Algèbre 2

Cours de Vlerë Mehmeti*

0 Rappels sur les anneaux

0.1 Anneaux

Définition 0.1.1. Un *anneau* $(A, +, \cdot)$ est un ensemble muni de deux lois de composition internes $+$ et $\cdot$ telles que

(1) $(A, +)$ est un groupe abélien (on note son élément neutre 0_A)

(2) $\cdot$ est associative

(3) $\cdot$ se distribue sur $+$.

S'il existe un élément neutre pour $\cdot$, on le note 1_A et on dit que A est *unitaire*. Si $\cdot$ est commutatif, on dit que A est *commutatif*.

Remarque. Dans ce cours, sauf mention explicite, tout anneau considéré sera unitaire et commutatif.

Définition 0.1.2. Un élément $a \in A \setminus \{0\}$ est dit *un diviseur de zéro* s'il existe $b \in A \setminus \{0\}$ tel que $ab = 0$. Si A ne possède pas de diviseurs de zéros, on dit que A est *intègre*. Un élément $a \in A$ est dit *inversible* s'il existe $b \in A$ tel que $ab = ba = 1$. On notera l'ensemble des éléments inversibles $A^\times$.

Remarque.

(1) Si $a \in A^\times$ est inversible, l'élément $b \in A$ tel que $ab = 1$ est unique [1]. On le note a^{-1}.

(2) Un élément inversible n'est pas un diviseur de zéro.

Dans un anneau intègre A, pour tous $a, b \in A$, $ab = ac$ implique $a = 0$ ou $b = c$. En particulier, si $a \neq 0$, on peut simplifier par a.

Exemple 0.1.3. (1) $(\mathbb{Z}, +, \cdot)$ est un anneau.

(2) $(\mathbb{Z}[\sqrt{d}], +, \cdot)$ est un anneau.

(3) $(\mathbb{Z}/n\mathbb{Z}, +_n, \cdot_n)$ l'est aussi.

(4) $(\mathcal{M}_n(\mathbb{R}), +, \cdot)$ est un anneau non commutatif.

(5) L'anneau des quaternions $(\mathbb{H}_\mathbb{C}, +, \cdot)$ est aussi non commutatif.

Tous ces exemples sont des anneaux intègres.

*Notes originales trouvables à `https://webusers.imj-prg.fr/~vlere.mehmeti/teaching.html`

1. En effet, si $ab = b'a = 1$, alors $b' = b'ab = b$

(6) Si A, B sont des anneaux, alors $A \times B$ muni des lois produits (composante par composante) est un anneau en général non intègre car $(1_A, 0) \cdot (0, 1_B) = (0, 0)$. On peut généraliser à un produit quelconque d'anneaux.

(7) Soit A un anneau. Alors $(A[X], +, \cdot)$ est un anneau où $+, \cdot$ sont l'addition et la multiplication usuelle des polynômes à coefficients dans A. On peut définir récursivement, pour $n \in \mathbb{N}^*$, $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$, et les lois internes $+$ et $\cdot$ induites de celles de $A[X_1, \ldots, X_{n-1}]$. Par convention, pour $n = 0, A[X_1, \ldots, X_n] = A$.

(8) Soit A un anneau et X un ensemble. Alors $A^X = \{f \mid f : X \to A\}$ muni des lois données par

$$\begin{cases} (f+g)(x) & = f(x) +_A g(x) \\ (f \cdot g)(x) & = f(x) \cdot_A g(x) \end{cases}$$

est un anneau.

(9) L'ensemble $\{f : \mathbb{R} \to \mathbb{R} \mid \exists [a_f, b_f] \subseteq \mathbb{R}, f_{|[a_f, b_f]^c} = 0\}$ est un anneau.

(10) L'anneau nul $\{0\}$ est l'unique anneau où $0 = 1$.

Proposition 0.1.4. *Soit A un anneau. Alors*

(1) $a0 = 0a = 0$ *pour tout* $a \in A$

(2) $(-a)b = a(-b) = -(ab)$ *pour tous* $a, b \in A$

(3) $(-a)(-b) = ab$ *pour tous* $a, b \in A$

(4) $-a = (-1)a$ *pour tout* $a \in A$.

Définition 0.1.5. Un *sous-anneau* R d'un anneau $(A, +, \cdot)$ est un sous-groupe R de $(A, +)$ tel que pour tous $a, b \in R$, $ab \in R$.

Remarque. R est un sous-anneau si et seulement si $0 \in R$ (ou $R \neq \varnothing$) et pour tous $a, b \in R$, $a - b \in R$ et $ab \in R$.

Remarque. L'anneau nul n'est pas intègre.

Exemple 0.1.6.

(1) $n\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}$ pour tout $n \in \mathbb{Z}$.

(2) $(\mathbb{Q}, +, \cdot)$ est un anneau et $\{\frac{m}{n} \mid m, n \in \mathbb{Z} \setminus \{0\}, m \wedge n = 1, n \text{ impair}\} \cup \{0\}$ est un sous-anneau. Si on remplace « n impair » par « m impair », ce n'est plus le cas.

Définition 0.1.7. Un *morphisme d'anneaux unitaires* est une application $\varphi : A \to B$ telle que

(1) $\varphi(a + b) = \varphi(a) + \varphi(b)$

(2) $\varphi(ab) = \varphi(a)\varphi(b)$

(3) $\varphi(1_A) = 1_B$

Le morphisme φ est dit un *isomorphisme* s'il est bijectif.
Si φ est un isomorphisme et $A = B$, on dit que φ est un *automorphisme de A*.

Remarque. On notera par $\mathrm{Aut}(A)$ l'ensemble des automorphismes de A. Muni de la composition, c'est un groupe.

Proposition 0.1.8. *Soit $\varphi : A \to B$ un morphisme d'anneaux. Alors*

(1) $\mathrm{Im}(\varphi)$ *est un sous-anneau de* B.

(2) φ *est injectif si et seulement si*

$$\ker(\varphi) = \{a \in A \mid \varphi(a) = 0_B\} = \{0_A\}$$

Proposition 0.1.9. *Si* $\varphi : A \to B$ *et* $\psi : B \to C$ *sont deux morphismes d'anneaux, alors* $\psi \circ \varphi : A \to C$ *en est un aussi.*

Exemple 0.1.10.

(1) $\pi : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ m & \mapsto & m \mod n \end{array}$ est un morphisme d'anneaux (surjectif, mais pas injectif).

(2) $\psi_n : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z} \\ x & \mapsto & nx \end{array}$ n'est pas un morphisme d'anneaux unitaires si $n \neq 1$.

(3) $\theta : \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & \overline{z} \end{array}$ est un automorphisme de $\mathbb{C}$.

(4) $\begin{array}{ccc} \mathbb{Q}[X] & \to & \mathbb{Q} \\ P(X) & \mapsto & P(0) \end{array}$ est un morphisme d'anneaux (surjectif, non injectif).

(5) $\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z} \times \mathbb{Z} \\ (a,b) & \mapsto & (a,0) \end{array}$ n'est pas un morphisme d'anneaux unitaires.

Définition 0.1.11. Un *corps* est un anneau commutatif unitaire non nul où tout élément non nul est inversible.

Exemple 0.1.12.

(1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps (de nombres).

(2) Le corps des fractions rationnelles $\mathbb{Q}(T) = \{\frac{P}{Q} \mid P, Q \in \mathbb{Q}[T]\}$ est un corps.

(3) Le corps des nombres algébriques $\overline{Q} = \{x \in \mathbb{C} \mid \exists P \in \mathbb{Q}[X] \setminus \{0\}, P(x) = 0\}$ est un corps.

Définition 0.1.13. Soit A un anneau sans diviseur de zéro. Le *corps des fractions de* A, noté $\mathrm{Frac}\, A$, est

$$\left\{ \frac{a}{b} \,\middle|\, a \in A, b \in A \setminus \{0\} \right\} / \sim \quad \text{où} \quad \frac{a}{b} \sim \frac{c}{d} \iff ad - bc = 0$$

Proposition 0.1.14. *Les lois suivantes sont bien définies sur* $\mathrm{Frac}\, A$ *et en font un corps :*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

Proposition 0.1.15. *L'application* $\varphi : \begin{array}{ccc} A & \to & \mathrm{Frac}\, A \\ a & \mapsto & \frac{a}{1} \end{array}$ *est un morphisme d'anneaux injectif. Si* A *est un corps, c'est un isomorphisme.*

Remarque. $\mathrm{Frac}\, A$ est le plus petit corps contenant A.

Exemple 0.1.16.

(1) $\mathrm{Frac}\, \mathbb{Z} = \mathbb{Q}$

(2) Pour $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ a des diviseurs de zéro, sauf si n est premier et dans ce cas c'est un corps.

(3) $\mathrm{Frac}\, \mathbb{Q}[X] = \mathbb{Q}(X)$. Plus généralement, on définit $K(X_1, \ldots, X_n) = \mathrm{Frac}\, K[X_1, \ldots, X_n]$ pour K un corps.

0.2 Idéaux

Définition 0.2.1. Soit A un anneau (commutatif, unitaire). Un idéal de A est un sous-ensemble $I \subseteq A$ tel que

(1) $(I, +)$ est un sous-groupe de $(A, +)$

(2) Pour tous $a \in A$ et $b \in I$, $ab \in I$.

On note $I \lhd A$.

Remarque. Comme $(A, +)$ est un groupe abélien et I en est un sous-groupe, il est distingué, donc A/I est un groupe abélien muni de l'addition $(a + I) + (b + I) = (a + b) + I$.

Proposition 0.2.2. *Soit I un idéal de l'anneau A. Alors $(A/I, +, \cdot)$ est un anneau de loi multiplicative $(a + I)(b + I) = ab + I$. En particulier, cette opération est bien définie. On appelle A/I* l'anneau quotient de A par I. *De plus, la projection canonique* $\pi : \begin{array}{ccc} A & \to & A/I \\ x & \mapsto & x + I \end{array}$ *est un morphisme d'anneaux surjectif.*

Remarque. La définition d'idéal est précisément faite pour que la proposition ci-dessus fonctionne.

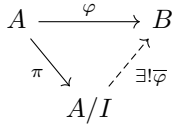
Théorème 0.2.3 (Premier théorème d'isomorphisme)**.**

(1) Si $\varphi : A \to B$ est un morphisme d'anneaux, alors $\ker \varphi$ *est un idéal de A et* $A/\ker \varphi \simeq \operatorname{im} \varphi$.

(2) Si I est un idéal de A alors $\pi : A \to A/I$ est surjective de noyau I.

Remarque. Les autres théorèmes d'isomorphisme fonctionnent aussi, par exemple si $I \subseteq J$ sont deux idéaux de A, alors $A/J \simeq (A/I)(J/I)$.

Théorème 0.2.4 (Propriété universelle du quotient)**.** *Soit $\varphi : A \to B$ un morphisme d'anneaux. Soit I un idéal de A tel que $\varphi(I) = \{0_B\}$. Alors il existe un unique $\overline{\varphi} : A/I \to B$ tel que $\varphi = \overline{\varphi} \circ \pi$ avec $\pi : A \to A/I$ la projection canonique.*



Exemple 0.2.5.

(1) $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$ pour $n \in \mathbb{N}$

(2) $\{0\}$ et A sont des idéaux de A

(3) $\{XP(X) \mid P \in \mathbb{Q}[X]\}$ est un idéal de $Q[X]$

Proposition 0.2.6. *Soit I un idéal de A. L'application*

$$\begin{array}{ccc} \{\text{idéaux de } A \text{ contenant } I\} & \to & \{\text{idéaux de } A/I\} \\ J & \mapsto & J/I \end{array}$$

est une bijection.

Démonstration. **TODO** □

Exemple 0.2.7. Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont $m\mathbb{Z}/n\mathbb{Z}$ tel que $m\mathbb{Z} \supseteq n\mathbb{Z}$ c'est-à-dire tels que $m \mid n$.

Proposition 0.2.8. *Un anneau A est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et A.*

Démonstration. Si A est un corps et $J \subseteq A$ un idéal non nul, alors J contient un élément $x \in A\setminus\{0\}$. Ainsi pour tout $a \in A$, $a = ax^{-1}x \in J$, donc $J = A$. Réciproquement, si les seuls idéaux de A sont $\{0\}$ et A, pour $x \in A \setminus \{0\}$, l'ensemble $\{ax \mid a \in A\}$ est un idéal non nul de A, donc égal à A, d'où il existe $a \in A$ tel que $ax = 1$. □

Corollaire 0.2.9. *Soit $A \neq 0$ un anneau et K un corps. Tout morphisme d'anneaux $\varphi : K \to A$ est injectif.*

Démonstration. Le noyau $\ker\varphi$ est un idéal de K et $1_K \notin \ker\varphi$ car $\varphi(1_K) = 1_A$ donc $\ker\varphi = \{0\}$. □

Proposition 0.2.10. *Une intersection d'idéaux est un idéal.*

Définition 0.2.11. Soit A un anneau et $S \subseteq A$. *L'idéal engendré par S* est le plus petit idéal de A contenant S. On le note (S).

Remarque.

(1) $(S) = \bigcap_{\substack{I \lhd A \\ S \subseteq I}} I$

(2) $(S) = \left\{ \sum_{\text{finie}} as \,\middle|\, a \in A, s \in S \right\}$

(3) Si $S = \{a\}$, alors $(a) = \{ax \mid x \in A\}$ et $(a) = A$ si et seulement si $a \in A^\times$ et $(a) = \{0\}$ si et seulement si $a = 0$.

Définition 0.2.12. Un idéal I de A est dit *principal* s'il existe $a \in A$ tel que $I = (a)$. Si A est intègre et que tout idéal de A est principal, A est dit *principal*. L'idéal I est dit de *type fini* s'il existe $S \subseteq A$ finie telle que $I = (S)$.

Remarque. Soit A intègre et $a, b \in A \setminus \{0\}$. Alors

$$(a) = (b) \iff \exists x \in A^\times, a = bx$$

Exemple 0.2.13.

(1) L'idéal (X, Y^2+1) de $\mathbb{Q}[X, Y]$ est celui des polynômes de la forme $P(X, Y)X+Q(X, Y)(Y^2+1)$ avec $P, Q \in \mathbb{Q}[X, Y]$.

(2) On a $(X, X - 1) = \mathbb{Q}[X]$ car $1 = X - (X - 1)$.

Remarque. Il est en général difficile de déterminer si un idéal est de type fini et de trouver un ensemble générateur. Un ensemble générateur d'un idéal n'est pas unique, par exemple $(1) = (X, X-1)$ ou $(X - Y, Y) = (X, Y) = (X, Y, X + Y)$.

0.3 Idéaux premiers et maximaux

Définition 0.3.1.

(1) Un idéal $\mathfrak{p}$ de A est dit *premier* si $\mathfrak{p} \neq A$ et pour tous $a, b \in A$, $ab \in \mathfrak{p}$ implique $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$.

(2) Un idéal $\mathfrak{m}$ de A est dit *maximal* si $\mathfrak{m} \neq A$ et que les seuls idéaux de A qui le contiennent sont $\mathfrak{m}$ et A.

Théorème 0.3.2.

(1) Un idéal $\mathfrak{p}$ de A est premier si et seulement si $A/\mathfrak{p}$ est intègre.

(2) Un idéal $\mathfrak{m}$ de A est maximal si et seulement si $A/\mathfrak{m}$ est un corps.

En particulier, tout idéal maximal est premier.

Démonstration. Soient $a, b \in A$. Alors, $(a + \mathfrak{p})(b + \mathfrak{p}) = \mathfrak{p}$ si et seulement si $ab \in \mathfrak{p}$ si et seulement si $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$ si et seulement si $(a + \mathfrak{p}) = \mathfrak{p}$ ou $b + \mathfrak{p} = \mathfrak{p}$. De cela découle (1).
On sait qu'on a une bijection entre les idéaux de A qui contiennent $\mathfrak{m}$ et les idéaux de $A/\mathfrak{m}$. De cette bijection et du fait que $A/\mathfrak{m}$ est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et lui-même, on déduit (2). □

Exemple 0.3.3.

(1) $n\mathbb{Z}$ est un idéal premier (ou maximal) de $\mathbb{Z}$ si et seulement si n est premier.

(2) $(P) \subseteq \mathbb{Q}[X_1, \ldots, X_n]$ est premier si et seulement si P nul ou irréductible c'est-à-dire non constant et que si $P = AB$, alors A ou B est constant.

(3) Si K est un corps, (X) est un idéal maximal de $K[X]$ car $K[X]/(X) \simeq K$ (premier théorème d'isomorphisme appliqué au morphisme d'évaluation en 0_K).

(4) Pour $\alpha_1, \ldots, \alpha_n \in K$, l'idéal $(X_1 - \alpha_1, \ldots, X_n - \alpha_n) \subseteq K[X_1, \ldots, X_n]$ est maximal.

Proposition 0.3.4. *Soit A un anneau commutatif unitaire. Tout idéal propre de A est inclus dans un idéal maximal.*

Démonstration. Soit I un idéal de A distinct de A. On considère $\mathcal{J} = \{J \lhd \mathrm{A} |\ I \subseteq J, J \neq A\}$. Par propreté de I, cet ensemble est non vide. Il est ordonné pour l'inclusion. Soit $\mathcal{A} \subseteq \mathcal{J}$ une partie de $\mathcal{J}$ totalement ordonnée pour l'inclusion. On pose $\bigcup_{J \in \mathcal{A}} J$. C'est un idéal car $\mathcal{A}$ est totalement ordonnée pour l'inclusion. De plus, pour tout $J \in \mathcal{A}$, $1 \notin J$, donc $1 \notin \bigcup_{J \in \mathcal{A}} J$. Ainsi, $\bigcup_{J \in \mathcal{A}} J$ est une borne supérieure de $\mathcal{A}$ dans $\mathcal{J}$. Cela démontre que $\mathcal{J}$ est un ensemble inductif. Ainsi, le lemme de Zorn donne l'existence d'un élément maximal $\mathfrak{m} \in \mathcal{J}$. Par l'absurde, si $\mathfrak{m}$ n'est pas un idéal maximal, on dispose de $J \neq A$ idéal qui contient strictement $\mathfrak{m}$. Cela contredit la maximalité de $\mathfrak{m}$ dans $(\mathcal{J}, \subseteq)$. □

Exemple 0.3.5.

(1) (X) est un idéal premier mais non maximal de $\mathbb{Z}[X]$.

(2) $(X, 2)$ est un idéal maximal de $\mathbb{Z}[X]$.

(3) $(\mathbb{Q}, +, \cdot_0)$ où $\cdot_0$ est définie par $a \cdot_0 b = 0$ pour tous $a, b \in \mathbb{Q}$ n'a pas d'idéaux maximaux. C'est un anneau non unitaire.

0.4 Anneaux principaux

Remarquons que $\mathbb{Z}$ est un exemple d'anneau principal et $\mathbb{Z}[X]$ un exemple d'anneau non-principal, car $(X, 2) \lhd \mathbb{Z}[X]$ n'est pas principal.

Proposition 0.4.1. *Soit A un anneau principal. Alors, un idéal propre (distinct de A) et non-trivial (distinct de $\{0\}$) est premier si et seulement s'il est maximal.*

Démonstration. Un idéal maximal est toujours premier. Soit (a) avec $a \in A$ un idéal premier. On a $(a) \neq A$. Soit $(b) \supseteq (a)$ un autre idéal le contenant. Alors, $a = bx$ avec $x \in A$. Par primalité de (a), ou bien $b \in (a)$, dans ce cas $(a) = (b)$, ou bien $x \in (a)$, dans ce cas $x = ay$ avec $y \in A$, donc $a = aby$, donc $by = 1$ par intégrité, donc $(b) = A$. Ainsi (a) est maximal. □

Définition 0.4.2. Pour $a, b \in A$, on dit que a *divise* b et on écrit $a \mid b$ s'il existe $x \in A$ tel que $b = ax$.

Remarque. Pour $a, b \in A$, $a \mid b$ équivaut à $(b) \subseteq (a)$. Si $x \in A^\times$, alors $x \mid a$ pour tout $a \in A$.

Brièvement, quelques rappels sur $K[X]$.

Théorème 0.4.3. *Soit K un corps. Alors $K[X]$ est un anneau principal.*

Théorème 0.4.4. *Soit K un corps. Pour tout polynôme $P \in K[X] \setminus \{0\}$, il existe une unique décomposition $P = \alpha \prod_{i=1}^{d} P_i^{n_i}$ (unique à permutation près des P_i) avec $\alpha \in K^\times$, P_i unitaires et irréductibles et deux à deux distincts.*

Lemme 0.4.5. *Un idéal (P) est premier si et seulement si $P = 0$ ou P est irréductible.*

Quelques rappels :

(1) L'algorithme de division euclidienne fonctionne dans $K[X]$.

(2) Si $P, Q \in K[X]$ alors leur PGCD est bien défini (à multiplication par un élément de $K^\times$ près) et $(P, Q) = (\mathrm{pgcd}(P, Q))$.

(3) Si $K \subseteq L$ avec L un corps, pour $P, Q \in K[X]$, on a $\mathrm{pgcd}_K(P, Q) = \mathrm{pgcd}_L(P, Q)$.

Référence : Abstract Algebra de Dummit and Foote.

1 Théorie des corps

1.1 Extensions de corps

Définition 1.1.1. Soit K un corps. Une *K-algèbre* est un anneau A muni d'un morphisme d'anneaux $i : K \to A$ (forcément injectif car K est un corps). Si $K \xrightarrow{i} A$ et $K \xrightarrow{j} B$ sont deux K-algèbres, un *morphisme de K-algèbres* (parfois appelé un *K-morphisme*) est un morphisme d'anneaux $\varphi : A \to B$ tel que $\varphi \circ i = j$.

Définition 1.1.2. Soit K un corps. Une *extension de corps de K* est un corps L muni d'un morphisme de corps $K \xrightarrow{\theta} L$. On écrit L/K. Une *sous-extension de L/K* est un corps E muni de morphismes de corps $K \xrightarrow{i} E \xrightarrow{j} L$ tels que $j \circ i = \theta$. On écrit $L/E/K$ et on parle de *tour de corps*.

Remarque. Comme le morphisme θ dans la définition précédente est injectif, on fait régulièrement l'abus de notation d'identifier K à $\theta(K)$ pour écrire $K \subseteq L$.

Exemple 1.1.3.

(1) $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$, $\mathbb{C}/\mathbb{R}$ sont des extensions de corps.

(2) $\begin{array}{ccc} \mathbb{Q}(i) & \to & \mathbb{C} \\ i & \mapsto & i \end{array}$ et $\begin{array}{ccc} \mathbb{Q}(i) & \to & \mathbb{C} \\ i & \mapsto & -i \end{array}$ sont deux $\mathbb{Q}$-morphismes (où $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$).

(3) $\begin{array}{ccc} \mathbb{Q}(\sqrt[3]{2}) & \to & \mathbb{C} \\ \sqrt[3]{2} & \mapsto & \sqrt[3]{2} \end{array}$ et $\begin{array}{ccc} \mathbb{Q}(\sqrt[3]{2}) & \to & \mathbb{C} \\ \sqrt[3]{2} & \mapsto & j\sqrt[3]{2} \end{array}$ sont deux $\mathbb{Q}$-morphismes, où $j^3 = 1$ et $j \neq 1$ et $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$.

(4) Pour $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ avec p premier, l'application Frob : $\begin{array}{ccc} \mathbb{F}_p(T) & \to & \mathbb{F}_p(T) \\ x & \mapsto & x^p \end{array}$ est un morphisme de corps (donc est injective) mais n'est pas surjective. Le fait que $\mathrm{Frob}(1) = 1$ et $\mathrm{Frob}(xy) = \mathrm{Frob}(x)\,\mathrm{Frob}(y)$ est clair. De plus,

$$(x + y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$$

Et par primalité de p et comme $p = 0$ dans $\mathbb{Z}/p\mathbb{Z}$, pour $0 < k < p$, $\binom{p}{k} = 0$. Ainsi, $(x + y)^p = x^p + y^p$.

(5) Soit $f : \mathbb{R} \to \mathbb{R}$ un morphisme de corps. Comme $f(1) = 1$, on a $f(n) = n$ pour tout $n \in \mathbb{Z}$, puis $f(r) = r$ pour tout $r \in \mathbb{Q}$, donc f stabilise $\mathbb{Q}$. Pour $x \geq 0$, $x = \sqrt{x}^2$, donc $f(x) = f(\sqrt{x})^2 \geq 0$, donc f préserve $\mathbb{R}^+$. Ainsi, si $x \geq y$, $x - y \geq 0$, donc $f(x - y) \geq 0$, donc $f(x) \geq f(y)$, donc f est croissante. Soit (x_n) une suite réelle telle que $x_n \to x \in \mathbb{R}$. Alors, $x - x_n \to 0$, donc on peut trouver deux suites de rationnels $(r_n), (s_n)$ de limites nulles telles que pour tout n, $r_n \leq x - x_n \leq s_n$. Par croissance de f et comme f préserve $\mathbb{Q}$, $r_n \leq f(x) - f(x_n) \leq s_n$. Ainsi, $f(x_n) \to f(x)$, ce qui démontre que f est continue. Par densité de $\mathbb{Q}$ dans $\mathbb{R}$ et comme $f_{|\mathbb{Q}} = \mathrm{id}$, on en déduit que $f = \mathrm{id}$. Ainsi, le seul automorphisme de corps de $\mathbb{R}$ est l'identité.

Définition 1.1.4. Soit I un ensemble et $S = (X_i)_{i \in I}$ une famille d'indéterminées indexée par I. On définit :

$$K[X_i \mid i \in I] = \{P(X_{i_n}, \ldots, X_{i_m}) \mid \exists \{i_1, \ldots, i_n\} \subseteq I, P \in K[X_{i_1}, \ldots, X_{i_n}]\}$$

Remarquons que $K[X_i \mid i \in I] = \bigcup_{E \subseteq I \text{ fini}} K[X_i \mid i \in E]$, ce qui permet de définir les lois internes $+$ et $\cdot$ sur $K[X_i \mid i \in I]$. On construit ainsi une structure de K-algèbre sur $K[X_i \mid i \in I]$. De plus, $K[X_i \mid i \in I]$ est intègre.

Définition 1.1.5. On définit $K(X_i \mid i \in I) = \mathrm{Frac}\, K[X_i \mid i \in I]$. C'est une extension de corps de K.

Exemple 1.1.6. Soit $I = \mathbb{N}$. Le K-morphisme $\begin{array}{ccc} K(X_i \mid i \in I) & \to & X_i \\ K(X_i \mid i \in I) & \mapsto & X_{i+1} \end{array}$ est un morphisme de corps non surjectif.

Si I est fini, on écrit $I = \{1, 2, \ldots, n\}$ et on a $K[X_i \mid i \in I] = K[X_1, \ldots, X_n]$ et $K(X_i \mid i \in I) = K(X_1, \ldots, X_n)$.

Proposition 1.1.7. *Si L/K est une extension de corps, alors L est muni d'une structure de K-espace vectoriel par la loi externe* $\begin{array}{ccc} K \times L & \to & L \\ (k,v) & \mapsto & k \cdot_L v \end{array}$ *(ou si on ne fait pas l'identification, $(k,v) \mapsto i(k) \cdot_L v$).*

Définition 1.1.8. Le *degré* d'une extension de corps L/K est la dimension de L vu comme K-espace vectoriel. On le note $[L : K]$. Si $[L : K] < \infty$, on dira que L/K est une *extension finie*. Si $[L : K] = \infty$, elle est dite *infinie*.

Remarque. Le résultat bien connu d'algèbre linéaire qui dit qu'en dimension finie, toutes les bases ont même cardinal est vrai en général (deux bases dans un espace vectoriel sont toujours en bijection). Ainsi, on peut parler du degré d'une extension infinie de manière plus précise en parlant du cardinal des bases.

Exemple 1.1.9.

(1) On a $[\mathbb{C} : \mathbb{R}] = 2 = [\mathbb{Q}(i) : \mathbb{Q}]$ et $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

(2) $[\mathbb{R} : \mathbb{Q}]$ est non dénombrable sinon $\mathbb{R}$ serait dénombrable.

(3) $[K(X) : K] = \max(\mathrm{Card}(K), \mathrm{Card}(\mathbb{N}))$. Une base est donnée par

$$\left\{ X^j, \frac{X^i}{P^n} \,\middle|\, j \in \mathbb{N}, i, n \in \mathbb{N}^*, i < \deg P, P \text{ unitaire irréductible dans } K[X] \right\}$$

Théorème 1.1.10. *Soit $M/L/K$ une tour de corps. Alors*

$$[M : K] = [M : L][L : K]$$

En particulier, M/K est finie si et seulement si M/L et L/K le sont.

Remarque. La relation est à lire : si $\mathcal{B}_1$ est une base de M/L et $\mathcal{B}_2$ une base de L/K, alors $\dim_K M = \mathrm{Card}(\mathcal{B}_1 \times \mathcal{B}_2)$.

Démonstration. Soit $(e_i)_{i \in I}$ une base du L-espace vectoriel M et $(f_j)_{j \in J}$ une base du K-espace vectoriel L. On montre que $(e_i f_i)_{(i,j) \in I \times J}$ est une base de M/K.

Cette famille est libre : si $\sum_{i,j} \lambda_{ij} e_i f_j = 0$ avec $\lambda_{ij} \in K$ presque nulle, alors $\sum_{i \in I} e_i \left(\sum_{j \in J} \lambda_{ij} f_j \right) = 0$. Comme (e_i) est libre sur L, on a pour tout $i \in I$, $\sum_{j \in J} \lambda_{ij} f_j = 0$. Comme (f_j) est libre sur K, les λ_{ij} sont nuls, d'où la liberté. Cette famille est génératrice : pour $x \in M$,

$$x = \sum_{j \in J} \lambda_j f_j = \sum_{j \in J} \sum_{i \in I} \mu_i e_i f_j$$

Où les $\lambda_j \in L$ existent car (f_j) engendre M et les $\mu_i \in K$ existent car (e_i) engendre L. □

Définition 1.1.11. Soit L/K une extension de corps et $S \subseteq L$.

(1) Le *sous-anneau de L/K engendré par S*, noté $K[S]$, est défini par

$$K[S] = \bigcap_{\substack{K \cup S \subseteq A \subseteq L \\ A \text{ sous-anneau} \\ \text{de } L}} A$$

C'est le plus petit sous-anneau de L qui contient K et S.

(2) La *sous-extension L/K engendrée par S*, notée $K(S)$ est définie par

$$K(S) = \bigcap_{\substack{K \cup S \subseteq E \subseteq L \\ E \text{ sous-corps} \\ \text{de } L}} E$$

C'est le plus petit sous-corps de L qui contient K et S.

(3) On dira que L/K est *de type fini* s'il existe $S \subseteq L$ fini tel que $L = K(S)$.

Remarque.

(1) On a $K[S] = \mathrm{Vect}_K(\mathcal{B})$ avec $\mathcal{B} = \left\{ \prod_{\text{fini}} \alpha \;\middle|\; \alpha \in S \right\}$.

(2) On a $K(S) = \mathrm{Frac}\, K[S]$. Si $S = \{a_1, \ldots, a_n\} \subseteq L$, on écrira $K[a_1, \ldots, a_n]$ et $K(a_1, \ldots, a_n)$ pour $K[S]$ et $K(S)$, respectivement.
On a alors $K[a_1, \ldots, a_n] = \{P(a_1, \ldots, a_n) \mid P \in K[X_1, \ldots, X_n]\}$.

(3) $K(S) = \bigcup_{\substack{A \subseteq S \\ \text{finie}}} K(A)$ car $\bigcup_{A \text{ finie}} K(A)$ est un corps.

(4) Toute extension de corps finie est de type fini (car une base est un ensemble générateur).

Exemple 1.1.12.

(1) $\mathbb{Q}(\mu_n)/\mathbb{Q}$ avec $\mu_n \in \mathbb{C}$ une racine primitive n-ième de l'unité où $n \in \mathbb{N}^*$ est une extension finie. On remarque que $\mathbb{Q}(\mu_n) = \mathbb{Q}[\mu_n]$ car $\mu_n^n = 1$. On dit que $\mathbb{Q}(\mu_n)/\mathbb{Q}$ est une *extension cyclotomique*.

(2) $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ est finie.

(3) $K(X)/K$ est de type fini, mais pas finie.

(4) $K(X_n \mid n \in \mathbb{N})/K$ n'est pas de type fini. $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$ ne le sont pas non plus. On verra cela en utilisant des bases de transcendance.

1.2 Extensions algébriques et transcendantes

Définition 1.2.1. Soit L/K une extension de corps. Un élément $\alpha \in L$ est dit *algébrique sur K* s'il existe $P \in K[X] \setminus \{0\}$ tel que $P(\alpha) = 0$. Sinon, il est dit *transcendant sur K*. L'extension L/K est dite *algébrique* si tout élément de L est algébrique sur K. Sinon, on dira qu'elle est *transcendante*.

Exemple 1.2.2.

(1) e est transcendant dans $\mathbb{C}/\mathbb{Q}$ (Hermite 1873). π est transcendant dans $\mathbb{C}/\mathbb{Q}$ (Lindemann 1882).

(2) $\sqrt{2}$ et $\sqrt[n]{n}$ sont algébriques dans $\mathbb{C}/\mathbb{Q}$.

(3) $2^{\sqrt{2}}$ est transcendant dans $\mathbb{R}/\mathbb{Q}$ (Gelfond-Schneider 1934).

(4) On ne sait pas si $e + \pi$ ou $e - \pi$ sont transcendants.

Théorème 1.2.3. *Soit $\alpha \in L$. Soit* $E_\alpha : \begin{array}{ccc} K[X] & \to & L \\ P(X) & \mapsto & P(\alpha) \end{array}$ *. C'est un K-morphisme d'anneaux.*

De plus :

(1) L'élément α est transcendant dans L/K si et seulement si E_α est injectif. Dans ce cas, il induit un isomorphisme de K-algèbres $K[X] \simeq K[\alpha]$ qui se prolonge en un K-isomorphisme $K(X) \to K(\alpha)$. Dans ce cas, $\dim_K K[\alpha]$ et $\dim_K K(\alpha)$ sont infinies.

(2) L'élément α est algébrique dans L/K si et seulement si E_α n'est pas injectif. Dans ce cas, il existe un unique polynôme unitaire P_α dans $K[X]$ de degré minimal tel que $P_\alpha(\alpha) = 0$. Ce polynôme est irréductible sur K. De plus, $K[\alpha] = K(\alpha) \simeq K[X]/(P_\alpha)$ et $[K(\alpha) : K] = \deg P_\alpha$.

Définition 1.2.4. Le polynôme $P_\alpha \in K[X]$ issu du théorème précédent est appelé le *polynôme minimal de $\alpha \in L$ sur K*.

Preuve du théorème 1.2.3.

(1) L'élément α est transcendant si et seulement si E_α est injectif par définition. Alors, $E_\alpha(K[X]) \simeq \mathrm{Im}(E_\alpha) = K[\alpha]$, donc E_α induit un K-isomorphisme $K[X] \xrightarrow{\sim} K[\alpha]$ et il se prolonge à $K(X) \xrightarrow{\sim} K(\alpha)$ par $\frac{P}{Q} \mapsto P(\alpha)Q(\alpha)^{-1}$ (bien défini car $Q(\alpha) \neq 0$ pour $Q \in K[X] \setminus \{0\}$).

(2) L'élément α est algébrique si et seulement si $\ker E_\alpha \neq \{0\}$ par définition. Comme $K[X]$ est principal, $\ker E_\alpha = (P_\alpha)$ pour un certain polynôme $P_\alpha \in K[X]$ qu'on peut choisir unitaire. Ce polynôme est de degré minimal dans $\ker E_\alpha \setminus \{0\}$. De plus, $\ker E_\alpha$ est premier, donc P_α est irréductible. Comme $K[X]$ est principal, $\ker E_\alpha$ est maximal, donc $K[X]/(\ker E_\alpha)$ est un corps, isomorphe à $K[\alpha]$ par théorème d'isomorphisme. En particulier, $K(\alpha) = K[\alpha]$. En notant $n = \deg P_\alpha$, $\{1, \alpha, \dots, \alpha^{n-1}\}$ est une base de $K[\alpha]/K$. En effet, elle est libre, sinon on aurait un polynôme de $K[X]$ annulateur de α de degré strictement plus petit que $\deg P_\alpha$. De plus, pour $x \in K[\alpha]$, il existe $T \in K[X]$ tel que $x = T(\alpha)$. Par division euclidienne, on a $T = QP_\alpha + R$ avec $\deg R < n$, donc $T(\alpha) = R(\alpha)$, donc $x \in \mathrm{Vect}(1, \alpha, \dots, \alpha^{n-1})$. On a donc $[K(\alpha) : K] = \dim_K K[\alpha] = \deg P_\alpha$.

□

Remarque.

(1) On a aussi montré que $[K[X]/(P_\alpha) : K] = \deg P_\alpha$ et que $K[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in K\}$, où $\alpha \in L$ est algébrique sur K et $n = \deg P_\alpha$.

(2) Si P est un polynôme irréductible dans $K[X]$, alors (P) est un idéal maximal, donc $L = K[X]/(P)$ est un corps et L/K une extension. Soit $\alpha = X + (P) \in L$. Alors, le morphisme projection $\begin{array}{ccc} K[X] & \to & L \\ X & \mapsto & \alpha \end{array}$ coïncide avec E_α. Dans ce cas, $P_\alpha = uP$ où $u \in K^\times$ est tel que P_α soit unitaire. On a alors $[L : K] = \deg P$.

(3) Pour $\alpha \in L$ algébrique sur K et $Q \in K[X]$, on a $Q(\alpha) = 0$ si et seulement si $P_\alpha \mid Q$ dans $K[X]$.

Exemple 1.2.5.

(1) Dans $\mathbb{C}/\mathbb{R}$, tout polynôme minimal d'un élément de $\mathbb{C}$ est de degré au plus 2.

(2) Dans $K(X)/K$, l'élément transcendant X est transcendant sur K.

(3) Dans $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, le polynôme minimal de $a + b\sqrt{2}$ avec $b \neq 0$ est $(X - a)^2 - 2b^2 \in \mathbb{Q}[X]$.

Proposition 1.2.6. *Tout extension de corps finie est algébrique.*

Démonstration. Soit L/K une extension finie. Soit $\alpha \in L$. Alors, $K(\alpha)/K$ est aussi finie, donc α est algébrique. □

Exemple 1.2.7. On verra plus tard que $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algébrique dans } \mathbb{C}/\mathbb{Q}\}$ est dénombrable. Remarquons que par définition, $\overline{\mathbb{Q}}/\mathbb{Q}$ est algébrique. De plus, on démontrera que $\overline{\mathbb{Q}}/\mathbb{Q}$ n'est pas finie et donc pas de type fini.

Corollaire 1.2.8. *Soit L/K une extension de type fini. Si L est engendré par des éléments algébriques, alors L/K est finie et algébrique.*

Démonstration. Soit $L/E/K$ une tour de corps telle que E/K soit finie et algébrique et $x \in L$ algébrique sur K. Alors, x est algébrique sur E donc $E(x)/E$ est finie donc $E(x)/K$ est finie (donc algébrique) par le théorème 1.1.10. Le corollaire suit par récurrence sur le cardinal de l'ensemble générateur. □

Corollaire 1.2.9. *La somme et le produit de deux éléments algébriques de L/K sont algébriques. L'ensemble des éléments algébriques de L/K est une sous-extension, notée $\overline{K}^L$ et appelée* clôture algébrique de K dans L. *De plus, $\overline{K}^L/K$ est algébrique.*

Démonstration. Soient $x, y \in L$ algébriques sur K. Alors, $K(x,y)/K$ est une extension algébrique par ce qui précède. Comme $x - y, xy \in K(x,y)$ (et $y^{-1} \in K(x,y)$ si $y \neq 0$), ces éléments sont algébriques sur K. Le reste en découle. □

Exemple 1.2.10.

(1) L'extension $\mathbb{R}/\mathbb{Q}$ n'est ni algébrique, ni de type fini.

(2) L'extension $K(X)/K$ est de type fini mais pas algébrique.

(3) L'extension $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ est algébrique et finie.

(4) L'extension $\overline{\mathbb{Q}}/\mathbb{Q}$ où $\overline{\mathbb{Q}}$ est la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$ n'est pas de type fini ou finie mais est algébrique.

Définition 1.2.11. Soit L/K une extension. Si $\overline{K}^L = K$, on dit que K *est algébriquement clos dans* L. Remarquons qu'alors l'extension $L/\overline{K}^L$ est totalement transcendante.

Corollaire 1.2.12. *Une extension de corps engendrées par des éléments algébriques est algébrique.*

Démonstration. Soit L/K une extension de corps et $S \subseteq L$ où S contient uniquement des éléments algébriques sur K tel que $L = K(S)$. Alors, $S \subseteq \overline{K}^L$ et L/K est algébrique. □

Proposition 1.2.13. *Soit $M/L/K$ une tour de corps. Alors, M/K est algébrique si et seulement si M/L et L/K le sont.*

Démonstration. Le sens direct est clair. Supposons donc M/L et L/K algébriques. Soit $\alpha \in M$. On dispose de $P = \sum_{i=0}^{n} a_i X^i \in L[X]$ non nul tel que $P(\alpha) = 0$. Alors, α est algébrique dans $M/K(a_1, \ldots, a_n)$. Alors, $[K(a_0, \ldots, a_n)(\alpha) : K(a_0, \ldots, a_n)] < \infty$. De plus, les éléments a_i sont algébriques sur K car L/K est algébrique, donc $[K(a_0, \ldots, a_n) : K] < \infty$. Le théorème 1.1.10 donne $[K(a_0, \ldots, a_n)(\alpha) : K] < \infty$, ce qui démontre que α est algébrique sur K. Ainsi, M/K est algébrique. □

1.3 Degré de transcendance

Définition 1.3.1. Soit L/K une extension de corps. Une famille $(\alpha_i)_{i\in I}$ d'éléments de L est dite *algébriquement indépendante* sur K si le morphisme de K algèbres $\begin{array}{ccc} K[X_i \mid i \in I] & \to & L \\ X_i & \mapsto & \alpha_i \end{array}$ est injectif. L'extension L/K est dite *transcendante pure* si elle est engendrée par une famille algébriquement indépendante. Cela est équivalent à demander que L soit K-isomorphe à $K(X_i \mid i \in I)$.

Remarque.

(1) La famille d'éléments $(\alpha_i)_{i\in I}$ de L/K est algébriquement indépendante si et seulement si pour tout $\{i_1, \ldots, i_n\} \subseteq I$ et pour tout $P(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$, on a $P(\alpha_{i_1}, \ldots, \alpha_{i_n}) \neq 0$.

(2) Si $(\alpha_i)_{i\in I}$ est algébriquement indépendante dans L/K, le K-morphisme $\begin{array}{ccc} K[X_i \mid i \in I] & \to & L \\ X_i & \mapsto & \alpha_i \end{array}$ est injectif et se prolonge donc à un K-morphisme de corps $\begin{array}{ccc} K(X_i \mid i \in I) & \to & L \\ \frac{P(X_{i_1},\ldots,X_{i_n})}{Q(X_{j_1},\ldots,X_{j_m})} & \mapsto & \frac{P(\alpha_{i_1},\ldots,\alpha_{i_n})}{Q(\alpha_{j_1},\ldots,\alpha_{j_m})} \end{array}$ qui a pour image $K(\alpha_i \mid i \in I)$.

Lemme 1.3.2. *Soit L/K une extension de corps et $S \subseteq L$ un ensemble algébriquement indépendant dans L/K. Soit $x \in L \setminus S$. Alors $S \cup \{x\}$ est algébriquement indépendant dans L/K si et seulement si x est transcendant dans $L/K(S)$.*

Démonstration. Supposons x algébrique dans $L/K(S)$. Soit $P \in K(S)[X] \setminus \{0\}$ tel que $P(x) = 0$. On écrit $P = \sum_{i=0}^{n} a_i X^i$ avec $a_i \in K(S)$. On dispose alors de $\exists b_i, c_i \in K[S]$ tels que $a_i = \frac{b_i}{c_i}$ avec les c_i non nuls. En multipliant P par $\prod_i c_i$, on obtient un polynôme $P_1 \in K[S][X] \setminus \{0\}$ qui annule x. Comme S est algébriquement indépendant, le morphisme $\begin{array}{ccc} K[X_s \mid s \in S] & \to & K[S] \\ X_s & \mapsto & s \end{array}$ est injectif. Par l'absurde, si $S \cup \{x\}$ est algébriquement indépendant, on a

$$\begin{array}{ccccc} K[X, X_s \mid s \in S] & \hookrightarrow & K[S][X] & \hookrightarrow & L \\ X_s & \longmapsto & s & \longmapsto & s \\ X & \longmapsto & X & \longmapsto & x \end{array}$$

Ce qui contredit l'existence de $P_1 \in K[S][X] \setminus \{0\}$ qui annule x.
Réciproquement, supposons x transcendant dans $L/K(S)$. Comme S est algébriquement indépendant, le K-morphisme $\begin{array}{ccc} K[X_s \mid s \in S] & \to & K(S) \\ X_s & \mapsto & s \end{array}$ est injectif. La transcendance de x implique que le $K(S)$-morphisme $\begin{array}{ccc} K(S)[X] & \to & L \\ X & \mapsto & x \end{array}$ est injectif. Donc, le K-morphisme

$$\begin{array}{ccc} K[X, X_s \mid s \in S] & \to & L \\ X_s & \mapsto & s \\ X & \mapsto & x \end{array}$$

est injectif, d'où $S \cup \{x\}$ est algébriquement indépendant dans L/K. □

Exemple 1.3.3.

(1) L'ensemble $\{\pi, \pi - 1\}$ n'est pas algébriquement indépendant dans $\mathbb{R}/\mathbb{Q}$.

(2) On ne sait pas si $\{\pi, e\}$ est algébriquement indépendant dans $\mathbb{R}/\mathbb{Q}$ et donc on ne sait pas si $\mathbb{Q}(\pi, e)/\mathbb{Q}$ est purement transcendante.

(3) $\{\sqrt{2}, \pi\}$ n'est pas algébriquement indépendant dans $\mathbb{R}/\mathbb{Q}$ et $\mathbb{Q}(\sqrt{2}, \pi)/\mathbb{Q}$ n'est pas transcendante pure.

(4) $K(X_1, \ldots, X_n)/K$ est transcendante pure.

(5) $\mathbb{R}(X, \sqrt{1 - X^2})/\mathbb{R}$ est transcendante pure car égale à $\mathbb{R}\left(\frac{1-X}{\sqrt{1-X^2}}\right)/\mathbb{R}$ (paramétrisation du cercle).

(6) $\mathbb{Q}(X, \sqrt{X^3 - X})/\mathbb{Q}$ n'est pas transcendante pure, même si elle est transcendante.

(7) Dans la tour $\mathbb{R}(X, Y)/\mathbb{R}(X + Y)/\mathbb{R}$, l'extension $\mathbb{R}(X, Y)/\mathbb{R}(X + Y)$ est transcendante pure.

Définition 1.3.4. Une *base de transcendance pour* L/K est un sous-ensemble algébriquement indépendant dans L/K maximal.

Lemme 1.3.5. *Un ensemble algébriquement indépendant $S \subseteq L$ est une base de transcendance de L/K si et seulement si $L/K(S)$ est algébrique.*

Démonstration. Le lemme précédent nous dit qu'on peut ajouter un élément x à S en préservant l'indépendance algébrique si et seulement si x est transcendant dans $L/K(S)$, ce qui conclut. □

Théorème 1.3.6. *Soit L/K une extension. Elle contient une base de transcendance. Toute les bases de transcendance de L/K ont même cardinal.*

Définition 1.3.7. Le cardinal commun des bases de transcendance d'une extension L/K est appelé le *degré de transcendance de* L/K et noté $\mathrm{degtr}(L/K)$.

Preuve de l'existence. Soit $E \subseteq L$ un ensemble algébriquement indépendant dans L/K. Soit $S \subseteq L$ un ensemble générateur de L/K tel que $E \subseteq S$. Soit

$$\mathcal{B} = \{U \subseteq L \mid U \text{ algébriquement indépendant}, E \subseteq U \subseteq S\}$$

C'est un ensemble non vide ordonné pour l'inclusion. Soit $(T_i)_{i \in I}$ une chaîne dans $\mathcal{B}$. Alors, $\bigcup_i T_i \in \mathcal{B}$ est un majorant de la chaîne. En effet, si des éléments $a_1, \ldots, a_n$ dans l'union sont annulés par un polynôme P, comme (T_i) est totalement ordonné pour l'inclusion, ces éléments sont contenus dans un certain T_j qui est algébriquement indépendant, donc $P = 0$, donc l'union est bien dans $\mathcal{B}$. Par le lemme de Zorn, on dispose d'un ensemble algébriquement indépendant maximal B contenu dans S.
S'il existe $t \in S \setminus B$ tel que t est transcendant sur $L/K(B)$, alors $B \cup \{t\} \subseteq S$ est algébriquement indépendant par le lemme 1.3.2. Cela contredit la maximalité de B, donc tout $t \in S \setminus B$ est algébrique sur $L/K(B)$, d'où $\underbrace{K(B)(S \setminus B)}_{L}/K(B)$ est algébrique et on conclut que B est une base de transcendance par le lemme 1.3.5. □

Remarque. La preuve précédente montre que tout ensemble générateur de l'extension L/K contient une base de transcendance.

Preuve de l'unicité des cardinaux. Soient $B_1, B_2 \subseteq L$ deux bases de transcendance de L/K. Quitte à permuter, on suppose $\mathrm{Card}(B_1) \leq \mathrm{Card}(B_2)$.
Supposons d'abord $\mathrm{Card}(B_2)$ infini. Pour $\alpha \in B_1$, il existe $B_\alpha \subseteq B_2$ fini (il suffit de prendre les coefficients d'un polynôme annulateur de α et de remarquer qu'ils s'expriment chacun à partir d'un nombre fini d'éléments de B_2) tel que α est algébrique sur $K(B_\alpha)$. Soit $B' = \bigcup_{\alpha \in B_1} B_\alpha$. Soit $\beta \in B_2 \setminus B'$. Alors β est algébrique dans $L/K(B_1)$. De plus, par construction de B', $K(B_1)/K(B')$ est algébrique. Ainsi β est algébrique dans $L/K(B')$, ce qui est absurde car $B' \cup \{\beta\} \subseteq B_2$ n'est pas algébriquement indépendante. Ainsi $B_2 = B'$, d'où B_1 est infinie (sinon $B' = B_2$ serait finie) et l'arithmétique des cardinaux nous dit que $\mathrm{Card}(B_1) = \mathrm{Card}(B_2)$.
Supposons maintenant $\mathrm{Card}(B_2)$ fini. Alors, $\mathrm{Card}(B_1)$ est fini aussi par hypothèse. On explicite $B_1 = \{\beta_1, \ldots, \beta_m\}$ et $B_2 = \{\alpha_1, \ldots, \alpha_n\}$, alors $m \leq n$. On raisonne par récurrence sur m. Si $m = 0$, alors L/K est algébrique, donc forcément $B_2 = \varnothing$ et $n = 0$. Si $m > 0$, on dispose d'un polynôme $P \in K[X, Y_1, \ldots, Y_n]$ tel que $P(\beta_1, \alpha_1, \ldots, \alpha_n) = 0$ avec β_1 et au moins un des α_i qui apparaissent. Supposons quitte à permuter que c'est α_1 qui apparaît. Soit $B' = \{\beta_1, \alpha_2, \ldots, \alpha_n\}$. Alors, $K(B', \alpha_1)/K(B')$ est algébrique. Si B' n'était pas algébriquement indépendant, on trouverait un polynôme Q à coefficients dans K tel que $Q(\beta_1, \alpha_2, \ldots, \alpha_n) = 0$ où forcément β_1 apparaîtrait, d'où β_1 serait algébrique sur $K(\alpha_2, \ldots, \alpha_n)$ et donc α_1 aussi, ce qui est absurde. Alors, B' est algébriquement indépendant dans L/K. Ainsi $\{\alpha_2, \ldots, \alpha_n\}$, $\{\beta_2, \ldots, \beta_m\}$ sont des bases de transcendance de $L/K(\beta_1)$, et on conclut avec l'hypothèse de récurrence. □

Remarque. On a $\mathrm{degtr}(L/K) = 0$ si et seulement si L/K est algébrique.

Remarque. Soit $L = K(\alpha)/K$ avec α transcendant. Soit M/K une extension. Alors, on a une bijection

$$\{K\text{-morphismes } L = K(\alpha) \to M\} \overset{\text{bij}}{\longleftrightarrow} \{\text{transcendants de } M/K\}$$
$$(\varphi : \alpha \mapsto \beta) \longmapsto \beta$$

Remarque. Pour L/K, on peut toujours prendre une sous-extension maximale E telle que E/K est purement transcendante et L/E algébrique.

Exemple 1.3.8.

(1) $L = K(X)/K$, $B_1 = \{X\}$, $B_2 = \{X^2\}$. $K(B_1) = K(X)$, $K(B_2) = K(X^2)$.
(2) $\mathrm{degtr}(K(X_i \mid i \in I)/K) = \mathrm{Card}(I)$.
(3) $1 \leq \mathrm{degtr}(\mathbb{Q}(\pi, e)/\mathbb{Q}) \leq 2$.
(4) $\mathrm{degtr}(\mathbb{R}(X, \sqrt{1 - X^2}/\mathbb{R})) = 1$
(5) $\mathrm{degtr}(\mathbb{Q}(X, \sqrt{X^3 - X})/\mathbb{Q}) = 1$
(6) $\mathrm{degtr}(\mathbb{C}/\mathbb{Q}) = \infty$

Corollaire 1.3.9. *Soit $M/L/K$ une tour de corps. Alors*

$$\mathrm{degtr}(M/K) = \mathrm{degtr}(M/L) + \mathrm{degtr}(L/K)$$

Démonstration. Soient B_1, B_2 des bases de transcendance de M/L et L/K, respectivement. On a $B_1 \cap B_2 = \varnothing$ car $B_1 \cap L = \varnothing$ et $B_2 \subseteq L$. L'ensemble $B_1 \cup B_2$ est algébriquement indépendant dans M/K. Sinon, on obtiendrait une relation de la forme

$$P(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) = 0$$

où $\alpha_1, \dots, \alpha_n \in B_1$ et $\beta_1, \dots, \beta_m \in B_2$ sont distincts deux à deux et P est un polynôme à coefficients dans K. Mais alors, par indépendance algébrique de B_1, aucun α_i ne peut apparaître dans le polynôme (car les β_i sont dans L), d'où $P(\beta_1, \dots, \beta_m) = 0$ et contredit l'indépendance algébrique de B_2. De plus, $M/K(B_1 \cup B_2)$ est algébrique. En effet, $M/L(B_1)$ et $L/K(B_2)$ le sont, donc $M/L(B_1 \cup B_2)$ est algébrique et les éléments de $L, B_1 \cup B_2$ sont algébriques dans $M/K(B_1 \cup B_2)$. □

Proposition 1.3.10 (Critère d'Eisenstein)**.** *Soit $P(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$. On suppose qu'il existe p premier tel que $p \mid a_0, \dots, p \mid a_{n-1}$, $p \nmid a_n$ et $p^2 \nmid a_0$. Alors, P est irréductible dans $\mathbb{Q}[X]$.*

Démonstration. Soit une factorisation $P = QR$ avec $Q, R \in \mathbb{Q}[X]$ de degrés non nuls. **TODO** □

Corollaire 1.3.11. *L'extension $\overline{\mathbb{Q}}/\mathbb{Q}$ n'est pas finie. De même, $\overline{\mathbb{Q}}^{\mathbb{R}} = \overline{\mathbb{Q}} \cap \mathbb{R}$ n'est pas une extension finie de $\mathbb{Q}$.*

Démonstration. Pour $n \in \mathbb{N}^*$ et p premier fixé, $P_n(X) = p + pX + \cdots pX^{n-1} + X^n \in \mathbb{Z}[X]$ est irréductible par le critère d'Eisenstein. Ainsi, $[\mathbb{Q}[X]/(P_n(X)) : \mathbb{Q}] = n$. De plus, si $\alpha_n \in \mathbb{C}$ est une racine de P_n, on a $\mathbb{Q}[X]/(P_n(X)) \underset{\mathbb{Q}}{\simeq} \mathbb{Q}(\alpha_n)$. Comme $\mathbb{Q}(\alpha_n) \subseteq \overline{\mathbb{Q}}$, $\overline{\mathbb{Q}}$ contient des extensions de $\mathbb{Q}$ de degré arbitrairement grand, ce qui prouve $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. Pour $\overline{\mathbb{Q}}^{\mathbb{R}}$, on peut prendre $\alpha_n \in \mathbb{R}$ pour n impair. □

Remarque. On a $\overline{\mathbb{Q}} = \bigcup_{P \in \mathbb{Q}[X]} \{\text{racines de } P\}$ donc $\overline{\mathbb{Q}}$ est dénombrable comme union dénombrable d'ensembles finis.

Proposition 1.3.12. *On a $\operatorname{degtr}(\mathbb{C}/\mathbb{Q}) = \operatorname{degtr}(\mathbb{C}/\overline{\mathbb{Q}}) = \infty$ non dénombrable.*

Démonstration. **TODO** □

Remarque. De manière similaire, $\operatorname{degtr}(\overline{\mathbb{Q}}^{\mathbb{R}}/\mathbb{Q}) = \infty$ non dénombrable.

Exemple 1.3.13. Soit B une base de transcendance de $\mathbb{C}/\mathbb{Q}$. Soit $\varphi : B \to B$ une application quelconque injective. Elle induit un $\overline{\mathbb{Q}}$-morphisme $\overline{\mathbb{Q}}(B) \xrightarrow{\overline{\varphi}} \overline{\mathbb{Q}}(B)$ qui peut toujours se prolonger (a priori non uniquement) à $\mathbb{C} \xrightarrow{\varphi_0} \mathbb{C}$. Si φ n'est pas surjective, alors φ_0 sera un morphisme de corps non surjectif.

Références :

- Fields and Galois Theory, James Stuart Milne
- Polycopiés du cours algèbre 2 de l'ENS en français de Jean-François Dat, Olivier Debarre et Ariane Mézard [2]
- Algebra, Serge Lang

2. Son poly n'est pas sur son site à ce moment mais est accessible à travers la *Wayback Machine*.

1.4 Racines de polynômes

Soit K un corps.

Lemme 1.4.1. *Si $P \in K[X]$ a une racine $\alpha \in K$, alors $(X - \alpha) \mid P$.*

Démonstration. La division euclidienne fonctionne dans $K[X]$ car K est un corps, donc $P = (X - \alpha)Q + c$ avec $c \in K$ et évaluer en α donne le résultat. □

Corollaire 1.4.2. *Si $P \in K[X]$ est de degré d, alors P a au plus d racines dans K.*

Démonstration. Se déduit du lemme précédent avec une récurrence. □

Définition 1.4.3. On dit que P est *scindé* si $P = c\prod_{i=1}^{d}(X - \alpha_i)$ dans $K[X]$. Autrement dit, les facteurs irréductibles de P sont de degré 1 (ou $P \in K$). Ici, $c \in K$.

Exemple 1.4.4. $X^4 - 1$ est scindé dans $\mathbb{C}[X]$ mais pas dans $\mathbb{R}[X]$.

Définition 1.4.5. Soit L/K une extension de corps et $P \in K[X]$ irréductible. On dit que L est *un corps de rupture de P* s'il existe $\alpha \in L$ tel que $P(\alpha) = 0$ et $L = K(\alpha)$.

Exemple 1.4.6.

(1) $\mathbb{C}$ est un corps de rupture de $X^2 + 1 \in \mathbb{R}[X]$.
(2) $\mathbb{Q}(\sqrt{2})$ est un corps de rupture de $X^2 - 2 \in \mathbb{Q}[X]$.
(3) $\mathbb{Q}(\sqrt[3]{2})$ et $\mathbb{Q}(j\sqrt[3]{2})$ sont des corps de rupture de $X^3 - 2 \in \mathbb{Q}[X]$.
(4) $\mathbb{Q}(\sqrt[5]{3})$ est un corps de rupture de $X^5 - 3 \in \mathbb{Q}[X]$.

Remarque. Un corps de rupture n'est pas en général un corps dans lequel le polynôme est scindé, c'est-à-dire qu'en général il ne contient pas « toutes » les racines du polynôme.

Proposition 1.4.7. *Soit $P \in K[X]$ irréductible. Pour toute extension L/K et toute racine $\alpha \in L$ de P, on a un unique K-morphisme de corps $K_P = K[X]/(P) \hookrightarrow L$ tel que $X + (P)$ soit envoyé sur α. En particulier, si L est un corps de rupture de P, alors ce morphisme est un isomorphisme. On a alors $[L : K] = \deg P$.*

Démonstration. Prenons le K-morphisme $E_\alpha : \begin{array}{ccc} K[X] & \to & L \\ Q & \mapsto & Q(\alpha) \end{array}$. Comme α est racine de P, $(P) \subseteq \ker E_\alpha$, d'où E_α induit un K-morphisme $K[X]/(P) \hookrightarrow L$. Pour l'unicité, si $\phi : K[X]/(P) \to L$ est un autre K-morphisme tel que $\phi(X + (P)) = \alpha$, alors on a $\phi \circ \pi = E_\alpha$ où π est la projection canonique $K[X] \to K[X]/(P)$, donc par la propriété universelle du quotient $\phi = E_\alpha$. Si L est un corps de rupture de P, alors $L = K(\alpha) = K[\alpha] = \operatorname{im} E_\alpha$, donc E_α est surjectif et le K-morphisme $K_P \hookrightarrow L$ induit est un isomorphisme. On a alors $[L : K] = [K_P : K] = \deg P$ (voir le théorème 1.2.3). □

Corollaire 1.4.8. *Soit $P \in K[X]$ irréductible et L/K un corps de rupture. Soit M/K une extension dans laquelle P a une racine. Il existe un K-morphisme $L \hookrightarrow M$ et le nombre de tels morphismes est le nombre de racines distinctes de P dans M. C'est donc au plus $\deg P = [L : K]$, avec égalité si P a $\deg P$ racines distinctes dans M.*

Démonstration. Par la proposition précédente, on a un morphisme $\varphi : L \to M$. Pour $\alpha \in L$ une racine de P, comme φ est un morphisme de corps, $P(\varphi(\alpha)) = \varphi(P(\alpha)) = 0$. Ainsi $\varphi(\alpha)$ est une racine de P dans M. Comme φ est un K-morphisme et qu'on peut supposer $L = K(\alpha)$, on déduit que φ est uniquement déterminé par $\varphi(\alpha)$, donc le nombre de morphismes est bien le nombre de racines de P dans M. □

Théorème 1.4.9. *Soit L/K une extension de corps engendrée par des racines d'un polynôme $P \in K[X]$. Soit M/K une extension dans laquelle P est scindé. Il existe un K-morphisme de corps $L \hookrightarrow M$. Il y a au plus $[L : K]$ tels morphismes avec égalité quand P a $\deg P$ racines dans M.*

Démonstration. Soit $L = K(\alpha_1, \ldots, \alpha_n)$, où $\alpha_1, \ldots, \alpha_n \in L$ sont des racines de P. Soit $P_{\alpha_1} \in K[X]$ le polynôme minimal de α_1 dans L/K. Comme $P(\alpha_1) = 0$, $P_{\alpha_1} \mid P$ dans $K[X]$. Comme $K \subseteq M$ et P est scindé dans $M[X]$, P_{α_1} est scindé dans $M[X]$, avec $\deg P_{\alpha_1}$ racines si P a $\deg P$ racines dans M. Par le corollaire précédent, il existe un K-morphisme de corps $K(\alpha_1) \overset{\varphi_1}{\hookrightarrow} M$ et le nombre de tels morphismes est au plus $[K(\alpha_1) : K]$ avec égalité dans le cas où P (et donc P_{α_1}) a $\deg P$ (resp. $\deg P_{\alpha_1}$) racines dans M.
On considère maintenant P_{α_2} le polynôme minimal de α_2 dans $L/K(\alpha_1)$. On a encore $P_{\alpha_2} \mid P$ dans $K(\alpha_1)[X]$, donc $\varphi_1(P_{\alpha_2})$ est scindé dans $M[X]$ avec $\deg P_{\alpha_2}$ racines si P a $\deg P$ racines dans M, car $P_{\alpha_2} \mid P$ dans $K(\alpha_1)[X]$ implique $\varphi_1(P_{\alpha_2}) \mid \varphi_1(P) = P$ dans $\varphi_1(K(\alpha_1))$. Alors, on a un $K(\alpha_1)$-morphisme $\varphi_2 : K(\alpha_1, \alpha_2) \hookrightarrow M$ (on injecte $K(\alpha_1)$ dans M par φ_1) et il y a au plus $[K(\alpha_1, \alpha_2) : K(\alpha_1)]$ tels morphismes avec égalité quand P a $\deg P$ racines dans M. Ainsi, en itérant ce procédé, on obtient qu'il y a un K-morphisme $L \hookrightarrow M$ et au plus

$$[K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})] \cdots [K(\alpha_1) : K] = [L : K]$$

tels morphismes, avec exactement ce nombre quand P a $\deg P$ racines dans M. □

Définition 1.4.10. Soit $P \in K[X]$. Une extension L/K est dite *un corps de décomposition de P* si P est scindé dans L et que L est engendré par les racines de P.

Corollaire 1.4.11. *Soit $P \in K[X]$ un polynôme. Il existe une extension L/K qui est un corps de décomposition de P. Deux corps de décomposition de P sont K-isomorphes. De plus, $[L : K] \leq (\deg P)!$.*

Démonstration. SOit L_1/K un corps de rupture pour un facteur irréductible de $P \in K[X]$. Soit $L_1 = K(\alpha_1)$ avec $P(\alpha_1) = 0$. Alors, $\frac{P}{X-\alpha_1} \in L_1[X]$ et on construit un corps de rupture $L_2 = L_1(\alpha_2)$ d'un facteur irréductible de $\frac{P}{X-\alpha_1} \in L_1[X]$. On continue ainsi jusqu'à ce que $\frac{P}{Q} \in L_{\deg P}[X]$ soit de degré 1. On a alors $[L_1 : K] \leq \deg P$, $[L_2 : L_1] \leq \deg P - 1$, …, $[L_{\deg P} : L_{\deg P - 1}] \leq 2$, d'où $[L_{\deg P} : K] \leq (\deg P)!$. Soit maintenant M/K un autre corps de décomposition de P. Par le théorème précédent, il existe des K-morphismes $L \hookrightarrow M$ et $M \hookrightarrow L$, d'où $[M : K] = [L : K]$ et $M \simeq L$. □

Exemple 1.4.12.

(1) $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ est un corps de décomposition de $X^3 - 2$ de degré $3! = 6$.

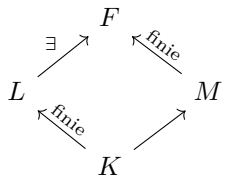
(2) $\mathbb{Q}(i)/\mathbb{Q}$ est un corps de décomposition de $X^4 - 1$ de degré $2 < 4!$.

(3) Soit $P = X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$, irréductible et $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ ses racines. Alors pour deux de ces racines, par exemple α_1, α_2, $\mathbb{Q}(\alpha_1, \alpha_2)/\mathbb{Q}$ est un corps de décomposition de P. On a aussi $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 3$, d'où $3 = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}] \leq 3! = 6$ et $3 \mid [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]$, donc $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}] \in \{3, 6\}$.

(4) Pour $P = 1 + X + \cdots + X^{p-1} \in \mathbb{Q}[X]$ avec p premier, corps de décomposition de P est $\mathbb{Q}(\mu_p)/\mathbb{Q}$ une extension cyclotomique.

(5) Pour $P = X^3 - 2$, $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}] = 6$, pour $P = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$, $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}] = 3$.

Corollaire 1.4.13. *Soit L/K une extension finie et M/K une extension. Alors le nombre de K-morphismes $L \hookrightarrow M$ est au plus $[L : K]$. Il existe une extension finie F/M tel qu'il existe un K-morphisme $L \hookrightarrow F$.*



Démonstration. Soit $L = K(\alpha_1, \ldots, \alpha_n)$ où $\alpha_1, \ldots, \alpha_n$ sont algébriques dans L/K. Soit $P \in K[X]$ le produit des polynômes minimaux de $\alpha_1, \ldots, \alpha_n$ sur K. Soit F/M un corps de décomposition de $P \in K[X] \subseteq M[X]$. Par le théorème, il existe un K-morphisme $L \hookrightarrow F$ et le nombre de tels morphismes est au plus $[L : K]$. Tout K-morphisme $L \hookrightarrow M$ induit un K-morphisme $L \hookrightarrow F$, donc il y a au plus $[L : K]$ tels morphismes. □

Corollaire 1.4.14. *Soient L_i/K, $i = 1, 2, \ldots, n$ des extensions finies et M/K une extension. Il existe une extension finie F/M telle qu'il existe des K-morphismes $L_i \hookrightarrow F$, $i = 1, 2, \ldots, n$.*

Démonstration. Par le corollaire précédent, il existe M_1/M finie telle qu'il existe un K-morphisme $L_1 \hookrightarrow M_1$. On applique maintenant ce même corollaire aux extensions L_2/K et M_1/K pour obtenir une extension M_2/K finie et l'existence d'un K-morphisme $L_2 \hookrightarrow M_2$. En continuant ce procédé, nous arrivons à une extension $F = M_n/M$ finie qui satisfait l'énoncé. □

Définition 1.4.15. Soit $(P_i)_{i \in I}$ une famille de polynômes dans $K[X]$. Une extension L/K est dite *un corps de décomposition pour la famille* $(P_i)_{i \in I}$ si pour tout $i \in I$, P_i est scindé dans L avec pour ensemble de racines $R_i \subseteq L$ et que $L = K\left(\bigcup_{i \in I} R_i\right)$.

1.5 Clôture algébrique

Soit K un corps.

Proposition 1.5.1. *Les assertions suivantes sont équivalentes :*

(1) Tout polynôme $P \in K[X] \setminus K$ a au moins une racine dans K.

(2) Tout $P \in K[X] \setminus K$ est scindé dans K.

(3) Les polynômes irréductibles dans $K[X]$ sont ceux de degré 1.

(4) Si L/K est une extension algébrique, alors $L = K$.

Démonstration. **TODO** □

Définition 1.5.2.

(1) Un corps K satisfaisant les propriétés équivalentes de la proposition est dit *algébriquement clos*.

(2) Un corps L est dit la *clôture algébrique* d'un sous-corps K si L est algébriquement clos et que L/K est algébrique.

Exemple 1.5.3.

(1) $\mathbb{C}$ est algébriquement clos. $\mathbb{R}$ et $\mathbb{Q}$ ne le sont pas. $K(T)$ ne l'est pas non plus.

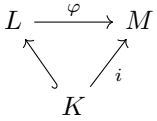
(2) $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$ mais pas une clôture algébrique de $\mathbb{Q}$.

(3) Si L/K est une extension de corps avec L algébriquement clos, alors $\overline{K}^L$ est une clôture algébrique de K, donc $\overline{\mathbb{Q}}$ est algébriquement clos et c'est une clôture algébrique de $\mathbb{Q}$.

Proposition 1.5.4. *Soit une extension L/K. Alors L est une clôture algébrique de K si et seulement si l'extension L/K est algébrique et tout polynôme de $K[X]$ est scindé sur L.*

Démonstration. Le sens direct est immédiat. Pour le sens réciproque, soit $P \in L[X]$ un polynôme irréductible. Soit M/L un corps de rupture de P. Alors, M/L, L/K sont algébriques donc M/K est algébrique. Soit $\alpha \in M$ une racine de P et P_α son polynôme minimal sur K. Alors, $P_\alpha \mid P$ dans $L[X]$, mais P est irréductible, donc $cP = P_\alpha$ pour un certain $c \in L$. Or, $P_\alpha \in K[X]$ est scindé dans L par hypothèse,donc P aussi. Comme P est irréductible, forcément $\deg P = 1$, ce qui démontre que L est algébriquement clos. Comme L/K est algébrique, on obtient le résultat. □

Proposition 1.5.5. *Soit L/K algébrique et M un corps algébriquement clos. Tout morphisme $i : K \to M$ se prolonge en un morphisme $\varphi : L \to M$.*



Démonstration. **TODO**zorn □

Proposition 1.5.6. *Soit M/K algébrique.*

(1) Si M est algébriquement clos, toute extension algébrique L/K est K-isomorphe à un sous-corps de M (une sous-extension de M/K). De plus, M est une clôture algébrique de L.

(2) Si toute extension finie L/K est isomorphe à une sous-extension de M/K, alors M est algébriquement clos.

Démonstration. Pour le (1), on prolonge l'inclusion $K \hookrightarrow M$ en un morphisme $L \hookrightarrow M$ par la proposition précédente. Soit $P \in K[X]$. P est scindé dans un de ses corps de décomposition L/K qui est une extension finie. Ainsi, par hypothèse, L/K est isomorphe à une sous-extension de M/K, donc P est scindé sur M. On conclut par la proposition 1.5.4. □

Remarque. Soit M/K une extension avec M algébriquement clos. Alors, par la proposition, pour tout polynôme $P \in K[X]$, M contient *exactement* (**TODO** : comprendre pourquoi) un corps de décomposition de P. De même, pour tout famille de polynôme $(P_i)_{i\in I}$, M contient exactement un corps de décomposition de (P_i).

Théorème 1.5.7 (Steinitz 1910)**.** *Soit K un corps. Il existe une clôture algébrique de K. Deux clôtures algébriques de K sont K-isomorphes.*

Démonstration. **TODO** □

Remarque. Si $\varphi : K \to K'$ est un isomorphisme de corps et que M et M' sont des clôtures algébriques de K, K' respectivement, alors φ se prolonge en un isomorphisme de corps $\psi : M \to M'$ (non unique en général).

Exemple 1.5.8. Le morphisme $\varphi : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x \end{array}$ peut se prolonger en deux morphismes par $\begin{array}{ccc} \mathbb{R}(i) & \to & \mathbb{R}(i) \\ i & \mapsto & i \end{array}$ et $\begin{array}{ccc} \mathbb{R}(i) & \to & \mathbb{R}(i) \\ i & \mapsto & -i \end{array}$.

Définition 1.5.9. Le théorème de Steinitz nous autorise à faire un abus de langage et parler de « la » clôture algébrique d'un corps K. On la notera $\overline{K}$.

Exemple 1.5.10.

(1) $\overline{\mathbb{Q}} \subsetneq \overline{\mathbb{Q}(\pi)} \subsetneq \overline{\mathbb{C}}$. On sait que la deuxième inclusion est stricte car $\overline{\mathbb{Q}(\pi)}$ est dénombrable.

(2) En général, il est difficile de décrire $\overline{K}$ pour un corps K. Par exemple, $\overline{K(T)}$ pour un corps K arbitraire.

1.6 Éléments conjugués

Définition 1.6.1. Soit L/K une extension de corps. Deux éléments algébriques $\alpha, \beta \in L$ sont dits *conjugués* sur K si leur polynômes minimaux sur K sont les mêmes.

Exemple 1.6.2.

(1) $i, -i$ sont conjugués dans $\mathbb{C}/\mathbb{R}$.

(2) $\sqrt[3]{2}, j\sqrt[3]{2}$ sont conjugués dans $\mathbb{C}/\mathbb{Q}$.

(3) $\sqrt{3}, i\sqrt{3}$ ne sont pas conjugués dans $\mathbb{C}/\mathbb{Q}$.

Proposition 1.6.3. *Soit L/K une extension de corps. Les énoncés suivants sont équivalents :*

(1) α, β sont conjugués dans L/K

(2) Il existe un K-isomorphisme $\begin{array}{ccc} K(\alpha) & \to & K(\beta) \\ \alpha & \mapsto & \beta \end{array}$.

Démonstration. Si α, β sont conjugués dans L/K, alors les isomorphismes

$$\begin{array}{ccc} K(\alpha) & \to & K[X]/(P_\alpha) \\ \alpha & \mapsto & X + (P_\alpha) \end{array} \qquad \begin{array}{ccc} K(\beta) & \to & K[X]/(P_\beta) \\ \beta & \mapsto & X + (P_\beta) \end{array}$$

montrent (2). Réciproquement, si $\begin{array}{ccc} K(\alpha) & \to & K(\beta) \\ \alpha & \mapsto & \beta \end{array}$ est un K-isomorphisme, on a que $P_\alpha(\beta) = P_\alpha(\alpha) = 0$ et symétriquement $P_\beta(\alpha) = 0$, d'où $P_\beta \mid P_\alpha$ et $P_\alpha \mid P_\beta$, d'où $P_\alpha = P_\beta$. □

Remarque. Dans $\overline{K}$, les conjugués de $\alpha \in \overline{K}$ sont les racines de $P_\alpha \in K[X]$. Si L/K est une extension et $\alpha \in L$ est algébrique dans L/K, alors les conjugués de α dans L sont les racines de $P_\alpha \in K[X]$ et il y en a au plus $\deg P_\alpha$.

Exemple 1.6.4.

(1) Dans $\mathbb{F}_p(T)$, le polynôme minimal de $\sqrt[p]{T} \in \overline{\mathbb{F}_p(T)}$ est $X^P - T = (X - \sqrt[p]{T})^p$, donc le seul conjugué de $\sqrt[p]{T}$ est lui-même.

(2) $\sqrt[3]{2}$ est son seul conjugué dans $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

Proposition 1.6.5. *Deux éléments $\alpha, \beta \in \overline{K}$ sont conjugués sur K si et seulement s'il existe un K-isomorphisme $\overline{K} \to \overline{K}$ qui envoie α sur β.*

Démonstration. Si α, β sont conjugués, ils sont algébriques, donc $\overline{K}$ est un clôture algébrique de $K(\alpha)$ et $K(\beta)$. Ainsi, l'isomorphisme de corps $K(\alpha) \xrightarrow{\sim} K(\beta)$ qui envoie α sur β se prolonge en un isomorphisme $\overline{K} \to \overline{K}$. La réciproque est immédiate. □

1.7 Extension normales

Définition 1.7.1. Une extension algébrique L/K est dite *normale* si tout polynôme $P \in K[X]$ irréductible qui a une racine dans L est scindé sur L.

Exemple 1.7.2.

(1) $\overline{K}/K$ est normale.

(2) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n'est pas normale, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ non plus.

(3) $\mathbb{Q}(i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ sont normales.

Proposition 1.7.3. *Soit L/K algébrique, $\overline{K}$ une clôture algébrique de K et $L \hookrightarrow \overline{K}$. Les énoncés suivants sont équivalents :*

(1) L/K est normale.

(2) Pour $\alpha \in L$, les conjugués de α dans $\overline{K}/K$ sont des éléments de L.

(3) Tout K-isomorphisme de $\overline{K}$ envoie L sur lui-même.

(4) L est le corps de décomposition d'une famille de polynômes à coefficients dans K.

Démonstration. Supposons L/K normale. Alors, L est le corps de décomposition de la famille $(P_\alpha)_{\alpha \in L}$ des polynômes minimaux des éléments de L sur K.
Supposons que L est le corps de décomposition de $(P_i)_{i \in I} \in K[X]^I$, et soit $\varphi : \overline{K} \xrightarrow{\sim} \overline{K}$ un K-isomorphisme. Soit $R_i \subseteq \overline{K}$ l'ensemble des racines de P_i dans $\overline{K}$. Alors, $L = K(\bigcup_{i \in I} R_i)$. De plus, $\varphi(R_i) = R_i$ pour tout i. Ainsi, $\varphi(K(\bigcup_{i \in I} R_i)) = K(\bigcup_{i \in I} R_i)$.
Supposons (3). Soit $\alpha \in L$ et $\beta \in \overline{K}$ un conjugué de α dans $\overline{K}/K$. Alors, il existe un K-isomorphisme $\begin{array}{ccc} \overline{K} & \to & \overline{K} \\ \alpha & \mapsto & \beta \end{array}$, d'où $\beta = \varphi(\alpha) \in \varphi(L) = L$.
Supposons (2). Soit $P \in K[X]$ irréductible qui possède une racine $\alpha \in L$. Quitte à multiplier par un élément de $K^\times$ pour rendre P unitaire, on peut supposer $P = P_\alpha$. Alors, par (2), les conjugués de α dans $\overline{K}/K$, qui sont les racines de P_α dans $\overline{K}$, sont dans L, d'où P est scindé sur L. □

Corollaire 1.7.4. *Soit $M/L/K$ une tour de corps. Si M/K est normale, alors M/L l'est aussi.*

Démonstration. Immédiat par l'équivalence (1) $\iff$ (4) de la proposition 1.7.3. □

Corollaire 1.7.5. *Une extension L/K est normale et finie si et seulement si L est le corps de décomposition d'un polynôme sur K.*

Démonstration. Le sens inverse est vrai par le (4) de la proposition 1.7.3. Supposons donc L/K normale et finie. Raisonnons par récurrence sur $[L : K]$. Si $[L : K] = 1$, le résultat est clair. Supposons le résultat vrai pour $[L : K] < n, n \in \mathbb{N}^*$. Soit L/K tel que le résultat est vrai $[L : K] = n$. Soit $\alpha_0 \in L/K$ et $P_{\alpha_0} \in K$ son polynôme minimal. Alors, P_{α_0} est scindé sur L. Soit $K_0 \subseteq L$ sont corps de décomposition. Comme $K \subsetneq K_0 \subseteq L$, $[L : K_0] < n$. Comme L/K_0 est normale par le corollaire précédent, par hypothèse de récurrence on dispose de $Q \in K_0[X]$ dont L est le corps de décomposition. Soient $\alpha_1, \ldots, \alpha_n \in L$ les racines de Q. On a $L = K_0(\alpha_1, \ldots, \alpha_n)$, donc $L = K(\alpha_0, \alpha_1 \ldots, \alpha_n)$. Alors, L est le corps de décomposition du polynôme obtenu comme produit des polynômes minimaux des α_i sur K. □

Exemple 1.7.6.

(1) Dans la tour $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, l'extension $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ est normale mais pas $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

(2) Dans la tour $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, les extensions $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ sont normales, mais $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ne l'est pas.

Corollaire 1.7.7. *Soit L/K algébrique et M un corps algébriquement clos tel que M/K est algébrique (? ? **TODO**)*

Démonstration. **TODO** □

Corollaire 1.7.8. *Soit $M/L/K$ une tour de corps avec M/K normale. Alors, L/K est normale si et seulement si pour tout K-automorphisme φ de M, on a $\varphi(L) = L$.*

Démonstration. **TODO** □

Corollaire 1.7.9. *Soit L/K normale. Tout automorphisme de K se prolonge en un automorphisme de L. Cela est faux. Je sais pas trop quoi en faire du coup. **TODO***

Démonstration. **TODO** □

Théorème 1.7.10. *Soit L/K algébrique et M un corps algébriquement clos tel que $L \subseteq M$. Il existe une plus petite extension normale E/K telle que $L \subseteq E \subseteq M$. On dira que E est la* clôture normale de L dans M.

Démonstration. **TODO** □

1.8 Polynômes séparables

Définition 1.8.1. Soit K un corps. Soit θ l'unique morphisme d'anneaux $\mathbb{Z} \to K$ donné par $\theta(1) = 1_K$. Le noyau de θ est de la forme $n\mathbb{Z}$. Si θ est injectif, $n = 0$ et on dit que K *est de caractéristique nulle*. Si θ n'est pas injectif, alors $\ker\theta$ est un idéal premier de $\mathbb{Z}$ car K est un corps, donc $n = p$ est premier et on dit que K *est de caractéristique p*.
On note la caractéristique de K par $\mathrm{car}(K)$.

Proposition 1.8.2. *Si un corps K est de caractéristique nulle, alors le morphisme $\mathbb{Z} \to K$ se prolonge en un morphisme de corps $\mathbb{Q} \to K$. Si K est de caractéristique $p > 0$, alors le morphisme $\mathbb{Z} \to K$ se factorise en un morphisme de corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \hookrightarrow K$ et l'application*

$$\begin{array}{rccc} \mathrm{Fr}_K : & K & \to & K \\ & x & \mapsto & x^p \end{array}$$

est un automorphisme de K appelé le morphisme de Frobenius.

Démonstration. On démontre seulement le fait que le Frobenius est un morphisme. On a $\mathrm{Fr}_K(1) = 1$ et $\mathrm{Fr}_K(xy) = (xy)^p = x^p y^p = \mathrm{Fr}_K(x)\,\mathrm{Fr}_K(y)$. De plus

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$$

Comme p est premier, $p \mid \binom{p}{k}$ pour $0 < k < p$. Comme « $p = 0$ » dans K, on obtient

$$(x+y)^p = y^p + x^p$$

D'où Fr_K est bien un automorphisme de K (il est en particulier injectif !). □

Exemple 1.8.3.

(1) La caractéristique de $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(T), \mathbb{R}(T), \mathbb{C}(T)$ est nulle.

(2) La caractéristique de $\mathbb{F}_p, \mathbb{F}_p(T), \mathbb{F}_p(T_1, \ldots, T_n)$ est p pour p premier quelconque.

Définition 1.8.4. Pour un polynôme $P = \sum a_i X^i \in K[X]$, on définit son *polynôme dérivé* par $P' = \sum i a_i X^{i-1} \in K[X]$ (où i est en fait $\theta(i)$ où θ est l'unique morphisme $\mathbb{Z} \to K$).

Proposition 1.8.5. *L'application dérivée*

$$\begin{array}{rccc} \partial : & K[X] & \to & K[X] \\ & P & \mapsto & P' \end{array}$$

est une application K-linéaire. C'est l'unique application K-linéaire de $K[X]$ dans $K[X]$ qui satisfait la relation de Leibniz $\partial(PQ) = \partial(P)Q + P\partial(Q)$.

Proposition 1.8.6. *Soit $P \in K[X]$ tel que $P' = 0$.*

— *Si $\mathrm{car}(K) = 0$, alors $\deg P = 0$ ou $P = 0$.*

— *Si $\mathrm{car}(K) = p > 0$, alors il existe un unique $Q \in K[X]$ tel que $P = Q(X^p)$.*

Démonstration. On explicite $P = \sum a_i X^i$. Supposons $\mathrm{car}(K) = 0$. Alors, $i a_i = 0$ pour tout i. Ainsi, $a_i = 0$ pour tout $i > 0$, donc $\deg P = 0$ (ou $P = 0$). Supposons maintenant $\mathrm{car}(K) = p > 0$. Il subsiste que $a_i = 0$ pour tout i non divisible par p, donc les seuls monômes non nuls dans P sont de la forme $a_{pk} X^{pk} = (X^p)^k$, ce qui conclut. □

Définition 1.8.7. Soit L/K une extension de corps et $P \in K[X]$. Alors, $\alpha \in L$ est dit *une racine de multiplicité m de P* si $P(\alpha) = 0$ et $(X - \alpha)^m \mid P$ dans $L[X]$ mais que $(X - \alpha)^{m+1} \nmid P$ dans $L[X]$. Si $m = 1$, α est dite *une racine simple de P*, sinon on parle de *racine multiple*.

Remarque. Si P est scindé sur L, alors α est une racine de multiplicité m de P si et seulement si

$$P = (X - \alpha)^m c \prod_{i=1}^{s} (X - \beta_i)^{r_i}$$

avec $\beta_i \neq \alpha$ pour tout i et $c \in K^\times$.

Définition 1.8.8. Un polynôme $P \in K[X]$ est dit *séparable* si l'idéal (P, P') est $K[X]$, c'est-à-dire si P et P' sont premiers entre eux.

Exemple 1.8.9.

(1) Si $\deg P = 1$, alors P est séparable.

(2) Dans $\mathbb{C}[X]$, $X^2 + 1$ est séparable.

(3) Dans $\mathbb{F}_p(T)[X]$, $X^p - T$ n'est pas séparable.

Lemme 1.8.10. *Un polynôme est séparable si et seulement s'il n'a pas de racines multiples dans son corps de décomposition.*

Démonstration. Par contraposée, supposons que $P \in K[X]$ ait une racine multiple α dans son corps de décomposition L/K. Alors, $(X-\alpha)^2 \mid P$, donc il existe $Q \in L[X]$ tel que $P = (X-\alpha)^2 Q$, d'où

$$P' = ((X-\alpha)^2 Q)' = 2(X-\alpha)Q + (X-\alpha)^2 Q'$$

Donc α est aussi racine de P'. Ainsi, en notant $\Pi_\alpha \in K[X]$ le polynôme minimal de α sur K (existe car L/K algébrique), $(P, P') \supset (\Pi_\alpha)$, donc P n'est pas séparable.
Supposons maintenant toutes les racines de P simples dans son corps de décomposition L/K. Soit $R \in K[X]$ irréductible tel que $(R) = (P, P')$. Comme $R \mid P$ dans $L[X]$ et que P est scindé dans L, R est aussi scindé dans $L[X]$. Une racine que P et P' ont en commun est une racine double de P, donc nécessairement $R \in K$ et $(P, P') = K[X]$. □

Remarque. Le polynôme $P \in K[X]$ est séparable si et seulement si P a exactement $\deg P$ racines dans $\overline{K}$.

Corollaire 1.8.11.

(1) Un polynôme $P \in K[X]$ irréductible est séparable si et seulement si $P' \neq 0$.

(2) Si $\mathrm{car}(K) = 0$, tout polynôme irréductible est séparable.

(3) Si $\mathrm{car}(K) = p > 0$, alors $P \in K[X]$ irréductible est séparable si et seulement si $P \notin K[X^p]$.

Démonstration. (1) : l'anneau $K[X]$ est principal, donc $(P, P') = (R)$ pour un $R \in K[X]$, d'où $R \mid P$. Comme P est irréductible, $R = \alpha P$ avec $\alpha \in K^\times$ ou $R \in K^\times$. Si P est séparable, $R \in K^\times$ et $P' \neq 0$ car $(P, 0) = (P) \neq K[X]$. Si $P' \neq 0$, comme $R \mid P'$, forcément $R \in K^\times$ (car sinon $\deg R = \deg P > \deg P'$), donc $(P, P') = K[X]$ ie P est séparable.
(2) : en caractéristique 0, $P' = 0$ implique $P \in K$ ce qui empêche que P soit irréductible, donc par contraposée, tout polynôme irréductible est séparable. (3) : en caractéristique $p > 0$, on a $P' = 0$ si et seulement si $P \in K[X^p]$, d'où le résultat. □

Corollaire 1.8.12. *$P \in K[X]$ est séparable si et seulement si c'est le produit de polynômes irréductibles séparables deux à deux distincts.*

Démonstration. **TODO** □

Étant donné ce qu'il se passe en caractéristique zéro, on peut se poser la question : sur quels corps les polynôme irréductibles sont-ils tous séparables ?

Définition 1.8.13. Un corps K est dit *parfait* si tout polynôme irréductible de $K[X]$ est séparable.

Proposition 1.8.14. *Un corps K est parfait si $\mathrm{car}(K) = 0$ ou $\mathrm{car}(K) = p > 0$ et le morphisme de Frobenius Fr_K est surjectif.*

Démonstration. Commençons par le sens inverse. On a déjà vu que les corps de caractéristique nulle sont parfaits. Supposons $\mathrm{car}(K) = p > 0$ et Fr_K surjectif. Soit $P \in K[X]$ irréductible. Supposons par l'absurde $P \in K[X^p]$. Comme Fr_K est surjectif, les coefficients de P sont des puissances p-ièmes, donc en fait $P = Q^p$. Ainsi, P ne peut pas être irréductible, ce qui conclut pour le sens inverse.
Supposons maintenant K parfait et $\mathrm{car}(K) = p > 0$. Soit $\alpha \in K \setminus K^p$ un élément non atteint par le morphisme de Frobenius. On considère le polynôme non séparable $X^p - \alpha$. Montrons qu'il est irréductible. Soit $Q \in K[X]$ tel que $Q \mid X^p - \alpha$. Alors, dans un corps de rupture L/K de $X^p - \alpha$, on dispose de $\beta \in L$ tel que $\beta^p = \alpha$. Ainsi, $Q \mid (X-\beta)^p$ dans $L[X]$, donc $Q = (X-\beta)^m$ pour un certain m. Si m et p sont premiers entre eux, alors on dispose de $u, v \in \mathbb{Z}$ tels que $um + vp = 1$. Comme $Q \in K[X]$, $Q(0) \in K[X]$, donc $\beta^m \in K$. Comme $\beta^p = \alpha \in K$, on en déduit $\beta^{um+vp} = \beta \in K$. Cela est absurde car $\alpha = \beta^p$ est alors atteint par le morphisme de Frobenius. □

Exemple 1.8.15.

(1) Tout corps fini est parfait (le morphisme de Frobenius est injectif donc surjectif).

(2) Tout corps algébriquement clos est parfait.

(3) $\mathbb{F}_p(T)$ n'est pas parfait.

1.9 Extensions séparables

Définition 1.9.1. Une extension de corps L/K algébrique est dite *séparable* si pour tout $\alpha \in L$, le polynôme minimal de α sur K est séparable. Le *degré séparable* d'une extension algébrique M/K est défini par

$$[M : K]_s = \mathrm{Card}(\{\sigma : M \hookrightarrow \overline{K} \mid \sigma \text{ prolonge } K \hookrightarrow \overline{K}\})$$

où $\overline{K}$ est une clôture algébrique de K.

Remarque. Le degré séparable est bien défini : par le théorème de Steinitz, $[M : K]_s$ ne dépend pas de la clôture algébrique $\overline{K}/K$. De plus, on sait que $[M : K]_s > 0$.

Exemple 1.9.2.

(1) $\mathbb{C}/\mathbb{R}$ est séparable et $[\mathbb{C} : \mathbb{R}]_s = 2$.

(2) Soient p premier, $L = \mathbb{F}_p(T)$ et $K = L^p = \mathbb{F}_p(T^p)$. Alors, $[L : K] = p$. Si $\sigma : L \to \overline{K}$ est un prolongement de $i : K \hookrightarrow \overline{K}$, alors $\sigma(T) = \sigma(T^p)^{1/p} = i(T^p)^{1/p}$, d'où σ est uniquement déterminé par i, car $X^p - i(T^p) = (X - \sigma(T))^p$ dans $\overline{K}[X]$. Donc, $[L : K]_s = 1 < p = [L : K]$.

Remarque.

(1) Soient $\sigma_1 : K \hookrightarrow \overline{K_1}$ et $\sigma_2 : K \hookrightarrow \overline{K_2}$ deux clôtures algébriques de K. Par la proposition 1.5.5, comme $\overline{K_1}/K$ est algébrique, il existe $\varphi : \overline{K_1} \hookrightarrow \overline{K_2}$ qui prolonge σ_2. Soit $\alpha \in \overline{K_2}$ et $P_\alpha \in K[X]$ son polynôme minimal sur K. En enlevant les identifications, on a $(\sigma_2 P_\alpha)(\alpha) = 0$, où $(\sigma_2 P_\alpha) \in \overline{K_2}[X]$. Alors, $(X - \alpha) \mid (\sigma_2 P_\alpha)$ dans $\overline{K_2}[X]$. Comme $\overline{K_1}$ est algébriquement clos, $\varphi(\overline{K_1})$ l'est aussi, donc $\sigma_2 P_\alpha = (\varphi \circ \sigma_1) P_\alpha \in \varphi(\overline{K_1})[X]$ est scindé dans $\varphi(\overline{K_1})[X] \subseteq \overline{K_2}$, d'où $X - \alpha \in \varphi(\overline{K_1})[X]$ et $\alpha \in \varphi(\overline{K_1})$. Ainsi, φ est surjectif donc un K-isomorphisme.

(2) Soit L/K une extension de corps algébrique. Soient $\sigma_1 : K \to \overline{K_1}$ et $\sigma_2 : K \to \overline{K_2}$ deux clôtures algébriques de K. Alors, en prenant φ comme ci-dessus un K-isomorphisme entre $\overline{K_1}$ et $\overline{K_2}$, l'application

$$\begin{array}{ccc} \{\pi : L \to \overline{K_1} \mid \pi_{|K} = \sigma_1\} & \to & \{\psi : L \to \overline{K_2} \mid \psi_{|K} = \sigma_2\} \\ \pi & \mapsto & \varphi \circ \pi \end{array}$$

est une bijection, d'où $[L : K]_s$ ne dépend pas de la clôture algébrique de K.

(3) Si L/K n'est pas algébrique, alors $[L : K]_s = 0$. Sinon, $[L : K]_s > 0$ par la proposition 1.5.5.

Lemme 1.9.3. *Soit $M/L/K$ une tour de corps algébrique. Alors,*

$$[M : K]_s = [M : L]_s[L : K]_s$$

Démonstration. Soit $\overline{K}/K$ une clôture algébrique de K. Soit $(\sigma_i)_{i\in I}$ la famille des K-plongements $L \hookrightarrow \overline{K}$. Par définition, $[L : K]_s = \mathrm{Card}(I)$. Pour $i \in I$ fixé, $\sigma_i : L \hookrightarrow \overline{K}$ est une clôture algébrique de L. Ainsi, par la remarque précédente, il existe $[M : L]_s$ morphismes $M \hookrightarrow \overline{K}$ qui fixent L. Notons-les $(\varphi^i_j)_{j\in J}$ avec $[M : L]_s = \mathrm{Card}(J)$. Alors, les prolongements de $K \hookrightarrow \overline{K}$ à $M \hookrightarrow \overline{K}$ sont en bijection avec $(\varphi^i_j)_{(i,j)\in I\times J}$, d'où la conclusion. □

Théorème 1.9.4. *Soit L/K une extension finie.*

(1) S'il existe $S \subseteq L$ fini et contenant uniquement des éléments séparables dans L/K, alors L/K est une extension séparable.

(2) On a $[L : K]_s \leq [L : K]$ avec égalité si et seulement si L/K est séparable.

Démonstration. Si $L = K(\alpha)$ avec $P_\alpha \in K[X]$ le polynôme minimal de α sur K, alors $[L : K]_s$ est le nombre de racines distinctes de P_α dans $\overline{K}$ une clôture algébrique de K. Il y en a au plus $[L : K]$ par le corollaire 1.4.8, d'où $[L : K]_s \leq [L : K]$ avec égalité si et seulement si P_α a exactement $\deg P_\alpha$ racines dans $\overline{K}$ c'est-à-dire si P_α est séparable.
Soit maintenant $L = K(S)$. Comme L/K est finie, on peut supposer S fini quitte à passer à un sous-ensemble. Écrivons $S = \{\alpha_1, \ldots, \alpha_n\}$. En appliquant la multiplication du degré et du degré séparable à la tour de corps

$$L/K(\alpha_1, \ldots, \alpha_n)/\cdots/K(\alpha_1)/K$$

on obtient $[L : K]_s \leq [L : K]$ par le paragraphe précédent.
Si on suppose que S ne contient que des éléments séparables dans L/K, alors pour tout i, α_i est séparable dans $K(\alpha_1, \ldots, \alpha_i)/K(\alpha_1, \ldots, \alpha_{i-1})$, car le polynôme minimal de α_i sur un surcorps de K divise celui sur K, qui n'a que des racines simples dans $\overline{K}$. Ainsi, $[L : K]_s = [L : K]$ dans ce cas par le premier paragraphe.
Réciproquement, si $[L : K] = [L : K]_s$, alors pour tout $\alpha \in L$, on a $[L : K(\alpha)]_s = [L : K(\alpha)]$ et $[K(\alpha) : K]_s = [K(\alpha) : K]$ d'où α est séparable dans L/K. Ainsi, L/K est séparable. □

Remarque. Si $K = \mathbb{Q}$ et $L = \mathbb{Q}(\sqrt{p} \mid p \text{ premier})$, alors $[L : \mathbb{Q}]$ est infini dénombrable, mais $\{\sigma : L \to \overline{\mathbb{Q}} \mid \sigma\ K\text{-morphisme}\}$ est de cardinal $2^{\aleph_0}$ (il faut choisir $\sqrt{p}$ ou $-\sqrt{p}$ pour tout p), donc $[L : K]_s$ est infini non dénombrable.

Proposition 1.9.5. *Soit $M/L/K$ une tour de corps. Si $\alpha \in M$ est séparable dans M/L et que L/K est séparable, alors α est séparable dans M/K. Par conséquence, M/K est séparable si et seulement si M/L et L/K le sont.*

Démonstration. Soit $P_\alpha \in L[X]$ le polynôme minimal de α sur L. Soit K'/K la sous-extension de L/K engendrée par les coefficients de P_α. Alors, K'/K est engendrée par un nombre fini d'éléments algébriques séparable, donc est finie, donc séparable, par le théorème précédent. Ainsi, $[K' : K]_s = [K' : K]$. Comme $P_\alpha \in K'[X]$, P_α est le polynôme minimal de α dans M/K', donc α est séparable dans M/K'. Cela implique par le théorème précédent que $K'(\alpha)/K'$ est séparable, donc $[K'(\alpha) :$

$K']_s = [K'(\alpha) : K']$. On obtient $[K'(\alpha) : K] = [K'(\alpha) : K]_s$, donc $K'(\alpha)/K$ est séparable, d'où α est séparable dans M/K.
Ainsi, si M/L et L/K sont séparables, M/K l'est aussi. Réciproquement, supposons M/K séparable. Alors, L/K est séparable. De plus, si $\alpha \in M$ et P_α^K, P_α^L sont ses polynômes minimaux sur K et L, alors $P_\alpha^L \mid P_\alpha^K$, donc si P_α^K est séparable, P_α^L aussi, d'où M/L est séparable. □

Corollaire 1.9.6. *L'ensemble des éléments séparables d'une extension L/K est une sous-extension séparable sur K. On l'appelle la* clôture séparable de K dans L.

Démonstration. Pour $\alpha, \beta \in L$ séparables dans L/K, $K(\alpha, \beta)/K$ est séparable, donc $\alpha - \beta, \alpha\beta^{-1}$ aussi. □

Remarque.

(1) Si L/K est algébrique et $L = K(S)$ avec $S \subseteq L$ contenant uniquement des éléments séparables, alors L/K est séparable.

(2) On peut définir *« la » clôture séparable* d'un corps K comme étant la clôture séparable de K dans $\overline{K}$. On la note $\overline{K}^{\text{sep}}$ ou $\overline{K}^{s}$. Elles sont toutes K-isomorphes.

Définition 1.9.7. Une extension algébrique L/K est dite *purement inséparable* ou *radicielle* si la clôture séparable de K dans L est K.

Remarque.

(1) L'extension $\overline{K}/\overline{K}^{\text{sep}}$ est purement inséparable.

(2) S'il existe une extension L/K purement inséparable avec $[L : K] > 1$ (c'est vrai ça ? ? ? **TODO**), alors $\operatorname{car} K > 0$. En particulier, si $\operatorname{car} K = 0$, on a $\overline{K} = \overline{K}^{\text{sep}}$.

Exemple 1.9.8. L'extension $\mathbb{F}_p(T)/\mathbb{F}_p(T^p)$ est purement inséparable.

Proposition 1.9.9.

(1) Soit K un corps. Alors, K est parfait si et seulement si $\overline{K} = \overline{K}^{\text{sep}}$.

(2) Si $L/\overline{K}^{\text{sep}}$ est séparable, on a $L = \overline{K}^{\text{sep}}$.

(3) Si $\alpha \in \overline{K} \setminus \overline{K}^{\text{sep}}$, α n'est pas séparable dans $\overline{K}/\overline{K}^{\text{sep}}$ et pas séparable dans $\overline{K}/K$.

Démonstration.

(1) K est parfait si et seulement si tous les polynômes irréductibles de $K[X]$ sont séparables si et seulement si tous les polynômes minimaux sur K d'éléments de $\overline{K}$ sont séparables si et seulement si $\overline{K} = \overline{K}^{\text{sep}}$.

(2) $L/\overline{K}^{\text{sep}}$ est algébrique donc il existe un plongement $L \hookrightarrow \overline{K}$. Comme L/K est séparable, on a $L \subseteq \overline{K}^{\text{sep}}$ et donc $L = \overline{K}^{\text{sep}}$.

(3) Voir (2). (rendre ça plus sympathique au lecteur **TODO**)

□

Définition 1.9.10. Un corps K est dit *séparablement clos* si $K = \overline{K}^{\text{sep}}$.

Proposition 1.9.11.

(1) Un corps K est séparablement clos si et seulement si tout polynôme irréductible séparable sur K est de degré 1.

*(2) Toute extension séparable d'un corps K se plonge dans $\overline{K}^{\text{sep}}$. (déjà fait juste au-dessus non ? **TODO**)*

Démonstration. **TODO** □

1.10 Théorème de l'élément primitif

Théorème 1.10.1. *Soit K un corps et $L = K(\alpha_1, \dots, \alpha_n)$ une extension finie de K. Si $\alpha_2, \dots, \alpha_n$ sont séparables dans L/K, alors il existe $\beta \in L$ tel que $L = K(\beta)$. On dit dans ce cas que L/K est une* extension simple.

Démonstration. Supposons d'abord K fini. Alors, L est fini comme extension finie de K. Alors, $L^\times$ est cyclique [3], donc $L = K(\alpha)$ pour $\alpha \in L$ un générateur de $L^\times$.
Supposons maintenant K infini. Il suffit de montrer le résultat pour $n = 2$ puis de faire une récurrence (c'est ici que le choix de ne pas supposer α_1 séparable prend son sens). Soient $P_{\alpha_1}, P_{\alpha_2}$ les polynômes minimaux de α_1, α_2 sur K, respectivement. Soit M/L un corps de décomposition de $P_{\alpha_1} P_{\alpha_2}$. Alors, dans $M[X]$, on a

$$P_{\alpha_1} = \prod_{i=1}^{s} (X - x_i) \quad \text{et} \quad P_{\alpha_2} = \prod_{j=1}^{t} (X - y_j)$$

avec $x_1 = \alpha_1$, $y_1 = \alpha_2$ et les y_j distincts deux à deux (car α_2 est séparable). On choisit

$$\gamma \in K \setminus \left\{ \frac{x_i - \alpha_i}{\alpha_2 - y_j} \;\middle|\; 2 \le j \le t, 1 \le i \le s \right\}$$

Un tel γ existe car K est supposé infini. Soit $\beta = \alpha_1 + \gamma\alpha_2 \in K$. Montrons que $K(\beta) = K(\alpha_1, \alpha_2)$. Par construction, on a $P_{\alpha_1}(\beta - \gamma\alpha_2) = P_{\alpha_1}(\alpha_1) = 0$ et $P_{\alpha_2}(\beta - \gamma y_j) \neq 0$ pour $j \neq 1$. Ainsi, les polynômes P_{α_2} et $R = P_{\alpha_1}(\beta - \gamma X)$ dans $K(\beta)[X]$ ont $\alpha_2 \in L$ pour seule racine commune. Ainsi, $\operatorname{pgcd}(P_{\alpha_2}, R) = X - \alpha_2$. Comme le PGCD ne dépend pas du corps ambiant, $X - \alpha_2 \in K(\beta)[X]$ d'où $\alpha_2 \in K(\beta)$, d'où $\alpha_1 = \beta - \gamma\alpha_2 \in K(\beta)$. Ainsi, $K(\beta) = K(\alpha_1, \alpha_2)$. □

Exemple 1.10.2.

(1) $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ est séparable, donc simple. Elle est engendrée par $\sqrt[3]{2} + j$. En général, il n'est pas évident de trouver un $x \in L$ tel que $L = K(x)$.

(2) Soit $L = \mathbb{F}_p(X, Y)$ et $K = L^p = \mathbb{F}_p(X^p, Y^p)$. Alors, L/K n'est pas simple :
   — $\{X^i Y^j \mid 0 \le i, j \le p-1\}$ est une base de L/K, donc $[L : K] = p^2$.
   — Tout $\alpha \in L$, est racine de $T^p - \alpha^p \in K[T]$ d'où son polynôme minimal sur K divise $T^p - \alpha^p$ donc est degré au plus p. Ainsi, $[K(\alpha) : K] \le p$ donc $L \neq K(\alpha)$.

Théorème 1.10.3. *Soit L/K une extension finie. Sont équivalents :*

(1) Il n'y a qu'un nombre fini de corps intermédiaires E entre K et L.

(2) Il existe $\alpha \in L$ tel que $L = K(\alpha)$ i.e. L/K est simple.

Démonstration. Dans le cas où K est fini, l'énoncé est clair. Supposons donc K infini.
Supposons (1). Soit $L = K(\alpha_1, \dots, \alpha_n)$. Il suffit de traiter le cas $n = 2$ par récurrence. La famille d'extensions donnée par $(K(\alpha_1 + \beta\alpha_2))_{\beta \in K}$ étant finie, on dispose de $u, v \in K$ distincts tels que $K(\alpha_1 + u\alpha_2) = K(\alpha_1 + v\alpha_2)$. Alors, $\alpha_2 = \frac{(\alpha_1 + v\alpha_2) - (\alpha_1 + u\alpha_2)}{v - u} \in K(\alpha_1 + u\alpha_2)$, d'où $\alpha_1 \in K(\alpha_1 + u\alpha_2)$ et on obtient $K(\alpha_1, \alpha_2) = K(\alpha_1 + u\alpha_2)$.
Supposons (2). Soit $L = K(\alpha)$ avec P_α le polynôme minimal de α sur K. Soit E un corps tel que

3. **TODO**mettre une ref

$K \subseteq E \subseteq L$. Alors, le polynôme minimal $P_{\alpha,E}$ de α sur E satisfait $P_{\alpha,E} \mid P_\alpha$ dans $E[X] \subseteq L[X]$. On remarque que P_α n'a qu'un nombre fini de diviseurs unitaires dans $L[X]$. Soit E_0 le corps engendré sur K par les coefficients de $P_{\alpha,E}$. Alors, $E \supseteq E_0 \supseteq K$ et $P_{\alpha,E}$ est irréductible sur $E_0[X]$, donc c'est le polynôme minimal de α sur E_0. On a donc $[L : E_0] = \deg P_{\alpha,E} = [L : E]$ d'où $E = E_0$. Ainsi, on peut retrouver E à partir de $P_{\alpha,E}$. On obtient une injection

$$\begin{array}{rcl} \{\text{corps intermédiaires dans } L/K\} & \to & \{\text{facteurs irréductibles unitaires de } P_\alpha \text{ dans } L[X]\} \\ E & \mapsto & P_{\alpha,E} \end{array}$$

d'où le résultat. □

1.11 Corps finis

Un corps K est dit fini si son cardinal est fini. On remarque qu'alors $\operatorname{car} K > 0$ car 1 est d'ordre fini dans $(K, +)$. Ainsi, il existe p premier tel que $\operatorname{car} K = p$. Soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Alors, $\mathbb{F}_p$ est un sous-corps de K. On a donc $\operatorname{Card}(K) = p^{[K:\mathbb{F}_p]}$ où $[K : \mathbb{F}_p] < \infty$ car K est fini et une extension de $\mathbb{F}_p$.

Proposition 1.11.1. *Pour tout p premier et tout $n \in \mathbb{N}^*$, il existe un corps K à p^n éléments. Ce corps est un corps de décomposition du polynôme $X^{p^n} - X \in \mathbb{F}_p[X]$, d'où tous deux corps à p^n éléments sont isomorphes.*

Démonstration. Soit K un corps de décomposition de $X^{p^n} - X \in \mathbb{F}_p[X]$. Comme ce polynôme est séparable, ses racines dans K sont simples et sont distinctes donc il y en a p^n. De plus, le sous-ensemble $K_0 = \{x \in K \mid x^{p^n} = x\}$ est un sous-corps de K, car

$$(xy)^{p^n} = x^{p^n} y^{p^n} \quad (x + y)^{p^n} = x^{p^n} + y^{p^n}$$

comme on travaille en caractéristique p. Ainsi, K_0 est un corps de décomposition de $X^{p^n} - X$ lui-même. Comme deux corps de décomposition d'un même polynôme sont isomorphes, $K_0 \simeq K$. Le corps K_0 est fini comme ensemble des racines d'un polynôme, donc $K = K_0$ et $\operatorname{Card}(K) = p^n$. Maintenant, si K est n'importe quel corps à p^n éléments, on sait que $K^\times$ est cyclique d'ordre $p^n - 1$. Ainsi, le théorème de Lagrange assure que si $x \in K^\times$, $x^{p^n-1} = 1$. En particulier, pour tout $x \in K$, $x^{p^n} = x$. Comme $\operatorname{car} K = p$ et que $\mathbb{F}_p \hookrightarrow K$, K est en fait un corps de décomposition de $X^{p^n} - X \in \mathbb{F}_p[X]$, car il est minimal pour la propriété de posséder toutes les racines de $X^{p^n} - X$. □

Dans la suite, on fait l'abus de notation de noter $\mathbb{F}_q$ un corps à q éléments. On a $q = p^n$ pour p premier et $n \in \mathbb{N}^*$.

Proposition 1.11.2. *Soit p premier et $n, m \in \mathbb{N}^*$. Alors, il existe un morphisme $\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$ si et seulement si $m \mid n$.*

Démonstration. S'il existe un morphisme de corps $\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$, alors en notant $d = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]$, on a $\operatorname{Card}(\mathbb{F}_{p^n}) = p^n = (\operatorname{Card}(\mathbb{F}_{p^m}))^d = (p^m)^d = p^{md}$ d'où $m \mid n$.
Réciproquement, supposons $n = dm$ pour $d \in \mathbb{N}^*$. Alors, $p^m - 1 \mid p^n - 1$. Écrivons $p^n - 1 = (p^m - 1)A$ pour $A \in \mathbb{N}^*$. On remarque que $\mathbb{F}_{p^n}$ est un corps de décomposition de $X^{p^n-1} - 1 \in \mathbb{F}_p[X]$. Comme

$$X^{p^n-1} - 1 = X^{A(p^m-1)} - 1 = ((X^{p^m-1}) - 1)Q$$

avec $Q \in \mathbb{F}_p[X]$ et $X^{p^n-1} - 1$ est séparable, on déduit que $X^{p^m-1} - 1$ est scindé dans $\mathbb{F}_{p^n}$. Ainsi, par le théorème 1.4.9, il existe un morphisme $\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$. □

Proposition 1.11.3. *Soit p premier. Soit $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$. Alors, pour tout $n \in \mathbb{N}^*$, $\overline{\mathbb{F}_p}$ contient exactement un corps à p^n éléments.*

Démonstration. Comme $\mathbb{F}_{p^n}$ est le corps de décomposition de $X^{p^n} - X \in \mathbb{F}_p[X]$, la clôture algébrique $\overline{\mathbb{F}_p}$ n'en contient qu'une seule copie. □

Remarque. On a en fait $\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$. Montrons l'inclusion $\subseteq$. Soit $x \in \overline{\mathbb{F}_p}$. Alors, $\mathbb{F}_p(x)/\mathbb{F}_p$ est algébrique et de type finie donc finie d'où $\mathrm{Card}(\mathbb{F}_p) < \infty$ avec $\mathrm{car}\, \mathbb{F}_p(x) = p$ d'où $\mathbb{F}_p(x) \simeq \mathbb{F}_{p^n}$.

Exemple 1.11.4. Une extension algébrique infinie de $\mathbb{F}_p$ qui n'est pas sa clôture algébrique est $\bigcup_{n \geq 1} \mathbb{F}_{p^{2^n}}$.

1.12 Théorie de Galois

Définition 1.12.1. Soit L/K une extension de corps. Le *groupe de Galois de L/K*, noté $\mathrm{Gal}(L/K)$, est par définition l'ensemble $\{\sigma \in \mathrm{Aut}(L) \mid \sigma_{|K} = \mathrm{id}_K\}$ muni de la composition.

Exemple 1.12.2.

(1) $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, z \mapsto \overline{z}\} \simeq \mathbb{Z}/2\mathbb{Z}$.

(2) $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}) = \{\mathrm{id}\}$.

(3) $\mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = \{\mathrm{id}\}$.

(4) On ne sait pas décrire $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

(5) Les groupes de Cremona $\mathrm{Gal}(\mathbb{C}(X_1, \ldots, X_n)/\mathbb{Q})$ sont compliqués à décrire pour $n \geq 3$.

Théorème 1.12.3. *Soit L/K une extension finie. Alors*

$$|\,\mathrm{Gal}(L/K)| \underset{(1)}{\leq} [L : K]_s \underset{(2)}{\leq} [L : K]$$

avec égalité pour (1) si et seulement si L/K est normale et égalité pour (2) si et seulement si L/K est séparable.

Démonstration. On a une action de $G = \mathrm{Gal}(L/K)$ sur $X = \{\sigma : L \to \overline{K} \mid \sigma \text{ est un } K\text{-morphisme}\}$ donnée par

$$\sigma \cdot g = \sigma \circ \sigma \in X$$

On remarque que $\sigma \circ g = \sigma$ implique $g = \mathrm{id}_L$ par injectivité de σ. On obtient donc une application injective

$$\begin{array}{rccc} \varphi_\sigma : & G & \to & X \\ & g & \mapsto & \sigma \circ g \end{array}$$

pour un $\sigma \in X$ fixé. Ainsi, $|G| \leq |X| = [L : K]_s$. De plus, l'application φ_σ est surjective si et seulement si tout morphisme de X est de la forme $\sigma \circ g$, c'est-à-dire si l'action est transitive. Cela est vrai si et seulement si pour tout K-morphisme $\varphi : L \to \overline{K}$, $\varphi(L)$ est toujours le même, ce qui est équivalent à la normalité de L/K (corollaire **TODO**jsp ce que c'est). Pour l'inégalité (2), voir le théorème 1.9.4. □

Remarque. On a en particulier dans le théorème précédent si L/K est « le » corps de décomposition d'un polynôme séparable.

Exemple 1.12.4.

(1) Dans $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{id}\}$, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]_s = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

(2) Dans $\mathbb{F}_p(T)/\mathbb{F}_p(T^p)$, on a $|\mathrm{Gal}(\mathbb{F}_p(T)/\mathbb{F}_p(T^p))| = [\mathbb{F}_p(T) : \mathbb{F}_p(T^p)]_s = 1$ et $[\mathbb{F}_p(T) : \mathbb{F}_p(T^p)] = p$.

Remarque. L'inégalité (1) du théorème reste vraie pour toute extension algébrique (même preuve). Si L/K est normale, alors on a égalité pour (1). Si on a égalité pour (1), cela n'implique pas L/K normale.

Définition 1.12.5. Soit L un corps et G un sous-groupe de $\mathrm{Aut}(L)$. On définit

$$L^G = \{\alpha \in L \mid \forall g \in G, g(\alpha) = \alpha\}$$

le *sous-corps de L fixé par G*. On remarque que G est un sous-groupe de $\mathrm{Gal}(L/L^G)$.

Théorème 1.12.6 (Artin)**.** *Si G est fini, on a*

$$[L : L^G] = \mathrm{Card}(G)$$

et L/L^G est une extension finie, normale, séparable, avec $\mathrm{Gal}(L/L^G) = G$.

Démonstration. Soient $K = L^G$ et $x \in L$. Soit $Q_x = \prod_{y \in G \cdot x} (X - y)$ où $G \cdot x = \{g(x) \mid g \in G\} \subseteq L$. Alors, pour $g \in G$, on a $g \cdot Q_x = Q_x$ (où on applique g à Q_x coefficient par coefficient). Ainsi, tout élément de G fixe les coefficients de Q_x, d'où $Q_x \in K[X]$. De plus, Q_x est séparable par construction, donc x est séparable sur K car annulé par un polynôme séparable, donc L/K est séparable. De plus, pour P_x le polynôme minimal de x, $\deg P_x \leq \deg Q_x \leq |G|$.
Soit $\alpha \in L$ tel que $\deg P_\alpha$ soit maximal parmi les $\deg P_x, x \in L$. Alors, l'extension $K(\alpha, x)/K$ est séparable et finie, donc par le théorème de l'élément primitif, il existe $z \in K(\alpha, x)$ tel que $K(\alpha, x) = K(z)$. Comme $K(z)$ est un corps de rupture de $P_z \in K[X]$, on a

$$[K(z) : K] = \deg P_z \leq \deg P_\alpha = [K(\alpha) : K] \leq [K(z) : K]$$

donc en fait $K(\alpha) = K(z) = K(\alpha, x)$. Ainsi, $x \in K(\alpha)$, donc $L = K(\alpha)$. En particulier, L/K est finie. Alors,

$$|G| \leq |\mathrm{Gal}(L/K)| \leq [L : K] = \deg P_\alpha \leq |G|$$

Donc, $[L : L^G] = \mathrm{Card}(G)$ et $G = \mathrm{Gal}(L/L^G)$. La normalité vient du théorème 1.12.3. □

Définition 1.12.7. Une extension de corps L/K est dite *galoisienne* si elle est normale et séparable.

Remarque. Une extension finie L/K est galoisienne si et seulement si $[L : K] = |\mathrm{Gal}(L/K)|$.

Remarque. Soit $M/L/K$ une tour de corps. Si M/K est galoisienne, alors M/L l'est aussi, mais L/K en général non. De plus, $\mathrm{Gal}(M/K) = \{\sigma \in \mathrm{Aut}(M) \mid \sigma_{|L} = \mathrm{id}_L\} \subseteq \mathrm{Gal}(M/K)$.

Théorème 1.12.8. *Soit L/K une extension. Sont équivalents :*

(1) L est le corps de décomposition d'un polynôme séparable sur K

(2) L/K est finie et $K = L^{\mathrm{Gal}(L/K)}$

(3) $K = L^G$ pour un certain sous-groupe G de $\mathrm{Aut}(L)$ *fini*

(4) L/K est galoisienne finie

Démonstration. Supposons (1). Alors, L/K est finie. Soit $K' = L^{\mathrm{Gal}(L/K)}$. Par le théorème d'Artin, $\mathrm{Gal}(L/K') = \mathrm{Gal}(L/K)$. De plus, comme L/K est séparable et normale (corollaire **TODO**5.5 inconnu et théorème 1.9.4), par le théorème 1.12.3, on a $|\mathrm{Gal}(L/K)| = [L : K]$. De manière similaire, comme un polynôme séparable sur K est aussi séparable sur K', L/K est normale et séparable, d'où $|\mathrm{Gal}(L/K')| = [L : K']$. On a donc $[L : K] = [L : K']$, ce qui implique $K = K'$.
Supposons maintenant (2). En posant $G = \mathrm{Gal}(L/K)$, G est un sous-groupe de $\mathrm{Aut}(L)$. Par le théorème 1.12.3, $|G| \leq [L : K] < +\infty$ (par hypothèse), donc G est fini.
L'implication (3) $\implies$ (4) est traitée par le théorème d'Artin.
L'implication (4) $\implies$ (1) vient de **TODO**les deux mêmes trucs que dans (1) implique (2) □

Proposition 1.12.9. *Soit L/K une extension de corps séparable. La clôture normale de L dans une clôture algébrique $\overline{K}/L/K$ de K est séparable, donc galoisienne sur K. On l'appelle la* clôture galoisienne *de L dans $\overline{K}$.*

Démonstration. Dans la preuve du théorème 1.7.10, les polynômes **TODO** □

Remarque.

(1) Si L/K est galoisienne, pour $\alpha \in L$ algébrique, les conjugués de α sont les éléments $g(\alpha)$ pour $g \in \mathrm{Gal}(L/K)$. Ainsi, le polynôme minimal de α est donné par $\prod_{g \in \mathrm{Gal}(L/K)} (X - g(\alpha))$.
On remarque que comme L/K est galoisienne, elle contient *tous* les conjugués de α dans une clôture algébrique $\overline{K}/L/K$ de K.

(2) Soit $P \in K[X]$. Soit L/K une extension de corps et $\alpha \in L$ tel que $P(\alpha) = 0$. Alors, pour tout $\sigma \in \mathrm{Gal}(L/K)$, comme $P(\sigma(\alpha)) = 0$, le groupe $\mathrm{Gal}(L/K)$ agit sur les racines de P, donc on a un morphisme de groupes
$$\mathrm{Gal}(l/K) \to S_{\{x \in L | P(x) = 0\}}$$
En général, ce morphisme n'est pas injectif. Cependant, si $L = K(\alpha)$ et $P_\alpha \in K[X]$ est le polynôme minimal de α, alors le morphisme est injectif :
$$\mathrm{Gal}(L/K) \hookrightarrow S_{\{x \in L | P(x) = 0\}} = S_{\mathrm{Gal}(L/K) \cdot \alpha}$$

Proposition 1.12.10. *Soit L/K une extension galoisienne. Soit $P \in K[X]$ un polynôme séparable et scindé dans L. Alors, l'action naturelle de $\mathrm{Gal}(L/K)$ sur les racines de P dans L est transitive si et seulement si P est irréductible sur K.*

Démonstration. Supposons l'action transitive. Soit $P = QR$ une factorisation de P dans $K[X]$. Comme P est scindé dans L, Q et R le sont aussi. Par séparabilité de P, Q et R n'ont pas de racines communes dans L. Or, l'action de $\mathrm{Gal}(L/K)$ envoie une racine de Q sur une autre racine de Q et idem pour R. Comme il n'existe qu'une seule orbite par hypothèse, nécessairement Q ou R n'a pas de racine, donc est constant. Ainsi, P est irréductible.
Réciproquement, supposons P irréductible. Soit $\alpha \in L$ une de ses racines. Alors, P est le polynôme minimal de α sur K. On en déduit par la remarque précédente
$$P = \prod_{\sigma \in \mathrm{Gal}(L/K)} (X - \sigma(\alpha))$$
ce qui montre que l'action est transitive. □

Remarque. Pour montrer que deux corps de décomposition d'une famille $(P_i)_{i\in I}$ de polynômes sur K sont K-isomorphes, on peut appliquer le théorème de Steinitz.

Exemple 1.12.11. Soit l'extension $\mathbb{Q}(\sqrt[3]{2}, i, j)/\mathbb{Q}$. Elle est galoisienne et le corps de décomposition de $(X^3-2)(X^2+1)$. L'action du groupe de Galois sur les racines est non transitive : aucun élément de $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, i, j)/\mathbb{Q})$ n'envoie $\sqrt[3]{2}$ sur i.

Corollaire 1.12.12. *Soit L/K une extension algébrique. Sont équivalents :*

(1) $K = L^{\mathrm{Gal}(L/K)}$

(2) L/K *est galoisienne*

Démonstration. Supposons $K = L^{\mathrm{Gal}(L/K)}$. Soit $\alpha \in L$ et $Q = \prod_{\sigma\in\mathrm{Gal}(L/K)} (X - \sigma(\alpha)) \in L[X]$. Comme L/K est algébrique, $\mathrm{Gal}(L/K)\cdot\alpha$ est fini. De plus, $\sigma \cdot Q = \sigma$, pour tout $\sigma \in \mathrm{Gal}(L/K)$, donc par hypothèse $Q \in K[X]$. Ainsi, $P_\alpha \mid Q$ où $P_\alpha \in K[X]$ est le polynôme minimal de α sur K. De plus, pour tout $x \in \mathrm{Gal}(L/K)\cdot\alpha$, comme $\sigma \cdot P_\alpha = P_\alpha$ pour tout $\sigma \in \mathrm{Gal}(L/K)$, on a $P_\alpha(x) = 0$. Ainsi, $Q \mid P_\alpha$ dans $L[X]$. Comme P_α, Q sont unitaires, on obtient $Q = P_\alpha$. Ainsi, P_α est séparable et L contient toutes ses racines dans une clôture algébrique. On en déduit que L/K est séparable et normale, c'est-à-dire galoisienne.
Réciproquement, supposons L/K galoisienne. Soit $K' = L^{\mathrm{Gal}(L/K)}$. Alors, $K \subseteq K'$. Soit $\alpha \in K'$ et $P_\alpha \in K[X]$ son polynôme minimal sur K. Il est scindé dans L et séparable. Si $\beta \in L$ est une racine de P_α, par la proposition précédente, comme P_α est irréductible, il existe $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma(\alpha) = \beta$. Comme $\alpha \in K'$, on a $\sigma(\alpha) = \alpha$, donc $\alpha = \beta$, d'où $\deg P_\alpha = 1$ et $\alpha \in K$. Ainsi, $K' = K$. □

1.13 Correspondance de Galois

Théorème 1.13.1. *Soit L/K une extension galoisienne finie et $G = \mathrm{Gal}(L/K)$.*

(1) L'application

$$\begin{array}{rccc} \varphi : & \{\text{sous-groupes de } G\} & \to & \{\text{sous-extensions de } L/K\} \\ & H & \mapsto & L^H \end{array}$$

est une bijection qui a pour réciproque $\psi : E \mapsto \mathrm{Gal}(L/E)$.

(2) Si H_1, H_2 sont des sous-groupes de G, alors $H_1 \subseteq H_2$ si et seulement si $L^{H_2} \subseteq L^{H_1}$ et dans ce cas $[H_2 : H_1] = [L^{H_1} : L^{H_2}]$.

(3) Pour $\sigma \in G$, $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$, où $H \subseteq G$. Cela équivaut à $\mathrm{Gal}(L/\sigma(E)) = \sigma H \sigma^{-1}$ pour $L/E/K$ avec $H = \mathrm{Gal}(L/E)$.

(4) Pour H un sous-groupe de G, H est distingué dans G si et seulement si l'extension de corps L^H/K est normale[4] *(donc galoisienne). Dans ce cas,* $\mathrm{Gal}(L^H/K) = G/H$.

Démonstration.

(1) On montre $\psi \circ \varphi = \mathrm{id}$ et $\varphi \circ \psi = \mathrm{id}$. On a $\mathrm{Gal}(L/L^H) = H$ par le théorème d'Artin, donc $\psi(\varphi(H)) = H$. On a aussi $L^{\mathrm{Gal}(L/E)} = E$ par le théorème 1.12.8, car L/K est galoisienne donc L/E l'est aussi.

4. Ce qui justifie l'appellation !

(2) Si $H_1 \subseteq H_2$, alors $L^{H_2} \subseteq L^{H_1}$. De même, si $L^{H_2} \subseteq L^{H_1}$, on a $\mathrm{Gal}(L/L^{H_1}) \subseteq \mathrm{Gal}(L/L^{H_2})$, c'est-à-dire $H_1 \subseteq H_2$. De plus, par le théorème d'Artin, pour H sous-groupe de G, on a

$$[L : L^H] = |\operatorname{Gal}(L/L^H)| = |H|$$

De plus, $[L : L^{H_2}] = [L : L^{H_1}][L^{H_1} : L^{H_2}]$ et $|H_2| = [H_2 : H_1]|H_1|$, d'où $[L^{H_1} : L^{H_2}] = [H_2 : H_1]$.

(3) Pour $\tau \in G$ et $\alpha \in L$, on a

$$\tau(\alpha) = \alpha \iff (\sigma\tau\sigma^{-1})(\sigma(\alpha)) = \sigma(\alpha)$$

c'est-à-dire que τ fixe α si et seulement si $\sigma\tau\sigma^{-1}$ fixe $\sigma(\alpha)$. Ainsi, pour un corps intermédiaire E de L/K, τ fixe E si et seulement si $\sigma\tau\sigma^{-1}$ fixe $\sigma(E)$. Alors, $\mathrm{Gal}(L/\sigma(E)) = \sigma \operatorname{Gal}(L/E)\sigma^{-1}$. Par (1), cela montre que $L^{\sigma H \sigma^{-1}} = \sigma L^H \sigma^{-1}$ pour H sous-groupe de G.

(4) Par le corollaire précédent, L^H/K est normale si et seulement si pour tout $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(L^H) = L^H$. Par injectivité de φ (dans (1)), cela équivaut à $\sigma H \sigma^{-1} = H$ pour tout $\sigma \in G$, c'est-à-dire $H \lhd G$. Pour conclure, on a un morphisme surjectif $\begin{array}{ccc} \mathrm{Gal}(L/K) & \to & \mathrm{Gal}(L^H/K) \\ g & \mapsto & g_{|L^H} \end{array}$ de noyau H.

□

TODOrelire cette preuve, je suis pas convaincu

2 Langage des catégories

L'auteur de ce document a pris quelques (beaucoup de) libertés par rapport aux notes originales.

2.1 Introduction aux catégories

La théorie des catégories a été introduite par Samuel Eilenberg et Saunders MacLane en 1945 pour formaliser la notion de « naturalité », c'est-à-dire d'absence de choix. Par exemple, si E est un espace vectoriel de dimension finie, il est isomorphe à son dual (par dimension) et à son bidual (encore une fois par dimension). Cependant, trouver un isomorphisme $E \xrightarrow{\sim} E^*$ demande de faire un choix : il n'y a pas d'isomorphisme canonique. Toutefois, entre E et E^{**}, il existe un isomorphisme « naturel » :

$$\begin{array}{ccc} E & \to & E^{**} \\ x & \mapsto & (\mathrm{ev}_x : \phi \in E^* \mapsto \phi(x)) \end{array}$$

La théorie des catégories permet de rendre précises ces notions. Elle a ensuite été utilisée afin de donner des noms à des concepts de topologie algébrique (Eilenberg et Steenrod 1952) puis s'est imposée comme langage permettant d'unifier beaucoup de constructions en algèbre.

Motivation des catégories. On donne un exemple venant de la topologie algébrique, mais il n'est pas nécessaire d'avoir fait de la topologie algébrique pour le comprendre. Le but de la topologie algébrique est de prendre un espace topologique et d'essayer de comprendre sa structure avec de l'algèbre, ce qui permet en particulier de distinguer des espaces. Par exemple, supposons qu'on veuille démontrer que la sphère de dimension deux $\mathbb{S}^2$ n'est pas homéomorphe au tore $\mathbb{T}^2$. Considérer toutes applications continues possibles $f : \mathbb{S}^2 \to \mathbb{T}^2$ est *a priori* très compliqué. La solution est de définir, pour $\mathbb{S}^2$ et $\mathbb{T}^2$, deux groupes, appelés leurs *groupes fondamentaux* et notés $\pi_1(\mathbb{S}^2)$ et $\pi_1(\mathbb{T}^2)$ qui encodent une partie de leur topologie. Ensuite, on démontre que si $\mathbb{S}^2$ et $\mathbb{T}^2$ sont homéomorphes, leurs groupes fondamentaux sont isomorphes, puis on calcule leurs groupes fondamentaux et on constate qu'ils sont non isomorphes (précisément, $\pi_1(\mathbb{S}^2) \simeq \{0\}$ et $\pi_1(\mathbb{T}^2) \simeq \mathbb{Z}^2$). Ainsi, $\mathbb{S}^2$ et $\mathbb{T}^2$ ne peuvent pas pas être homéomorphes. Plus généralement, on peut définir pour un espace topologique X son groupe fondamental $\pi_1(X)$, il encode une partie de la topologie de X et est en particulier invariant par homéomorphisme. Toutefois, on ne démontre pas *directement* que si deux espaces X et Y sont homéomorphes, alors leur groupes fondamentaux sont isomorphes. On démontre en réalité quelque chose de bien plus fort : n'importe quelle application continue $f : X \to Y$ induit un morphisme de groupes $\pi_1(f) : \pi_1(X) \to \pi_1(Y)$. En particulier, la définition de π_1 implique que si on a $X = Y$ et $f = \mathrm{id}_X$, on a $\pi_1(\mathrm{id}_X) = \mathrm{id}_{\pi_1(X)}$ (ce qui n'est peut-être pas très surprenant). De plus, si Z est un troisième espace topologique et $g : Y \to Z$ est une application continue, on a la relation

$$\pi_1(g \circ f) = \pi_1(g) \circ \pi_1(f)$$

et c'est de là que découle l'invariance par homéomorphisme : si X et Y sont homéomorphes, alors on dispose de $f : X \to Y$ continue bijective telle que $f^{-1} : Y \to X$ soit aussi continue. Mais alors,

$$\pi_1(f^{-1}) \circ \pi_1(f) = \pi_1(f^{-1} \circ f) = \pi_1(\mathrm{id}_X) = \mathrm{id}_{\pi_1(X)}$$

et de manière similaire, $\pi_1(f) \circ \pi_1(f^{-1}) = \mathrm{id}_{\pi_1(Y)}$, donc $\pi_1(X)$ et $\pi_1(Y)$ sont isomorphes. Plus généralement la relation $\pi_1(g \circ f) = \pi_1(g) \circ \pi_1(f)$ est très utile quand on travaille avec les groupes fondamentaux (voir n'importe quel cours de topologie algébrique qui parle de revêtements).

On peut alors remarquer que la relation $\pi_1(g \circ f) = \pi_1(g) \circ \pi_1(f)$ ressemble beaucoup à la définition d'un morphisme de groupes (ou au moins, de monoïdes). Effectivement, si on ne considère que les applications continues d'un espace dans lui-même, elles forment un monoïde pour la composition et $f \mapsto \pi_1(f)$ est un morphisme de monoïdes (des fonctions continues $X \to X$ dans les endomorphismes de groupe de $\pi_1(X)$). Néanmoins, la relation en toute généralité est plus qu'un morphisme de monoïdes. Le groupe fondamental est bien un morphisme d'une certaine structure et la réponse à la question « quelle structure ? » est « une catégorie ».

Un autre exemple. Soit E et F deux espaces vectoriels sur un corps k et $f : E \to F$ une application linéaire. Si $\phi : F \to k$ est une forme linéaire sur F, on peut lui associer une forme linéaire sur E en écrivant $\phi \circ f$. On obtient une application linéaire $f^* : \begin{array}{ccc} F^* & \to & E^* \\ \phi & \mapsto & \phi \circ f \end{array}$. On remarque que si $E = F$ et $f = \mathrm{id}_E$, alors $\mathrm{id}_E^* = \mathrm{id}_{E^*}$, comme précédemment. Maintenant, si G est un autre k-espace vectoriel et $g : F \to G$ est une autre application linéaire, on a la relation $\phi \circ (g \circ f) = (\phi \circ g) \circ f$ pour toute forme linéaire $\phi \in G^*$, c'est-à-dire que $(g \circ f)^* = f^* \circ g^*$. Cette relation est différente de celle pour le groupe fondamental, car ici on a retourné le sens de la composition. On parle de « contravariance ».

Définition 2.1.1. Une *catégorie* $\mathcal{C}$ est la donnée :

- D'une collection d'objets notée $\mathrm{Ob}(\mathcal{C})$
- Pour tous deux objets $X, Y \in \mathrm{Ob}(\mathcal{C})$, une collection notée $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ appelée les *morphismes de X vers Y*.
- Pour tous $X, Y, Z \in \mathrm{Ob}(\mathcal{C})$, une loi de composition

$$\circ_{X,Y,Z} : \mathrm{Hom}_{\mathcal{C}}(Y, Z) \times \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{C}}(X, Z)$$

telles que :

(1) La composition soit associative, au sens où pour tous $W, X, Y, Z \in \mathrm{Ob}(\mathcal{C})$ et $f \in \mathrm{Hom}_{\mathcal{C}}(W, X)$, $g \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ et $h \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$, on ait :

$$(h \circ_{X,Y,Z} g) \circ_{W,X,Y} f = h \circ_{X,Y,Z} (g \circ_{W,X,Y} f)$$

(2) Pour tout $X \in \mathrm{Ob}(\mathcal{C})$, il existe $\mathrm{id}_X \in \mathrm{Hom}(X, X)$ tel que pour tout objet $Y \in \mathrm{Ob}(\mathcal{C})$ et $f : X \to Y$, $g : Y \to X$, on ait

$$f \circ \mathrm{id}_X = f \quad \text{et} \quad \mathrm{id}_X \circ g = g$$

Ce morphisme est appelé *l'identité de X*.

Dans la suite, on omettra de préciser quels objets sont considérés pour la composition (on écrira juste $\circ$ au lieu de $\circ_{X,Y,Z}$). Pour dire $f \in \mathrm{Hom}_{\mathcal{D}}(X, Y)$, on écrira aussi $f : X \to Y$.

Remarque. Dans l'idée, les objets de $\mathcal{C}$ sont des objets mathématiques d'un certain type et les morphismes de $\mathcal{C}$ sont des applications entre eux. Par exemple, il existe une catégorie, notée **Set**, dont les objets sont les ensembles et les morphismes sont les applications entre eux (et la composée est la composée de fonctions usuelle et les identités sont des applications identités). C'est cela qui force à ne pas demander que $\mathrm{Ob}(\mathcal{C})$ soit un ensemble : il n'existe pas d'ensemble de tous les

ensembles. Si on travaille en théorie des classes, on peut par exemple comprendre le mot « collection » comme voulant dire « classe » et s'en sortir, car il existe une classe des tous les ensembles (mais attention, on ne peut alors pas former de catégorie dont les objets seraient toutes les classes). Plus généralement, il faut en gros restreindre la taille des objets considérés pour échapper à des paradoxes comme celui de Russell. Le livre [truc] développe en plus de détail. Ici, nous ne nous inquiéterons pas plus des difficultés liées aux ensembles.

Remarque. Dans l'écrasante majorité des catégories utiles en pratique, les collections $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ sont bien des ensembles. En général, une catégorie ayant cette propriété est dite *localement petite*. Nous supposons dorénavant que toutes les catégories sont localement petites afin de ne pas avoir à le préciser à chaque fois.

Exemple 2.1.2. Donnons quelques exemples usuels de catégories. La composition est implicitement la composition usuelle.

(1) La catégorie **Set**, dont les objets sont les ensembles et les morphismes sont les applications entre eux.

(2) La catégorie **Grp**, dont les objets sont les groupes et les morphismes sont les morphismes de groupes.

(3) La catégorie **Ring**, dont les objets sont les anneaux (commutatifs, unitaires) et les morphismes sont les morphismes d'anneaux.

(4) Soit k un corps. On note k-**Vect** la catégorie dont les objets sont les espaces vectoriels sur k et les morphismes sont les applications k-linéaires, ainsi que k-**Alg** la catégorie dont les objets sont les k-algèbres et les morphismes sont les morphismes de k-algèbres.

(5) La catégorie **Top**, dont les objets sont les espaces topologiques et les morphismes sont les applications continues.

Dans énormément de cas, les flèches représentent des vraies applications, mais rien la définition d'une catégorie ne requiert que ce soit le cas. Par exemple :

Exemple 2.1.3. Soit $(E, \leq)$ un ensemble partiellement ordonné. On peut former une catégorie $\mathcal{C}$ à partir de E en posant $\mathrm{Ob}(\mathcal{C}) = E$ et pour $x, y \in E$, $\mathrm{Hom}_{\mathcal{C}}(x, y) = \{(x \leq y)\}$ si $x \leq y$ et $\varnothing$ sinon. La composition est définie de la seule manière possible. Le fait que $(E, \leq)$ soit partiellement ordonné permet de vérifier qu'on définit bien une catégorie.

Remarque. Comme cas particulier, si X est un espace topologique, on peut former la catégorie $\mathrm{Ouv}(X)$ qui est la catégorie associée à l'ensemble partiellement ordonné formé par les ouverts de X avec l'inclusion. Cette catégorie est utile en géométrie pour définir la notion de faisceau.

La notion de catégorie permet de rendre précise la notion d'isomorphisme :

Définition 2.1.4. Deux objets $X, Y \in \mathrm{Ob}(\mathcal{C})$ d'une catégorie $\mathcal{C}$ sont dits *isomorphes* s'il existe deux morphismes $f : X \to Y$ et $g : Y \to X$ tels que $g \circ f = \mathrm{id}_X$ et $f \circ g = \mathrm{id}_Y$.

Exemple 2.1.5. Dans **Grp**, **Ring**, k-**Vect**, la notion catégorique d'isomorphisme correspond à la notion usuelle. Dans **Set**, deux ensembles sont isomorphes si et seulement s'ils sont en bijection. Dans **Top**, deux espaces sont isomorphes si et seulement s'il sont sont homéomorphes.

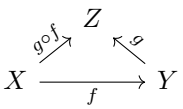
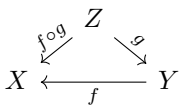
Exemple 2.1.6. Si on considère la catégorie associée à l'ordre partiel $(\mathbb{R}[X], |)$, alors deux polynômes sont isomorphes si et seulement si ils sont associés.

On peut conceptualiser une catégorie comme étant plein de points (les objets) avec des flèches entre les objets (les morphismes). On peut alors formellement renverser les flèches pour obtenir une nouvelle catégorie :

Définition 2.1.7. Soit $\mathcal{C}$ une catégorie. La *catégorie opposée* $\mathcal{C}^{\mathrm{op}}$ est obtenue en posant :

— $\mathrm{Ob}(\mathcal{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathcal{C})$

— Pour tous $X, Y \in \mathrm{Ob}(\mathcal{C}^{\mathrm{op}})$, $\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X)$.

La composition va alors à l'envers :  dans $\mathcal{C}$ devient  dans $\mathcal{C}^{\mathrm{op}}$.

Le renversement des flèches mène à la notion de dualité catégorique, qu'on examinera plus tard. Comme pour la plupart des structures algébriques, on a une notion de sous-structure pour les catégories :

Définition 2.1.8. Une *sous-catégorie* $\mathcal{C}'$ d'une catégorie $\mathcal{C}$ est une catégorie telle que :

— Les objets de $\mathcal{C}'$ forment une sous-collection de $\mathrm{Ob}(\mathcal{C})$

— Pour tous $X, Y \in \mathcal{C}'$, $\mathrm{Hom}_{\mathcal{C}'}(X, Y)$ est une partie de $\mathrm{Hom}_{\mathcal{C}}(X, Y)$

— La composition dans $\mathcal{C}'$ est induite par celle de $\mathcal{C}$.

De plus, si $\mathrm{Hom}_{\mathcal{C}'}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(X, Y)$ pour tous $X, Y \in \mathrm{Ob}(\mathcal{C}')$, on dit que $\mathcal{C}'$ est une *sous-catégorie pleine de* $\mathcal{C}$.

Exemple 2.1.9. Plusieurs catégories utiles sont des sous-catégories.

(1) La catégorie **Ab**, dont les objets sont les groupes abéliens et les morphismes les morphismes de groupes entre eux, est une sous-catégorie pleine de **Grp**.

(2) La catégorie k-**FinVect**, dont les objets sont les k-espaces vectoriels de dimension finie et les morphismes les applications linéaires entre eux, est une sous-catégorie pleine de k-**Vect**.

(3) La catégorie **Mon** des monoïdes avec les morphismes de monoïdes est une sous-catégorie non pleine de la catégorie des semi-groupes avec morphismes de semi-groupes **Sgr**. En effet, considérons le monoïde trivial $A = \{1\}$ et le monoïde $B = \{0, 1\}$. Alors, on a deux morphismes de semi-groupes $A \to B$ mais un seul morphisme de monoïdes $A \to B$ car un morphisme de monoïdes doit préserver les neutres.

2.2 Foncteurs

On a motivé les catégories comme étant la réponse à la question « de quelle structure est-ce que π_1 est un morphisme ? ». Maintenant que nous avons la structure, il est temps de définir les morphismes.

Définition 2.2.1. Soient $\mathcal{C}$ et $\mathcal{D}$ deux catégories. Un *foncteur covariant* F de $\mathcal{C}$ dans $\mathcal{D}$, ce qu'on note $F : \mathcal{C} \to \mathcal{D}$, est la donnée de :

— Pour tout objet $X \in \mathrm{Ob}(\mathcal{C})$, un objet $F(X) \in \mathrm{Ob}(\mathcal{D})$

— Pour tous deux objets $X, Y \in \mathrm{Ob}(\mathcal{C})$ et morphisme $f : X \to Y$ dans $\mathcal{C}$, un morphisme $F(f) : F(X) \to F(Y)$ dans $\mathcal{D}$.

vérifiant :

(1) Pour tout $X \in \mathrm{Ob}(\mathcal{C})$, $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$

(2) Pour tous morphismes composables $X \xrightarrow{f} Y \xrightarrow{g} Z$, $F(g \circ f) = F(g) \circ F(f)$.

Un foncteur *contravariant* de $\mathcal{C}$ dans $\mathcal{D}$ est un foncteur $F : \mathcal{C}^{\mathrm{op}} \to \mathcal{D}$. De manière équivalente, c'est un foncteur de $\mathcal{C}$ dans $\mathcal{D}$ mais on inverse le sens des flèches : un morphisme $f : X \to Y$ est envoyé sur un morphisme $F(f) : F(Y) \to F(X)$ et la condition (2) devient $F(g \circ f) = F(f) \circ F(g)$.

Sans précision supplémentaire, « un foncteur » est implicitement un foncteur covariant.

Exemple 2.2.2. Recontextualisons de ce qui a déjà été dit.

(1) Le groupe fondamental π_1 est un foncteur covariant **Top** $\to$ **Grp**.

(2) L'opération $E \mapsto E^*$ et $f \mapsto f^*$ définit un foncteur contravariant k-**Vect** $\to$ k-**Vect**.

Donnons de nouveaux exemples de foncteurs.

Exemple 2.2.3. Beaucoup de catégories qu'on a déjà vues ont pour objets des « ensembles avec une structure supplémentaire ». On en déduit la notion de foncteur d'oubli. Par exemple, on a un foncteur **Grp** $\to$ **Set** qui à un groupe $(G, \cdot)$ associe l'ensemble sous-jacent G et à un morphisme de groupes $f : (G, \cdot) \to (H, \star)$ associe l'application entre ensembles $f : G \to H$. On obtient par le même procédé des foncteurs d'oubli **Ring** $\to$ **Set**, **Top** $\to$ **Set**, k-**Vect** $\to$ **Set**. On peut aussi choisir d'oublier seulement une partie de la structure. Par exemple, on a un foncteur **Ring** $\to$ **Ab** qui à un anneau associe le groupe abélien obtenu avec l'addition (le foncteur oublie la multiplication). De même, on peut prendre un espace vectoriel normé et en oublier la norme, *et cetera*. Ces foncteurs sont moins inutiles qu'ils n'y paraissent à première vue car ils permettent de formaliser la notion d'« objet libre » avec la notion d'adjonction qu'on introduira plus tard.

Exemple 2.2.4. L'opération abélianisation définition un foncteur **Grp** $\to$ **Ab**, donné par

$$G \mapsto G/[G,G] \quad \text{et} \quad (f : G \to H) \mapsto (\tilde{f} : G/[G,G] \to H/[H,H])$$

où $\tilde{f}$ est obtenu à partir de f par composition avec la projection $H \to H/[H,H]$ puis par passage au quotient.

Définition 2.2.5. Un foncteur $F : \mathcal{C} \to \mathcal{D}$ est dit *fidèle/plein/pleinement fidèle* si pour tous $X, Y \in \mathrm{Ob}(\mathcal{C})$, l'application $\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(X,Y) & \to & \mathrm{Hom}_{\mathcal{D}}(F(X),F(Y)) \\ f & \mapsto & F(f) \end{array}$ est injective/surjective/bijective.

Exemple 2.2.6. TODO

(1) Le foncteur canonique **Ab** $\to$ **Grp** est pleinement fidèle.

(2) Le foncteur d'oubli **Grp** $\to$ **Set** est fidèle, mais pas plein.

(3)

Les foncteurs sont des morphismes de catégories. Comme avec n'importe quels morphismes, on peut les composer pour en obtenir un autre :

Proposition 2.2.7. *Soient $\mathcal{C}, \mathcal{D}, \mathcal{E}$ trois catégories et $F : \mathcal{C} \to \mathcal{D}$, $G : \mathcal{D} \to \mathcal{E}$ deux foncteurs. Alors, on définit un foncteur $G \circ F : \mathcal{C} \to \mathcal{E}$ sur les objets par $(G \circ F)(X) = G(F(X))$ et sur les morphismes par $(G \circ F)(f) = G(F(f))$.*

On a les catégories et les foncteurs entre eux. On aurait envie de parler de la « catégorie des catégories », mais il faut faire attention avec ce concept car la catégorie ne peut pas être objet d'elle-même. On peut parler en général de la catégorie des « petites » catégories (on impose une restriction sur la taille des catégories considérées afin d'échapper au paradoxe de Russell).

2.3 Transformations naturelles

Il existe une notion pertinente de morphisme entre foncteurs.

Définition 2.3.1. Soient $\mathcal{C}$ et $\mathcal{D}$ deux catégories et $F, G : \mathcal{C} \to \mathcal{D}$ deux foncteurs. Une *transformation naturelle* (ou morphisme de foncteurs) de F dans G est la donnée pour tout $X \in \mathrm{Ob}(\mathcal{C})$ d'un morphisme $\eta_X : F(X) \to G(X)$ telle que pour tous $X, Y \in \mathrm{Ob}(\mathcal{C})$ et $f : X \to Y$, le diagramme

$$\begin{array}{ccc} F(X) & \xrightarrow{\eta_X} & G(X) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(Y) & \xrightarrow{\eta_Y} & G(Y) \end{array}$$

commute. On note $\eta : F \Rightarrow G$. On dit que η est un *isomorphisme naturel* s'il existe une autre transformation naturelle $\psi : G \Rightarrow F$ telle que $\psi_X \circ \varphi_X = \mathrm{id}_{F(X)}$ et $\varphi_X \circ \psi_X = \mathrm{id}_{G(X)}$ pour tout $x \in \mathrm{Ob}(\mathcal{C})$. On écrit dans ce cas $F \cong G$.

Exemple 2.3.2. Pour tout foncteur $F : \mathcal{C} \to \mathcal{D}$, la transformation naturelle identité de F, donnée par $(\mathrm{id})_X = \mathrm{id}_{F(X)}$ est un isomorphisme naturel $F \Rightarrow F$.

Soient $F, G, H : \mathcal{C} \to \mathcal{D}$ trois foncteurs et $\eta : F \Rightarrow G$, $\phi : G \Rightarrow H$ deux transformations naturelles. Alors, pour $X, Y \in \mathrm{Ob}(\mathcal{C})$ et $f : X \to Y$, on a le diagramme commutatif

$$\begin{array}{ccccc} F(X) & \xrightarrow{\eta_X} & G(X) & \xrightarrow{\phi_X} & H(X) \\ \downarrow{\scriptstyle F(f)} & & \downarrow{\scriptstyle G(f)} & & \downarrow{\scriptstyle H(f)} \\ F(Y) & \xrightarrow{\eta_Y} & G(Y) & \xrightarrow{\phi_Y} & H(Y) \end{array}$$

d'où la donnée des morphismes $\phi_X \circ \eta_X$ donne une transformation naturelle $F \Rightarrow H$. On a donc les foncteurs, les transformations naturelles entre eux et une manière de composer les transformations naturelles. On obtient la notion de catégorie de foncteurs :

Définition 2.3.3. Soient $\mathcal{C}$ et $\mathcal{D}$ deux catégories. La *catégorie des foncteurs de $\mathcal{C}$ dans $\mathcal{D}$*, notée $\mathrm{Fun}(\mathcal{C}, \mathcal{D})$ ou $\mathcal{D}^{\mathcal{C}}$, a pour objets les foncteurs $\mathcal{C} \to \mathcal{D}$ et pour morphismes les transformations naturelles entre eux, où la composition est la composition « objet par objet ».

Les catégories étant des structures algébriques, on aimerait bien dire quand ce sont « les mêmes ». On peut vouloir poser la définition suivante :

Définition 2.3.4. Deux catégories $\mathcal{C}$ et $\mathcal{D}$ sont *isomorphes* s'il existe deux foncteurs $F : \mathcal{C} \to \mathcal{D}$ et $G : \mathcal{D} \to \mathcal{C}$ tels que $G \circ F = \mathrm{id}_{\mathcal{C}}$ et $F \circ G = \mathrm{id}_{\mathcal{D}}$.

Malheureusement, la notion d'isomorphisme de catégorie est trop restrictive en pratique. On lui préfère la notion d'équivalence :

Définition 2.3.5. Deux catégories $\mathcal{C}$ et $\mathcal{D}$ sont *équivalentes* s'il existe deux foncteurs $F : \mathcal{C} \to \mathcal{D}$ et $G : \mathcal{D} \to \mathcal{C}$ tels que $G \circ F \simeq \mathrm{id}_{\mathcal{C}}$ et $F \circ G \simeq \mathrm{id}_{\mathcal{D}}$.

Elle rappelle fortement la notion d'équivalence d'homotopie qui apparaît en topologie algébrique. L'équivalence de catégorie est une sorte d'« isomorphisme, à isomorphisme près ».

Exemple 2.3.6. Soit k un corps et considérons la catégorie k-**FinVect** des espaces vectoriels de dimension finie sur k. On sait intuitivement que l'algèbre linéaire sur k en dimension finie se résume à l'étude des espaces k^n pour $n \in \mathbb{N}$ et des applications linéaires entre eux. On peut rendre ça précis avec la notion d'équivalence. Soit $\mathcal{C}$ la catégorie dont les objets sont les espaces k^n et les morphismes les applications linéaires entre eux. On a un foncteur d'« inclusion » $I : \mathcal{C} \to k$-**FinVect**. Pour E un k-espace vectoriel de dimension finie n, choisissons et fixons $\phi_E : E \to k^n$ un isomorphisme d'espaces vectoriels. Alors, on définit un foncteur $H : k$-**FinVect** $\to \mathcal{C}$ par $H(E) = \phi_E(E)$ et $H(f : E \to F) = \phi_F \circ f \circ \phi_E^{-1}$. Montrons que I et H donnent l'équivalence de catégories souhaitée. **TODO**

Exemple 2.3.7. La catégorie des surfaces de Riemann compactes avec les morphismes holomorphes non constants entre elles est équivalente à la catégorie opposée des extensions de corps de $\mathbb{C}(T)$. C'est un résultat non trivial et permet de par exemple d'identifier le groupe de Galois absolu de $\mathbb{C}(T)$.

Exemple 2.3.8 (Dualité de Gelfand)**. TODO**

Exemple 2.3.9 (Dualité de Boole-Stone)**. TODO**

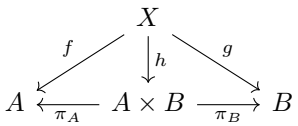
Exemple 2.3.10. Soit $\mathbf{Set}^p$ la catégorie des ensembles et des fonctions partielles entre eux, c'est-à-dire des fonctions pas forcément définies sur tout leur domaine de départ. Soit $\mathbf{Set}^*$ la catégorie des ensembles pointés, c'est-à-dire la catégorie dont les objets sont les paires (A, x) où A est un ensemble et $x \in A$, et où les morphismes $(A, x) \to (B, y)$ sont les applications $f : A \to B$ telles que $f(x) = y$. Ces catégories sont équivalentes. **TODO**

Théorème 2.3.11. *Un foncteur $F : \mathcal{C} \to \mathcal{D}$ est une équivalence de catégories si et seulement s'il est pleinement fidèle et* essentiellement surjectif*, c'est-à-dire si pour tout $Y \in \mathrm{Ob}(\mathcal{D})$, il existe $X \in \mathrm{Ob}(\mathcal{C})$ tel que $F(X) \simeq Y$.*

Démonstration. **TODO** □

2.4 Propriétés universelles

Un des points forts de la théorie des catégories est qu'elle permet de bien formaliser le concept de propriété universelle, qui consiste à décrire un objet par une propriété sur les morphismes autour de cet objet plutôt que de décrire l'objet lui-même directement. Donnons un exemple. Soient A, B deux ensembles. Si X est un ensemble et $f : X \to A, g : X \to B$ sont des applications, alors on peut former l'application $h : \begin{array}{ccc} X & \to & A \times B \\ x & \mapsto & (f(x), g(x)) \end{array}$ qui fait commuter le diagramme



où π_A, π_B sont les projections canoniques. De plus, h est l'*unique* application $X \to A \times B$ qui puisse faire commuter le diagramme. C'est la propriété universelle du produit cartésien de A et B : pour tout ensemble X avec deux applications $f : X \to A$ et $g : X \to B$, il existe une unique application $h : X \to A \times B$ faisant commuter le diagramme. Maintenant, la partie intéressante est que cette

propriété suffit à caractériser le produit cartésien avec les deux projections à unique bijection près. En effet, supposons qu'un autre ensemble C avec deux projections $p_A : C \to A$ et $p_B : C \to B$ vérifie la même propriété. On a alors les diagrammes **TODO**