendré par $\mu_n$, c'est-à-dire l'ensemble des combinaisons linéaires à coefficients entiers des éléments de $\mu_n$. La propriété des automorphismes $\xi_{\overline{k}}$ qui nous sera utile plus tard sera la suivante.

**Lemme 2.** Soit $\alpha \in A_n$. Alors on a $\xi_{\overline{k}}(\alpha) = \alpha$ pour tout $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement si $\alpha \in \mathbb{Z}$.

*Démonstration.* Chaque $\xi_{\overline{k}}$ est un automorphisme de corps de $K_n$ ; il fixe donc chaque élément de $\mathbb{Q}$, et en particulier chaque élément de $\mathbb{Z}$.

Réciproquement, soit $\alpha \in A_n$. Fixons $\zeta \in \mu_n^\circ$. Puisque $\zeta$ engendre $\mu_n$, il existe $P \in \mathbb{Z}[X]$ tel que $\alpha = P(\zeta)$. Puisque $\varphi_n$ est unitaire à coefficients entiers, il existe $Q, R \in \mathbb{Z}[X]$ avec $\deg(R) < \phi(n)$ tels que $P = Q\varphi_n + R$, et alors $\alpha = R(\zeta)$. En particulier, il existe $\lambda_0, \cdots, \lambda_{\phi(n)-1} \in \mathbb{Z}$ tels que

$$\alpha = \sum_{i=0}^{\phi(n)-1} \lambda_i \cdot \zeta^i.$$

Supposons maintenant que $\xi_{\overline{k}}(\alpha) = \alpha$ pour tout $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Alors, avec les notations précédentes on a

$$\sum_{i=0}^{\phi(n)-1} \lambda_i \cdot \zeta^{ki} = \alpha$$

pour tout entier $k$ entre 1 et $n$ premier à $n$. Notons ces entiers $k_1, \cdots, k_{\phi(n)}$ (de façon aléatoire), et notons $V$ la matrice de Vandermonde associée aux nombres complexes $\zeta^{k_i}$, c'est-à-dire qu'on pose $V = ((\zeta^{k_i})^{j-1})_{i,j=1,\cdots,\phi(n)}$. Puisque ces nombres complexes sont deux à deux distincts, $V$ est inversible, et les égalités précédentes montrent que

$$V \cdot a = V \cdot (\alpha e_1)$$

où $a = (\lambda_0, \cdots, \lambda_{\phi(n)-1})$ et $e_1$ est le premier vecteur de la base canonique de $\mathbb{C}^{\phi(n)}$. On en déduit que $a = \alpha e_1$, ce qui implique que $\lambda_i = 0$ pour tout $i \geq 1$, et donc que $\alpha = \lambda_0 \in \mathbb{Z}$. □

5.2. **Condition pour qu'un groupe ait sa table des caractères à coefficients entiers.** Dans cette partie on fixe un groupe fini $G$, dont on note $n$ le cardinal.

**Proposition 1.** La table des caractères de $G$ est à coefficients entiers (c'est-à-dire que $\chi(g) \in \mathbb{Z}$ pour tout $\chi$ caractère d'une représentation irréductible de $G$ et tout $g \in G$) si et seulement si pour tout $g \in G$ et tout $k \in \mathbb{Z}$ premier à $n$, $g$ et $g^k$ sont conjugués dans $G$.

*Démonstration.* Pour tout $g \in G$ et toute représentation complexe $\rho$ de $G$, on a $\rho(g)^n = \rho(g^n) = \rho(e) = \mathrm{id}$. Puisque le polynôme $X^n - 1$ est scindé à racines simples, on en déduit que $\rho(g)$ est diagonalisable, et que toutes ses valeurs propres sont dans $\mu_n$. Si on note $\chi$ le caractère de $\rho$, on a alors $\chi(g) \in A_n$. On a donc montré que la table des caractères de $G$ est à coefficients dans $A_n$.

Notons encore $\rho$ une représentation complexe de $G$, et $\chi$ le caractère associé. Fixons également un entier $k$ premier à $n$, et $g \in G$. Puisque $\chi(g)$ appartient à $A_n$ on peut considérer $\xi_{\overline{k}}(\chi(g))$. On a alors

$$\xi_{\overline{k}}(\chi(g)) = \chi(g^k). \tag{1}$$

En effet, $\chi(g)$ est la somme (avec multiplicités) des valeurs propres de $\rho(g)$. D'après la construction de $\xi_{\overline{k}}$, $\xi_{\overline{k}}(\chi(g))$ est alors la somme (avec les mêmes multiplicités) des puissances $k$-ièmes des valeurs propres de $\rho(g)$, c'est-à-dire la somme (avec multiplicités) des valeurs propres de $\rho(g)^k = \rho(g^k)$. On en déduit que $\xi_{\overline{k}}(\chi(g)) = \mathrm{tr}(\rho(g^k)) = \chi(g^k)$, comme annoncé.

On peut maintenant conclure. Tout d'abord, pour $g \in G$ fixé, si $g$ et $g^k$ sont conjugués on a $\chi(g) = \chi(g^k)$ ; si ceci est vrai pour tout $k$ premier à $n$, alors l'égalité (1) montre que pour tout caractère $\chi$ d'une représentation complexe de $G$ on a $\xi_{\overline{k}}(\chi(g)) = \chi(g)$ pour tout $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$, et donc que $\chi(g) \in \mathbb{Z}$ d'après le Lemme 2. Si ceci est vrai pour tout $g \in G$, ceci implique que la table de caractères de $G$ est à coefficients entiers.

Réciproquement, supposons que la table de caractères de $G$ est à coefficients entiers, et fixons $g \in G$ et $k$ un entier premier à $n$. Alors pour tout caractère $\chi$ d'une représentation complexe de $G$ on a $\chi(g) = \chi(g^k)$. Puisque ces caractères engendrent l'espace des fonctions centrales sur $G$ (c'est-à-dire l'ensemble des fonctions de $G$ dans $\mathbb{C}$ constantes sur les classes de conjugaison), on en déduit que $f(g) = f(g^k)$

pour toute telle fonction $f$. En particulier, considérons la fonction $f$ qui vaut 1 sur la classe de conjugaison de $g$, et 0 ailleurs. On a

$$f(g^k) = f(g) = 1,$$

donc $g^k$ appartient à la classe de conjugaison de $g$. En d'autres termes $g$ est conjugué à $g^k$, ce qui achève la preuve. □

5.3. **Application au groupe $\mathfrak{S}_m$.** Pour conclure, on va maintenant montrer que les groupes symétriques $\mathfrak{S}_m$ vérifient le critère de la Proposition 1.

**Lemme 3.** Soit $r \in \{1, \cdots, m\}$, et soit $\sigma \in \mathfrak{S}_m$ un $r$-cycle. Si $k$ est un entier premier à $r$, alors $\sigma^k$ est un $r$-cycle, de même support que $\sigma$.

*Démonstration.* La permutation $\sigma$ fixe chacun des $m - r$ entiers qui ne sont pas dans son support ; il en donc de même de $\sigma^k$. Pour conclure, il suffit donc de vérifier que le support de $\sigma$ est encore une unique orbite pour l'action des puissances de $\sigma^k$. Pour cela on choisit un entier $i$ dans le support de $\sigma$. Si $p$ est un entier, alors on a

$$(\sigma^k)^p(i) = i \quad \Leftrightarrow \quad \sigma^{kp}(i) = i \quad \Leftrightarrow \quad r \mid kp \quad \Leftrightarrow \quad r \mid p$$

puisque $r$ est premier à $k$. Donc l'orbite de $i$ pour l'action des puissances de $\sigma^k$ est de cardinal $r$, ce qui achève la preuve. □

**Théorème 1.** Pour tout $m \geq 1$, la table des caractères du groupe $\mathfrak{S}_m$ est à coefficients entiers.

*Démonstration.* D'après la Proposition 1, pour démontrer le théorème il suffit de montrer que pour tout $g \in \mathfrak{S}_m$ et pour tout $k$ premier à $m!$, $g$ et $g^k$ sont conjugués. Pour cela, d'après la description des classes de conjugaison de $\mathfrak{S}_m$ via la décomposition en cycles à supports disjoints, il suffit de démontrer que dans les décompositions de $g$ et $g^k$ en produit de cycles à supports disjoints, les longueurs des cycles qui apparaissent sont les mêmes. Considérons donc la décomposition de $g$ en produit de cycles à supports disjoints :

$$g = \sigma_1 \cdots \sigma_r.$$

On a alors

$$g^k = \sigma_1^k \cdots \sigma_r^k.$$

Puisque $k$ est premier à $m!$, il est premier à la longueur de $\sigma_i$, pour tout $i \in \{1, \cdots, r\}$. D'après le Lemme 3, ceci implique que chacun des $\sigma_i^k$ est un cycle de même longueur et de même support que $\sigma_i$. Donc $g^k = \sigma_1^k \cdots \sigma_r^k$ est la décomposition de $g^k$ en produit de cycles à support disjoint, ce qui achève la preuve. □

## 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

[CG1] P. Caldero et J. Germoni, *Nouvelles histoires hédonistes de groupes et de géométries, Tome I*, Calvage & Mounet, 2017.

[CG2] P. Caldero et J. Germoni, *Nouvelles histoires hédonistes de groupes et de géométries, Tome II*, Calvage & Mounet, 2018.

[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, algèbre 1*, Cassini, 2001.

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

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