Compte rendu de stage de L2 : Corps et Théorie de Galois

Malik YAHAIOUI

Juillet 2025

1 Introduction

Je remercie Mathilde Herblot pour sa disponibilité et ses conseils tout au long du stage. Je remercie également Vincent de Daruvar, qui a été le premier à me conseiller de travailler sur ce sujet.

L'objectif de ce stage était de découvrir la théorie de Galois au travers de la théorie des corps. Il a nécessité un travail préalable sur les corps et les anneaux qui sont au programme de L3. Ce compte rendu retrace les principales notions étudiées, de la définition d'un corps à la correspondance de Galois. Il couvre toutes les notions nécessaires à la correspondance de Galois qui ne sont pas au programme de L2. Quelques exemples sont présents ainsi que des applications de la correspondance de Galois à la fin du document. Certaines preuves utilisant les anneaux quotients comme le théorème d'isomorphisme ne sont pas nécéssaires en elles mêmes à la compréhension de la théorie de Galois mais sont tout de même présentes dans ce document car utilisées dans d'autres démonstrations centrales.

2 Théorie des corps

2.1 Terminologie

Soit A un ensemble $(+, \cdot)$ deux lois de composition internes sur A et $I \subseteq A$.

Définition 2.1.1 (Anneau). *On dit que A est un anneau si $(A; +)$ est un groupe abélien, $(A; \cdot)$ est un monoïde et $\cdot$ se distribue sur $+$. On notera 0_A le neutre de A pour l'addition et 1_A le neutre de A pour le produit.*

Définition 2.1.2 (Idéal). *Si A est un anneau, I est un idéal de A si $(I, +)$ est un sous-groupe de $(A, +)$ et $\forall x \in I, \forall a \in A, x \cdot a \in I$ et $a \cdot x \in I$*

Définition 2.1.3 (Quotient par un idéal). *Pour A un anneau et I un idéal de A. On définit $A/I = \{x + I \mid x \in A\}$ avec $x + I = \{x + i \mid i \in I\}$. On notera $\overline{x} = x + I$ qu'on appellera classe de x.*

Remarque. *Si on prend x et y dans A, $\overline{x} = \overline{y}$ si et seulement si $x - y \in I$*

Proposition 2.1.4. *Soit A un anneau et I un de ses idéaux, $(A/I, +, \cdot)$ avec $\overline{x} + \overline{y} = \overline{x+y}$ et $\overline{x} \cdot \overline{y} = \overline{xy}$ est un anneau*

Preuve. Montrons d'abord que l'addition est bien définie :
Soit $a' \in \overline{a}$, $b' \in \overline{b}$, alors $\exists i_1 i_2 \in I$ tels que $a' = a + i_1$ et $b' = b + i_2$. Donc $a + b - (a' + b') \in I$ donc $\overline{a' + b'} = \overline{a + b}$, i.e. $\overline{a'} + \overline{b'} = \overline{a} + \overline{b}$. L'addition est bien définie.
Produit bien défini :
Reprenons a' et b', $\overline{a'} \cdot \overline{b'} = \overline{a'b'} = \overline{ab + i_1 b + i_2 a + i_1 i_2} = \overline{ab}$ Le produit est bien défini.
Les associativités du produit et de la somme viennent directement de celles du produit et de la somme dans A. De même pour la commutativité de la somme et la distributivité du produit sur la somme.
Pour les neutres : $\overline{1} \cdot \overline{a} = \overline{1 \cdot a} = \overline{a}$ et $\overline{0} + \overline{a} = \overline{0 + a} = \overline{a}$. On a bien une structure d'anneau $\square$

Définition 2.1.5 (Morphisme d'anneau)**.** *Soient $(E, +, \cdot)$ et $(F, \oplus, \times)$ deux anneaux, $f : E \to F$, f est un morphisme d'anneau si :*

- $\forall x, y \in E, f(x + y) = f(x) \oplus f(y)$
- $\forall x, y \in E, f(x \cdot y) = f(x) \times f(y)$
- $f(0_E) = 0_F$ *et* $f(1_E) = 1_F$

Définition 2.1.6 (Corps)**.** *$(A, +, \cdot)$ est un corps si c'est un anneau et si $(A \setminus \{0_A\}, \cdot)$ est un groupe. On dit d'une application que c'est un morphisme de corps si c'est un morphisme d'anneaux entre deux corps.*

2.2 Extensions

Définition 2.2.1 (Extension de corps)**.** *Soit K un corps, on dit que L est une extension de K si L est un corps et que $K \subseteq L$.*

Dans toute cette partie, on considérera une extension $K \subseteq L$

Définition 2.2.2 (Degré d'extension)**.** *On définit le degré de $K \subseteq L$ comme la dimension de L comme K espace vectoriel. On le note $[L : K]$.*

Définition 2.2.3 (Algébrique/transcendant)**.** *Soit $x \in L$, x est dit algébrique sur K s'il existe un polynôme non nul à coefficients dans K qui l'annule. Il est dit transcendant sinon.*

Définition 2.2.4. *On dit que $K \subseteq L$ est :*

- *Finie, si $[L : K]$ est entier.*
- *Algébrique, si tous les éléments de L sont algébriques sur K.*

Exemple. *L'extension $\mathbb{R} \subseteq \mathbb{C}$ est finie de degré 2. En tant que $\mathbb{R}$-espace vectoriel, $\mathbb{C} = vect(1, i)$. L'extension $\mathbb{Q} \subseteq R$ est infinie, les puissances de $\mathbb{Q}$ sont dénombrables et $\mathbb{R}$ est indénombrable.*

Théorème 2.2.5 (Base télescopique)**.** *On suppose $K \subseteq L$ finie et U une extension finie de L, on a $K \subseteq U$ finie de degré $[U : L] \cdot [L : K]$.*

Preuve. On note $n = [L : K]$ et $m = [U : M]$.
On pose $(l_1, l_2, ...l_n)$ une base de L en tant que K-ev, et $(u_1, u_2, ...u_m)$ une base de U en tant que L-ev.
Soit $x \in U$, $\exists!(\lambda_1, ..., \lambda_m) \in L^m$ tel que

$$x = \sum_{k=1}^{m} \lambda_k u_k$$

Or, pour $k \in [m]$, $\exists!(\mu_1, ..., \mu_n)$ tels que

$$\lambda_k = \sum_{i=1}^{n} \mu_i l_i$$

.
Donc

$$x = \sum_{k=1}^{m} \sum_{i=1}^{n} \mu_i l_i u_k = \sum_{i=1}^{n} \mu_i \sum_{k=1}^{m} l_i u_k$$

.
Conclusion : x s'écrit d'une unique façon comme combinaison linéaire des $(l_i u_k)_{i \in [n], k \in [m]}$. □

Proposition 2.2.6. *Toute extension finie est algébrique.*

Preuve. On note $n = [L : K]$, pour $x \in L$, la famille $(1, x, x^2, ..., x^n)$ est liée sur le K-espace vectoriel L, donc il existe un polynôme non nul à coefficients dans K qui annule x. □

Définition 2.2.7 (Polynôme minimal)**.** *Pour tout $x \in L$, il existe un unique $P \in K[X]$ unitaire non nul tel que $P(x) = 0$, et pour $0 \leq d < \deg(P)$, P est de degré $d \Rightarrow P(x) \neq 0$. P est appelé polynôme minimal de x sur K, on le note $\Pi_{x,K}$. On appelle degré de x sur K le degré de son polynôme minimal. Les autres racines de $\Pi_{x,K}$ sont appelées K-conjugués de x.*

Preuve. Soit $x \in L$, comme l'extension est algébrique, il existe P non nul qui annule x, comme $\deg(p)$ est fini, on peut trouver d tel que tout polynôme de degré entier inférieur à d n'annule pas x.
Soient P_1, $P_2 \in K_d[X]$ unitaires qui annulent x. Par minimalité de d on a $\deg(P_1) = \deg(P_2) = d$, on a $P_1 - P_2(x) = 0$ et $\deg(P_1 - P2) < d$ (car tous les deux unitaires), si $P_1 \neq P_2$ on a alors un polynôme non nul de degré $< d$, contradiction avec la minimalité de d. □

Exemple. $\sqrt{2}$ *est algébrique sur $\mathbb{Q}$ de polynôme minimal $X^2 - 2$.*

Proposition 2.2.8. *Pour tout $x \in L$, $P \in K[X]$ annulé par x, $\Pi_{x,K}$ divise P. L'ensemble des polynômes de $K[X]$ annulateurs de x est donc un idéal engendré par $\Pi x, K$.*

Preuve. Soit $P \in K[X]$ qui annule x, comme $deg(P) \geq deg(\Pi_{x,K})$ on peut effectuer la division euclidienne de P par $\Pi_{x,K}$.
Il existe alors $Q, R \in K[X]$ tels que $deg(R) < deg(\Pi_{x,K})$ et $P = \Pi_{x,K}Q + R$, ainsi :

$$0 = P(x) = \Pi_{x,K}(x)Q(x) + R(x) = R(x)$$

Donc R annule x, par minimalité de $\Pi_{x,K}$, R=0.
On a naturellement une structure d'idéal, si un polynôme annule x, son produit avec n'importe quel polynôme annule x.

□

Théorème 2.2.9. *Les éléments de L algébriques sur K forment un sous-corps de L.*

Preuve. Montrons d'abord que la somme et le produit de deux éléments algébriques est algébrique.

Soient $x, y \in L$ algébriques sur K, on pose $K[x, y] = vect_K(x^i y^j)_{i,j \in \mathbb{N}}$, et on note d_1 et d_2 respectivement les degrés de x et de y.
Comme x est algébrique, x^i peut s'exprimer comme combinaison linéaire des $(x^k)_{k \in [d_1]}$, réciproquement pour y.
Donc $K[x, y] = vect(x^i y^j)_{(i,j) \in [d_1] \times [d_2]}$. C'est un K-ev de dimension finie.

Or, x+y et xy appartiennent à K[x,y]. Ainsi $((x + y)^n)_{0 \leq n \leq [d_1 d_2]}$ est une famille liée, donc il existe un polynôme à coefficient dans K qui annule $x + y$. Même raisonnement pour xy.

Montrons ensuite que le caractère algébrique est stable par passage à l'inverse:
Soit $x \in L$ algébrique, $P = \sum_{i=0}^{d} a_i X^i$ son polynôme minimal. On pose $Q = \sum_{i=0}^{d} a_{d-i} X^i$, alors

$$x^d Q(x^{-1}) = \sum_{i=0}^{d} a_{d-i} x^{d-i} = P(x) = 0$$

Donc x^{-1} est bien algébrique. □

Exemple. $\overline{\mathbb{Q}}$ *L'ensemble des nombres complexes algébriques sur $\mathbb{Q}$ est un corps.*

Définition 2.2.10. *Pour $x \in L$ on définit $K[x] = \{P(x) \mid P \in K[X]\}$*

Lemme 2.2.11. *Soit $x \in L$ non nul et algébrique sur K, alors $x^{-1} \in K[x]$*

Preuve. Montrons d'abord que $\Pi_{x,K}(0) \neq 0$:
On suppose par l'absurde que c'est le cas. Alors $X \mid \Pi_{x,K}$, i.e. $\exists P \in K[X]$ tel que :

$$\Pi_{x,K} = XP$$

En composant par x on a :

$$XP(x) = \Pi_{x,K}(x) = 0$$

et $x \neq 0$ donc $P(x) = 0$ et $\deg(P) < \deg(\Pi_{x,K})$ absurde par minimalité.

On note $\Pi_{x,K} = \sum_{k=0}^{d} a_k X^k$, on sait que :

$$\begin{aligned} a_0 x^{-1} &= \sum_{k=1}^{d} a_k x^{k-1} \\ \Rightarrow x^{-1} &= \sum_{k=1}^{d} a_k x^{k-1} \quad (\text{car } a_0 \neq 0) \\ \Rightarrow x^{-1} &= \sum_{k=0}^{d-1} a_{k+1} x^k \end{aligned}$$

□

Théorème 2.2.12. *Pour $x \in L$, $K[x]$ est un corps si x est algébrique.*

Preuve. Les sommes et produits de polynômes en x restent des polynômes en x et le produit se distribue bien sur la somme. Soit $a \in K[x]$ non nul, on sait que a est algébrique (2.2.7) et que $a^{-1} \in K[a]$ par le lemme, la composée de deux polynômes est un polynôme donc a^{-1} est un polynôme en x. □

Proposition 2.2.13. *Soit $x \in L$, algébrique non nul. Alors $[K[x] : K] = \deg(\Pi_{x,K})$.*

Preuve. On pose $d = deg(\Pi_{x,K})$, on sait que la famille $(1, x, ..., x^{d-1})$ est libre sinon on aurait un polynôme de $K[X]$ de degré d-1 annulant x, impossible par minimalité de d. Et on sait que la famille $(1, x, ..., x^d)$ est liée comme $\Pi_{x,K}$ annule x.
Donc $deg(\Pi_{x,K})$ est le cardinal maximal d'une famille libre, c'est bien la dimension de $K[x]$. □

2.3 Corps et polynômes

Dans cette partie, on considère un corps K.

Définition 2.3.1. *Soit Ω une extension de K. On dit que Ω est une clôture algébrique de K si :*

- *$K \subseteq \Omega$ est algébrique.*

- *Tout polynôme à coefficient dans Ω s'annule dans Ω (ie Ω est algébriquement clos).*

Exemple. *$\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$ et $\overline{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$. On a ici un exemple de clôture de degré fini et un de degré infini.*

Théorème 2.3.2 (Théorème de Steinitz (admis))**.** *Tout corps admet une clôture algébrique.*

Définition 2.3.3 (Corps de rupture)**.** *Soit $P \in K[X]$. Une extension L est appelée corps de rupture de P s'il existe $a \in L$ tel que $P(a) = 0$ et $L = K[a]$.*

Définition 2.3.4 (Corps de décomposition)**.** *Soit $P \in K[X]$. Une extension L est appelée corps de décomposition de P si elle contient $\{a_1, a_2, ..., a_n\}$ l'ensemble des racines de P et que $L = K[a_1, a_2, ..., a_n]$.*

Remarque. *Les notions de corps de rupture et de corps de décomposition sont liées mais distinctes. Si on prend le polynôme $P = X^3 - 2$. $\mathbb{Q}[\sqrt{3}]$ est un corps de rupture de P par définition, mais ce n'est pas son corps de décomposition ; en effet $P(j\sqrt{3}) = 0$, $j\sqrt{3} \notin R$ et $\mathbb{Q}[\sqrt{3}] \subset R$, donc $j\sqrt{3} \notin \mathbb{Q}[\sqrt{3}]$. Il ne contient donc pas toutes les racines, contrairement au corps de décomposition.*

Définition 2.3.5 (Extension séparable)**.** *Soit L une extension algébrique de K. $x \in L$ est dit séparable sur K si les racines de $\Pi_{x,K}$ dans une clôture algébrique sont simples. On dit que $K \subseteq L$ est séparable si tout $x \in L$ est séparable sur K.*

Lemme 2.3.6. *Soit L une extension de K. A et B dans $K[X]$. Alors le pgcd de A et B dans $K[X]$ est le même que celui dans $L[X]$.*

Preuve. On considère que le pgcd est unitaire pour garantir l'unicité.

On considère P le pgcd de A et B dans $K[x]$ et Q leur pgcd dans $L[X]$. On sait qu'il existe $D_1, D_2 \in K[X]$ tel que :

$$A = D_1 P \text{ et } B = D_2 P$$

Or par Bézout, $\exists U, V \in L[X]$ tels que :

$$Q = AU + BV = P(D_1 U + D_2 V)$$

donc $P \mid Q$

Comme P est le pgcd de A et B dans $K[X]$, on sait qu'il existe $U, V \in K[X]$ tels que :

$$P = AU + BV$$

et par un raisonnement analogue, Q divise A et B donc il divise P.

Ainsi comme les deux polynômes se divisent l'un l'autre et qu'ils sont unitaires, ils sont égaux. □

Proposition 2.3.7. *Pour L une extension de K, $x \in L$ est séparable sur K si et seulement si $\Pi_{x,K}$ est premier avec sa dérivée.*

Preuve. Par définition, x est séparable si et seulement si $\Pi_{x,K}$ est premier avec sa dérivée dans une clôture algébrique. Ce qui équivaut à être premiers dans K par le lemme. □

Proposition 2.3.8. *Soit $P \in K[X]$ à racines simples, le corps de décomposition de P est une extension séparable de K.*

Preuve. Soit α une racine de P, $\Pi_{x,K}$ divise P donc est aussi à racines simples. Si on note $(x_1, ..., x_n)$ les racines de P, et E le corps de décomposition de P, on sait que $E = K[x_1, ..., x_n]$.

Montrons que $K \subseteq K[x_1]$ est séparable :
Soit $\beta \in K[x_1]$, on sait que β est algébrique donc que $K[\beta]$ est une extension de K, ainsi comme x_1 est algébrique sur K, il l'est aussi sur $K[\beta]$, on pose donc $\Pi_{x_1,K[\beta]} = \sum_{k=0}^{d} a_k X^k$.

$$\sum_{k=0}^{d} a_k x_1^k = 0$$

Comme pour chaque a_k il existe $P_k \in K[X]$ tel que $a_k = P_k(\beta) =$, on a

$$\sum_{k=0}^{d} Q_k(\beta) x_1^k = 0$$

Or c'est aussi un polynôme en β à coefficients dans $K[x_1]$. Et il est bien à racines simples.

□

Définition 2.3.9 (Extension normale)**.** *On dit qu'une extension L algébrique de K est normale si pour tout $x \in L$, les K-conjugués de x sont dans L.*

Proposition 2.3.10. *Si $K \subseteq L$ est normale, alors pour $x \in L$, $\Pi_{x,k}$ est le polynôme minimal des K-conjugués de x.*

Preuve. Soit $\alpha \in L$ un K-conjugué de x, d'après (2.2.8) on sait qu'il existe $Q \in K[X]$ tel que :

$$\Pi_{x,K} = \Pi_{\alpha,K} Q$$

En évaluant en x on a :

$$0 = \Pi_{x,K}(x) = \Pi_{\alpha,K}(x) Q(x) \tag{1}$$

Or, $\deg(\Pi_{\alpha,K}) \leq \deg(\Pi_{x,K})$, donc par minimalité de $\Pi_{x,K}$, Q est de degré 0. Et comme les deux polynômes minimaux sont unitaires $Q = 1$. □

Définition 2.3.11. *On dit qu'une extension L de K est galoisienne si elle est normale et séparable.*

3 Théorie de Galois

3.1 Prolongement de morphismes

On considère $K \subseteq L$ une extension finie et Ω une clôture algébrique de K.

Proposition 3.1.1. *Il y a au plus $[L : K]$ morphismes $L \to \Omega$ qui fixent K (cad $f_{\{K\}} = Id_K$). On appelle ceux-ci des K-morphismes.*

Preuve. On sait qu'il existe $x_1, x_2, ..., x_n \in L$ tels que $L = K[x_1, x_2, ...x_n]$.
Pour construire φ un K-morphisme, on choisit d'abord l'image de x_1 :
Si $\Pi_{x_1,K} = \sum_{k=0}^{d} a_k X^k$ alors pour $x \in L$:

$$\varphi(\Pi_{x_1,K}) = \varphi(\sum_{k=0}^{d} a_k X^k) = \sum_{k=0}^{d} a_k \varphi(X)^k \text{car } \varphi \text{ est un K-morphisme}$$

En particulier :

$$\Pi_{x_1,K}(\varphi(x_1)) = \varphi(\Pi_{x_1,K}(x_1)) = 0$$

$\varphi(x_1)$ est donc un K-conjugué de x_1, on a donc au plus $[K[x_1] : K]$ choix.

Pour l'image $\varphi(x_2)$, si $\Pi_{x,K[x_1]} = \sum_{k=0}^{m} b_k X^k$ (on a l'existence car x est algébrique sur K et $K \subseteq K[x1]$) alors :

$$0 = \varphi(0) = \varphi(\Pi_{x,K[x_1]}(x_2)) = \sum_{k=0}^{m} \varphi(b_k)\varphi(x_2)^k$$

Ainsi, $\varphi(x_2)$ est racine de $Q = \sum_{k=0}^{m} \varphi(b_k)\varphi(X)^k$. Or, comme $\varphi(b_k) \neq 0$ pour $b_k \neq 0$ car φ est un morphisme de corps, $\deg(Q) = deg(\Pi_{x_2,K[x_1]})$ on a donc $[K[x_1, x_2] : K[x_1]]$ choix.
En continuant de proche en proche jusqu'à x_n, si on pose N le nombre de K-morphismes, on a :

$$N \leq [K[x_1] : K] \cdot \Pi_{i=2}^{n} [K[x_1, ..., x_i], K[x_1, ..., x_{i-1}]] = [K[x_1, x_2, ...x_n], K] = [L, K]$$

□

Proposition 3.1.2. *On note N le nombre de K-morphismes $L \to \Omega$. Les assertions suivantes sont équivalentes :*

- $N = [L : K]$
- $K \subseteq L$ *est séparable*
- *Il existe $x_1, ..., x_n \in L$ séparables sur K tels que $L = K[x_1, ..., x_n]$.*

Preuve. Pour un polynôme $P \in L[X] \mid P = \sum_{k=0}^{d} a_k X^k$, et φ un morphisme de corps $L \to \Omega$, on note $\varphi(P) = \sum_{k=0}^{d} \varphi(a_k)\varphi(X)^k$.

En notant $L = K[x_1, ..., x_n]$ on a précédemment montré que $N = [L : K]$ si et seulement si $\Pi_{x_1,K}$ était à racines simples, $\varphi(\Pi_{x_2,K[x_1]})$ était à racines simples, etc...
On suppose que x_2 est séparable sur $K[x_1]$ montrons que $\varphi(\Pi_{x_2,K[x_1]})$ est à racines simples : On sait que $\Pi_{x_2,K[x_1]}$ est premier avec sa dérivée, on écrit une relation de Bézout. Il existe $A, B \in K[x_1][X]$ tels que

$$\Pi_{x_2,K[x_1]}A + \Pi'_{x_2,K[x_1]}B = 1$$

En composant par φ, on a :

$$\varphi(\Pi_{x_2,K[x_1]})\varphi(A) + \varphi(\Pi'_{x_2,K[x_1]}\varphi(B)) = 1$$

Donc $\varphi(\Pi_{x_2,K[x_1]})$ est premier avec sa dérivée.
En utilisant la même méthode récursivement jusqu'à x_n, on montre que $N = [L : K]$ si x_1 est séparable sur K, x_2 est séparable sur $K[x_1]$, etc.

Réciproquement, si $\varphi(\Pi_{x_2,K[x_1]})$ est à racines simples, on peut écrire la relation de Bézout, remonter et obtenir l'équivalence.

On a donc montré que $N = [L : K] \Leftrightarrow$ (x_1 est séparable sur K, x_2 est séparable sur $K[x_1]$, etc...)
Il suffit de montrer que ces assertions sont équivalentes au fait que $K \subseteq L$ soit séparable :
Si $N = [L : K]$, on sait que pour tout $x \in L$, $L = K[x, x_1, x_2, ..., x_n]$ et d'après la preuve précédente, x est séparable sur K.
Si $K \subseteq L$ est séparable, alors pour $i \in [n], x_i$ est séparable sur K, donc il est séparable sur les extensions de K. □

3.2 Correspondance de Galois

On considère $K \subseteq L$ une extension finie et Ω une clôture algébrique de K.

Définition 3.2.1 (Groupe de Galois)**.** *On note $Gal(L/K)$ l'ensemble des K-automorphismes $L \to L$. C'est-à-dire les K-morphismes dont l'image est L.*

Théorème 3.2.2. *Les assertions suivantes sont équivalentes :*

- $|Gal(L/K)| = [L : K]$
- *$K \subseteq L$ est galoisienne*
- *il existe un $P \in K[X]$ scindé à racines simples dans L donc $K \subseteq L$ est une extension de décomposition*

Preuve. $(1 \Rightarrow 2)$
Soit $\alpha \in L$ et P son polynôme minimal sur K. Pour tout $r \in \Omega$ K-conjugué de α, il existe un unique K-morphisme φ de $K[\alpha]$ vers Ω $\alpha \mapsto r$. Or, par hypothèse $\varphi(L) = L$ donc P est scindé dans L.

$(2 \Rightarrow 3)$
On considère $x_1, ..., x_n \in L$ tels que $L = K[x_1, ..., x_n]$. Les polynômes minimaux P_i des x_i sont scindés à racines simples dans L car $K \subseteq L$ est normale et séparable (galoisienne).
On pose $P = ppcm(X_i)_{i \in [n]}$, comme tous les

$(3 \Rightarrow 2)$
Si L est l'extension de décomposition d'un tel polynôme, soit φ un K-morphisme $L \to \Omega$, $\varphi(L) \subseteq L$. On note $(x_1, ..., x_n)$ les racines de P, on sait que $\varphi(x_i)$ annule aussi P, en particulier $\varphi(x_i) \in L$. Or $L = K[x_1, ..., x_n]$, donc pour $x \in L$, $\varphi(x)$ est un multinôme à coefficients dans K (en particulier dans L) évalué dans L, donc $\varphi(x) \in L$.
Ainsi $\varphi(L) \subseteq L$, or φ est injective comme morphisme de corps, et bijective en tant qu'endomorphisme d'espace vectoriel injectif. Or $K \subseteq L$ est séparable comme extension de décomposition d'un polynôme à racines simples. Donc $\varphi \in Gal(L/K)$. Donc $|Gal(L/K)| = [L : K]$

□

Proposition 3.2.3 (Lemme d'Artin). *Soit F un corps et G un groupe fini d'automorphismes de F. Alors $E = F^G = \{x \in F \mid \forall \sigma \in G, \sigma(x) = x\}$ est un sous-corps de F tel que $[F : E] = |G|$. En conséquence, $E \subseteq F$ est galoisienne de groupe de Galois G.*

Preuve. Pour $x, y \in E$, et $\sigma \in G$. $\sigma(x + y) = \sigma(x) + \sigma(y) = x + y$, $\sigma(xy) = \sigma(x)\sigma(y) = xy$, $\sigma(-x) = -\sigma(x) = -x$ et si x est non nul, $\sigma(\frac{1}{x}) = \frac{\sigma(1)}{\sigma(x)} = \frac{1}{x}$. Donc E est bien un sous-corps de F

On suppose par l'absurde que $[F : E] > card(G)$ et on pose $n = card(G) + 1$. Il existe donc $(a_1, \ldots, a_n)$ dans F libre sur K. Comme $n > |G|$, le système d'équations :

$$\sum_{k=1}^{n} \sigma(a_k) x_k = 0 \quad \sigma \in G$$

admet des solutions non triviales, on choisit $(x_1, \ldots, x_n)$ une dont le nombre de coefficients non nuls est minimal, quitte à changer l'ordre et à diviser par x_m, on peut supposer que c'est $(x_1, ..., x_m)$ et que $x_m = 1$. On a donc :

$$(*) \sum_{k=1}^{m-1} \sigma(a_k) x_k + \sigma(a_m) = 0 \quad \sigma \in G$$

Soit $\tau \in G$, tout $\sigma \in G$ s'écrit d'une manière unique comme $\tau^{-1} \circ \delta$ avec $\delta \in G$.

Ainsi :

$$\sum_{k=1}^{m-1} \tau^{-1} \circ \delta(a_k)x_k + \tau^{-1} \circ \delta(a_m) = 0 \quad \delta \in G \tag{2}$$

en composant par τ on obtient la relation : (3)

$$(**) \sum_{k=1}^{m-1} \delta(a_k)\tau(x_k) + \delta(a_m) = 0 \quad \delta \in G \tag{4}$$

$$(**) - (*) \sum_{k=1}^{m-1} \delta(a_k)[\tau(x_k) - x_k)] = 0 \quad \delta \in G \tag{5}$$

Par minimalité de $(x_1, ..., x_m)$, on a $\tau(x_k) = x_k$. Ainsi, la relation (**) devient :

$$\sum_{k=1}^{m} \delta(a_k)x_k = 0 \quad \delta \in G \tag{6}$$

$$(\text{en prenant } \delta = Id) \Rightarrow \sum_{k=1}^{m} a_k x_k = 0 \tag{7}$$

Absurdité car les a_k sont supposés indépendants. Donc $[F : E] \leq |G|$.
Or chaque automorphisme de G est un E-morphisme, donc $[F : E] \geq |G|$. On a donc égalité. □

Théorème 3.2.4 (Correspondance de Galois)**.** *Si $K \subseteq L$ est galoisienne de groupe de Galois G :*

- *Pour tout sous groupe $H \subseteq G$, $L^H = \{x \in L \mid \forall \sigma \in H, \sigma(x) = x\}$ est un sous corps de L. Et $[L^H : K] = \frac{|G|}{|H|}$.*
- *Pour tout sous corps $K \subseteq E \subseteq L$, l'extension $E \subseteq L$ est galoisienne de groupe $Gal(L/E) = \{\sigma \in Gal(L/K) \mid \forall x \in E, \sigma(x) = x\}$*
- *Les applications $H \mapsto L^H$ et $E \mapsto Gal(L/E)$ sont des bijections décroissantes, réciproques l'une de l'autre entre l'ensemble des sous groupes de G et l'ensemble des sous corps de L contenant K.*

Preuve. Soit H un sous-groupe de G, d'après le lemme d'Artin, $L^H \subseteq L$ est galoisienne de groupe de Galois H et $[L : L^H] = card(H)$, donc $[L^H : K] = \frac{[L:K]}{[L:L^H]} = \frac{|G|}{|H|}$
Soit E une extension de K contenue dans L. Comme $K \subseteq L$ est galoisienne, c'est l'extension de décomposition d'un polynôme $P \in K[X]$ scindé à racines simples dans L. Or, $P \in E[X]$ donc $E \subseteq L$ est galoisienne, par définition son groupe de Galois ne peut-être autre que le sous-groupe de G suivant :

$$H = \{\sigma \in G \mid \forall x \in E, \sigma(x) = x\}$$

On sait que $[L:L^H] = card(H) = \frac{[L:K]}{[E:K]} = [L:E]$. Par définition, L^H contient E, comme ils sont de même degré sur L ils sont égaux. $\square$

3.3 Groupe de Galois et racines

On considère un corps K

Proposition 3.3.1. *Soit $P \in K[X]$ un polynôme à racines simples et L une extension de décomposition de P. On note $\mathcal{R}$ l'ensemble des racines de P.*

- *Pour tout $\sigma \in Gal(L/K)$ et $\alpha \in \mathcal{R}$, $\sigma(\alpha) \in \mathcal{R}$.*
- *La restriction d'un automorphisme de $Gal(L/K)$ à $\mathcal{R}$ est une permutation de $\mathcal{R}$. Et l'application $\sigma \in Gal(L/K) \mapsto \sigma_{\{\mathcal{R}\}}$ est injective.*

Preuve. Soit $\alpha \in \mathcal{R}$ et $\sigma \in Gal(L/K)$ on sait que ;

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

Donc $\sigma(\alpha) \in \mathcal{R}$.

Tout morphisme de $Gal(L/K)$ est injectif. Donc sa restriction à $\mathcal{R}$ est injective, comme $\mathcal{R}$ est fini, c'est une permutation.
Ainsi l'application $\sigma \in Gal(L/K) \mapsto \sigma_{\{\mathcal{R}\}} \in S_{\mathcal{R}}$ est un morphisme de groupe.

Montrons qu'elle est injective en passant par le noyau :
Soit $\sigma \in Gal(L/K]$ tel que $\forall x \in \mathcal{R}, \sigma(x) = x$, et H, le groupe engendré par σ.
On sait que L^H est un sous corps de L contenant K, qui par hypothèse, contient les racines de P c'est donc une extension de décomposition de P.
Donc $L = L^H$, tout élément de L est fixé par σ, i.e. $\sigma = Id$ $\square$

Théorème 3.3.2 (Premier théorème d'isomorphisme)**.** *Soient A et B deux anneaux, $f : A \to B$ un morphisme d'anneau, Im(f) est un sous anneau de B et il existe un isomorphisme d'anneaux $\tilde{f} : \overline{a} \in A/Ker(f) \mapsto f(a) \in Im(f)$.*

Preuve. Im(f) est clairement stable par addition et par produit, il contient également $1_B = f(1_A)$, c'est donc un sous anneau de B.

On considère $\tilde{f} : \overline{a} \mapsto f(a)$, montrons d'abord qu'elle est bien définie :
Soient $a, a' \in A$ tels que $\overline{a} = \overline{a'}$, alors $\overline{a - a'} = \overline{0}$ donc $a - a' \in Ker(f)$, donc $f(a) = f(a')$.

Montrons maintenant que $\tilde{f}$ est un isomorsphisme d'anneau ;

$\tilde{f}(\overline{a+a'}) = f(a+a') = f(a) + f(a') = \tilde{f}(\overline{a}) + \tilde{f}(\overline{a'})$

$\tilde{f}(\overline{aa'}) = f(aa') = f(a)f(a') = \tilde{f}(\overline{a})\tilde{f}(\overline{a'})$

$\tilde{f}(\overline{1_A}) = f(1_A) = 1_B$

Injectivité : Si $\tilde{f}(\overline{a}) = 0, f(a) = 0$ donc $a \in Ker(f)$ ce qui équivaut à $\overline{a} = 0$

Surjectivité : Pour $i \in Im(f), \exists a \mid i = f(a)$ donc $i = \tilde{f}(\overline{a})$

□

Proposition 3.3.3. *Soit $P \in K[X]$ à racines simples et L une extension de décomposition de P.*

$$\forall x, y \in \mathcal{R}, \exists \sigma \in Gal(L/K) \mid \sigma(x) = y \Leftrightarrow P \textit{ est irréductible}$$

Preuve. Si P n'est pas irréductible, il existe $A, B \in K[X]$ tels que :

$$P = AB$$

On peut supposer A et B premiers entre eux, ainsi :

$$\mathcal{R} = \mathcal{R}_A \sqcup \mathcal{R}_B$$

Donc l'image d'une racine de A ne peut pas être une racine de B.

Si P est irréductible, on prend $x, y \in \mathcal{R}$, on sait que P est leur polynôme minimal.
On sait qu'il existe un morphisme d'anneau surjectif $f : P \in K[X] \mapsto P(x) \in K[x]$.
D'après le premier théorème d'isomorphisme, $K[X]/Ker(f) \cong K[x]$. Or $Ker(f) = (P)$ l'idéal engendré par P. Avec le même raisonnement pour $K[y]$, on obtient les deux isomorphismes d'anneau :

$$\tilde{f} : \overline{Q} \in K[X]/P \mapsto Q(x) \in K[x]$$

$$\tilde{g} : \overline{Q} \in K[X]/P \mapsto Q(y) \in K[y]$$

La composée $\varphi = \tilde{g} \circ \tilde{f}^{-1} : K[x] \to K[y]$ est donc un isomorphisme de corps.
Montrons que c'est un K-isomorphisme qui envoie x sur y :

$$\varphi(x) = \tilde{g}(\overline{X}) = y$$

$$\text{Pour } a \in K, \varphi(a) = \tilde{g}(\overline{a}) = a$$

Ainsi φ est bien un K isomorphisme de corps défini sur des sous corps de L, pour le prolonger à L il suffit de choisir les images des autres racines de P et on obtient un élément du groupe de Galois qui envoie x sur y. □

4 Exemple d'application

Dans cette partie nous détaillerons une application élémentaire de la théorie de Galois pour identifier les sous corps de l'extension de décomposition d'un polynôme.

On considère $P = (X^4 - 1)(X^2 + 5)$ dans $\mathbb{Q}$, son corps de décomposition est $L = \mathbb{Q}[\sqrt{5}, \sqrt{5}, i, -i, 1, -1] = \mathbb{Q}[\sqrt{5}, i]$.

$$[L : \mathbb{Q}] = [L : \mathbb{Q}[\sqrt{5}]] \cdot [\mathbb{Q}[\sqrt{5}] : \mathbb{Q}]$$

On sait que $[\mathbb{Q}[\sqrt{5}] : \mathbb{Q}] = 2$, et que $[L : \mathbb{Q}[\sqrt{5}]] = [Q[\sqrt{5}][i] : \mathbb{Q}[\sqrt{5}]] \leq 2$ car i est de degré 2 sur $\mathbb{Q}$. Or, si i est de degré 1 sur $\mathbb{Q}[\sqrt{5}]$ il serait réel car $Q[\sqrt{5}] \subset \mathbb{R}$, absurde donc :

$$[L : \mathbb{Q}] = 4$$

Ainsi, $G = Gal(L/\mathbb{Q})$ est isomorphe à un sous-groupe de S_4 d'ordre 4. Pour $\sigma \in G$, $\sigma(i)$ doit annuler $X^2 + 1$ donc $\sigma(i) = \pm i$, de même $\sigma(\sqrt{5}) = \pm\sqrt{5}$.
Si on choisi $1 = \sqrt{5}, 2 = -\sqrt{5}, 3 = i, 4 = -i$, pour alléger les notations. Alors,

$$G \cong \{Id, (1, 2), (3, 4), (1, 2)(3, 4)\}$$

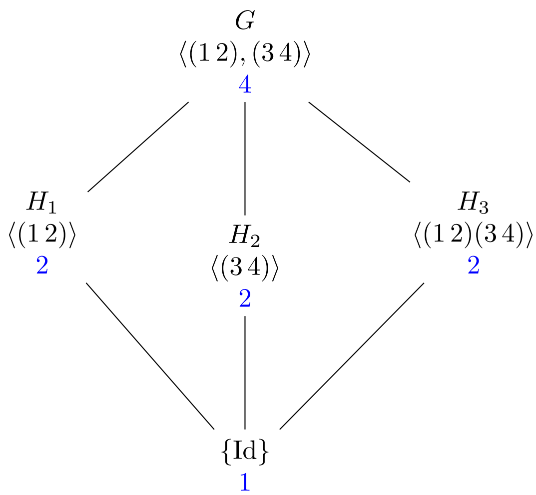
D'après le théorème de Lagrange, les sous-groupes de G sont d'ordre 1,2 ou d'ordre 4.

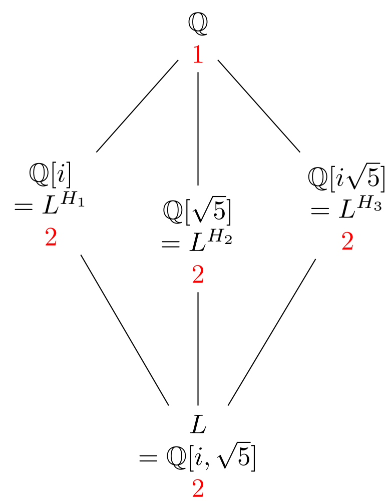
- Ordre 4 : G
- Ordre 2 : $H_1 \cong \langle(1, 2)\rangle, H_2 \cong \langle(3, 4\rangle, H_3 \cong \langle(1, 2)(3, 4)\rangle$.
- Ordre 1 : {Id}

Par la correspondance de Galois, il existe donc trois sous-extensions de L de degré 2 sur $\mathbb{Q}$.

$L^{H_1} = \mathbb{Q}[i]$, en effet $\forall x \in \mathbb{Q}[i], \sigma \in H_1, \sigma(x) = x$, on a donc une inclusion, or on sait aussi par la correspondance que $[L^{H_1} : \mathbb{Q}] = \frac{card(G)}{card(H_1)} = 2$. Par l'égalité des degrés, on a l'égalité des ensembles.
Par le même raisonnement, on montre que $L^{H_2} = \mathbb{Q}[\sqrt{5}]$.
Enfin on remarque que $Q[i\sqrt{5}]$ est fixé par H_3. Donc le dernier sous-corps est bien $L^{H_3} = \mathbb{Q}[i\sqrt{5}]$.

Ci dessous les treillis des sous groupes de G et des sous extensions de L, afin d'illustrer la correspondance :





Sous-groupe	**Ordre**	**Corps fixe (degré)**
G	4	$\mathbb{Q}$ (1)
$H_1 = \langle(1\,2)\rangle$	2	$\mathbb{Q}[i]$ (2)
$H_2 = \langle(3\,4)\rangle$	2	$\mathbb{Q}[\sqrt{5}]$ (2)
$H_3 = \langle(1\,2)(3\,4)\rangle$	2	$\mathbb{Q}[i\sqrt{5}]$ (2)
$\{\mathrm{Id}\}$	1	L (4)