ANNALES MATHÉMATIQUES BLAISE PASCAL

EMMANUEL ANDRÉO
RICHARD MASSY

# Parallélogrammes galoisiens infinis

*Annales mathématiques Blaise Pascal*, tome 8, nº 2 (2001), p. 21-45
<http://www.numdam.org/item?id=AMBP_2001__8_2_21_0>

ANNALES MATHEMATIQUES BLAISE PASCAL, VOL. 8, N° 2, PP 21-45 (2001)

# Parallélogrammes galoisiens infinis

Emmanuel Andréo
Richard Massy†

**Résumé**

We introduce a Galois theory for Galois parallelograms of infinite degree. This theory improves widely the results of [8]. In particular, we generalize the Krull theorem for infinite Galois extensions.

## 1 Introduction

Dans [8], Massy a introduit la notion de parallélogramme galoisien qui généralise celle d'extension galoisienne. Cependant, le théorème final se limite au degré fini. Une application est fournie dans [9]. Le but de ce papier est d'étendre les résultats de [8] aux parallélogrammes de degré infini. Nous mettons en évidence section 4 une théorie générale des parallélogrammes galoisiens de nature essentiellement algébrique. Les topologies de Krull sur les groupes de Galois des extensions constituant ces parallélogrammes n'interviennent que dans la section 5. Nous y présentons une théorie de Galois infinie en dimension 2 généralisant aux parallélogrammes de degré quelconque le théorème de Krull pour les extensions galoisiennes infinies. Cette théorie sera appliquée dans [1] pour développer en toute généralité une notion de raffinement de tours galoisiennes, jouant pour les extensions galoisiennes de corps un rôle analogue à celui du raffinement des suites normales de groupes.

## 2 Définitions

Plusieurs des démonstrations de [8] ne nécessitent pas que les sous-groupes considérés soient normaux, autrement dit que les extensions quotients (cf. infra) soient galoisiennes : voir en particulier la section 4 pour de nouveaux résultats n'utilisant pas la normalité. Ceci justifie que l'on introduise la notion de quadrilatère corporel suivante qui généralise celle de parallélogramme galoisien.

*Définition:* Nous appelons "quadrilatère corporel" (ou "quadrilatère" en abrégé)

†Correspondant : Richard.Massy@univ-valenciennes.fr

tout quadruplet de corps $(J, K, N, L)$ dans lequel :

$(Q_0)$ $K$ et $L$ sont contenus dans un même corps ;
$(Q_1)$ $K \cap L = J$ ;
$(Q_2)$ $KL = N$ .

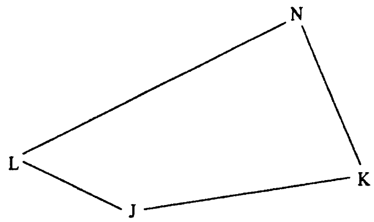


FIG. 1 -

Le quadrilatère ${}^t(J, K, N, L) = (J, L, N, K)$ sera dit "transposé" de $(J, K, N, L)$.

La définition suivante est initée dans la section 3 de [8]. Le cas des extensions galoisiennes justifie la terminologie.

*Définition:* (1) Soit $E/F$ une extension algébrique. Nous appelons "sous-extension" (resp. "extension quotient") de $E/F$ toute extension $E/M$ (resp. $M/F$) où $M$ est un corps intermédiaire : $F \subseteq M \subseteq E$.

(2) Soit $(J, K, N, L)$ un quadrilatère corporel. Nous appelons "sous-quadrilatère" (resp. "quadrilatère quotient") de $(J, K, N, L)$ tout quadrilatère $(M, E, N, F)$ (resp. $(J, E, C, F)$ ) où $E$ et $F$ sont deux corps intermédiaires :

$K \subseteq E \subseteq N$ , $L \subseteq F \subseteq N$ $\quad \big($resp. $J \subseteq E \subseteq K$ , $J \subseteq F \subseteq L\big)$.

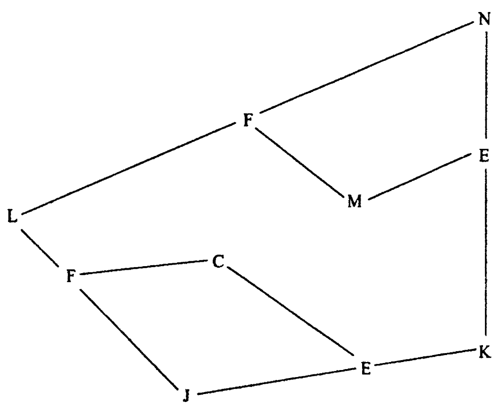


FIG. 2 -

Nous aurons besoin du lemme immédiat suivant pour les monotonies des bijections des sections 5 et 6.

**Lemme 2.1** *(1) Soit $E/F$ une extension algébrique. Dans l'ensemble des sous-extensions (resp. des extensions quotients) de $E/F$, la relation définie par*

$$(E/M') \leq (E/M) \Leftrightarrow M \subseteq M' \quad \Big(\text{resp. } (M/F) \leq (M'/F) \Leftrightarrow M \subseteq M' \Big)$$

*est une relation d'ordre.*

*(2) Soit $(J, K, N, L)$ un quadrilatère corporel. Dans l'ensemble des sous-quadrilatères (resp. des quadrilatères quotients) de $(J, K, N, L)$, la relation définie par*

$$(M', E', N, F') \leq (M, E, N, F) \quad \Leftrightarrow \quad (E \subseteq E' \,,\, F \subseteq F')$$
$$\Big(\text{resp. } (J, E, C, F) \leq (J, E', C', F') \quad \Leftrightarrow \quad (E \subseteq E' \,,\, F \subseteq F')\Big)$$

*est une relation d'ordre.*

Bien qu'exprimée en termes différents, la définition suivante coïncide avec celle de [8, Déf.1.1].

*Définition:* Nous appelons "parallélogramme galoisien" (ou "parallélogramme" en abrégé) un quadrilatère corporel $(J, K, N, L)$ dans lequel toutes les arêtes $K/J$, $N/K$, $N/L$, $L/J$ sont des extensions galoisiennes. Nous le notons alors $[J, K, N, L]$.

Clairement, pour qu'un quadrilatère $(J, K, N, L)$ soit un parallélogramme, il faut et il suffit que les extensions $K/J$ et $L/J$ soient galoisiennes. En convenant de figurer par des segments parallèles de longueurs égales les extensions dont les groupes de Galois sont isomorphes, on obtient une figure du type

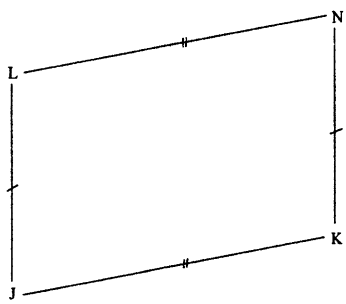


FIG. 3 -

Par composition, la "diagonale $N/J$" d'un parallélogramme $[J, K, N, L]$ est nécessairement galoisienne. Dans [8] , "le degré" d'un parallélogramme galoisien $[J, K, N, L]$ est défini comme étant le couple des degrés des extensions $N/K$ et $K/J$ :

$$deg[J, K, N, L] := \big( [N : K] \,,\, [K : J] \big).$$

Ce degré sera dit "infini" quand l'un des degrés $[N : K]$ ou $[K : J]$ est infini. Lorsque $K = J$ ou $L = J$, nous disons que le quadrilatère $(J, K, N, L)$ est "plat". Tout corps s'identifie au quadrilatère plat $(F, F, F, F)$. Toute extension (resp. toute extension galoisienne) $E/F$ s'identifie au quadrilatère plat (resp. au parallélogramme plat) $(F, E, E, F)$ (resp. $[F, E, E, F]$) ou à son transposé.

Pour définir enfin le groupe de Galois d'un parallélogramme, plaçons-nous dans la catégorie produit $\mathbf{Gr^2} = \mathbf{Gr} \times \mathbf{Gr}$ de la catégorie des groupes par elle-même. Nous appelons "bigroupe" un objet de $\mathbf{Gr^2}$, c'est à dire un couple de groupes. Autrement dit, un bigroupe est un (objet en) groupe(s) dans la catégorie produit $\mathbf{Ens^2}$ de la catégorie des ensembles par elle-même.

*Définition:* [8, Déf.3.6] Soit $[J, K, N, L]$ un parallélogramme galoisien. Nous appelons "groupe de Galois de $[J, K, N, L]$ ", et nous notons $Gal[J, K, N, L]$ le bigroupe :

$$Gal[J, K, N, L] := (Gal(N/K), Gal(N/L)).$$

Les notions de sous-groupe, de sous-groupe normal et de groupe quotient de $Gal[J, K, N, L]$ se définissent de manière évidente à partir des objets correspondants de $\mathbf{Gr^2}$ (cf. [8, Sect.3] ). Munis des topologies convenables, nous y reviendrons section 6.

## 3 Propriétés topologiques

Cette section 3 est préparatoire ; elle regroupe des résultats indépendants nécessaires aux raisonnements des sections 4 et 6.

Soit $E/F$ une extension galoisienne de degré infini. Munissons le groupe de Galois $G := Gal(E/F)$ de sa topologie de Krull (cf. [6] ou [5, p.340]). Par les propriétés générales des groupes topologiques, on sait que pour tout sous-groupe $H$ de $G$, l'adhérence $\overline{H}$ de H est un sous-groupe de G [3, TG III.7]. C'est le groupe de Galois de $E$ sur le corps des invariants de $H$ dans $E$ [5, p.344] i.e.

$$\overline{H} = Gal(E/E^H). \tag{3.1}$$

**Proposition 3.1** *(1) La normalité d'un sous-groupe de G dans un autre implique la normalité de leurs adhérences :*

$$\forall A \leq G \quad \forall B \leq G \qquad A \trianglelefteq B \quad \Rightarrow \quad \overline{A} \trianglelefteq \overline{B}.$$

*(2) Pour tout sous-groupe H de G, le corps des invariants dans E du sous-groupe H et de son adhérence $\overline{H}$ sont égaux :*

$$E^H = E^{\overline{H}}.$$

PREUVE: (1) Fixons-nous $\alpha \in A$, et considérons l'application

$$\begin{aligned} f_\alpha &: G \longrightarrow G \\ &\gamma \longmapsto \alpha^\gamma = \gamma^{-1}\alpha\gamma \end{aligned}$$

Par la normalité de $A$ dans $B$, on a clairement $f_\alpha(B) \subseteq A$, et comme $f_\alpha$ est continue [3, TGI.9]

$$f_\alpha(\overline{B}) \subseteq \overline{f_\alpha(B)} \subseteq \overline{A}.$$

Fixons-nous ensuite un $\beta \in \overline{B}$. Pour l'automorphisme intérieur

$$\begin{aligned} g_\beta &: G \longrightarrow G \\ &\gamma \longmapsto \gamma^\beta, \end{aligned}$$

on a

$$\forall \alpha \in A \quad g_\beta(\alpha) = f_\alpha(\beta) \in \overline{A},$$

de sorte que

$$\forall \beta \in \overline{B} \quad g_\beta(A) \subseteq \overline{A}.$$

Par la continuité de $g_\beta$, on en déduit que

$$g_\beta(\overline{A}) \subseteq \overline{g_\beta(A)} \subseteq \overline{A}.$$

Donc

$$\forall \beta \in \overline{B} \quad \forall \alpha \in \overline{A} \quad g_\beta(\alpha) = \alpha^\beta \in \overline{A},$$

ce qui exprime précisément que $\overline{A} \trianglelefteq \overline{B}$.
(2) D'après le (2-1) ci-dessus et le fait que la sous-extension $E/E^H$ soit galoisienne, on a directement

$$E^{\overline{H}} = E^{Gal(E/E^H)} = E^H .$$

□

**Proposition 3.2** *Soit $N/K$ une extension galoisienne. Pour tout corps intermédiaire $E$, $K \subseteq E \subseteq N$, la topologie de Krull de $Gal(N/E)$ est égale à la topologie induite sur $Gal(N/E)$ par la topologie de Krull de $Gal(N/K)$.*

PREUVE: Posons $\Gamma := Gal(N/K)$, $A := Gal(N/E)$ et soit $\alpha$ un élément quelconque de $A$. Prouvons d'abord que tout voisinage $V$ de $\alpha$ pour la topologie de Krull de $A$ est aussi un voisinage de $\alpha$ pour la topologie induite sur $A$ par celle de $\Gamma$. Par définition de la topologie de Krull de $A$, il existe une extension galoisienne finie $M/E$, avec $M \subseteq N$, telle que $V \supseteq \alpha Gal(N/M)$. En vertu du théorème de l'élément primitif, il existe d'autre part un élément $x \in E$ tel que $M = E(x)$. Soient $P(X) = Irr(x, K, X)$ le polynôme minimal de $x$ sur $K$, et $R := \{x{=}x_1, \ldots, x_n\}$ l'ensemble des racines de $P(X)$ dans une clôture algébrique fixée de $K$. Puisque l'extension $N/K$ est normale, on a $R \subseteq N$. Considérons alors le corps intermédiaire $F := K(R)$. C'est un corps de décomposition, donc l'extension $F/K$ est galoisienne finie, et comme $x = x_1 \in R$, on a clairement $M = E(x) \subseteq EF$. On en déduit que

$$Gal(N/M) \geq Gal(N/EF) = Gal(N/E) \cap Gal(N/F) = A \cap Gal(N/F)\,,$$

d'où

$$V \supseteq \alpha\, Gal(N/M) \supseteq \alpha\,(A \cap Gal(N/F)) = \alpha A \cap \alpha\, Gal(N/F)\,.$$

Ainsi $V \supseteq A \cap \alpha\, Gal(N/F)$ car $\alpha \in A$. Or $\alpha\, Gal(N/F)$ est un voisinage de $\alpha$ pour la topologie de Krull de $\Gamma$ puisque $F/K$ est galoisienne finie. Ceci prouve que $V$ est bien un voisinage de $\alpha$ pour la topologie induite sur A par celle de $\Gamma$.

La réciproque reprend certains des arguments précédents dans l'ordre inverse. Soit $V = U \cap A$ un voisinage de $\alpha$ dans lequel $U$ est un voisinage de $\alpha$ pour la topologie de Krull de $\Gamma$. Il existe une extension galoisienne finie $F/K$, $F \subseteq N$, telle que $U \supseteq \alpha\, Gal(N/F)$. Ainsi

$$V \supseteq \alpha\, Gal(N/F) \cap A = \alpha\, Gal(N/F) \cap \alpha A = \alpha\,(Gal(N/F) \cap A).$$

Or

$$Gal(N/F) \cap A = Gal(N/F) \cap Gal(N/E) = Gal(N/EF),$$

d'où $V \supseteq \alpha\, Gal(N/EF)$. Comme l'extension $EF/E$ est galoisienne finie par translation de $F/K$ par $E/K$, on a bien prouvé que $V$ est un voisinage de $\alpha$ pour la topologie de Krull de $A$. □

## 4 Propriétés générales

La propriété suivante de décomposition en produit direct du groupe de Galois de la diagonale d'un parallélogramme intervient fréquemment dans les démonstrations qui suivent.

**Proposition 4.1** (dite de "scindement de la diagonale")
*Pour tout parallélogramme galoisien $[J, K, N, L]$, le groupe de Galois de la diagonale $N/J$ se décompose en produit direct sous la forme*

$$Gal(N/J) = Gal(N/K) \times Gal(N/L).$$

PREUVE: Posons pour abréger

$$\Delta := Gal(N/J), \quad \Gamma := Gal(N/K), \quad \Lambda := Gal(N/L).$$

On a $\Gamma \cap \Lambda = 1$ car tout élément de l'intersection doit laisser fixe le compositum $KL = N$. De plus, les extensions $K/J$ et $L/J$ étant galoisiennes, les sous-groupes $\Gamma$ et $\Lambda$ sont normaux dans $\Delta$. On en déduit que leurs éléments commutent; d'où l'existence du produit direct $\Gamma \times \Lambda$. Reste à prouver que $\Delta = \Gamma\Lambda$. Soit $\delta \in \Delta$. Dans le parallélogramme $[J, K, N, L]$, la restriction à $K$

$$\begin{aligned} \rho_K \ : \ \Lambda &\xrightarrow{\sim} Gal(K/J) \\ \lambda &\longmapsto \lambda_{|K} \end{aligned}$$

est un isomorphisme de groupes. Considérons l'antécédent $\lambda := \rho_K^{-1}(\delta_{|K})$, et posons $\gamma := \delta\lambda^{-1}$. Comme $\lambda_{|K} = \delta_{|K}$, on a pour tout élément $k \in K$

$$\gamma(k) = \delta((\lambda^{-1})_{|K}(k)) = \delta_{|K}((\lambda_{|K})^{-1}(k)) = \lambda_{|K} \circ (\lambda_{|K})^{-1}(k) = k,$$

ce qui prouve que $\gamma \in \Gamma$. Donc $\delta = \gamma\lambda \in \Gamma\Lambda$, ce que l'on voulait. □

Nous généralisons maintenant la partie I du théorème 1.3 de [8]. Il est surprenant de constater qu'aucune propriété topologique (de fermeture) n'est exigée sur les groupes considérés.

**Théorème 4.1** *Soit $[J, K, N, L]$ un parallélogramme galoisien de degré quelconque.*
*(1) Pour tout sous-groupe $A$ de $Gal(L/J)$ :*
*(1-1) On a le sous-parallélogramme $[L^A, KL^A, N, L]$ où $L^A$ désigne le corps des invariants dans $L$ de $A$.*
*(1-2) Si de plus $A$ est normal dans $Gal(L/J)$, on a le parallélogramme quotient $[J, K, KL^A, L^A]$.*
*(2) Pour tout sous-groupe $A$ de $Gal(N/K)$ :*
*(2-1) On a le sous-parallélogramme $[L^{(A_{|L})}, N^A, N, L]$ où $L^{(A_{|L})}$ désigne le corps des invariants dans $L$ de l'image de $A$ par la restriction à $L$.*
*(2-2) Si de plus $A$ est normal dans $Gal(N/K)$, on a le parallélogramme quotient $[J, K, N^A, L^{(A_{|L})}]$.*
*(3) Pour tous sous-groupes $A_0$ et $A_1$ de $Gal(L/J)$ (resp. $Gal(N/K)$), avoir $A_1$ normal dans $A_0$ : $A_1 \trianglelefteq A_0$, implique que l'on ait le parallélogramme*

$$[L^{A_0}, KL^{A_0}, KL^{A_1}, L^{A_1}] \qquad \Big(resp.\ [L^{(A_{0|L})}, N^{A_0}, N^{A_1}, L^{(A_{1|L})}]\Big).$$

PREUVE: (1) Posons pour simplifier $F := L^A$.

(1-1) La donnée du parallélogramme $[J, K, N, L]$ induit l'isomorphisme de restriction à $K$

$$\begin{aligned} \rho_K \ : \ Gal(N/L) &\xrightarrow{\sim} Gal(K/J)\ . \\ \lambda &\longmapsto \lambda_{|K} \end{aligned}$$

Clairement, $K \cap L = J$ implique $K \cap F = J$. En translatant l'extension galoisienne $K/J$ par $F/J$, on obtient l'extension galoisienne $KF/F$ et l'isomorphisme de restriction à K

$$r_K \ : \ Gal(KF/F) \xrightarrow{\sim} Gal(K/J)$$

[7, p.266,Th.1.12]. Translatons ensuite l'extension galoisienne $KF/F$ par $L/F$ : comme $KFL = N$, on obtient l'isomorphisme de restriction à KF

$$\rho_{KF} \ : \ Gal(N/L) \xrightarrow{\sim} Gal(KF/KF \cap L).$$

Il est clair que $\rho_K = r_K \circ \rho_{KF}$. Soit alors $\gamma \in Gal(KF/F)$. Il existe $\lambda \in Gal(N/L)$ tel que $r_K(\gamma) = \rho_K(\lambda)$, d'où

$$r_K(\gamma) = r_K(\rho_{KF}(\lambda)) \quad \Leftrightarrow \quad \gamma = \rho_{KF}(\lambda)$$

par injectivité de $r_K$. On en déduit que $\gamma$ appartient à $Gal(KF/KF \cap L)$ et l'égalité $Gal(KF/F) = Gal(KF/KF \cap L)$. Ainsi :

$$F = (KF)^{Gal(KF/F)} = (KF)^{Gal(KF/KF \cap L)} = KF \cap L\,;$$

d'où le parallélogramme $[F, KF, N, L] = [L^A, KL^A, N, L]$.

(1-2) D'après la proposition 3.1(1), la normalité de $A$ dans $Gal(L/J)$ implique celle de son adhérence pour la topologie de Krull de $Gal(L/J)$

$$\overline{A} = Gal(L/L^A) \trianglelefteq Gal(L/J).$$

On en déduit que l'extension $F = L^A/J$ est galoisienne. En la translatant par $K/J$, on obtient l'extension galoisienne $KF/K$. Comme celle-ci est galoisienne par le (1-1), ceci suffit à prouver l'existence du parallélogramme $[J, K, KF, F]$.

(2) (2-1) Par la proposition 4.1, $Gal(N/J) = Gal(N/K) \times Gal(N/L)$. En particulier :

$$\forall \delta \in Gal(N/L^{(A_{|L})}) \quad \exists! \kappa \in Gal(N/K) \quad \exists! \lambda \in Gal(N/L) \qquad \delta = \kappa\lambda,$$

et par restriction à $L$ dans $Gal(N/J)$ : $\delta_{|L} = \kappa_{|L}$. Restreinte au sous-groupe $Gal(N/L^{(A_{|L})})$, cette restriction à L est à valeurs dans $Gal(L/L^{(A_{|L})})$, de sorte que $\kappa_{|L} \in Gal(L/L^{(A_{|L})})$. De plus, en vertu du parallélogramme $[J, K, N, L]$, on a l'homéomorphisme de groupes profinis munis de leurs topologies de Krull :

$$\begin{aligned} \rho_L \ : \ Gal(N/K) &\xrightarrow{\sim} Gal(L/J)\,. \\ \gamma &\longmapsto \gamma_{|L} \end{aligned}$$

Or, par un homéomorphisme, l'adhérence de l'image d'une partie est égale à l'image de l'adhérence de cette partie. D'où

$$\overline{\rho_L(A)} = \rho_L(\overline{A})\,.$$

Ainsi, par l'égalité (3.1) de la section 3,

$$Gal(L/L^{(A_{|L})}) = Gal(L/L^{\rho_L(A)}) = \rho_L(\overline{A}) = \rho_L(Gal(N/N^A)).$$

Donc $\kappa_{|_L} = \rho_L(\kappa) \in \rho_L(Gal(N/N^A))$, et par injectivité, $\kappa$ appartient nécessairement à $Gal(N/N^A)$. Ceci prouve que $Gal(N/L^{(A_{|L})})$ est inclus dans le produit direct $Gal(N/N^A) \times Gal(N/L)$. Comme par ailleurs $Gal(N/N^A)$ et $Gal(N/L)$ sont inclus dans $Gal(N/L^{(A_{|L})})$, on a l'égalité

$$Gal(N/L^{(A_{|L})}) = Gal(N/N^A) \times Gal(N/L).$$

On en déduit que

$$\begin{aligned} N^A \cap L &= N^{Gal(N/N^A)} \cap N^{Gal(N/L)} \\ &= N^{<Gal(N/N^A), Gal(N/L)>} \\ &= N^{Gal(N/L^{(A_{|L})})} = L^{(A_{|L})}. \end{aligned}$$

De plus, $N = KL \subseteq N^A L \subseteq N$ d'où $N = N^A L$, et l'on a bien le parallélogramme $[L^{(A_{|L})}, N^A, N, L]$.

(2-2) Posons pour simplifier $F := L^{(A_{|L})}$ et $E := N^A$. En vertu du (2-1) précèdent, on a le parallélogramme $[F, E, N, L]$ et l'extension $E/F$ est galoisienne. Dans les notations de la démonstration de ce même (2-1), on a

$$Gal(L/F) = \rho_L(Gal(N/E)) .$$

Or par la proposition 3.1(1), la normalité de $A$ dans $Gal(N/K)$ implique celle de $\overline{A} = Gal(N/E)$ qui se transmet par l'isomorphisme $\rho_L$ à $Gal(L/F)$, de sorte que $F/J$ est une extension galoisienne. Clairement d'autre part, $K \cap F = J$ (car $K \cap L = J$) et $KF \subseteq E$. Il reste à prouver que cette dernière inclusion est une égalité. Appliquons pour cela la proposition 4.1 dans les parallélogrammes $[F, E, N, L]$ et $[F, KF, N, L]$ (cf. (1-1)). On a :

$$Gal(N/F) = Gal(N/E) \times Gal(N/L) = Gal(N/KF) \times Gal(N/L).$$

Pour tout $\kappa \in Gal(N/KF)$, il existe donc $\alpha \in Gal(N/E)$ et $\lambda \in Gal(N/L)$ tels que $\kappa\, id_N = \alpha\lambda$. Or, de $KF \subseteq E$ suit $Gal(N/E) \subseteq Gal(N/KF)$ d'où $\alpha \in Gal(N/KF)$. Par unicité des décompositions dans un produit direct, on en déduit que $\kappa = \alpha \in Gal(N/E)$, ce qui prouve que $Gal(N/KF) = Gal(N/E)$. Mais alors :

$$E = N^{Gal(N/E)} = N^{Gal(N/KF)} = KF$$

ce que l'on voulait.

(3) Par le (1-1) (resp. le (2-1)), la donnée d'un sous-groupe $A_0$ de $Gal(L/J)$ (resp. $Gal(N/K)$ ) induit le parallélogramme

$$[L^{A_0}, KL^{A_0}, N, L] \quad (\text{resp. } [L^{A_0|_L}, N^{A_0}, N, L] ).$$

De plus, d'après la proposition 3.1(1), avoir $A_1 \trianglelefteq A_0$ implique que $\overline{A_1} \trianglelefteq \overline{A_0}$. Si $\overline{A_0} = Gal(L/L^{A_0})$, le (1-2) fournit donc le parallélogramme

$$[L^{A_0}, KL^{A_0}, KL^{A_0}L^{\overline{A_1}}, L^{\overline{A_1}}] = [L^{A_0}, KL^{A_0}, KL^{A_1}, L^{A_1}]$$

en vertu du (2) de la proposition 3.1. Enfin, si $\overline{A_0} = Gal(N/N^{A_0})$, en utilisant que par l'homéomorphisme de restriction à L

$$(\overline{A_1})_{|L} = \overline{(A_{1|L})}\,,$$

on obtient par le (2-2) le parallélogramme

$$[L^{(A_{0|L})}, N^{A_0}, N^{\overline{A_1}}, L^{\overline{(A_{1|L})}}] = [L^{(A_{0|L})}, N^{A_0}, N^{A_1}, L^{(A_{1|L})}]\,.$$

□

**Corollaire 4.1** *Soit $[J, K, N, L]$ un parallélogramme galoisien de degré quelconque.*
*(1) Pour tout corps intermédiaire $J \subseteq F \subseteq L$, on a le sous-parallélogramme $[F, KF, N, L]$.*
*(2) Pour tout corps intermédiaire $K \subseteq E \subseteq N$, le fait d'avoir l'extension quotient $E/K$ galoisienne implique l'existence du parallélogramme quotient $[J, K, E, E \cap L]$.*

## 5 Théorie de Galois générale algébrique en dimension 2

On développe dans cette section une théorie de Galois générale en dimension 2 dont les résultats sont indépendants de toute topologie. Elle contient la théorie de Galois générale des extensions de corps, celles-ci n'étant que des parallélogrammes plats (Sect.2).

Le théorème suivant associe à tout sous-groupe du groupe de Galois d'un parallélogramme (Déf. Sect.2) un sous-parallélogramme et un quadrilatère quotient.

**Théorème 5.1** *Soit $[J, K, N, L]$ un parallélogramme galoisien de degré quelconque.*

*(1) Pour tout sous-groupe $A$ (resp. $B$) de $Gal(N/K)$ (resp. $Gal(N/L)$), on a le sous-parallélogramme galoisien*

$$[N^{A\times B}, N^A, N, N^B]\,,$$

*et le quadrilatère corporel*

$$(J, K^{(B_{|K})}, N^{A\times B}, L^{(A_{|L})})\,,$$

*où $A_{|L}$ (resp. $B_{|K}$) est l'image de $A$ (resp. $B$) par la restriction à L (resp. K).*

*(2) Si de plus $A$ (resp. $B$) est normal dans $Gal(N/K)$ (resp. $Gal(N/L)$), on a le parallélogramme galoisien quotient $[J, K^{(B_{|K})}, N^{A\times B}, L^{(A_{|L})}]$.*

PREUVE: (1) *Existence de $[N^{A\times B}, N^A, N, N^B]$.* Clairement, le sous-groupe de $Gal(N/J)$ engendré par $A$ et $B$ est égal au produit direct de $A$ par $B$, d'où

$$N^A \cap N^B = N^{<A,B>} = N^{A\times B}\,.$$

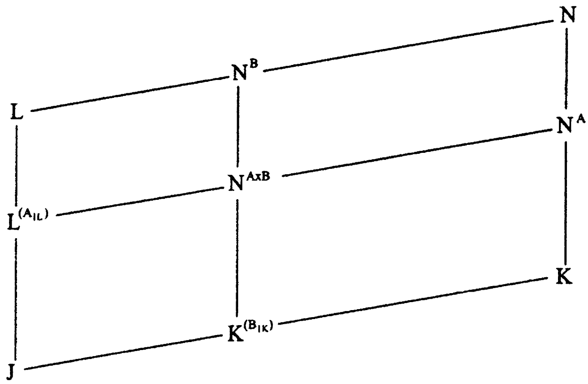


FIG. 4 -

Ensuite, on déduit de $K \subseteq N^A \subseteq N$ et $L \subseteq N^B \subseteq N$ que

$$KL = N \subseteq N^A N^B \subseteq N\,,$$

d'où $N^A N^B = N$. Ceci prouve l'existence du sous-quadrilatère $(N^{A\times B}, N^A, N, N^B)$. De plus, on a le sous parallélogramme $[L^{(A|_L)}, N^A, N, L]$ d'après le (2-1) du théorème 4.1. En particulier, l'extension $N^A/L^{(A|_L)}$ est galoisienne. Comme

$$L^{(A|_L)} = N^A \cap L \subseteq N^A \cap N^B = N^{A\times B}\,,$$

la sous-extension $N^A/N^{A\times B}$ est galoisienne. Par le même raisonnement dans le parallélogramme transposé $[J, L, N, K]$, on déduit cette fois du sous-parallélogramme $[K^{(B|_K)}, N^B, N, K]$ que l'extension $N^B/N^{A\times B}$ est galoisienne.

*Existence de* $(J, K^{(B|_K)}, N^{A\times B}, L^{(A|_L)})$. A l'évidence, $K \cap L = J$ implique $K^{(B|_K)} \cap L^{(A|_L)} = J$. Reste à prouver que $K^{(B|_K)} L^{(A|_L)} = N^{A\times B}$. En appliquant le scindement de la diagonale (Prop.4.1) dans les parallélogrammes galoisiens $[K^{(B|_K)}, N^B, N, K]$ et $[L^{(A|_L)}, N^A, N, L]$, on a respectivement

$$Gal(N/K^{(B|_K)}) = Gal(N/K) \times Gal(N/N^B)\,,$$

$$Gal(N/L^{(A|_L)}) = Gal(N/N^A) \times Gal(N/L)\,.$$

Ainsi, l'intersection

$$Gal(N/K^{(B|_K)}) \cap Gal(N/L^{(A|_L)}) = Gal(N/K^{(B|_K)}\, L^{(A|_L)})$$

est égale à

$$Gal(N/N^A) \times Gal(N/N^B) = Gal(N/N^{A\times B})$$

en vertu du sous-parallélogramme $[N^{A\times B}, N^A, N, N^B]$. On en déduit

$$K^{(B|_K)}\, L^{(A|_L)} = N^{Gal(N/K^{(B|_K)} L^{(A|_L)})} = N^{Gal(N/N^{A\times B})} = N^{A\times B}$$

ce que l'on voulait.

(2) D'après le (2-2) du théorème 4.1, le fait que $A$ (resp. $B$) soit normal dans $Gal(N/K)$ (resp. $Gal(N/L)$) induit le parallélogramme

$$[J, K, N^A, L^{(A_{|L})}] \qquad \left(\text{ resp. } [J, L, N^B, K^{(B_{|K})}]\ \right).$$

En particulier, les extensions $L^{(A_{|L})}/J$ et $K^{(B_{|K})}/K$ sont galoisiennes. Ceci suffit à prouver que le quadrilatère $(J, K^{(B_{|K})}, N^{A\times B}, L^{(A_{|L})})$ du (1) est bien un parallélogramme. □

La proposition suivante est générale et algébrique dans la mesure où elle s'énonce sans argument topologique. Elle conduira, par restriction aux sous-groupes fermés pour la topologie de Krull, au théorème final 6.2.

**Proposition 5.1** *Soit $[J, K, N, L]$ un parallélogramme galoisien de degré quelconque.*

*(1) Sous-parallélogrammes galoisiens*

*(1-1) L'application*

$$\Phi_s\ :\ [M, E, N, F] \longmapsto Gal[M, E, N, F]$$

*est une injection de l'ensemble des sous-parallélogrammes de $[J, K, N, L]$ dans l'ensemble des sous-bigroupes du groupe de Galois de $[J, K, N, L]$ (cf. Déf. Sect. 2).*

*(1-2) L'application*

$$\Psi_s\ :\ (A, B) \longmapsto [N^{A\times B}, N^A, N, N^B]$$

*est une surjection de l'ensemble des sous-bigroupes de $Gal[J, K, N, L]$ sur l'ensemble des sous-parallélogrammes de $[J, K, N, L]$.*

*(1-3) Le composé $\Psi_s \circ \Phi_s$ est l'identité.*

*(2) Parallélogrammes galoisiens quotients*

*(2-0) Pour tout parallélogramme quotient $[J, E, C, F]$ de $[J, K, N, L]$, il existe un unique sous-bigroupe normal $(A, B)$ de $Gal[J, K, N, L]$ tel que l'on ait par restriction $A_{|L} = Gal(L/F)$ et $B_{|K} = Gal(K/E)$. Précisément :*

$$A = Gal(N/KF) \quad , \qquad B = Gal(N/EL)\,.$$

*(2-1) Dans les notations du (2-0), l'application*

$$\Phi_q\ :\ [J, E, C, F] \longmapsto (A, B)$$

*est une injection de l'ensemble des parallélogrammes quotients de $[J, K, N, L]$ dans l'ensemble des sous-bigroupes normaux de $Gal[J, K, N, L]$.*

*(2-2) L'application*

$$\Psi_q\ :\ (A, B) \longmapsto [J, K^{(B_{|K})}, N^{A\times B}, L^{(A_{|L})}]$$

*est une surjection de l'ensemble des sous-bigroupes normaux de* $Gal[J,K,N,L]$ *sur l'ensemble des parallélogrammes quotients de* $[J,K,N,L]$.

*(2-3) Le composé* $\Psi_q \circ \Phi_q$ *est l'identité.*

*(2-4) Dans les notations du (2-0), on a l'isomorphisme*

$$Gal[J,E,C,F] \xrightarrow{\sim} Gal[J,K,N,L]\,/\,(A,B)\,.$$

PREUVE: (1) (1-1) Par la définition Sect.2,

$$Gal[M,E,N,F] = Gal[M',E',N,F'] \quad \Leftrightarrow \quad \begin{cases} Gal(N/E) & = Gal(N/E') \\ Gal(N/F) & = Gal(N/F') \end{cases} .$$

En prenant les invariants dans $N$ de ces groupes, on en déduit que $E = E'$ et $F = F'$ ; d'où $M = E \cap F = E' \cap F' = M'$, et l'injectivité de $\Phi_s$ est prouvée.

(1-2) L'application $\Psi_s$ existe en vertu du (1) du théorème 5.1. Sa surjectivité résulte immédiatement du (1-3) ci-dessous.

(1-3) Soit $[M,E,N,F]$ un sous-parallélogramme de $[J,K,N,L]$. D'après la proposition 4.1, $Gal(N/E) \times Gal(N/F) = Gal(N/M)$, de sorte que

$$\begin{aligned} \Psi_s \circ \Phi_s([M,E,N,F]) &= \Psi_s(Gal(N/E)\,,\, Gal(N/F)) \\ &= [N^{Gal(N/M)}, N^{Gal(N/E)}, N, N^{Gal(N/F)}] \\ &= [M,E,N,F]\,. \end{aligned}$$

(2) (2-0) D'après le (1) du corollaire 4.1, on a le parallélogramme $[F,KF,N,L]$ dans lequel $Gal(N/KF)_{|L} = Gal(L/F)$ . De plus, dans le parallélogramme $[J,E,C,F]$, l'extension $F/J$ est galoisienne et, d'après le (1-2) du théorème 4.1, on a le parallélogramme quotient $[J,K,KF,F]$. En particulier l'extension $KF/K$ est galoisienne et $Gal(N/KF)$ est un sous-groupe normal de $Gal(N/K)$, ce qui permet de poser $A := Gal(N/KF)$. Même raisonnement dans le parallélogramme transposé $[J,L,N,K]$ en prenant $B := Gal(N/EL)$. De plus, dans $[J,K,N,L]$, les restrictions à $L$ et $K$ sont des isomorphismes; donc les sous-groupes A et B sont nécessairement uniques.

(2-1),(2-2),(2-3) L'existence de l'application $\Phi_q$ résulte de l'unicité du sous-bigroupe normal $(A,B)$ du (2-0). L'application $\Psi_q$ résulte quant à elle du (2) du théorème 5.1. Pour $A = Gal(N/KF)$ et $B = Gal(N/EL)$, on a par (2-0) :

$$\begin{aligned} \Psi_q \circ \Phi_q([J,E,C,F]) &= \Psi_q(A,B) \\ &= [J, K^{Gal(K/E)}, N^{A\times B}, L^{Gal(L/F)}] \\ &= [J,E,N^{A\times B},F]\,. \end{aligned}$$

De ce dernier parallélogramme, on déduit en particulier que $EF = N^{A\times B}$, et dans $[J,E,C,F]$, on a $EF = C$. Finalement le composé $\Psi_q \circ \Phi_q$ est l'identité, ce qui implique que $\Phi_q$ est injective et $\Psi_q$ surjective.

(2-4) Par définition

$$Gal[J,E,C,F] = (Gal(C/E), Gal(C/F)) \xrightarrow{\sim} (Gal(F/J), Gal(E/J)).$$

De l'existence des parallélogrammes $[J,K,KF,F]$ et $[J,L,EL,E]$ (cf. Th 4.1 (1-2)), on déduit alors que

$$\begin{aligned} Gal[J,E,C,F] &\xrightarrow{\sim} (Gal(KF/K), Gal(EL/L)) \\ &\xrightarrow{\sim} (Gal(N/K)/Gal(N/KF)\,,\, Gal(N/L)/Gal(N/EL)) \\ &\xrightarrow{\sim} Gal[J,K,N,L]/(A,B) \end{aligned}$$

par (2-0). □

Le théorème suivant fournit des égalités générales entre corps assez surprenantes au vu des hypothèses minimalistes. Elles laissent entrevoir des propriétés inattendues des extensions galoisiennes qui seront étudiées dans un autre article avec la notion de tour galoisienne de composition [1]. De plus, ces égalités induisent comme une dualité entre le compositum et l'intersection de deux corps $K$ et $L$. Nous la traduisons pour ce qui nous concerne en termes de quadrilatères dans la proposition 5.2 à suivre : il y a correspondance biunivoque entre les sous-quadrilatères et les quadrilatères quotients de tout parallélogramme $[K \cap L, K, KL, L]$.

**Théorème 5.2** ( dit "de l'écartelé" †)
*Soient $K$ et $L$ deux corps contenus dans un même corps et $J := K \cap L$. On suppose seulement les extensions $K/J$ et $L/J$ galoisiennes, leurs degrés étant quelconques. Alors :*
*(1) Pour tous corps intermédiaires $E$ et $F$ : $J \subseteq E \subseteq K$ , $J \subseteq F \subseteq L$ , on a l'égalité*

$$KF \cap EL = EF\,.$$

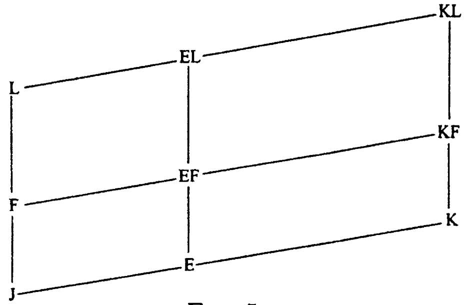


FIG. 5 –

† du nom du blason qu'évoquent, en héraldique, les figures correspondant au théorème.

*(2) Pour tous corps intermédiaires $E$ et $F$ : $K \subseteq E \subseteq KL$ , $L \subseteq F \subseteq KL$ , on a l'égalité*

$$(K \cap F)(E \cap L) = E \cap F\,.$$

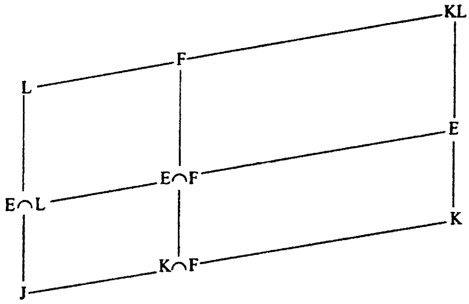


FIG. 6 –

PREUVE: Posons $N := KL$. Comme les extensions $K/J$ et $L/J$ sont galoisiennes, on dispose du parallélogramme galoisien $[J, K, N, L]$.
(1) D'après le (1) du corollaire 4.1, on a le sous-parallélogramme $[F, KF, N, L]$. Dans celui-ci, le scindement de la diagonale (Prop. 4.1) fournit l'égalité

$$Gal(N/F) = Gal(N/KF) \times Gal(N/L)\,.$$

De même, dans le parallélogramme transposé $[J, L, N, K]$, on a le sous-parallélogramme $[E, EL, N, K]$ et l'égalité

$$Gal(N/E) = Gal(N/K) \times Gal(N/EL)\,.$$

On en déduit que

$$Gal(N/EF) = Gal(N/F) \cap Gal(N/E) = Gal(N/KF) \times Gal(N/EL)$$

et ainsi

$$EF = N^{Gal(N/EF)} = N^{Gal(N/KF) \times Gal(N/EL)}\,.$$

Il en résulte, par le (1-2) de la proposition 5.1, que

$$\Psi_s(Gal(N/KF), Gal(N/EL)) = [EF, KF, N, EL]\,,$$

et en particulier $KF \cap EL = EF$.
(2) Posons $A := Gal(N/E)$, $B := Gal(N/F)$. D'après le (2-1) du théorème 4.1, on a les parallélogrammes $[L^{(A_{|L})}, E, N, L]$ , $[K^{(B_{|K})}, F, N, K]$, et donc

$$E \cap L = L^{(A_{|L})}\,,\ K \cap F = K^{(B_{|K})}\,.$$

D'autre part, d'après le (1) du théorème 5.1, on a le quadrilatère

$$(J, K^{(B_{|K})}, N^{A \times B}, L^{(A_{|L})})$$

où $N^{A \times B} = N^A \cap N^B$. Ainsi :

$$E \cap F = N^A \cap N^B = N^{A \times B} = K^{(B_{|K})} L^{(A_{|L})} = (K \cap F)(E \cap L)\,.$$

□

**Corollaire 5.1** *Soient $K$ et $L$ deux corps contenus dans un même corps. On suppose seulement que les extensions $K/(K \cap L)$ et $L/(K \cap L)$ sont galoisiennes.*
*Alors :*
*(1) Pour tous corps intermédiaires $E$ et $F$ : $K \cap L \subseteq E \subseteq K$ , $K \cap L \subseteq F \subseteq L$, on a le parallélogramme galoisien*

$$[EF, KF, KL, EL]$$

*et le quadrilatère corporel*

$$(K \cap L, E, EF, F)\,.$$

*(2) Pour tous corps intermédiaires $E$ et $F$ : $K \subseteq E \subseteq KL$ , $L \subseteq F \subseteq KL$, on a le parallélogramme galoisien*

$$[E \cap F, E, KL, F]$$

*et le quadrilatère corporel*

$$(K \cap L, K \cap F, E \cap F, E \cap L)\,.$$

PREUVE: (1) Le parallélogramme $[EF, KF, KL, EL]$ apparaît déjà dans la démonstration du (1) du théorème 5.2. Et il est clair que $E \cap F = K \cap L$.
(2) Soit $N := KL$. D'après le (1) du théorème 5.1 appliqué avec $A = Gal(N/E)$ et $B = Gal(N/F)$, on a le sous-parallélogramme

$$[N^{A\times B}, E, N, F] = [E \cap F, E, N, F]$$

en vertu du (2) de la démonstration du théorème 5.2 qui donne aussi le quadrilatère

$$(K \cap L, K \cap F, E \cap F, E \cap L)\,.$$

□

**Proposition 5.2** *Soit $[J, K, N, L]$ un parallélogramme galoisien de degré quelconque. Notons*

$$\mathcal{S}quad\,[J,K,N,L] \text{ ou } \mathcal{S}quad \left( \text{resp. } \mathcal{R}quad\,[J,K,N,L] \text{ ou } \mathcal{R}quad \right)$$

*l'ensemble des sous-quadrilatères (resp. des quadrilatères quotients) de $[J, K, N, L]$. Pour les relations d'ordre du (2) du lemme 2.1 :*
*(1) L'application*

$$\begin{aligned} \mathcal{R} \, : \, \mathcal{S}quad &\longrightarrow \mathcal{R}quad \\ (M, E, N, F) &\longmapsto (J, K \cap F, M, E \cap L) \end{aligned}$$

*est une bijection décroissante.*

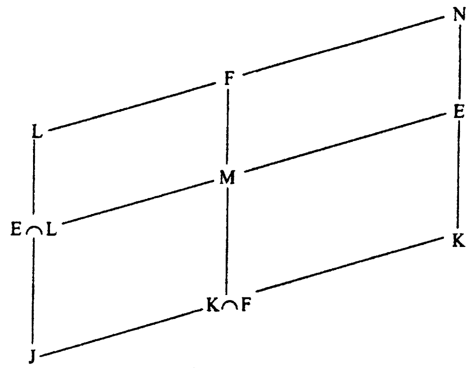


FIG. 7 -

*(2) L'application*

$$\begin{aligned} \mathcal{S} \,:\, \mathcal{R}quad &\longrightarrow \mathcal{S}quad \\ (J,E,C,F) &\longmapsto (C,KF,N,EL) \end{aligned}$$

*est une bijection décroissante.*

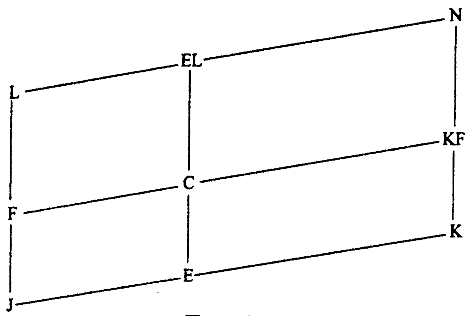


FIG. 8 -

*(3) Les applications $\mathcal{R}$ et $\mathcal{S}$ sont réciproques l'une de l'autre.*
*(4) On a l'égalité des cardinaux (éventuellement infinis)*

$$|\ \mathcal{R}quad\ | = |\ \mathcal{S}quad\ |\ .$$

PREUVE: Dans le parallélogramme $[J,K,N,L]$, les extensions $K/J$ et $L/J$ sont galoisiennes.
(1) L'application $\mathcal{R}$ existe bien car d'après le (2) du théorème de l'écartelé (5.2)

$$(K \cap F)(E \cap L) = E \cap F = M\ ,$$

d'où le quadrilatère quotient $(J, K \cap F, M, E \cap L)$. La décroissance de $\mathcal{R}$ résulte directement de la définition des relations d'ordre du lemme 2.1.(2) car

$$(M',E',N,F') \leq (M,E,N,F) \ \Leftrightarrow\ (E \subseteq E'\ ,\ F \subseteq F')$$

implique que

$$\begin{gathered}(E \cap L \subseteq E' \cap L\,,\ K \cap F \subseteq K \cap F')\\ \Updownarrow\\ (J, K \cap F, M, E \cap L) \leq (J, K \cap F', M', E' \cap L)\,.\end{gathered}$$

La bijectivité de $\mathcal{R}$ est une conséquence du (3) ci-dessous.
(2) L'application $\mathcal{S}$ existe bien car d'après le (1) du théorème de l'écartelé

$$KF \cap EL = EF\,,$$

d'où le sous-quadrilatère $(C, KF, N, EL)$. La décroissance de $\mathcal{S}$ résulte directement du lemme 2.1.(2) car

$$(J, E, C, F) \leq (J, E', C', F') \Leftrightarrow (E \subseteq E'\,,\ F \subseteq F')$$

implique que

$$\begin{gathered}(KF \subseteq KF'\,,\ EL \subseteq E'L)\\ \Updownarrow\\ (C', KF', N, E'L) \leq (C, KF, N, EL)\,.\end{gathered}$$

La bijectivité de $\mathcal{S}$ est une conséquence du (3) suivant.
(3) Pour tout sous-quadrilatère $(M, E, N, F) \in \mathcal{S}quad$, on a

$$\mathcal{S} \circ \mathcal{R}(M, E, N, F) \;=\; \mathcal{S}(J, K \cap F, M, E \cap L) \;=\; (M, K(E \cap L), N, (K \cap F)L)\,.$$

Or d'après le (2) du théorème de l'écartelé appliqué à $E$ et $N$ (resp. $N$ et $F$) on obtient

$$K(E \cap L) = E \qquad \big(\text{ resp. } (K \cap F)L = F\big)\,,$$

ce qui prouve que $\mathcal{S} \circ \mathcal{R} = id_{\mathcal{S}quad}$.
Pour tout quadrilatère quotient $(J, E, C, F) \in \mathcal{R}quad$, on a

$$\mathcal{R} \circ \mathcal{S}(J, E, C, F) \;=\; \mathcal{R}(C, KF, N, EL) \;=\; (J, K \cap EL, C, KF \cap L)\,.$$

Or d'après le (1) du théorème de l'écartelé appliqué à $J$ et $E$ (resp. $F$ et $J$ ), on obtient

$$K \cap EL = E \qquad \big(\text{ resp. } KF \cap L = F\big)\,,$$

ce qui prouve que $\mathcal{R} \circ \mathcal{S} = id_{\mathcal{R}quad}$. $\square$

# 6 Généralisation topologique de la théorie de Galois finie en dimension 2

Dans cette section, nous enrichissons la proposition algébrique 5.1 en munissant les groupes de Galois de leur topologie de Krull. Considérées dans la catégorie produit $\mathbf{ProGr^2}$ de la catégorie des groupes profinis $\mathbf{ProGr}$ par elle-même, les applications $\Phi$ et $\Psi$ de la proposition 5.1 deviennent des bijections. Le théorème 6.2 final généralise ainsi, d'une part le théorème principal de la théorie de Galois finie en dimension 2 [8, Th.4-2] généralisant lui-même la bijection de Galois classique, d'autre part le théorème de Krull [6] qui se retrouve en particularisant à des parallélogrammes galoisiens infinis plats.

Par définition dans [10, p.101], tout sous-groupe d'un sous-groupe topologique est fermé. On sait que tout sous-groupe fermé $H$ d'un groupe profini $G$ est profini, et si $H$ est normal, le quotient $G/H$ est aussi profini. Ceci nous conduit à poser la définition suivante.

*Définition:* (1) Nous appelons "sous-groupe profini" (resp. "sous-groupe profini normal") d'un groupe profini $G$ tout sous-groupe (resp. sous-groupe normal) $H$ de $G$ fermé pour la topologie de $G$. Nous écrirons

$$H \leq_c G \qquad \big(\text{ resp. } H \trianglelefteq_c G\big)\,.$$

(2) Nous appelons "sous-bigroupe profini" (resp. "sous-bigroupe profini normal") d'un bigroupe profini $(G_1, G_2)$ tout bigroupe $(H_1, H_2)$ tel que l'on ait

$$H_i \leq_c G_i \qquad \big(\text{ resp. } H_i \trianglelefteq_c G_i\big) \quad (\text{i=1,2})\,.$$

Nous écrirons

$$(H_1, H_2) \leq_c (G_1, G_2) \qquad \big(\text{ resp. } (H_1, H_2) \trianglelefteq_c (G_1, G_2)\big)\,.$$

(3) Nous appelons "bigroupe profini quotient" d'un bigroupe profini $(G_1, G_2)$ par son sous-bigroupe profini normal $(H_1, H_2)$ le bigroupe $(G_1/H_1, G_2/H_2)$. Nous écrirons

$$(G_1, G_2)/(H_1, H_2) := (G_1/H_1, G_2/H_2)\,.$$

(4) Nous appelons "isomorphisme de bigroupes profinis"

$$(f_1, f_2) \,:\, (G_1, G_2) \xrightarrow{\sim} (G'_1, G'_2)$$

un morphisme de $\mathbf{ProGr^2}$ tel que chacun des

$$f_i \,:\, G_i \xrightarrow{\sim} G'_i \quad (i = 1, 2)$$

soit un isomorphisme de groupes profinis.

Pour éviter toute ambiguïté dans la démonstration du lemme 6.2 ci-dessous, sortons du contexte le fait général suivant.

**Lemme 6.1** *Soient $X$ un espace topologique et $A$ une partie fermée de $X$. Pour toute partie $B$ de $A$, avoir $B$ fermée dans $A$ muni de la topologie induite par celle de $X$ équivaut à avoir $B$ fermée dans $X$.*

**Lemme 6.2** *Soit $E/F$ une extension galoisienne. Pour tous corps intermédiaires $M$ et $M'$ entre $F$ et $E$, on a les équivalences*

$$M \subseteq M' \Leftrightarrow Gal(E/M') \leq Gal(E/M) \Leftrightarrow Gal(E/M') \leq_c Gal(E/M)$$

*où les groupes $Gal(E/M)$ et $Gal(E/M')$ sont munis de leurs topologies de Krull.*

PREUVE: La première équivalence étant claire, il suffit de prouver la seconde et plus précisément le sens direct de celle-ci. Appliquons le lemme 6.1 précédent avec

$$X := Gal(E/F)\,,\ A := Gal(E/M)\,,\ B := Gal(E/M')\,.$$

Par hypothèse $B \subseteq A$, et d'après le théorème de Krull classique, on a

$$A \leq_c X\,,\ B \leq_c X\,.$$

Donc $B$ est fermé dans $A$ muni de la topologie induite par celle de $X$. Or, en vertu de la proposition 3.2, cette topologie induite sur $A$ coïncide avec la topologie de Krull de $A$. On a donc bien montré que $Gal(E/M')$ est fermé dans $Gal(E/M)$ muni de sa topologie de Krull. □

Les groupes profinis qui interviennent dans la suite sont des groupes de Galois. Nous convenons une fois pour toutes qu'étant donnée une extension galoisienne, son groupe de Galois est muni de sa topologie de Krull.

**Proposition 6.1** *Lorsque $E/F$ est une extension galoisienne, la relation d'ordre du lemme 2.1.(1) dans l'ensemble des sous-extensions de $E/F$ (resp. des extensions galoisiennes quotients de $E/F$) s'écrit*

$$\begin{aligned} (E/M') \leq (E/M) \quad &\Leftrightarrow \quad Gal(E/M') \leq_c Gal(E/M) \\ \Big(\text{resp. } (M/F) \leq (M'/F) \quad &\Leftrightarrow \quad Gal(E/M') \leq_c Gal(E/M)\Big). \end{aligned}$$

PREUVE: Immédiate par le lemme 6.2. □

Pour le généraliser en dimension 2, reformulons maintenant le théorème de Krull classique [4, AV.64,Th.4].

**Théorème 6.1** (Théorème de Krull revisité)

*Soit $N/K$ une extension galoisienne de degré quelconque. On munit l'ensemble des sous-extensions (resp. des extensions galoisiennes quotients) de $N/K$ de la relation d'ordre de la proposition 6.1 ci-dessus. Alors :*
*(1) L'application*

$$(N/E) \longmapsto Gal(N/E)$$

*est une bijection croissante de l'ensemble des sous-extensions de $N/K$ sur l'ensemble des sous-groupes profinis de $Gal(N/K)$. Sa réciproque est l'application, elle-même croissante,*

$$H \longmapsto (N/N^H).$$

*(2) L'application*

$$(E/K) \longmapsto Gal(N/E)$$

*est une bijection décroissante de l'ensemble des extensions galoisiennes quotients de $N/K$ sur l'ensemble des sous-groupes profinis normaux de $Gal(N/K)$. Sa réciproque est l'application, elle-même décroissante,*

$$H \longmapsto (N^H/K).$$

*De plus, la restriction à $E$ induit un isomorphisme de groupes profinis*

$$Gal(E/K) \xrightarrow{\sim} Gal(N/K)/Gal(N/E).$$

PREUVE: Tout résulte directement du théorème de Krull classique, à l'exception de la monotonie des réciproques (lorsque les ordres sont partiels, la réciproque d'une bijection monotone n'est pas nécessairement monotone).
(1) Soient $H_1$ et $H_2$ deux sous-groupes profinis de $Gal(N/K)$ tels que $H_1 \leq_c H_2$. Par définition, on a

$$H_1 = \overline{H_1} = Gal(N/N^{H_1}) \leq_c H_2 = \overline{H_2} = Gal(N/N^{H_2}),$$

ce qui équivaut à $(N/N^{H_1}) \leq (N/N^{H_2})$ par la proposition 6.1.
(2) Dans les notations du (1), supposons de plus $H_1$ et $H_2$ normaux dans $Gal(N/K)$. On a toujours $Gal(N/N^{H_1}) \leq_c Gal(N/N^{H_2})$, ce qui équivaut par la proposition 6.1 à avoir $(N^{H_2}/K) \leq (N^{H_1}/K)$. □

**Proposition 6.2** *Soit $[J,K,N,L]$ un parallélogramme galoisien. La relation d' ordre du lemme 2.1 dans l'ensemble des sous-parallélogrammes galoisiens (resp. des parallélogrammes galoisiens quotients) de $[J,K,N,L]$ s'écrit*

$$[M',E',N,F'] \leq [M,E,N,F] \quad \Leftrightarrow \quad Gal[M',E',N,F'] \leq_c Gal[M,E,N,F]$$

$\Big($ *resp.*

$$[J,E,C,F] \leq [J,E',C',F'] \Leftrightarrow Gal[C',KF',N,E'L] \leq_c Gal[C,KF,N,EL] \Big).$$

PREUVE: (1) *Sous-parallélogrammes.* Par définition

$$[M',E',N,F'] \leq [M,E,N,F] \quad \Leftrightarrow \quad (E \subseteq E' \ , \ F \subseteq F')$$

et en vertu du lemme 6.2

$$\Leftrightarrow \begin{cases} Gal(N/E') & \leq_c Gal(N/E) \\ Gal(N/F') & \leq_c Gal(N/F) \end{cases} \Leftrightarrow Gal[M',E',N,F'] \leq_c Gal[M,E,N,F].$$

(2) *Parallélogrammes quotients.* D'après la proposition 5.2, on a l'équivalence

$$[J,E,C,F] \leq [J,E',C',F'] \;\Leftrightarrow\; [C',KF',N,E'L] \leq [C,KF,N,EL] ;$$

d'où la conclusion par le (1) précédent. □

Le théorème 6.2 qui suit généralise en degré quelconque le théorème principal de la théorie de Galois finie en dimension 2 (Th.4.2. de [8]). En se limitant à des sous-groupes fermés, il rend bijectives les injections $\Phi$ et les surjections $\Psi$ de la proposition algébrique 5.1. De plus, en se limitant à des parallélogrammes plats, il redonne exactement la double bijection du théorème de Krull revisité. Ainsi, le théorème 6.2 suivant généralise en dimension 2 le théorème de Krull, tout comme le théorème 4.2 de [8] généralisait le théorème de Galois classique pour des extensions finies.

**Théorème 6.2** *Soit $[J,K,N,L]$ un parallélogramme galoisien de degré quelconque, de groupe de Galois $Gal[J,K,N,L]$ (Déf. Sect.2). On munit l'ensemble des sous-parallélogrammes galoisiens (resp. des parallélogrammes galoisiens quotients) de $[J,K,N,L]$ de la relation d'ordre de la proposition 6.2. Alors :*
*(1) Sous-parallélogrammes galoisiens*
*L'application*

$$[M,E,N,F] \longmapsto Gal[M,E,N,F]$$

*est une bijection croissante de l'ensemble des sous-parallélogrammes de $[J,K,N,L]$ sur l'ensemble des sous-bigroupes profinis de $Gal[J,K,N,L]$, dont la réciproque est l'application, elle-même croissante,*

$$(A,B) \longmapsto [N^{A\times B}, N^A, N, N^B] .$$

*(2) Parallélogrammes galoisiens quotients*

*(2-0) Pour tout parallélogramme quotient $[J,E,C,F]$ de $[J,K,N,L]$, il existe un unique sous-bigroupe profini normal $(A,B)$ de $Gal[J,K,N,L]$ tel que l'on ait $A_{|L} = Gal(L/F)$ et $B_{|K} = Gal(K/E)$. Précisément :*

$$A = Gal(N/KF) \quad , \qquad B = Gal(N/EL) .$$

*(2-1) Dans les notations du (2-0), l'application*

$$[J,E,C,F] \longmapsto (A,B)$$

*est une bijection décroissante de l'ensemble des parallélogrammes quotients de $[J,K,N,L]$ dans l'ensemble des sous-bigroupes profinis normaux de $Gal[J,K,N,L]$ dont la réciproque est l'application, elle-même décroissante,*

$$(A,B) \longmapsto [J, K^{(B_{|K})}, N^{A\times B}, L^{(A_{|L})}] .$$

*(2-2) Dans les notations du (2-0), on a l'isomorphisme de bigroupes profinis*

$$Gal[J,E,C,F] \xrightarrow{\sim} Gal[J,K,N,L] \,/\, (A,B) .$$

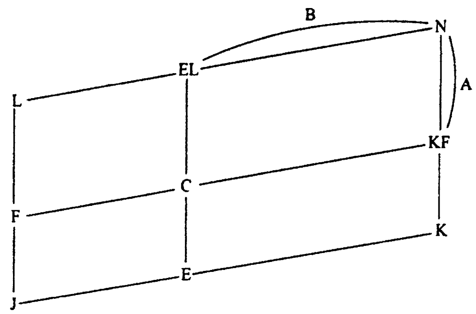


FIG. 9 -

PREUVE: On reprend les notations $\Phi$ et $\Psi$ des applications de la proposition 5.1 en ajoutant des tildes pour marquer que l'on se limite aux sous-bigroupes profinis de $Gal[J, K, N, L]$.

(1) L'application $\widetilde{\Phi}_s \ : \ [M, E, N, F] \longmapsto Gal[M, E, N, F]$ du (1) existe bien car par définition $Gal[M, E, N, F] = (Gal(N/E), Gal(N/F))$ où $Gal(N/E)$ (resp. $Gal(N/F)$) est fermé dans $Gal(N/K)$ (resp. $Gal(N/L)$) en vertu du théorème de Krull, de sorte que

$$(Gal(N/E), Gal(N/F)) \leq_c Gal[J, K, N, L]$$

Soit $\widetilde{\Psi}_s \ : \ (A, B) \longmapsto [N^{A\times B}, N^A, N, N^B]$ la restriction à l'ensemble des sous-bigroupes profinis de $Gal[J, K, N, L]$ de l'application $\Psi_s$ du (1-2) de la proposition 5.1. D'après le (1-3) de cette même proposition, le composé $\widetilde{\Psi}_s \circ \widetilde{\Phi}_s$ est l'identité. De plus, pour tout sous-bigroupe profini $(A, B)$ de $Gal[J, K, N, L]$, on a

$$\widetilde{\Phi}_s \circ \widetilde{\Psi}_s(A, B) = \widetilde{\Phi}_s([N^{A\times B}, N^A, N, N^B]) = (Gal(N/N^A), Gal(N/N^B)) = (\overline{A}, \overline{B}).$$

Mais par définition

$$(A, B) \leq_c Gal[J, K, N, L] \quad \Leftrightarrow \quad \begin{cases} A \leq_c Gal(N/K) \\ B \leq_c Gal(N/L) \end{cases}$$

de sorte que $\widetilde{\Phi}_s \circ \widetilde{\Psi}_s(A, B) = (A, B)$. Les applications $\widetilde{\Phi}_s$, $\widetilde{\Psi}_s$ sont donc réciproques l'une de l'autre, et en particulier bijectives. Montrons qu'elles sont croissantes. C'est clair directement pour $\widetilde{\Phi}_s$ d'après la proposition 6.2. Pour $\widetilde{\Psi}_s$, considérons deux sous-bigroupes profinis de $Gal[J, K, N, L]$ tels que $(A', B') \leq (A, B)$, d'où

$$(A', B') \leq_c (A, B)$$

par le lemme 6.1 ; et posons

$$[M, E, N, F] := \widetilde{\Psi}_s(A, B)\,, \quad [M', E', N, F'] := \widetilde{\Psi}_s(A', B')\,.$$

Par ce qui précède

$$Gal[M, E, N, F] = \widetilde{\Phi}_s([M, E, N, F]) = \widetilde{\Phi}_s \circ \widetilde{\Psi}_s(A, B) = (A, B)\,.$$

Donc
$$Gal[M',E',N,F'] = (A',B') \leq_c (A,B) = Gal[M,E,N,F]\,,$$
ce qui équivaut, par la proposition 6.2, à $[M',E',N,F'] \leq [M,E,N,F]$.
(2) (2-0) Ce n'est que le (2-0) de la proposition 5.1 en rajoutant le fait que $A = Gal(N/KF)$ et $B = Gal(N/EL)$ sont des sous-groupes fermés en vertu du théorème de Krull.

(2-1) L'application $\widetilde{\Phi}_q \ :\ [J,E,C,F] \longmapsto (A,B)$ du (2-1) existe bien car d'après le (2-0) précèdent, on a
$$(A,B) \trianglelefteq_c Gal[J,K,N,L]\,.$$
Soit $\widetilde{\Psi}_q \ :\ (A,B) \longmapsto [J, K^{(B_{|K})}, N^{A\times B}, L^{(A_{|L})}]$ la restriction à l'ensemble des sous-bigroupes profinis normaux de $Gal[J,K,N,L]$ de l'application $\Psi_q$ du (2-2) de la proposition 5.1. D'après le (2-3) de cette même proposition, le composé $\widetilde{\Psi}_q \circ \widetilde{\Phi}_q$ est l'identité. De plus, pour tout sous-groupe profini normal $(A,B)$ de $Gal[J,K,N,L]$, on a
$$\widetilde{\Phi}_q \circ \widetilde{\Psi}_q(A,B) \ = \ \widetilde{\Phi}_q([J, K^{(B_{|K})}, N^{A\times B}, L^{(A_{|L})}] \ = \ (A',B')$$
où par définition $A'$ (resp. $B'$) est l'unique sous-groupe de $Gal(N/K)$ (resp. $Gal(N/L)$) tel que $A'_{|L} \ = \ Gal(L/L^{(A_{|L})}) \ \left(\text{resp. } B'_{|K} \ = \ Gal(K/K^{(B_{|K})}\right)$. Or dans le parallélogramme galoisien $[J,K,N,L]$, la restriction à $L$ est un isomorphisme de groupes profinis de $Gal(N/K)$ sur $Gal(L/J)$. Ainsi : $\overline{(A_{|L})} = (\overline{A})_{|L}$. Comme $A$ est fermé, on en déduit que $Gal(L/L^{(A_{|L})}) = A_{|L}$. De la même façon $Gal(K/K^{(B_{|K})}) = B_{|K}$. Il en résulte par unicité que $\widetilde{\Phi}_q \circ \widetilde{\Psi}_q(A,B) = (A,B)$. Les applications $\widetilde{\Phi}_q$, $\widetilde{\Psi}_q$ sont donc réciproques l'une de l'autre, et en particulier bijectives. Montrons qu'elles sont décroissantes. Pour $\widetilde{\Phi}_q$, on a d'après la proposition 6.2
$$[J,E,C,F] \leq [J,E',C',F'] \quad \Leftrightarrow \quad Gal[C',KF',N,E'L] \leq_c Gal[C,KF,N,EL]$$
$$\Leftrightarrow \left\{ \begin{array}{l} Gal(N/KF') \leq_c Gal(N/KF) \\ Gal(N/E'L) \leq_c Gal(N/EL) \end{array} \right. \Leftrightarrow \ \widetilde{\Phi}_q([J,E',C',F']) \ \leq_c \ \widetilde{\Phi}_q([J,E,C,F])\,.$$
Pour $\widetilde{\Psi}_q$, considérons deux sous-bigroupes profinis normaux de $Gal[J,K,N,L]$ tels que
$$(A',B') \leq_c (A,B)\,.$$
(cf. le (1) pour $\widetilde{\Psi}_s$). Comme le composé $\widetilde{\Phi}_q \circ \widetilde{\Psi}_q$ est l'identité, on a d'après l'équivalence obtenue précédemment pour la décroissance de $\widetilde{\Phi}_q$,
$$\begin{aligned} (A',B') \leq_c (A,B) \quad &\Leftrightarrow \quad \widetilde{\Phi}_q(\widetilde{\Psi}_q(A',B')) \leq_c \widetilde{\Phi}_q(\widetilde{\Psi}_q(A,B)) \\ &\Leftrightarrow \quad \widetilde{\Psi}_q(A,B) \ \leq_c \ \widetilde{\Psi}_q(A',B') \end{aligned}$$
ce qui exprime la décroissance de $\widetilde{\Psi}_q$.

(2-2) Tous les isomorphismes de la démonstration du (2-4) de la proposition 5.1 sont topologiques. □

## Références

[1] E. Andréo et R. Massy. Raffinements de tours galoisiennes. En préparation.

[2] J.R. Bastida. *Field Extensions and Galois Theory.* Addison-Wesley, Reading, MA, 1984.

[3] N. Bourbaki. *Topologie Générale, Chap. 1 à 4.* Hermann, Paris, 1971.

[4] N. Bourbaki. *Algèbre, Chap. 4 à 7.* Masson, Paris, 1981.

[5] G. Karpilovsky. *Topics in Field Theory.* North-Holland Mathematics Studies 155, Amsterdam, 1989.

[6] W. Krull. Galoissche Theorie der unendlichen algebraischen Erweiterungen. *Math. Ann.*, 100 : 687–698, 1928.

[7] S. Lang. *Algebra, $3^{rd}$ ed.* Addison-Wesley, Reading, MA, 1995.

[8] R. Massy et S. Monier-Derviaux. Parallélogrammes galoisiens. *J. of Algebra*, 217 : 229–248, 1999.

[9] R. Massy et S. Monier-Derviaux. Descente et parallélogramme galoisiens. *J. Théorie des Nombres Bordeaux*, 11 : 161–172, 1999.

[10] L.S. Pontryagin. *Topological Groups.* Gordon and Breach, New York, 1966.

EMMANUEL ANDRÉO
UNIVERSITÉ DE VALENCIENNES
DÉPARTEMENT DE MATHÉMATIQUES
LE MONT HOUY
F-59313 VALENCIENNES
FRANCE
Emmanuel.Andreo@univ-valenciennes.fr

RICHARD MASSY†
UNIVERSITÉ DE VALENCIENNES
DÉPARTEMENT DE MATHÉMATIQUES
LE MONT HOUY
F-59313 VALENCIENNES
FRANCE
Richard.Massy@univ-valenciennes.fr