كلية العلوم و التقنيات فاس
ⵜⴰⵖⵚⵍⵓⵉⵜ ⵏ ⵜⵇⵙⵙⵉⵙⵉ ⴰ ⵜⵙⵏⵙⵜⵙⵉ
Faculté des Sciences et Techniques de Fès

جامعة سيدي محمد بن عبد الله
ⵜⴰⵙⴷⴰⵡⵉⵜ ⵙⵉⴷⵉ ⵎⵓⵃⴰⵎⴷ ⴱⵏ ⵄⴱⴷⵍⵍⴰⵀ
Université Sidi Mohamed Ben Abdellah

**Licence Mathématiques et Applications**

**(MA)**

**MEMOIRE DE FIN D'ETUDES**

**Pour l'obtention du Diplôme de Licence Sciences et Techniques (LST)**

# Introduction à la théorie de Galois

**Réalisé par : Abdelhadi Zabraoui**

**Encadré par : Pr. Lahcen OUKHTITE**

**Soutenu le 05 juin 2018**

**Devant le jury composé de:**

| | |
|---|---|
| Pr. Mohamed BEKKALI | Faculté des Sciences et Techniques Fès |
| Pr. Rachid EL AYADI | Faculté des Sciences et Techniques Fès |
| Pr. Seddik GMIRA | Faculté des Sciences et Techniques Fès |
| Pr. Lahcen OUKHTITE | Faculté des Sciences et Techniques Fès |

**Année Universitaire 2017-2018**

# Remerciement

Je tiens à remercier mon encadrant le professeur Lahcen OUKHTITE, qui a proposé ce sujet, et qui a bien voulu encadrer ce modeste travail. Je lui exprime aussi ma gratitude pour son dévouement et le temps quil ma consacré.

Je remercie également les membres de jury les Professeurs Mohamed BEKKALI, Rachid El AYADI et Seddik GMIRA, davoir accepté dexaminer notre modeste travail, sans oublier laide énorme des personnes travaillant à la bibliothèque de la FST.

Mes remerciements vont également à tous mes professeurs du département de mathématiques.

Enfin, je remercie ma famille, et surtout mes parents, qui mont toujours soutenu durant mes études.

# Table des matières

# INTRODUCTION

En ce début du XIXe siècle, il est si naturel de penser que les solutions des équations sont des ≪ racines ≫, construites par extraction de ≪ racines ≫, qu'on les dénomme ainsi. La question, cependant, reste lancinante : quelles sont les équations dont les solutions s'expriment par des radicaux (c'est-à-dire par extraction de racines) ?

Abel a montré que l'équation générale de degré 5 ne se résout pas par radicaux. Ce résultat sonne-t-il le glas de l'algèbre en tant qu'art de résolution des équations ? En mai 1829, un mois après la mort d'Abel, Galois adresse à l'Académie de Paris un mémoire où il propose un critère de résolubilité des équations ; ce critère permet de savoir quand une résolution est possible et pourquoi. L'algèbre n'a pas dit son dernier mot !

Galois précise : ≪ Il [Abel] n'a rien laissé sur la discussion générale du problème qui nous a occupé. Car une fois pour toutes, ce que notre théorie a de remarquable, c'est dans tous les cas de répondre oui ou non. ≫ Sur les traces de Lagrange, Galois s'intéresse aux relations entre les solutions d'une équation et aux permutations des solutions qui conservent ces relations. Combien en existe-t-il ? Galois montre que

si le nombre de ces substitutions peut être suffisamment réduit, l'équation est résoluble par radicaux. Pour arriver à ce grand résultat, Galois combine les travaux de Lagrange sur la résolution des équations et ceux de Cauchy sur les ≪ groupes ≫ de substitutions, en une théorie infaillible et puissante donnant les conditions de résolubilité des équations par radicaux.

# Histoire de la résolution des équations

# Équation de degré 2

$$ax^2 + bx + c = 0 \tag{1}$$

avec $a, b, c \in \mathbb{C}$ et $a \neq 0$

On divise l'équation (1) par $a$ on obtient l'équation :

$$x^2 + px + q = 0 \Rightarrow (x - x_1)(x - x_2) = 0$$

Donc $x_1 + x_2 = -p$ et $x_1 x_2 = q$

On considère la fonction : $y = x_1 - x_2$ qui n'est pas symétrique en $x_1$ et $x_2$, mais dont le carré l'est :

$$\begin{aligned} y^2 &= (x_1 - x_2)^2 \\ &= x_1^2 - 2x_1x_2 + x_2^2 \\ &= (x_1 + x_2)^2 - 4x_1x_2 \\ &= p^2 - 4q \end{aligned}$$

D'où les formules bien connus :

$$y = \pm\sqrt{p^2 - 4q}$$

$$x_1, x_2 = \frac{1}{2}(-p \pm \sqrt{p^2 - 4q})$$

## Équation de degré 3

Formule de Cardan :

Soit l'équation : $\alpha x^3 + \beta x^2 + \gamma x + \delta = 0$ avec $\alpha \neq 0$.

On divise $\alpha$, on pose $x \to x + \frac{a}{3}$, on obtient l'équation :

$x^3 + px + q = 0$.

On cherche une racine sous la forme $x = u + v$. Donne

$(u+v)^3 + p(u+v) + q = 0 \Leftrightarrow u^3 + v^3 + (u+v)(3uv+p) + q = 0$.

Ça se simplifie si on impose $3uv = -p$ et $u^3 + v^3 + q = 0$.

Donc si $u$,$v$ vérifient :

$$\begin{cases} u^3 + v^3 &= -q \\ uv &= -\frac{p}{3} \end{cases}$$

On pose $y = u^3$ et $z = v^3$, on obtient

$$\begin{cases} y + z &= -q \\ yz &= -\frac{p^3}{27} \end{cases}$$

Si $S = y + z$ et $P = yz$, alors $u$ et $v$ sont solutions de l'équation $X^2 - SX + P = 0$, donc : $y = -\frac{q}{2} \pm \sqrt{\frac{p^3}{27} - \frac{q^2}{4}}$

## Équation de degré 4

L'équation du 4ème degré fut résolue en 1540 par Ferrari et sa solution repose sur la méthode de Cardan dont il était d'ailleurs l'élève.

On cherche à résoudre l'équation $x^4 = px^2 + qx + r$. Comme pour l'équation de degré 3, un changement de variable permet de ramener toute équation du quatrième degré à une équation de cette forme-là.

L'idée de Ferrari consiste à rajouter un paramètre supplémentaire $t$ en écrivant que $x^4 = (x^2 + t)^2 - 2x^2t - t^2$. On obtient alors $(x^2 + t)^2 - 2x^2t - t^2 = px^2 + qx + r$ ou encore $(x^2 + t)^2 = (2t + p)x^2 + qx + (t^2 + r)$.

On choisit alors une valeur de $t$ convenable de telle sorte que la quantité $(2t+p)x^2 + qx + (t^2+r)$ se factorise sous la forme $(\alpha x + \beta)^2$. Or, dire que $ax^2 + bx + c$ se factorise sous la forme $(\alpha x + \beta)^2$ revient à dire que son discriminant $b^2 - 4ac$ est nul.

Dans notre cas, la condition sur $t$ est donc $q^2 - 4(2t+p)(t^2+r) = 0$. Ceci donne lieu à une équation du troisième degré en $t$. Pour la résoudre, Ferrari utilise la méthode de Cardan. Il trouve alors $t$ et $\alpha$, $\beta$ sont exprimés par radicaux en fonction de $p, q$ et $r$.

Comme $A^2 = B^2$ équivaut à $A = \pm B$, on en déduit que $x$ vérifie l'une des deux

équations suivantes

$$\begin{cases} x^2+t &= \alpha x+\beta \\ x^2+t &= -\alpha x+\beta \end{cases}$$

de degré 2 que l'on sait résoudre par radicaux. On en déduit que l'équation de degré 4, $x^4 = px^2 + qx + r$ est résoluble par radicaux.

## Équation de degré 5

On a : $(x^5 - 2) = (x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5)$ où $x_k = \sqrt[5]{2}\exp(i\frac{2k\pi}{5})$

Donc $x^5 - 2 = 0$ est une équation "résoluble par radicaux".

En revanche nous verrons plus tard que l'équation $x^5 - x - 1 = 0$ n'est par résoluble par radicaux.

Chapitre 1

# Préliminaire

## 1.1 Groupes

### 1.1.1 Groupes symétriques

**Définition 1.1.** ([4], Définition 3.1, page 10)

*Soit $X$ un ensemble non vide. Une* **permutation** *de $X$ est une bijection $\sigma : X \to X$. On note $S_X$ l'ensemble de toutes les permutations de $X$.*

*Dans le cas où $X = \{1, \ldots, n\}$, on écrit $S_n$ au lieu de $S_X$.*

**Notations**

- $S_n$ est dit le groupe **symétrique d'ordre** $n$.

- Une permutation $\sigma \in S_n$ telle que $\sigma : i \mapsto \sigma(i)$ est notée

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

L'ordre des colonnes n'est pas important.
On peut écrire la même permutation sous la forme

$$\sigma = \begin{pmatrix} 4 & n & \ldots & 2 \\ \sigma(4) & \sigma(n) & \ldots & \sigma(2) \end{pmatrix}$$

Ainsi, l'inverse de $\sigma$ peut s'écrire

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \ldots & \sigma(n) \\ 1 & 2 & \ldots & n \end{pmatrix}$$

Pour alléger les écritures, on notera, pour tout couple $(\sigma, \psi)$ d'éléments de $S_n$, $\sigma\psi$ à la place de $\sigma \circ \psi$. On parlera de produit de deux permutations plutôt que de composition de deux permutations.

**Exemple**

1) La permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$ s'écrit également $\sigma = \begin{pmatrix} 3 & 2 & 5 & 1 & 4 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix}$.
En outre son inverse est
$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 4 & 5 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$.

2) Le produit des deux permutations $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ et $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$
est $\sigma_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$.

**Proposition 1.1.** ([4], Proposition 3.3, page 11)

*La cardinal de $S_n$ est $n!$.*

**Preuve.** Soit $S_n$ l'ensemble des permutation de $\{1, \ldots, n\}$. Il est clair que pour établir un bijection de $\{1, \ldots, n\}$ sur lui même, il suffit d'envoyer 1 sur n'importe quel élément de $\{1, \ldots, n\}$, ainsi on a $n$ possibilité. Par contre pour l'image de 2, une fois l'image de 1 est fixé, on n'a que $n-1$ possibilités. Ainsi de suite, on n'aura qu'un seul choix pour l'image $n$. Donc $|S_n| = n!$. ∎

**Définition 1.2.** ([4], Définition 3.4, page 11)

*Soient $i_1, \ldots, i_k$,$1 \leqslant k < n$ des éléments distincts de $\{1, \ldots, n\}$. Le $k$-cycle $(i_1, \ldots, i_k)$ est la permutation $\sigma \in S_n$ telle que $\sigma(i_l) = i_{l+1}$ pour $1 \leqslant l \leqslant k-1$, $\sigma(i_k) = i_1$ et $\sigma(j) = j$ pour $j \notin \{i_1, \ldots, i_k\}$. Si $k \geqslant 2$, l'ensemble $\{i_1, \ldots, i_k\}$ est le support du cycle. On dit que $k$ est sa longueur.*

**Remarque**

1) Un cycle de longueur deux est une transposition.

2) Les cycles $(i_1, \ldots, i_k)$, $(i_2, \ldots, i_k, i_1)$ , . . . , $(i_k, i_1, \ldots, i_{k-1})$ sont identiques.

3) Soient $\sigma$ une permutation et c=$(i_1, \ldots, i_k)$ un cycle. Alors $\sigma c \sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_k))$.

**Définition 1.3.** ([4], Définition 3.5, page 12)

*Le support d'une permutation $\sigma \in S_n$ est l'ensemble des $1 \leqslant i \leqslant n$ tels que $\sigma(i) \neq i$. On le note supp$(\sigma)$.*

**Proposition 1.2.** ([4], Proposition 3.6, page 12)

*Deux permutations à supports disjoints commutent.*

**Preuve.** Soit $\sigma$ et $\psi$ deux éléments de $S_n$. Soit $i$ compris entre 1 et $n$. Si $i$ appartient au support de $\sigma$ alors $\sigma(i)$ appartient au support de $\sigma$ car si $\sigma(\sigma(i)) = \sigma(i)$ alors $\sigma(i) = i$. D'où, puisque les support de $\sigma$ et $\psi$ sont disjoints, $\sigma(i)$ n'appartient pas au support de $\psi$ et par conséquent $\sigma\psi(i) = \sigma(i) = \psi\sigma(i)$ si $i$ appartient au support de $\psi$.

Si $i$ n'appartient ni au support de $\sigma$ ni au support de $\psi$ alors $\sigma\psi(i) = i = \psi\sigma(i)$. ∎

**Exemples**

1) $(1,3,4)(1,2,5) = (1,2,5,3,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}$.

2) Si $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 4 & 2 & 5 \end{pmatrix}$, alors $\text{supp}(\sigma) = \{2,3,5,6\}$.

**Définition 1.4.** ([4], Définition 3.7, page 12)

*Soit $\sigma \in S_n$, l'ordre de $\sigma$ est le plus petit entiers $p \in \mathbb{N}^*$ tels que $\sigma^p = id$.*

**Notation**

Si $\tau \in S_n$ est une transposition alors l'ordre de $\tau$ est 2.

**Exemple**

Cherchons l'ordre de $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 6 & 2 \end{pmatrix}$.

Comme $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}, \sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}, \sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}, \sigma^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}, \sigma^6 = id$, il résulte que $\sigma$ est dordre 6.

**Proposition 1.3.** ([3], Proposition 4.14, page 76)

*Tout élément de $S_n$ peut se décomposer en un produit (commutatif) de cycles de support disjoints, cette décomposition est unique à l'ordre près.*

**Exemple**

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 4 & 2 & 5 \end{pmatrix} = (1,3,7)(2,4,8)(6,9) = (6,9)(1,3,7)(2,4,8)$
$= (1,3,7)(6,9)(2,4,8)$.

**Corollaire 1.1.** ([3], proposition 4.14, page 76)

*Tout p-cycle de $S_n$ est égal à un produit de transposition*

**Preuve.** D'après la proposition 1.3, il suffit de montrer qu'un cycle est produit de transposition. Mais il est facile de voir que :

$(i_1 i_2 \dots i_k) = (i_1 i_2)(i_2 i_3) \dots (i_{k-2} i_{k-1})(i_{k-1} i_k)$. ∎

**Exemple**

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 5 & 6 & 4 & 3 & 2 & 8 & 1 \end{pmatrix}$ peut s'écrire

$\sigma = (1,7,8)(2,5,3,6) = (1,8)(1,7)(2,6)(2,3)(2,5)$.

**Définition 1.5.** ([5], Définition 5.3.1, page 20)

*Soit $n \geqslant 2$ un entier. Pour toute permutation $\sigma \in S_n$, on appelle nombre d'inversions de $\sigma$ l'entier*

$I(\sigma) = card\{(i,j) \in \{1,2,\dots,n\}^2 | i < j \quad et \quad \sigma(i) > \sigma(j)\}$.

*On appelle signature de $\sigma$ l'entier valant +1 ou -1 défini par : $\varepsilon(\sigma) = (-1)^{I(\sigma)}$.*

*$\sigma$ est dite paire (resp. impaire) si $\varepsilon(\sigma) = 1$ (resp. $\varepsilon(\sigma) = -1$).*

**Exemple**

1) Si $\tau$ est une transposition de $S_n$, on a $\varepsilon(\tau) = -1$.

2) Si $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (1,2,3,4,5)$, alors $I(\sigma_1) = 4$ et $\varepsilon(\sigma_1) = 1$.

**Proposition 1.4.** ([5], proposition 5.3.3, page 21)

*1) Soient $x_1, \dots, x_n$ des éléments d'un anneau commutatif unitaire. Pour tout $\sigma \in S_n$, on a*

$$\prod_{1 \leqslant i < j \leqslant n} (x_{\sigma(i)} - x_{\sigma(j)}) = \epsilon(\sigma) \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j). \tag{1.1}$$

*2) La signature $\epsilon : S_n \to \{-1, +1\}$ est un morphisme de groupes : on a $\epsilon(id) = 1$ et $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$.*

**Preuve.** Les facteurs des deux produits sont les mêmes au signe près et on vérifie que ce signe est $\epsilon(\sigma)$.

On applique la relation (1.1) une première fois avec des $x_i$ distincts dans $\mathbb{Z}$ et $\sigma(S_n)$ et une seconde fois avec les $y_i := x_{\sigma(i)}$ et $\tau \in S_n$. ∎

**Remarque**

La proposition 1.4 permet de calculer facilement la signature d'une permutation une fois qu'elle est décomposée en produit de cycles. Tout d'abord, un $r$-cycle est produit de $r-1$ transpositions, donc sa signature est $(-1)^{r-1}$. Ensuite, s'il est un peu long de calculer le nombre d'inversions de la permutation.

### 1.1.2 Groupes quotients

**Définition 1.6.** ([2], Définition 0.1, page 11)

*Soit $H$ un sous-groupe d'un groupe $G$. On appelle* **classe à gauche** *de un élément $a \in G$ relativement à $H$ le sous-ensemble $aH = \{g \in G | g = ah,\ h \in H\}$ et on définit de même les classes à droite $Ha$. Les classes à gauche forment une partition de $G$. Leur ensemble est noté $G/H$.*

**Notations** :

• $G/H$ n'est pas un groupe en général.

• Le cardinal de $G/H$ est appelé l'**indice** de $H$ dans $G$ et noté $[G : H]$.

**Définition 1.7.** ([2], Définition 2.1, page 13)

*Soit $G$ un groupe. Un sous-groupe $H$ de $G$ est dit distingué dans $G$ si et seulement si $\forall g \in G,\ gHg^{-1} = H$.*

**Théorème 1.1.** ([2], Théorème 0.2, page 11)

*Soit $H$ un sous-groupe distingué de $G$. L'ensemble quotient $G/H$ est un groupe pour la loi $(\bar{x}, \bar{y}) \mapsto \overline{xy}$ où $\bar{z}$ désigne la classe de $z$.*

**Preuve.** 1) La correspondance

$$\phi : (G/H)^2 \to G/H$$

$$(\bar{x}, \bar{y}) \to \overline{xy}$$

est bien une application. En effet, soient $x', y' \in G$ tels que $\bar{x} = \bar{x'}$ et $\bar{y} = \bar{y'}$. Nous avons : $\bar{x} = \bar{x'} \Longrightarrow x'x^{-1} \in H$ et $\bar{y} = \bar{y'} \Longrightarrow y'y^{-1} \in H$. Compte tenu du fait que $x'y'(xy)^{-1} = x'y'y^{-1}x^{-1} = x'x^{-1}(xy'y^{-1}x^{-1})$ et du fait que $xy'y^{-1}x^{-1} \in H$, il en résulte que $x'y'(xy)^{-1} \in H$ et ainsi $\overline{xy} = \overline{x'y'}$.

2) L'associativité est facile, en effet si $\bar{z}$ est une troisième classe, on a : $\bar{x}(\bar{y}\bar{z}) = \bar{x}(\overline{yz}) = \overline{x(yz)} = \overline{(xy)z} = (\overline{xy}\bar{z}) = (\bar{x}\bar{y})\bar{z}$. L'élément neutre est $\bar{1} = H$. L'inverse de la classe de $x$ est la classe $x^{-1}$. Ainsi, $G/H$ est un groupe. ∎

## 1.2 Polynômes symétriques et discriminant

**Définition 1.8.** ([9], Définition 6.10.1, page 209)

*Un polynôme $P$ est dit* **symétrique** *si $P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = P(X_1, \ldots, X_n)$ pour tout $\sigma \in S_n$.*

**Exemples**

✓ $X_1 + X_2$ *et* $X_1^2 + 4X_1X_2 + X_2^2$ sont des polynômes symétriques en deux variables.

✓ $X_1^2X_2 + X_1^2X_3 + X_1X_2^2 + X_1X_3^2 + X_2^2X_3 + X_2X_3^2$ est un polynôme symétrique en trois variables.

**Définition 1.9.** ([9], Définition 6.10.2, page 210)

*Dans $A[X_1, \ldots, X_n]$ les $n$ polynômes $\Sigma_p$, $(1 \leqslant p \leqslant n)$ définie par :*

$\Sigma_p = \sum_{1 \leqslant i_1 < \ldots < i_p \leqslant n} X_{i_1} \ldots X_{i_p}$ *sont symétrique et portent le nom de* **polynômes symétriques élémentaires**.

**Exemple**

1) Pour $n = 1$, $\Sigma_1 = X_1$.

2) Pour $n = 2$, $\Sigma_1 = X_1 + X_2$ et $\Sigma_2 = X_1X_2$.

3) Pour $n = 3$, $\Sigma_1 = X_1 + X_2 + X_3$, $\Sigma_2 = X_1X_2 + X_1X_3 + X_2X_3$ et $\Sigma_3 = X_1X_2X_3$.

**Définition 1.10.** ([10], Définition 3.5.1, page 31)

*Soit $K$ un corps contenu dans un corps algébriquement clos $\Omega$. Soient $F$ et $G$ deux polynômes de $K[X]$ de degrés $m$ et $n$ respectivement. On suppose que $F(X) = a\prod_{1 \leqslant i \leqslant m}(X - x_i)$ et $G(X) = b\prod_{1 \leqslant i \leqslant n}(X - y_i)$ dans $\mathbb{C}[X]$. On appelle résultant des deux polynômes non nuls $F$ et $G$ le produit : $Res(F, G) = a^n b^m \prod_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n}(x_i - y_i)$. Si $F = 0$ ou $G = 0$, on pose $Res(F, G) = 0$.*

**Remarque**

a) Le résultant de deux polynômes de $K[X]$ est nul si, et seulement si, les deux

polynômes ont une racine commune dans $\Omega$.

b) Le résultant de deux polynômes non nuls de $K[X]$ est un élément de $K$ et l'on a :

Formule (1) : $Res(F,G) = a^n \prod_{1\leqslant i\leqslant m} G(x_i)$

Formule (2) : $Res(G,F) = (-1)^{mn} Res(F,G)$

Formule (3) : $Res(F,G) = (-1)^{mn} b^{m-deg(R)} Res(G,R)$

si la division euclidienne de $F$ par $G$ donne $F = GQ + R$, $deg(R) < deg(G)$ ; si $R = 0$, on a $Res(F,G) = 0$.

Formule (4) : $Res(F,b) = b^m$ pour un polynôme constant $b$.

**Définition 1.11.** ([10], Définition 3.6.1, page 33)

*Soit K un corps contenu dans un corps algébriquement clos $\Omega$. Le discriminant $D(P)$ d'un polynôme non nul P de $K[X]$ de degré n et de coefficient dominant a est :*

$$D(P) = \frac{(-1)^{\frac{n(n-1)}{2}} Res(P,P')}{a}.$$

**Proposition 1.5.** ([10], Proposition 3.6.2, page 33)

*Le discriminant D(P) d'un polynôme non constant P est un élément de K, nul si et seulement si P a une racine de multiplicité supérieure ou égale à 2 dans $\Omega$.*

**Preuve.** Le fait que $D(P) \in K$ résulte de (Remarque a)). Le discriminant de P, qui est le résultant de $P$ et de $P'$ est, d'après (Remarque b)), nul si et seulement si $P$ a une racine commune avec $P'$ dans $\Omega$, c'est-à-dire si P a une racine de multiplicité supérieure ou égale à 2 dans $\Omega$. ∎

**Lemme 1.1.** *On a les propriétés suivantes :*

*1)* $D(aX^2 + bX + c) = b^2 - 4ac$.

*2)* $D(X^3 + pX + q) = -4p^3 - 27q^2$.

*3) Si* $F(X) = a\prod_{1\leqslant i\leqslant n}(X - x_i)$, *alors*

$D(F) = a^{2n-2}\prod_{1\leqslant i<j\leqslant n}(x_i - x_j)^2$.

**Preuve.** 1) Si $x_1$ et $x_2$ désignent les racines dans $\mathbb{C}$ de $aX^2 + bX + c$, on a :

$D(aX^2 + bX + c) = -(2ax_1 + b)(2ax_2 + b) = -4a^2(\frac{c}{a}) - 2ab(-\frac{b}{a}) - b^2 = b^2 - 4ac.$

2) Puisque $\sqrt{\frac{-p}{3}}, -\sqrt{\frac{-p}{3}}$ sont les racines de $3X^2 + p$ alors

$D(X^3+pX+q) = -Res(X^3+pX+q, 3X^2+p) = -27[(\sqrt{\frac{-p}{3}})^3+p\sqrt{\frac{-p}{3}}+q][(\sqrt{\frac{-p}{3}})^3-$

$p\sqrt{\frac{-p}{3}}+q] = -27[\frac{2p}{3}\sqrt{\frac{-p}{3}}+q][-\frac{2p}{3}\sqrt{\frac{-p}{3}}+q] = -4p^3-27q^2$.

3) On a $D(F) = \frac{(-1)^{\frac{n(n-1)}{2}} Res(F,F')}{a} = \frac{(-1)^{\frac{n(n-1)}{2}} a^{n-1}\prod_{1\leqslant i\leqslant n} F'(x_i)}{a}$

$= (-1)^{\frac{n(n-1)}{2}} a^{n-2}\prod_{1\leqslant i\leqslant n}(a\prod_{1\leqslant i\leqslant n, j\neq i}(x_i-x_j))$

$= a^{2n-2}\prod_{1\leqslant i\leqslant j\leqslant n}(x_i-x_j)^2$

compte tenu des $\frac{n(n-1)}{2}$ changements de signes à faire dans le produit. ∎

## Polynômes à coefficients réels

### a) Polynômes du second degré

Soient $a, b$ *et* $c$ des réels. On a $D(aX^2+bX+c) = b^2-4ac = a^2(x_1-x_2)^2$ où $x_1$ et $x_2$ désignent les racines dans $\mathbb{C}$ de $aX^2+bX+c$. Si $x_1$ et $x_2$ sont réelles distinctes, alors $b^2-4ac>0$ ; si $x_1$ et $x_2$ ne sont pas réelles, elles sont conjuguées dans $\mathbb{C}$ et $x_1-x_2$ est un imaginaire pur et $b^2-4ac<0$.

### b) Polynômes du troisième degré

Soient $p$ *et* $q$ des réels et notons $a, b, c$ les racines de $X^3+pX+q$ dans $\mathbb{C}$. On a :

$D(X^3+pX+q) = -4p^3-27q^2 = (a-b)^2(a-c)^2(b-c)^2$.

Si les trois racines sont réelles distinctes $-4p^3-27q2>0$, c'est le cas irréductible. Le second cas est celui où deux des racines, disons $a$ et $b$, ne sont pas réelles mais sont conjuguées dans $\mathbb{C}$ ; $a-b$ est alors imaginaire pur et son carré est négatif ; $(a-c)^2$ et $(b-c)^2$ sont conjugués et leur produit est strictement positif donc $-4p^3-27q2<0$.

Ces résultats sont résumés dans le tableau 1.1.

| | D > 0 | D < 0 |
|---|---|---|
| Degré 2 | 2 racines réelles | 2 racines non réelles conjuguées |
| Degré 3 | 3 racines réelles | 1 racine réelle, 2 racines non réelles conjuguées |

TABLE 1.1 – Racines réelles et signe du discriminant.

Chapitre 2

# Extensions de corps

**Définition 2.1.** ([6], Définition 1.8, page 18)

*Soit $K$ un corps. On appelle extension de $K$ tout corps $L$ contenant un sous-corps isomorphe à $K$.*

**Remarque** ([7], Remarque 2.2, page 31)

• Si $K$ est un sous-corps de $L$, alors $L$ est une extension de $K$ (considère l'injection canonique $i : K \longrightarrow L$).

• Réciproquement un homomorphisme de corps $\phi : K \longrightarrow L$ est forcément injectif. Par conséquent, le sous-corps $K' = \phi(K)$ de $L$ est isomorphe à $K$. Identifiant $K$ et $K'$, on peut donc dire que $K$ est un sous-corps de $L$.

• En conclusion, aux notation abusives (bien pratique) près :

$L$ est une extension de $K \Longleftrightarrow K$ est un sous-corps de $L$.

**Exemple**

• $\mathbb{C}$ est une extension de $\mathbb{R}$, $\mathbb{R}$ est une extension de $\mathbb{Q}$.

• $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ est une extension de $\mathbb{Q}$.

**Définition 2.2.** ([7], Définition 2.5, page 32)

*Soient $K$ un corps et $L$ une extension de $K$. On appelle degré de l'extension $L$ de $K$ (ou $L/K$) et on note $[L : K]$, la dimension de $L$ comme $K$-espace vectoriel :* $[L : K] = dim_K L$.

**Remarque** ([7], Remarque 2.6-2.7, page 32)

• Pour une extension $L$ de $K$, on a : $[L : K] = 1 \Longleftrightarrow K = L$.

• Le degré d'une extension peut être fini (par exemple $[\mathbb{C} : \mathbb{R}] = 2$) ou infini (par exemple $[\mathbb{R} : \mathbb{Q}] = +\infty$ car $\mathbb{Q}$ est dénombrable et $\mathbb{R}$ ne l'est pas, autre exemple : $[K(X) : K] = +\infty$).

## 2.1 Extensions algébriques, Extensions transcendantes

**Définition 2.3.** ([1], Définition 11.1.1, page 271)

*Soit $L/K$ une extension de corps. Un élément $\alpha$ de $L$ est* **algébrique** *sur $K$ s'il existe $P(X) \in K[X]$ tel que $P(\alpha) = 0$.*

**Définition 2.4.** ([1], Définition 11.1.3, page 273)

*On dit que $L$ est algébrique sur $K$ si tous les élément de $L$ sont algébrique sur $K$.*

**Définition 2.5.** ([1], Définition 11.1.4, page 275)

*On appelle* **nombre algébrique** *tout nombre complexe algébrique sur $\mathbb{Q}$.*

**Exemple**

$\sqrt{2}$, $\sqrt[3]{2}$, $\exp(\frac{2i\pi}{n})$ sont des nombres complexes algébriques sur $\mathbb{Q}$.

**Définition 2.6.** ([1], Définition 2.4, page 26)
*Soit $L/K$ une extension de corps et soient $x_1, \ldots, x_n$ des éléments de $K$. On pose $K[x_1, \ldots, x_n] = \{P(x_1, \ldots, x_n) \mid P \in K[X_1, \ldots, X_n]\}$, c'est le plus petit sous-anneau de $L$ contenant $K$ et $x_1, \ldots, x_n$.*

La proposition suivante, est l'outil qui permet de ramener l'étude des éléments algébriques à l'algèbre linéaire.

**Proposition 2.1.** ([3], Proposition 6.8, page 133)
*Soit $L/K$ une extension de corps. Un élément $x$ de $L$ est algébrique sur $K$ si et seulement si le $K$-espace vectoriel $K[x]$ est de dimension finie.*

**Preuve.** Supposons $x$ est algébrique sur $K$, donc $x$ est racine d'un polynôme $P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in K[X]$. Alors $x^n$ s'exprime comme combinaison linéaire à coefficients dans $K$ de $x^{n-1}, \ldots, x, 1$. On vérifie, par récurrence sur $m$, qu'il en est de même pour toutes les puissances $x^m$, donc pour tous les éléments de $K[x]$.
La famille à $n$ éléments $(x^{n-1}, \ldots, x, 1)$ engendre donc le $K$-espace vectoriel $K[x]$, de sorte que $\dim_K L[x] \leqslant n$.
Inversement, supposons $\dim_K L[x] \leqslant n < \infty$. Alors, la famille à $n+1$ éléments $(x^{n-1}, \ldots, x, 1)$ est liée.
Il existe donc $a_0, \ldots, a_n$ des éléments de $K$ non tous nuls tels que $P(x) = \sum_{i=0}^{n} a_i x^i = 0$. D'où $x$ est algébrique sur $K$. ∎

**Corollaire 2.1.** ([3], Corollaire 6.9, page 135)
*Soit $L/K$ une extension de corps. Si $L$ est un $K$-espace vectoriel de dimension finie, alors l'extension $L/K$ est algébrique.*

**Preuve.** Il s'agit de montrer que tout élément $x$ de $L$ est algébrique sur $K$. L'espace vectoriel $K[x]$ est un sous-espace vectoriel de $L$, donc est de dimension finie. La proposition permet de conclure. ∎

De même, si $x$ est algébrique sur $K$, tout élément $y$ de $K[x]$ est algébrique sur $K$ d'après la proposition, puisque $K[y]$ est un sous-espace vectoriel de $K[x]$.

**Proposition 2.2.** *Soit $L/K$ une extension de corps. Si $x \in L$ est algébrique sur $K$, l'anneau $K[x]$ est un corps, extension algébrique de $K$.*

**Preuve.** Soit $y$ un élément non nul de $K[x]$. On vient de voir que $y$ est algébrique sur $K$. Choisissons un polynôme $P(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ non nul de degré $n$ minimal vérifiant $P(y) = 0$ c'est-à-dire :

$a_n y^n + a_{n-1} y^{n-1} + \ldots + a_1 y + a_0 = 0.$

Si $a_0$ était nul, on aurait $a_n y^n + \ldots + a_1 y = 0$, d'où $a_n y^{n-1} + \ldots + a_1 = 0$, contredisant la minimalité de $n$. On a donc $a_0 \neq 0$.

En divisant par $y$, on tire de l'équation $a_n y^n + \ldots + a_1 y + a_0 = 0$, la formule dans $L$ :

$$y^{-1} = -\frac{a_n y^n + \ldots + a_1}{a_0} \in K[y] \subset K[x].$$

On a donc montré que l'inverse $y^{-1}$ de $y$ dans $L$ est bien dans $K[x]$, qui est ainsi un corps. ∎

**Exemple** :

Considérons le réel $\sqrt{2}$ algébrique sur $\mathbf{Q}$. Alors $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ est bien un corps ; cela résulte de la formule

$$\frac{1}{a + b\sqrt{2}} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

**Définition 2.7.** ([1], Définition 11.2.1, page 276)

*Soit $L/K$ une extension. Un élément de $L$ qui n'est pas algébrique sur $K$ est dit* ***transcendant*** *sur $K$.*

**Remarque** ([1], Remarque 11.2.1, page 276)

Un élément $x \in L$ est transcendant sur $K$ si et seulement si les éléments $x^n$, $n \in \mathbb{N}$, sont linéairement indépendants sur $K$. Dans ce cas, $dim_K K(x) = +\infty$ : il en est donc de même pour $dim_K L$.

**Proposition 2.3.** ([1], Proposition 11.2.1, page 277)

*Soit $K$ un corps. Le corps des fractions rationnelles $K(X)$ est une extension transcendante sur $K$.*

**Preuve.** Le seul polynôme de $K[X]$ annulé par $X$ est le polynôme nul. ∎

## 2.2 Corps algébriquement clos

**Définition 2.8.** ([2], Définition 1.17, page 69-70)

*Un corps $K$ est dit* **algébriquement clos** *s'il vérifie l'une quelconque des propriétés équivalentes suivantes :*

*1) tout polynôme $P \in K[X]$ de degré $\geqslant 1$ admet une racine dans $K$,*

*2) tout polynôme $P \in K[X]$ est produit de polynômes de degré 1,*

*3) les éléments irréductibles de $K[X]$ sont les $X - a$, $a \in K$,*

*4) si une extension $L/K$ est algébrique, alors $L = K$.*

**Exemple**

$\mathbb{Q}$ n'est pas algébriquement clos. En effet $X^2 - 1$, $X^2 + 1$ et $X^2 + X + 1$ n'ont pas de racine dans **Q**.

$\mathbb{R}$ n'est pas algébriquement clos. En effet $X^2 + 1$ et $X^2 + X + 1$ n'ont pas de racine dans $\mathbb{R}$.

$\mathbb{C}$ est algébriquement clos.

**Proposition 2.4.** ([7], Proposition 5.25, page 72)

*Tout corps algébriquement clos est infini.*

**Preuve.** Si $K$ est le corps fini $K = \{a_1, \ldots, a_p\}$, le polynôme $(X - a_1) \ldots (X - a_p) + 1$ de $K[X]$ est de degré $p \geqslant 2$, et n'a pas de racine dans $K$. ∎

**Définition 2.9.** ([8], Définition 4.2.5, page 96)

*Tout corps est contenu dans un corps algébriquement clos.*

**Définition 2.10.** ([2], Définition 1.33, page 74)

*Une extension $\overline{K}$ de $K$ est appelée une* ***clôture algébrique*** *de $K$ si elle vérifie :*

*1) $\overline{K}$ est algébriquement clos,*

*2) $\overline{K}$ est algébrique sur $K$.*

**Exemple**

$\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

## 2.3 Polynôme minimal et conjugués

**Définition 2.11.** ([3], Définition 3.6, page 58)
*Soient $K$ un corps et $x$ un élément algébrique sur $K$. L'unique polynôme $P \in K[X]$ unitaire, de degré minimal vérifiant $P(x) = 0$ s'appelle le polynôme minimal de $x$ (sur $K$). On le note $P_{min,x}$.*

Ce polynôme est bien unique : si $Q$ en est un autre, il a même degré et $P - Q$ est un polynôme de degré $< deg(P)$ dont $x$ est racine ; il est donc nul.

**Exemple**

• Le polynôme minimal sur $\mathbb{Q}$ du nombre réel $\sqrt{2}$ est $X^2 - 2$.

• Le polynôme minimal sur $\mathbb{Q}$ du nombre réel $\sqrt[3]{2}$ est $X^3 - 2$.

• Le polynôme minimal sur $\mathbb{Q}$ du nombre complexe $\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$ est $X^4 + 1$, son polynôme minimal sur $\mathbf{R}$ est $X^2 - \sqrt{2}X + 1$.

• On a vu que $\sqrt{2} + \sqrt{3}$ est algébrique (sur $\mathbb{Q}$), son polynôme minimal est
$(X - \sqrt{2} - \sqrt{3})(X - \sqrt{2} + \sqrt{3})(X + \sqrt{2} - \sqrt{3})(X + \sqrt{2} + \sqrt{3}) = X^4 - 10X^2 + 1$.

• Le polynôme minimal sur $\mathbb{Q}$ de n'importe quelle racine complexe du polynôme $X^5 - X - 1$ est $X^5 - X - 1$.

**Proposition 2.5.** *$P_{min,x}$ est irréductible dans $K[X]$.*

**Preuve.** Si on écrit $P_{min,x} = P_1P_2$, avec $P_1, P_2 \in K[X]$ unitaires, alors
$0 = P_{min,x}(x) = P_1(x)P_2(x)$, donc par exemple, $P_1(x) = 0$.
Par définition de $P_{min,x}$, on a alors $deg(P_1) \geqslant deg(P_{min,x})$, contradiction. ∎

**Proposition 2.6.** ([8], Proposition 7.25, page 97)
*Soient $K$ un corps et $x$ un élément algébrique sur $K$. Pour tout $P \in K[X]$,*

$$P(x) = 0 \Leftrightarrow P_{min,x} \mid P.$$

**Preuve.** Il est clair que si $P_{min,x} \mid P$, on a $P(x) = 0$.
Inversement, si $P(x) = 0$, on effectue la division euclidienne de $P$ par $P_{min,x}$ :
$P = P_{min,x}Q + R$ *avec* $deg(R) < deg(P_{min,x})$.
En évaluant en $x$, on obtient $0 = 0Q(x) + R(x)$ *donc* $R(x) = 0$.

Si $R$ n'est pas nul, on le divise par son coefficient dominant pour obtenir un polynôme unitaire, de degré$< deg(P_{min,x})$, qui annule $x$ : c'est absurde car cela contredit la définition du polynôme minimal. On a donc $R = 0$ et $P_{min,x}$ divise $P$. ∎

Soit $K$ un corps, Steinitz dit : il existe un corps algébriquement clos $\Omega \supset K$. Lorsque $K = \mathbb{Q}$, on peut prendre par exemple $\Omega = \mathbb{C}$. Soit $x \in \Omega$ algébrique sur $K$. Le polynôme $P_{min,x}$ est scindé dans $\Omega$. On appelle conjugué de $x$ (dans $\Omega$) les racines de $P_{min,x}$ dans $\Omega$. Les conjugués de $x$ engendrent ce qu'on a appelé le corps des racines de $P_{min,x}$. Au plus $deg(P_{min,x}) = deg_K(x)$ conjugués.

**Exemple**

Lorsque $K = \mathbb{R}$ et $\Omega = \mathbb{C}$, l'ensemble des conjugués de $z \in \mathbb{C}$ est $\{z, \overline{z}\}$.
Lorsque $K = \mathbb{Q}$, les conjugués de $\sqrt{2}$ sont $\sqrt{2}$ et -$\sqrt{2}$; le corps des racines est $\mathbb{Q}[\sqrt{2}]$.
Lorsque $K = \mathbb{Q}$, les conjugués de $\sqrt[3]{2}$ sont $\sqrt[3]{2},\ \sqrt[3]{2}\exp(i\frac{2\pi}{3})$ et $\sqrt[3]{2}\exp(i\frac{4\pi}{3})$, le corps des racines est $\mathbb{Q}[\sqrt[3]{2}, \exp(i\frac{2\pi}{3}]$.
Lorsque $K = \mathbb{Q}$, les conjugués de $\sqrt{2}+\sqrt{3}$ sont $\sqrt{2}+\sqrt{3},\ \sqrt{2}-\sqrt{3},\ -\sqrt{2}+\sqrt{3}$ et $-\sqrt{2}-\sqrt{3}$; le corps des racines est $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.
Lorsque $K = \mathbb{Q}$, les conjugués de n'importe quelle racine complexe de $X^5 - X - 2$ sont les 5 racines complexe de ce polynôme.

Un morphisme de corps entre des corps K et L est une application $u : K \to L$ telle que : $u(1_K) = 1_L,\ u(x+y) = u(x) + u(y),\ u(xy) = u(x)u(y)$.
Une telle application est nécessairement injective : si $x \in K$ est non nul, on a $u(\frac{1_K}{x})u(x) = u(\frac{1_K}{x} \cdot x) = u(1_K) = 1_L \neq 0_L$, donc $u(x)$ est non nul.

**Théorème 2.1.** ([8], Théorème 17.5.4, page 326)
*Soient $L/K$ une extension finie de corps et $\Omega$ un corps algébriquement clos contenant $K$. Il existe un morphisme de corps $L \to \Omega$ dont la restriction à $K$ est l'inclusion $K \subset \Omega$.*

On dit qu'on a prolongé l'extension $K \subset \Omega$ à $L$.

**Preuve.** Comme $L$ est un $K$-e.v de dimension finie, il existe $x_1, \ldots, x_n \in K$ tels que $L = K[x_1, \ldots, x_n]$. Procédons par récurrence sur $n$, le cas $n = 0$ vide.
Supposons $L = K[x_1, \ldots, x_n]$, avec $n \geqslant 1$ et $K'$ le sous-corps $K[x_1, \ldots, x_{n-1}]$ de $L$.
L'hypothèse de récurrence dit qu'on peut prolonger l'extension $K \subset \Omega$ à $K'$.
Il s'agit donc de prolonger l'extension $K' \to \Omega$ en un morphisme de corps $L = K'[x_n] \to \Omega$.
Posons $x := x_n$. Les éléments de $L = K'[x]$ s'écrivent tous $P(x)$, avec $P \in K'[X]$ et $P(x) = Q(x)$ si et seulement si $P - Q$ est divisible par le polynôme minimal $P_{min,x}$ de $x$ sur $K'$. On choisit une racine a de $P_{min,x}$ dans $\Omega$ et on définit un morphisme de corps par

$$K'[x] \to \Omega$$
$$P(x) \mapsto P(a).$$

Ce morphisme est bien défini car si $P(x) = Q(x)$ dans $K'[x]$, le polynôme $P - Q$ est divisible par $P_{min,x}$, donc $P(a) = Q(a)$ dans $\Omega$.
Sur le sous-corps $K'$ de $K'[x]$, c'est bien l'extension $K' \to \Omega$, donc sur $K$, c'est l'extension $K \subset \Omega$ de départ.
C'est donc un morphisme qui satisfait les propriétés demandées. ∎

**Proposition 2.7.** ([8], Proposition 12.5.4, page 236) *Soient $L/K$ une extension finie de corps, et $\Omega$ un corps algébriquement clos contenant $L$ et soit $x \in L$. L'ensemble des $u(x)$, pour tous les prolongements $u : L \to \Omega$ de l'extension $K \subset \Omega$ à $L$, est exactement l'ensemble des conjugués de $x$ dans $\Omega$.*

**Preuve.** Tout d'abord, étant donné un tel prolongement $u$, on a, comme $u$ est l'identité sur $K$ et que $P_{min,x}$ est à coefficient dans $K$, $P_{min,x}(u(x)) = u(P_{min,x}(x)) = u(0) = 0$, donc $u(x)$ doit être racine de $P_{min,x}$, c'est-à-dire un conjugué de $x$.
Ensuite, étant donné un conjugué $y$ de $x$ dans $\Omega$. la preuve de théorème précédent

montre qu'on peut prolonger l'extension $K \subset \Omega$ au corps $K[x]$ en envoyant $x$ sur $y$. On applique alors le théorème pour prolonger de nouveau chacune de ces extensions de $K[x]$ à $L$. On obtient ainsi un morphisme $u : L \to \Omega$ avec $u(x) = y$. ∎

## 2.4 Éléments primitifs

**Définition 2.12.** ([1], Définition 13.4.1, page 331)
*Soient $L/K$ une extension et $\alpha \in L$. On dit que $\alpha$ est un élément* **primitif** *de l'extension $L/K$ si $L = K[\alpha]$.*

**Lemme 2.1.** ([1], Lemme 13.4.2, page 331)
*Soient $x$ et $y$ des éléments (d'un corps algébriquement clos $\Omega$ contenant $K$) algébriques sur k. Si $x$ et $y$ sont racines des polynômes de $K[X]$ à racines simples dans $\Omega$ et si $K$ est infini, il existe $t \in K$ tel que $k[x, y] = k[x + ty]$.*

**Preuve.** Soit $P_x \in K[X]$ un polynôme annulant $x$ et à racines simples $x = x_1, \ldots, x_m$ dans $\Omega$. De même, soit $P_y \in K[X]$ un polynôme annulant $y$ et à racines simples $y = y_1, \ldots, y_n$ dans $\Omega$.
Pour $t \in K^*$, posons $z = x + ty$ et $L = K[z]$.
Il suffit de prouver $x \in L$, car alors $y = \frac{z-X}{t} \in L$, et on a bien $K[x, y] = L$.
Le polynôme $\mathbb{Q}(X) = P_y(\frac{z-X}{t})$ est à coefficients dans $L$ et annule $x$ par construction. Soit $R = pgcd(Q, P_x) \in L[X]$.
Le calcul du pgcd par l'algorithme d'Euclide montre qu'il reste le même dans tout corps contenant les coefficients de $Q$ et de $P_x$. On peut ainsi faire ce calcul dans $\Omega$. En écrivant $P_x = \prod_{i=1}^{m}(X - x_i)$, on obtient $R(X) = \prod_{i,Q(x_i)=0}(X - x_i)$, Regardons donc les racines de $\mathbb{Q}(X) = P_y(\frac{z-X}{t})$. Elles s'écrivent $z - ty_i = x + t(y - y_i)$. Donc, $Q(x_i) = 0$ si et seulement si il existe $j$ tel que $x_i = x + t(y - y_i)$ c'est-à-dire

$$(j = 1 \text{ et } x_i = x) \text{ ou } (j > 1 \text{ et } t = \frac{x_i - x}{y - y_i}).$$

Choisissons $t \in K^*$ tel que $t \neq \frac{x_i - x}{y - y_i}$, pour tout $i$ et tout $j > 1$ (c'est possible car **K** est infini).
Par construction, $x = x_1$ est la seule racine commune de $P_x$ et $Q$ de sorte que $R = pgcd(Q, P_x) = X - x$. Mais on a déjà vu $R \in \mathbf{L}[X]$, ce qui montre $x \in \mathbf{L}$. ∎

**Exemple**

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

donc $\sqrt{2}+\sqrt{3}$ est un élément primitif pour l'extension $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$.

Chapitre 3

# La correspondance de Galois

## 3.1 Généralité

**Définition 3.1.** ([7], Définition 2.23, page 34)

*Soient $L$ et $M$ deux extensions d'un même corps $K$. On appelle $K$-homomorphisme (de corps) de $L$ dans $M$ tout homomorphisme (de corps) de $L$ dans $M$ qui laisse invariant chaque élément de $K$, c'est-à-dire toute application $f : L \to M$ qui vérifie :*

- $\forall (x, y) \in L^2,\ f(x + y) = f(x) + f(y)$ *et* $f(xy) = f(x)f(y)$,
- $f(1_L) = 1_M$,
- $\forall u \in K,\ f(u) = u$.

• Lorsque $L = M$, on dit que $f$ est un $K-$endomorphisme de $L$.

• Lorsque $f$ est bijective, on dit que $f$ est un $K$-isomorphisme de $L$ dans $M$.

• Lorsque $L = M$ et $f$ est bijective, on dit que $f$ est un $K$-automorphisme de $L$.

**Proposition 3.1.** ([7], Définition 11.11, page 143) *soient $L$ un corps et $g$ un automorphisme du corps $L$. Le corps fixe $L^g := \{x \in L \,|\, g(x) = x\}$ est un sous-corps de $L$.*

**Preuve.** Il suffit de montrer que $L^g$ est un sous-anneau de $L$. On a bien $0, 1 \in L^g$. Soient $x, y \in L^g$. On a $g(x-y) = g(x) - g(y) = x - y$, donc $x - y \in L^g$. Soient $x, y \in L^g$, on a $g(xy) = g(x)g(y) = xy$, donc $xy \in L^g$. ∎

Plus généralement, si $S$ est un ensemble d'automorphismes du corps $L$, le corps fixe $L^S := \{x \in L | \forall g \in S \ g(x) = x\}$ de $S$ est aussi un sous-corps de $\mathbf{L}$ puisque c'est l'intersection $\cap_{g \in S} L^g$.

## 3.2 Lemme d'Artin

Le premier pas est de démontrer le lemme d'Artin. On se donne un corps $L$ et un sous-groupe $G$ du groupe des $L$-automorphismes. Notons $K := L^G = \{x \in L \mid \forall g \in G \ g(x) = x\}$ l'ensemble des points fixes pour l'action de G.

Avant d'énoncer le lemme, observons que $G$ agit naturellement sur $L[X]$ par la formule $g \cdot \sum_i a_i X^i = \sum_i g(a_i) X^i$.

Le calcul des polynômes fixes est immédiat : $(L[X])^G = L^G[X] = K[X]$.

Cette action respecte visiblement la somme et le produit : $g \cdot (R + PQ) = g \cdot R + (g \cdot P)(g \cdot Q)$ comme on le voit en développant chaque membre. En particulier, si $x \in L$ est racine de $P$, le polynôme $P$ est divisible par $X - x$, donc $g \cdot P$ est divisible par $g \cdot (X - x) = X - g(x)$, et $g(x)$ est racine de $g \cdot P$.

**Lemme 3.1.** ([6], lemme 7.25, page 134)

*Soit $G$ un groupe fini d'automorphismes d'un corps $L$. Pour tout $x \in L$, le polynôme $P(X) = \prod_{g \in G}(X - g(x))$ est à coefficients dans le corps $K = L^G$. En particulier, tout élément de $L$ est algébrique sur $K$, de degré $\leqslant Card(G)$.*

**Preuve.** Soit $h \in G$. On a :

$h \cdot P = \prod_{g \in G} h \cdot (X - g(x)) = \prod_{g \in G}(X - hg(x)) \overset{g'=hg}{=} \prod_{g' \in G}(X - g'(x)) = P$

car $g \mapsto g'$ est une bijection de $G$ qui ne fait que permuter les facteurs de $P$. Le polynôme $P$ est ainsi fixé sous $G$, donc à coefficients dans $K$. ∎

**Théorème 3.1.** ([6], Théorème 7.26, page 134-135)

*Soit $G$ un groupe fini d'automorphismes d'un corps $L$ de caractéristique nulle. Posons $K := L^G$.*

*1) L'extension $L/K$ est algébrique et les conjugués de $x \in L$ (dans un corps algébriquement clos contenant $L$) sont les $g(x)$, pour $g$ décrivant $G$. En particulier, ce sont des éléments de $L$.*

*2) L'extension $L/K$ est finie de degré $Card(G)$.*

*3) Le groupe $G$ est égal au groupe $Aut_K(L)$ des automorphisme $K$-linéaires de $L$.*

**Preuve.** Soit $x \in L$. D'après le lemme 3.1, le polynôme $\prod_{g\in G}(X - g(x))$ est dans $K[X]$ et annulé par $x$. C'est donc un multiple du polynôme minimal $P_{min,x} \in K[X]$. Ce dernier est ainsi scindé dans $L$ et ses racines, c'est-à-dire les conjugués de $x$, sont parmi les $g(x)$, avec $g \in G$.
Inversement, pour tout $g \in G$, $g(x)$ est racine du polynôme $g \cdot P_{min,x} = P_{min,x}$, donc c'est un conjugué de $x$. Cela montre le premier point. ∎

Pour montrer le second point, nous commençons par le résultat suivant.

**Lemme 3.2.** ([6], Lemme 7.27, page 136)
*Soit $L/K$ une extension algébrique de corps de caractéristique nulle. Supposons qu'il existe un entier $n$ tel que tout élément de $L$ est algébrique de degré $\leqslant n$ sur $K$, alors $L/K$ est une extension finie de degré $\leqslant n$.*

**Preuve.** Soit $x \in L$ de degré maximal ($\leqslant n$) sur $K$ (qui existe par hypothèse). Montrons $L = K[x]$. Soit $y \in L$ et soit $M = K[x, y] \subset L$ le corps engendré par $x$ et $y$. C'est une extension finie de $K$, qui est donc engendrée par un $z \in K[x; y]$ (théorème de l'élément primitif). Comme $K[x] \subset K[z]$, on a $deg(x) \leqslant deg(z)$. Par maximalité, on a $deg(x) = deg(z)$ et donc $K[x] = K[z]$. On conclut ainsi $y \in k[x, y] = k[z] = k[x]$. ∎

**Preuve du théorème 3.1**

2) Comme tous les éléments de $L$ sont de degré $\leqslant Card(G)$ d'après le lemme 3.1, l'extension $L/K$ est donc finie, engendrée par un élément primitif $x \in L$, de degré $[L : K] \leqslant Card(G)$. Comme $L = K[x]$ et que le groupe $G' := Aut_K(L)$ agit comme l'identité sur $K$ par définition, tout élément $g'$ de $G'$ est déterminé par $g'(x)$, qui est

racine du polynôme $g' \cdot P_{min,x} = P_{min,x}$, donc un conjugué de $x$. L'application

$$G' \to \{conjugues\ de\ x\}$$
$$g' \mapsto g'(x)$$

est ainsi injective. Comme $x$ a au plus (en fait ici exactement) $deg(x) = [L : K]$ conjugués, on en déduit $Card(G') \leqslant [L : K]$.
Comme $K = L^G$, on a $G \subset G'$ et donc $Card(G) \leqslant Card(G') \leqslant [L : K]$. d'où $Card(G) = [L : K]$.
3) Comme on sait aussi $[L : K] \leqslant Card(G)$, on a $G = G' = Aut_K(L)$ et $Card(G) = [L : K]$, ce qui achève la preuve du lemme d'Artin. ∎

## 3.3 Extensions galoisiennes

**Définition 3.2.** ([6], Définition 7.22, page 133)
*Une extension finie $L/K$ de corps de caractéristique nulle est dite galoisienne si les conjugués de tout élément de $L$ sont dans $L$.*

On fixe désormais un corps de caractéristique nulle $K$ et un corps algébriquement clos $\Omega$ contenant $K$.

**Proposition 3.2.** *Les extensions galoisiennes de $K$ sont exactement les corps de racines des polynômes de $K[X]$.*

**Preuve.** Soit $L = K[x_1, \ldots, x_n]$ le corps des racines d'un polynôme $P = \prod_{i=1}^{n}(X - x_i) \in K[X]$.
Pour montrer que l'extension $L/K$ est galoisienne, il faut montrer qu'étant donné $y \in L$, tous les conjugués de y (dans $\Omega$) sont dans $L$.
Un tel conjugué s'écrit $\sigma(y)$, où $\sigma$ est un prolongement à $L$ de l'extension $K \subset \Omega$.
De $y \in K[x_1, \ldots, x_n]$, on tire $\sigma(y) \in \sigma(K[x_1, \ldots, x_n]) = K[\sigma(x_1), \ldots, \sigma(x_n)]$.
Comme $\prod_{i=1}^{n}(X - \sigma(x_i)) = \sigma \cdot P = P = \prod_{i=1}^{n}(X - x_i)$, alors $\sigma$ permute les $x_i$, de sorte que $K[\sigma(x_1), \ldots, \sigma(x_n)] = K[x_1, \ldots, x_n] = L$ et $\sigma(y) \in L$. ∎

**Définition 3.3.** ([6], Définition 7.3, page 124)
*Soit $L$ une extension finie et galoisienne d'un corps $K$ de caractéristique nulle et soit $P$ un polynôme à coefficients dans $K$.*

*1) Le groupe de Galois $Gal(L/K)$ est le groupe $Aut_K(L)$ des $K$-automorphismes de $L$.*

*2) Le groupe de Galois $Gal_K(P)$ est le groupe de Galois du corps des racines de $P$.*

Avec les notations du lemme d'Artin, on a $Gal(L/L^G) = G$, ce qui entraîne la jolie formule tautologique $L^{Gal(L/K)} = K$, tautologique car $K = L^G$ par définition dans ce contexte.
Remarquablement, cette formule est toujours vraie, et c'est la seconde clef de la correspondance de Galois comme on va le voir bientôt.

**Lemme 3.3.** *Soit $L/K$ une extension galoisienne (contenue dans $\Omega$).*
*On a $Hom_K(L, \Omega) = Gal(L/K)$. En particulier, les conjugués de $x \in K$ sont les $g(x)$, pour $g$ décrivant $Gal(L/K)$.*

**Preuve.** On a $Gal(L/K) = Aut_K(L) \subset Hom_K(L, \Omega)$.
Inversement, la réunion des $\sigma(L)$, lorsque $\sigma$ décrit l'ensemble $Hom_K(L, \Omega)$ des prolongements à $L$ de l'extension $K \subset \Omega$, est l'ensemble des conjugués des éléments de $L$, donc est $L$ car l'extension $L/K$ est galoisienne. D'où $\sigma \in Hom_K(L, \Omega) \subset Hom_K(L, L) \subset Aut_K(L) = Gal(L/K)$. ∎

**Proposition 3.3.** ([6], Remarque 7.23, page 133)
*Soit $L/K$ une extension galoisienne. On a les propriétés suivantes :*

*1)* $L^{Gal(L/K)} = K$.

*2)* $[L : K] = Card(Gal(L/K))$.

**Preuve.** Soit $x \in L$ invariant sous l'action du groupe de Galois. Alors, tous ses conjugués sont égaux à $x$ qui est donc la seule racine de son polynôme minimal. Comme le polynôme minimal est à racines simples, il s'écrit $P_{min,x} = X - x$ et appartient à $K[X]$ : on a donc $x \in K$.
Pour le second point, on applique le lemme d'Artin à $L$ et au groupe $G = Gal(L/K)$.

∎

## 3.4 La correspondance de Galois

Soit $L/K$ une extension galoisienne (de caractéristique nulle) de groupe de Galois $G$.

On considère les applications

$$\gamma : \{sous - groupe\ de\ G\} \to \{sous - extensions\ de\ L/K\}$$
$$H \mapsto L^H = \{invariants\ de\ L\ sous\ H\}$$

et

$$\phi : \{sous - extension\ de\ L/K\} \to \{sous - groupe\ de\ G\}$$
$$M \mapsto Gal(L/M).$$

**Théorème 3.2.** ([7], Théorème 11.17, page 144)

*1) Avec les notations précédentes, $\gamma$ et $\phi$ sont des bijections strictement décroissantes inverses l'une de l'autre.*

*2) Pour tout $g \in G$ et toute sous-extension $M$ de $L/K$, on a : $\phi(g(M)) = Gal(L/g(M)) = gGal(L/M)g^{-1} = g\phi(M)g^{-1}$.*

*3) L'extension $M/K$ est galoisienne si et seulement si le sous-groupe $Gal(L/M)$ est distingué dans $Gal(L/K)$. Dans ce cas, le morphisme naturel de restriction $Gal(L/K) \to Gal(M/K)$ s'identifie à la surjection canonique*
*$Gal(L/K) \to Gal(L/K)/Gal(L/M)$.*

**Preuve.** Les décroissances (larges) sont évidentes. Par ailleurs, on a
$\gamma \circ \phi(M) = \gamma(Gal(L/M)) = L^{Gal(L/M} = M$, d'après le calcul des invariants pour $L/M$, de sorte que $\gamma \circ \phi = Id$. Ensuite, $\phi \circ \gamma(H) = \phi(K^H) = Gal(L/L^H) \overset{lemme\ d'Artin}{=} H$ prouvant $\phi \circ \gamma = id$ et donc le premier point.
Dire $h \in Gal(L/g(M))$, c'est dire $\forall \lambda \in M\ \ h(g(\lambda)) = g(\lambda)$, ou encore $\forall \lambda \in M\ g^{-1}hg(\lambda) = \lambda$, c'est-à-dire $g^{-1}hg \in Gal(L/M)$, ce qui prouve le second point.
On sait que les conjugués de $\lambda \in M$ sont les $g(\lambda)$, pour $g$ décrivant $Gal(L/K)$. Donc, $M/L$ est galoisienne si et seulement si $g(M) = M$ pour tout $g$ ou encore, grâce à la bijectivité de $\phi$, si $g\phi(M)g^{-1} = \phi(g(M)) = \phi(M)$ pour tout $g$, ce qui par définition signifie $Gal(L/M)\ est$ distingué $dans\ Gal(L/K)$.
Pour le dernier point, si $M/K$ est galoisienne, ou $Gal(L/M) \lhd Gal(L/K) = G$, tout

$g \in G$ laisse stable $M$. L'application $g \mapsto g_{|M}$ de restriction à $M$ définit donc bien un morphisme $Gal(L/K) \to Gal(M/K)$.

Il est surjectif (théorème de prolongement des morphismes) et son noyau est l'ensemble des $g \in G$ tels que $g_{|M} = id$, soit $Gal(L/M)$. La propriété universelle du quotient assure qu'on a ainsi défini un isomorphisme canonique

$$Gal(L/K)/Gal(L/M) \to Gal(M/K).$$ ∎

**Corollaire 3.1.** *Une extension finie de corps, de caractéristique zéro, $L/K$ a un nombre finie de sous-extensions.*

**Preuve.** Par le théorème de l'élément primitif, on peut écrire $L = K[x]$. Soit $L' := corps\,des\,racines\,de\,(P_{min,x,k})$. C'est une extension galoisienne de $K$ contenant $L$, de groupe de Galois $G$.

Par la correspondance de Galois, les sous-extensions de $L'/K$ correspondent (bijectivement) aux sous-groupes de $G$, qui sont en nombre finie car $G$ est finie. Il n'y a donc a fortiori qu'un nombre finie de sous-extensions de $L/K$. ∎

## 3.5 Groupe de Galois et groupe symétrique

Soit $P$ un polynôme de $K[X]$. Notons $L$ son corps des racines et numérotons ses racines $x_1, \ldots, x_n$.

Soit $G = Gal(L/K)$ le groupe de Galois de $P$. Comme pour tout $g \in G$, il existe une unique permutation $\gamma \in S_n$ telle que pour tout $i$, $g(x_i) = x_{\gamma(i)}$. On définit ainsi un morphisme de groupes $G \to S_n$, injectif car les $x_i$ engendrent $L$.

**Corollaire 3.2.** *Toute numérotation des racines de $P$ définit un morphisme injectif de groupes $G \to S_n$.*

**Remarque**

En général, des numérotations différentes conduisent à des plongements conjugués, ce qui ne change rien dans l'étude du groupe de Galois. La plupart du temps, la numérotation des racines sera donc implicite.

**Exemple**

Soit $P = X^2 + aX + b \in K[X]$. Notons $L$ son corps des racines.

• On a $L = K[\delta]$ où $\delta$ désigne une racine carrée du discriminant $a^2 - 4b$.

• Si $a^2 - 4b$ est un carré dans $K$, le groupe de Galois est réduit à $id$.

• Si $a^2 - 4b$ n'est pas un carré dans $K$, le groupe de Galois est de cardinal 2, engendré par l'automorphisme $\sigma$ tel que $\sigma(\delta) = -\delta$. L'image de $\sigma$ dans $S_2$ est la transposition $(1, 2)$.

**Proposition 3.4.** *Avec les notations précédentes, on a :*

*1) $discr(P) \neq 0$ si et seulement si $P$ est à racines simples ;*

*2) $discr(P) \in K$ ;*

*3) si $P$ est à racines simples, $discr(P)$ est un carré dans $K$ si et seulement si $Gal_K(P) \subset A_n$.*

# BILBLIOGRAPHIE


[**1**] Daniel Guin, Thomas Hausberger, *Algèbre T1 : Groupes, Corps et Théorie de Galois.*, EDP Sciences, 2008, Enseignement SUP-Maths.

[**2**] Daniel Perrin, *Cours d'algèbre*, Ellipses Marketing 1998, CAPES / Agrégation.

[**3**] Jean-Jacques Risler, Pascal Boyer, *algèbre pour la licence 3 : groupes, anneaux, corps*, Dunod, 2006, Sciences Sup.

[**4**] Alberto Mînguez, *Théorie de groupes*, Jussieu, Institut de Mathématiques de Jussieu, Université Paris 6.

[**5**] François Dumas, *Algèbre : groupe et anneaux 1*, Université Blaise Pascal U.F.R. Sciences et Technologies, 2007.

[**6**] Josette Calais, *Extensions de corps : Théorie de Galois*, Ellipses Marketing, 2006, Mathématiques à l'Université.

[**7**] Ivan Gozard, *Théorie de Galois*, Ellipses Marketing, 2009, Mathématiques à l'Université.

[**8**] Patrice Tauvel, *Corps commutatifs et théorie de Galois* , Calvage et Mounet, 2008, Mathématiques en devenir.

[**9**] Edmon Ramis, Claude Deschamps, Jacques Odoux *Cours de mathématiques spéciales 1*, Dunod, 2017.

[**10**] Jean-Pierre Escofier, *Théorie de Galois : Cours et exercices corrigés*, Dunod, 2004, Sciences Sup.