Corps et extensions de corps

Baptiste Calmès

1er février 2021

Table des matières

1 Corps

Dans ce cours, tous les anneaux seront supposés unitaires, et les morphismes d'anneaux seront supposés respecter l'unité, sauf mention explicite.

Rappelons rapidement la définition d'un corps, ainsi que quelques exemples.

1.1 Définition. Un *corps* est un anneau unitaire dans lequel $0 \neq 1$ et tous les éléments sauf 0 sont inversibles.

Dans ce cours, tous les corps seront implicitement supposés *commutatifs*.

1.2 Définition. Lorsque K et L sont des corps tels que $K \subset L$ par une inclusion d'anneaux, alors on dit que K est un *sous-corps* de L et que L est un *sur-corps* de K.

1.3 Lemme. *Tout morphisme d'anneaux (unitaires) d'un corps K vers un anneau $A \neq \{0\}$ est injectif.*

1.4 Remarque. Un tel morphisme vérifie donc automatiquement que si x est inversible, $f(x)$ l'est et $f(x)^{-1} = f(x^{-1})$.

1.5 Définition. Si K et L sont des corps, un *morphisme de corps* $f : K \to L$ est un morphisme d'anneaux unitaires de K vers L (automatiquement injectif par le lemme précédent).

1.6 Exercice. Le seul morphisme de corps $\mathbb{Q} \to \mathbb{Q}$ est l'identité.

1.7 Exercice. La conjugaison complexe est un (iso)morphisme de corps $\mathbb{C} \to \mathbb{C}$. C'est l'unique morphisme de corps $\mathbb{C} \to \mathbb{C}$ différent de l'identité qui fixe tout élément de $\mathbb{R}$.

1.8 Définition. La caractéristique d'un corps K (ou plus généralement d'un anneau) est le plus petit entier $n \geq 1$, s'il existe, tel que $0 = 1 + \cdots + 1$ (n fois). S'il n'existe pas, on dit que le corps est de caractéristique 0. On la note $\mathrm{car}(K)$.

1.9 Lemme. *Si K est un corps (ou plus généralement un anneau intègre), alors soit $\mathrm{car}(K) = 0$, soit $\mathrm{car}(K)$ est un nombre premier.*

1.10 Exemple. Les corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique nulle. Si p est un nombre premier, l'anneau $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est un corps de caractéristique p (il est de plus fini).

⚠ Il existe des corps de caractéristique $p > 0$ qui ne sont pas finis, par exemple les fractions rationnelles à coefficients dans $\mathbb{F}_p$.

1.11 Exercice. Le seul morphisme de corps $\mathbb{F}_p \to \mathbb{F}_p$ est l'identité.

1.12 Proposition. *Tout corps de caractéristique nulle contient un unique sous-corps isomorphe à $\mathbb{Q}$. Tout corps de caractéristique $p > 0$ contient un unique sous-corps isomorphe à $\mathbb{F}_p$. Dans les deux cas, un tel isomorphisme est unique.*

1.13 Remarque. On dit alors souvent, par un léger abus de terminologie, qu'un corps "contient $\mathbb{Q}$" ou bien "contient $\mathbb{F}_p$", selon sa caractéristique.

2 Algèbres

2.1 Définition (algèbre)**.** Une algèbre sur un corps K, aussi appelée K-algèbre, est la donnée d'un anneau A et d'un morphisme d'anneaux $\phi : K \to A$ (automatiquement injectif si $A \neq \{0\}$ par le lemme 1.3).

Par notre convention sur les anneaux, toute les algèbres dans ce cours sont donc implicitement commutatives. Mais vous connaissez des algèbres non commutatives, par exemple les matrices $A = \mathrm{M}_n(K)$ avec $n > 1$.

2.2 Exemple. Lorsqu'un corps K est contenu dans un autre corps L, alors L (muni de l'inclusion) est une algèbre sur K. Par exemple, $\mathbb{C}$ est une algèbre sur $\mathbb{R}$, et $\mathbb{R}$ est une algèbre sur $\mathbb{Q}$.

2.3 Exemple. Si K est un corps, les polynômes $K[X]$ (munis de l'inclusion évidente de K comme polynômes constants) forment une algèbre sur K. De même, les fractions rationnelles $K(X)$ forment une algèbre sur K (qui contient la précédente).

2.4 Exemple. Si $P \in K[X]$ est un polynôme non nul, et si (P) désigne l'idéal de $K[X]$ engendré par P, alors $K[X]/(P)$ est une K-algèbre. C'est l'algèbre nulle si $\deg(P) = 0$ et elle est canoniquement isomorphe à $K[X]$ si $P = 0$ (donc de degré $-\infty$).

2.5 Lemme. *L'algèbre $K[X]/(P)$ est un corps si et seulement si P est irréductible.*

Remarquez que cette preuve est la même que celle qui montre que $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est nombre premier, et qu'elle donne un algorithme pour trouver l'inverse d'un élément non nul dans $K[X]/(P)$.

2.6 Définition. Si (A, ϕ) et (B, ψ) sont des K-algèbres, alors un morphisme de K-algèbres $(A, \phi) \to (B, \psi)$ est un morphisme d'anneaux $f : A \to B$ tel que $f \circ \phi = \psi$.

On vérifie immédiatement qu'un tel morphisme est injectif si et seulement si son noyau est réduit à 0, et qu'il est un isomorphisme (i.e. qu'il admet un morphisme inverse) si et seulement s'il est injectif et surjectif.

2.7 Proposition (propriété universelle des polynômes)**.** *Soit (A, ϕ) une K-algèbre et soit $a \in A$. Alors il existe un unique morphisme de K-algèbres $f : K[X] \to A$ tel que $f(X) = a$. De même, si $a_1, \ldots, a_n \in A$, il existe un unique morphisme de K-algèbres $f : K[X_1, \ldots, X_n] \to A$ tel que $f(X_1) = a_1$, $f(X_2) = a_2$, etc.*

Autrement dit, pour définir un morphisme de K-algèbres de $K[X]$ vers une K-algèbre A, il suffit de dire sur quoi on envoie X.

2.8 Corollaire. *Soit $P \in K[X]$, et soit P_ϕ son image dans $A[X]$ par ϕ. Si $P_\phi(a) = 0$, il existe un unique morphisme $\bar{f} : K[X]/(P) \to A$ tel que $\bar{f}(\bar{X}) = a$, et si $P_\phi(a) \neq 0$, il n'en existe pas.*

2.9 Exercice. Montrer que $\mathbb{R}[X]/(X^2 + 1)$ est un corps, et qu'il est isomorphe au corps $\mathbb{C}$.

2.10 Proposition (propriété universelle des fractions rationelles)**.** *Soit (A, ϕ) une K-algèbre et soit $a \in A$. Alors le morphisme $K[X] \to A$ envoyant X sur a s'étend en un unique morphisme de K-algèbres $f : K(X) \to A$ si et seulement si pour tout $P \in K[X]$, $P \neq 0$, l'élément $P_\phi(a)$ est inversible dans A.*

Voyons quelques techniques pour vérifier si un polynôme est irréductible.

Un élément p dans un anneau R est dit *premier* s'il engendre un idéal premier, c'est-à-dire si le quotient $R/(p)$ est intègre. Un élément p est dit *irréductible* s'il n'est pas inversible et ne peut s'écrire comme un produit de deux éléments non inversibles. Un anneau est *factoriel* s'il est intègre et si tout élément non nul se décompose de manière unique en produit d'éléments premiers, à éléments inversibles près ; la notion d'élément *premier* se confond alors avec la notion d'élément *irréductible*. Soit R un anneau (intègre) factoriel de corps des fractions K. Ce peut être par exemple un anneau principal.

2.11 Lemme. *Un polynôme $P \in R[X]$ est irréductible si et seulement si soit*

- *il est de degré 0 et premier dans R ;*
- *il est primitif (pgcd des coefficients est 1) et irréductible dans $K[X]$.*

2.12 Lemme (Critère d'Eisenstein)**.** *Soit $P = \sum_{i=0}^{n} a_i X^i$ un polynôme dans $R[X]$, où R est factoriel. S'il existe $p \in R$ premier tel que*

$$\begin{cases} p|a_i \text{ pour } 0 \leq i \leq (n-1) \text{ mais } p \not| a_n \\ p^2 \not| a_0 \end{cases}$$

alors P est irréductible dans $R[X]$. Il sera donc irréductible dans $K[X]$ s'il est de plus primitif.

2.13 Remarque. Ceci permet de fabriquer énormément de polynômes irréductibles P dans $\mathbb{Q}[X]$, et donc énormément de nouveaux corps de la forme $\mathbb{Q}[X]/(P)$.

2.14 Lemme. *Soient L un corps et $f : R \to L$ un morphisme d'anneaux (toujours avec R factoriel). Soit $P \in R[X]$ primitif. Si $f(P) \in L[X]$ est irréductible et $f(a_n) \neq 0$, alors P est irréductible dans $R[X]$ et donc irréductible dans $K[X]$.*

2.15 Exercice. Montrer que $\frac{1}{2}X^3 + 10X + 5$ est irréductible dans $\mathbb{Q}[X]$.

Soit (A, ϕ) une K-algèbre.

2.16 Définition (sous-algèbre)**.** Une sous-algèbre de A est la donnée d'un sous-anneau B de A tel que $\phi(K) \subset B$.

2.17 Définition (sous-algèbre engendrée par un élément)**.** On appelle sous-algèbre engendrée par $a \in A$ la plus petite sous-algèbre de A qui contient a. On la note $K[a]$ (lorsque A est claire par le contexte). De même, lorsque $a_1, \ldots, a_n \in A$, on note $K[a_1, \ldots, a_n]$ la plus petite sous-algèbre de A contenant $\{a_1, \ldots, a_n\}$.

2.18 Lemme. *La sous-algèbre $K[a]$ est égale à l'ensemble des éléments de A qui peuvent s'écrire $P_\phi(a)$ pour un polynôme $P \in K[X]$, ou encore à l'image de l'unique morphisme de K-algèbre $K[X] \to A$ envoyant X vers a obtenu par la propriété universelle 2.7.*

2.19 Définition. S'il existe un polynôme $P \in K[X]$ non nul tel que $P_\phi(a) = 0$, on dit que a est *algébrique*. S'il n'en existe pas, on dit que a est *transcendant*.

Considérons l'idéal I_a de $K[X]$ défini par

$$I_a = \{P \in K[X] \text{ t.q. } P_\phi(a) = 0\}.$$

Si a est algébrique (ce qui est équivalent à $I_a \neq \{0\}$ par définition), $\exists! P_a \neq 0$ unitaire tel que $I_a = (P_a)$.

2.20 Définition. On appelle ce polynôme le *polynôme minimal* de a.

2.21 Proposition. *Si l'algèbre A est intègre alors*

1. *soit a est algébrique, son polynôme minimal P_a est irréductible, $K[a]$ est un corps et $X \mapsto a$ définit un isomorphisme de K-algèbres de $K[X]/(P_a)$ vers $K[a]$;*
2. *soit au contraire a est transcendant, et $K[a]$ est isomorphe à $K[X]$ (et n'est pas un corps).*

3 Extensions de corps

3.1 Définition. Une *extension* d'un corps K est une K algèbre (L, ϕ) telle que L est un corps (rappel : ϕ est alors automatiquement injectif).

On omet souvent la mention de ϕ, et on parle souvent d'une extension L/K pour dire que L est une extension de K.

⚠ Un morphisme de corps $K \hookrightarrow K$ n'est pas forcément surjectif. Le morphisme $k(X) \to k(X)$ envoyant X sur X^2 n'atteint pas X. En caractéristique p, on a aussi le Frobénius $x \mapsto x^p$, défini sur tout corps de caractéristique p, et qui n'est pas surjectif si $K = \mathbb{F}_p(X)$, puisque X n'est pas atteint.

3.2 Remarque. Lorsque K est un sous-corps de L, on a une extension évidente (L, i) sur K, où i est l'inclusion $K \subset L$.

3.3 Proposition. *Lorsque (L, ϕ) est une extension de K, alors l'image $\phi(K)$ dans L est un sous-corps de L et ϕ induit un isomorphisme de corps de K vers $\phi(K)$.*

On identifie parfois K à ce sous-corps par ϕ, sauf quand on s'intéresse justement aux différents ϕ possibles.

3.4 Définition. Une *sous-extension* d'une extension $\phi : K \hookrightarrow L$ est une sous-algèbre de L qui est un corps. Autrement dit, c'est un sous-corps F de L contenant $\phi(K)$, qu'on peut donc voir naturellement comme une extension $\phi : K \hookrightarrow F$.

Étant donné que l'intersection d'une famille de sous-corps est un sous-corps de manière évidente, on peut poser :

3.5 Définition. Soit (L, ϕ) une extension du corps K. Soit $(x_i)_{i \in I}$ une famille d'éléments de L. On appelle *sous-corps engendré par la famille* (x_i) et on note $K(x_i, i \in I)$ le plus petit sous-corps de L contenant $\phi(K)$.

3.6 Proposition. *Soit x un élément de L. Alors de deux choses l'une :*

— *soit x est algébrique et $K[x] = K(x)$.*

— *soit x est transcendant et $K(x)$ est isomorphe au corps des fractions rationnelles $K(X)$.*

Une K-algèbre est naturellement munie d'une structure de K-espace vectoriel.

3.7 Définition. On appelle *degré* d'une K-algèbre A (par exemple une extension de corps) la dimension de A comme K-espace vectoriel. On la note $[A : K]$. C'est donc soit un nombre entier non nul soit ∞. Lorsque $[A : K]$ est fini, on dit que A est *finie*.

Si L/K est une extension de corps et A est une L algèbre, alors on peut considérer A comme une K-algèbre.

3.8 Proposition. *A est une K-algèbre finie si et seulement si elle est finie sur L et L est fini sur K. On a alors $[A : L][L : K] = [A : K]$.*

3.9 Théorème. *Si A est une K-algèbre (commutative)* intègre *finie, c'est un corps et tous ses éléments sont algébriques.*

3.10 Définition (Extension algébrique)**.** Une extension de corps L/K dont tous les éléments sont algébriques est appelée une extension algébrique.

3.11 Lemme. *Toute extension finie est algébrique.*

⚠ Il existe des extensions algébriques qui ne sont pas finies. Par exemple, comme nous allons le voir, l'ensemble $\overline{\mathbb{Q}}$ des complexes qui sont algébriques est un sous-corps de $\mathbb{C}$ qui n'est pas fini comme extension de $\mathbb{Q}$.

3.12 Théorème. *Soit A une K-algèbre commutative intègre et $a_1, \ldots, a_n$ des éléments de A. Les conditions suivantes sont équivalentes :*

1. *Pour tout i, l'élément a_i est algébrique ;*
2. *Pour tout i, la K-algèbre $K[a_i]$ est finie ;*
3. *La K-algèbre $K[a_1, \ldots, a_n]$ est finie ;*
4. *$K[a_1, \ldots, a_n]$ est une extension de corps algébrique de K.*

3.13 Corollaire. *Si x et y dans une K-algèbre A intègre sont algébriques sur K, alors il en est de même de $x+y$, de xy, et si $y \neq 0$, il est inversible et x/y est également algébrique. En particulier, l'ensemble des éléments de A algébriques sur K est un sous-corps de A.*

3.14 Corollaire. *Soient M/L et L/K deux extensions de corps, avec L/K algébrique. Alors $x \in M$ est algébrique sur L si et seulement s'il est algébrique sur K. En particulier, M/L et L/K sont algébriques si et seulement si M/K est algébrique.*

4 Décomposition des polynômes

Soit P un polynôme non constant dans $K[X]$. Bien entendu, en général, P ne se décompose pas en facteurs de degré 1, autrement dit, toutes les racines de P n'existent pas dans K. On s'intéresse maintenant au plus petit corps possible dans lequel P possède toutes ses racines.

4.1 Définition (Extension de décomposition)**.** On dit qu'une extension L/K est une extension de décomposition pour P si

— P se décompose en produit de facteurs de degré 1 dans L et

— il n'existe pas de sous-extension stricte de L pour laquelle c'est encore le cas.

4.2 Remarque. De manière analogue, on dit qu'un sur-corps L de K est un corps de décomposition si vu comme extension L/K, c'est une extension de décomposition, autrement dit, P se décompose en produit de facteurs de degré 1 dans L mais il n'existe pas de corps L' avec $K \subset L' \subsetneq L$ pour lequel c'est déjà le cas.

4.3 Remarque. Soient E/K et L/E des extensions. Si la composée L/K est une extension de décomposition de P, alors L/E est une extension de décomposition de P sur E.

4.4 Proposition. *L'extension L/K est de décomposition pour un polynôme P de degré n si et seulement si P se décompose dans $L[X]$ en produit*

$$\lambda \prod_{i=1}^{n} (X - \alpha_i),\ \lambda \in K,\ \alpha_i \in L\ \forall i$$

et $L = K[\alpha_1, \ldots, \alpha_n]$. En particulier, L/K est algébrique et finie.

4.5 Corollaire. *Supposons que $P = QR$ dans $K[X]$. Supposons également que L/K est une extension de décomposition de Q et que M/L est une extension de décomposition de R (vu dans $L[X]$). Alors l'extension composée M/K est une extension de décomposition de P.*

4.6 Lemme. *Soit Q un facteur irréductible d'un polynôme $P \in K[X]$ et soit L/K une extension de décomposition de P. Notons E l'extension $K[X]/(Q)$. Alors on peut factoriser L/K en L/E et E/K, et L/E est une extension de décomposition de P sur E.*

4.7 Théorème. *Il existe un corps de décomposition de P, et si L_1/K et L_2/K sont deux corps de décomposition de P, il existe un isomorphisme d'extensions $L_1 \to L_2$.*

Autrement dit, un corps de décomposition est unique à isomorphisme près.

4.8 Remarque. On peut généraliser la définition d'une extension de décomposition au cas d'une famille de polynômes. Quand la famille est finie, cela se ramène à un seul polynôme, en considérant le produit. Quand elle ne l'est pas, il faut plus de travail en montrer l'existence, et ce n'est plus une extension finie en général. Elle reste toutefois algébrique, et est toujours unique à isomorphisme près.

5 Clôture algébrique

5.1 Définition (corps algébriquement clos)**.** On dit qu'un corps est algébriquement clos si tout polynôme dessus qui est non constant a une racine.

5.2 Remarque. De manière équivalente, tout polynôme non constant est scindé, ou encore tout polynôme irréductible est de degré 1.

5.3 Exemple. Le corps $\mathbb{C}$ est algébriquement clos (voir ci-après), mais pas $\mathbb{R}$, puisque X^2+1 n'a pas de racine dans $\mathbb{R}$. Les corps finis ne sont pas algébriquement clos.

5.4 Lemme. *Un corps est algébriquement clos si et seulement s'il n'a pas d'extension algébrique non triviale (i.e. toute extension algébrique est en fait un isomorphisme).*

5.5 Lemme. *Soit Ω/K une extension algébrique. Pour que Ω soit algébriquement clos, il faut et il suffit que tout polynôme non constant dans $K[X]$ se décompose en facteurs de degrés 1 dans Ω.*

5.6 Théorème. *Soit K un corps (infini) et soit E un corps de décomposition de X^2+1. On suppose que :*

- *tout polynôme dans $K[X]$ de degré impair a une racine dans E ;*
- *tout polynôme dans $K[X]$ de degré 2 a une racine dans E.*

Alors E est algébriquement clos.

5.7 Corollaire (théorème fondamental de l'algèbre)**.** *Le corps $\mathbb{C}$ est algébriquement clos.*

5.8 Définition (clôture algébrique)**.** On dit qu'une extension Ω/K est une clôture algébrique de K si elle est algébrique et si Ω est algébriquement clos.

5.9 Exemple. L'extension $\mathbb{C}/\mathbb{R}$ est une clôture algébrique de $\mathbb{R}$. Par contre, $\mathbb{C}/\mathbb{Q}$ n'est pas une clôture algébrique de $\mathbb{Q}$, parce que ce n'en est pas une extension algébrique.

⚠ Attention, une clôture algébrique peut, pour certains corps, être une extension finie (comme dans le cas $\mathbb{C}/\mathbb{R}$), mais cela peut également être une extension de degré infini (bien qu'algébrique), comme pour la clôture algébrique de $\mathbb{Q}$.

5.10 Proposition. *Pour qu'une extension Ω/K soit une clôture algébrique de K, il faut et il suffit qu'elle soit algébrique et que tout polynôme non constant de $K[X]$ se décompose en facteurs de degrés 1 dans Ω.*

5.11 Proposition. *Si $\phi : K \hookrightarrow L$ est une extension finie, et si $\omega : K \hookrightarrow \Omega$ est une clôture algébrique, alors il existe une extension $\psi : L \hookrightarrow \Omega$ telle que $\omega = \psi \circ \phi$, autrement dit telle que Ω/K soit la composée de Ω/L et L/K. De plus, dans ce cas, ψ fait alors de Ω une clôture algébrique de L.*

5.12 Remarque. Cette proposition est en fait vraie plus généralement si L/K est algébrique (pas nécessairement finie).

⚠ Il n'y a pas unicité d'un tel ψ. Par exemple, si $K=\mathbb{R}$ de clôture algébrique $\mathbb{C}$, alors si on prend $L=\mathbb{C}$ également, on peut prendre comme ψ l'identité ou la conjugaison complexe.

Le théorème suivant est vrai, mais sa preuve est un peu technique :

5.13 Théorème (Steinitz)**.** *Tout corps K admet une clôture algébrique et elle est unique à K-isomorphisme d'extension près.*

À la place, nous utiliserons en pratique le plus souvent la proposition suivante.

5.14 Proposition. *Soit C un corps algébriquement clos. Soit $K \subset C$ un sous-corps de C. Posons $\Omega = \{x \in C,\ x \text{ algébrique sur } K\}$. Alors $K \subset \Omega$ est une clôture algébrique de K et c'est l'unique sous-corps de C ayant cette propriété.*

5.15 Exemple. Le sous-corps $\overline{\mathbb{Q}} \subset \mathbb{C}$ constitué des éléments algébriques sur $\mathbb{Q}$ est la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$.

6 Extensions normales

6.1 Définition (extension normale)**.** Une extension L/K est dite normale si tout polynôme irréductible $P \in K[X]$ ayant une racine dans L a toutes ses racines dans L (autrement dit est décomposable en facteurs de degré 1 dans L).

6.2 Proposition. *Une extension d'un corps K est de degré fini et normale si et seulement si elle est une extension de décomposition d'un polynôme sur K.*

6.3 Proposition. *Soient M/L et L/K des extensions finies de corps. Si M/K est normale, alors M/L est normale.*

⚠ Attention, L/K n'est pas forcément normale.

6.4 Théorème. *Si $\mathrm{car}(K) = 0$, alors tout polynôme irréductible dans $K[X]$ est à racines simples dans une clôture algébrique de K.*

6.5 Remarque. Dans ce cours, nous nous restreindrons désormais souvent au cas où $\mathrm{car}(K) = 0$. La théorie marche très bien aussi lorsque $\mathrm{car}(K) > 0$, mais son exposition oblige à expliquer la notion d'extension *séparable* et toutes ses propriétés. En caractéristique 0, toute extension est séparable, il n'y a donc nul besoin de faire de distinction. Nous nous contenterons donc de signaler qu'une plus grande généralité existe en note de bas de page afin que le lecteur qui consulte la littérature ne soit pas déboussolé.

6.6 Théorème (de l'élément primitif, $\mathrm{car}(K) = 0$)**.** *Soit L/K une extension finie d'un corps K de car 0* [1]*. Alors il existe un élément $x \in L$ tel que $L = K[x]$.*

1. Plus généralement, ce théorème est vrai en caractéristique quelconque si l'on suppose l'extension séparable.