YVES GÉRARD

Un exemple de groupe de Galois d'une extension transcendante

Publications du Département de Mathématiques de Lyon, 1982, fascicule 6A
« Quelques éléments pour l'étude du groupe de Galois d'une extension transcendante », ,
p. 15-22

<http://www.numdam.org/item?id=PDML_1982___6A_15_0>

UN EXEMPLE DE GROUPE DE GALOIS D'UNE EXTENSION TRANSCENDANTE

par Yves GERARD

0) INTRODUCTION.

On se propose d'exhiber une extension transcendante $\mathbb{C} \to K$ dont le groupe des $\mathbb{C}$-automorphismes $\mathrm{Gal}(K|\mathbb{C})$ est isomorphe à un produit semi-direct topologique $G \underset{s}{\times} \mathbb{Q}^{\times}$, où $\mathbb{Q}^{\times}$ est muni de la topologie discrète et G est une limite projective de groupes discrets de la forme $\mathbb{C}|nL$, pour $n \in \mathbb{N}^{\times}$. Cet exemple est dû à A. ROBERT qui en donne une démonstration esquissée dans [1].

On a choisi volontairement des références qui, notamment pour la géométrie algébrique, renvoient autant que possible à des ouvrages élémentaires, et l'on a pris le soin d'écrire en détail certaines démonstrations "bien connues".

1) CONSTRUCTION DE K - STRUCTURE DE K.

(1.1) On considère dans $\mathbb{C}$ un réseau L non singulier, i.e. tel que $\mathrm{End}(L) = \mathbb{Z}$. Pour tout $n \in \mathbb{N}^{\times}$, on note $K_n = R(\mathbb{C}|nL) = \mathbb{C}(\wp_n, \wp'_n)$ le corps des fonctions nL-elliptiques ($\wp_n$ est la fonction de Wierstrass relative à nL et $\wp'_n$ sa dérivée) (voir par exemple [3]).
Si $n|m$ on a $mL \subset nL$ et $K_n \subset K_m$. Les K_m sont d'ailleurs tous distincts pour $n \in \mathbb{N}^{\times}$ (voir lemme (5.3) plus loin).

Si l'on pose $K = \bigcup_{n \in \mathbb{N}^{\times}} K_n$, K est une extension (transcendante) de $\mathbb{C}$, de dimension algébrique 1.

(1.2) $K_1 \to K_m$, pour tout $m \in \mathbb{N}$, est *une extension algébrique de degré fini égal à* m^2.

En effet (voir par exemple [2] , th. 4, p. 18, théorie des diviseurs) on a

$$[K_m : \mathbb{C}(\wp_1)] = 2m^2$$

et l'on sait que $[K_1 : \mathbb{C}(\wp_1)] = 2$ (voir par exemple [3], ou [2] p. 36).

Plus généralement : $[K_m : K_n] = (\frac{m}{n})^2$ si $n|m$.

(1.3) $K_n \to K_m$ (n divisant m) est en fait une *extension algébrique galoisienne dont le groupe de galois est isomorphe à* nL/mL.

En effet, on a une suite exacte

$$0 \to mL \to nL \to \mathrm{gal}(K_m/K_n)$$
$$\omega \to t_\omega$$

en posant $t_\omega(f)(z) = f(z+\omega)$. (voir démonstration du lemme (5.3), pour le noyau).

On a donc une injection $nL/mL \overset{i}{\hookrightarrow} \mathrm{gal}/K_m/K_n)$ et ces "translations" dans gal (K_m/K_n) montrent déjà que

$$K_m^{\mathrm{gal}(K_m/K_n)} = K_n \text{ , i.e. } K_n \hookrightarrow K_m \text{ est galoisienne.}$$

De plus nL/mL est de cardinal fini égal à $(\frac{m}{n})^2 = [K_m:K_n]$ et ainsi i est une bijection.

2) $\mathbb{Q}^\times \underset{s}{\hookrightarrow} \mathrm{Gal}(K/\mathbb{C})$.

Si $a \in \mathbb{Q}^\times$, on définit une "homothétie" s_a par

$$s_a(f)(z) = f(az) \text{ ,} \qquad z \in \mathbb{C} \text{ (si z n'est pas un pôle de f) et } f \in K.$$

Si $a = \frac{m}{n} \in \mathbb{Q}^\times$, on a un $\mathbb{C}$-isomorphisme $K_{pm} \xrightarrow{\sim} K_{pn}$ pour tout $p \in \mathbb{N}^\times$, et ainsi $a \to s_a$ est un morphisme injectif de groupes $s : Q^\times \hookrightarrow \mathrm{Gal}(K|\mathbb{C})$ (voir plus loin, démonstration du lemme (5.3)).

3) On peut faire opérer $\mathbb{C}$ par translation sur la variable de $f \in K$ et obtenir ainsi, pour tout $n \in \mathbb{N}^\times$, un groupe d'automorphismes de K_n, isomorphe à $\mathbb{C}|nL$. Dans $\mathrm{Gal}(K|\mathbb{C})$, on aura donc des "translations généralisées" qui seront par définition des éléments de $\varprojlim_{n \in \mathbb{N}^\times} \mathbb{C}/nL$.

$\mathbb{Q}^\times$ opère sur $\varprojlim \mathbb{C}/nL$ (voir (2) et (6.1)) et la *seule difficulté est de montrer que tout élément de* $\mathrm{Gal}(K|\mathbb{C})$ *est obtenu par composition d'une homothétie avec une translation généralisée.*

Dans la suite on va, en fait, définir un morphisme $\pi : \mathrm{Gal}(K|\mathbb{C}) \to \mathbb{Q}^\times$ qui aura pour section s, ce qui donnera le produit semi-direct cherché. Auparavant, on a besoin de rappeler la description d'une structure de variété algébrique sur le tore analytique $\mathbb{C}/nL$.

4) STRUCTURE ALGEBRIQUE ET STRUCTURE ANALYTIQUE SUR $\mathbb{C}/nL$.

(4.1) On sait que l'on a une bijection (pour tout $n \in \mathbb{N}^\times$), notée α,

$$\begin{aligned} \mathbb{C}/nL - \{0\} &\longrightarrow V = V(Y^2-4X^3+g_2X+g_3) \\ z &\longmapsto (\wp_n(z), \wp_n'(z)) \end{aligned}$$

où V est la sous-variété affine de $\mathbb{C}^2$ définie par $P(X,Y) = Y^2-4X^3+g_2X+g_3$ (voir [2], [3], [4] ou [8] où l'on trouve en particulier les définitions de g_2 et g_3).

Par transport de structure, on peut considérer $\mathbb{C}/nL - \{0\}$ *comme une variété algébrique affine.*

(4.2) $\mathbb{C}/nL - \{0\}$ est *irréductible.*

Car $P(X,Y) = Q(Y) = Y^2-q(X)$ et Q est irréductible dans $(\mathbb{C}[X])[Y]$.

(4.3) $\mathbb{C}/nL - \{0\}$ est *sans singularité.*

Si $(x,y) \in V$ on ne peut avoir $\begin{cases} -12x^2+g_2 = 0 \\ 2y = 0 \end{cases}$, car $(\pm(\frac{g_2}{12})^{1/2},0)$ n'appartient pas à V (autrement en remplaçant dans $4\,X^3-g_2X-g_3=0$ on obtiendrait $g_2^3-27g_3^2=0$ ce qui est contradictoire car l'équation a 3 racines distinctes (voir par exemple [4] p. 11).

(4.4) $\mathbb{C}/nL$ *est une variété projective irréductible* (complétion projective de $\mathbb{C}/nL-\{0\}$) .

Si l'on note $q : \mathbb{C}^3-\{0\} \to \mathbb{P}_2(\mathbb{C})$ la projection canonique, on peut identifier $\mathbb{C}^2$ avec une partie de $\mathbb{P}_2(\mathbb{C})$ avec par exemple :

$$(x,y) \to q(x,y,1).$$

V alors s'injecte dans sa complétion projective $\bar{V} = V_p(ZY^2-4X^3+g_2XZ^2+g_3Z^3)$ (sous-variété fermée de $P_2(\mathbb{C})$ et l'on a

$$\bar{V}\cap\mathbb{C}^2 = V$$

$$\text{et} \qquad \bar{V} = V\cup\{\infty\} \qquad \text{avec} \quad \infty = q(0,1,0),$$

et puisque V est irrédutible, $\bar{V}$ l'est aussi. On prolonge α (voir (4.1)) en un *isomorphisme algébrique* $\bar{\alpha} : \mathbb{C}/nL \xrightarrow{\sim} \bar{V}$ en posant

$$\bar{\alpha}(0) = \infty.$$

(4.5) $\mathbb{C}/nL$ est une variété projective *sans singularité.*

Dans la carte $U_2 \simeq \mathbb{C}^2$ (2ème composante homogène non nulle), ∞ s'identifie à (0,0) et la courbe est définie par

$$H(X,Z) = Z-4X^3+ g_2XZ^2+g_3Z^3$$

$$\text{donc} \quad \frac{\partial H}{\partial Z}\ (0,0) \neq 0.$$

(4.6) *Le corps des fonctions rationnelles sur* $\mathbb{C}/nL$ est

$$k(\mathbb{C}/nL) \simeq K_n.$$

En effet, $k(\mathbb{C}/nL)$ est isomorphe à $k(\mathbb{C}/nL-\{0\})$. Si l'on note x (resp. y) la restriction de la projection pr_1 (resp. pr_2) à V et $\mathbb{C}[x,y]$ la sous-algèbre de $\mathscr{F}(V,\mathbb{C})$ (algèbre des fonctions de V danc $\mathbb{C}$), le morphisme canonique $\mathbb{C}[X,Y] \to \mathbb{C}[x,y]$ donne par passage au quotient un isomorphisme $\Gamma(V) \xrightarrow{\sim} \mathbb{C}[x,y]$ où $\Gamma(V) = \mathbb{C}[X,Y]/I(V)$ est l'anneau des fonctions régulières de la variété affine V. Ainsi, par α (voir (4.1)), $\Gamma(\mathbb{C}/nL-\{o\}) \xrightarrow{\sim} \mathbb{C}[\wp_n, \wp'_n]$ et son corps des fractions $k(\mathbb{C}/nL-\{\ \})$ s'identifie à $\mathbb{C}(\wp_n, \wp'_n) = K_n$.

(4.7) $\bar{V}$ *est aussi une sous-variété analytique de* $\mathbb{P}_2(\mathbb{C})$ (voir (4.3)).
et $\alpha : \mathbb{C}/nL \to \bar{V}$ *est un isomorphisme analytique.*

(L'application $z \to (\wp_n(z), \wp'_n(z))$ a une dérivée non nulle en tout point de $C/nL-\{0\}$ et le prolongement de α peut s'écrire :

$$\bar{\alpha}\ (z) = q\ (z^3\ \wp_n(z),\ z^3\ \wp'_n(z), z^3)).$$

5) CONSTRUCTION DE Π : $\mathrm{Gal}(K/\mathbb{C}) \to \mathbb{Q}^\times$.

(5.1) Soit $\sigma \in \mathrm{Gal}(K/\mathbb{C})$. Pour tout $n \in \mathbb{N}^\times$, il existe $m_n \in \mathbb{N}^\times$ tel que $\sigma(K_n) \subset K_{m_n}$, d'où un $\mathbb{C}$-endomorphisme σ_n :

$$\begin{tikzcd}
K_n \arrow[rr, "\sigma_n"] \arrow[dr, "\sigma/K_n"'] & & K_n \\
& K_{m_n} \arrow[ur, dashed, "s_{m_n/n}"'] &
\end{tikzcd}$$

($s_{m_n/n}$ homothétie , voir 2)).

Il existe donc un *unique morphisme algébrique dominant* (ici surjectif)

$$\omega_n : \mathbb{C}/nL \to \mathbb{C}/nL$$

tel que $\sigma_n(f) = f \circ \omega_n$ $(f \in K_n)$ et un diagramme commutatif

$$\begin{tikzcd}
\mathbb{C}/nL & & \mathbb{C}/nL \arrow[ll, "\omega_n"'] \arrow[dl, dashed, "m_n/n"] \\
& \mathbb{C}/m_nL \arrow[ul] &
\end{tikzcd}$$

dont on dérive le précédent par "transposition".

(Voir par exemple [5] , p. 161 cor. 2 dans le cadre des variétés quasi-projectives ou bien [6] p. 81, ou bien Mumford [7] cité dans [6] , dans un cadre plus général de variétés).

(5.2) LEMME. - *Pour tout* $\sigma \in \mathrm{Gal}(K/\mathbb{C})$ *et tout* $n \in \mathbb{N}^{\times}$, *il existe* $\mu_n \in \mathbb{Q}^{\times}$ *et* $\eta_n \in \mathbb{C}$ *tels que* $\sigma(f)(z) = f(\mu_n z+\eta_n)$, *pour tout* $f \in K_n$ *et tout* $z \in \mathbb{C}$ *(qui n'est pas un pôle de* $\sigma(f)$ *).*

En fait, ω_n défini en (5.1) est nécessairement analytique. En effet, $\bar{\alpha}$ est un isomorphisme algébrique et analytique (voir (4.1) et (4.7)) et les morphismes (réguliers) sur $\bar{V}$ sont analytiques (voir leur forme, par exemple, dans [6] , p. 35 dans le cadre des variétés quasi-projectives).

Puisque ω_n est analytique, il est de la forme $z \mapsto \nu_n z+ \eta_n$ avec $\nu_n, \eta_n \in \mathbb{C}$ (voir par exemple [8] , p. I-35). D'autre part, $\nu_n \neq 0$ puisque ω_n est surjectif. Et, enfin, $\nu_n \in \mathbb{Z} - \{0\}$ car L est non singulier et $\nu_n(nL) \subset nL$.

Si maintenant, on écrit l'image d'un élément dans le deuxième diagramme de (5.1) sous la forme :

$$\begin{tikzcd}[column sep=small] \frac{m\nu_n}{m_n}\left(\frac{m_n}{n}Z\right)+\eta_n = \nu_n Z+\eta_n & & Z \arrow[ll, "\omega_n"'] \arrow[dl, leftrightarrow, "m_n/n"] \\ & (m_n/n)Z \arrow[ul, leftrightarrow, dotted] & \end{tikzcd}$$

On obtient $\sigma_n(f)(Z) = \sigma(f)(Z) = f(\omega_n(Z)) = f(\mu_m Z+\eta_n)$ $(f \in K_n)$ en posant $\mu_m = \dfrac{n\nu_n}{m_n} \in \mathbb{Q}^{\times}$.

(5.3) *On peut évidemment définir* K_m pour $a \in \mathbb{Q}^{\times}$ *et l'on a encore* $K = \bigcup_{a \in \mathbb{Q}^{\times}} K_a$ (réunion filtrante pour la relation a divise b).

LEMME. - *(L étant non singulier), les* K_a *sont tous distincts pour* $a \in \mathbb{Q}_+^\times$.

(Remarque : $K_a = K_{-a}$*).*

Si $a,b \in \mathbb{Q}^\times$, $K_a \subset K_b$ implique $\wp_a(z+bL) = \wp_a(z)$. $z = 0$ étant un pôle de $\wp_a$ on a $bL \subset aL$ (aL est l'ensemble des pôles de $\wp_a$).

(5.4) LEMME. - *Pour tout* $a \in \mathbb{Q}^\times$ *, on a* $\mu_a = \mu_\sigma$ *, où* μ_σ *est un nombre qui ne dépend que de* σ *et* η_a *est défini modulo* aL.

Il suffit de voir que μ_a est unique pour tout $a \in \mathbb{Q}^\times$.

D'après le lemme précédent on a, si $\sigma(K_a) = K_a/\mu_a = K_a/\mu'_a$,

$$\mu_a = \pm\mu'_a.$$

Si l'on avait $\mu_a = -\mu'_a$, on aurait pour $f \in K_a$:

$$f(z) = f(-z+\bar{\eta}_a+\eta'_a)$$

donc $\eta_a+\eta'_a \in aL$ (si f est une fonction ayant aL exactement pour pôles) donc $f(z) = f(-z)$ (contradiction si f est paire). μ_a est donc unique et raisonnement analogue pour $\eta_a-\eta'_a \in aL$ si l'on a

$$f(\mu_a x+\eta_a) = f(\mu_a x+\eta'_a).$$

(5.5) D'après (5.4) on peut poser $\pi(\sigma) = \mu_\sigma$ et on a ainsi défini un *morphisme de groupes :*

$$\mathrm{gal}(K/\mathbb{C}) \overset{\Pi}{\to} \mathbb{Q}^\times$$

qui est continu (pour $\mathbb{Q}^\times$ discret) car gal $(K/K_1) \subset \mathrm{Ker}\,\Pi$ (unicité de μ_σ).

6) STRUCTURE DE Gal(K/$\mathbb{C}$).

(6.1) L'application $s : \mathbb{Q}^\times \to \mathrm{gal}(K/\mathbb{C})$ est une *section* (continue) du *morphisme* Π . On a ainsi un produit semi-direct topologique :

$$\mathrm{Ker}\,\Pi \underset{s}{\times} \mathbb{Q}^\times \overset{\sim}{-} \mathrm{Gal}(K/\mathbb{C}).$$

(6.2) LEMME. - *On a un isomorphisme topologique* $\ker\Pi \xrightarrow{\sim} \varprojlim_{n \in \mathbb{N}^\times} \mathbb{C}/nL$ *les* $\mathbb{C}/nL$ *étant des groupes discrets (infinis).*

On a un morphisme continu $\beta_n : \mathrm{Ker}\Pi \to \mathbb{C}/nL$ pour $n \in \mathbb{N}^\times$ et si $n|m$, on a $\eta_m - \eta_n \in nL$ (raisonnement analogue à celui du lemme (5.4)), d'où un morphisme *continu :*

$$\ker\Pi \xrightarrow{\beta} \varprojlim_{n \in \mathbb{N}^\times} \mathbb{C}/nL$$

qui est évidemment *bijectif.*

β est une application *ouverte* car $(\mathrm{gal}(K/K_n))_{n \in \mathbb{N}^\times}$ est un système fondamental de voisinages de l'unité dans Ker Π, et l'on a

$\beta_n^{-1}(\{0\}) = \mathrm{Gal}(K/K_n) = \beta^{-1} f_n^{-1}(\{0\})$ (si $f_n \varprojlim_m \mathbb{C}/mL \to \mathbb{C}/nL$ est la projection canonique).

i.e. : $\beta(\mathrm{Gal}(K/K_n)) = f_n^{-1}(\{0\})$.

BIBLIOGRAPHIE.

[1] A. ROBERT, *Automorphism groups of transcendental field extensions*, J. Algebra 16 (1970), p. 252-270.

[2] J.C. CHEVALLEY, *Introduction to the theory of algebraic functions of one variable*, Math. Surveys n° VI, A.M.S., 1951.

[3] J. BRACONNIER, *Théorie élémentaire des fonctions elliptiques et modulaires*, cours polycopié. Dépt. Math. Lyon.

[4] S. LANG, *Elliptic functions*, Addison-Wesley, Pub. company, 1973.

[5] W. FULTON, *Algebraic curves*, Math. Lecture note Series, BENJAMIN, 1969.

[6] A. BOREL, *Linear algebraic groups*, Math. Lecture note series, BENJAMIN, 1969.

[7] D. MUMFORD, *Introduction to algebraic geometry*, cours polycopié, Princeton.

[8] A. ROBERT, *Elliptic curves*, Lecture notes in Math. 326, Springer-Verlag, 1973.

[9] K. UENO, *Classification theory of algebraic varieties and compact couples spaces*, lecture notes in Math 439, Springer-Verlag, 1975.