Aspects élémentaires de théorie de Galois inverse

Colas Bardavid
colas.bardavid@gmail.com
hx4 - mp⋆4

2000-2001

Table des matières

1 Résultats de théorie de Galois

La présentation faite ici de la théorie de Galois est une formalité dans le sens où le rôle de cette introduction n'est pas de faire comprendre la théorie mais de fixer définitions et notations, et de rappeler les grands résultats.

1.1 Quelques définitions

Définition 1 *Soient K un corps et L une extension de K.*

*On note $[\boldsymbol{L : K}]= dim_K(L)$ et on parle alors du **degré de $\boldsymbol{L/K}$**. Si $[L : K] \in \mathbb{N}$, on dit que l'**extension est finie**.*

*En notant $\boldsymbol{K(x)}$ la plus petite extension de K contenant x, on dit que $\boldsymbol{L/K}$ **est algébrique** si $\forall\, x \in L$, $[K(x) : K] \in \mathbb{N}$.*

*On dit que l'extension $\boldsymbol{K/L}$ **est normale** si pour tout polynôme $P \in K[X]$ irréductible, $\exists\, x \in L \,/\, P(x) = 0 \Longrightarrow$ P est scindé sur L.*

*Le **groupe de Galois de $\boldsymbol{L/K}$** est le sous-groupe de $Aut\,(L)$ des morphismes induisant l'identité sur K. On note : $\boldsymbol{Gal\,(L/K)}= Aut_K(L)$.*

*Enfin, si $G \subset Aut\,(K)$, on appelle **corps fixe de $\boldsymbol{K}$ fixe par $\boldsymbol{G}$ le corps $\boldsymbol{K_G}$**$= \{x \in K \,/\, \forall\, g \in G,\, g(x) = x\}$.*

Définition 2 (Steinitz) *Soit K un corps. On appelle **clôture algébrique de $\boldsymbol{K}$** et on note $\boldsymbol{\overline{K}}$ l'unique corps L à isomorphisme près tel que L/K soient une extension algébrique et que tout polynôme de L non constant admette une racine dans L.*

Définition 3 *Soient K un corps et $P \in K[X]$. On fixe $\overline{K}$ une clôture algébrique de K. On se place implicitement dans $\overline{K}$.* [1]

*On appelle **corps de décomposition de $\boldsymbol{P}$ sur $\boldsymbol{K}$** l'unique corps L tel que :*

1) $K \subset L$

2) $\exists\, (x_i)_{i\leq p} \in L^n \,/\, L = K\,(x_i)_{i\leq n}$ et $\exists\, \lambda \in K,\, P = \lambda \prod_{i=1}^{p} (X - x_i)$.

On note $\boldsymbol{L = K\Big|^{P}}$.

*Soient $x_1, \ldots, x_p$ les p racines de P dans $K\Big|^{P}$. En réordonnant les racines, on note $x_1, \ldots, x_n$ $(n \leq p)$ les n racines distinctes. On appelle **groupe de Galois de $\boldsymbol{P}$ sur $\boldsymbol{K}$** et on note $\boldsymbol{Gal_K(P)}$, le sous-groupe G de $\mathfrak{S}_n$ tel que*

$$\big(R(x_1, \ldots, x_n) = 0 \Longrightarrow \sigma R(x_1, \ldots, x_n) \equiv R\left(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}\right) = 0\big) \Longleftrightarrow \sigma \in G.$$

1.2 Les grands lemmes

Proposition 1 *Soient K un corps et $P \in K[X]$. On a : $Gal_K(P) \simeq Gal\left(K\Big|^{P}/K\right)$.*

Proposition 2 *Soit L/K une extension finie. Alors, $\left|Hom_K\big(L, \overline{K}\big)\right| \leq [L : K]$. Si K est de caractéristique nulle, on a l'égalité. Si de plus L/K est normale, on a $Hom_K\big(L, \overline{K}\big) = Gal(L/K)$.*

Théorème 1 (Dedekind) *Soient M un monoïde, K un corps et $(\phi_i)_{i\leq n}$ des morphismes distincts de M dans $(K^*, \times)$. Alors les ϕ_i sont linéairement indépendants.*

Théorème 2 (Artin) *Soient K un corps et G un groupe fini d'automorphismes de K. Alors, $Gal(K/K_G) = G$ et l'extension K/K_G est normale finie.*

1.3 La correspondance de Galois

Soit L/K une extension normale finie, avec K corps fini ou de caractéristique nulle. On cherche à établir une bijection entre les deux ensembles suivants :

- l'ensemble $\mathcal{K}_{L/K}$ des sous-corps de L contenant K ; L est une extension normale finie de ces sous-corps.
- l'ensemble $\mathcal{G}_{L/K}$ des sous-groupes de $Gal(L/K)$

Théorème 3 (Correspondance de Galois 1) *Soit L/K une extension normale finie. Soient*

$$\boldsymbol{\Upsilon_{L/K}} \;:\; \begin{array}{c} \mathcal{K}_{L/K} \to \mathcal{G}_{L/K} \\ M \mapsto Gal(L/M) \end{array} \qquad \text{et} \qquad \boldsymbol{\Omega_{L/K}} \;:\; \begin{array}{c} \mathcal{G}_{L/K} \to \mathcal{K}_{L/K} \\ G \mapsto L_G \end{array}.$$

Alors $\boldsymbol{\Upsilon_{L/K}}$ et $\boldsymbol{\Omega_{L/K}}$ sont deux bijections réciproques.

[1] De façon plus générale, deux corps de décomposition sont isomorphes.

Théorème 4 (Correspondance de Galois 2) *Soient L/K une extension normale finie et M un corps intermédiaire à K et L. Alors,*

$$Gal(L/M) \lhd Gal(L/K) \iff M/K \text{ est normale .}$$

Dans ce cas, on a :

$$Gal(L/K)/_{Gal(L/M)} \simeq Gal(M/K).$$

1.4 Problématique de la théorie de Galois inverse

C'est peut-être parce qu'il est difficile de calculer un groupe de Galois que l'on s'est posé les problèmes suivants :

Problème 1 *Étant donné un groupe G, existe-t-il une extension L/K telle que $Gal(L/K) = G$?*

Problème 2 *Étant donné un groupe G fini, existe-t-il une extension L/K normale finie telle que $K/\mathbb{Q}$ soit une extension finie et $Gal(L/K) = G$?*

Problème 3 *Si G est un groupe fini, existe-t-il une extension normale finie L de $\mathbb{Q}$ telle que $Gal(L/\mathbb{Q}) = G$?*

Je n'étudierai en fait que partiellement le problème 1, à travers les problèmes 2 et 3 (en remarquant que résoudre le problème 3 résout le problème 2), entre autres car je ne connais pas la théorie de Galois des extensions infinies.

On dira que *G est un groupe de Galois sur K* s'il existe une extension normale finie L/K telle que $Gal(L/K) = G$.

Dans l'état actuel de la recherche, sachant qu'aucun groupe fini n'étant pas groupe de Galois sur $\mathbb{Q}$ n'a été exhibé, on ne peut qu'énoncer la

Conjecture 1 *Tout groupe fini est un groupe de Galois sur $\mathbb{Q}$.*

2 Un premier résultat

On peut commencer par faire ce qui est le plus simple : paradoxalement, énoncer une propriété générale des groupes de Galois sur un corps K, avant même d'avoir exhibé aucun exemple intéressant.

Résultat 1 *Soit G un groupe de Galois sur K. Alors tout quotient de G est un groupe de Galois sur K*

Démonstration : On note $G = Gal(L/K)$. Soit $H \lhd G$. D'après la première partie de la correspondance de Galois, on peut trouver un corps M intermédiaire à K et L tel que $H = Gal(L/M)$. On applique alors à ce corps la seconde partie de la correspondance pour obtenir : $G/_H \simeq Gal(M/K)$. ■

3 Le groupe symétrique $\mathfrak{S}_n$

On va établir dans ce paragraphe que $\mathfrak{S}_n$ est un groupe de Galois sur $\mathbb{Q}$. Pour ce faire, on mènera notre étude du point de vue polynômial. Comme on considérera, en dernier lieu, des polynômes de $\mathbb{Z}/_{p\mathbb{Z}}$, dans un premier temps, on portera notre attention sur les corps finis. Ensuite, on reliera de façon agréable les polynômes de $\mathbb{Z}[X]$ et leur réduit modulo p. Enfin, on conclura.

3.1 Corps finis

Lemme 1 *Soit K un corps de caractéristique $p > 0$. Alors, $\forall\, x,\, y \in K$, $\forall\, n \in \mathbb{N}$, $(x+y)^{p^n} = x^{p^n} + y^{p^n}$.*

Proposition 3 (Structure des corps finis)

a) Soit K un corps fini de caractéristique p. Alors, $\exists\, !n \in \mathbb{N}$ / $card\, K = p^n$.
b) Si K' est un autre corps tel que $card\, K = card\, K'$, alors $K \simeq K'$.
c) $\forall\, p \in \mathcal{P}$, $\forall\, n \in \mathbb{N}^*$, $\exists\, K$ corps / $card\, K = p^n$. On note $\mathbb{F}_{p^n}$ ce corps.

Un corps fini est aussi appelé champ de Galois.

Lemme 2 *Soit $q = p^n$. Le groupe des automorphismes de $\mathbb{F}_q$ est cyclique, engendré par f_q, où on note f_q :* $\begin{array}{c} \mathbb{F}_q \to \mathbb{F}_q \\ x \mapsto x^p \end{array}$.

Démonstration : On sait que $f_q^n = Id$. Donc l'ordre d de f_q divise n. En outre, $\forall\, x \in \mathbb{F}_q,\ x^{p^d} - x = 0$. Comme $P = X^{p^d} - X$ a au plus p^d racines, c'est que $p^d \geq p^n$ et donc $d \geq n$. Ainsi $d = n$. On se sert alors de la proposition 2, à savoir : $|Aut(\mathbb{F}_q)| \leq \left|Hom\left(\mathbb{F}_q,\ \overline{\mathbb{F}_q}\right)\right| = \left|Hom_{\mathbb{F}_p}\left(\mathbb{F}_q,\ \overline{\mathbb{F}_q}\right)\right| \leq [\mathbb{F}_q : \mathbb{F}_p] = n$. Finalement, $Aut(\mathbb{F}_q) = \langle f_q \rangle \simeq \mathbb{Z}/n\mathbb{Z}$. ■

Corollaire 1 (Structure des groupes de Galois sur les corps finis) *Soit $P \in \mathbb{F}_p[X]$. Alors $Gal_{\mathbb{F}_p}(P)$ est un groupe cyclique.*
Plus précisément, si $P = \prod_i P_i$ où les P_i sont irréductibles de degré n_i, alors $Gal_{\mathbb{F}_p}(P)$ est engendré par $\prod_i \sigma_i$ où les σ_i sont des n_i-cycles à support disjoints.

Démonstration : Pour justifier cela, prenons Q un facteur irréductible de P (il est à racines simples, on le prouve dans un autre énoncé, plus loin) : $\sigma(Q) = Q$, et on peut donc définir la restriction de σ aux racines de Q, que l'on notera σ_Q. On peut prouver, à l'aide d'un lemme de prolongements des morphismes, que $\left\{\sigma_Q,\ \sigma \in Gal_{\mathbb{F}_p}(P)\right\}$ est transitif. D'où le résultat. ■

3.2 Groupe de Galois et réduction modulo p

Notons désormais la réduction modulo p, qui est un morphisme d'anneaux, χ_p.
On adopte dans tout cette sous-partie les **notations :**
$P = \prod_{i \leq n}(X - x_i) \in \mathbb{Z}[X]$ tel que les x_i soient distincts.
$K = \mathbb{Q}(x_1, \ldots, x_n) = \mathbb{Q}\Big|^P$. $A = \mathbb{Z}[x_1, \ldots, x_n]$, sous-anneau de K.
On fixe $p \in \mathcal{P}$. On suppose $\chi_p(P)$ séparable (dans $\mathbb{F}_p$).
L'idée que l'on développe ici est d'étudier les prolongements de la réduction modulo p, depuis A vers le corps de décomposition de $\chi_p(P)$, noté $\mathbb{E}_p$.

3.2.1 Rang d'un $\mathbb{Z}$-module libre de type fini

Définition 4 *Soit B un $\mathbb{Z}$-module (*ie *un groupe abélien). On dit que B* est libre *ssi B admet une base : $\exists\, (e_i)_{i \in I}\ /\ \forall\, b \in B,\ \exists\, !\, (\lambda_i) \in \mathbb{Z}^{(I)}\ /\ b = \sum_{i \in I} \lambda_i e_i$.*

Théorème-Définition 1 *Soit B un $\mathbb{Z}$-module libre de type fini. (*ie *engendré par une sous partie finie). Alors toutes les bases ont même cardinal. Ce cardinal est le* rang de B*, noté rg B.*

3.2.2 Un $\mathbb{Z}$-module de type fini sans torsion est libre

Si je laisse dans ce paragraphe les démonstrations et les résultats intermédiaires, c'est parce qu'ils me sont personnels.

Complétion d'une famille libre en une une famille basique La situation n'est pas simple. En effet, on ne peut pas compléter une quelconque famille libre en base. Par exemple, dans $\mathbb{Z}^2$, $(4, 6)$ n'est pas complétable en une base (comme tout vecteur du type $\delta(a, b)$, $|\delta| > 1$).

Lemme 3 *Soit $(\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n$ ($n \geq 2$) tel que les λ_i soient premiers dans leur ensemble. Alors, il existe $(\alpha_{i,j})_{\substack{1 \leq i \leq n \\ 2 \leq j \leq n}} \in \mathbb{Z}^{(n-1)n}$ telle que :*

$$\begin{vmatrix} \lambda_1 & \alpha_{12} & \ldots & \alpha_{1n} \\ \lambda_2 & \alpha_{22} & \ldots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_n & \alpha_{n2} & \ldots & \alpha_{nn} \end{vmatrix} = 1$$

Démonstration : On raisonne par récurrence sur n.

$\underline{n = 2}$: $\lambda_1 \wedge \lambda_2 = 1$, donc $\exists\, (m, n) \in \mathbb{Z}^2\ /\ \lambda_1 m - n\lambda_2 = 1$, c'est-à-dire $\begin{vmatrix} \lambda_1 & n \\ \lambda_2 & m \end{vmatrix} = 1$.

$\underline{HR_{n-1} \Longrightarrow HR_n}$: On note δ le $pgcd$ de $\{\lambda_i\}_{i\leq n-1}$, et on note $\mu_i = \frac{\lambda_i}{\delta}$ pour $i \leq n-1$. Les μ_i sont premiers dans leur ensemble. Soit donc $(\alpha_{i,j})_{\substack{1\leq i\leq n-1\\ 2\leq j\leq n-1}}$ telle que : $\begin{vmatrix} \mu_1 & \alpha_{12} & \dots & \alpha_{1n-1} \\ \mu_2 & \alpha_{22} & \dots & \alpha_{2n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mu_{n-1} & \alpha_{n-12} & \dots & \alpha_{n-1n-1} \end{vmatrix} = 1$. On sait que δ et λ_n sont premiers entre eux. Ainsi, $\exists\,(k,\,l) \in \mathbb{Z}^2 \;/\; k\delta + l\lambda_n = 1$. On vérifie alors que la matrice

$$\begin{pmatrix} \lambda_1 & \alpha_{12} & \dots & \alpha_{1n-1} & (-1)^{n-1}l\mu_1 \\ \lambda_2 & \alpha_{22} & \dots & \alpha_{2n-1} & (-1)^{n-1}l\mu_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \lambda_{n-1} & \alpha_{n-12} & \dots & \alpha_{n-1n-1} & (-1)^{n-1}l\mu_{n-1} \\ \lambda_n & 0 & \dots & 0 & (-1)^{n-1}k \end{pmatrix}$$

a pour déterminant 1, en développant par rapport à la dernière ligne. ■

Proposition 4 *Soit $\lambda = (\lambda_1, \dots, \lambda_n) \in \mathbb{Z}^n$ tel que les λ_i soient premiers dans leur ensemble. Alors, il existe $(e_i)_{i\leq n-1} \in (\mathbb{Z}^n)^{n-1}$ telle que $(\lambda, e_1, \dots, e_n)$ soit une $\mathbb{Z}$-base de $\mathbb{Z}^n$.*

Démonstration : On complète le vecteur colonne $(\lambda_1, \dots, \lambda_n)$ en une matrice

$$M = \begin{pmatrix} \lambda_1 & \alpha_{12} & \dots & \alpha_{1n} \\ \lambda_2 & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_n & \alpha_{n2} & \dots & \alpha_{nn} \end{pmatrix} = (C_1, \dots, C_n)$$

de déterminant 1, grâce au lemme précédent. Sachant alors que $\widetilde{M}M = \det(M)I_n = I_n$, où $\widetilde{M}$ est la transposée de la comatrice de M, on en déduit que $M^{-1} \in \mathcal{M}_n(\mathbb{Z})$.

Vérifions que $(C_1, \dots, C_n)$ est une $\mathbb{Z}$-base de $\mathbb{Z}^n$. Notons $\varepsilon_i \in \mathcal{M}_{1n}(\mathbb{Z})$ tel que $(\varepsilon_i)_j = \delta_{ij}$. On a dans ce cas, $MX = \varepsilon_i \Longleftrightarrow X = M^{-1}\varepsilon_i \in \boldsymbol{\mathcal{M}_{1n}}(\mathbb{Z})$. Donc, $\varepsilon_i = \sum_{j\leq n} X_j C_j$. Ainsi, $(C_j)_{j\leq n}$ est génératrice de $\mathbb{Z}^n$ et libre car de bon cardinal. ■

Étude des quotients de $\mathbb{Z}^n$ On caractérise dans ce paragraphe les groupes quotients de $\mathbb{Z}^n$ sans torsion.

Théorème 5 (Structure des quotients sans torsion de $\mathbb{Z}^n$) *Soit G un sous-groupe de $\mathbb{Z}^n$ tel que ${}^{\mathbb{Z}^n}\!/_G$ soit sans torsion. Alors il existe $k \in \mathbb{N}$ tel que ${}^{\mathbb{Z}^n}\!/_G \simeq \mathbb{Z}^k$.*

Les $\mathbb{Z}$-modules de type fini sans torsion sont libres Les modules ont ceci de différent d'avec les espaces vectoriels qu'ils n'admettent pas forcément de base, même s'ils sont de type fini. On peut donner l'exemple de ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$, qui n'admet pas de famille libre. Cependant, on a le théorème suivant :

Théorème 6 *Soit M un $\mathbb{Z}$-module de type fini et sans torsion. Alors, M est libre.*

3.2.3 Étude de A

Fait 1 *A est un $\mathbb{Z}$-module non nul, libre et de type fini.*
Par ailleurs, on a $rg(A) = [K : \mathbb{Q}]$.

Démonstration : A est de type fini car engendré en tant que $\mathbb{Z}$-module par $(\prod_{j\leq n} {\alpha_j}^{n_j})_{n_j\leq n}$. C'est uniquement ici qu'intervient le fait essentiel que P soit unitaire.

La première assertion provient de l'étude faite précédemment sur les $\mathbb{Z}$-modules sans torsion, de type fini. Soit donc $e = (e_i)_{i\leq p}$ une base de A. Comme on sait que $K = \{R(x_1, \dots, x_n),$
$R \in \mathbb{Q}(X_1, \dots, X_n)\}$ et $A = \{R(x_1, \dots, x_n),\, R \in \mathbb{Z}(X_1, \dots, X_n)\}$, si x est un élément de K, alors $x = \frac{x'}{m}$ où $x' \in A$ et $m \in \mathbb{Z}$. On en déduit le caractère générateur de e. La liberté s'obtient par un argument similaire. ■

Fait 2 *Soit A un $\mathbb{Z}$-module non nul libre de type fini. Alors ${}^{A}\!/_{pA}$ est un anneau fini non nul.*

3.2.4 Les préliminaires à la démonstration

Lemme 4 $\sigma \in Gal_{\mathbb{Q}}(P) \Longrightarrow \sigma_{|A} \in Aut\,(A)$, *et* $\psi : \begin{array}{c} Gal_{\mathbb{Q}}(P) \to Aut\,(A) \\ \sigma \mapsto \sigma_{|A} \end{array}$ *est un isomorphisme de groupes.*

Lemme 5 $Hom\,(A,\, \mathbb{E}_p) \neq \varnothing$.

Démonstration : Soit $\mathcal{M}$ un idéal de A maximal contenant p (l'existence est assurée par le fait 2 et le lemme de Krull). Soit $\phi : A \to {}^{A}\!/_{\mathcal{M}}$ le morphisme surjectif canonique d'anneaux. On a $\mathbb{F}_p \subset {}^{A}\!/_{\mathcal{M}}$ car $\phi(p) = 0$ et $\phi(1) \neq 0$ (${}^{A}\!/_{pA}$ est non nul). Par ailleurs, ${}^{A}\!/_{\mathcal{M}}$ est généré par $(\phi(x_i))_{i\leq n}$ et est un corps. Enfin, $\phi(P) = \chi_p(P) = \prod_{i\leq n}(X - \phi(x_i))$, donc les $\phi(x_i)$ sont les racines de $\chi_p(P)$.

Donc ${}^{A}\!/_{\mathcal{M}} = \mathbb{F}_p\big[\chi_p(P) = \mathbb{E}_p$. Donc, $\phi \in Hom\,(A,\, \mathbb{E}_p)$. ■

Fixons $\tau \in Hom\,(A,\, \mathbb{E}_p)$ une fois pour toutes.

3.2.5 Structure de $Hom\,(A,\, \mathbb{E}_p)$

Lemme 6 *Soit M un $\mathbb{Z}$-module libre de type fini et L un corps. Alors, $End_{\mathbb{Z}}(M,\, L)$ est de dimension égale au rang de M.*

Proposition 5 (description des prolongements de la réduction modulo p)

$$Hom\,(A,\, \mathbb{E}_p) = \{\tau \circ \sigma,\, \sigma \in Aut\,(A)\}\,.$$

Démonstration : On a déjà $Hom\,(A,\, \mathbb{E}_p) \subset \{\tau \circ \sigma,\, \sigma \in Aut\,(A)\}$. On conclut par un argument de cardinalité.

Le théorème de Dedekind permet d'affirmer que les élément de $Hom\,(A,\, \mathbb{E}_p)$ sont linéairement indépendants. Or, $Hom\,(A,\, \mathbb{E}_p) \subset End_{\mathbb{Z}}(A,\, \mathbb{E}_p)$. Donc,

$$\begin{array}{ccccc} dim_{\mathbb{E}_p}(End_{\mathbb{Z}}(A,\, \mathbb{E}_p)) & \geq & \#Hom\,(A,\, \mathbb{E}_p) & \geq & [K : \mathbb{Q}] \\ || & & & & \\ \text{rg } A = [K : \mathbb{Q}] & & & & \end{array},$$

l'inégalité de droite provenant du fait que les $\tau \circ \sigma$ sont deux-à-deux distincts et $\#Aut\,(A) = \#Gal_{\mathbb{Q}}(P) = [K : \mathbb{Q}]$. Pourquoi les $\tau \circ \sigma$ sont-il deux-à-deux distincts ? $\boldsymbol{\chi_p(P)}$ **est séparable** : donc τ est injectif sur $\{x_i\}_{i\leq n}$. Or, $\sigma \neq \sigma' \Longrightarrow \exists\, i \;/\; \sigma(x_i) \neq \sigma'(x_i)$ (les x_i engendrent A). D'où le résultat. ■

3.2.6 Groupe de Galois et réduction modulo p

Théorème 7 *Soit $P \in \mathbb{Z}[X]$, de racines distinctes $x_1,\, \ldots,\, x_n$, tel que $\chi_p(P)$ soit encore à racines simples dans son corps de décomposition. Alors,*

$$\boldsymbol{Gal_{\mathbb{F}_p}(\chi_p(P))} \textbf{ est un sous-groupe de } \boldsymbol{Gal_{\mathbb{Q}}(P)}.$$

Démonstration : Soit $\sigma \in Gal_{\mathbb{F}_p}(\chi_p(P))$. Soit $\tilde{\sigma}$ l'unique élément de $Aut\,(A)$ tel que $\sigma \circ \tau = \tau \circ \tilde{\sigma}$, d'après la proposition 5.

Alors, $\Phi : \begin{array}{c} Gal_{\mathbb{F}_p}(\chi_p(P)) \to Aut\,(A) \simeq Gal_{\mathbb{Q}}(P) \\ \sigma \mapsto \tilde{\sigma} \end{array}$ est un morphisme injectif de groupes.

Vérifions que c'est un morphisme : $\sigma_1 \circ \sigma_2 \circ \tau = \tau \circ \Phi(\sigma_1 \circ \sigma_2) = \sigma_1 \circ (\sigma_2 \circ \tau) = (\sigma_1 \circ \tau) \circ \Phi(\sigma_2) = \tau \circ \Phi(\sigma_1) \circ \Phi(\sigma_2)$. D'après la même proposition : $\Phi(\sigma_1 \circ \sigma_2) = \Phi(\sigma_1) \circ \Phi(\sigma_2)$.

Enfin, il est injectif car si $\Phi(\sigma) = Id$, *ie* $\sigma \circ \tau = \tau$, σ laisse forcément invariants les $\tau(x_i)$, qui sont distincts. Donc $\sigma = Id$. ■

3.3 $\mathfrak{S}_n$ est un groupe de Galois sur $\mathbb{Q}$

Lemme 7 *Soit $G \subset \mathfrak{S}_n$ un groupe de permutations transitif contenant un $(n-1)$-cycle et une transposition. Alors, $G = \mathfrak{S}_n$.*

Lemme 8 *Soient $p \in \mathcal{P}$ et n un entier. Alors, il existe un polynôme irréductible et à racines simples de degré n dans $\mathbb{F}_p[X]$.*

Démonstration : Le sous-groupe fini $(F_{p^n}^*, \times)$ est cyclique : il est donc engendré par un élément α. Or, on sait que $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = deg \prod_{\alpha}^{\mathbb{F}_p} = n$: le polynôme minimal de α est donc irréductible de degré n sur $\mathbb{F}_p$.

On note que si dP est non-nul, alors $pgcd\ (P,\ dP) = 1$, et donc P est à racines simples. Supposons $dP = 0$. Alors, $P \in \mathbb{F}_p[X^p]$: $P = \sum a_i (X^p)^i = \sum a_i^p (X^p)^i = \sum (a_i X^i)^p = (\sum a_i X^i)^p$, d'après le lemme 1. Cela signifierait que P est réductible. C'est absurde.

Donc, P est irréductible à racine simples. ■

Résultat 2 *Il existe $P \in \mathbb{Z}[X]$ tel que $Gal\left(\mathbb{Q}^{\left|P\right.}/\mathbb{Q}\right) \simeq Gal_{\mathbb{Q}}(P) = \mathfrak{S}_n$.*

Démonstration : Soit p un nombre premier tel que $p \geq n$. D'après le lemme précédent, on peut poser sans aucun problème : $P_1,\ P_2,\ P_3 \in \mathbb{Z}[X]$, unitaires et de degré n tels que :

- $\chi_2(P_1)$ est irréductible,
- $\chi_3(P_2)$ est le produit d'un facteur irréductible de degré $n-1$ par X,
- $\chi_5(P_3)$ est le produit d'un facteur irréductible de degré 2 et d'un facteur irréductible de degré $n-2$,

et tels que ces trois polynômes soit à racines simples.

Posons alors $P = -15P_1 + 10P_2 + 6P_3$, tel que la réduction modulo 2, 3 et p de P soit égale (à un facteur non-nul près) à respectivement celle de P_1, P_2 et P_3. P est à racines simples car sa réduction modulo 2 l'est aussi. On peut donc appliquer le théorème 7 et le corollaire 1 pour conclure que $Gal_{\mathbb{Q}}(P)$ est transitif, contient un cycle de longueur $n-1$ et une transposition.

Le lemme 7 assure alors que $Gal_{\mathbb{Q}}(P) = \mathfrak{S}_n$. ■

Il existe d'autres démonstrations de ce résultat.

Dans le problème 14 de [4] une des premières méthodes de théorie de Galois inverse est présentée. Basée sur la propriété de Hilbert [2] , que tout corps de nombres vérifie, elle se résume dans cet énoncé simplifié [3] :

Résultat 3 *Pour tout corps K vérifiant la propriété de Hilbert, si G est un groupe de Galois sur $K\,(X_1,\ \ldots,\ X_n)$ alors G est un groupe de Galois sur K.*

Voici un résultat plus précis, plus constructif et dont la démonstration est plus ardue est donné dans [2].

Résultat 4 *Soit $n \geq 2$ un entier. Alors, $X^n - X - 1$ est irréductible sur $\mathbb{Q}$ et son groupe de Galois sur $\mathbb{Q}$ est $\mathfrak{S}_n$.*

4 Résolution du problème 2

Définition 5 *On appelle* corps de nombres *toute extension finie de $\mathbb{Q}$.*

Ni $\mathbb{R}$, ni $\mathbb{C}$, ni la clôture algébrique de $\mathbb{Q}$ne sont pas des corps de nombres.

Résultat 5 *Soit G un groupe fini. Alors, il existe une extension normale finie L d'un corps de nombres K tels que $G = Gal(L/K)$.*

En fait, on va montrer plus que le résultat annoncé : on peut supposer que $K/\mathbb{Q}$ est une extension finie.

Démonstration : Notons n le cardinal de G. G peut être vu comme un sous-groupe de $\mathfrak{S}_n$ puisque $\varphi : \begin{matrix} G \to \mathfrak{S}_n \\ h \mapsto \tau_h \end{matrix}$, où τ_h désigne la translation à gauche par h, est un morphisme injectif de groupes. Soit alors, d'après le résultat 2, $K/\mathbb{Q}$ une extension normale telle que $Gal(K/\mathbb{Q}) = \mathfrak{S}_n$. On applique ensuite le théorème d'Artin qui dit que K/K_G est une extension normale finie de groupe de Galois G. ■

[2] Soit K un corps :
Une partie $A \subset K^n$ est *Zariski-dense* si le polynôme nul est le seul élément de $K[X_1,\ \ldots,\ X_n]$ à s'annuler sur tout A.
Propriété de Hilbert : pour tout entier $n \geq 1$ et pour tout polynôme $P_{X_1,\ldots,X_n}(T)$ irréductible de $K\,(X_1,\ \ldots,\ X_n)\,[T]$, il existe une partie A Zariski-dense de K^n telle que $\forall\, x_1,\ \ldots,\ x_n \in A$, $P_{x_1,\ldots,x_n}(T)$ soit irréductible dans $K[T]$.

[3] L'énoncé donné dans [4] étend le résultat à tout corps vérifiant la propriété de Hilbert, à condition de considérer les extensions de corps *galoisiennes*.

5 Les groupes abéliens

5.1 Groupe de Galois de $\mathbb{Q}/\mathbb{Q}(\xi)$, ξ racine n-ième primitive

Dans la suite, on fixe n et on adopte la notation $\xi = e^{2i\pi/n}$; on note φ l'indicatrice d'Euler.

Définition 6 *Pour $n \in \mathbb{N}^*$, on appelle* n-ième polynôme cyclotomique*, que l'on note Φ_n,*

$$\Phi_n = \prod_{\substack{0\leq k\leq n\\ k\wedge n=1}} \left(X - e^{2ik\pi/n}\right) = \prod_{z\in\mathbb{C}^* \ / \ \omega(z)=n} (X-z).$$

Voici une première propriété intéressante :

Proposition 6 $\Phi_n \in \mathbb{Z}[X]$.

Lemme 9 *Soit x une racine n-ième de l'unité. Alors, pour tout p premier ne divisant pas n, $\prod_{x^p}^{\mathbb{Q}} = \prod_x^{\mathbb{Q}}$.*

Démonstration : Grâce au lemme 1, on remarque que $\overline{\prod_x^{\mathbb{Q}}(X^p)} = \overline{\prod_x^{\mathbb{Q}}(X)}^p$, où $\overline{P}$ désigne le réduit modulo p de P. Ainsi, $\overline{\prod_x^{\mathbb{Q}}(X)}$ annule x^p. Supposons alors $\prod_{x^p}^{\mathbb{Q}} \neq \prod_x^{\mathbb{Q}}$: comme ces polynômes sont irréductibles et divisent tous deux X^n-1, leur produit divise X^n-1. Ainsi, x^p est racine double de X^n-1, ce qui est absurde car $p\wedge n = 1$ et donc $pgcd\left(X^n-1,\, nX^{n-1}\right) = 1$. ■

Proposition 7 *Φ_n est le polynôme minimal sur $\mathbb{Q}$ de ξ.*

Démonstration : Soit x une racine de Φ_n. Alors, $x = \xi^k$ où $k\wedge n = 1$. Si $\prod_i p_i$ est la décomposition en nombres premiers de k, on sait alors que $\forall\, i,\ p_i \wedge n = 1$. En appliquant un nombre fini de fois le lemme précédent, on obtient que x est racine de $\prod_\xi^{\mathbb{Q}}$. Comme par ailleurs, $\Phi_n \in \mathbb{Z}[X]$ et est unitaire, on a $\prod_\xi^{\mathbb{Q}} = \Phi_n$. ■

Proposition 8

$$Gal(\mathbb{Q}(\xi)/\mathbb{Q}) \simeq \left(\mathbb{Z}/_{n\mathbb{Z}}\right)^*.$$

Démonstration : On montre que $\Psi \ : \ \begin{array}{c}\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^* \to Gal(\mathbb{Q}(\xi)Q)\\ \chi_n(p) \mapsto \sigma_p\end{array}$, où σ_p est défini par $\sigma_p(\xi) = \xi^p$, est un isomorphisme.

Montrons d'abord que σ_p est bien défini. Soit $P(\xi) = Q(\xi) \in \mathbb{Q}(\xi)$; alors, en effectuant la division euclidienne de P puis Q par Φ_n, on obtient des restes R_P et R_Q tels que $R_P(\xi) - R_Q(\xi) = 0$. Pour des arguments de minimalité de degré, on a forcément $R_P = R_Q$; or, $\Phi_n(\xi^p) = 0$ car p est premier avec n et donc ξ^p une racine primitive. Donc : $P(\xi^p) = Q(\xi^p) = R_P(\xi^p)$. Ensuite, σ_p, qui laisse donc stable $\mathbb{Q}$, est surjectif car, si $kn + mp = 1$, alors $\sigma_p(\xi^{(k-1)n}) = \xi$. Enfin, σ_p est injectif car $P(\xi^p) = 0$ implique $\Phi_n = \prod_{\xi^p}^{\mathbb{Q}} \mid P$.

Il est alors facile de vérifier que Ψ est un morphisme bien défini, injectif. Le caractère bijectif résulte de l'égalité des cardinaux. ■

5.2 Tout groupe abélien fini est un groupe de Galois sur $\mathbb{Q}$

On suppose connus dans ce paragraphe, et on admet, deux résultats :

Théorème 8 (Structure des groupes abéliens finis) *Soit G un groupe abélien fini. Alors, il existe $(n_i)_{i\leq n} \in (\mathbb{N}^* \setminus \{1\})^q$ tels que $G \simeq \prod_{i\leq q} \mathbb{Z}/_{n_i\mathbb{Z}}$.*

Théorème 9 *Soit $n \geq 2$. Alors il existe une infinité de nombres premiers congrus à 1 modulo n.*

Résultat 6 *Tout groupe abélien fini G est un groupe de Galois sur $\mathbb{Q}$.*

Démonstration : On montre d'abord un résultat intéressant à savoir que G est un quotient de $\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^*$ pour n bien choisi. D'après le théorème de structure des groupes abéliens finis, soit $(n_i)_{i\leq q} \in (\mathbb{N}^* \setminus \{1\})^q$ telle que $G \simeq \prod_{i\leq q} \mathbb{Z}/_{n_i\mathbb{Z}}$. Ensuite, d'après le cas particulier du théorème de progression arithmétique exposé ci-dessus,

notons p_i q nombres premiers distincts tels que $\forall\, i,\ p_i \equiv 1\,[n_i]$. On en déduit qu'il existe un morphisme surjectif de $\prod_{i\leq p} \mathbb{Z}/(p_i-1)\mathbb{Z}$ sur G. Or, $\prod_{i\leq p} \mathbb{Z}/(p_i-1)\mathbb{Z}$ est classiquement isomorphe à $\prod_{i\leq p} \left(\mathbb{Z}/p_i\mathbb{Z}\right)^*$, lui-même isomorphe, d'après le théorème chinois à $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$, en posant $n = \prod_{i\leq q} p_i$. Ainsi, G est un quotient de $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$.

Soit alors $\xi = e^{2i\pi/n}$. On sait que $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ et $Gal(\mathbb{Q}(\mu)/\mathbb{Q})$ sont isomorphes. On applique alors le résultat 1 pour conclure que G est un groupe de Galois. ■

Disposant déjà de trois résultats, remarquons qu'il est difficile, en les combinant de parvenir à en établir d'autres. En effet, on n'a pas de résultats précis sur les produits directs de groupes de Galois. Par ailleurs, tous les quotients de groupes abéliens sont abéliens, et les seuls quotients de $\mathfrak{S}_n$ sont $\mathfrak{S}_n$, $\mathbb{Z}/2\mathbb{Z}$ et le groupe nul, pour $n \geq 5$.

6 Aperçu d'autres résultats (admis)

Résultat 7 *$GL_2(\mathbb{F}_p)$ est un $\mathbb{Q}$-groupe de Galois.*

Résultat 8 (Shafarevich 1954) *Tout groupe fini résoluble est un $\mathbb{Q}$-groupe de Galois.*

Résultat 9 (Feit et Thompson 1962) *Tout groupe fini d'ordre impair est un $\mathbb{Q}$-groupe de Galois.*

Démonstration : En fait, le résultat démontré par Feit et Thomson est que tout groupe fini d'ordre impair est résoluble. ■

Références

[1] Daniel Perrin, *Cours d'algèbre*, ENSJF, 1988

[2] Alain Kraus, *Théorie de Galois, cours accéléré de DEA*, Université de Paris VI, Octobre 1998

[3] Claude Mutafian, *Équations algébriques et théorie de Galois*, Vuibert, 1980

[4] Bruno Deschamps, *Problèmes d'arithmétique des corps et de théorie de Galois*, Hermann

[5] Nicolas Tosel, *Théorie de Galois élémentaire*, 1999

[6] Nicolas Markey, *La théorie de Galois*, ENS Cachan, 1999