

EXTENSIONS DE CORPS

Leçons directement concernées (2019)

- (123) Corps finis. Applications.
- (125)* Extensions de corps. Exemples et applications.
- (141) Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Leçons directement liées, dans lesquelles on peut parler d'extensions de corps (2019)

- (122)* Anneaux principaux. Applications.
- (151) Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.
- (153) Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.
- (157) Endomorphismes trigonalisables. Endomorphismes nilpotents.

Leçons où des extensions de corps peuvent également apparaître sporadiquement (2019)

- (102)* Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.
- (126) Exemples d'équations en arithmétique.
- (142)* PGCD et PPCM, algorithmes de calcul. Applications.
- (144)* Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.
- (154)* Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications.

Ce qui est dans le programme

- (c) Corps, sous-corps. Caractéristique, morphisme de Frobenius. Extension de corps. Corps des fractions d'un anneau intègre. Le corps \mathbb{Q} des nombres rationnels. Le corps \mathbb{R} des nombres réels. Le corps \mathbb{C} des nombres complexes. Théorème de d'Alembert-Gauss. Éléments algébriques et transcendants. Extensions algébriques. Corps algébriquement clos. Corps de rupture et corps de décomposition. Corps finis.

Bibliographie

- À suivre...

Ce polycopié présente les notions de base sur les extensions de corps et leurs applications (incluant les corps finis), allant jusqu'à la préparation de la théorie de Galois.

Tous les corps considérés seront commutatifs, et on désigne toujours par K un corps de base fixé.

1 Extensions

1.1 Généralités

On rappelle qu'un morphisme de corps n'est rien d'autre qu'un morphisme d'anneau $K \rightarrow L$ entre deux corps K et L . En particulier, tout morphisme de corps est injectif.

Définition 1.1. Une *extension de corps* L de K , notée L/K , est la donnée d'un corps L et, de manière équivalente,

- (i) d'un morphisme de corps $\iota : K \rightarrow L$;
- (ii) d'une structure de K -espace vectoriel sur L .

Pour faciliter les notations, on supposera souvent que $K \subset L$ en tant qu'ensembles. Le morphisme de corps est alors l'inclusion, et la structure de K -espace vectoriel est celle donnée par multiplication par les éléments de K dans L .

Une *sous-extension de L/K* est un sous-corps M de L contenant K . Autrement dit, on a deux extensions de corps $L/M/K$.

Exercice 1. Vérifier l'équivalence, et pourquoi on peut toujours se ramener à $K \subset L$.

1.2 Degré

Définition 1.2 (Degré). L'extension L/K est dite *finie* si L est de dimension finie en tant que K -espace vectoriel, et est dite *infinie* sinon. On appelle *degré de l'extension*, noté $[L : K]$, cette dimension.

Fait 1.3. Si L/K est une extension finie et si M en est une sous-extension, alors les extensions L/M et M/K sont finies.

Démonstration. L'extension M/K est finie car M est un sous- K -espace vectoriel de L . Si $(e_i)_{1 \leq i \leq n}$ est une base de L sur K , alors c'est une famille génératrice de l'espace vectoriel L sur M . \square

La réciproque de ce résultat est vraie et plus précise :

Proposition 1.4 (Théorème de la base télescopique).

Soient M/L et L/K deux extensions finies. On pose $(e_i)_{i \in I}$ une K -base de L et $(f_j)_{j \in J}$ une L -base de M . Alors, $(e_i f_j)_{(i,j) \in I \times J}$ est une K -base de M .

En particulier, M/K est une extension finie et $[M : K] = [M : L][L : K]$.

Démonstration. Soit $m \in M$. Par hypothèse, on peut écrire $m = \sum_{j \in J} \mu_j f_j$, $\mu_j \in L$.

Ensuite, par hypothèse sur L , pour tout $j \in J$, on peut écrire $\mu_j = \sum_{i \in I} \lambda_{i,j} e_i$.

Alors, on a $m = \sum_{\substack{i \in I \\ j \in J}} \lambda_{i,j} e_i f_j$, ce qui prouve que la famille $(e_i f_j)_{i,j}$ est K -génératrice de M .

Réciproquement, supposons qu'on a une telle écriture pour $m = 0$. Montrons que les $\lambda_{i,j}$ sont tous nuls. On écrit $0 = \sum_{j \in J} (\sum_{i \in I} \lambda_{i,j} e_i) f_j$. Alors, par liberté de $(f_j)_j$, pour tout $j \in J$, on a $\sum_{i \in I} \lambda_{i,j} e_i = 0$, et donc les $\lambda_{i,j}$ sont tous nuls par liberté de $(e_i)_i$. On a donc bien prouvé que notre famille est une K -base, et le reste en découle directement. \square

Exemple 1.5. Le corps \mathbb{C} est une extension de \mathbb{R} finie de degré 2 et \mathbb{R} est une extension infinie de \mathbb{Q} pour des raisons de cardinalité.

1.3 Morphismes

Définition 1.6 (Morphismes).

Si L/K et L'/K sont deux extensions de K , on appelle K -morphisme $\sigma : L \rightarrow L'$ un morphisme de corps qui est, de plus, K -linéaire (ce qui revient à dire qu'il est l'identité sur K si $K \subset L, L'$).

Si σ est un isomorphisme, son inverse est également K -linéaire et on parle alors d'*isomorphisme de K -extensions*.

En particulier, les automorphismes de L/K sont les automorphismes K -linéaires de L , on note leur ensemble $\text{Aut}_K(L)$.

Exemple 1.7. On a $\text{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\text{id}_{\mathbb{C}}, \iota\}$ où ι est la conjugaison complexe. En effet, un élément $f \in \text{Aut}_{\mathbb{R}}(\mathbb{C})$ vérifie $f(i)^2 = f(i^2) = f(-1) = -1$ car $-1 \in \mathbb{R}$ doit être fixé. Donc $f(i) = \pm i$ car c'est une racine du polynôme $X^2 + 1$ dans \mathbb{C} . Comme $(1, i)$ est une \mathbb{R} -base de \mathbb{C} et que f est \mathbb{R} -linéaire, ceci détermine entièrement f .

En revanche, c'est un problème difficile – et ouvert – de décrire $\text{Aut}_{\mathbb{Q}}(\mathbb{C})$.

Exercice 2.

1. Montrer que $\text{Aut}_{\mathbb{Q}}(\mathbb{R}) = \{\text{id}_{\mathbb{R}}\}$.
2. (Plus difficile) Montrer que $\text{Aut}_{\mathbb{Q}}(\mathbb{R}(X)) \simeq \text{PGL}_2(\mathbb{R})$.

Indication : On pourra caractériser \mathbb{R}_+ dans $\mathbb{R}(X)$ comme l'ensemble des éléments qui admettent une racine n -ème pour tout $n \in \mathbb{N}^*$.

2 Corps de rupture

Voici une construction naturelle d'extension de corps. Avant de la poser, on donne le lemme suivant, car il sera utilisé à répétition (et sans mention explicite) dans la suite.

Lemme 2.1. Soient A et A' deux K -algèbres unitaires commutatives. Alors, pour tout morphisme de K -algèbres $\sigma : A \rightarrow A'$, tout polynôme $Q \in K[X]$ et tout $a \in A$, on a $Q(\sigma(a)) = \sigma(Q(a))$.

En particulier, si $A = K[a]$ pour un certain a , un tel morphisme σ est entièrement déterminé par $\sigma(a)$.

Démonstration. C'est une conséquence immédiate de la propriété universelle des anneaux de polynômes : Soit $a \in A$. Il existe deux morphismes de K -algèbres $\varphi_1 : K[X] \rightarrow A$ et $\varphi_2 : K[X] \rightarrow A'$ uniquement déterminés par $\varphi_1(X) = a$ et $\varphi_2(X) = \sigma(a) = \sigma \circ \varphi_1(X)$. Ainsi le diagramme suivant commute :

$$\begin{array}{ccc} A & \xrightarrow{\sigma} & A' \\ & \swarrow \varphi_1 & \nearrow \varphi_2 \\ & K[X] & \end{array}$$

□

Définition 2.2. Soit $P \in K[X]$ irréductible. Le *corps de rupture* de P sur K est le corps $K[X]/(P)$.

Fait 2.3. (1) C'est une extension de corps de K de degré $\deg P$.

(2) Pour toute extension L/K , les K -morphisms $\sigma : K[X]/(P) \rightarrow L$ sont en bijection avec les racines de P dans L via l'application $\sigma \mapsto \sigma(\bar{X})$. Le corps de rupture est ainsi « la plus petite extension contenant une racine de P ».

Démonstration. (1) Tout d'abord, $K[X]/(P)$ est bien un corps car P étant irréductible, l'idéal (P) est maximal dans l'anneau principal $K[X]$. La structure d'extension de K peut se voir alternativement comme la structure K -linéaire naturelle, ou bien l'image de K via la projection canonique $K[X] \rightarrow K[X]/(P)$.

(2) Soit maintenant une extension L/K . Si σ est un K -morphisme de $K[X]/(P)$ dans L alors, par construction, pour tout polynôme Q de $K[X]$ et tout $x \in K[X]/(P)$ on a $\sigma(Q(x)) = Q(\sigma(x))$. En particulier, pour $x = \bar{X}$ et $Q = P$, on a $P(\sigma(\bar{X})) = \sigma(P(\bar{X})) = \sigma(\bar{P}) = 0$. Donc $\sigma(\bar{X})$ est bien une racine de P dans L .

Réciproquement, si x est une racine de P dans L , le morphisme d'évaluation $K[X] \rightarrow L$ qui à Q associe $Q(x)$ est un morphisme d'anneaux, et son noyau contient (P) par hypothèse, d'où la factorisation $K[X]/(P) \rightarrow L$. □

Exemple 2.4. Le corps \mathbb{C} est isomorphe au corps de rupture de $X^2 + 1$ sur \mathbb{R} .

Les corps $\mathbb{Q}(\sqrt[3]{2})$ et $\mathbb{Q}(j\sqrt[3]{2})$, où j est une racine primitive 3-ème de l'unité, sont isomorphes car isomorphes au corps de rupture de $X^3 + 2$ sur \mathbb{Q} .

Exercice 3. Montrer que -1 n'est pas un carré dans $\mathbb{Q}(j\sqrt[3]{2})$.

Indication : on pourra contempler la non quadrature de -1 dans \mathbb{R} .

3 Générateurs

Lorsqu'on s'intéresse à une extension de corps, on essaie, comme souvent, de la décrire la plus simplement possible, donc par générateurs.

Définition 3.1 (Générateurs).

Soit L une extension de K et S une partie de L . On note $K(S)$ la plus petite sous-extension de L contenant S (par exemple l'intersection de toutes ces sous-extensions). C'est également l'ensemble des fractions rationnelles en les éléments de S .

En particulier, pour tout $x \in L$, on note $K(x)$ l'extension engendrée par x . On dit que L/K est engendrée par x si $L = K(x)$.

Remarque 3.2. Attention, le fait d'être engendré par une certaine famille dépend du corps de base ! Penser à $L = L(1)$ par exemple, ou un peu plus subtilement à \mathbb{C}/\mathbb{Q} comparée à \mathbb{C}/\mathbb{R} .

Exercice 4. Trouver des générateurs de \mathbb{C}/\mathbb{R} et $K(X)/K$ autres que i et X .

3.1 Éléments algébriques et transcendants

Maintenant qu'on a affaire à des générateurs, il s'agit de comprendre la structure d'un $K(x)$.

Définition 3.3 (Éléments algébriques ou transcendants). Soit L/K une extension de corps et $x \in L$. On considère le morphisme d'évaluation donné par la propriété universelle des algèbres de polynômes $\Psi : P \in K[X] \mapsto P(x) \in L$.

- Un élément de L est dit *transcendant sur K* si le morphisme Ψ est injectif et il est dit *algébrique* dans le cas contraire.
- Si x est algébrique, on appelle *polynôme minimal de x sur K* , noté $\mu_{x,K}$, le polynôme unitaire qui engendre l'idéal $\ker \Psi$ de l'anneau principal $K[X]$.
- Si x est algébrique, on appelle *degré* de x le degré du polynôme $\mu_{x,K}$ et sinon, on dit que le degré de x est infini sur K .

Proposition 3.4. Soit L/K une extension de corps et $x \in L$.

- Si $x \in L$ est algébrique, alors $\mu_{x,K}$ est irréductible. De plus, le corps $K(x)$ est égal à $K[x] = \text{im } \Psi$, l'ensemble des polynômes en x , lui-même K -isomorphe à $K[X]/(P)$. Enfin, le degré de x est exactement $[K(x) : K]$.
- Si $x \in L$ est transcendant sur K , alors $K(x)$ est K -isomorphe à $K(X)$, en particulier de dimension infinie.
- Un élément $x \in L$ est donc algébrique si et seulement si $K(x)/K$ est finie.

Démonstration. Le polynôme minimal est irréductible ici car si $(QR)(x) = 0$, par intégrité $Q(x) = 0$ ou $R(x) = 0$.

Ensuite, si x est algébrique, le morphisme naturel du corps de rupture de P vers L qui à \bar{X} associe x a pour image exactement $K[x]$, d'où l'isomorphisme. L'égalité dimension/degré en découle.

Si x est transcendant, le morphisme d'anneaux intègres $\Psi : K[X] \rightarrow L$ est injectif donc il s'étend en un morphisme de corps $\tilde{\Psi} : K(X) \rightarrow L$ d'image $K(x)$ dans L . D'où l'isomorphisme. \square

3.2 Extensions algébriques et transcendants

Définition 3.5. Une extension L/K est dite *algébrique* si tous ses éléments sont algébriques, et *transcendante* sinon. Elle est *purement transcendante* si tous les éléments de $L \setminus K$ sont transcendants.

Exemple 3.6. 1. Les corps de rupture sont des extensions algébriques.

2. $K(X, Y) = K(X)(Y)$ est purement transcendante sur K .

3. $\mathbb{C}(X)$ est purement transcendante sur \mathbb{C} mais pas sur \mathbb{R} .

On peut maintenant formuler et démontrer une forme d'unicité du corps de rupture

Définition 3.7. Une extension L/K est un *corps de rupture* de $P \in K[X]$ irréductible si elle est de la forme $L = K[x]$ avec x une racine de P dans L . Tous les corps de rupture de P sont K -isomorphes.

Démonstration. Soit L un corps de rupture de P et x une racine de P dans L telle que $L = K[x]$. Alors, par la construction originale du corps de rupture, on a un K -morphisme $K[X]/(P) \rightarrow L$ envoyant \bar{X} sur x , mais il est surjectif par hypothèse, donc c'est un isomorphisme, ce qui prouve par transitivité le résultat. \square

Proposition 3.8. *Toute extension finie L/K est algébrique.*

Réciproquement, une extension L/K est algébrique si, et seulement si, elle est réunion de ses sous-extensions finies.

De plus, si $x, y \in L$ sont algébriques sur K , alors $x + y$ et xy le sont également.

Ainsi, l'ensemble des éléments algébriques de L sur K est une sous-extension de L .

Démonstration. Soit L/K une extension finie de degré n et $x \in L$. Par hypothèse, la famille $(1, x, \dots, x^n)$, de cardinal $n + 1$, est nécessairement K -liée, d'où l'existence d'un polynôme annulateur de x (de degré au plus n), celui-ci est donc algébrique.

Réciproquement, si L/K est algébrique, alors chaque $x \in L$ est contenu dans l'extension finie $K[x]/K$.

Prenons maintenant $x, y \in L$ algébriques sur K . Alors, y est algébrique sur le corps $K[x]$, car il l'est déjà sur K . On a donc $K[x][y]/K$ finie, mais cette extension contient entre autres $x + y$ et xy , donc ceux-ci sont algébriques par le raisonnement précédent.

Enfin, x^{-1} est algébrique car $K(x^{-1}) = K(x)$ qui est une extension finie de K . \square

Exercice 5.

1. Soit L une extension de K et x, y algébriques sur K de degrés respectifs m et n premiers entre eux. Montrer que $[K(x, y) : K] = mn$.
2. Soient M/L et L/K deux extensions de corps. Montrer que si L/K est algébrique, tout $x \in M$ algébrique sur L est également algébrique sur K .

Exercice 6.

1. Calculer les polynômes minimaux de \sqrt{d} pour tout entier $d \in \mathbb{Z}$ (on choisit une racine carrée de d dans \mathbb{C}), et en déduire les degrés des $\mathbb{Q}(\sqrt{d})$ sur \mathbb{Q} . Faire de même pour d'autres racines n -ièmes d'entiers de votre choix.
2. Montrer que pour tout corps K , l'extension $K(X)/K$ est purement transcendante. Montrer que toute extension purement transcendante de K engendrée par un seul élément est en fait celle-ci.
3. Montrer que l'extension \mathbb{R}/\mathbb{Q} est transcendante mais n'est pas purement transcendante.
4. Soit L/K une extension algébrique et $\sigma : L \rightarrow L$ un morphisme de corps K -linéaire. En raisonnant sur toutes les racines des polynômes minimaux d'éléments de x , montrer que σ est automatiquement un automorphisme.

3.3 Nombres transcendants

On va maintenant donner des exemples « explicites » de nombres transcendants. Culturellement, on sait qu'il est en général très difficile de savoir si un nombre est transcendant ou non, et même, l'irrationalité de certaines valeurs pose souvent problème. Par exemple, on sait que e et π sont transcendants, mais que c'est assez difficile à démontrer, que $\zeta(2n)$ est transcendant pour $n \in \mathbb{N}^*$ (c'est difficile : ça fait intervenir les nombres de Bernoulli et les puissances paires de π et qu'on ne sait rien dire sur l'algébricité, ou non, de $\zeta(2n + 1)$).

D'un point de vue théorie des ensemble, les nombres complexes algébriques sur \mathbb{Q} sont en quantité dénombrable car l'ensemble des polynômes irréductible de $\mathbb{Q}[X]$ est lui-même dénombrable. Donc, en un certain sens, presque tout nombre complexe est transcendant et pourtant la plupart des nombres qu'on est amené à écrire sont algébriques !

Théorème 3.9 (Liouville). *Soit $\alpha \in \mathbb{C}$ algébrique irrationnel de degré d sur \mathbb{Q} . Alors il existe une constante $C > 0$ telle que pour tout rationnel $\frac{a}{b}$, on a l'inégalité $|\alpha - \frac{a}{b}| \geq \frac{C}{b^d}$.*

Démonstration. Soit $\mu_{\alpha, \mathbb{Q}} \in \mathbb{Q}[X]$ le polynôme minimal de α sur \mathbb{Q} de degré d . On fixe $m \geq 1$ tel que $P = m\mu_{\alpha, \mathbb{Q}} \in \mathbb{Z}[X]$. Pour toute fraction $\frac{a}{b} \in \mathbb{Q}$, par l'égalité des accroissements finis, il existe $y \in [\alpha, \frac{a}{b}]$ (ou l'intervalle inverse) tel que

$$\left| P\left(\frac{a}{b}\right) \right| = \left| P(\alpha) - P\left(\frac{a}{b}\right) \right| = \left| \alpha - \frac{a}{b} \right| |P'(y)|.$$

Mais comme P est à coefficients entiers et n'annule pas $\frac{a}{b}$ (sinon, comme il est irréductible, il serait de degré 1, or α est irrationnel), on a $\left| P\left(\frac{a}{b}\right) \right| \geq \frac{1}{b^d}$. On a donc $\left| \alpha - \frac{a}{b} \right| \geq \frac{1}{q^d |P'(y)|}$. Il suffit alors de poser

$$C = \min\left(1, \min_{|y-1| \leq 1} \frac{1}{|P'(y)|}\right) \text{ pour conclure.} \quad \square$$

Exercice 7. On appelle *nombre de Liouville* tout nombre réel α tel que pour tout $d \geq 2$ et tout $C > 0$, il existe un rationnel $\frac{a}{b}$ tel que $0 < \left| \alpha - \frac{a}{b} \right| < Cb^{-d}$.

1. Montrer que tout nombre de Liouville est transcendant.
2. Donner un exemple direct de nombre de Liouville.
3. Montrer que l'ensemble des nombres de Liouville est de mesure de Lebesgue nulle, mais que l'ensemble des réels transcendants est de mesure pleine.

4 Scindage des polynômes

La construction par corps de rupture revient à s'autoriser l'adjonction d'une racine d'un polynôme irréductible. Cependant, ce procédé ne suffit pas à ajouter toutes les racines d'un polynôme. Typiquement $\mathbb{Q}(\sqrt[3]{2})$ ne contient pas toutes les racines de $X^3 - 2$ bien que c'en soit un corps de rupture sur \mathbb{Q} .

4.1 Clôture algébrique

Définition 4.1. Un corps L est dit *algébriquement clos* si tous les polynômes irréductibles de $L[X]$ sont de degré 1 (ce qui revient à dire qu'il n'admet aucune extension algébrique/finie non triviale).

Une *clôture algébrique* du corps K est une extension L/K qui est à la fois algébrique et algébriquement close.

Exemple 4.2. Le corps \mathbb{C} est algébriquement clos, et l'ensemble des nombres complexes algébriques sur \mathbb{Q} est une clôture algébrique de \mathbb{Q} .

Théorème 4.3. *Il existe toujours une telle extension, souvent notée \overline{K} , et les clôtures algébriques de K sont toujours K -isomorphes deux à deux.*

Construction de la clôture algébrique. La démonstration de l'existence et de l'unicité est proposée en exercice (cf. TD), comme suit :

On fixe un corps K quelconque.

1. Soit S l'ensemble des polynômes irréductibles de $K[X]$. On pose $A = K[(X_P)_{P \in S}]$ et I l'idéal de A engendré par les $P(X_P)$, $P \in S$. Montrer que $I \neq A$.
2. En prenant \mathfrak{m} un idéal maximal de A contenant I , montrer que dans l'extension $K_1 = A/\mathfrak{m}$ de K , tout polynôme irréductible de $K[X]$ a une racine.
3. Itérer le procédé pour construire une suite d'extensions de corps

$$K \subset K_1 \subset K_2 \subset \dots$$

et montrer que $K_\infty = \bigcup_{n \in \mathbb{N}} K_n$ est un corps algébriquement clos.

4. En posant \overline{K} l'ensemble des éléments de K_∞ algébriques sur K , montrer que \overline{K} est bien une clôture algébrique de K .
5. Pour toute extension algébrique L de K , montrer qu'il existe un plongement de L dans \overline{K} prolongeant l'inclusion $K \subset \overline{K}$. En déduire que la clôture algébrique de K est unique à isomorphisme près.
6. Montrer que pour toute extension finie L de \overline{K} , il existe au plus $[L : K]$ plongements K -linéaires distincts de L dans \overline{K} .
7. On note $[L : K]_s$ le nombre de ces plongements. Montrer que pour une extension finie M de L , on a $[M : K]_s = [M : L]_s [L : K]_s$ (utile pour l'exercice sur les extensions séparables).

□

4.2 Corps de décomposition

Plutôt que de manipuler impunément la clôture algébrique (qui relève en général de l'axiome du choix), on peut se concentrer sur une autre manière d'avoir les racines d'un polynôme : le corps de décomposition.

Définition 4.4 (Corps de décomposition). Soit $P \in K[X]$. Un *corps de décomposition* de P sur K est une extension (finie) L de K telle que P est scindé de racines $\alpha_1, \dots, \alpha_r$ sur K et que

$$L = K(\alpha_1, \dots, \alpha_r).$$

Exercice 8. Donner des corps de décomposition de $X^4 - 1$ et $X^3 - 2$ sur \mathbb{Q} .

Proposition 4.5. Soit $P \in K[X]$. Il existe toujours un corps de décomposition de P sur K , et si L et L' sont deux tels corps, il existe un K -isomorphisme entre L et L' . On s'autorise donc souvent à dire « le » corps de décomposition de P .

Démonstration. La preuve de l'existence, est relativement directe. Si P n'est pas scindé sur K (auquel cas K convient), soit Q un facteur irréductible de P sur $K[X]$. Alors, dans K_1 le corps de rupture de Q sur K , le polynôme P admet une racine, notée α , et $K_1 = K[\alpha]$. On a donc

$$P = (X - \alpha)P_1, \quad P_1 \in K_1[X].$$

On recommence avec un facteur irréductible de P_1 si celui-ci n'est pas scindé sur K_1 , ce qui donne une tour d'extensions

$$K \subset K_1 \subset \dots \subset K_d$$

où d est majoré par le degré de P (vu que le degré du polynôme considéré décroît de 1 à chaque étape). Par construction, K_d est une extension dans laquelle P devient scindé, et on n'a utilisé que des racines de P pour l'engendrer, donc c'est bien un corps de décomposition.

La preuve de l'unicité est un peu plus subtile et requiert une définition supplémentaire. Supposons qu'on a un isomorphisme de corps $i : K \rightarrow K'$ et des extensions respectives L et L' de K et K' . Alors un i -isomorphisme $\sigma : L \rightarrow L'$ est un isomorphisme de corps entre L et L' tel que pour tous $\lambda \in K, x \in L$,

$$\sigma(\lambda x) = i(\lambda)\sigma(x).$$

Pour tout polynôme $P \in K[X]$, on note $i(P) \in K'[X]$ le polynôme obtenu en appliquant i à chacun de ses coefficients. On va alors montrer le lemme suivant :

Lemme 4.6. Pour tous corps K, K' , tout $i : K \rightarrow K'$ isomorphisme, et tout polynôme $P \in K[X]$, si L et L' sont des corps de décomposition respectivement de P sur K et $i(P)$ sur K' , alors il existe un i -isomorphisme $\sigma : L \rightarrow L'$.

Ce lemme, appliqué à $K' = K$ et i l'identité, implique bien l'unicité des corps de décomposition, et on va le démontrer par récurrence sur le degré de P .

Si P est constant ou de degré 1, il n'y a rien à faire car forcément ses racines appartiennent au corps de base donc $L = K$ et $L' = K'$.

Supposons maintenant que le lemme est vrai pour tout polynôme (et tous corps notés comme ci-dessus) de degré n . Soit $P \in K[X]$ de degré $n + 1$, soit L un corps de décomposition de P sur K et L' un corps de décomposition de P sur K' , avec $i : K \rightarrow K'$ un isomorphisme de corps.

Alors, en prenant une racine α_1 de P dans L , considérons son polynôme minimal P_1 sur K . Il est irréductible sur K donc $i(P_1)$ est irréductible sur K' , mais par ailleurs il divise $i(P)$ qui est scindé sur L' par hypothèse. Il existe donc α'_1 une racine de $i(P_1)$ dans L' .

On peut alors construire un i -isomorphisme j entre $K[\alpha_1]$ et $K'[\alpha'_1]$, en envoyant α_1 sur α'_1 (en passant par les corps de rupture respectifs de P_1 et $i(P_1)$). Mais par hypothèse, L est alors un corps de décomposition de $P/(X - \alpha_1)$ sur $K[\alpha_1]$, et de même pour L' et $i(P)/(X - \alpha'_1) = j(P/(X - \alpha_1))$. On peut donc appliquer l'hypothèse de récurrence à ce polynôme, aux extensions et à j , ce qui conclut la preuve. \square

Exercice 9. Montrer que le corps de décomposition d'un polynôme de degré au plus n sur K est de degré au plus $n!$ sur K .

Exercice 10. Décrire les corps de décomposition de $X^3 + X + 1$, $X^4 - 2$, $X^5 - 3$ et $X^n - 1$ sur \mathbb{Q} .

L'unicité du corps de décomposition a une application très importante : les corps finis. Rendez-vous très bientôt en cours d'option C!

4.3 Frobeniusseries

Commençons par une remarque préliminaire :

Fait 4.7. Soit L/K une extension de corps. Alors $\text{car}(L) = \text{car}(K)$.

Démonstration. Le morphisme canonique $\mathbb{Z} \rightarrow K$ s'étend par composition par l'injection $K \rightarrow L$ en le morphisme canonique $\mathbb{Z} \rightarrow L$. Ces morphismes ont donc même noyau définissant la caractéristique de ces deux corps. \square

Soit K un corps et $P \in K[X] \setminus \{0\}$ un polynôme unitaire. Soit $p = \text{car}(K)$.

Fait 4.8. Si $p = 0$, alors $P' = 0 \iff P = 1$.

Si $p > 0$, alors $P' = 0 \iff \exists Q \in K[X] \setminus \{0\}$ unitaire tel que $P = Q \circ X^p$.

Démonstration. Si $p = 0$, alors le coefficient de P' est n qui n'est pas égal à 0 dans K .

Si $p > 0$, écrivons $P = \sum_k a_k X^k$ et $P' = \sum_k k a_k X^{k-1}$. Alors pour tout $k \wedge p = 1$, on a $k a_k = 0$ donc $a_k = 0$. Ainsi $P = \sum_{k=pl} a_{pl} X^l \circ X^p$ et on prend $Q = \sum_{k=pl} a_{pl} X^l$. Réciproquement $(Q \circ X^p)' = Q' \circ X^p \cdot (pX^{p-1}) = 0$. \square

Lemme 4.9. Si p est un nombre premier, alors $p \mid \binom{p}{k}$ pour tout $k \in \llbracket 1, p-1 \rrbracket$.

Démonstration. On observe que pour tout $1 \leq k \leq p-1$, on a $v_p(k) = 0$ et, en particulier, $v_p(k!) = 0$.

Ainsi $v_p \left(\binom{p}{k} \right) = v_p \left(p \frac{(p-1)!}{k!(p-k)!} \right) = 1$. \square

Remarque 4.10. Ceci est en général faux lorsque p n'est pas premier. Par exemple, 4 ne divise pas $6 = \binom{4}{2}$.

Si $p > 0$, on définit l'application suivante appelée *morphisme de Frobenius* par :

$$F_K : K \rightarrow K \\ x \mapsto x^p$$

Si le corps K est clair dans le contexte, on le notera plus simplement F .

Fait 4.11. On suppose $p = \text{car}(K) > 0$.

(1) Le morphisme de Frobenius F est un morphisme de corps, donc injectif.

(2) De plus, on a $(P(X))^p = P(X^p)$ pour tout polynôme $P \in K[X]$.

(3) Si $m \in \mathbb{N}^*$, alors l'ensemble des points fixés par $F^m = F \circ \dots \circ F$ est un sous-corps fini de K .

Démonstration. (1) Il suffit de montrer que c'est stable par addition et multiplication. Or $F(x+y) = (x+y)^p = \sum_{k=0}^p \binom{p}{k} x^k y^{p-k} = x^p + y^p = F(x) + F(y)$ et $F(xy) = (xy)^p = x^p y^p = F(x)F(y)$. Enfin $F(1) = 1^p = 1$.

(2) Il suffit de prendre l'endomorphisme de Frobenius du corps $K(X)$ qui est aussi de caractéristique p .

(3) L'ensemble A des points fixes de F^m est l'ensemble des racines du polynôme $X^{p^m} - X$ dans K , donc est fini. On observe immédiatement que A est un sous-anneau de K , donc intègre. De plus, si $a \in A \setminus \{0\}$, alors $a^{p^m} = a$ donne $a^{p^m-2}a = 1$ donc a est inversible. \square

Remarque 4.12. En général le noyau de $F^m - \text{Id}$ n'est cependant pas un corps à p^m éléments mais un corps plus petit.

Définition 4.13. Un corps K est dit *parfait* s'il est de caractéristique 0 ou si l'endomorphisme de Frobenius est un automorphisme de K .

Un polynôme est dit *séparable* s'il est à racines simples dans son corps de décomposition.

On dispose alors des résultats suivants que l'on démontrera en exercice :

Proposition 4.14. Soit K un corps de caractéristique p et $P \in \mathbb{K}[X]$ un polynôme unitaire.

1. Le polynôme P est séparable si et seulement si P et P' sont premiers entre eux.

2. Les corps finis et les corps algébriquement clos sont parfaits.

3. Si le corps K est parfait et si le polynôme P est irréductible, alors P est séparable.

Exercice 11. Soit $L = \mathbb{F}_p(T)$ et K l'image du morphisme de Frobenius F_L . Montrer que le polynôme $X^p - T^p \in K[X]$ est irréductible sur K mais pas sur L et qu'il n'est pas séparable.