Chapitre 12. Corps

Un **anneau non-unitaire** correspond à un la donnée de $A, +, \times, 0_A$ tels que $(A, +)$ groupe commutatif de neutre 0_A et $\times$ l.c.i. associative sur A et distributive a gauche et a droite par rapport a $+$.

Un **anneau = anneau unitaire** correspond à un la donnée de $A, +, \times, 0_A, 1_A$ tel que $(A, +, \times, 0_A)$ anneau et 1_A élément neutre pour la multiplication.

Un **anneau commutatif** est un anneau dans lequel $\times$ est commutatif

Un anneau non nul est **intègre** ssi $ab = 0 \Rightarrow a = 0$ ou $b = 0$

On note $\boldsymbol{A^\times}$ l'ensemble des éléments inversibles d'un anneau. On note $\boldsymbol{A^*} = A \setminus \{0_A\}$

Un **sous-anneau** d'un anneau $(A, +, \times)$ est une partie non vide de A qui est encore un anneau pour les lois induites et qui contient le neutre multiplicatif de A. Autrement dit c'est une partie $B \subseteq A$ telle que $\forall x, y \in B\ x + y \in B, \forall x \in B - x \in B,\ \forall x, y \in B\ xy \in B,\ 1_A \in B$. (entraine automatiquement $B \neq \emptyset$)

Un **morphisme d'anneaux (unitaires)** est une application $f : A \to B$ entre deux anneaux $(A, +, \times), (B, +, \times)$ telle que $\forall x, y \in A\ \ f(x + y) = f(x) + f(y),\ f(xy) = f(x)f(y),\ f(1_A) = 1_B$

Un **corps** est un anneau unitaire commutatif dans lequel tout élément non nul est inversible $A^\times = A^*$.

Un **morphisme de corps** est une application $f : \mathbb{K} \to \mathbb{L}$ entre deux corps $(\mathbb{K}, +, \times), (\mathbb{L}, +, \times)$ telle que $\forall x, y \in \mathbb{K}\ f(x + y) = f(x) + f(y),\ f(xy) = f(x)f(y)$, on a alors $f(1_\mathbb{K}) = 1_\mathbb{L}$

Un morphisme de corps est donc un morphisme d'anneaux unitaires.

On dit que $(\boldsymbol{E}, +, \cdot)$ **est un** $(\mathbb{K}, +_\mathbb{K}, \times)$ **espace vectoriel** ssi $(\mathbb{K}, +_\mathbb{K}, \times)$ est un corps, $(E, +)$ est un groupe abélien, $\cdot$ est une l.c.e. sur $(E, \mathbb{K})$, et pour tous $x, y \in E, \alpha, \beta \in \mathbb{K}$ on a $\begin{cases} 1_\mathbb{K} x = x \\ \alpha(\beta x) = (\alpha\beta)x \\ \alpha(x + y) = \alpha x + \alpha y \\ (\alpha +_\mathbb{K} \beta)x = \alpha x + \beta x \end{cases}$

Un morphisme d'evs, d'un $\mathbb{K}$ev E vers un $\mathbb{K}$ev F sur le même corps $\mathbb{K}$ est une application $u : E \to F$ telle que $\forall x, y \in E\ \ u(x + y) = u(x) + u(y)$ et $\forall \alpha \in \mathbb{K}\ \forall x \in E\ u(\alpha x) = \alpha u(x)$, càd telle que $\forall \alpha \in \mathbb{K}\ \forall x, y \in E\ \ u(\alpha x + y) = \alpha u(x) + u(y)$

On dit que $(\boldsymbol{E}, +, \cdot, \times)$ **est une** $(\mathbb{K}, +_\mathbb{K}, \times_\mathbb{K})$**-algèbre (unitaire)** ssi $(E, +, \cdot)$ est un $(\mathbb{K}, +_\mathbb{K}, \times_\mathbb{K})$-espace vectoriel, $(E, +, \times)$ est un anneau (unitaire), et pour tous $x, y \in E, \alpha \in \mathbb{K}\ \ \alpha(xy) = (\alpha x)y = x(\alpha y)$

Une $\mathbb{K}$**-sous-algèbre** d'une $\mathbb{K}$-algèbre E est une partie non vide F de E, telle que $1_F = 1_E$ / $1_E \in F$, et qui munie des lois induites $+, \cdot, \times$ est encore une $\mathbb{K}$-algèbre.

Caractérisation sous-algèbre. Une partie $F \subseteq E$ d'une $\mathbb{K}$-algèbre E, est une $\mathbb{K}$**-sous-algèbre** de E ssi $(F, +, \times)$ est un sous-anneau unitaire de $(E, +, \times)$ et $(F, +, \cdot)$ $\mathbb{K}$-sev de $(E, +, \cdot)$ ssi $\forall \alpha \in \mathbb{K}\ \forall x, y \in F\ \ \alpha x + y \in F,\ \ xy \in F$ et $1_E \in F$

On a donc (dans le cas unitaire) $\ 1_F = 1_E$.

Un **morphisme d'algèbres**, d'une $\mathbb{K}$-algèbre E vers une $\mathbb{K}$-algèbre F sur le même corps $\mathbb{K}$ est à la fois un morphisme d'anneau et un morphisme d'espaces vectoriels de E vers F càd que c'est une application $u : E \to F$ telle que $\forall \alpha \in \mathbb{K}\ \forall x, y \in E\ \ u(\alpha x + y) = \alpha u(x) + u(y),\ u(xy) = u(x)u(y),\ u(1_E) = 1_F$.

Séries formelles. On note V un ensemble quelconque d'indéterminées.

Une **série formelle d'indéterminées $\boldsymbol{V}$ sur un anneau commutatif $\boldsymbol{A}$** correspond à un élément $A^{\mathbb{N}^{(V)}} = \{a : \mathbb{N}^{(V)} \to A\}$. On note $\sum_{\alpha \in \mathbb{N}^{(V)}} a_\alpha X^\alpha$, la série formelle correspondant a $a : \mathbb{N}^{(V)} \to A$.

On note $\boldsymbol{A}[\![\boldsymbol{V}]\!]$ l'ensemble des séries formelles d'indéterminées V sur un anneau commutatif A.

On définit $\sum_{\alpha \in \mathbb{N}^{(V)}} a_\alpha X^\alpha + \sum_{\alpha \in \mathbb{N}^{(V)}} b_\alpha X^\alpha = \sum_{\alpha \in \mathbb{N}^{(V)}} (a_\alpha + b_\alpha) X^\alpha$

On définit $\left(\sum_{\alpha \in \mathbb{N}^{(V)}} a_\alpha X^\alpha\right) \times \left(\sum_{\alpha \in \mathbb{N}^{(V)}} b_\alpha X^\alpha\right) = \sum_{\gamma \in \mathbb{N}^{(V)}} \left(\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta\right) X^\gamma$

$\left(A[\![V]\!], +, \times\right)$ est un anneau commutatif unitaire, avec $0 = \sum_{\alpha \in \mathbb{N}^{(V)}} 0 X^\alpha$, de $1 = 1X^0$.

Polynômes.

Un **polynôme d'indéterminées $\boldsymbol{V}$ sur un anneau commutatif $\boldsymbol{A}$** correspond à une série formelle

$\sum_{\alpha\in\mathbb{N}^{(V)}} a_\alpha X^\alpha$, donc à un $a\colon \mathbb{N}^{(V)} \to A$, tel que $\{\alpha \in \mathbb{N}^{(V)} \mid a_\alpha \neq 0\}$ est fini.
On note $\boldsymbol{A[V]}$ l'ensemble des polynômes formels d'indéterminées V sur A.
$(A[V], +, \times)$ est un anneau commutatif unitaire, avec $0 = 0X^0, 1 = 1X^0$.
Soit $\mathbb{K}$ un corps, et $\mathbb{L}$ un sur-corps de $\mathbb{K}$.
Pour $P \in \mathbb{K}[V]$, et $x = (x_v)_{v\in V} \in \mathbb{L}^V$, on note $\boldsymbol{P(x)}$ l'évaluation de P en x.
On note $\boldsymbol{\phi}^{\mathbb{L}}\colon \mathbb{K}[V] \times \mathbb{L}^V \to \mathbb{L}\colon (P, x) \mapsto P(x)$
On note $\boldsymbol{\phi}_{\boldsymbol{P}}^{\mathbb{L}} = \widetilde{\boldsymbol{P}}\colon \mathbb{L}^V \to \mathbb{L}\colon x \mapsto P(x)$, **la fonction polynomiale $\boldsymbol{P}$ sur** $\mathbb{L}$. $\tilde{P}(x) = P(x) = \phi(P, x)$
On note $\boldsymbol{\phi}_{\boldsymbol{x}}^{\mathbb{L}}\colon \mathbb{K}[V] \to \mathbb{L}\colon P \mapsto P(x)$, **le morphisme d'évaluation en un point $\boldsymbol{x} \in \mathbb{L}^V$**.
On note $\widetilde{\ }^{\mathbb{L}}\colon \mathbb{K}[V] \to (\mathbb{L}^V \to \mathbb{L})\colon P \mapsto \tilde{P}$, **la fonctionnalisation polynômiale dans** $\mathbb{L}$.
La fonctionnalisation polynomiale est un morphisme de $\mathbb{K}$-algèbres.
Le morphisme d'évaluation en un point est un morphisme de $\mathbb{K}$-algèbres.
Fractions rationnelles.
Pour un corps $\mathbb{K}$, $\mathbb{K}[V]$ est un anneau intègre.
Pour un corps $\mathbb{K}$, $\mathbb{K}(\boldsymbol{V}) = Frac(\mathbb{K}[V]) = \left\{\frac{\sum_{\alpha\in\mathbb{N}^{(V)}} a_\alpha X^\alpha}{\sum_{\alpha\in\mathbb{N}^{(V)}} b_\alpha X^\alpha} : \sum_{\alpha\in\mathbb{N}^{(V)}} a_\alpha X^\alpha \in \mathbb{K}[V], \sum_{\alpha\in\mathbb{N}^{(V)}} b_\alpha X^\alpha \in \mathbb{K}[V]^*\right\}$
Pour un corps $\mathbb{K}$, $(\mathbb{K}(V), +, \times)$ est un corps.
Soit $\mathbb{K}$ un corps, et $\mathbb{L}$ un sur-corps de $\mathbb{K}$.
L'ensemble de définition d'une fraction $F = \frac{P}{Q} \in \mathbb{K}(V)$ dans $\mathbb{L}$ est $\boldsymbol{D}_{\mathbb{L}}(\boldsymbol{F}) = \{x \in \mathbb{L}^V \mid Q(x) \neq 0\}$
Pour $F \in \mathbb{K}(V)$, et $x \in D(F)$, on note $\boldsymbol{F(x)}$ l'évaluation de F en x.
Pour $F \in \mathbb{K}(V)$, et $x \in \mathbb{K}^V \setminus D(F)$, on note $\boldsymbol{F(x)} = \infty$
On note $\boldsymbol{\phi}\colon \mathbb{K}(V) \times \mathbb{L}^V \to \mathbb{L}\colon (F, x) \mapsto F(x)$
On note $\boldsymbol{\phi}_{\boldsymbol{F}} = \widetilde{\boldsymbol{F}}\colon \mathbb{L}^V \to \mathbb{L}\colon x \mapsto F(x)$, **la fonction rationnelle $\boldsymbol{F}$**. $\tilde{F}(x) = F(x) = \phi(F, x)$
On note $\boldsymbol{\phi}_{\boldsymbol{x}}\colon \mathbb{K}(V) \to \mathbb{L}\colon F \mapsto F(x)$, **le morphisme d'évaluation en $\boldsymbol{x}$**.
On note $\widetilde{\ }\colon \mathbb{K}(V) \to (\mathbb{L}^V \to \mathbb{L})\colon F \mapsto \tilde{F}$, **la fonctionnalisation rationnelle**.
La fonctionnalisation rationnelle est un morphisme de $\mathbb{K}$-algèbres.
Le morphisme d'évaluation en un point est un morphisme de $\mathbb{K}$-algèbres.
I. Extensions de corps
Un morphisme de corps est non nul et injectif.
Un morphisme d'anneaux d'un corps vers un anneau est soit nul soit injectif.
Pour un corps $\mathbb{K}$, il existe un unique morphisme d'anneaux $c_{\mathbb{K}} : (\mathbb{Z}, +, \times) \to (\mathbb{K}, +, \times)$ tel que $c_{\mathbb{K}}(1) = 1_{\mathbb{K}}$
On a $\forall n \in \mathbb{Z}\ \ c_{\mathbb{K}}(n) = n1_{\mathbb{K}}$, la **caractéristique du corps** $\mathbb{K}$ est le générateur $\boldsymbol{car}(\mathbb{K})$ positif de $\ker c_{\mathbb{K}}$
qui est un idéal de $\mathbb{Z}$ donc un $n\mathbb{Z}$ pour un unique n qui s'avère être le plus petit $n \geq 2$ tel que $n1_{\mathbb{K}} = 0_{\mathbb{K}}$
La caractéristique d'un corps est soit nulle, soit un nombre premier.
Le morphisme $c_{\mathbb{K}}$ est injectif ssi la caracteristique de $\mathbb{K}$ est nulle.
Dans ce cas $c_{\mathbb{K}}$ se prolonge en un morphisme de corps $c_{\mathbb{K}}\colon \mathbb{Q} \to \mathbb{K}\colon \frac{p}{q} \mapsto \frac{c_{\mathbb{K}}(p)}{c_{\mathbb{K}}(q)}$
$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times\right)$ est un corps ssi c'est un anneau intègre ssi n est premier.
Un sous-groupe fini du groupe multiplicatif d'un corps est cyclique.
Pour $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}, +, \times\right)$ avec p premier, le groupe $\left(\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*, \times\right)$ est cyclique, ce qui n'était pas évident a priori.
Un **sous-corps d'un corps** $\mathbb{K}$ correspond à une partie $\mathbb{H}$ de $\mathbb{K}$ qui muni des lois induites est un corps.

L'intersection de sous-corps $\mathbb{K}$, est un sous-corps de $\mathbb{K}$

Le sous-corps engendré par une partie $\boldsymbol{P} \subseteq \mathbb{K}$ d'un corps $\mathbb{K}$, est le plus petit sous-corps de $\mathbb{K}$ qui contient P. On le note $\langle \boldsymbol{P} \rangle_{\mathbb{K}}$**.**

Un **sur-corps d'un corps** $\mathbb{K}$ correspond à un corps $\mathbb{L}$, dont $\mathbb{K}$ est un sous-corps.

Une **extension d'un corps** $\mathbb{K}$ correspond à un couple $(\mathbb{L}, j)$ où $\mathbb{L}$ est un corps et j un morphisme de corps injectif de $\mathbb{K}$ dans $\mathbb{L}$. $j: \mathbb{K} \to j(\mathbb{K}) \subseteq \mathbb{L}$ est un isomorphisme de corps, donc on identifie généralement $\mathbb{K}$ et $j(\mathbb{K})$, et on identifie j a l'inclusion $i: j(\mathbb{K}) \approx \mathbb{K} \to \mathbb{L}: x \mapsto x$.

Pour cette raison, <u>on identifie généralement sur-corps et extension de corps</u>.

Cependant, certaines constructions d'extensions ne sont pas naturellement des sur-corps (par exemple le corps de rupture) et la définition d'extension ci-dessus permet plus de souplesse.

On note un sur-corps/extension de corps $\mathbb{L}: \mathbb{K}$. On n'explicite généralement pas j, on considère $\mathbb{K} \subseteq \mathbb{L}$.

Toute extension $\mathbb{L}$ d'un corps $\mathbb{K}$ est une $\mathbb{K}$ algèbre. En particulier tout corps $\mathbb{K}$ est une $\mathbb{K}$ algèbre.

Une **tour d'extensions**, est une suite croissante finie ou non d'extensions de corps, càd une suite croissante de sur-corps.

L'extension formelle engendrée par un ensemble $\boldsymbol{V}$ sur un corps $\mathbb{K}$ est l'ensemble des fractions rationnelles sur $\mathbb{K}$, d'indéterminées V, càd $\mathbb{K}(V)$. C'est une extension $\mathbb{K}(V): \mathbb{K}$.

$\mathbb{M}$ **est sous-extension de** $\mathbb{L}: \mathbb{K}$ ssi $\mathbb{M}$ est un sous-corps de $\mathbb{L}$ et un sur-corps de $\mathbb{K}$.

Autrement dit ssi $\mathbb{K} \to \mathbb{M} \to \mathbb{L}$ est une tour d'extensions de corps.

On dit aussi que $\mathbb{M}$ **est corps intermédiaire entre** $\mathbb{K}$ **et** $\mathbb{L}$

On dit aussi que $\mathbb{L}$ **est une sur-extension de** $\mathbb{M}: \mathbb{K}$

L'intersection de sous-extensions de $\mathbb{L}: \mathbb{K}$, est une sous-extension de $\mathbb{L}: \mathbb{K}$.

On définit **la sous-extension de** $\mathbb{L}: \mathbb{K}$ **engendrée par une partie** $\boldsymbol{V \subseteq \mathbb{L}}$ **notée** $\mathbb{K}_{\mathbb{L}}(\boldsymbol{V})$ comme la plus petite sous-extension de $\mathbb{L}: \mathbb{K}$ contenant V, càd comme le plus petit sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et V, soit $\mathbb{K}_{\mathbb{L}}(\boldsymbol{V}) = \langle \mathbb{K} \cup V \rangle_{\mathbb{L}}$.

$\mathbb{K}_{\mathbb{L}}(V)$ est constitué des éléments de $\mathbb{L}$ pouvant être obtenus à partir d'éléments de $\mathbb{K}$ et de V grâce à un nombre fini d'additions, de multiplications et d'inversions. Autrement dit $\mathbb{K}_{\mathbb{L}}(V) = \phi^{\mathbb{L}}(\mathbb{K}(V), \mathbb{L}^V)$.

On obtient $\mathbb{K}_{\mathbb{L}}(V)$ **en évaluant** $\mathbb{K}(\boldsymbol{V})$ **dans** $\mathbb{L}$**.**

$\mathbb{K} \to \mathbb{K}_{\mathbb{L}}(V) \to \mathbb{L}$ est une tour d'extensions.

Le corps $\mathbb{K}(V)$ est unique, mais attention le corps $\mathbb{K}_{\mathbb{L}}(V)$, en général <u>dépend de $\mathbb{L}$</u>.

Par contre si $\mathbb{K} \to \mathbb{L} \to \mathbb{L}'$, et $V \subseteq \mathbb{L}$ alors $\mathbb{K}_{\mathbb{L}}(V) = \mathbb{K}_{\mathbb{L}'}(V)$. $\mathbb{K}_{\mathbb{L}}(V)$ ne dépend donc pas du corps considéré dans une tour d'extension fixée.

Une **extension** $\mathbb{L}: \mathbb{K}$ **est engendrée par une partie** $\boldsymbol{V \subseteq L}$ ssi $\mathbb{L} = \mathbb{K}_{\mathbb{L}}(V)$ càd ssi on l'obtient en évaluant $\mathbb{K}(V)$ dedans.

$\mathbb{K}(V): \mathbb{K}$ est une extension engendrée par V sur $\mathbb{K}$ car $\mathbb{K}(V) = \mathbb{K}_{\mathbb{K}(V)}(V)$.

Dans $\mathbb{L}: \mathbb{K}$, pour $V \subseteq \mathbb{L}$, $\mathbb{K}_{\mathbb{L}}(V)$ est engendrée par V car $\mathbb{K}_{\mathbb{L}}(V) = \mathbb{K}_{\mathbb{K}_{\mathbb{L}}(V)}(V)$ car $\mathbb{K} \to \mathbb{K}_{\mathbb{L}}(V) \to \mathbb{L}$ tour.

Une **extension simple d'un corps** $\mathbb{K}$ est une extension de $\mathbb{K}$ engendrée par un seul de ses éléments, donc correspond à $(\mathbb{L}, \alpha)$ avec $\mathbb{L}: \mathbb{K}$ extension $\alpha \in \mathbb{L}$, tels que $\mathbb{L} = \mathbb{K}_{\mathbb{L}}(\alpha) = \langle \mathbb{K} \cup \{\alpha\} \rangle_{\mathbb{L}}$.

Dans une extension $\mathbb{L}: \mathbb{K}$, pour $\alpha \in \mathbb{L}$, $\mathbb{K}_{\mathbb{L}}(\alpha)$ est une extension simple de $\mathbb{K}$.

L'extension formelle engendrée par une unique indéterminée α et un corps $\mathbb{K}$, càd $\mathbb{K}(\alpha)$ est une extension simple de $\mathbb{K}$.

Remarque : En théorie des corps il faut distinguer $\mathbb{K}_{\mathbb{L}}(\alpha)$ de $\mathbb{K}(\alpha)$. Bien que ce soient deux concepts

légèrement distincts, ils se comportent souvent de la même façon. On écrit souvent $\mathbb{K}_{\mathbb{L}}(\alpha)$ seulement $\mathbb{K}(\alpha)$, ce qui prête a confusion avec le corps des fractions formelles, si on a $\alpha \in \mathbb{L}$, on interprétera $\mathbb{K}(\alpha)$ comme signifiant $\mathbb{K}_{\mathbb{L}}(\alpha)$ (en général on utilise une minuscule grecque), si on a juste une indéterminée on écrit généralement une majuscule X, et $\mathbb{K}(X)$ se réfère au corps des fractions, pas a $\mathbb{K}_{\mathbb{L}}(X)$.
Pour A partie d'une extension $\mathbb{L}:\mathbb{K}$, $A \subseteq \mathbb{K}(A)$
Pour A partie d'une extension $\mathbb{L}:\mathbb{K}$, $\mathbb{K}\big(\mathbb{K}(A)\big) = \mathbb{K}(A)$
Pour A, B parties d'une extension $\mathbb{L}:\mathbb{K}$, $A \subseteq B \Rightarrow \mathbb{K}(A) \subseteq \mathbb{K}(B)$
Pour A, B parties d'une extension $\mathbb{L}:\mathbb{K}$, $\mathbb{K}(A)(B) = \mathbb{K}(A \cup B)$
Un **corps est premier** ssi il n'a pas d'autre sous-corps que lui-même.
$\mathbb{Q}$ est un corps premier. Pour p premier, $\mathbb{F}_p$ est un corps premier.
Le **sous-corps premier d'un corps** $\mathbb{K}$, est le plus petit sous-corps de $\mathbb{K}$ c'est-à-dire $\langle 1\rangle_{\mathbb{K}}$. Il est premier.
Le sous-corps premier d'un corps de caractéristique nulle, est isomorphe a $\mathbb{Q}$.
Le sous-corps premier d'un corps de caractéristique p premier, est isomorphe a $\mathbb{F}_p \approx \frac{\mathbb{Z}}{p\mathbb{Z}}$.
Un corps est premier ssi il coïncide avec son sous-corps premier.
Des corps d'une tour d'extensions, ont le même sous-corps premier.
Attention il existe des corps finis avec un nombre non premier d'éléments.
Un $\mathbb{K}$-**morphisme d'extensions de corps entre deux extensions** $\mathbb{L}:\mathbb{K}$ **et** $\mathbb{M}:\mathbb{K}$ est un morphisme d'anneaux de $\mathbb{L} \to \mathbb{M}$ qui vaut l'identité sur $\mathbb{K}$. Un tel morphisme est toujours injectif.
En fait, f: $\mathbb{K}$-morphisme d'extensions de corps $\mathbb{L} \to \mathbb{M}$ ssi f morphisme de $\mathbb{K}$-algebres de $\mathbb{L} \to \mathbb{M}$.
Un $\mathbb{K}$-**endomorphisme d'une extension** $\mathbb{L}:\mathbb{K}$ est un morphisme d'extensions de corps de $\mathbb{L} \to \mathbb{L}$.
Un $\mathbb{K}$-**automorphisme d'une extension** $\mathbb{L}:\mathbb{K}$ est un $\mathbb{K}$-endomorphisme bijectif de $\mathbb{L}:\mathbb{K}$.
Vu dans $\mathbb{K}:\mathbb{K}$, un $\mathbb{K}$-endomorphisme, n'est autre qu'un morphisme de corps $\mathbb{K}$.
On note $\boldsymbol{Aut}(\mathbb{K})$ l'ensemble des automorphismes sur le corps $\mathbb{K}$. Pour $\circ$, c'est un sous-groupe de $S(\mathbb{K})$ le groupe des permutations de $\mathbb{K}$.
Algébricité et Transcendantalité dans une algèbre.
Le morphisme d'évaluation polynomial en un point $\boldsymbol{a}$ d'une $\mathbb{K}$-algèbre $\boldsymbol{A}$: $\boldsymbol{\phi_a}: \mathbb{K}[X] \to A: P \mapsto P(a)$.
On note $\mathbb{K}_{\boldsymbol{A}}[\boldsymbol{a}]$ (ou juste $\mathbb{K}[a]$) l'image de ce morphisme, et $\boldsymbol{I}_{\mathbb{K},\boldsymbol{A}}(\boldsymbol{a})$ le noyau du morphisme.
$\mathbb{K}_A[a]$ est une $\mathbb{K}$ sous-algèbre de A appelée **sous-algèbre engendrée par $\boldsymbol{a}$**.
$I_{\mathbb{K},A}(a)$ est un idéal (principal) de $\mathbb{K}[X]$ appelé **idéal annulateur de $\boldsymbol{a}$.**
Le morphisme d'évaluation est un morphisme de $\mathbb{K}$-algèbres, surjectif dans $\mathbb{K}[a]$ par construction.
Le **morphisme d'évaluation polynomial factorisé** $\overline{\boldsymbol{\phi_a}}: \frac{\mathbb{K}[X]}{I_a} \to \mathbb{K}[a]$ est un isomorphisme de $\mathbb{K}$-algèbres.
Le morphisme d'évaluation fractionnel en un point $\boldsymbol{a}$ d'une $\mathbb{K}$-algebre $\boldsymbol{A}$: $\boldsymbol{\phi_a}: \mathbb{K}(X) \to A: F \mapsto F(a)$.
On note $\mathbb{K}_{\boldsymbol{A}}(\boldsymbol{a})$ (ou juste $\mathbb{K}(a)$) l'image de ce morphisme. On a $Ker(\psi_a) = I_a$
Le **morphisme d'évaluation fractionnel factorisé** $\overline{\boldsymbol{\psi_a}}: \frac{\mathbb{K}(X)}{I_a} \to \mathbb{K}(a)$ est un isomorphisme de $\mathbb{K}$-algèbres.
Pour $\mathrm{m} \in \mathbb{K}[\mathrm{X}]$ non constant, $\frac{\mathbb{K}[\mathrm{X}]}{\langle \mathrm{m}\rangle}$ est un corps ssi m est irréductible ssi $\langle \mathrm{m}\rangle$ idéal maximal.
Pour $\mathrm{m} \in \mathbb{K}[\mathrm{X}]$ non constant, $\frac{\mathbb{K}[\mathrm{X}]}{\langle \mathrm{m}\rangle}$ est $\mathbb{K}$-algèbre de dimension $\mathrm{d} = \deg(\mathrm{m})$ dont $\left(1, \overline{\mathrm{X}}, \overline{\mathrm{X}}^2, \dots, \overline{\mathrm{X}}^{\mathrm{d}-1}\right)$ est une base.
$\mathbb{K}[\mathrm{X}]$ est une $\mathbb{K}$-algèbre de dimension infinie dont $\left(X^k\right)_{k\in\mathbb{N}}$ est une base.

Un **élément d'une $\mathbb{K}$-algebre est transcendantal sur** $\mathbb{K}$ ssi $I_a = \{0\}$
Dans ce cas :
$\mathbb{K}[a]$ est $\mathbb{K}$-algèbre-isomorphe a $\mathbb{K}[X]$. Donc $\dim \mathbb{K}[a] = \infty$, $(a^n)_{n\in\mathbb{N}}$ base de $\mathbb{K}[a]$
$\mathbb{K}(a)$ est $\mathbb{K}$-algèbre-isomorphe a $\mathbb{K}(X)$.
Un **élément d'une $\mathbb{K}$-algebre est algébrique sur** $\mathbb{K}$ ssi $I_a \neq \{0\}$
Dans ce cas, le **polynôme minimal** d'un élément algébrique $a \in A$ noté $\boldsymbol{\pi_a^{\mathbb{K},A}}$ est l'unique polynôme de $\mathbb{K}[X]$ unitaire générant l'idéal annulateur de cet élément $\langle \pi_a \rangle = I_a$.
Autrement dit, c'est l'unique polynôme annulateur de a, unitaire de $\mathbb{K}[X]$. On a donc $\deg \pi_a \geq 1$
Ainsi, être un polynôme annulateur de a signifie être multiple du polynôme minimal.
$\mathbb{K}[a]$ est $\mathbb{K}$-algèbre-isomorphe a $\frac{\mathbb{K}[X]}{\langle \pi_a \rangle}$.
Dans le cas algébrique on a $\dim \mathbb{K}[a] = \dim\left(\frac{\mathbb{K}[X]}{\langle \pi_a \rangle}\right) = \deg(\pi_a) < \infty$.
$\left(1, a, a^2, \dots, a^{d-1}\right)$ est une base de $\mathbb{K}[a]$ avec $d = \dim \mathbb{K}[a] = \deg \pi_a$.
De plus, si A est intègre, π_a est irréductible sur $\mathbb{K}[X]$ et $\mathbb{K}[a] \approx \frac{\mathbb{K}[X]}{\langle \pi_a \rangle}$ est un corps, et donc $\mathbb{K}(a) = Frac(\mathbb{K}[a]) = \mathbb{K}[a]$. $\mathbb{K}(a) = \mathbb{K}[a] = vect\left(1, a, a^2, \dots, a^{d-1}\right)$
Tout élément de $\mathbb{K}(\alpha)$ s'écrit de façon unique comme un polynôme $\in \mathbb{K}[\alpha]$ de degré $< \deg \pi_\alpha$
Caractérisation dans un anneau intègre:
$a \in A^*$ est algébrique ssi $[\mathbb{K}[\alpha]\colon \mathbb{K}]$ fini ssi $[\mathbb{K}(\alpha)\colon \mathbb{K}]$ fini ssi $\mathbb{K}[a] = \mathbb{K}(a)$ ssi $a^{-1} \in \mathbb{K}[a]$ ssi a appartient à une extension finie de $\mathbb{K}$. Dans le cas contraire, a est transcendant.

I.1. Nombres algébriques – Nombres transcendants.

Pour une extension de corps $\mathbb{L}\colon \mathbb{K}$, on peut appliquer les définitions précédentes avec $a \in \mathbb{L}$ en voyant $\mathbb{L}$ comme une $\mathbb{K}$-algebre, qui est aussi un anneau intègre.
Un scalaire d'un corps $\mathbb{L}$ est dit **algébrique sur un corps** $\mathbb{K}$ si c'est un zéro d'un polynôme non nul de $\mathbb{K}$
Un scalaire d'un corps $\mathbb{L}$ est **transcendant sur un corps** $\mathbb{K}$ s'il n'est pas zéro d'un polynôme non nul de $\mathbb{K}$
Un **entier algébrique** est un zéro d'un polynôme unitaire (non nul) de $\mathbb{Z}[X]$.
Un nombre algébrique (tout court) est un nombre algébrique sur $\mathbb{Q}$. $i, \sqrt{2}, \sqrt{2} + \sqrt{3}$ sont algébriques.
$\sum_{n=0}^{\infty} 10^{-n!}$ est transcendant, e, π sont transcendants.
Si α et β sont algébriques (resp. entiers algébriques), alors $\alpha\beta$ aussi, et $\alpha + \beta$ aussi.
L'ensemble des entiers algébriques est un sous-anneau de $\mathbb{C}$.
L'ensemble des nombres algébriques est un sous-corps de $\mathbb{C}$ dénombrable.
Donc il existe beaucoup de nombre transcendants car $\mathbb{C}$ n'est pas dénombrable.
Une extension algébrique simple est une extension simple $\mathbb{K}(\alpha)\colon \mathbb{K}$ avec $\alpha \in \mathbb{L}$ algébrique sur $\mathbb{K}$.
Une extension transcendante simple est extension simple $\mathbb{K}(\alpha)\colon \mathbb{K}$ avec $\alpha \in \mathbb{L}$ transcendant sur $\mathbb{K}$.
Plus généralement une **extension algébrique (resp. transcendante)** d'un corps $\mathbb{K}$ est une extension dont tout $x \in \mathbb{L}$ est algébrique (resp. transcendant) sur $\mathbb{K}$.
Pour une extension de corps $\mathbb{K} \to \mathbb{L}$, la somme, le produit, l'inverse par un non nul, ou le quotient par un non nul, d'éléments de $\mathbb{L}$ algébriques sur $\mathbb{K}$, donne encore un élément de $\mathbb{L}$ algébrique sur $\mathbb{K}$.
La composée de deux extensions algébriques est algébrique.
$\sqrt[3]{2}$ algébrique de polynôme minimal $X^3 - 2$. Si p premier, $\sqrt{p}$ algébrique de polynôme minimal $X^n - p$
Nombre de Liouville. Les réels $\sum_{n=1}^{\infty} a_n 10^{-n!}$ avec $(a_n)_{n\in N} \in \{0, \dots, 9\}^N$ sont transcendants.

Le cardinal des réels transcendants est donc égal au cardinal de R.

I.2. Extensions algébriques

Le polynôme minimal n'est défini que dans le cadre d'une extension de corps algébrique et est toujours irréductible, puisque $\mathbb{L}$ est intègre.

Pour $\alpha \in \mathbb{L}$ algébrique, $\frac{\mathbb{K}[X]}{\langle \pi_\alpha \rangle} \approx \mathbb{K}[\alpha]$, $\mathbb{K}[\alpha]$ est un corps, $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.

Deux extensions algébriques simples qui admettent le même polynôme minimal sont isomorphes.

Un morphisme d'extensions entre $\mathbb{L}\colon \mathbb{K}$ et $\mathbb{M}\colon \mathbb{K}$ qui envoie $\alpha \in \mathbb{L}$ sur $\beta \in \mathbb{M}$ induit un isomorphisme entre les extensions simples $\mathbb{K}(\alpha) \approx \mathbb{K}(\beta)$, α algebrique ssi β algebrique et dans ce cas $\pi_\alpha = \pi_\beta$.

Sur une extension algébrique, tout endomorphisme d'extension est bijectif, et donc un automorphisme.

I.3. Extensions transcendantes

$\mathbb{K} \to \mathbb{K}(X)$ est une extension transcendante simple.

Toute extension transcendante simple $\mathbb{K} \to \mathbb{K}(\alpha)$ est algèbre-isomorphe à l'extension $\mathbb{K} \to \mathbb{K}(X)$.

I.4. Corps de rupture.

Un **corps de rupture d'un polynôme irréductible** $\boldsymbol{P} \in \mathbb{K}[\boldsymbol{X}]$ est une extension simple $\mathbb{K} \to \mathbb{K}(\alpha)$ dans laquelle α est une racine de P. De façon équivalente c'est une extension simple $\mathbb{K}(\alpha)$ algèbrement-isomorphe au quotient $\frac{\mathbb{K}[X]}{\langle P \rangle}$. Un corps de rupture d'un polynôme irréductible est toujours un corps.

Un polynôme irréductible P sur $\mathbb{K}$ admet toujours $\mathbb{K}[X]/\langle P \rangle$ pour corps de rupture et celui-ci est unique a isomorphisme près (puisqu'ils y sont tous isomorphe). On choisira généralement $\mathbb{K}[X]/\langle P \rangle$ par défaut.

Une extension algébrique simple est toujours un corps de rupture de son polynôme minimal.

Réciproquement, un corps de rupture est toujours une extension algébrique simple.

Dans $\mathbb{R}[X]$, $X^2 + 1$ est irréductible, on pose i une indéterminée, on pose $\mathbb{C} = \frac{\mathbb{R}[i]}{\langle i^2+1 \rangle}$ le corps de rupture de $X^2 + 1$, $\mathbb{C}$ est donc un corps et dans $\mathbb{C}$, $i^2 + 1 = 0$. i est algébrique de polynôme minimal $X^2 + 1$, donc $\mathbb{C} \approx \mathbb{R}[i] = \mathbb{R}(i)$ est de dimension 2, $\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$. La somme ne change pas le degré donc se calcule comme la somme de polynômes $(a + ib) + (a' + ib') = (a + a') + i(b + b')$, le produit dépassant le degré 1, doit passer au modulo $X^2 + 1$: $(a + ib)(a' + ib') = aa + i(ba' + ab') + i^2bb' = aa - bb' + i(ba' + ab')$. On retrouve donc les lois usuelles de $\mathbb{C}$.

Dans $\mathbb{C}[X]$, on peut donc factoriser: $X^2 + 1 = (X + i)(X - i)$

Attention dans un corps de rupture $\mathbb{K}(\alpha)$, P admet α pour racine par construction, mais P n'est pas forcement scindé dans $\mathbb{K}(\alpha)[X]$.

Exemple classique : $P = X^3 - 2 = (X - \alpha)(X^2 + \alpha X + \alpha^2)$ sur le corps de rupture $\mathbb{Q}(\alpha)[X]$ de P

II. Utilisation de l'algèbre linéaire

II.1. Degré d'une extension

Pour toute extension de corps $\mathbb{L}\colon \mathbb{K}$, alors $\mathbb{L}$ est un Kev.

Le **degré d'une extension de corps** $\mathbb{L}\colon \mathbb{K}$ noté $[\mathbb{L}\colon \mathbb{K}]$ est la dimension de $\mathbb{L}$ en tant que $\mathbb{K}$ev.

Pour une extension simple transcendante $\mathbb{K}(\alpha)\colon \mathbb{K}$ on a $[\mathbb{K}(\alpha)\colon \mathbb{K}] = \infty$

Pour une extension simple algébrique $\mathbb{K}(\alpha)\colon \mathbb{K}$ on a $[\mathbb{K}(\alpha)\colon \mathbb{K}] = \deg \pi_\alpha$

Pour deux extensions 2 corps successives $\mathbb{K} \to \mathbb{L} \to \mathbb{M}$ on a $[\mathbb{M}\colon \mathbb{K}] = [\mathbb{M}\colon \mathbb{L}] \times [\mathbb{L}\colon \mathbb{K}]$

Ainsi $[\mathbb{M}\colon \mathbb{K}] = \infty$ ssi $[\mathbb{M}\colon \mathbb{L}] = \infty$ ou $[\mathbb{L}\colon \mathbb{K}] = \infty$

Une **extension finie de corps**, est une extension de corps, de degré fini.

Une extension finie de corps est toujours algébrique.

Une extension algébrique simple est toujours finie.
Cependant il existe des extensions algébriques (non simples) de degré infini. (TODO).
Une extension de corps $\mathbb{L}$: $\mathbb{K}$ est finie ssi $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$ avec $\alpha_1, \dots, \alpha_n$ algébriques sur $\mathbb{K}$.

II.2. Construction à la règle et au compas

On se place dans $\mathbb{R}^2$ on fixe un ensemble fini de points $E_0 \subseteq \mathbb{R}^2$:
On considère toutes les droites reliant 2 points de E_0, et tous les cercles de centre un point de E_0 et de rayon une distance entre 2 points de E_0.
E_1 est l'ensemble fini des points d'intersection entre 2 de ces droites, entre 2 de ces cercles, ou entre une de ces droites et un de ces cercles. On a donc construit $E_1 = f(E_0)$
On définit par récurrence $E_2 = f(E_1)$, …, $E_n = f(E_{n-1})$ pour tout $n \in \mathbb{N}$
Un point (x, y) de R^2 est **constructible à la règle (non graduée) et au compas en 1 étape à partir de E_0** ssi $(x, y) \in E_1$.
Un point (x, y) de R^2 est **constructible à la règle et au compas à partir de E_0 (en un nombre fini d'étapes)** ssi $(x, y) \in \bigcup_{n\in\mathbb{N}} E_n$
Attention, dire un point est constructible en n etapes ne signifie pas qu'il est dans E_n.
Un **nombre réel est constructible à la règle et au compas** ssi il est l'abscisse ou l'ordonnée d'un point de $\mathbb{R}^2$ constructible a la règle et au compas en partant de $E_0 = \{(0,0), (0,1)\}$.
On note $\boldsymbol{E_{\mathbb{R}}}$ l'ensemble des réels constructibles à la règle et au compas.
Un **polygone convexe est constructible à la règle et au compas** ssi ses sommets le sont en partant d'un ensemble E_0 formé de deux sommets adjacents.
Un pentagone régulier est constructible à la règle et au compas.
Une **famille séquentiellement constructible à la règle et au compas en n étapes à partir de E_0** est une famille de n points $\big(p_1(x_1, y_1), \dots, p_n(x_n, y_n)\big)$ de $\mathbb{R}^2$ telle que $\forall k \in \{1, \dots, n\}$ le point p_k est constructible à la règle et au compas en 1 étape à partir de $E_0 \cup \{p_1, \dots, p_{k-1}\}$.
Un point est **constructible en n étapes** ssi il est le nième point d'une famille séquentiellement constructible.

Théorème de Wantzel, 1837. Soit une famille séquentiellement constructible à la règle et au compas en n étapes à partir de E_0 $\big(p_1(x_1, y_1), \dots, p_n(x_n, y_n)\big)$, en notant K_i le sous-corps de $\mathbb{R}$ engendré par les coordonnées des points de $\mathbb{R}^2$ de $E_0 \cup \{p_1, \dots, p_i\}$, alors on a pour tout i,
$\mathbb{K}_i = \mathbb{K}_{i-1}(x_i, y_i)$, x_i, y_i sont racines de polynômes de degré 2 a coefficients dans $\mathbb{K}_{i-1}$ et le degré $[\mathbb{K}_i : \mathbb{K}_{i-1}]$ est 1 ou 2. Par multiplicativité des degrés $[\mathbb{K}_n : \mathbb{K}_0]$ est une puissance de 2

Réciproque Wantzel. Soit E_0 une partie finie de $\mathbb{R}^2$, on pose $\mathbb{K}_0$ le sous-corps de $\mathbb{R}$ engendré par les coordonnées des points de E_0. Soit une famille $\big(p_1(x_1, y_1), \dots, p_n(x_n, y_n)\big)$, de n points de $\mathbb{K}^2$, on pose par récurrence $\mathbb{K}_i = \mathbb{K}_{i-1}(x_i, y_i)$. Si pour tout i, $\mathbb{K}_{i-1} \to \mathbb{K}_i$ est une extension de degré 1 ou 2, alors la famille $(p_1, \dots, p_n)$ est séquentiellement constructible à la règle et au compas en n étapes à partir de E_0.

Théorème de Wantzel, version réelle. L'ensemble des réels constructibles à la règle et au compas $E_{\mathbb{R}}$ est un sous-corps de $\mathbb{R}$ et donc une extension du sous-corps premier $\mathbb{Q}$. Un réel α est constructible ssi $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^s$ avec $s \in N$ ssi le degré du polynôme minimal sur $\mathbb{Q}$ de α est une puissance de 2.

Impossibilité de la duplication du cube. On ne peut pas construire à la règle et au compas, le côté d'un cube de volume double du volume d'un cube de côté donné. Autrement dit, $\sqrt[3]{2}$ n'est pas constructible.

Impossibilité de la trisection d'un angle en général. L'angle $\frac{\pi}{3}$ ne peut pas être divisé à la règle et au

compas en trois angles égaux. Autrement dit $\cos\left(\frac{\pi}{9}\right)$ n'est pas constructible.

Impossibilité de la quadrature du cercle. On ne peut pas construire à la règle et au compas le côté d'un carré dont l'aire est égale à celle d'un disque donné. Autrement dit $\sqrt{\pi}$ n'est pas constructible.

Impossibilité de la construction de l'heptagone régulier. On ne peut pas construire à la règle et au compas, le côté d'un heptagone régulier. Autrement dit $\cos\left(\frac{2\pi}{7}\right)$ n'est pas constructible.

L'ensemble des réels constructibles $E_{\mathbb{R}}$ est stable par $(x,y) \mapsto x+y,\ (x,y) \mapsto xy,\ (x, y \neq 0) \mapsto \frac{x}{y}$, $x > 0 \mapsto \sqrt{x}$

II.3. Corps de décomposition – Extensions normales – Extensions séparables

Un **corps de décomposition d'un polynôme non nul $\boldsymbol{P} \in \mathbb{K}[\boldsymbol{X}]^*$ sur un corps** $\mathbb{K}$ correspond à une extension de corps $\mathbb{K} \to \mathbb{L}$ minimale pour l'inclusion qui rend P scindé sur $\mathbb{L}$. Sur une telle extension, P admet autant de racines que son degré n et s'écrit $P = \lambda(X-\alpha_1)\dots(X-\alpha_n)$, ce qui permet d'écrire l'extension $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$

Un corps de décomposition est une extension finie.

F_4 est un corps de décomposition de X^2+X+1 sur F_2

$Q(\exp(2i\pi/n))$ est un corps de décomposition du n-ieme polynome cyclotomique ϕ_n sur Q. (vérifier)

$Q\left(\sqrt[3]{2}\right)$ n'est pas un corps de décomposition de X^3-2 sur Q

$Q\left(\sqrt[3]{2}, j\right)$ est un corps de décomposition de X^3-2 sur Q.

Existence d'un corps de décomposition. Un polynôme non nul sur un corps K, admet toujours un corps de décomposition sur K.

Unicité a isomorphisme près du corps de décomposition.

Soit 2 corps isomorphes $K \approx K'$ par l'isomorphisme $i: K \to K'$, soit un polynôme non nul $P \in K[X]$ et sa version $Q = i(P)$ dans $K'[X]$. Si $L: K$ est un corps de décomposition de P, et $L': K'$ est un corps de décomposition de $Q = i(P)$, alors $L \approx L'$ $\mathbb{K}$-isomorphes

Un **corps est algébriquement clos** ssi tout polynôme est scindé sur lui autrement dit ssi tout polynôme de degré ≥ 1 admet au moins une racine ssi il n'admet pas d'extension algébrique propre.

Une clôture algébrique d'un corps $\boldsymbol{K}$ est une extension <u>algébrique</u> $L: K$ telle que L est algébriquement clos.

Une clôture algébrique de K est un corps algébriquement clos <u>minimal</u> contenant K, puisque si M est un corps algébriquement clos contenant K alors, parmi les éléments de M, ceux qui sont algébriques sur K forment une clôture algébrique de K.

Une clôture algébrique d'un corps K a le même cardinal que K si K est infini ; elle est dénombrable si K est fini.

Souvent entre deux clôtures algébriques de K il n'y a pas unicité d'isomorphismes. Eviter de dire « la ».

$\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$. (théorème fondamental de l'algèbre)

Il existe des corps algébriquement clos dénombrables inclus dans C, qui contiennent (strictement) le corps des nombres algébriques ; ce sont les clôtures algébriques des extensions transcendantes du corps des rationnels, comme celle de l'extension $\mathbb{Q}(\pi)$.

Théorème de Steinitz. Tout corps K possède une clôture algébrique. (par Zorn ou Krull (requiert AC))

Deux clôtures algébriques de K sont toujours reliées par un isomorphisme de corps laissant invariants les éléments de K.

Un polynôme irréductible de $K[X]$ est dit **séparable sur K** ssi dans son corps de décomposition sur K, il n'a pas de racine multiple / toutes ses racines sont simples. Dans le cas contraire il est dit **inséparable sur K.**

Par exemple, $X^p - T \in F_p(T)[X]$ est irréductible et inséparable sur le corps de fractions $F_p(T)$.

Sur un corps K de caracteristique nulle, tout polynôme irréductible de $K[X]$ est séparable sur K.

Sur un corps K de caracteristique un premier p, un polynôme irréductible P de $K[X]$ est inséparable ssi $\exists Q \in K[X]\ P = Q(X^p)$.

Un polynôme de $K[X]$ réductible, dont tous les facteurs irréductibles sont séparables, est séparable.

Un élément $\alpha \in L$ d'une extension algébrique $L:K$ est dit **séparable** ssi son polynôme minimal sur K est séparable ssi α n'est pas racine du polynôme minimal dérivé : $\pi'_\alpha(\alpha) \neq 0$

Une **extension algébrique séparable**, est une extension algébrique dont tous les $\alpha \in L$ sont séparables.

Un polynôme est séparable si et seulement s'il est premier avec sa dérivée formelle.

Un polynôme irréductible est séparable si et seulement si sa dérivée formelle n'est pas nulle.

Supposons *K* de caractéristique *p* et *P*(*X*) un polynôme irréductible. Il est séparable si et seulement s'il n'existe pas de polynôme *Q*(*X*) dans *K*[*X*] tel que l'on ait l'égalité $P(X) = Q(X^p)$.

Soient *L* une extension algébrique de *K* et *M* une extension algébrique de *L*. Alors *M* est séparable sur *K* si et seulement si *M* est séparable sur *L* et *L* est séparable sur *K*.

Un corps K est dit **parfait** si toutes ses extensions algébriques sont séparables, autrement dit ssi tout polynôme irréductible de *K*[*X*] est séparable.

Tout corps de caractéristique nulle est parfait.

Un corps K est parfait si et seulement s'il est de caractéristique nulle ou, lorsqu'il est de caractéristique $p > 0$, si l'endomorphisme de Frobenius $x \mapsto x^p$ est surjectif (autrement dit tout élément de *K* possède une racine *p*-ième dans K). En particulier tout corps fini est parfait.

Tout corps algébrique sur un corps parfait est lui-même un corps parfait.

En revanche, en caractéristique non nulle *p* (un nombre premier), tous les corps ne sont pas parfaits. Considérons $L = F_p(X)$ le corps des fractions rationnelles sur le corps fini de cardinal *p*, *K* le sous-corps $F_p(X^p)$, et le polynôme irréductible $P(Y) = Y^p - X^p$ de *K*[*Y*]. Alors l'élément *X* de *L* est racine multiple (d'ordre *p*) de *P*(*Y*), qui n'est donc pas séparable.

Soit $L : K$ une extension finie de degré d et $M: K$ une extension quelconque. Alors, il existe au plus d K-morphismes distincts $L \to M$. En fait, si M est algébriquement clos, alors $L : K$ est séparable ssi il existe exactement d K-morphisme distincts $L \to M$.

Théorème de l'élément primitif. Tout extension finie séparable, est simple, c'est-à-dire engendrée par un seul élément appelé **l'élément primitif**.

Une **extension normale de corps** est une extension <u>algébrique</u> de corps $L: K$ qui reste stable par tout morphisme d'extension vers une sur-extension $M: K$ de $L: K$

Autrement dit c'est une extension <u>algébrique</u> telle que tout polynôme <u>irréductible</u> de $K[X]$ qui admet une racine sur L, est scindé sur L.

Une extension de corps $L: K$ est normale et finie ssi cette extension est le corps de décomposition d'un polynôme non nul de $K[X]$.

Les corps de décomposition sont les extensions normales finies.

Les corps de rupture sont les extensions algébriques simples.

III. Utilisation de la théorie des groupes

III.1. Automorphismes de corps – Groupe de Galois

Le **groupe de Galois d'une extension de corps $L:K$,** $Gal(L:K)$ est l'ensemble des K-automorphismes d'extension de $L:K$. Le groupe de Galois d'une extension de corps est un groupe.

Le **groupe de Galois d'un polynôme non nul $P \in K[X]$** est le groupe de Galois du corps de décomposition du polynôme sur K (donc vu comme une extension de K).

Th. Soit un polynôme non nul sur un corps $P \in K[X]$, de corps de décomposition $L = K(\alpha_1, \dots, \alpha_n)$, avec $\alpha = \{\alpha_1, \dots, \alpha_n\} \subset L$ l'ensemble des racines de P sur L, alors tout K-automorphisme de L induit une bijection de α sur α, et est meme déterminé par cette permutation qu'il induit sur α. Autrement dit, l'application $Gal(L:K) \to G_n$ qui a un K-automorphisme de L, associe la permutation des indices induite sur α, est un morphisme injectif de groupes. On retrouve le théorème de Cayley applique à ce groupe.

On a $n \leq \deg P$, si P est séparable, $n = \deg P$, si P inseparable, $n < \deg P$

Si P est un produit d'irréductibles distincts $P = P_1 \dots P_r$, le théorème précèdent peut être précisé. En effet les $\sigma \in Gal(L:K)$ définissent une bijection des racines de chacun des $P_1, \dots, P_r$, il peut être donc préférable de voir $Gal(L:K)$ comme un sous-groupe de $G_{n_1} \times \dots \times G_{n_r}$ avec n_k nb de racines de P_k.

Pour 2 extensions de corps successives $K \to M \to L$ on a $Gal(L:M) \leq Gal(L:K)$.

Pour un sous-groupe H d'un groupe de Galois $Gal(L:K)$, on définit **la sous-extension de $L:K$ invariante par H** : $L^H = \{x \in L \mid \forall \sigma \in H\ \sigma(x) = x\}$

L^H est bien une sous-extension de $L:K$, cad $K \to L^H \to L$. Et $Gal(L:L^H) \leq Gal(L:K)$

Pour une extension $L:K$, toute sous extension $M:K$ (on a $K \to M \to L$) vérifie : $M \subseteq L^{Gal(L:M)}$

Exemples de calculs de groupe de Galois TODO (illisibles).

Une **extension de Galois** est une extension (algébrique) normale et séparable. Autrement dit une extension algébrique dans laquelle le polynôme minimal de tout élément $\alpha \in L$ est scindé (vérifier).

Le corps de décomposition du polynôme $X^3 + pX + q$ sur un corps K de caracteristique $\neq 2{,}3$ est une extension $L:K$ normale, finie, et séparable, càd une extension galoisienne finie.

De plus soit $-4p^3 - 27q^2$ est un carré dans K, et dans ce cas $[L:K] = 3,\ Gal(L:K) \approx A_3$,

soit $-4p^3 - 27q^2$ n'est pas un carré dans K, et dans ce cas $[L:K] = 6,\ Gal(L:K) \approx G_3$

Th. de Galois, 1831. Une extension algébrique finie $L:K$ est galoisienne ssi son degré est égal à l'ordre de son groupe de Galois $[L:K] = |Gal(L:K)|$. Dans ce cas pour $L:K$ galoisienne finie, la sous-extension invariante par le groupe de Galois n'est autre que le corps K. Autrement dit $L^{Gal(L:K)} = K$

Théorème de Galois. Soit une extension finie de Galois $L:K$ et G son groupe de Galois. Alors les applications $M \mapsto H = Gal(L:M)$ et $H \mapsto M = L^H$ établissent une bijection décroissante entre les extensions intermédiaires M et les sous-groupes H de G.

De plus, avec ces notations, une extension intermédiaire M est de Galois ssi G/H existe et dans ce cas $Gal(M:K) \approx G/H$.

Exemple : Le groupe de Galois du polynôme $G = X^5 - 6X + 3$ sur Q est le groupe symétrique G_5. Son corps de décomposition sur Q est de degré $|G_5| = 5! = 120$.

Soit $P \in Q[X]$ irréductible de degré p premier impair (≥ 3), ayant 2 racines complexes non réelles et $p - 2$ racines réelles. Alors le groupe de Galois de P sur Q correspond au groupe symétrique G_p, et le corps de décomposition de P est de degré $p!$ dans Q.

III.2. Résolution par radicaux

Soient *K* un corps et *L* une extension de *K*.
Un élément de *L* est dit **radical** sur *K* si l'une de ses puissances appartient à *K*.
On dit qu'un élément de *L* s**'exprime par radicaux** sur *K* s'il est le dernier terme d'une suite finie de premier terme nul et dont chaque terme est radical sur l'extension de *K* engendrée par les termes précédents. Justification vague : créer des extensions sert à imbriquer des radicaux en créant des racines de polynômes.
On dit que l'extension *L* de *K* est **résoluble par radicaux** si chaque élément de *L* s'exprime par radicaux sur *K*. Lorsque l'extension est finie, cela revient à dire que *L* est contenu dans une extension $K(\alpha_1, \dots, \alpha_k)$ telle que $\forall i \in \{1, \dots, k\}\ \exists n_i \in N$ tel que $\alpha_i^{n_i}$ appartient à $K(\alpha_1, \dots, \alpha_{i-1})$
On dit qu'un polynôme est résoluble ou résoluble par radicaux si toutes ses racines s'expriment par radicaux sur *K*. Autrement dit : l'extension de *K* engendrée par les racines du polynôme est résoluble par radicaux.
Si par exemple on a un polynôme de degré 3, on notera G son groupe de Galois, L son corps de décomposition, on cherche $\{1\} = G_1 \lhd G_2 \lhd G_3 = G$ avec $\frac{G_3}{G_2}, \frac{G_2}{G_1}$ abéliens, ce qui donne une suite d'extensions intermédiaires $K \to L^{G_3} \to L^{G_2} \to L^{G_1} = L$ ce qui facilite l'étude de $K \to L$.

III.2.1. Le cas du degré 3

Th. Cardan. TODO

III.2.2. Le cas du degré 4

Th. Ferrari. TODO

III.2.3. Le cas du degré ≥ 5

Un groupe fini résoluble est un groupe fini tel qu'il existe une suite finie $G_1, \dots, G_n$ de sous-groupes de G verifiant $\{1\} = G_1 \lhd G_2 \lhd \dots \lhd G_{n-1} \lhd G_n = G$ et les groupes $\frac{G_2}{G_1}, \frac{G_3}{G_2}, \dots, \frac{G_n}{G_{n-1}}$ sont abéliens.
Soit $P \in K[X]$ un polynôme de degré n, on note L son corps de décomposition, K corps de caracteristique nulle contenant les k-iemes racines de l'unité pour tout $k \in \{3, \dots, n\}$. Alors $P(X) = 0$ est une **équation résoluble par radicaux** ssi il existe une suite finie d'extensions intermédiaires $K = K_0 \to K_1 \to \cdots \to K_m = L$ telles que $\forall p \in \{0, \dots, m-1\}$ l'extension $K_p \to K_{p+1}$ est normale et K_{p+1} est isomorphe a $\frac{K_p[T]}{\langle T^{d_p} - a_p \rangle}$ pour un certain degre $d_p \leq n$ et un certain $a_p \in K_p$.
Le groupe G_n n'est pas résoluble pour $n \geq 5$.

IV. Clôture algébrique de Q

On note $\overline{Q}$ l'ensemble des nombres complexes algébriques sur Q. $Q \to \overline{Q}$ est une extension de corps de degré infini. Le corps $\overline{Q}$ est une clôture algébrique de Q. $\overline{Q}$ est dénombrable.
L'ensemble des nombres complexes transcendants sur Q est infini non dénombrable. ($C \setminus \overline{Q}$)

Complément. Correspondance de Galois

démonstrations plus détaillées de la théorie de Galois

Chapitre 13. Corps finis

I. Clôture algébrique de F_p

Pour p premier, le corps $\boldsymbol{F_p} = \frac{Z}{pZ}$ admet une clôture algébrique $\overline{F_p}$. Cette clôture algébrique $\overline{F_p}$ est dénombrable. Attention ici on ne définit F_p que pour p premier, la définition de F_{p^n} sera différente.

On note $\{P_1, \dots, P_n, \dots\}$ les polynômes irréductibles de F_p (il en existe une infinité dénombrable).
Si on note K_n le corps de décomposition de $P_1 P_2 \dots P_n$ sur F_p, on a $\overline{F_p} = \bigcup_{n=1}^{\infty} K_n$
Une clôture algébrique d'un corps fini d'ordre premier *p* est un corps dénombrable. Pour tout entier naturel *n* non nul, il contient un et un seul sous-corps F_{p^n} d'ordre p^n, et il est égal à la réunion de tous ces sous-corps (ou plus savamment : leur limite inductive, avec $\mathrm{F}_{p^d} \subseteq \mathrm{F}_{p^n}$ avec *d* un diviseur de *n*).

II. Existence et unicité du corps à p^n elements

II.1. Unicité à isomorphisme près du corps à p^n éléments

Un corps fini K de caractéristique, un premier p, de degré $n = [K: F_p]$, possède p^n éléments et K est le corps de décomposition du polynôme $X^{p^n} - X$ sur F_p, tout corps a p^n éléments est isomorphe à K et l'extension $F_p \to K$ est galoisienne finie, de degré n.

II.2. Existence du corps a p^n éléments

Soit p premier, et $n \in N^*$. L'ensemble $\boldsymbol{F_{p^n}} = \{\alpha \in \overline{F_p} \mid \alpha^{p^n} - \alpha = 0\}$ des racines de $X^{p^n} - X$ est un corps a p^n éléments isomorphe au corps de décomposition de $X^{p^n} - X$ sur F_p. C'est un sous-corps de $\overline{F_p}$
En résumé, il existe toujours un corps à p^n éléments unique à isomorphisme près, c'est F_{p^n}.

II.3. Groupe multiplicatif du corps a p^n éléments

Rappel : L'exposant d'un groupe fini est le ppcm des ordres de ses éléments.
Rappel : Tout groupe abélien fini est isomorphe a un $\frac{Z}{n_1 Z} \times \dots \times \frac{Z}{n_k Z}$ et donc $e(G) = ppcm(n_1, \dots, n_k)$
Sur un corps, pour $d \geq 1$, l'équation $X^d = 1$ admet au plus d solutions.
Un groupe fini qui vérifie pour tout d (divisant $\#G$) $X^d = 1$ admet au plus d solutions, est cyclique.
Le groupe multiplicatif des inversibles $F_{p^n}^{\times}$ du corps fini F_{p^n} est cyclique.
Tout groupe abélien fini admet un élément d'ordre l'exposant du groupe.
Bien qu'identiques pour $n = 1$, le corps F_{p^n} et l'anneau $\frac{Z}{p^n Z}$ ne sont jamais isomorphes pour $n \geq 2$.

III. Sous-corps de F_{p^n}

III.1. Sous-corps et extensions

On a $F_{p^d} \subseteq F_{p^n}$ ssi d divise n et dans ce cas l'extension $F_{p^n}: F_{p^d}$ est galoisienne finie.

III.2. Automorphismes des corps finis

On appelle **automorphisme de Frobenius sur F_{p^n}** l'application $\phi: F_{p^n} \to F_{p^n}: x \mapsto x^p$.
L'automorphisme de Frobenius sur F_{p^n} est un automorphisme d'extension sur $F_{p^n}: F_p$
Le groupe de Galois $Gal(F_{p^n}: F_p)$ de l'extension $F_{p^n}: F_p$ est cyclique d'ordre n et engendré par l'automorphisme de Frobenius sur F_{p^n}.
La sous-extension de $F_{p^n}: F_p$ invariante par son groupe de Galois est le corps F_p.
$(F_{p^n}: F_p)^{Gal(F_{p^n}: F_p)} = F_p$
F_p est aussi l'ensemble des éléments de F_{p^n} laisses fixes par ϕ ou par le groupe engendre par ϕ, puisque les elements de F_p sont les $x \in F_{p^n}$ tels que $x^p = x$. Le théorème de Galois prouve que les seuls automorphismes sont les puissances de l'automorphisme de Frobenius sur F_{p^n}.
Soit d un diviseur de n positif.
$Gal(F_{p^n}: F_{p^d})$ est cyclique d'ordre n/d engendre par ϕ^d, c'est un sous-groupe de $Gal(F_{p^n}: F_p)$.

$\frac{Gal\left(F_{p^n}:F_p\right)}{Gal\left(F_{p^n}:F_{p^d}\right)} \approx Gal\left(F_{p^d}:F_p\right)$

Sur le diagramme suivant, ↓ represente un isomorphisme, les → à gauche représentent un morphisme injectif, les → à droite représentent un morphisme surjectif.

$$\begin{array}{ccccc} Gal\left(F_{p^n}:F_{p^d}\right) & \rightarrow & Gal\left(F_{p^n}:F_p\right) & \rightarrow & Gal\left(F_{p^d}:F_p\right) \\ \downarrow & & \downarrow & & \downarrow \\ \{Id, \phi^d, \phi^{2d}, \dots, \phi^{n-d}\} & \rightarrow & \{Id, \phi, \phi^2, \dots, \phi^{n-1}\} & \rightarrow & \{Id, \phi, \phi^2, \dots, \phi^{d-1}\} \\ \downarrow & & \downarrow & & \downarrow \\ dZ/nZ & \rightarrow & Z/nZ & \rightarrow & Z/dZ \end{array}$$

III.3. Nouvelle construction de la clôture algébrique de F_p

Pour tout $n, m \in N^*$ F_{p^n} admet une unique extension de degré m : $F_{p^{nm}}$. Ce fait permet de simplifier la construction de $\overline{F_p}$.

$\overline{F_p} = \cup_{n=1}^{\infty} F_{p^{n!}}$

IV.1. Existence d'un polynôme irréductible de degré n dans $F_p[X]$

Tout F_{p^n} contient au moins un α qui n'appartient à aucun F_{p^d} avec d diviseur strict de n. Autrement dit $\cup_{d|n,d<n} F_{p^d}$ la réunion des sous-corps de F_{p^n} est strictement incluse dans F_{p^n}.

Pour un tel $\alpha \in F_{p^n} \setminus \cup_{d|n,d<n} F_{p^d}$, alors $\boldsymbol{R_\alpha(X)} = \prod_{j=0}^{n-1}\left(X - \phi^j(\alpha)\right)$ est un polynôme de $F_p[X]$, irréductible, séparable, et de degré n. De plus le corps de rupture de R_α sur F_p est aussi le corps de décomposition de ce polynôme. Le morphisme de F_p-algèbres $F_{p^n} = F_p(\alpha) \rightarrow \frac{F_p[X]}{\langle R_\alpha(X)\rangle} : \alpha \mapsto \overline{X}$ est un isomorphisme.

IV.2. Corps finis via la caractéristique nulle.

On a vu que pour tout premier p et entier $n \in N^*$ $F_p[X]$ a au moins un polynôme irréductible de degré n, soit $\overline{R_n}(X) = X^n + \overline{a_{n-1}}X^{n-1} + \cdots + \overline{a_0}$, et soit $R_n(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ le polynôme correspondant dans $Z[X]$. $R_n(X)$ est irréductible dans $Z[X]$

Alors $Z[X]/\langle p, R_n(X)\rangle$ est un corps fini a p^n éléments donc isomorphe a F_{p^n}

De plus $\langle p, R_n(X)\rangle$ est un idéal maximal de $Z[X]$.

Attention un idéal de la forme $\langle p, R\rangle$ avec p premier et $R \in Z[X]$ irréductible n'est pas forcément un idéal maximal : contre-exemple fournit par $R = X^4 + 1$

IV.3. Dénombrement des polynômes irréductibles

Pour tout $n \in N^*$ le polynôme $X^{p^n} - X$ est exactement le produit de tous les polynômes unitaires irréductibles de $F_p[X]$ dont le degré divise n.

En notant $\boldsymbol{m_p(d)}$ le **nombre de polynômes unitaires irréductibles de degré d dans $F_p[X]$** on a $p^n = \sum_{d|n} d \cdot m_p(d)$

Ces égalités pour $n = 1,2, \dots, N$ permettent de calculer successivement les nombres $m_p(d)$

Par exemple on calcule $m_p(6)$ avec les égalités $p = m_p(1), p^2 = m_p(1) + 2m_p(2), p^3 = m_p(1) + 3m_p(3), p^6 = m_p(1) + 2m_p(2) + 3m_p(3) + 6m_p(6)$

IV.4. Exemples de corps finis

Pour effectuer des calculs dans F_{p^n} il faut pouvoir nommer ses éléments, puis les additionner et les multiplier. La construction du corps de rupture d'un polynôme indique la démarche à suivre : trouver un

polynôme R unitaire irreductible de degre n dans $F_p[X]$, utiliser l'isomorphisme $F_{p^n} \approx \frac{F_p[X]}{\langle R(X)\rangle}$ et effectuer les calculs dans $\frac{F_p[X]}{\langle R(X)\rangle}$. Cependant en général, pas de méthode canonique pour trouver R parmi les $m_p(n)$ possibles. De plus $m_p(n) \sim_{n\to\infty} \frac{p^n}{n}$. Parmi les polynômes unitaires environ $\frac{1}{n}$ est irréductible.
Exemple de $F_{256} = F_{2^8}$ TODO

V. Polygones réguliers constructibles à la règle et au compas

Gauss, 1796*. Le polygone régulier à 17 côtés est constructible à la règle et au compas.

Gauss, 1796*. Le polygone régulier à n côtés est constructible à la règle et au compas ssi $n = 2^r p_1 \dots p_s$ ou $r \in N, s \in N$ et $p_1, \dots, p_s$ sont des nombres premiers distincts de la forme $p_i = 1 + 2^{2^{r_i}}$ c'est-à-dire des nombres de Fermat.

Lemmes :

Le polynôme minimal sur Q d'une racine primitive p-ieme de l'unité $e^{\frac{2i\pi}{p}}$ avec p premier est le p-ieme polynome cyclotomique $\phi_p = \frac{X^p-1}{X-1}$ (preuve par critère Eisenstein)

Le polynôme minimal sur Q d'une racine primitive p^2-ieme de l'unité $e^{\frac{2i\pi}{p^2}}$ avec p premier est le p^2-ieme polynome cyclotomique $\phi_{p^2} = \frac{X^{p^2}-1}{X^p-1} = 1 + X^p + X^{2p} + \cdots + X^{p(p-1)}$

Le polygone régulier à p^2 côtés avec p premier impair, n'est pas constructible à la règle et au compas.

VI. Théorème de Wedderburn

Tout corps au sens large (commutatif ou non) fini est automatiquement commutatif.

Tout anneau intègre fini est un corps.

Complément : Quaternions

1. Construction des quaternions

L'ensemble des quaternions $\boldsymbol{H} = \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} : \alpha, \beta \in C \right\}$ est un Rev de dimension 4 et un corps non commutatif appelé algèbre des quaternions.

Le groupe spécial unitaire $SU_2(C)$ est un sous-groupe multiplicatif de H et $\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \in SU_2(C)$ ssi $\alpha\overline{\alpha} + \beta\overline{\beta} = 1$

On pose $1_H = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i_H = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, j_H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, k_H = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ qui forme une base de H

$i_H^2 = j_H^2 = k_H^2 = -1_H, i_H j_H = -j_H i_H = k_H, j_H k_H = -k_H j_H = i_H, k_H i_H = -i_H k_H = j_H$

Tout quaternion non nul est inversible d'inverse $\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}^{-1} = \frac{1}{D}\begin{pmatrix} \overline{\alpha} & -\beta \\ \overline{\beta} & \alpha \end{pmatrix}$ avec $D = \alpha\overline{\alpha} + \beta\overline{\beta} \neq 0$

On peut définir l'isomorphisme d'ev $H \to R \times R^3 : x1_H + yi_H + zj_H + tk_H \mapsto \big(x, (y,z,t)\big) = (x, \vec{v})$

L'image de la base $(1_H, i_H, j_H, k_H)$ est donc une b.o.n qu'on supposera directe.

Via cet isomorphisme, les opérations de H s'écrivent : $(a, \vec{v}) + (b, \vec{w}) = (a+b, \vec{v} + \vec{w})$ et $(a, \vec{v}) \wedge (b, \vec{w}) = (ab - \vec{v}\cdot\vec{w}, a\vec{w} + b\vec{v} + \vec{v} \wedge \vec{w})$

L'algèbre des quaternions possède une infinité de racines de -1.

Le **conjugue d'un quaternion $\boldsymbol{q} = (\boldsymbol{a}, \boldsymbol{\vec{v}})$** est $\boldsymbol{\overline{q}} = \overline{(a, \vec{v})} = (a, -\vec{v})$.

On a $\overline{q_1 q_2} = \overline{q_1}\,\overline{q_2}$

La **norme d'un quaternion q** est $\|q\| = \sqrt{q\overline{q}}$ elle est bien définie car $q\overline{q} \in R_+$. Elle coincide avec la norme euclidienne sur R^4.

On a $\|q\|^2 = \det(q) = \alpha\overline{\alpha} + \beta\overline{\beta} = |\alpha|^2 + |\beta|^2$

L'inverse d'un quaternion non nul est $q^{-1} = \frac{\overline{q}}{\|q\|^2}$

On a $\|q_1 q_2\| = \|q_1\|\|q_2\|$ et $(q_1 q_2)^{-1} = q_2^{-1} q_1^{-1}$

$SU_2(C) = \{q \in H \mid \|q\| = 1\}$

2. Paramétrage de $SO_3(R)$ et de $SO_4(R)$ via les quaternions

L'isomorphisme $H \to R \times R^3$ fournit une bijection entre $SU_2(C)$ et la sphère unité S^3 de R^4

En munissant $SU_2(C)$ et S^3 de leur structure naturelle d'espace topologique (fermés de R^4), cette bijection est un homéomorphisme. Par transport de structure, S^3 est un groupe. S^3 est simplement connexe, il en est donc de même pour $SU_2(C)$. Autrement dit tout chemin C^1 fermé sur $SU_2(C)$ est homotope a un point.

Un **quaternion réel** est un quaternion de la forme $x1_H$ avec $x \in R$

Un **quaternion pur** est un quaternion de la forme $yi_H + zj_H + tk_H$ avec $(y, z, t) \in R^3$

Identifions R^3 avec l'espace vectoriel $\{0\} \times R^3$ de H des quaternions purs.

Soit s un quaternion de norme 1

On peut écrire $s = \cos\theta\ 1_H + \sin\theta\ \ v$ avec v quaternion pur de norme 1 associe a un vecteur unitaire $\vec{v}$

L'application $R_s : R^3 \to R^3 : q \mapsto sqs^{-1} = sq\overline{s}$ est la rotation d'angle 2θ autour de $\vec{v}$. L'application $SU_2(C) \to SO_3(R) : s \mapsto R_s$ est un morphisme de groupes continu et surjectif de noyau $\{1_H, -1_H\}$, autrement dit on a la suite exacte $\{1\} \to \{1_H, -1_H\} \to SU_2(C) \to SO_3(R) \to \{1\}$

Pour $i = 1$ ou 2, soit r_i la rotation d'angle θ_i autour du vecteur unitaire $\overrightarrow{v_i}$. Alors la rotation composée $r_1 \circ r_2$ est la rotation R_s définie par le quaternion $s = (\cos\theta_1\ 1_H + \sin\theta_1\ v_1)(\cos\theta_2\ 1_H + \sin\theta_2\ v_2)$

$s = (\cos\theta_1 \cos\theta_2 - \sin\theta_1 \sin\theta_2\ \overrightarrow{v_1} \cdot \overrightarrow{v_2})1_H + \cos\theta_2 \sin\theta_1\ \overrightarrow{v_1} + \cos\theta_1 \sin\theta_2\ \overrightarrow{v_2} + \sin\theta_1 \sin\theta_2\ \overrightarrow{v_1} \wedge \overrightarrow{v_2}$

TODO