Les correspondances de Galois

1 Groupe de Galois

Soit E une extension normale finie d'un corps K. L'ensemble des K-automorphismes de E forment un groupe pour la composition d'application.

Définition Soit E une extension normale finie d'un corps K. Le groupe de tous les K-automorphismes de E sera appelé le groupe de Galois de l'extension E de K. Le groupe de Galois d'une extension E de K sera noté $G(E/K)$.

Exemple $\mathbb{C}$ est une extension normale finie de $\mathbb{R}$. Son groupe de Galois possède deux éléments : l'identité et le $\mathbb{R}$-automorphisme σ qui associe à chaque nombre complexe z son conjugué $\overline{z}$.

Théorème Soit E une extension normale finie d'un corps K. $G(E/K)$ est un groupe fini dont l'ordre est le degré galoisien $\overline{[E:K]}$ de l'extension.

Démonstration $G(E/K)$ est l'ensemble I de tous les K-isomorphismes de E dans une clôture normale de E. Or E est sa propre clôture normale car elle est une extension normale de K. D'où $G(E/K) = I$.

Corollaire Soit E une extension normale finie d'un corps K. $Ord\,(G(E/K)) \leq [E:K]$.

2 Les correspondance de Galois

Soit E une extension finie de K.

Définition L'extension finie E de K sera dite une **extension galoisienne** si, et seulement si, E est une extension normale et séparable de K.

Exemple $\mathbb{C}$ est une extension galoisienne de $\mathbb{R}$.

Théorème Si E est une extension galoisienne de K, alors

$$Ord\,(G(E/K)) = [E:K].$$

Démonstration Nous avons $Ord\,(G(E/K)) = \overline{[E:K]} = [E:K]$.

Soit $G(E/K)$ le groupe de Galois d'une extension galoisienne finie E de K, $\mathcal{C}$ l'ensemble des corps intermédiaires entre K et E et $\mathcal{H}$ l'ensemble des sous-groupes de $G(E/K)$. Pour tout $L \in \mathcal{C}$, on pose

$$S(L) = \{u \in G(E/K) \quad / \quad (\forall x \in L)\,[u(x) = x]\}$$

et pour tout $H \in \mathcal{H}$

$$I(H) = \{x \in E \quad / \quad (\forall u \in H)\,[u(x) = x]\}$$

Il est facile de prouver que $S(L)$ est un sous-groupe de $G(E/K)$ et $I(H)$ est un corps intermédiaire entre K et E. Ainsi, nous avons deux applications $S; \mathcal{C} \longrightarrow \mathcal{H}$ et $I; \mathcal{H} \longrightarrow \mathcal{C}$. Ces deux applications sont visiblement décroissantes.

Théorème Pour tout $L \in \mathcal{C}$, E est une extension galoisienne finie de L et $G(E/L) = S(L)$.

Démonstration E, étant une extension normale de K, elle est le corps des racines pour un polynôme $P \in K[X]$ sur K. E est aussi un corps des racines pour P sur L. Donc, E est une extension normale de L. D'un autre côté, tout élément $a \in E$ est séparable sur K. Ceci prouve que toutes les racines de $Irr(a,K)$ sont simples. Il en résulte que $Irr(a,L)$ (qui divise $Irr(a,K)$) possède la même propriété. On en déduit que E est une extension séparable de L et par suite une extension galoisienne de L. Enfin, $G(E/L)$ est l'ensemble des L-automorphismes de E.

Théorème $S \circ I = id_{\mathcal{H}}$.

Démonstration Nous avons à prouver $(S \circ I)(H) = S(I(H)) = H$ pour tout $H \in \mathcal{H}$. Soit $L = I(H)$ et $H' = S(L) = (S \circ I)(H)$. Alors $H' = G(E/L)$ et $H \subseteq H'$. D'un autre côté, soit $H = \{\sigma_1,...,\sigma_n\}$ et a un élément primitif de l'extension E de K. Nous avons $E = K(a) = L(a)$. Le polynôme $P = \prod_{i=1}^{i=n} (X - \sigma_i(a))$ appartient à $L[X]$, en effet

$$\widehat{\sigma}(P) = \prod_{i=1}^{i=n} (X - (\sigma \circ \sigma_i)(a)) = P$$

pour tout $\sigma \in H$, car $\{\sigma_1,...,\sigma_n\} = H = \{\sigma \circ \sigma_1,...,\sigma \circ \sigma_n\}$ (H est un groupe). Nous avons

$$\begin{aligned}[P(a) = 0] &\Longrightarrow [Irr(a,L)/P] \\ &\Longrightarrow \left[\begin{array}{c} Ord(H') = [E:L] = \deg(Irr(a,L)) \\ \leq \deg(P) = n = Ord(H) \end{array}\right]\end{aligned}$$

Or H est un sous-groupe du groupe fini H'. D'où $Ord(H) \leq Ord(H')$ et par suite $H = H'$, car H' est un groupe fini.

Théorème $I \circ S = id_{\mathcal{C}}$.

Démonstration Soit L un élément de $\mathcal{C}$. Posons $H = S(L)$ et $L' = I(H) = (I \circ S)(L)$. Nous avons $L \subseteq L'$. D'un autre côté, si $b \in L'$, alors b est laissé fixe par tout élément de $H = S(L) = G(E/L)$. Toutes les racines de $Irr(b,L)$ sont simples, car $Irr(b,L)$ divise $Irr(b,K)$ et b est séparable sur K. Or, si b' est une autre racine de $Irr(b,L)$, il existe un L-isomorphisme de $L(b)$ dans E qui transforme b en b'. Ce L-isomorphisme peut être prolongé en un L-automorphisme σ de E. On en déduit qu'il existe $\sigma \in G(E/L) = H$ tel que $\sigma(b) = b' \neq b$ ce qui prouve $b \notin L'$ en contradiction avec le choix de b. Il en résulte que b est l'unique racine de $Irr(b,L)$ et par suite $b \in L$. Donc $L = L'$.

Corollaire L'application de $\mathcal{C}$ dans $\mathcal{H}$ qui associe à L l'élément $G(E/L)$ est une bijection décroissante.

Théorème Si $K \subseteq L \subseteq E$, alors nous avons : L est une extension normale de K si, et seulement si, $G(E/L)$ est un sous-groupe distingué de $G(E/K)$.

Démonstration Soit $\sigma \in G(E/K)$. Nous avons $\sigma(x) \in L$ pour tout $x \in L$ car L est une extension normale de K. Il en résulte

$$\left(\sigma^{-1} \circ \tau \circ \sigma\right)(x) = \sigma^{-1}(\tau(\sigma(x))) = \sigma^{-1}(\sigma(x)) = x$$

pour tout $\tau \in G(E/L)$. Ainsi, $\sigma^{-1} \circ \tau \circ \sigma \in G(E/L)$ pour tout $\tau \in G(E/L)$, ce qui prouve que ce sous-groupe de $G(E/K)$ est distingué. Réciproquement, si $G(E/L)$ est un sous-groupe distingué de $G(E/K)$, alors tout K-isomorphisme τ de L dans E est un K-automorphisme de L : τ peut être prolongé en un K-automorphisme $\overline{\tau}$ de E et $\overline{\tau}^{-1} \circ \sigma \circ \overline{\tau} \in G(E/L)$ pour tout $\sigma \in G(E/L)$. Si $x \in L$, alors $x = \left(\overline{\tau}^{-1} \circ \sigma \circ \overline{\tau}\right)(x)$ et $\overline{\tau}(x) = (\sigma \circ \overline{\tau})(x)$ pour tout $\sigma \in G(E/L)$. Il en résulte que $\overline{\tau}(x) \in L$ et $\tau(x) \in L$. D'où $\tau(L) \subseteq L$ et τ est un K-automorphisme de L ce qui prouve que L est une extension normale de K.

Théorème Soit L un corps intermédiaire, extension normale de K. Le groupe $G(L/K)$ est isomorphe au groupe quotient $G(E/K)/G(E/L)$.

Démonstration $G(E/L)$ est un sous-groupe distingué de $G(E/K)$, car L est une extension normale de K. Soit φ l'application de $G(E/K)$ dans $G(L/K)$ qui associe à σ sa restriction à L. C'est une application de $G(E/K)$ dans $G(L/K)$ car la restriction de σ à L est un K-isomorphisme de L dans E et par suite un K-automorphisme de L, car L est une extension normale de K. L'application φ est surjective, car tout $\alpha \in G(L/K)$, étant un K-isomorphisme de L dans E, peut être prolongé en un K-automorphisme $\overline{\sigma}$ de E. Finalement, φ est un homomorphisme de groupes et son noyau est $G(L/K)$, d'où $G(E/K)/G(E/L) \approx G(L/K)$.

3 EXEMPLE

Soit R le corps des racine du polynôme $X^4-2 \in \mathbb{Q}[X]$ sur $\mathbb{Q}$. Nous avons $R = \mathbb{Q}\left(i,\sqrt[4]{2}\right)$.

Degré de R sur $\mathbb{Q}$: Nous avons $[R:\mathbb{Q}] = \left[R:\mathbb{Q}\left(\sqrt[4]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[4]{2}\right):\mathbb{Q}\right]$. $\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right] =$ 4, car X^4-2 est irréductible dans $\mathbb{Q}[X]$. $\left[R:\mathbb{Q}\left(\sqrt[4]{2}\right)\right] = 2$, car $Irr\left(i,\mathbb{Q}\left(\sqrt[4]{2}\right)\right) = X^2+1$. D'où $[R:\mathbb{Q}] = 8$.

Groupe $G(R/\mathbb{Q})$: Si $\sigma \in G(R/\mathbb{Q})$, alors

- $\sigma(i)$ est une racine de X^2+1. Donc $\sigma(i) = \pm i$.
- $\sigma\left(\sqrt[4]{2}\right)$ est une racine de X^4-2. Donc

$$\sigma\left(\sqrt[4]{2}\right) = \pm\sqrt[4]{2}$$

ou

$$\sigma\left(\sqrt[4]{2}\right) = \pm i\sqrt[4]{2}$$

.

Or σ est complètement déterminé par son action sur i et $\sqrt[4]{2}$ car ces éléments engendrent R sur $\mathbb{Q}$. Il en résulte que le groupe de Galois de l'extension R de $\mathbb{Q}$ est

Groupe de Galois de l'extension de $R/\mathbb{Q}$

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

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

Sous-groupes de $G(R/\mathbb{Q})$:

- Sous-groupe d'ordre 1 : $\{\sigma_1\}$
- Sous-groupe d'ordre 2 : $A = \{\sigma_1,\sigma_2\}$, $B = \{\sigma_1,\sigma_5\}$, $C = \{\sigma_1,\sigma_6\}$, $D = \{\sigma_1,\sigma_7\}$ et $E = \{\sigma_1,\sigma_8\}$.

– Sous-groupe d'ordre 4 : $F=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$, $G=\{\sigma_1,\sigma_2,\sigma_5,\sigma_6\}$ et $H=\{\sigma_1,\sigma_2,\sigma_7,\sigma_8\}$.
– Sous-groupe d'ordre : $G(R/\mathbb{Q})$.

Diagramme des sous-groupes :

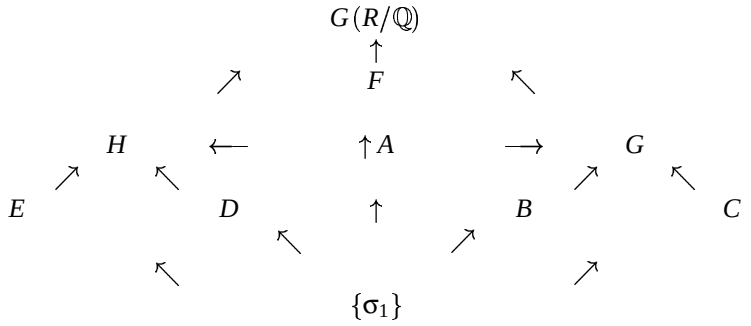
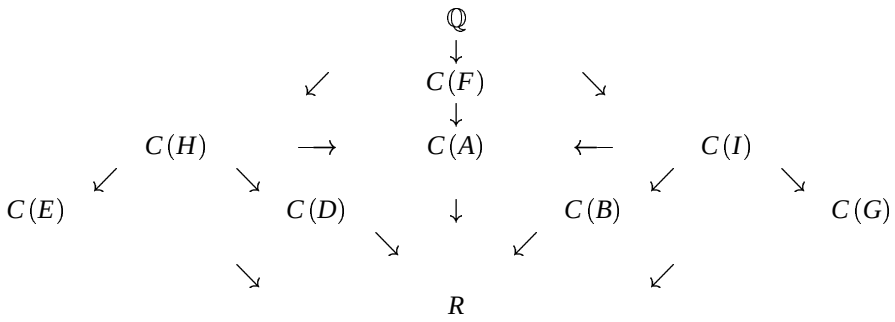


Diagramme des corps intermédiaires :



où $C(M)$ est le corps intermédiaire associé au sous-groupe M de $G(R/\mathbb{Q})$. Pour déterminer ces corps intermédiaires, on considère une base du $\mathbb{Q}$-espace vectoriel R exprimée en termes de i et $\sqrt[4]{2}$. Nous avons la base

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

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

$$x=b_0+b_1\sqrt[4]{2}+b_2\left(\sqrt[4]{2}\right)^2+b_3\left(\sqrt[4]{2}\right)^3c_0i+c_1i\sqrt[4]{2}+c_2i\left(\sqrt[4]{2}\right)^2+c_3i\left(\sqrt[4]{2}\right)^3$$

Pour déterminer $C(A)$, on utilise l'équivalence

$$[x\in C(A)]\Longleftrightarrow[\sigma_2(x)=x]$$

Or

$$\sigma_2(x) = b_0 - b_1\sqrt[4]{2} + b_2\left(\sqrt[4]{2}\right)^2 - b_3\left(\sqrt[4]{2}\right)^3 c_0 i - c_1 i\sqrt[4]{2} + c_2 i\left(\sqrt[4]{2}\right)^2 - c_3 i\left(\sqrt[4]{2}\right)^3$$

Donc

$$[x \in C(A)] \Longleftrightarrow [\sigma_2(x) = x] \Longleftrightarrow [b_1 = b_3 = c_1 = c_3 = 0]$$
$$\Longleftrightarrow \left[x \in \mathbb{Q}\left(i, \left(\sqrt[4]{2}\right)^2\right)\right]$$

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

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

Sous-groupes distingués de $G(R/\mathbb{Q})$: Les sous-groupes d'ordre 4 sont distingués. A est la seule sous-groupe distingué d'ordre 2.

Extensions normale de $\mathbb{Q}$: Les corps intermédiaires qui sont des extensions normales de $\mathbb{Q}$ sont ceux associés aux sous-groupes distingués de $G(R/\mathbb{Q})$. Ces corps sont : $\mathbb{Q}(i)$, $\mathbb{Q}\left(\sqrt{2}\right)$, $\mathbb{Q}\left(i\sqrt{2}\right)$ and $\mathbb{Q}\left(i, \sqrt{2}\right)$.