كلية العلوم و التقنيات فاس
ⵜⴰⵖⵙⵓⵍⵜ ⵏ ⵜⵇⴰⵏⵉⵜ ⴷ ⵜⵙⵙⵙⵜⵙ
Faculté des Sciences et Techniques de Fès

جامعة سيدي محمد بن عبد الله
ⵜⴰⵙⵎⵓⵔⵜ ⵙⴰⵏ ⵇⵓⵔⵔⴰⵔⵓ ⵙⵉ ⵎⵓⵃⴰⵎⵎⴰⴷ
Université Sidi Mohamed Ben Abdellah

Licence Sciences et Techniques (LST)

MATHEMATIQUES ET APPLICATIONS

MEMOIRE DE FIN D'ETUDES

Pour l'obtention du Diplôme de Licence Sciences et Techniques

Extension de corps

Présenté par :

- **Karim El-khanchouli**

Encadré par :

- **Pr. Najib Mahdou**

Soutenu Le 9 Juin 2018 devant le jury composé de:

- **Pr. Abdelmajid Hilali**
- **Pr. Najib Mahdou**
- **Pr. Aziza Rahmouni Hassani**

Année Universitaire 2017 / 2018

Dédicace

Je dédie ce travail :

- ✓ A mes très chers parents à qui nous adressons à Dieu les vœux les plus ardents pour la conservation de leur santé et de leur vie.
- ✓ A mes chers frères et sœurs pour leur soutien et encouragement durant mes études.
- ✓ A mes chers amis, avec eux j'ai partagé des moments inoubliables de souffrance et de joie.
- ✓ A tous mes professeurs pour leur soutien au cours de toutes mes années d'études.
- ✓ A tous mes collègues dans toutes ces années d'études.

REMERCIEMENTS

***A**u terme de ce travail, je voudrais exprimer mes remerciements et ma profonde reconnaissance à tous ceux qui ont contribué de prêt ou de loin à sa réalisation :*

***J**e voudrais remercier tout particulièrement le Professeur Najib Mahdou qui a accepté en toute modestie de m'accompagner tout au long de ce projet, qui a lu mon rapport et m'a aidé à réaliser la version finale. Il m'a apporté énormément de connaissances en algèbre, il a été toujours à l'écoute de mes questions, et s'est toujours intéressé à l'avancée de mon travail. Cela qui m'a permis d'enrichir mes connaissances dans ce domaine, et de m'approcher du monde des mathématiques et de la recherche scientifique.*

***J**e tiens également à exprimer toute ma gratitude et tout mon sentiment de reconnaissance aux professeurs Abdelmajid Hilali et Aziza Rahmouni Hassani pour l'honneur qu'ils me font d'accepter d'être membres de jury de ce mémoire.*

***J**'adresse mes sincères remerciements et ma grande reconnaissance à tous mes professeurs de la Licence Mathématique et Applications. Je tiens à remercier également la doctorante Rachida El Khalfaoui et mes meilleures amies Zakia et Hanae qu'ont m'aidé à faire ce projet.*

***J**'exprime ma gratitude à tous mes collègues de licence pour leur soutien amical durant cette année.*

Table des matières

Introduction

L'idée principale derrière l'apparition de la théorie des extensions de corps est la résolution des équations polynomiales.

Autrement dit, on cherche les racines d'un polynôme à coefficients dans K (où K est un corps), si on ne réussit pas à trouver ces racines dans K, on les cherche dans un autre corps plus "grand" qui s'appelle une extension de K.

Par exemple, supposons que dans la théorie des ensembles on ne connait que le corps des rationnelles $\mathbb{Q}$ et on veut résoudre toutes les équations polynomiales à coefficients dans $\mathbb{Q}$. On vous demande de trouver les racines du polynôme :

$$P(x) = x^2 - 2$$

qui est effectivement un polynôme à coefficients dans $\mathbb{Q}$.

Du fait que vous ne connaissez que l'ensemble $\mathbb{Q}$ vous seriez bloquer, car ce polynôme n'admet pas de solution dans $\mathbb{Q}$ même si ses coefficients sont dans $\mathbb{Q}$, et comme ça on affirme que l'ensemble des rationnelles est insuffisant pour résoudre toutes les équations polynomiales à coefficients dans $\mathbb{Q}$.
Donc, que peut-on faire pour résoudre $x^2 - 2 = 0$?

Le présent travail a pour but de présenter des constructions d'extension de corps, concernant l'extension algébrique, transcendante, normale, séparable et galoisienne.
Ainsi, ce mémoire est divisé en cinq chapitres :

Le premier chapitre :
Dans ce chapitre, on rappelle certaines définitions et propriétés concernant les anneaux et corps et nous introduisons également la définition de l'action de groupe sur un ensemble.

Le deuxième chapitre :
Le second chapitre est intéressé à la définition d'extension, des propriétés et des exemples sur l'extension, de plus il rappelle des définitions de l'extension algébrique et transcendante.

Le troisième chapitre :
Le troisième chapitre sera consacré à des définitions, des propriétés, des théorèmes et des exemples de corps de rupture, corps de décomposition et clôture algébrique.

Le quatrième chapitre :
Le quatrième chapitre est intéressé sur les extensions normales et séparables.

Le cinquième chapitre :

Dans ce chapitre, on donne des définitions et quelque propriétés sur le groupe de Galois pour les extensions et les extensions galoisiennes, et à la fin on rappelle le théorème fondamental de Galois pour les extensions galoisiennes finie.

1

Généralités sur les anneaux et les corps

1.1 Anneaux

Définition 1.1.1.
On appelle ***anneau*** *un ensemble A muni de deux lois de composition internes, une addition et une multiplication telles que :*
i) $(A, +)$ *est un groupe commutatif ;*
ii) La multiplication est associative ;
iii) La multiplication est distributive par rapport à l'addition.

• *Si en outre, la multiplication est commutative, on dit que A est un* ***anneau commutatif****.*
• *Si A possède un élément neutre pour la multiplication, on note 1_A cet élément unité et on dit que A est un* ***anneau unitaire****.*
• *Un anneau A est dit un* ***anneau intègre*** *si :*

$$\forall x, y \in A,\ on\ a\ :\ xy = 0 \Rightarrow x = 0\ ou\ y = 0$$

• *Soit A un anneau unitaire, l'ensemble :*

$$U(A) = \{x \in A\ :\ xy = 1\ et\ yx = 1\ avec\ y \in A\}$$

s'appelle l'ensemble des éléments inversibles.
• *Une partie B d'un anneau A est dite* ***sous-anneau*** *de A si, et seulement si :*
- $B \neq \emptyset$;
- $\forall a, b \in B, a - b \in B$;
- $\forall a, b \in B, ab \in B$.

• *L'intersection d'une famille quelconque de sous-anneau de A est un sous-anneau de A.*

Sauf mention du contraire, tous les anneaux considérés par la suite, sont supposés commutatifs et unitaires.

Exemple 1.1.1.
$(\mathbb{Z}, +, .)$; $(\mathbb{Q}, +, .)$; $(\mathbb{R}, +, .)$; $(\mathbb{C}, +, .)$ *sont des anneaux commutatifs unitaires intègres.*

1.2 Morphisme d'anneaux

Définition 1.2.1.
*Une application f d'un anneau A dans un anneau B est dite un **morphisme** (ou homomorphisme) d'anneaux si elle satisfait les relations suivantes :*

$$f(a+b) = f(a) + f(b) \quad et \quad f(ab) = f(a)f(b) \quad pour\ tout\ a, b \in A.$$

*- Un **endomorphisme** est un morphisme d'un anneau A dans lui même.*
*- Un **isomorphisme** est un morphisme bijective.*
*- Un **automorphisme** est un endomorphisme bijective.*

1.3 Idéal

Définition 1.3.1.
*Un ensemble I d'un anneau $(A, +, .)$ est dit un **idéal** si on a :*
- $(I, +)$ est un groupe ;
- $\forall x \in I, \forall y \in A,$ on a $xy \in I$.

Exemple 1.3.1.
1. Les seuls idéaux de l'anneau $(\mathbb{Z}, +, .)$ sont sous forme $n\mathbb{Z}$, car les seuls sous-groupes de $(\mathbb{Z}, +, .)$ sont sous forme $n\mathbb{Z}$.
2. Soit A un anneau et $a \in A$, on a l'ensemble : $Aa = \{xa \ : \ x \in A\}$ est un idéal de A.

Définition 1.3.2. Idéaux premiers et les idéaux maximaux
Soient A un anneau commutatif unitaire et P un idéal de A :
*- P est dit **premier** si $\forall x, y \in A$, $xy \in P \Rightarrow x \in P$ ou $y \in P$.*
*- P est dit **maximal** si $P \neq A$ et si les seuls idéaux compris entre P et A sont P et A.*

Théorème 1.3.1.
1. Le noyau d'un morphisme d'anneaux est un idéal.
2. Un morphisme d'anneaux est injectif si, et seulement si, son noyau est nul.

Preuve :
1. Soit $f : A \longrightarrow B$ un morphisme d'anneaux.
On a $Ker(f) = \{x \in A \ : \ f(x) = 0_B\}$ est un sous groupe additif de A. En outre , si $a \in Ker(f)$ et $b \in A$, on a $f(ab) = f(a)f(b) = 0_B f(b) = 0_B$, de sorte que $ab \in Ker(f)$.
Ainsi $Ker(f)$ est un idéal de A.
2. Si le morphisme est injectif, le 0_B a un seul antécédent qui est 0_A, c'est à dire que :
$Ker(f) = \{0_A\}$.
Inversement, on a :
$f(x) = f(y) \Rightarrow f(x) - f(y) = 0_B \Rightarrow f(x - y) = 0_B$, car f est un morphisme, c'est à dire que $x - y \in Ker(f) = \{0_A\}$ et par la suite $x = y$. Cela veut dire que f est injectif. □

1.4 Caractéristique d'un anneau

Soit A un anneau. L'application :

$$\begin{array}{rccc} f & : & \mathbb{Z} & \to & A \\ & & n & \mapsto & n1_A \end{array}$$

est un morphisme d'anneaux. Son noyau est un idéal de $\mathbb{Z}$, et donc de la forme $p\mathbb{Z}$ avec $p \in \mathbb{N}$. On obtient, d'après le 1^{er} théorème d'isomorphisme : $\mathbb{Z}/p\mathbb{Z} \cong f(\mathbb{Z})(= Im(f))$ qui est un sous anneau de A.

Définition 1.4.1.
*L'entier naturel **p** ainsi définit s'appelle la **caractéristique de l'anneau** A et se note **Car(A)**.*

Remarque 1.4.1.
- $Car(A) = 0$, alors $Ker(f) = \{0\}$ et donc $\mathbb{Z} \cong Im(f) \subseteq A$. Donc A contient un sous anneau isomorphe à $\mathbb{Z}$ et en particulier A est infini.
- $Car(A) = p \neq 0 \Longleftrightarrow [\forall n \in \mathbb{N}, (n1 = 0) \Rightarrow p|n]$.
- L'anneau A est intègre, sa caractéristique est soit 0 soit un nombre premier.

Exemple 1.4.1.
$Car(\mathbb{Z}/n\mathbb{Z}) = n$, $Car(\mathbb{Q}) = Car(\mathbb{R}) = Car(\mathbb{C}) = 0$.

1.5 Corps

Définition 1.5.1.
*Un **corps** est un anneau unitaire dans lequel tout élément non nul est inversible, c'est à dire que $A - \{0\}$ est un groupe pour la multiplication.*
Si la multiplication d'un corps est commutative, on dit que le corps est commutatif.

- *Soient K un corps et L une partie de K. On dit que L est un **sous-corps** de K si :*
  - $L \neq \emptyset$;
  - $\forall x, y \in L : x - y \in L$;
  - $\forall (x, y) \in (L^*)^2 : xy^{-1} \in L^*$.
- *L'intersection d'une famille quelconque de sous-corps de K est un sous-corps de K.*

Exemple 1.5.1.
$(\mathbb{R}, +, .)$ *est un corps.*
$(\mathbb{Q}, +, .)$ *est un corps, de plus est un sous corps de $\mathbb{R}$.*

Remarque 1.5.1.
- Tout corps est intègre. En effet, si $ab = 0$ avec $a \neq 0$, alors $0 = a^{-1}ab = b$, car a est inversible.
- Tout corps contient 1 et 0 avec $1 \neq 0$.
- Les seuls idéaux d'un corps K sont $\{0\}$ et K.
- Comme un corps est un anneau intègre, donc sa caractéristique est soit 0 soit un nombre premier p.

Théorème 1.5.1.
Soient A un anneau commutatif unitaire et P un idéal de A. Alors on a :
- P est premier si, et seulement si, A/P est intègre.
- M est maximal si, et seulement si, A/M est corps.

Preuve :
1. Supposons que P est premier :
Soit $a, b \in A$ tel que $\bar{a}\bar{b} = \bar{0}$ avec $\bar{a} \neq \bar{0}$, ces relations se traduisent dans A par $ab \in P$ et $a \notin P$. L'hypothèse "P est premier" entraine que $b \in P$, c'est à dire que $\bar{b} = \bar{0}$.
Réciproquement, supposons A/P est intègre :
Soient $a, b \in A$ tel que $ab \in P$. Par passage au quotient on obtient $\overline{ab} = \bar{a}\bar{b} = \bar{0}$ et par la suite $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$ (car A/P est intègre) de sorte que $a \in P$ ou $b \in P$. Ainsi P est premier.
2. Supposons que M est maximal :
Soit $\bar{a} \in (A/M) - \{\bar{0}\}$, où $a \in A$, montrons que $\bar{a}$ est inversible dans A/M. Pour cela considérons l'idéal $aA + M$ qui contient strictement l'idéal M (car $a \notin M$). A cause de la maximalité de M, on a : $aA + M = A$. Ainsi il existe $t \in A$ et $u \in M$ tel que $1 = at + u$. Par passage aux classes modulo M, on obtient $\bar{a}\bar{t} = \bar{1}$ et $\bar{a}$ est inversible dans A/M. Ainsi, l'anneau A/M est un corps.
Réciproquement, supposons A/M est corps :
Soient I un idéal tel que $M \subsetneq I$ et $a \in I - M$. On a $\bar{a} \neq \bar{0}$ car $a \notin M$, d'après l'hypothèse on a $\bar{a}$ est inversible dans A/M, c'est à dire qu'il existe $t \in A$ tel que $\bar{1} = \overline{at}$, ce qui implique $\overline{1 - at} = \bar{0}$ de sorte que $1 - at \in M \subsetneq I$. Donc $1 = (1 - at) + at \in I$ puisque $at \in I$ $(a \in I)$ et par la suite $I = A$. Ainsi, M est un idéal maximal. □

Définition 1.5.2. CORPS DES FRACTIONS
*On appelle le **corps des fractions** d'un anneau intègre A est le plus petit corps commutatif contenant A.*
Les éléments de ce corps se notent $\frac{a}{b}$, avec $(a, b) \in A \times A^*$. On identifie les fractions $\frac{a}{b}$ et $\frac{a'}{b'}$ lorsque la relation $ab' = a'b$ est vérifiée.

Exemple 1.5.2.
1. Le corps des fractions de l'anneau $\mathbb{Z}$ est le corps $\mathbb{Q}$.
2. Pour les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, le corps des fractions est l'anneau lui même car $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.
3. Soit $\mathbb{K}$ un corps. le corps des fractions du anneau $\mathbb{K}[X]$ (l'anneau des Polynômes en une indéterminée à coefficient dans un corps $\mathbb{K}$) est $\mathbb{K}(X)$ (le corps des fractions rationnelles à coefficient dans $\mathbb{K}$).

1.6 Anneaux principaux

Définition 1.6.1.
*Un anneau A est dit **principal** si tout idéal de A est principal, c'est à dire que pour tout idéal I de A on a $I =< a >$ pour un certain $a \in I$.*

Exemple 1.6.1. [1]
1. Les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ sont principaux.
2. L'anneau $\mathbb{K}[X, Y]$ n'est pas principal.

1. Voir la démonstration de l'exemple dans l'ouvrage :
Mahdou Najib, Cours et exercices corrigés : structure algébriques 2017/2018, page 135

1.7 Divisibilité - Éléments irréductibles

Définition 1.7.1.
Soit A un anneau.
*Soient a et b deux éléments de A. On dit que a **divise** b, et on note $a|b$, s'il existe $c \in A$ tel que $b = ac$, Autrement dit :*

$$< b > \subseteq < a >$$

Définition 1.7.2.
Soit A un anneau intègre.
*Soient a et b deux éléments de A. On dit que a et b sont **associés** si $a|b$ et $b|a$, autrement dit :*

$$\exists u \in U(A) \ \ tel\ que\ :\ a = bu$$

Définition 1.7.3.
*Soient A un anneau et $p \in A$. On dit que p est **irréductible** si :*
- $p \notin U(A)$
- Si $p = ab$, avec $a, b \in A$, alors $a \in U(A)$ ou $b \in U(A)$.
Autrement dit les seuls diviseurs de p sont : les éléments inversibles, p et les associés de p.

*On dit que les éléments a et b de A sont **premiers entre eux** si leurs seuls diviseurs communs sont les éléments de $U(A)$.*
*a et b sont premiers entre eux si, et seulement si, il existe deux entiers $x, y \in A$ tels que $xa + yb = 1$ (**théorème de Bézout**).*

Proposition 1.7.1.
Soient A un anneau intègre, principal et a un élément non nul de A. Les propriétés suivantes sont équivalentes :
(i) l'idéal $< a >$ est premier ;
(ii) a est irréductible ;
(iii) l'idéal $< a >$ est maximal.

Preuve :
$(iii) \Rightarrow (i)$ On utilisant le théorème 1.5.1 :
$< a >$ est maximal alors $A/ < a >$ est un corps, donc il est intègre ce qui implique que $< a >$ est premier.
$(i) \Rightarrow (ii)$ Supposons que $< a >$ est premier :
Soient $b, c \in A$ tels que $a = bc$, alors on a : $bc \in < a >$ de sorte que $b \in < a >$ ou $c \in < a >$.
Si $b \in < a > \Rightarrow \exists d \in A$ tel que : $b = ad$ donc $a = adc$, c'est à dire que $a(1 - dc) = 0$, et comme a est non nul donc $dc = 1$. D'où c est inversible.
De même manière, on montre :

$$c \in < a > \Rightarrow b \text{ est inversible.}$$

Ainsi a est irréductible.
$(ii) \Rightarrow (iii)$ Par la absurde :
Supposons que $< a >$ n'est pas maximal, alors :

$$\exists p \in A \ tq \ \ < a > \subsetneq < p > \subsetneq A$$

donc $p|a$, ceci implique que p est soit inversible, soit associé à a (car a est irréductible) d'une part, et d'une autre :
Si p est associé à a, alors : $< p >=< a >$.
Si p est inversible, alors $:< p >= A$.
Dans les deux cas on trouve une contradictoire tel que $< p >$ n'est pas un idéal de A contenant $< a >$ autre que A ou $< a >$. Cela prouve la maximalité de $< a >$. □

1.8 Corps premier

Définition 1.8.1.
*On appelle **corps premier** d'un corps K le plus petit sous-corps de K.*
En d'autre termes, le corps premier est l'intersection de tous les sous-corps de K.

Remarque 1.8.1.
Si K est un corps, alors le corps premier de K est le sous-corps de K engendré par 1.

Proposition 1.8.1.
Le corps $\mathbb{Q}$ et les corps de type $\mathbb{Z}/p\mathbb{Z}$, où p est un nombre premier, n'ont pas un sous-corps propre.

Preuve :
- Soit L un sous-corps de $\mathbb{Q}$, alors il contient 0 et 1, ce qui implique que $\mathbb{Z} \subseteq L$. Or le plus petit corps contenant $\mathbb{Z}$ est son corps des fractions, c'est à dire $\mathbb{Q}$. Il résulte que $L = \mathbb{Q}$.
- Supposons que $\mathbb{Z}/p\mathbb{Z}$, p est un nombre premier, possède un sous-corps propre, donc il serait de la forme $m\mathbb{Z}/p\mathbb{Z}$, avec $p\mathbb{Z} \subsetneq m\mathbb{Z} \subsetneq \mathbb{Z}$, donc $m|p$ avec $m \neq p$ et $m \neq 1$, impossible car p est premier. Donc $\mathbb{Z}/p\mathbb{Z}$ n'a pas un sous-corps propre. □

Théorème 1.8.1.
Soit K un corps :
- Si $Car(K) = 0$, alors le sous corps premier de K est isomorphe à $\mathbb{Q}$.
- Si $Car(K) = p \neq 0$, alors le sous corps premier de K est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Preuve :
Soit ϕ le morphisme de $\mathbb{Z}$ dans K (morphisme de caractéristique) et Δ le sous-corps premier de K.
Δ contient 0 et 1 de K, et comme $Im(\phi) = \{n1 \ : \ n \in \mathbb{Z}\}$, donc $Im(\phi) \subseteq \Delta$.
- Si $Car(K) = 0$: alors $Im(\phi) \cong \mathbb{Z}$. On en déduit que Δ contient un sous-corps isomorphe au $\mathbb{Q}$ (corps des fractions de $\mathbb{Z}$), mais Δ est le plus petit sous-corps de K. Alors $\Delta \cong \mathbb{Q}$.
- Si $Car(K) = p \neq 0$: alors $Im(\phi) \cong \mathbb{Z}/p\mathbb{Z}$. Donc $Im(\phi)$ est un sous-corps (car p est premier) de Δ. D'où $\Delta = Im(\phi) \cong \mathbb{Z}/p\mathbb{Z}$. □

1.9 Action d'un groupe sur un ensemble

Définition 1.9.1.
Étant donné un ensemble E et un groupe G, dont la loi est notée multiplicativement et dont l'élément neutre est noté e, une action (ou opération) de G sur E est une application :

$$G \times E \to E$$
$$(g, x) \mapsto x \cdot g$$

vérifiant les propriétés suivantes :
- $\forall x \in E,\ x \cdot e = x$
- $\forall (g, g') \in G^2,\ \forall x \in E,\ \underbrace{(x \cdot g)}_{\in E} \cdot g' = x \cdot \underbrace{(gg')}_{\in G}$

Définition 1.9.2.
Une action de groupe G sur un ensemble E est dite ***transitive*** *si :*

$$\forall x, y \in E, \exists g \in G \ \ tel\ que\ \ y = x \cdot g$$

Définition 1.9.3.
Une action de groupe G sur un ensemble E est dite ***libre*** *si :*

$$\forall x \in E, \forall g \in G \ \ si\ \ x \cdot g = x\ alors\ g = e$$

Remarque 1.9.1.
Une action transitive d'un groupe fini G sur un ensemble E est libre si, et seulement si, G et E ont même cardinal.

2

Extensions algébriques - Extensions transcendantes

2.1 Notion d'extension de corps

Définition 2.1.1.
Étant donné un corps K, on appelle ***extension*** *de K tout corps E tel que $K \subseteq E$ (ou bien E contenant un sous corps isomorphe à K).*
On identifiera souvent cette extension par : $K \hookrightarrow E$.

Notation 2.1.1.
Soit A une partie de E, l'intersection de tous les sous-anneaux de E contenant K et A est donc un sous-anneau de E que l'on notera $K[A]$, appelé sous-anneau de E engendré par $K \cup A$.
De même, l'intersection d'une famille quelconque de sous-corps de E est encore un sous-corps de E. Il existe donc un plus petit sous-corps de E contenant K et A, que l'on appelle le sous-corps de E engendré par $K \cup A$, noté $K(A)$; c'est le corps des fractions de $K[A]$.

Exemple 2.1.1.
1. $\mathbb{C}$ est une extension de $\mathbb{Q}$ et $\mathbb{R}$.
2. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Q}\}$ est un corps tel que il contient $\mathbb{Q}$, alors il est un extension de $\mathbb{Q}$.
3. Tout corps K est un sous-corps du corps $K(X)$ des fractions rationnelles à coefficient dans K, alors $K(X)$ est une extension de K.

Théorème 2.1.1.
Si A et B sont deux parties d'une extension E de K, alors :

$$K(A \cup B) = K(A)(B)$$

Preuve :
$(\supset)$
Tout sous-corps de E qui contient K, A et B contient $K(A)$ et B. Donc $K(A)(B) \subset K(A \cup B)$.
$(\subset)$
Tout sous-corps de E qui contient $K(A)$ et B contient K, A et B. Donc $K(A \cup B) \subset K(A)(B)$.
□

Corollaire 2.1.1.
Soient $K \hookrightarrow E$ une extension de corps et $A = \{a_1, ..., a_n\} \subseteq E$, alors :

$$K(A) = K(a_1, ..., a_n) = K(a_1, ..., a_{i-1}, a_{i+1}, ..., a_n)(a_i)$$

avec $i \in \{1, ..n\}$

Proposition 2.1.1.
Soit $K \hookrightarrow E$ *une extension de corps. Alors* K *et* E *ont même caractéristique.*

Preuve :
En effet :

$$\forall n \in \mathbb{Z} \ : \ n1_K = 0_K \Leftrightarrow n1_E = 0_E \ (car \ 1_K = 1_E \ et \ 0_K = 0_E \ )$$

□

Théorème 2.1.2.
Soit E *une extension de* K*. Pour tout* $a \in E$*, il existe un homomorphisme d'anneaux et un seul :*

$$\sigma_a : K[X] \longrightarrow E$$

qui vérifier $\sigma_a(X) = a$ *et* $\sigma_a(k) = k$, $\forall k \in K$.

Preuve :
Existence :
Soit le morphisme :

$$\begin{array}{rccc} \sigma_a & : & K[X] & \to & E \\ & & P & \mapsto & P(a) \end{array}$$

σ_a *satisfait les conditions du théorème car* $\sigma_a(X) = a$ *et* $\sigma_a(k) = k$, $\forall k \in K$.
Unicité :
Si ϕ *est une autre solution, alors pour tout :*

$$P = \sum_{i=0}^{n} b_i X^i \in K[X]$$

on a :

$$\phi(P) = \phi(\sum_{i=0}^{n} b_i X^i) = \sum_{i=0}^{n} \phi(b_i)\phi(X)^i = \sum_{i=0}^{n} b_i a^i \ (car \ \phi(X) = a \ et \ \phi(b_i) = b_i)$$

donc

$$\phi(P) = P(a) = \sigma_a(P)$$

D'où :

$$\phi = \sigma_a.$$

□

Théorème 2.1.3.
$Im(\sigma_a)$ *est le sous-anneau* $K[a]$ *de* E *engendré par* $K \cup \{a\}$.

Preuve :
On a $Im(\sigma_a)$ *est un sous-anneau de* E*. Il contient* K $(= \sigma_a(K))$ *et* $a = \sigma_a(X)$*, donc :*
$K[a] \subseteq \sigma_a(K)$*, car* $K[a]$ *le plus petit sous anneaux contenant* K *et* a.
Or, pour tout $x \in Im(\sigma_a)$*, il existe* $P \in K[X]$ *tel que :*

$$x = P(a) \in K[a]$$

Finalement :

$$\sigma_a(K) = K[a]$$

□

2.2 Degré d'une extension de corps

Rappel sur les espaces vectoriels :

Soit K un corps.
On appelle un K-espace vectoriel un ensemble E muni de deux lois :
- Une loi interne "$+$" (l'addition vectoriel) tel que $(E,+)$ est un groupe commutatif.
- Une loi externe "$\cdot$" (la multiplication par un scalaire) qu'est une application de $K \times E$ dans E tel que :
$\forall \alpha, \beta \in K^2, \forall x \in E \ : \ (\alpha+\beta)x = \alpha x + \beta x$;
$\forall \alpha \in K, \forall x, y \in E^2 \ : \ \alpha(x+y) = \alpha x + \alpha y$;
$\forall \alpha, \beta \in K^2, \forall x \in E \ : \ \alpha(\beta x) = (\alpha\beta)x$;
$\forall x \in E \ : \ 1x = x$.

Soit E une extension de K, alors E est un K-espace vectoriel où l'addition vectoriel est l'addition de E est la multiplication par un scalaire est la restriction de la multiplication de E dans $K \times E$.

Définition 2.2.1.
Soit E est une extension d'un corps K.
*On appelle le **degré** de l'extension de E sur K est la dimension de K- espace vectoriel E et on le note par $[E : K]$.*
Une extension E de K est dite extension finie si le degré est fini.

Exemple 2.2.1.
1. $[\mathbb{C} : \mathbb{R}] = 2$, *car* $\{1, i\}$ *est une base pour le* $\mathbb{R}$*-espace vectoriel* $\mathbb{C}$.
2. $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, *car* $\{1, \sqrt{2}\}$ *est une base pour le* $\mathbb{Q}$*-espace vectoriel* $\mathbb{Q}(\sqrt{2})$.
3. $[\mathbb{C} : \mathbb{Q}] = [\mathbb{R} : \mathbb{Q}] = \infty$.

Théorème 2.2.1. Théorème de Degré
Soient $K \hookrightarrow L$ et $L \hookrightarrow E$ des extensions de corps. On a :

$$[E : K] = [E : L][L : K].$$

En particulier, l'extension $K \hookrightarrow E$ est finie si, et seulement si, les extensions $L \hookrightarrow E$ et $K \hookrightarrow L$ le sont.

Preuve :
Soient $\{x_i\}_{i\in I}$ une base du L-espace vectoriel E et $\{y_j\}_{j\in J}$ une base du K-espace vectoriel L.
On va montrer que la famille $\{x_i y_j\}_{(i,j)\in I\times J}$ est une base du K-espace vectoriel E :
*C'est **un système générateur**, en effet pour tout $z \in E$ s'écrit :*

$$z = \sum_{i\in I} a_i x_i$$

où $a_i \in L$ pour tout $i \in I$. Or tout a_i peut s'écrire sous forme :

$$a_i = \sum_{j\in J} b_{ij} y_j \ , \ \text{avec les } b_{ij} \in K.$$

Nous obtenons :

$$z = \sum_{i\in I} a_i x_i = \sum_{i\in I} (\sum_{j\in J} b_{ij} y_j) x_i$$

$$= \sum_{(i,j)\in I\times J} b_{ij} y_j x_i$$

C'est ***un système libre****, en effet :*
Si :

$$\sum_{(i,j)\in I\times J} b_{ij} y_j x_i = 0 \ , \ avec\ les\ b_{ij} \in K$$

alors :

$$\sum_{i\in I} (\sum_{j\in J} b_{ij} y_j) x_i = 0$$

ce qui implique :

$$\sum_{j\in J} b_{ij} y_j = 0 \ , \ \forall i \in I$$

car $\{x_i\}_{i\in I}$ *est une base du L-espace vectoriel E. Comme* $\{y_j\}_{j\in I}$ *une base du K-espace vectoriel L, alors* $b_{ij} = 0\ \forall (i,j) \in I \times J$.
Donc la famille $\{x_i y_j\}_{(i,j)\in I\times J}$ *est une base du K-espace vectoriel E. Nous avons alors :*

$$[E : K] = dim_K(E) = Card(I \times J) = Card(I)Card(J)$$

$$= dim_L(E) dim_K(L) = [E : L][L : K]. \qquad \square$$

Corollaire 2.2.1.
Si $K = E_0 \subseteq E_1 \subseteq ..... \subseteq E_n = E$, *alors :*

$$[E : K] = [E_n : E_0] = \prod_{i=1}^{n} [E_i : E_{i-1}].$$

Preuve :
Par une simple récurrence. $\square$

Exemple 2.2.2.
Soit :

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{\alpha + \beta\sqrt{3} \ : \ \alpha, \beta \in \mathbb{Q}(\sqrt{2})\}$$

$$= \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \ : \ a, b, c, d \in \mathbb{Q}\}$$

est une extension de $\mathbb{Q}$ *avec* $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ *est un base pour* $\mathbb{Q}$*-espace vectoriel* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, *donc* $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. *De plus on a* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ *est une extension de* $\mathbb{Q}(\sqrt{2})$ *avec* $\{1, \sqrt{3}\}$ *une base pour le* $\mathbb{Q}(\sqrt{2})$*-espace vectoriel* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, *donc* $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. *Or on ait déjà vu que* $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, *alors le théorème de degré est vérifier, autrement dit :*

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}].$$

2.3 Extension simple

Définition 2.3.1.
*Une extension E de K est **simple** si, et seulement si, $\exists a \in E$ tel que : $E = K(a)$.*

Exemple 2.3.1.
$\mathbb{C}$ est une extension simple de $\mathbb{R}$ car $\mathbb{C} = \mathbb{R}(i)$.
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est simple de $\mathbb{Q}$ avec $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, en effet :
$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ et $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) \Rightarrow \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
D'autre par, on a :
$(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}) \Rightarrow \sqrt{6} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ Alors :

$$\sqrt{6}(\sqrt{2} + \sqrt{3}) = 2\sqrt{3} + 3\sqrt{2} = 2(\sqrt{2} + \sqrt{3}) + \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

Donc $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, on en déduire que $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ et par la suite on a :

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

Finalement :

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

Théorème 2.3.1.
Soit $K \hookrightarrow E$ une extension de corps.
Si $[E : K]$ est finie alors cette extension est engendrée sur K par un nombre fini d'éléments, c'est à dire :

$$E = K(a_1, a_2, ..., a_n), \text{ avec les } a_i \in E.$$

Preuve :
Montrons par récurrence sur $d = [E : K]$:
Si $d = 2$: soit $a \in E - K$, alors $K \subsetneq K(a) \subseteq E$ et :

$$1 < [K(a) : K] \leqslant [E : K] = 2$$

par conséquence : $[K(a) : K] = [E : K] = 2$ et $E = K(a)$.
Supposons que le théorème est vrai pour toute extension de degré $\leqslant d-1$, et montrons qu'il est vrai pour d :
Soit $a_1 \in E - K$ on a : $K \subsetneq K(a_1) \subseteq E$, ce qui implique que $1 < [K(a_1) : K]$, donc :

$$[E : K(a_1)] = \frac{[E : K]}{[K(a_1) : K]} \leqslant d - 1$$

D'après la supposition, on a : $E = K(a_1)(a_2, ..., a_n) = K(a_1, ..., a_n)$.
Ce qui achève le preuve. □

2.4 Élément algébrique, élément transcendent

Définition 2.4.1.
*Soient $K \hookrightarrow E$ une extension de corps et x un élément de E. On dit que x est **algébrique** sur K s'il existe un polynôme non nul $P \in K[X]$ tel que :*

$$P(x) = 0.$$

*Dans le cas contraire, on dit que x est **transcendant** sur K.*

Exemple 2.4.1.
1. $\sqrt{2} \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$, car $\sqrt{2}$ est une racine de :

$$P(X) = X^2 - 2 \in \mathbb{Q}[X].$$

2. $i \in \mathbb{C}$ et algébrique sur $\mathbb{Q}$ et sur $\mathbb{R}$, car i est une racine de :

$$P(X) = X^2 + 1 \in \mathbb{R}[X] \quad (aussi \quad P \in \mathbb{Q}[X]).$$

3. $\pi \in \mathbb{R}$ est transcendant sur $\mathbb{Q}$, car pour tout polynôme $P \in \mathbb{Q}[X]$, π n'est pas une racine de P.

Soient $K \hookrightarrow E$ une extension de corps et $x \in E$. Soit le morphisme :

$$\begin{array}{rccc} \sigma_x & : & K[X] & \to & E \\ & & P & \mapsto & P(x) \end{array}$$

Théorème 2.4.1.
1. Si x est transcendant sur K, le morphisme σ_x est injectif, le K-espace vectoriel $K[x]$ est de dimension infinie et $K \hookrightarrow K(x)$ est infinie.
2. Si x est algébrique sur K, il existe un unique polynôme unitaire P de degré minimal vérifiant $P(x) = 0$. Ce polynôme est irréductible, on a $K[x] = K(x)$ et cette extension de K est finie de degré d $(= deg(P))$ et $\{1, x, x^2, ..., x^{d-1}\}$ est une base de K-espace vectoriel $K(x)$.
*On appelle P le **polynôme minimal** de x sur K.*

Preuve :
1. Si x est transcendant sur K, alors pour tout polynôme P de $K[X] - \{0\}$ on a $P(x) \neq 0$, donc $Ker(\sigma_x) = \{0\}$ ce qui implique que σ_x est injectif. Le 1^{er} théorème d'isomorphisme entraine que :

$$K[X]/\{0\} \cong K[X] \cong K[x] \ (= Im(\sigma_x) \ \ d'après\ le\ théorème\ \ 2.1.3)$$

alors $K[x]$ est un K-espace vectoriel de dimension infinie car $K[X]$ l'est. De plus $K[x] \subseteq K(x)$ qu'est le plus petit corps contenant K et x, alors $K(x)$ est une extension sur K avec $[K(x) : K]$ est infinie.
2. Si x est algébrique sur K, il existe au moins un polynôme non nul de $K[X]$ tel que $P(x) = 0$, donc $Ker(\sigma_x) \neq \{0\}$. Le noyau de σ_x est un idéal de $K[X]$, qui est principal, alors il est engendré par un polynôme non nul de degré minimal P $(P(x) = 0)$, il est unique si on le prend unitaire. D'après le 1^{er} théorème d'isomorphisme on a : $K[X]/ < P > \cong K[x]$ $(= Im(\sigma_x))$. Comme l'anneau $K[x]$ est intègre car c'est un sous-anneau de E (qui est un corps) ; donc

l'idéal $< P >$ est premier (car $K[X]/ < P >$ est intègre). Par la proposition 1.7.1 on a P est irréductible et $< P >$ est maximal donc $K[x]$ est un corps. Comme $K(x)$ est le plus petit corps contient K et x donc :

$$K[x] = K(x).$$

Il reste à montrer que $K(x)$ est une extension finie de K avec $dim_K(K(x)) = d$ $(= deg(P))$ et $\{1, x, x^2, ..., x^{d-1}\}$ est une base de K-espace vectoriel $K(x)$.
$\{1, x, x^2, ..., x^{d-1}\}$ est un système libre car sinon, on peut trouver un polynôme Q non nul de degré inférieur ou égale à $d-1$ tel que x est une racine. Ce polynôme appartient à $< P >$ ce qui impossible car $(deg(Q) < deg(P))$.
Pour prouver que $\{1, x, x^2, ..., x^{d-1}\}$ est un système générateur du K-espace vectoriel E, il suffit de montrer que :

$$x^m \in Vect(1, x, x^2, ..., x^{d-1}) \quad , \quad \forall m \in \mathbb{N}$$

car tout élément a de $K(x) = K[x]$ s'écrit sous forme

$$a = b_0 + b_1 x + ... + b_q x^q \text{ avec } q \in \mathbb{N}.$$

Ceci vrai pour $m \leqslant d-1$. Si $m \geqslant d$, alors m s'écrit $m = d + r$.
Nous allons démontrer $x^m \in Vect(1, x, x^2, ..., x^{d-1})$ par récurrence sur r.
Pour $r = 0$: on écrivant P sous forme

$$P(X) = a_0 + a_1 X + ... + X^d$$

on obtient :

$$P(x) = a_0 + a_1 x + ... + x^d = 0$$

et :

$$x^d = -a_0 - a_1 x - ... - a_{d-1} x^{d-1} \in Vect(1, x, x^2, ..., x^{d-1})$$

Supposons que : $x^{d+r} \in Vect(1, x, x^2, ..., x^{d-1})$ est vrai pour r, et montrons que :

$$x^{d+r+1} \in Vect(1, x, x^2, ..., x^{d-1}).$$

D'après la supposition, il existe $c_i \in K$ pour $i = 0, 1, ..., d-1$ tel que :

$$x^{d+r} = c_0 + c_1 x + ... + c_{d-1} x^{d-1}$$

donc :

$$x^{d+r+1} = c_0 x + c_1 x^2 + ... + c_{d-1} x^d$$

alors :

$$x^{d+r+1} \in Vect(1, x, x^2, ..., x^{d-1})$$

car :

$$c_0 x + c_1 x^2 + ... + c_{d-2} x^{d-1} \in Vect(1, x, x^2, ..., x^{d-1}) \text{ et } c_{d-1} x_d \in Vect(1, x, x^2, ..., x^{d-1})$$

Il résulte que $x^m \in Vect(1, x, x^2, ..., x^{d-1})$ pour tout $m \in \mathbb{N}$. Ceci prouve que :

$$dim_K(K(x)) = [K(x) : K] = d.$$

□

Remarque 2.4.1.
Le polynôme minimal sur un corps K d'un élément algébrique x d'une extension E de K divise tous les polynômes $P \in K[X]$ tel que : $P(x) = 0$.

2.5 Extensions algébriques, extensions transcendantes

Définition 2.5.1.
*Une extension E d'un corps K est dite **algébrique** sur K, si tout élément de E est algébrique sur K.*
*Dans le cas contraire, on dit que E est **transcendante** sur K.*

Exemple 2.5.1.
1. $\mathbb{C}$ est une extension algébrique sur $\mathbb{R}$, car pour tout $z = a + bi \in \mathbb{C}$ (avec $a, b \in \mathbb{R}$), z est une racine de polynôme $P(X) = X^2 - 2aX + a^2 + b^2 \in \mathbb{R}[X]$.
2. $\mathbb{R}$ est une extension transcendante sur $\mathbb{Q}$, car $\pi \in \mathbb{R}$ est transcendant sur $\mathbb{Q}$.

Théorème 2.5.1.
Toute extension E de degré fini sur un corps K est algébrique sur K.

Preuve :
Posons $[E : K] = n$, avec $n \in \mathbb{N}$. Soit $a \in E$:
Les éléments $1, a, a^2, ..., a^n$ sont linéairement dépendants car $dim_K(E) = n$. Il existe $b_0, b_1, ..., b_n$ des éléments de K, non tous nuls, tels que :

$$b_0 + b_1 a + ... + b_{n-1} a^{n-1} + b_n a^n = 0$$

Si :

$$P = b_0 + b_1 X + ... + b_{n-1} X^{n-1} + b_n X^n$$

alors $P \neq 0$ et $P(a) = 0$. Ce qui prouve que a est algébrique sur K. □

Remarque 2.5.1.
La réciproque est fausse, contre exemple :
Soit :

$$\overline{\mathbb{Q}} = \{x \in \mathbb{C} \ : \ x \text{ est algébrique sur } \mathbb{Q}\}$$

$\overline{Q}$ est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$ (voir la preuve de théorème 3.3.3), de plus $\overline{\mathbb{Q}}$ est une extension algébrique de $\mathbb{Q}$ mais $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$, car pour tout $n \in \mathbb{N}^*$, il existe $x \in \overline{\mathbb{Q}}$ tel que $[\mathbb{Q}(x) : \mathbb{Q}] > n$. Par exemple :
Soient $n \in \mathbb{N}$ fixé et $x = \sqrt[n+1]{2}$, x est une racine de $P(X) = X^{n+1} - 2 \in \mathbb{Q}[X]$ de plus P est irréductible sur $\mathbb{Q}[X]$, et comme la polynôme minimal P_x de x sur $\mathbb{Q}$ divise P sur $\mathbb{Q}[X]$, alors $P = P_x$ donc le $deg(P_x) = n + 1$. D'après le théorème 2.4.1 on a : $[\mathbb{Q}(x) : \mathbb{Q}] = n + 1$.
Donc pour tout $n \in \mathbb{N}^*$, $\overline{\mathbb{Q}}$ contient un sous-espace vectoriel de dimension supérieur à n, alors $\overline{\mathbb{Q}}$ est $\mathbb{Q}$-un espace vectoriel de dimension infinie.

Corollaire 2.5.1.
Une extension simple $E = K(a)$ est algébrique si, et seulement si, a est algébrique sur K.

Preuve :
Si a est algébrique sur K, d'après le théorème 2.4.1 E est une extension finie de K, ce qui prouve que cette extension est algébrique (théorème 2.5.1).
Réciproquement, si l'extension E est algébrique, alors a est algébrique sur K. □

Corollaire 2.5.2.
Toute extension E engendrée par un nombre fini d'éléments algébriques sur K est finie, donc algébrique.

Preuve :
Supposons que : $A = \{a_1, a_2, ..., a_n\}$ *un ensemble des éléments algébriques sur* K*, tel que* $E = K(a_1, a_2, ..., a_n)$*. Posons :*

$$K_0 = K \quad et \quad K_i = K(a_1, a_2, ..., a_i) \ pour \ i = 1, 2, ..., n$$

Soit $i \in \{1, 2, ..., n\}$*, nous avons* $K_i = K_{i-1}(a_i)$*. D'un autre côté,* a_i *est algébrique sur* K_{i-1}*, car il est algébrique sur* K *et* $K \subseteq K_{i-1} \subseteq K_i$*. Ceci implique que le degré* $[K_i : K_{i-1}]$ *est fini. On alors :*

$$[E : K] = [K_n : K_0] = \prod_{i=1}^{n} [K_i : K_{i-1}] \quad est \ fini.$$

Ainsi l'extension E *de* K *est finie. d'après le théorème 2.5.1* E *est algébrique sur* K*.* □

Théorème 2.5.2.
Soient $K \hookrightarrow L$ *et* $L \hookrightarrow E$ *des extensions de corps. Si un élément* x *de* E *est algébrique sur* L *et que* L *est une extension algébrique de* K*, alors* x *est algébrique sur* K*.*
En particulier, si $K \hookrightarrow L$ *et* $L \hookrightarrow E$ *deux extensions algébriques, alors :* $K \hookrightarrow E$ *est algébrique.*

Preuve :
Si un élément x *de* E *est algébrique sur* L*, alors il est racine d'un polynôme* $P \in L[X]$*, écrivons :*

$$P(X) = \sum_{i=0}^{n} a_i X^i \ avec \ a_i \in L$$

On pose $L' = K(a_0, ..., a_n) \subseteq L$ *est extension de* K*, comme l'extension* $K \hookrightarrow L$ *est algébrique donc les* a_i *sont algébriques sur* K*, alors* L' *est une extension finie de* K *d'après le corollaire 2.5.2. Comme* x *est algébrique sur* L' *car* $P \in L'[X]$*, l'extension* $L' \hookrightarrow L'(x)$ *est finie (théorème 2.4.1), entraîne que l'extension* $K \hookrightarrow L'(x)$ *est finie, donc algébrique (théorème 2.5.1), et* x *est algébrique sur* K*.* □

3

Polynômes et racines

3.1 Corps de rupture

Définition 3.1.1.
Soit K un corps et $P \in K[X]$ irréductible. On appelle ***corps de rupture*** *de P sur K toute extension E tel que :*
- Dans E, P admet une racine a.
- E est engendré par K et a (E est une extension simple $K(a)$).

Exemple 3.1.1.
Le polynôme $P(X) = X^2 + 1 \in \mathbb{R}[X]$ est irréductible, un corps de rupture de ce polynôme est $\mathbb{C}$, puisque $i \in \mathbb{C}$ est un racine de ce polynôme et $\mathbb{C} = \mathbb{R}(i)$.

Théorème 3.1.1. Décomposition en facteurs irréductibles
Soit P un polynôme non constant de $K[X]$. Alors il existe un scalaire λ non nul, des polynômes $P_1, P_2, ..., P_k$ irréductibles sur $K[X]$, unitaires, distincts deux à deux et des entiers positifs non nuls $n_1, n_2, ..., n_k$, uniques tels que :

$$P = \lambda \prod_{i=1}^{k} P_i^{n_i}$$

Cette décomposition est unique.

Preuve :
Voir la démonstration de ce lemme dans l'ouvrage :
Olivier Debarre : Algèbre 2, ENS, 2012-2013, page 4. □

Définition 3.1.2. Morphisme de K-extensions (ou K-morphisme)
Si E, F sont des extensions de corps K. On appelle ***K-morphisme*** *de E dans F un morphisme de corps qui vaut l'identité sur K.*

Théorème 3.1.2.
Si P est un polynôme irréductible dans $K[X]$ alors P possède un corps de rupture sur K.

Preuve :
Soit $M =< P >$, M est un idéal maximal car $K[X]$ est un anneau principal et P est irréductible (théorème 1.7.1). Soit $E = K[X]/M$, alors E est un corps. On peut regarder E comme une

extension de K. Pour voir ça, soit $f : K[X] \longrightarrow E$ la surjection canonique. La restriction $\tilde{f}$ de f à K est un homomorphisme non nul car $f(1) = \overline{1}$. Il résulte que cet homomorphisme est injectif car $\tilde{f}$ est un morphisme de corps (l'anneau de départ est un corps). On en déduit que $K \cong \tilde{f}(K) \subseteq E$. Ainsi E devient une extension de K (définition 2.1.1).
Soit $\alpha = \overline{X} = f(X)$. Écrivons :

$$P(X) = a_0 + a_1X + ... + a_nX^n$$

nous obtient :

$$\begin{aligned} P(\alpha) &= \sum_{i=0}^{n} a_i\alpha^i = \sum_{i=0}^{n} a_i\overline{X}^i = \sum_{i=0}^{n} a_i\overline{X^i} \\ &= \sum_{i=0}^{n} \overline{a_iX^i} = \sum_{i=0}^{n} f(a_iX^i) \\ &= f(\sum_{i=0}^{n} a_iX^i) = f(P(X)) \end{aligned}$$

comme $P \in M$, alors $f(P(X)) = \overline{0} = P(\alpha)$.
Donc E est une extension de K contenant la racine α de P, alors α est algébrique sur K.
Comme l'image de f, d'après le théorème 2.4.1, est $K[\alpha] = K(\alpha)$, donc :

$$K(\alpha) = E \ \ car\ f\ est\ surjectif.$$

D'où E est un corps de rupture de P. □

Corollaire 3.1.1.
Tout polynôme $P \in K[X]$ possède un corps de rupture sur K.

Preuve :
En effet, tout polynôme $P \in K[X]$ se décompose en produit de polynômes irréductibles. □

Théorème 3.1.3.
Soit P un polynôme de $K[X]$ irréductible. Deux corps de rupture de P sont K-isomorphes.

Preuve :
Soient x une racine de P dans un corps de rupture $E = K(x)$ de P et le morphisme d'annaux suivant :

$$\begin{array}{rccc} f & : & K[X] & \to & E \\ & & Q & \mapsto & Q(x) \end{array}$$

comme x est algébrique sur K, alors $Im(f) = K[x] = K(x) = E$. De plus $Ker(f) =< P >$, en effet :
comme $P(x) = 0$ on a $P \in Ker(f)$ ce qui implique que $< P > \subseteq Ker(f)$ de plus $< P >$ est maximal car P est irréductible, donc $Ker(f) =< P >$. D'où :

$$K[X]/ < P > \cong E$$

posons :
σ un isomorphisme de $K[X]/ < P >$ dans E.

S la surjection canonique de $K[X]$ dans $K[X]/ < P >$.
On a :

$$f = \sigma \circ S$$

alors

$$\forall k \in K \text{ on a } : \ f(k) = k = \sigma(S(k)) = \sigma(\bar{k}).$$

Finalement si $E = K(x)$ et $E^{'} = K(x^{'})$ deux corps de rupture, alors il sont K-isomorphes. □

Remarque 3.1.1.
L'isomorphisme entre deux corps de rupture n'est en général pas unique. Plus précisément, étant donnés des corps de rupture $K \hookrightarrow K(x)$ et $K \hookrightarrow K(x^{'})$ de P, il existe un unique K-isomorphisme $\theta : K(x) \longrightarrow K(x^{'})$ tel que : $\theta(x) = x^{'}$.

3.2 Corps de décomposition

Définition 3.2.1.
*Une extension E de K est un **corps de décomposition** pour P sur K si P peut être scindé dans $E[X]$, c'est à dire qu'il peut être décomposé en produit des polynômes linéaires dans $E[X]$ (de degré 1) et qui soit minimale pour cette propriété.*

Exemple 3.2.1.
Le corps $\mathbb{C}$ est un corps de décomposition sur $\mathbb{R}$ pour le polynôme $X^2 + 1$.

Théorème 3.2.1.
Tout polynôme $P \in K[X]$ possède un corps de décomposition sur K.

Preuve :
On procède par récurrence sur le degré n de P.
Si $n = 1$, K est un corps de décomposition de P sur K.
Supposons que le théorème est vrai pour tout polynôme de degré $\leqslant n-1$, et démontrons-le pour les polynômes de degré n. D'après le corollaire 3.1.1, on pose E un corps de rupture de K engendré par la racine a_1 de P. Nous avons $P(X) = (X - a_1)Q(X)$ dans $E[X]$ avec $deg(Q) = n - 1$. D'après hypothèse de récurrence, il existe un corps de décomposition F de Q sur E, donc :

$$Q(X) = k\prod_{i=2}^{n}(X - a_i) \ \ dans \ F[X]$$

et :

$$P(X) = (X - a_1)Q(X) = (X - a_1)k\prod_{i=2}^{n}(X - a_i)$$

$$= k\prod_{i=1}^{n}(X - a_i) \ \ dans \ F[X].$$

Ainsi F est un corps de décomposition pour P sur K □

Théorème 3.2.2.
Si E un corps de décomposition d'un polynôme $P \in K[X]$ de degré n. Alors E est une extension finie de K tel que :

$$[E : K] \leqslant n!$$

Preuve :
On procède par la récurrence sur n :
Si $n = 1$, le résultat est claire, car $E = K$ donc $[E : K] = 1$.
Supposons que le théorème est vrai pour tout polynôme de degré $\leqslant n-1$ et montrons qu'il est vrai pour n :
Soit $a \in E$ une racine de P, alors $K(a)$ un corps de rupture de P sur K. Soit Q le polynôme minimal de a sur K, on a alors $[K(a) : K] = deg(Q)$ (théorème 2.4.1) et $deg(Q) \leqslant deg(P)$.
Écrivons $P(X) = (X - a)R(X)$ sur $K(a)[X]$ tel que $deg(R) = n - 1$ et comme E est un corps de décomposition de R sur $K(a)$ alors, d'après l'hypothèse de récurrence, on a

$$[E : K(a)] \leqslant deg(R)! = (n-1)!$$

D'autre part, on a :

$$[E : K] = [E : K(a)][K(a) : K] = [E : K(a)]deg(Q) \leqslant deg(Q)(n-1)!$$

donc :

$$[E : K] \leqslant deg(P)(n-1)! = n(n-1)! = n!$$

□

Théorème 3.2.3.
Deux corps de décomposition E et E' pour un polynôme $P \in K[X]$ sont K-isomorphes.

Preuve :
Supposons que E et E' sont des corps des décompositions du polynôme $P \in K[X]$.
Montrons par la récurrence sur $[E : K]$.
Si $[E : K] = 1$, K est un corps de décomposition de P sur K donc toutes les racines de P sont dans K, la minimalité de corps de décomposition entraine que $E' = K$, donc $E = E'$.
Supposons que le théorème est vrai pour $n-1$. Montrons-le pour n :
Soient Q un facteur irréductible de P dans $K[X]$ et $x \in E$ une racine de Q, alors $K(x)$ est un corps de rupture de P avec $K(x)$ est un sous-corps de E et de E' car $x \in E'$. Dans $K(x)[X]$ on peut écrire $P(X) = (X - x)R(X)$ avec $R \in K(x)[X]$, de plus on a E et E' sont des corps de décomposition de R dans $K(x)$ et comme $[K(x) : K] > 1$ car $K \subsetneq K(x)$ donc :

$$[E : K(x)] = \frac{[E : K]}{[K(x) : K]} < n$$

D'après l'hypothèse de récurrence, E et E' sont $K(x)$-isomorphes ce qui implique que E et E' sont K-isomorphes car $K \subsetneq K(x)$. □

3.3 Clôture algébrique

Définition 3.3.1.
*Le corps Ω est dit **algébriquement clos** si tout polynôme non constant de $\Omega[X]$ a au moins une racine dans Ω.*
*Une **clôture algébrique** d'un corps K est une extension algébrique de corps $K \hookrightarrow \Omega$ telle que Ω est un corps algébriquement clos.*

Exemple 3.3.1.
1. $\mathbb{C}$ est algébriquement clos, mais $\mathbb{R}$ n'est pas algébriquement clos, car : $P(X) = X^2+1 \in \mathbb{R}[X]$ n'admet pas de racine sur $\mathbb{R}$.
2. Le corps $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$, mais pas de $\mathbb{Q}$ puisque il n'est pas algébrique sur $\mathbb{Q}$.

Proposition 3.3.1.
Si Ω un corps est dit algébriquement clos, tout polynôme $P \in \Omega[X]$ non constant est scindé dans $\Omega[X]$.

Preuve :
Par récurrence sur $n = deg(P)$:
Si $n = 1$: P est scindé dans $\Omega[X]$.
Supposons que la proposition est vraie pour tout polynôme de degré $< n$, et montrons-le pour n.
Soit $P \in \Omega[X]$ non constant de degré n, comme Ω est algébriquement clos donc P possède une racine x dans Ω, alors dans $\Omega[X]$, on a : $P(X) = (X - x)Q(X)$ avec $Q \in \Omega[X]$ tel que $deg(Q) = n - 1$, d'après l'hypothèse de récurrence Q est scindé dans $\Omega[X]$. Alors P est scindé $\Omega[X]$. □

Proposition 3.3.2.
Soit $K \hookrightarrow E$ une extension algébrique de corps. Si tout polynôme de $K[X]$ est scindé dans E, alors E est une clôture algébrique de K.

Preuve :
Pour montrer que E est une clôture algébrique il suffit de montrons que E est un corps algébriquement clos.
Soient $Q \in E[X]$ un polynôme irréductible et x une racine de Q dans une extension de E. Alors x est algébrique sur E, d'après le théorème 2.5.2 x est algébrique sur K. Soit $P \in K[X]$ le polynôme minimal de x sur K ; puisque Q est irréductible sur E, on a $Q|P$ dans $E[X]$. Mais par hypothèse, P est scindé dans E donc $x \in E$, et Q a donc une racine dans E. Comme pour tout polynôme $R \in E[X]$ est produit de polynômes irréductibles, alors R elle admet un racine dans E, donc E est algébriquement clos. On a alors montré que E est une clôture algébrique de K. □

Proposition 3.3.3.
Soient Ω un corps algébriquement clos et $K \subseteq \Omega$ un sous-corps. L'ensemble des éléments de Ω qui sont algébriques sur K est une clôture algébrique de K. On le note par :

$$\overline{K} = \{a \in \Omega \ : \ a \text{ est algébrique sur } K\}$$

Preuve :
L'ensemble $\overline{K}$ est un sous-corps de Ω, en effet :
- $\overline{K} \neq \emptyset$ car $K \subseteq \overline{K}$.
- Soient $x, y \in \overline{K}$, avec $y \neq 0$ on a x et y sont algébriques sur K. D'après la corollaire 2.5.2, $K \hookrightarrow K(x, y)$ est algébrique, comme $x - y \in K(x, y)$ et $xy^{-1} \in K(x, y)$, alors $x - y$ et xy^{-1} sont algébriques, donc :

$$x - y, xy^{-1} \in \overline{K}$$

D'où $\overline{K}$ une extension algébrique de K. Maintenant, il reste à montrons que $\overline{K}$ est algébriquement clos :

Soit $P \in \overline{K}[X] \subseteq \Omega[X]$ un polynôme non constant, comme Ω est algébriquement clos alors P possédé une racine $x \in \Omega$ c'est à dire x est algébrique sur $\overline{K}$, donc aussi sur K (théorème 2.5.2), de sorte que $x \in \overline{K}$. □

Théorème 3.3.1.
Soit $K \hookrightarrow K(x)$ une extension de corps tel que x est algébrique sur K, de polynôme minimal $P \in K[X]$. Toute extension $K \hookrightarrow \Omega$, où Ω est un corps algébriquement clos tel que $K \subseteq \Omega$, se prolonge en $K(x) \hookrightarrow \Omega$, et le nombre de ces prolongements est égal au nombre de racines distinctes de P dans son corps de décomposition.

Preuve :
Posons le morphisme d'un inclusion $i : K \hookrightarrow \Omega$.
- Soit le morphisme :

$$\begin{array}{rccc} \phi & : & K[X] & \to & \Omega \\ & & Q & \mapsto & Q(x) \end{array}$$

On a $Ker(\phi) =< P >$, posons :

$$\bar{\phi} : K[X]/ < P > \longrightarrow \Omega$$

Le morphisme qui s'en déduit.
Or, $K(x) \cong K[X]/ < P >$ via une K-isomorphisme θ. Alors $\sigma = \bar{\phi} \circ \theta$ est une prolongement de i à $K(x)$, car pour tout $k \in K$ on a :

$$\sigma(k) = \bar{\phi}(\theta(k)) = \bar{\phi}(\bar{k}) = \bar{\phi}(S(k)) = \phi(k) = k = i(k)$$

avec S la surjection canonique de $K[X]$ dans $K[X]/ < P >$.
- Comme pour tout K-morphisme σ de $K(x)$ dans Ω, on a :

$$P(\sigma(x)) = \sigma(P(x)) = 0$$

alors le donner d'un K-morphisme σ de $K(x)$ dans Ω est équivalent à se donner un élément $\sigma(x) \in \Omega$ qui vérifie $P(\sigma(x)) = 0$ car x est un générateur de $K(x)$. Il y a donc exactement autant de tels morphismes que de racines de P dans Ω qui est une extension de K et algébriquement clos, alors Ω il contient un corps de décomposition de P, ce qui montre le théorème. □

Corollaire 3.3.1.
Soit $K \hookrightarrow E$ une extension algébrique de corps. Toute extension $K \hookrightarrow \Omega$ où Ω est un corps algébriquement clos, se prolonge en $E \hookrightarrow \Omega$.

Preuve :
Dans cette démonstration, on va utilisé le lemme suivant :

Lemme 3.3.1. LEMME DE ZORN
Tout ensemble inductif admet au moins un élément maximal.

Rappel:

Soit E un ensemble partiellement ordonné.
*E est dit **inductif** si toute partie de E non vide et totalement ordonnée possède un majorant.*

Preuve :
Voir la démonstration de ce lemme dans le site suivant :
https://fr.wikipedia.org/wiki/Lemme_de_Zorn. □

Posons les injections canoniques suivantes :

$$u : K \hookrightarrow E \quad et \quad v : K \hookrightarrow \Omega$$

On désigne par $\mathcal{F}$ *l'ensemble des extensions algébriques* F *de* K *tel que* $K \subseteq F \subseteq E$ *et pour lesquelles il existe un monomorphisme* $\sigma : F \longrightarrow \Omega$, *tel que* $\sigma_{|K} = v$.
On considère l'ensemble $\mathcal{E}$ *des couples* (F, σ), *où* $F \in \mathcal{F}$. *on a* $\mathcal{E} \neq \emptyset$, *car* $(K, v) \in \mathcal{E}$.
On considère, dans $\mathcal{E}$, *la relation binaire, notée* $\leq$, *définie par :*

$$(F, \sigma) \leq (F^{'}, \sigma^{'}) \Leftrightarrow F \subseteq F^{'} \text{ et } \sigma^{'}_{|F} = \sigma$$

La relation $\leq$ *est une relation d'ordre partiel dans* $\mathcal{E}$, *en effet :*
Réflexivité :
Soit $(F, \sigma) \in \mathcal{E}$ *: on a* $F \subseteq F$ *et* $\sigma_{|F} = \sigma$. *Ainsi* $\leq$ *est réflexive dans* $\mathcal{E}$.
Antisymétrique :
Soient $(F, \sigma), (F^{'}, \sigma^{'}) \in \mathcal{E}$ *tel que* $(F, \sigma) \leq (F^{'}, \sigma^{'})$ *et* $(F^{'}, \sigma^{'}) \leq (F, \sigma)$, *alors :*
$(F \subseteq F^{'}$ *et* $\sigma^{'}_{|F} = \sigma)$ *et* $(F^{'} \subseteq F$ *et* $\sigma_{|F^{'}} = \sigma^{'})$ *ce qui implique que* $F = F^{'}$ *et* $\sigma = \sigma^{'}$. *Ainsi* $\leq$ *est antisymétrique dans* $\mathcal{E}$.
Transitivité :
Soient $(F, \sigma), (F^{'}, \sigma^{'}), (F^{''}, \sigma^{''}) \in \mathcal{E}$ *tel que* $(F, \sigma) \leq (F^{'}, \sigma^{'})$ *et* $(F^{'}, \sigma^{'}) \leq (F^{''}, \sigma^{''})$, *alors :*
$(F \subseteq F^{'}$ *et* $\sigma^{'}_{|F} = \sigma)$ *et* $(F^{'} \subseteq F^{''}$ *et* $\sigma^{''}_{|F^{'}} = \sigma^{'})$ *ce qui implique que :*

$$F \subseteq F^{''} \quad et \quad \sigma^{''}_{|F} = (\sigma^{''}_{|F^{'}})_{|F} = \sigma^{'}_{|F} = \sigma$$

donc $(F, \sigma) \leq (F^{''}, \sigma^{''})$. *Ainsi* $\leq$ *est transitive dans* $\mathcal{E}$.
Or, l'ensemble partiellement ordonné $\mathcal{E}$ *est inductif, en effet :*
Soit $\{(F_i, \sigma_i)\}_{i \in I} \subseteq \mathcal{E}$ *une famille totalement ordonnée, alors :*
$F = \cup_{i \in I} F_i$ *est un corps tel que* $K \subseteq F \subseteq \Omega$ *; de plus, pour tout* $i \in I$, *on a* F_i *est algébrique sur* K, *par la suite* F *est algébrique sur* K.
On définit un monomorphisme $\sigma : F \longrightarrow \Omega$ *en posant :*

$$\forall i \in I \ , \ \sigma_{|F_i} = \sigma_i$$

ce qui implique $\sigma_{|K} = v$ *car pour tout* $i \in I$, $\sigma_{i_{|K}} = v$.
On déduit que le couple (F, σ), *ainsi défini, appartient à* $\mathcal{E}$ *et est un majorant pour la famille* $\{(F_i, \sigma_i)\}_{i \in I}$. *Par la suite, l'ensemble partiellement ordonné* $\mathcal{E}$ *est inductif. Alors, selon le lemme de ZORN, il existe un élément maximal* (M_0, σ_0) *dans* $\mathcal{E}$.
Puisque E *est une extension algébrique de* K, *alors tout élément* $x \in E$ *est algébrique sur* $K \subseteq M_0$, *donc il est algébrique sur* M_0. *Le théorème précédent dit que l'on peut prolongé* σ_0 *en* $M_0(x) \hookrightarrow \Omega$. *Par maximalité de* (M_0, σ_0), *cela entraîne* $M_0(x) = M_0$ *c'est-à-dire* $x \in M_0$, *donc* $E = M_0$.
Ce qui achève le preuve. □

Théorème 3.3.2. Théorème de Steinitz
Soit K un corps.
1. K possède une clôture algébrique.
2. Deux clôtures algébriques de K sont K-isomorphes.

Preuve :
1. Soient $\mathcal{P} = K[X] - K$ ensemble des polynômes non constants et $\{X_P\}_{P\in\mathcal{P}}$ une famille d'indéterminées sur K. On pose :

$$A = K[\{X_P\}_{P\in\mathcal{P}}]$$

l'anneau des polynômes sur K à une infinité d'indéterminées.

Remarque 3.3.1.
$Q \in A \Leftrightarrow \exists n \in \mathbb{N}^*$ et $\exists\{P_1, ..., P_n\} \subseteq \mathcal{P}$ tel que $Q \in K[X_{P_1}, ..., X_{P_n}]$.
Soient $Q, R \in A$, si $Q \in K[X_{P_1}, ..., X_{P_n}]$ et $R \in K[X_{P'_1}, ..., X_{P'_m}]$, on a :

$$Q - R, QR \in K[X_{P_1}, ..., X_{P_n}, X_{P'_1}, ..., X_{P'_m}]$$

Soit I un idéal de A engendré par l'ensemble :

$$\{P(X_P) \in K[X_P] \subseteq A \ : \ P \in \mathcal{P}\}$$

Ce idéal est un idéal propre de A, en effet :
Supposons que $I = A$, ce qui implique que $1 \in I$, donc :

$$\exists n \in \mathbb{N}^* \text{ et } Q_1, ..., Q_n \in A \text{ et } P_1, ..., P_n \in \mathcal{P} \text{ tel que } 1 = \sum_{i=1}^{n} Q_i P_i(X_{P_i})$$

D'après le corollaire 3.1.1 pour tout $i \in \{1, ..., n\}$, il existe une extension (corps de rupture) de P_i sur K dans laquelle a une racine a_i. Considérant le corps $L = K(a_1, ..., a_n)$, la relation précédent reste valable sur $L[\{X_P\}_{P\in\mathcal{P}}]$, ce qui entraine la contradiction suivante :

$$1 = \sum_{i=1}^{n} Q_i P_i(a_i) = 0$$

alors $1 \notin I$ ce qui implique $I \neq A$.
D'où il existe un idéal maximal M de A contenant I.
Posons $E_1 = A/M$, On a E_1 est un corps, on peut considéré E_1 comme une extension de K, car :
Soient la projection canonique $\pi : A \longrightarrow E_1$ et l'injection canonique $i : K \longrightarrow A$, on a $f(= \pi \circ i) : K \longrightarrow E_1$ est un morphisme de corps non nul car :

$$f(1) = \pi \circ i(1) = \pi(i(1)) = \pi(1) = \bar{1}$$

alors f est injectif ce qui implique $K \cong f(K) \subseteq E_1$, d'après la définition 2.1.1 on peut considéré E_1 comme un extension de K.

Montrons que tout polynôme non constant de $K[X]$, a au mois une racine dans E_1.
Par définition de idéal I :

$$P(X_P) \in I \subseteq M \Rightarrow \pi(P(X_P)) = \bar{0} \ \ dans \ E_1$$

On pose : $\alpha = \pi(X_P)$ et $P(X_P) = \sum_{i=0}^{n} a_i X_P^i$ dans $K[X_P] - K$, alors :

$$P(\alpha) = \sum_{i=0}^{n} a_i \alpha^i = \sum_{i=0}^{n} a_i \pi(X_P)^i = \sum_{i=0}^{n} \pi(a_i X_P^i) = \pi(P(X_P)) = \bar{0}$$

Ainsi α est une racine de P dans E_1.
En reprenant, à partir du corps E_1, le raisonnement fait à partir de K, et on construire un corps E_2 qui est une extension de E_1 tel que :

$$K \subseteq E_1 \subseteq E_2$$

et $\forall P \in E_1[X] - E_1$ a une racine dans E_2.
On suive ce procédure, on obtient, de proche en proche, une chaine croissante au sens d'inclusion d'extensions de corps :

$$K \subseteq E_1 \subseteq E_2 \subseteq ... \subseteq E_n \subseteq E_{n+1} \subseteq ...$$

telle que $\forall n \in \mathbb{N}^*, \forall P \in E_n[X] - E_n$ a un racine dans E_{n+1}.
On pose :

$$E_0 = K \ \ et \ \ E = \bigcup_{n \in \mathbb{N}} E_n$$

la famille $\{E_n\}_{n \in \mathbb{N}}$ est totalement ordonnée par l'inclusion, donc E est un corps ce qui implique E est une extension de K. Vérifions que E est algébriquement clos.
Soit $P \in E[X] - E$ tel que :

$$P(X) = \sum_{i=0}^{n} a_i X^i, \ deg(P) = n \geqslant 1$$

il existe alors $k \in \mathbb{N}$ tel que $\{a_0, a_1, ..., a_n\} \subseteq E_k$, par la suite $P \in E_k[X] - E_k$.
Donc le polynôme P a une racine dans $E_{k+1} \subseteq E$, ce qui implique que E est algébriquement clos.
D'où la proposition 3.3.3 entraine que K possède une clôture algébrique.

2. Soient les inclusions $i : K \hookrightarrow \Omega$ et $j : K \hookrightarrow \Omega'$ sont des clôtures algébriques, j se prolonge par le corollaire 3.3.1 en un monomorphisme $\sigma : \Omega \longrightarrow \Omega'$, de plus ce monomorphisme est surjectif, en effet :
On a $\sigma(\Omega) \subseteq \Omega'$. D'autre par, Ω est algébriquement clos et $\Omega \cong \sigma(\Omega)$ alors $\sigma(\Omega)$ est algébriquement clos. Soit $x \in \Omega'$:
Posons P le polynôme minimal de x sur $\sigma(\Omega)[X]$ car $\sigma(\Omega) \subseteq \Omega'$, or $\sigma(\Omega)$ est algébriquement clos, donc $x \in \sigma(\Omega)$ ce qui implique $\Omega' \subseteq \sigma(\Omega)$.
Donc :

$$\sigma(\Omega) = \Omega'$$

Comme σ est un monomorphisme surjectif et pour tout $k \in K$ on a $\sigma(k) = k$, donc σ un K-isomorphisme de Ω dans Ω'. □

4

Extensions normales - Extensions séparables

4.1 Extensions normales

Définition 4.1.1.
Soit E une extension de corps K. E est dite ***normale*** *sur K, si :*
- E est algébrique sur K.
- Tout polynôme irréductible de $K[X]$, qui a une racine dans E, est scindé sur E.

Exemple 4.1.1.
1. $\mathbb{C}$ est une extension normale de $\mathbb{R}$.
2. L'extension $\mathbb{Q}(\sqrt[3]{2})$ de $\mathbb{Q}$ n'est pas normale, car $P(X) = X^3 - 2 \in \mathbb{Q}[X]$ possède une racine dans $\mathbb{Q}(\sqrt[3]{2})$ sans se décomposer en produit de facteurs linéaires dans $\mathbb{Q}(\sqrt[3]{2})[X]$, car :

$$P(X) = X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$$

$X^2 + \sqrt[3]{2}X + \sqrt[3]{4}$ est irréductible dans $\mathbb{Q}(\sqrt[3]{2})[X]$ car il est irréductible dans $\mathbb{R}[X]$.

Théorème 4.1.1.
Soit $K \hookrightarrow E$ une extension de corps. les propriétés suivantes sont équivalentes :
(i) $K \hookrightarrow E$ est un extension finie et normale ;
(ii) E est le corps de décomposition d'un polynôme $Q \in K[X]$.

Preuve :
$(i) \Rightarrow (ii)$
Supposons que $K \hookrightarrow E$ est un extension finie et normale :
Comme E est finie, d'après le théorème 2.3.1 on a : $E = K(a_1, ..., a_n)$ avec les $a_i \in E$.
Pour $i = 1, 2, ..., n$, posons $P_i \in K[X]$ le polynôme minimal de a_i. Comme $K \hookrightarrow E$ est normal alors les P_i sont scindés sur E (car $a_i \in E$ une racine de P_i), donc aussi :

$$Q = \prod_{i=1}^{n} P_i$$

est scindé sur E.
De plus E est engendré par des racines de Q, le corps E est corps de décomposition de Q (car elle est le minimal pour la décomposition).

$(i) \Leftarrow (ii)$
Supposons que E est le corps de décomposition d'un polynôme $Q \in K[X]$ sur K donc, E est une extension finie de K (le théorème 3.2.2).
Montrons que E est une extension normale de K :
Soit $P \in K[X]$ un polynôme irréductible a une racine a_1 dans E, soit M le corps de décomposition de P sur K, alors M est une extension de E, et soit a_2 une racine de P dans M. Pour montrer que $K \hookrightarrow E$ et normale il suffit de montrer que $a_2 \in E$, car cela entrainera que toutes les racines de P dans M sont en fait dans E.
Or, $\forall i \in \{1, 2\}$, on peut considéré que $E(a_i)$ est un corps de décomposition de Q sur $K(a_i)$. De plus $\forall i \in \{1, 2\}$, $K(a_i)$ est un corps de rupture de P sur K, donc il existe un K-isomorphisme entre $K(a_1)$ et $K(a_2)$. Les extensions $K(a_1) \hookrightarrow E(a_1) = E$ et $K(a_1) \cong K(a_2) \hookrightarrow E(a_2)$ sont des corps de décompositions de Q sur $K(a_1)$, d'après le théorème 3.2.3 E et $E(a_2)$ sont donc $K(a_1)$-isomorphes, ce qui implique que $E = E(a_2)$, alors $a_2 \in E$.
Ce qui achève le preuve. □

Remarque 4.1.1.
Si $K \hookrightarrow E$ est une extension finie et normale de corps et que L est un corps intermédiaire entre K et E, le théorème entraîne que l'extension de corps $L \hookrightarrow E$ est encore normale.

Corollaire 4.1.1.
Soit $K \hookrightarrow E$ une extension finie de corps et soit Ω un corps algébriquement clos contenant K. L'extension $K \hookrightarrow E$ est normale $\Leftrightarrow$ tous les K-morphismes de E dans Ω ont la même image. En particulier, si Ω est un corps algébriquement clos contenant E, l'extension finie $K \hookrightarrow E$ est normale si, et seulement si, tous les K-morphismes de E dans Ω sont d'image E.

Preuve :
$(\Rightarrow)$
Si $K \hookrightarrow E$ est normale, d'après le théorème précédent E est un corps de décomposition d'un polynôme $P \in K[X]$. D'autre part le corps $R = K(\{x_i \ : \ x_i$ est une racine de $P\})$ est un corps de décomposition de P sur K, d'après le théorème 2.3.1 E et R sont K-isomorphes.
Soit σ un K-morphisme de E dans Ω, alors σ est injectif car est un morphisme de corps non nulle ($car \ \forall k \in K \ : \ \sigma(k) = k$). Alors $\sigma(E) \cong E \cong R$, ce qui implique que $\sigma(E)$ est une extension de K ($car \ K \subseteq \sigma(E)$) engendré par les racines de P dans Ω. D'où image de E ne dépend pas du K-morphismes de E dans Ω.
$(\Leftarrow)$
Supposons que tous les K-morphismes de E dans Ω ont la même image, que l'on note $E' \subseteq \Omega$. Comme E est une extension finie, alors elle est algébrique sur K. Soit $P \in K[X]$ un polynôme irréductible a une racine $x \in E$. Montrons que P est scindé dans E :
Comme tout les racines de P sont dans Ω car $K \subseteq \Omega$, alors soit y une racine de P dans Ω on a :
les corps $K(x) \subseteq E$ et $K(y) \subseteq \Omega$ d'après le théorème 3.1.3 sont K-isomorphes. Posons σ un K-isomorphisme de $K(x)$ dans $K(y)$, on a $\sigma(K(x)) = K(y) \subseteq \Omega$, donc on peut considéré que Ω une extension de $K(x)$. Comme E est extension algébrique de $K(x)$ alors on peut prolonger σ d'après le corollaire 3.3.1 en un $K(x)$-morphisme $\tilde{\sigma} : E \longrightarrow \Omega$ dont l'image est E' ($\tilde{\sigma}(E) = E'$) donc $K(x) \subseteq E'$ et $K(y) \subseteq E'$. D'où $P \in K[X]$ est scindé dans E', donc dans E puisque ces deux extensions de K sont K-isomorphes. □

4.2 Polynômes séparables

Définition 4.2.1.
*On dit qu'un polynôme $P \in K[X]$ est **séparable** s'il n'a aucun racine multiple dans son corps de décomposition. Dans le cas contraire, on dit que P est **inséparable**.*

Exemple 4.2.1.
Soit $P(X) = X^5 - 1 \in \mathbb{R}[X]$, on a $\mathbb{C}$ est un corps de décomposition de P, et tel que ses racines dans $\mathbb{C}$ sont $z_i = e^{\frac{2k\pi i}{5}}$ $0 \leqslant i \leqslant 4$, deux à deux disjoints, alors P est séparable sur $\mathbb{R}$.

Lemme 4.2.1.
Une polynôme $P \in K[X]$ est séparable si, et seulement si, P et $P^{'}$ sont premier entre eux.

Preuve :
Le pgcd(P,P$^{'}$) est le même dans $K[X]$ ou dans $E[X]$ pour tout extension E de K, Si E est un corps de décomposition de P, donc :

$$P \text{ est séparable} \Leftrightarrow \text{les racines sont tous simple} \Leftrightarrow pgcd(P, P^{'}) = 1$$ □

Théorème 4.2.1.
Soit K un corps.
Si $Car(K) = 0$, alors pour tout polynôme irréductible $P \in K[X]$ est séparable.

Preuve :
Si P un polynôme irréductible $K[X]$, alors P n'est pas constant, donc $P^{'} \neq 0$, en effet :
Écrivons :

$$P(X) = \sum_{i=0}^{n} a_i X^i \text{ tel que } a_n \neq 0$$

On a :

$$P^{'}(X) = \sum_{i=1}^{n} i a_i X^i$$

Alors, si $Car(K) = 0$: alors $a_n \neq 0 \Rightarrow n a_n \neq 0 \Rightarrow P^{'}(X) \neq 0$.
De plus :

$$deg(P^{'}) < deg(P) \Rightarrow P \nmid P^{'}, \text{ dans } K[X]$$

L'irréductibilité du polynôme P implique alors : $pgcd(P, P^{'}) = 1$. D'après le lemme 4.2.1, P est séparable sur K. □

4.3 Extensions séparables

Définition 4.3.1.
Soit $K \hookrightarrow E$ une extension de corps.
*On dit qu'un élément de E est **séparable** sur K s'il algébrique sur K et que son polynôme minimal sur K est **séparable**.*
*L'extension $K \hookrightarrow E$ est **séparable** si tout élément de E est séparable sur K.*

Exemple 4.3.1.
$\mathbb{C}$ est une extension séparable de $\mathbb{R}$, en effet :
$\mathbb{C}$ est une extension algébrique de $\mathbb{R}$ et pour tout $z \in \mathbb{C}$, on a $z = a + ib$ avec $a, b \in \mathbb{R}$, alors :
- Si $b = 0$ le polynôme minimal de z dans $\mathbb{R}$ est :

$$P(X) = X - z.$$

donc P est séparable dans $\mathbb{C}$.
- Si $b \neq 0$ le polynôme minimal de z dans $\mathbb{R}$ est :

$$P(X) = X^2 - 2aX + a^2 + b^2 = (X - z)(X - \bar{z}).$$

donc P est séparable dans $\mathbb{C}$.

Degré de séparabilité

Notation 4.3.1.
Soient $K \hookrightarrow E$ une extension finie et Ω une clôture algébrique de K.
On note par $Hom_K(E, \Omega)$ l'ensemble de tous les K-morphismes de E dans Ω.

Proposition 4.3.1.
Soient $K \hookrightarrow E$ une extension finie de degré n et Ω une clôture algébrique de K. On a :

$$1 \leqslant Card(Hom_K(E, \Omega)) \leqslant n.$$

Preuve :
La première inégalité est une conséquence du corollaire 3.3.1.
Montrons la deuxième inégalité :
Soit $\{e_i\}_{i=1}^n$ une base pour le K-espace vectoriel E.
Supposons qu'il existe $\sigma_1, ..., \sigma_n, \sigma_{n+1} \in Hom_K(E, \Omega)$ sont deux à deux distinct. Cette famille des éléments de $Hom_K(E, \Omega)$ est libre sur Ω, en effet : Supposons par l'absurde que la famille est liée, et notons r son rang. Quitte à renuméroter les σ_i, on peut supposer que la famille $(\sigma_i)_{i=1}^r$ est libre. Il existe donc une unique famille de $(\lambda_i)_{i=1}^r \subseteq \Omega$ tel que :

$$\sigma_{r+1} = \sum_{i=1}^{r} \lambda_i \sigma_i$$

Par ailleurs, il existe nécessairement un i_0 tel que l'élément λ_{i_0} soit non nul.
Soit $y \in K$ non nul, d'après l'égalité précédente, pour tout $x \in K$, on a :

$$\sigma_{r+1}(xy) = \sum_{i=1}^{r} \lambda_i \sigma_i(xy)$$

Ce qu'on peut réécrire sous la forme, en prenant en compte le fait que les σ_i sont des morphismes d'anneaux :

$$\sigma_{r+1}(x) = \sum_{i=1}^{r} \lambda_i \frac{\sigma_i(y)}{\sigma_{r+1}(y)} \sigma_i(x)$$

Par unicité des λ_i, cela implique que pour tout $1 \leq i \leq r$:

$$\lambda_i = \lambda_i \frac{\sigma_i(y)}{\sigma_{r+1}(y)}$$

En particulier, puisque λ_{i_0} est non nul, cela implique que $\sigma_{r+1}(y) = \sigma_{i_0}(y)$, pour tout y non nul dans K. C'est absurde, puisque les σ_i sont supposés deux à deux distincts. Ce qui conclut.
Soit la matrice $M \in \mathcal{M}_{n,n+1}(\Omega)$ définit par :

$$M = \begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_{n+1}(e_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_n) & \cdots & \sigma_{n+1}(e_n) \end{pmatrix}$$

On a $rg(M) \leqslant n$.
Soient $C_1, ..., C_{n+1}$ les colonnes de M, d'après le $rg(M)$, ils sont liées.
Donc il existe $\lambda_1, ..., \lambda_{n+1} \in \Omega$, non tous nul, tel que :

$$\sum_{i=1}^{n+1} \lambda_i C_i = 0$$

donc $\forall j = 1, ..., n$, on a :

$$\sum_{i=1}^{n+1} \lambda_i \sigma_i(e_j) = 0 \Rightarrow (\sum_{i=1}^{n+1} \lambda_i \sigma_i)(e_j) = 0$$

Ce qui équivalent que $e_j = 0$ car les σ_i ne sont pas liées par la supposition. Ce qui absurde, car $e_j = 0$ est élément de la base.
D'où $\sigma_1, ..., \sigma_n, \sigma_{n+1}$ sont liées dans $Hom_K(E, \Omega)$.
finalement :

$$Card(Hom_K(E, \Omega)) \leqslant n.$$

□

Proposition 4.3.2.
Soient $K \hookrightarrow E$ une extension finie de degré n et Ω une clôture algébrique de K. On pose inclusion $\sigma : K \hookrightarrow \Omega$, on a :

$$Card(Hom_K(E, \Omega)) \text{ est indépendantde } \sigma \text{ et } \Omega.$$

Preuve :
Soit Ω' une clôture algébrique de K, alors Ω et Ω' sont K-isomorphes. Soit $\theta : \Omega' \longrightarrow \Omega$ un isomorphisme qui prolonge σ à Ω'.
Si $\phi \in Hom_K(E, \Omega)$, alors $\theta^{-1} \circ \phi \in Hom_K(E, \Omega')$, donc on peut définit l'application suivante :

$$\begin{array}{rccc} f & : & Hom_K(E, \Omega) & \to & Hom_K(E, \Omega') \\ & & \phi & \mapsto & \theta^{-1} \circ \phi \end{array}$$

cette application est bijective, en effet :
Posons l'application suivante :

$$\begin{array}{rccc} g & : & Hom_K(E, \Omega') & \to & Hom_K(E, \Omega) \\ & & \phi & \mapsto & \theta \circ \phi \end{array}$$

on a :

$$f \circ g = id_{Hom_K(E,\Omega')} \quad et \quad g \circ f = id_{Hom_K(E,\Omega)}$$

D'où

$$Card(Hom_K(E,\Omega)) = Card(Hom_K(E,\Omega'))$$

□

Définition 4.3.2.
Soient $K \hookrightarrow E$ une extension de corps de degré fini et Ω une clôture algébrique de K. On appelle le ***degré de séparabilité*** *de $K \hookrightarrow E$ est $Card(Hom_K(E,\Omega))$.*
Le degré de séparabilité de $K \hookrightarrow E$ sera noté $[E:K]_s$.

Exemple 4.3.2.
Soit $\mathbb{R} \hookrightarrow \mathbb{C}$:
Comme $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$, on a $Card(Hom_{\mathbb{R}}(\mathbb{C},\mathbb{C})) = 2$, en effet :
Soient $z \in \mathbb{C}$ et $\sigma \in Hom_{\mathbb{R}}(\mathbb{C},\mathbb{C})$, on a :

$$\sigma(z) = \sigma(a+ib) = \sigma(a) + \sigma(b)\sigma(i) = a + b\sigma(i).$$

De plus, on a :

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1 \Rightarrow \sigma(i) = \pm i$$

alors :

$$\sigma(z) = a \pm ib = \begin{cases} z \\ \bar{z} \end{cases}$$

Finalement les seuls $\mathbb{R}$-morphismes sont l'identité et le conjugué.
Alors le degré de séparabilité de cette extension est 2.

Théorème 4.3.1.
Soient $K \hookrightarrow L$ et $L \hookrightarrow E$ des extensions finies de corps. On a :

$$[E:K]_s = [E:L]_s[L:K]_s.$$

Preuve :
Soit Ω une clôture algébrique de E, puisque $K \hookrightarrow L$ et $L \hookrightarrow E$ sont finie, donc elles sont algébriques d'après le théorème 2.5.1. Alors Ω est aussi une clôture algébrique de L et de K.
Soit :

$$Hom_K(L,\Omega) = \{\sigma_i \ : \ i \in I\}$$

avec I l'ensemble d'indice tel que $Card(I) = [L:K]_s$.
Soit $i \in I$, considérons le morphisme $\sigma_i : L \longrightarrow \Omega$, d'après la proposition 4.3.2, on a le cardinal de l'ensemble des prolongements de σ_i à E est indépendant de i et vaut $[E:L]_s$. On peut donc noter $(\tau_{ij})_{j\in J}$ cet ensemble, avec $Card(J) = [E:L]_s$.
Alors on obtient $Hom_K(E,\Omega) = \{\tau_{ij} \ / \ (i,j) \in I \times J\}$, tel que :

$$\begin{aligned}[E:K]_s &= Card(Hom_K(E,\Omega)) = Card(I \times J) = Card(I)Card(J) \\ &= [L:K]_s[E:L]_s\end{aligned}$$

Ce qui achève le preuve. □

Théorème 4.3.2.
Soit $K \hookrightarrow E$ une extension finie de corps. On a :

$$[E : K]_s = [E : K] \Leftrightarrow L'extension\ K \hookrightarrow E\ est\ séparable.$$

Preuve :
($\Leftarrow$) Supposons que $K \hookrightarrow E$ est séparable :
Comme $K \hookrightarrow E$ est finie donc $E = K(a_1, ..., a_n)$ avec les $a_i \in E$, par conséquence les a_i sont séparables sur K ce qui implique que chaque a_i est séparable sur $K_{i-1} = K(a_1, ..., a_{i-1})$ (le polynôme minimal a_i sur ce corps divise son polynôme minimal sur K, donc est aussi séparable). Alors le nombre des racines de polynôme minimal de a_i sur K_{i-1} est égale à son degré. Or, d'après le théorème 3.3.1 :

$$[K_{i-1}(a_i) : K_{i-1}]_s = [K_{i-1}(a_i) : K_{i-1}]$$

Donc :
à partir de théorème degré, on a :

$$[E : K] = \prod_{i=1}^{n} [K_{i-1}(a_i) : K_{i-1}]$$

à partir de théorème 4.3.1, on a :

$$[E : K]_s = \prod_{i=1}^{n} [K_{i-1}(a_i) : K_{i-1}]_s$$

D'où :

$$[E : K]_s = [E : K]$$

($\Rightarrow$) Supposons $[E : K]_s = [E : K]$:
Pour tout $x \in E$, on a : $[E : K(x)]_s \leqslant [E : K(x)]$ et $[K(x) : K]_s \leqslant [K(x) : K]$, comme $[E : K]_s = [E : K(x)]_s[K(x) : K]_s$ et $[E : K] = [E : K(x)][K(x) : K]$, et d'après l'hypothèse, on a :

$$[K(x) : K]_s = [K(x) : K] \quad et \quad [E : K(x)]_s = [E : K(x)].$$

La discussion précédente dit alors que x est séparable sur K, car le degré de polynôme minimal de x sur K est égale à le nombre de ses racines. Donc l'extension $K \hookrightarrow E$ est séparable. □

Théorème 4.3.3.
Soient $K \hookrightarrow L$ et $L \hookrightarrow E$ des extensions de corps. Si un élément $x \in E$ est séparable sur L et que L est une extension séparable de K, alors x est séparable sur K.

Preuve :
Si un élément $x \in E$ est séparable sur L, donc il est algébrique sur L. Soit $P \in L[X]$ son polynôme minimal sur L. Écrivons :

$$P(X) = \sum_{i=0}^{n} a_i X^i \ avec\ a_i \in L$$

Posons $M = K(a_0, ..., a_n) \subseteq L$, si extension $K \hookrightarrow L$ est séparable, donc M est une extension finie de K car les a_i sont algébrique sur K et séparable. D'après le théorème 4.3.2 on a : $[M : K]_s = [M : K]$. Comme x est séparable sur M (car son polynôme minimal sur M est P qu'est séparable), d'après le théorème 3.3.1, $[M(x) : M]_s = deg(P) = [M(x) : M]$ donc l'extension $M \hookrightarrow M(x)$ est séparable et est finie car x est algébrique sur M. Le théorème 4.3.1 entraîne que $[M(x) : K]_s = [M(x) : K]$. L'extension $K \hookrightarrow M(x)$ est finie alors, d'après le théorème 4.3.2, elle est séparable, donc x est séparable sur K. □

Corollaire 4.3.1.
$K \hookrightarrow E$ est une extension séparable si, et seulement si, les extensions $K \hookrightarrow L$ et $L \hookrightarrow E$ le sont.

4.4 Théorème de l'élément primitif

Définition 4.4.1.
*On appelle **élément primitif** d'une extension finie E de K, tout élément $a \in E$ tel que :*

$$E = K(a).$$

Exemple 4.4.1.
$\sqrt{2} + \sqrt{3}$ est un élément primitive de extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ de $\mathbb{Q}$, la preuve voir exemple 2.3.1.

Théorème 4.4.1. Théorème de l'élément primitif
Toute extension $K \hookrightarrow E$ séparable et de degré finie possédé un élément primitif.

Preuve :
On va distinguer deux cas :
1^{er} cas : K est fini
E l'est aussi, donc le groupe $(U(E), .)$ est cyclique. Si $z \in U(E)$ qui engendre $U(E)$, donc il engendre aussi E, car E est un corps. Alors :

$$E = K(z).$$

$2^{éme}$ cas : K est infini
Posons $[E : K] = n$.
Soit Ω une clôture algébrique de K, comme E est séparable sur K, d'après théorème 4.3.2 on a $[E : K]_s = n = Card(Hom_K(E, \Omega))$, donc soient $\sigma_1, ..., \sigma_n$ les éléments de $Hom_K(E, \Omega)$. Posons pour tout $i, j \in \{1, ..., n\}$ avec $i \neq j$:

$$E_{i,j} = \{x \in E \ : \ \sigma_i(x) = \sigma_j(x)\}$$

Les $E_{i,j}$ sont sous-corps de E contient K, en effet :
- $E_{i,j} \neq \emptyset$, car :

$$\forall x \in K \subseteq E, \sigma_i(x) = \sigma_j(x) = x$$

- Soient $x, y \in E_{i,j}$ on a $x - y \in E_{i,j}$, en effet :

$$\sigma_i(x) = \sigma_j(x) \text{ et } \sigma_i(y) = \sigma_j(y) \Rightarrow \sigma_i(x - y) = \sigma_j(x - y)$$

- Soient $x, y \in E_{i,j}$ avec $y \neq 0$ on a $xy^{-1} \in E_{i,j}$, en effet : comme $\sigma_i(y), \sigma_j(y) \in \Omega$, alors ils sont inversibles car σ_i, σ_j sont des morphismes de corps injectif et $y \neq 0$, ce qui implique $\sigma_i(y^{-1}) = \sigma_j(y^{-1})$, donc :

$$\sigma_i(xy^{-1}) = \sigma_j(xy^{-1})$$

Alors, les $E_{i,j}$ sont des K-sous-espaces vectoriels de E et ils sont distincts de E car $\sigma_i \neq \sigma_j$ (car $i \neq j$).
pour continue la preuve, on va utiliser le lemme suivant :

Lemme 4.4.1.
Soient E un K-espace vectoriel, $n \in \mathbb{N}^*$ et $E_1, ..., E_n$ des sous-espaces de E distincts de E. Si $Card(K) \geqslant n$, On a :

$$E \nsubseteq \bigcup_{i=1}^{n} E_i$$

Preuve :
On va procède par la récurrence sur n :
Si $n = 1$, d'après l'hypothèse de lemme E_1 est distinct de E, alors $E \nsubseteq E_1$.
Supposons que le lemme est vrai pour $n-1$, et montrons-le pour n :
On va montrer par l'absurde :
Posons

$$F_i = \bigcup_{j=1}^{i} E_j$$

pour tout $i = 1, ..., n$.
Supposons que $Card(K) \geqslant n$ et $E \subseteq F_n$, alors $E = F_n = F_{n-1} \cup E_n$.
Comme $Card(K) \geqslant n \geqslant n-1$, d'après l'hypothèse de récurrence, on a $E \neq F_{n-1}$ (car $E \nsubseteq F_{n-1}$), alors il existe $x \in E_n - F_{n-1}$. Fixons $y \in E - E_n$, soit l'application suivante :

$$\begin{array}{rccc} u & : & K & \to & E \\ & & \lambda & \mapsto & \lambda x + y \end{array}$$

Comme $x \in E_n$ et $y \notin E_n$, on a : $u(\lambda) \notin E_n$, pour tout $\lambda \in K$, donc $u(K) \subseteq F_{n-1}$ car $E = F_{n-1} \cup E_n$. Puisque $Card(K) \geqslant n$, alors il existe $k \in \{1, ..., n-1\}$ et $\lambda, \mu \in K$ vérifiant :

$$\lambda \neq \mu \text{ et } u(\lambda), u(\mu) \in E_k$$

alors :

$$x = (\lambda - \mu)^{-1}(u(\lambda) - u(\mu)) \in E_k \subseteq F_{n-1}$$

contradiction avec $x \in E_n - F_{n-1}$. Alors :

$$E \nsubseteq F_n$$

Le lemme a été démonter.

□

D'après le lemme on a :

$$\exists x \in E \text{ tq } x \notin \bigcup_{i=1}^{n} \bigcup_{\substack{j=1 \\ j \neq i}}^{n} E_{i,j}$$

autrement dit, pour tout $i, j \in \{1, ..., n\}^2$ *avec* $i \neq j$ *on a :* $\sigma_i(x) \neq \sigma_j(x)$.
Alors pour tout $i \in \{1, ..., n\}$, *on a la restriction de* σ_i *sur* $K(x)$ *appartient à* $Hom_K(K(x), \Omega)$, *par la suite* $n \leqslant Card(Hom_K(K(x), \Omega))$. *D'après le théorème 4.3.2 :*

$$n \leqslant [K(x) : K] \leqslant [E : K] = n.$$

Finalement : $[K(x) : K] = [E : K]$ *ce qui implique que :*

$$E = K(x).$$

□

5

Extensions galoisiennes - Théorie de Galois

La Théorie de Galois est l'étude des extensions de corps $K \hookrightarrow E$ au moyen du groupes des K-automorphismes de E. Cette méthode, introduite par le mathématicien français Evariste Galois (1811-1832).

5.1 Groupe de Galois d'une extension de corps

Définition 5.1.1.
*Étant donnée une extension E d'un corps K, on dit qu'un automorphisme σ de corps E est un K-**automorphisme** de E si $\sigma_{|K} = id_K$.*

Remarque 5.1.1.
L'ensemble $Aut_K(E)$ des K-automorphismes de E est un sous groupe de groupe $(Aut(E), \circ)$.

Définition 5.1.2.
*On appelle **groupe de Galois** d'une extension de corps $K \hookrightarrow E$, le groupe $Aut_K(E)$. On le note par $Gal(E/K)$.*

Exemple 5.1.1.
1. Soit l'extension $\mathbb{R} \hookrightarrow \mathbb{C}$:
D'après l'exemple 4.3.2 les seuls $\mathbb{R}$-automorphismes de $\mathbb{C}$ sont l'identité et conjugué.
2. Soit extension $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt[3]{2})$:
on a :

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \ : \ a, b, c \in \mathbb{Q}\}$$

Soient : $\sigma \in Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ et $\alpha \in \mathbb{Q}(\sqrt[3]{2})$:
Écrivons : $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ avec $a, b, c \in \mathbb{Q}$
on a :

$$\sigma(\alpha) = \sigma(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a + b\sigma(\sqrt[3]{2}) + c\sigma(\sqrt[3]{4})$$

Or : $\sigma(\sqrt[3]{2})^3 = \sigma(\sqrt[3]{2}^3) = \sigma(2) = 2$
alors : $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$

$$\sigma = id_{\mathbb{Q}(\sqrt[3]{2})}$$

l'identité de $\mathbb{Q}(\sqrt[3]{2})$ est le seul $\mathbb{Q}$-automorphisme de $\mathbb{Q}(\sqrt[3]{2})$.

Théorème 5.1.1.
Soit $K \hookrightarrow E$ une extension finie de corps. On a :

$$Card(Gal(E/K)) \leqslant [E : K]_s$$

En particulier, cette inégalité est une égalité si, et seulement si, l'extension $K \hookrightarrow E$ est normale.

Preuve :
Soient Ω une clôture algébrique de K et $j \in Hom_K(E, \Omega)$. Posons l'application f définit par :

$$\begin{array}{rccc} f & : & Aut_K(E) & \to & Hom_K(E,\Omega) \\ & & \sigma & \mapsto & j \circ \sigma \end{array}$$

cette application est bien définie de plus il est injective, en effet :
Soient $\sigma, \gamma \in Aut_K(E)$:

$$f(\sigma) = f(\gamma) \Rightarrow j \circ \sigma = j \circ \gamma$$

alors :

$$\forall x \in E \text{ on a } : \ j(\sigma(x)) = j(\gamma(x))$$

et comme j est injective car j est un morphisme de corps non nul ce qui implique :

$$\forall x \in E \text{ on a } : \ \sigma(x) = \gamma(x)$$

donc :

$$f(\sigma) = f(\gamma) \Rightarrow \sigma = \gamma$$

Finalement :

$$Card(Aut_K(E)) \leqslant Card(Hom_K(E,\Omega)) \Rightarrow Card(Gal(E/K)) \leqslant [E : K]_s$$

Maintenant, on va montrer que :
$Card(Gal(E/K)) = [E : K]_s$ si, et seulement si, l'extension $K \hookrightarrow E$ est normale.
Le groupe $Gal(E/K)$ agit à droit sur l'ensemble $Hom_K(E, \Omega)$ par la formule :

$$\forall (g, \sigma) \in Gal(E/K) \times Hom_K(E,\Omega) \ : \ \sigma.g = \sigma \circ g$$

cette action est libre, car :

$$\sigma \circ g = \sigma \Rightarrow g = Id_E \ , \ car \ \sigma \ est \ injective.$$

Alors, pour montrer :
$Card(Gal(E/K)) = [E : K]_s$ si, et seulement si, $K \hookrightarrow E$ est normale , il suffit de montrer que :
l'action de groupe $Gal(E/K)$ sur l'ensemble $Hom_K(E, \Omega)$ est transitive si, et seulement si, tous les morphismes de $Hom_K(E, \Omega)$ ont même image.

- Supposons que l'action de groupe $Gal(E/K)$ sur l'ensemble $Hom_K(E, \Omega)$ est transitive, alors :

$$\forall \sigma, \gamma \in Hom_K(E,\Omega), \exists g \in Gal(E/K) \quad : \quad \sigma = \gamma \circ g$$

donc :

$$\sigma(E) = \gamma(g(E)) = \gamma(E) \text{ car } g \text{ est un automorphisme de } E.$$

Donc tous les morphismes de $Hom_K(E,\Omega)$ ont même image.
- Inversement, supposons que tous les morphismes de $Hom_K(E,\Omega)$ ont même image :
Soient $\sigma, \sigma' \in Hom_K(E,\Omega)$, on a $\sigma(E) = \sigma'(E)$.
L'application $g : E \longrightarrow E$ définie par $g = (\sigma_{E\to\sigma(E)})^{-1} \circ \sigma'$ est un K-automorphisme de E (facile à vérifie) tel que $\sigma' = \sigma \circ g$, donc l'action de groupe $Gal(E/K)$ sur l'ensemble $Hom_K(E,\Omega)$ est transitive.
Finalement, d'après le corollaire 4.1.1 et la remarque 1.9.1 on a :

$$Card(Gal(E/K)) = [E:K]_s \Leftrightarrow L'extension\ K \hookrightarrow E\ est\ normale$$

□

5.2 Extensions galoisiennes

Définition 5.2.1.
Une extension de corps $K \hookrightarrow E$ est dite ***galoisienne*** *si elle est séparable et normale.*

Remarque 5.2.1.
Si $K \hookrightarrow E$ est une extension finie alors :

$$K \hookrightarrow E \text{ est galoisienne} \Leftrightarrow Card(Gal(E/K)) = [E:K]$$

Remarque 5.2.2.
Si $K \hookrightarrow E$ est une extension de corps finie, galoisienne et que M est un corps intermédiaire entre K et E, l'extension $M \hookrightarrow E$ est encore galoisienne (remarque 4.1.1 et corollaire 4.3.1) et le groupe $Gal(E/M)$ est un sous-groupe de $Gal(E/K)$:

$$Gal(E/M) = \{g \in Gal(E/K) \ : \ g_{|M} = Id_M\}$$

En revanche, l'extension $K \hookrightarrow M$ n'est pas nécessairement galoisienne.

Proposition 5.2.1.
Soit $K \hookrightarrow E$ Une extension finie. Les propriétés suivantes sont équivalentes :
(i) $K \hookrightarrow E$ est galoisienne.
(ii) E est le corps de décomposition sur K d'un polynôme séparable.

Preuve :
$(ii) \Rightarrow (i)$
Si E est le corps de décomposition d'un polynôme séparable $Q \in K[X]$, l'extension E est isomorphe à le corps engendré par des éléments séparables (les racines de Q), donc E est une extension séparable de K. Elle est aussi normale par le théorème 4.1.1, donc elle est galoisienne.
$(i) \Rightarrow (ii)$
Supposons que $K \hookrightarrow E$ est galoisienne :
Comme $K \hookrightarrow E$ est finie, alors E est engendré par un nombre finie de ces éléments.
On écrit $E = K(x_1, ..., x_n)$ et l'on note $P_i \in K[X]$ le polynôme minimal de x_i sur K. Comme

$K \hookrightarrow E$ est normale (resp. séparable), chaque P_i est scindé (resp. à racines simples) dans E, donc aussi :

$$Q := ppcm(P_1, ..., P_n)$$

Comme E est engendré sur K par les x_i, qui sont des racines de Q, le corps E est un corps de décomposition du polynôme séparable $Q \in K[X]$ (car est un corps minimal pour cette décomposition).
Ce qui achève le preuve. □

Proposition 5.2.2.
Soit $K \hookrightarrow E$ une extension finie et normale de corps et soit $P \in K[X]$ un polynôme séparable scindé dans E. L'action de $Gal(E/K)$ sur l'ensemble des racines de P dans E est transitive si, et seulement si, P est irréductible dans $K[X]$.

Preuve :
Voir la démonstration de cette proposition dans l'ouvrage :
Olivier Debarre : Algèbre 2, ENS, 2012-2013, page 29. □

5.3 Correspondance de Galois

Avant d'expliquer la correspondance de Galois qu'est un dictionnaire entre théorie des corps et théorie des groupes, on va montrer le lemme d'Artin qui permet de démontrer la moitie de la correspondance de Galois, pour cela on va fixé des notations qu'on va utiliser dans cette section :
Soit E un corps, pour tout G sous-groupe des K-automorphismes de E, on note :
*$E^G := \{x \in E \ : \ \forall \sigma \in G, \sigma(x) = x\}$ le corps d'**invariant** de G dans E, qui est un sous corps de E en effet :*
$E^G \neq \emptyset$, car pour tout $\sigma \in G$, on a $\sigma(0) = 0$ et $\sigma(1) = 1$, alors $0, 1 \in E^G$.
Soient $x, y \in E^G$, on a pour tout $\sigma \in G$ les relations suivantes :
$\sigma(x - y) = \sigma(x) - \sigma(y) = x - y$
pour $y \neq 0$ on a :
$\sigma(xy^{-1}) = \sigma(x)\sigma(y^{-1}) = \sigma(x)\sigma(y)^{-1} = xy^{-1}$
alors $x - y, xy^{-1} \in E^G$.

Lemme 5.3.1. Lemme d'Artin
Soient $K \hookrightarrow E$ une extension finie et G un sous-groupe de $Gal(E/K)$. Alors l'extension $E^G \hookrightarrow E$ est finie galoisienne de groupe de Galois

$$Gal(E/E^G) = G$$

Ainsi :

$$[E : E^G] = Card(Gal(E/E^G)) = Card(G).$$

Preuve :
Pour tout $g \in G \subseteq Aut_K(E)$ on a $g \in Aut_{E^G}(E)$ alors :

$$G \subseteq Gal(E/E^G)$$

donc $Card(G) \leq Card(Gal(E/E^G))$*, de plus* E *est finie sur* K *alors* E *est finie sur* $E^G \supseteq K$*, d'après le théorème 5.1.1* $Card(Gal(E/E^G)) \leq [E : E^G]$*. Ainsi :*

$$Card(G) \leq Card(Gal(E/E^G)) \leq [E : E^G]$$

Alors pour montrer $Gal(E/E^G) = G$*, il suffit de montrer que*

$$[E : E^G] \leq Card(G)$$

Par l'absurde :
Supposons que $[E : E^G] > Card(G)$*. Posons* $n = 1 + Card(G)$ *et soient* $a_1, ..., a_n$ *des éléments de* E *linéairement indépendants. Soit le système suivant :*

$$(S) \ : \ \sum_{i=1}^{n} \sigma(a_i)x_i = 0, \quad \sigma \in G$$

est un système de $Card(G)$ *équations et* n *inconnues.*
Or, $n > Card(G)$ *et comme* $a_1, ..., a_n$ *sont des éléments de* E *linéairement indépendants, alors pour tout* $\sigma \in G$ *les éléments* $\sigma(a_1), ..., \sigma(a_n)$ *sont des éléments de* E *aussi linéairement indépendants, donc le rang de la matrice associe au système est* $Card(G)$*, alors ce système possède une infinité de solutions non nulles* $(x_1, ..., x_n)$*.*
On choisit une qui a le nombre des termes x_i *non nuls* m *est minimal. Quitte à renuméroter, on peut supposer qu'il s'agit* $x_1, ..., x_m$*. Par linéarité de la solution, on peut aussi supposer* $x_m = 1$*, d'où les relations :*

$$\sum_{i=1}^{m-1} \sigma(a_i)x_i + \sigma(a_m) = 0, \quad \sigma \in G \qquad (1)$$

Soit $\tau \in G$*, comme* $\tau^{-1} \circ \sigma \in G$ *pour tout* $\sigma \in G$*, alors en appliquant* τ *à les relations précédentes pour* $\tau^{-1} \circ \sigma \in G$*. On obtient :*

$$\sum_{i=1}^{m-1} \sigma(a_i)\tau(x_i) + \sigma(a_m) = 0, \quad \sigma \in G \qquad (2)$$

D'où, si l'on soustrait le système des relations (1) de (2), on trouve :

$$\sum_{i=1}^{m-1} \sigma(a_i)(\tau(x_i) - x_i) = 0 \qquad \sigma \in G$$

alors : $(\tau(x_1) - x_1, ..., \tau(x_{m-1}) - x_{m-1}, 0, ..., 0)$ *est une solution de système* (S)*, d'après la minimalité de* m *on a cette dernière est une solution nulle, autrement dit :*

$$\text{pour tout } i = 1, ..., m-1 \text{ et pour } \tau \in G \text{ on a } : \ \tau(x_i) = x_i$$

comme, pour tout $\tau \in G$ *on a :* $\sum_{i=1}^{m} \tau(a_i)x_i = 0$*, alors* $\sum_{i=1}^{m} \tau(a_i)x_i = \sum_{i=1}^{m} \tau(a_i x_i) = \tau(\sum_{i=1}^{m} a_i x_i) = 0$*, donc* $\sum_{i=1}^{m} a_i x_i = 0$ *et comme les* $x_i \in E^G$ *ne sont pas nulle pour les* $i = 1, ..., m$ *ce qui implique que les* a_i *sont des éléments de* E *linéairement dépendants, contradiction.*
D'où :

$$[E : E^G] \leq Card(G)$$

Finalement

$$[E : E^G] = Card(G) = Card(Gal(E/E^G))$$

ce qui implique que $E^G \hookrightarrow E$ *est finie galoisienne de groupe de Galois* G *(car* $G \subseteq Gal(E/E^G)$*).* □

Théorème 5.3.1. (Correspondance de Galois)
Soit $K \hookrightarrow E$ *une extension finie galoisienne de corps, de groupe de Galois* $G := Gal(E/K)$.
1. Il existe des bijections inverses l'une de l'autre :

$$\begin{array}{rccc} \Phi & : & \{sous-groupe\ de\ G\} & \to & \{extensions\ intermédiaires\ entre\ K\ et\ E\} \\ & & H & \mapsto & E^H \end{array}$$

$$\begin{array}{rccc} \Psi & : & \{extensions\ intermédiaires\ entre\ K\ et\ E\} & \to & \{sous-groupe\ de\ G\} \\ & & M & \mapsto & Gal(E/M) \end{array}$$

2. Si H *est un sous-groupe de* G*, l'extension* $K \hookrightarrow E^H$ *est galoisienne si et seulement si* H *est distingué dans* G*. Son groupe de Galois est alors le groupe quotient* G/H.

Preuve :
1. montrons que :

$$\Phi \circ \Psi = Id_{\{extensions\ intermédiaires\ entre\ K\ et\ E\}} \quad et \quad \Psi \circ \Phi = Id_{\{sous-groupe\ de\ G\}}.$$

Soit $M \in \{extensions\ intermédiaires\ entre\ K\ et\ E\}$*, alors l'extension* $M \hookrightarrow E$ *est finie galoisienne.*
Pour continue on va appliquer le lemme suivant :

Lemme 5.3.2.
Soient $K \hookrightarrow E$ *une extension finie galoisienne de corps et* G *son groupe de Galois. On a :*

$$K = E^G$$

Preuve :
Pour tout $x \in K$ *et pour tout* $g \in G$*, on a* $g(x) = x$*, alors* $K \subseteq E^G$.
Soient $x \in E^G$ *et* $P \in K[X]$ *son polynôme minimal sur* K *qui est séparable car* $K \hookrightarrow E$ *est séparable. Comme l'extension* $K \hookrightarrow E$ *est normale donc* P *est scindé dans* E*, soit* y *une racine de* P *dans* E*. Comme* P *est irréductible dans* $K[X]$*, d'après la proposition 5.2.2 il existe* $g \in G$ *tel que* $y = g(x)$*. Comme* $x \in E^G$*, on a* $y = x$*. Donc* P *n'a qu'une seule racine c'est à dire il est de degré* 1 *et* $x \in K$.
Ce qui achève le preuve. □

En appliquant ce lemme à l'extension finie galoisienne $M \hookrightarrow E$*, on obtient* $M = E^{Gal(E/M)}$*, c'est-à-dire* $M = \Phi(\Psi(M))$*. L'autre égalité* $H = \Psi(\Phi(H)) = Gal(E/E^H)$ *résulte du Lemme d'Artin ci-dessus. Ceci montre le point 1) du théorème.*

2. Soient H *un sous-groupe de* G *et* $g \in G$*. L'extension intermédiaire* $g(E^H)$ *(car* g *est un* K*-automorphisme de corps* E *et* E^H *est un corps intermédiaire entre* K *et* E*) correspond au sous-groupe* gHg^{-1} *de* G*, car* $g(E^H) = E^{gHg^{-1}}$*, en effet :*

D'une part, pour tout $y \in g(E^H)$, il existe $x \in E^H$ tel que $y = g(x)$. Or pour tout $h \in H$, on a :

$$[ghg^{-1}](y) = [ghg^{-1}](g(x)) = gh(x) = g(x) = y \quad , \; car \quad x \in E^H$$

alors :

$$g(E^H) \subseteq E^{gHg^{-1}}$$

D'autre part, pour $y \in E^{gHg^{-1}}$, soit $x = g^{-1}(y)$; pour $h \in H$ on a :

$$h(x) = hg^{-1}(y) = g^{-1}[ghg^{-1}](y) = g^{-1}(y) = x$$

D'où $x \in E^H$ et $y = g(x) \in g(E^H)$, puis :

$$E^{gHg^{-1}} \subseteq g(E^H)$$

Pour continue on va utiliser le lemme suivant :

Lemme 5.3.3.
Soit $K \hookrightarrow L$ et $L \hookrightarrow E$ des extensions finies de corps, où $K \hookrightarrow E$ est normale. L'extension $K \hookrightarrow L$ est normale si et seulement si, pour tout K-automorphisme g de E, on a $g(L) = L$.

Preuve :
Voir la démonstration de ce lemme dans l'ouvrage :
Olivier Debarre : Algèbre 2, ENS, 2012-2013, page 17. □

D'après ce lemme l'extension $K \hookrightarrow E^H$ est galoisienne ssi $g(E^H) = E^{gHg^{-1}} = E^H$ ssi $gHg^{-1} = H$ pour tout $g \in G$, c'est-à-dire si et seulement si H est un sous-groupe distingué de G.
De plus, considérons le morphisme de groupes :

$$\begin{array}{rccc} \phi & : & G & \to & Gal(E^H/K) \\ & & g & \mapsto & g_{|E^H} \end{array}$$

est bien défini car pour tout $g \in G$, on a $g(E^H) = E^{gHg^{-1}} = E^H$. Le morphisme ϕ est surjective d'après le prolongement des K-automorphismes de E^H à E .
Le noyau de ϕ est :

$$Ker(\phi) = \{g \in G \; : \; g_{|E^H} = Id_{E^H}\} = \{g \in G \; : g \in Gal(E/E^H)\}$$
$$= Gal(E/E^H)$$

D'après lemme d'Artin : $Ker(\phi) = H$.
D'après le 1^{er} théorème d'isomorphisme :

$$G/H \cong Gal(E^H/K)$$

Ce qui achève le preuve pour 2). □

5.4 Étude d'un exemple

Soit l'extension $\mathbb{Q}(i,\sqrt[4]{2})$ de corps $\mathbb{Q}$, cette extension est un corps de décomposition de polynôme $P(X)=X^4-2\in\mathbb{Q}[X]$, alors $\mathbb{Q}\hookrightarrow\mathbb{Q}(i,\sqrt[4]{2})$ est une extension finie et normale. De plus la $Car(\mathbb{Q})=0$, alors tout polynôme irréductible de $\mathbb{Q}$ est séparable, en particulier pour tout élément de $\mathbb{Q}(i,\sqrt[4]{2})$ son polynôme minimal sur $\mathbb{Q}$ est séparable, alors $\mathbb{Q}\hookrightarrow\mathbb{Q}(i,\sqrt[4]{2})$ est une extension séparable. D'où elle est finie galoisienne.
*- **Le degré** de $\mathbb{Q}(i,\sqrt[4]{2})$ sur $\mathbb{Q}$, on a :*

$$[\mathbb{Q}(i,\sqrt[4]{2}):\mathbb{Q}]=[\mathbb{Q}(i,\sqrt[4]{2}):\mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]$$

Or, $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]$ égale à le degré de polynôme minimal de $\sqrt[4]{2}$ sur $\mathbb{Q}$, comme ce dernier est un racine du polynôme $P(X)=X^4-2\in\mathbb{Q}[X]$ qui est irréductible (d'après le critère d'Eisenstein), unitaire et divisible par le polynôme minimal de $\sqrt[4]{2}$ sur $\mathbb{Q}$, alors il est le polynôme minimal de $\sqrt[4]{2}$ sur $\mathbb{Q}$, d'où $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]=4$. De plus on a $[\mathbb{Q}(i,\sqrt[4]{2}):\mathbb{Q}(\sqrt[4]{2})]=2$ car le polynôme minimal de i sur $\mathbb{Q}(\sqrt[4]{2})$ est $Q(X)=X^2+1$. Alors :

$$[\mathbb{Q}(i,\sqrt[4]{2}):\mathbb{Q}]=8$$

*- **La détermination de groupe** $Gal(\mathbb{Q}(i,\sqrt[4]{2})/\mathbb{Q})$ qui d'ordre 8 car $\mathbb{Q}\hookrightarrow\mathbb{Q}(i,\sqrt[4]{2})$ est galoisienne :*
Soit $\sigma\in Gal(\mathbb{Q}(i,\sqrt[4]{2})/\mathbb{Q})$ on a :
$\sigma(i)^2=\sigma(i^2)=-1$ alors : $\sigma(i)=\pm i$.
$\sigma(\sqrt[4]{2})^4=\sigma(2)=2$ alors : $\sigma(\sqrt[4]{2})=\pm\sqrt[4]{2}$ ou $\sigma(\sqrt[4]{2})=\pm i\sqrt[4]{2}$.
Or, σ est complètement déterminé par son action sur i et $\sqrt[4]{2}$ car ces éléments engendrent $\mathbb{Q}(i,\sqrt[4]{2})$ sur $\mathbb{Q}$. Il en résulte que le groupe de Galois de l'extension $\mathbb{Q}(i,\sqrt[4]{2})$ de $\mathbb{Q}$ est donnée par :

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
$\sigma(i)$	i	i	i	i	$-i$	$-i$	$-i$	$-i$
$\sigma(\sqrt[4]{2})$	$\sqrt[4]{2}$	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-i\sqrt[4]{2}$

La loi de composition de ce groupe est définie par le tableau suivant :

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
σ_2	σ_2	σ_1	σ_4	σ_3	σ_6	σ_5	σ_8	σ_7
σ_3	σ_3	σ_4	σ_2	σ_1	σ_7	σ_8	σ_6	σ_5
σ_4	σ_4	σ_3	σ_1	σ_2	σ_8	σ_7	σ_5	σ_6
σ_5	σ_5	σ_6	σ_8	σ_7	σ_1	σ_2	σ_4	σ_3
σ_6	σ_6	σ_5	σ_7	σ_8	σ_2	σ_1	σ_3	σ_4
σ_7	σ_7	σ_8	σ_5	σ_6	σ_3	σ_4	σ_1	σ_2
σ_8	σ_8	σ_7	σ_6	σ_5	σ_4	σ_3	σ_2	σ_1

- ***La détermination des Sous-groupes*** *de* $Gal(\mathbb{Q}(i,\sqrt[4]{2})/\mathbb{Q})$ *:*
L'ordre d'un sous-groupe de $Gal(\mathbb{Q}(i,\sqrt[4]{2})/\mathbb{Q})$ *est un diviseur de 8 (le théorème de Lagrange). Alors :*
Sous-groupe d'ordre 1 :

$$I = \{\sigma_1\}$$

Sous-groupe d'ordre 2 :

$$A = \{\sigma_1, \sigma_2\}, B = \{\sigma_1, \sigma_5\}, C = \{\sigma_1, \sigma_6\}, D = \{\sigma_1, \sigma_7\}, E = \{\sigma_1, \sigma_8\}$$

Sous-groupe d'ordre 4 :

$$F = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}, G = \{\sigma_1, \sigma_2, \sigma_5, \sigma_6\}, H = \{\sigma_1, \sigma_2, \sigma_7, \sigma_8\}$$

Sous-groupe d'ordre 8 :

$$Gal(\mathbb{Q}(i,\sqrt[4]{2})/\mathbb{Q})$$

On peut représenter les inclusions entre ces groupes par le diagramme ci-dessous, où chaque flèche (y compris composée) représente une inclusion :

$$\begin{array}{c} Gal(\mathbb{Q}(i,\sqrt[4]{2})/\mathbb{Q}) \\ \nearrow\uparrow\nwarrow \\ H \quad F \quad G \\ \nearrow\uparrow\nwarrow\uparrow\nearrow\uparrow\nwarrow \\ E \quad D \quad A \quad B \quad C \\ \nwarrow\nwarrow\uparrow\nearrow\nearrow \\ I \end{array}$$

- ***La détermination des sous-extensions*** *de* $\mathbb{Q} \hookrightarrow \mathbb{Q}(i,\sqrt[4]{2})$ *:*
D'après la théorie de Galois, on sait que chaque corps intermédiaire L, $\mathbb{Q} \subseteq L \subseteq \mathbb{Q}(i,\sqrt[4]{2})$, *est le corps des invariants d'un des groupes ci-dessus. De plus, chaque inclusion entre sous-groupes induit une inclusion (dans l'autre sens) entre corps intermédiaires. Si, pour un sous-groupe* H, *on note* $L(H)$ *le corps de ses invariants, on peut, avec la même convention que ci-dessus, représenter les corps intermédiaires par le diagramme suivant :*

$$\begin{array}{c} \mathbb{Q} = L(Gal(\mathbb{Q}(i,\sqrt[4]{2})/\mathbb{Q})) \\ \swarrow\downarrow\searrow \\ L(H) \quad L(F) \quad L(G) \\ \swarrow \downarrow \searrow \downarrow \swarrow \downarrow \searrow \\ L(E) \quad L(D) \quad L(A) \quad L(B) \quad L(C) \\ \searrow \searrow \downarrow \swarrow \swarrow \\ \mathbb{Q}(i,\sqrt[4]{2}) = L(I) \end{array}$$

Pour déterminer ces corps intermédiaires, on considère une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(i, \sqrt[4]{2})$ exprimée en termes de i et $\sqrt[4]{2}$. Nous avons la base suivante :

$$\{1, \sqrt[4]{2}, (\sqrt[4]{2})^2, (\sqrt[4]{2})^3, i, i\sqrt[4]{2}, i(\sqrt[4]{2})^2, i(\sqrt[4]{2})^3\}$$

obtenue en multipliant terme à terme la base $\{1, \sqrt[4]{2}, (\sqrt[4]{2})^2, (\sqrt[4]{2})^3\}$ de l'extension $\mathbb{Q}(\sqrt[4]{2})$ de $\mathbb{Q}$ et la base $\{1, i\}$ de l'extension $\mathbb{Q}(i, \sqrt[4]{2})$ de $\mathbb{Q}(\sqrt[4]{2})$.
Un élément $x \in \mathbb{Q}(i, \sqrt[4]{2})$ s'écrit, d'une manière unique, sous la forme :

$$x = b_0 + b_1\sqrt[4]{2} + b_2(\sqrt[4]{2})^2 + b_3(\sqrt[4]{2})^3 + b_4 i + b_5 i\sqrt[4]{2} + b_6 i(\sqrt[4]{2})^2 + b_7 i(\sqrt[4]{2})^3$$

avec les $b_i \in \mathbb{Q}$.
Pour déterminer,par exemple $L(A)$, on utilise l'équivalence :

$$x \in L(A) \Leftrightarrow \sigma_2(x) = x$$

Or :

$$\sigma_2(x) = b_0 - b_1\sqrt[4]{2} + b_2(\sqrt[4]{2})^2 - b_3(\sqrt[4]{2})^3 + b_4 i - b_5 i\sqrt[4]{2} + b_6 i(\sqrt[4]{2})^2 - b_7 i(\sqrt[4]{2})^3$$

Donc :

$$x \in L(A) \Leftrightarrow \sigma_2(x) = x \Leftrightarrow b_1 = b_3 = b_5 = b_7 = 0$$
$$\Leftrightarrow x \in \mathbb{Q}(i, (\sqrt[4]{2})^2)$$

et $L(A) = \mathbb{Q}(i, (\sqrt[4]{2})^2) = \mathbb{Q}(i, \sqrt{2})$. D'une manière analogue, on détermine les autres corps intermédiaires. Les résultats sont résumés dans le tableau suivant :

Sous-groupe	*Corps intermédiaire associé*
A	$\mathbb{Q}(i, \sqrt{2})$
B	$\mathbb{Q}(\sqrt[4]{2})$
C	$\mathbb{Q}(i\sqrt[4]{2})$
D	$\mathbb{Q}((1+i)\sqrt[4]{2})$
E	$\mathbb{Q}((1-i)\sqrt[4]{2})$
F	$\mathbb{Q}(i)$
G	$\mathbb{Q}(\sqrt{2})$
H	$\mathbb{Q}(i\sqrt{2})$

- ***Les sous-groupes distingués*** *de $Gal(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q})$:*
D'après le tableau de la loi de composition de $Gal(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q})$ au-dessus, on a les sous-groupes distingués sont :

$$I, A, F, G, H, Gal(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q})$$

- ***Des extensions galoisiennes*** *de $\mathbb{Q}$:*
A partir de la partie 2 de la théorème fondamental de correspondance de Galois, on a les corps intermédiaires qui sont galoisiennes de $\mathbb{Q}$ sont ceux associés aux sous-groupes distingués de $Gal(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q})$, Ces corps sont :

$$\mathbb{Q}(i, \sqrt[4]{2}); \mathbb{Q}(i, \sqrt{2}); \mathbb{Q}(i); \mathbb{Q}(\sqrt{2}); \mathbb{Q}(i\sqrt{2}); \mathbb{Q}$$

Bibliographie

[1] *Daniel Guin et Thomas Hausberger :* ▶Algèbre 1 : groupes, corps et Théorie de Galois, L3-M1, *EDP Sciences, (2008).*

[2] *I. El Hage :* ▶Théorie de Galois, *(2001).*

[3] *Josette Calais :* ▶Extensions de corps : Théorie de Galois, Niveau M1-M2, *ellipses, (2006).*

[4] *Mahdou Najib :* ▶Structure Algébrique, *FST-FES, (2017-2018).*

[5] *Olivier Debarre :* ▶Algèbre 2, *ENS, (2012-2013).*

[6] *https://fr.wikipedia.org/wiki/*