# Extension de Corps-125

C'est une leçon difficile qui nécessite un minimum de théorie de Galois afin d'avoir un peu de recul. Mais il n'est pas nécessaire que cette théorie soit digérée : on peut comprendre beaucoup de choses rien qu'en s'appuyant sur le *toy model* de l'extension $\mathbb{C}$ de $\mathbb{R}$ qui est en général bien comprise. Attention tout de même : il est rare qu'un corps possède aussi peu d'extensions finies que $\mathbb{R}$, il faut donc regarder d'autres exemples comme les extensions de corps finis. Bien des éléments de cette leçon peuvent être placés dans la leçon 151 sur la dimension. Le Perrin, [1] est une bonne référence !

## 0. Prequel

Sauf indication contraire $\mathbb{L}$ désignera une extension du corps $\mathbb{K}$.

Pourquoi étudier les extensions de corps ? Un réponse simple et légitime est qu'on va y chercher des racines. L'extension $\mathbb{R}$ de $\mathbb{Q}$ a été contruite pour résoudre des équations comme $X^2-2=0$ et l'extension $\mathbb{C}$ de $\mathbb{R}$ a été contruite pour résoudre des équations comme $X^2+1=0$, et même beaucoup plus !

Le morphisme d'évaluation $\mathrm{ev}_\alpha : \mathbb{K}[X] \to \mathbb{L}$, $P \mapsto P(\alpha)$, où $\alpha \in \mathbb{L}$.

Encore une fois, tout repose sur le fait que $\mathbb{K}[X]$ est un anneau principal. Si $\alpha$ est transcendant sur $\mathbb{K}$ (et dans ce cas, $\mathbb{L}$ est de degré infini sur $\mathbb{K}$), l'idéal $\ker(\mathrm{ev}_\alpha)$ est nul. Sinon, $\alpha$ est algébrique sur $\mathbb{K}$ et l'idéal est non nul et ainsi, $\alpha$ possède un polynôme minimal $\mu_{\alpha,\mathbb{K}}$, unique (à scalaire près). Mais cette fois-ci $\mathbb{K}[X]/\ker(\mathrm{ev}_\alpha)$ se plonge dans le corps $\mathbb{L}$, et donc $\ker(\mathrm{ev}_\alpha)$ est un idéal premier. Comme $\mathbb{K}[X]$ est factoriel, cela se solde par le fait que $\mu_{\alpha,\mathbb{K}}$ est irréductible [1] sur $\mathbb{K}$.

Il faut remarquer qu'un corps n'a pas d'idéal non trivial. Il en résulte qu'un morphisme de corps non trivial est forcément injectif. Finalement, étudier les extensions de corps revient à étudier les morphismes de corps.

**Peaux de bananes classiques et pièges à mammouths :**

1. Notez bien que si on avait évalué en un endomorphisme, on serait arrivé dans $\mathrm{End}(E)$ qui n'est pas intégre. Comme on le sait bien, le polynôme minimal d'un endomorphisme peut ne pas être irréductible.

1. Attention, la notion d'irréductibilité dépend dramatiquement du corps sur lequel on se trouve. On dit « irréductible sur le corps $\mathbb{K}$ », même chose pour le polynôme minimal d'un élément $\alpha$ : il dépend du corps et il n'est irréductible que sur le corps considéré. Par exemple $\mu_{\beta,\mathbb{L}}$ divise $\mu_{\beta,\mathbb{K}}$, ce qui prouve que $\mu_{\beta,\mathbb{K}}$ n'est *a priori* plus irréductible sur $\mathbb{L}$ (il peut l'être *a posteriori*).
2. Attention aux corps finis. Le piège le plus énorme est de croire que $\mathbb{F}_4$ est égal à $\mathbb{Z}/4\mathbb{Z}$. Il faut savoir répondre à la question « Pourquoi ne sont-ils pas isomorphes ? ».
3. Toujours les corps finis. Ne pas croire, par exemple, que $\mathbb{F}_4$ est inclus dans $\mathbb{F}_8$. En fait $\mathbb{F}_{q^m}$ est inclus dans $\mathbb{F}_{q^n}$ si et seulement si $m$ divise $n$. Notez que, par Bezout, l'intersection $\mathbb{F}_{q^m} \cap \mathbb{F}_{q^n} = \mathbb{F}_{q^d}$, où $d$ est le PGCD de $m$ et $n$.
4. Le nombre $i$ habite dans le corps des complexes. Ecrire, par exemple, $\mathbb{F}_5[i]$ ne veut rien dire, sinon que le candidat est en pleine confusion des genres. Dans le même ordre d'idées, les racines de $X^2 + 1 = 0$ sur $\mathbb{F}_5$ sont $\pm 2$.
5. Ne pas confondre corps de rupture et corps de décomposition sur $\mathbb{K}$. Le premier s'adresse aux polynômes irréductibles sur $\mathbb{K}$ (et assure, *a priori* qu'une seule racine), le second s'adresse à tous les polynômes, et englobe toutes les racines.
6. Tant qu'on est dans les corps de ruptures : attention, le corps de rupture est unique *à isomorphisme près*. Penser à titre de contre-exemple classique, au corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$. Il y a $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$. Ils sont isomorphes mais bien distincts.

## I. Les fondamentaux

1. Tout corps contient un unique sous-corps premier qui définit la caractéristique du corps.
2. Connaître la notion d'élément algébrique et transcendant sur un corps. Il y a, à l'inverse, la notion de corps de rupture : pour tout polynôme irréductible $P$ sur $\mathbb{K}$, il existe une extension finie de $\mathbb{K}$, unique à isomorphisme près qui contient une racine de $P$, et minimale.
3. Il y a deux opérations sur les extensions finies de $\mathbb{K}$ : l'intersection et le produit. L'intersection est claire, le produit l'est moins. Par récurrence à l'aide du degré, on voit que toute extension finie est engendrée par un nombre fini d'éléments [2]. Cela permet de définir, pour deux extensions

2. En fait, avec l'hypothèse de séparabilité, on peut se ramener à un seul élément.

$\mathbb{L}$ et $\mathbb{L}'$ de $\mathbb{K}$ l'extension

$$\mathbb{L}\mathbb{L}' := \{\sum_i l_i l'_i,\ l_i \in \mathbb{L},\ l'_i \in \mathbb{L}'\}.$$

On voit que c'est un corps car si $\mathbb{L}' := \mathbb{K}[\alpha_1]\cdots[\alpha_k]$, alors $\mathbb{L}\mathbb{L}' := \mathbb{L}[\alpha_1]\cdots[\alpha_k]$. C'est alors une extension finie. Cette notion est fondamentale pour passer du corps de rupture (qui demande un polynôme irréductible) au corps de décomposition (que l'on peut voir comme un produit de corps de ruptures), puis, à la clôture algébrique (que l'on peut voir comme une limite infinie de corps de décompositions).

4. Le degré d'une extension $\mathbb{K}[\alpha]$ est le degré du polynôme minimal de $\alpha$. Et inversement, un polynôme annulateur de $\alpha$ de degré $[\mathbb{K}[\alpha] : \mathbb{K}]$ est minimal, donc irréductible sur $\mathbb{K}$ ! Il faut bien mettre en valeur cette façon de déceler qu'un polynôme est irréductible.
5. Le théorème de la base téléscopique. Il introduit une divisibilité dans les degrés d'extensions intermédiaires, d'où un lien très utile avec l'arithmétique.
6. L'existence et l'unicité d'une clôture algébrique pour $\mathbb{K}$ (cela utilise le lemme de Zorn).
7. Le corps fini $\mathbb{F}_q$, avec $q = p^n$, $p$ premier, est, par définition, le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. On voit facilement (par une double inclusion) que c'est aussi l'ensemble des racines de $X^q - X$ ; on a l'unicité d'un corps à $q$ élément à isomorphisme près.
8. Si un polynôme unitaire sur $\mathbb{Z}[X]$ possède une réduction $\overline{P}$ irréductible modulo $p$, alors il est irréductible sur $\mathbb{Z}$ et sur $\mathbb{Q}$. Ceci justifie, entre autres, l'étude des corps finis $\mathbb{F}_p$ et de leurs extensions $\mathbb{F}_q$.
9. Ne pas louper les extensions cyclotomiques $\mathbb{Q}[\zeta_n]$, où $\zeta_n$ désigne une racine primitive $n$-ième de l'unité. Le polynôme minimal de $\zeta_n$ sur $\mathbb{Q}$ est le polynôme cyclotomique $\phi_n$. Les extensions cyclotomiques prennent toute leur importance dans la théorie des représentations des groupes finis, en particulier, dans la théorie des caractères, à travers le théorème de Lagrange des groupes finis (tout caractère est somme de valeurs propres et donc dans $\mathbb{Q}[\zeta_n]$).
10. La notion d'automorphisme d'une extension $\mathbb{L}$ fixant le corps $\mathbb{K}$, même sans parler de théorie de Galois, est fondamentale. Si on pose $G$ le groupe de ces automorphismes [3], on a des propriétés très utiles :

3. Penser que si $L = \mathbb{C}$ et $\mathbb{K} = \mathbb{R}$, on a le groupe $Z/2\mathbb{Z}$ constitué de l'identité et de $z \mapsto \overline{z}$.

(a) un critère qui dit, que sous certaines conditions (normalité-séparabilité), qu'un élément de $\mathbb{L}$ est dans $\mathbb{K}$ si et seulement s'il est $G$-invariant [4],

(b) une façon de fabriquer des racines d'un polynôme $P \in \mathbb{K}[X]$ à partir d'une seule, en faisant agir $G$ sur la racine [5].

(c) Mieux ! La décomposition de $P$ en irréductibles correspond exactement à la décomposition en $G$-orbites de l'ensemble de ses racines !

Evidemment, ces jolies propriétés demandent des hypothèses restrictives sur l'extension : être normale et séparable (extension galoisienne). La théorie dit alors que dans ce cas, les extensions intermédiaires entre $\mathbb{K}$ et $\mathbb{L}$ sont en bijection avec les sous-groupes de $G$. Mais on peut très bien ne pas faire de théorie de Galois si on garde tout de même en tête les principes cités ci-dessus.

## II. Questions classiques du jury

1. Pouvez-vous construire le corps $\mathbb{F}_4$ comme corps de rupture ?
   *Il faut trouver un polynôme irréductible sur $\mathbb{F}_2$ de degré 2, $X^2+X+1$ est en fait le seul !*
2. Y a-t-il des extensions intermédiaires entre $\mathbb{Q}$ et $\mathbb{Q}(\sqrt[3]{2})$ ?
   *Non, car le degré est le nombre premier 3. C'est lié au fait que $X^3-2$ est irréductible sur $\mathbb{Q}$ par le critère d'Eisenstein.*
3. Quel est le degré de l'extension $\mathbb{Q}[i+\sqrt{2}]$ sur $\mathbb{Q}$ ?
   *Par une considération de degrés, l'inclusion $\mathbb{Q}[i+\sqrt{2}] \subset \mathbb{Q}[\sqrt{2}, i]$ est une égalité. On trouve donc $2 \times 2 = 4$ par la base téléscopique.*
4. Connaissez-vous des corps algébriquement clos ?... et à part $\mathbb{C}$ ? Quelle est la clôture algébrique de $\mathbb{Q}$ ? celle de $\mathbb{F}_p$ ?
   *$\mathbb{C}$, le corps $\overline{\mathbb{Q}}$ des entiers algébriques sur $\mathbb{Q}$, la réunion $\cup_{n\geq 1}\mathbb{F}_{p^n}$.*
5. Montrer que $X^3+X+1$ est irréductible sur $\mathbb{F}_2$, puis, irréductible sur $\mathbb{F}_{16}$.
   *Ce polynôme est de degré 3 et n'a pas de racine sur $\mathbb{F}_2$, il est irréductible sur $\mathbb{F}_2$. On montre ensuite grâce au lemme de Gauss et à la base téléscopique que si $\alpha$ est une racine, $\mathbb{F}_{16}[\alpha]$ est de degré 3 sur $\mathbb{F}_{16}$, d'où l'irréductibilité.*
6. Montrer que le polynôme $X^5-X-1$ est irréductible sur $\mathbb{Q}$.

4. Par exemple, un nombre complexe est réel ssi il est bar-invariant.

5. Par exemple, si $P$ est un polynôme réel, si $\alpha$ est racine, $\overline{\alpha}$ l'est également. Et c'est encore plus fort sur $\mathbb{F}_q$ avec le Frobenius : si $\alpha$ est racine de $P \in \mathbb{F}_q[X]$, $\overline{\alpha}^q$ l'est également, on peut itérer le processus.

*Il suffit de le montrer sur $\mathbb{Z}$ car $\mathbb{Z}$ est factoriel, et pour ce faire, on montre qu'il est irréductible sur $\mathbb{F}_5$. Faire agir le Frobenius sur l'ensemble des racines du polynôme s'avère utile.*

7. Pouvez-vous déterminer le corps $\mathbb{F}_3(\alpha)$, où $\alpha$ est une racine primitive 7-ième de 1 ?
   *Pareil, on fait agir le Frobenius. L'orbite de $\alpha$ est $\{\alpha, \alpha^3, \alpha^2, \alpha^6, \alpha^4, \alpha^5\}$. Donc, le polynôme $\phi_7$ reste irréductible modulo 3 et $\mathbb{F}_3(\alpha) = \mathbb{F}_{3^6}$.*
8. Soit $\alpha$ une racine du polynôme $P$ sur $\mathbb{K}[X]$. On suppose $[\mathbb{K}(\alpha) : \mathbb{K}] > \deg P/2$. Montrer que $P$ est irréductible.
   *Il n'y a plus d'extension intermidiaire une fois passée le degré $\deg P/2$. Donc, le degré est bien $\deg P$, d'où l'irréductibilité du polynôme.*

**IV. Les développements**

1. Irréductibilité de $\phi_n$ sur $\mathbb{Z}$, [1]. Niveau : 4/5 Originalité : 3/5
2. Si le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est non cyclique, alors le polynôme $\phi_n$ n'est plus irréductible modulo $p$, et ce, pour tout $p$ premier, [2, Exercice 4.2.24]. Niveau : 4/5 Originalité : 4/5
3. La table des caractères du groupe de pemutations $\mathfrak{S}_n$ ne possède que des valeurs entières, [3, Exercice E.41]. Niveau : 4/5 Originalité : 5/5
4. Il y a un zéro dans toute ligne de la table de caractères irréductibles d'un groupe fini correspondant à une représentation de degré $> 1$, [3, Exercice E.36]. Niveau : 5/5 Originalité : 5/5
5. Algorithme de Berlekamp. Niveau : 4/5 Originalité : 3/5
6. La preuve par la réduction que $\mathbb{C}$ algébriquement clos, [2, Exercice 1.3.21] Niveau : 4/5 Originalité : 5/5
7. Le théorème de Springer qui affirme que si une forme quadratique sur $\mathbb{K}$ possède un vecteur isotrope non nul dans une extension de degré impair de $\mathbb{K}$, alors elle possède un vecteur isotrope non nul sur $\mathbb{K}$, [2, Exercice 2.5.3]. Niveau : 4/5 Originalité : 5/5.

# Références


[1] Daniel Perrin. *Cours d'algèbre.* Collection CAPES/agrégation. Éditions Ellipses, 1997.

[2] Philippe Caldero et Marie Peronnier. *Carnet de Voyage en Algébrie.* Calvage et Mounet, 2019.

[3] Philippe Caldero et Jérôme Germoni. *Nouvelles Histoires Hédonistes de Groupes et de Géométries, tome second.* Calvage et Mounet, 2018.