Journal of Algebra **217,** 229–248 (1999)
Article ID jabr.1998.7769, available online at http://www.idealibrary.com on IDEAL®

Parallélogrammes Galoisiens

Richard Massy* et Sylvie Monier-Derviaux

Département de Mathématiques, Université de Valenciennes, Le Mont Houy, B.P. 311,

Received May 26, 1998

We generalize the notion of a Galois extension by that of a Galois parallelogram; a Galois extension is just a flat Galois parallelogram. The existence of Galois parallelograms is proved in the number field case. We state numerous general properties of Galois parallelograms which give, in particular, the usual properties of classical Galois theory. Then, we introduce a "two-dimensional Galois theory" by generalizing to Galois parallelograms the classical Galois bijection for finite Galois extensions. © 1999 Academic Press

Key Words: parallélogramme galoisien.

0. INTRODUCTION

Un problème naturel de théorie de Galois des extensions de corps est le "Problème de la descente galoisienne": Soient K/J une extension algébrique et N/K une extension galoisienne. Existe-t-il un corps intermédiaire L entre J et N, $J \subseteq L \subseteq N$, tel que l'extension L/J soit galoisienne avec $K \cap L = J$ et $KL = N$?

Dans ce cas, nous disons que l'extension N/K est "descendable sur J" et que L/J est "une descendue de N/K (parallèlement à K/J)." La restriction à L induit un isomorphisme du groupe de Galois de N/K sur celui de L/J. Lorsqu'elle est galoisienne, l'extension K/J est descendue de l'extension galoisienne N/L.

Clairement, toute extension galoisienne est descendable sur son corps de base, de descendue elle-même. Un autre exemple d'extension descendable est le suivant. Soit N/J une extension galoisienne finie de groupe $\mathrm{Gal}(N/J)$

* E-mail: Richard.Massy@univ-valenciennes.fr.

0021-8693/99 $30.00

s'écrivant comme produit direct de deux de ses sous-groupes Γ et V. Notons K et L les corps des invariants dans N de Γ et V respectivement:

$$\mathrm{Gal}(N/J) = \Gamma \times V, \qquad K := N^{\Gamma}, \qquad L := N^{V}.$$

Alors, l'extension N/K est descendable sur J, de descendue L/J. Pour des degrés finis, cet exemple décrit toutes les extensions galoisiennes de K descendables sur J lorsque K/J est galoisienne. En effet, dans ce cas, une extension galoisienne N/K est descendable sur J si et seulement si l'extension N/J est galoisienne de groupe $\mathrm{Gal}(N/J)$ admettant un complément facteur direct à son sous-groupe $\mathrm{Gal}(N/K)$.

Un cas particulier du problème de la descente galoisienne a été étudié par G. Brattström [1]. Le problème est traité en général dans [5–7], notamment pour la descente non kummérienne des extensions construites dans [4, 9]. Voir aussi les résultats récents de A. Ledet [3].

La vie propre de la descente galoisienne donne naturellement naissance à une notion de "parallélogramme galoisien" que l'on peut voir comme une première figure d'une "théorie de Galois en dimension 2" à développer. Convenons en effet de figurer géométriquement par des segments parallèles de longueurs égales les extensions galoisiennes dont les groupes de Galois sont isomorphes. La donnée d'un triplet $(K/J, N/K, L/J)$ d'extensions galoisiennes dans lequel N/K est descendable sur J de descendue L/J prend alors la configuration d'un parallélogramme que nous qualifions de "galoisien":

$$\begin{tikzcd} & N \arrow[d, dash] \\ L \arrow[ur, dash] \arrow[d, dash] & K \\ J \arrow[ur, dash] & \end{tikzcd}$$

Le but de cet article est de montrer que, dans ses propriétés usuelles, la notion d'extension galoisienne peut être remplacée par celle, plus générale, de parallélogramme galoisien. Nous mettons en évidence de nombreuses propriétés mécaniques des parallélogrammes galoisiens (théorème 1.3) que l'on peut voir comme une généralisation "en dimension 2" de propriétés connues de théorie de Galois classique, car la donnée d'une extension galoisienne n'est que celle d'un parallélogramme "plat". Ceci nous sert ensuite à montrer que dans un parallélogramme galoisien les propriétés des extensions parallèles sont très liées, parfois semblables; on peut dire qu'elles se réfléchissent, modulo le respect des convenances pour les degrés. Par exemple, pour des corps de nombres, on a une parfaite similitude de la décomposition des idéaux premiers dans une extension galoisienne et sa descendue parallèlement à une extension galoisienne de degré étranger (théorème 2.1). Nous en déduisons, d'une part qu'un groupe de décomposition, ou d'inertie, se conserve par descente galoisienne, ce qui nous permet d'exhiber canoniquement des parallélogrammes de nature arithmétique; d'autre part que, comme une extension galoisienne, un parallélogramme galoisien se localise (corollaire 2.3).

Dans les sections 3 et 4, nous présentons un début de "théorie de Galois en dimension 2". Nous définissons le groupe de Galois d'un parallélogramme galoisien en nous plaçant dans la catégorie produit $\mathbf{Gr}^2$ de la catégorie des groupes par elle-même. Ceci nous permet d'établir le résultat principal de cet article: un analogue pour les parallélogrammes galoisiens de la bijection de Galois pour les extensions galoisiennes (de degré fini). Nous réénonçons d'abord cette bijection, traditionnellement présentée décroissante, en une double bijection: croissante pour les sous-extensions, décroissante pour les extensions galoisiennes quotient (théorème de Galois revisité). Puis nous prouvons qu'elle se généralise en une double bijection, croissante de même pour les sous-parallélogrammes et décroissante pour les parallélogrammes galoisiens quotient (théorème 4.2). Dans le cas particulier d'un parallélogramme plat, donc pour une extension galoisienne habituelle, cette double bijection sur les parallélogrammes redonne exactement la bijection classique de Galois (remarque 4.3).

1. DÉFINITION ET PROPRIÉTÉS GÉNÉRALES

La définition suivante généralise la notion d'extension galoisienne.

DÉFINITION 1.1. (1) Nous appelons "parallélogramme galoisien" (ou simplement "parallélogramme" par abus de langage) la donnée d'un triplet $(K/J, N/K, L/J)$ d'extensions galoisiennes dans lequel l'extension N/K est descendable sur J de descendue L/J: $K \cap L = J$, $KL = N$ (cf. sect. 0). On notera ce parallélogramme (J, K, N, L) en abrégé géométrique.

(2) Nous appelons "parallélogramme transposé de (J, K, N, L)" le parallélogramme galoisien (J, L, N, K):

$$^t(J, K, N, L) := (J, L, N, K).$$

(3) Nous définissons le degré de (J, K, N, L) comme étant le couple des degrés de N/K et K/J:

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

Ce degré sera dit "fini" quand $[N : K]$ et $[K : J]$ sont finis. Dans ce cas, nous disons que (J, K, N, L) est "de degré séparé" si et seulement si

$$pgcd\big([N : K], [K : J]\big) = 1.$$

(4) Nous disons que le parallélogramme (J, K, N, L) est “plat” lorsque $N = K$ ou $J = K$. Nous identifierons le parallélogramme plat (J, K, K, J) (resp. (K, K, N, N)) à l’extension galoisienne K/J (resp. N/K):

$$(J, K, K, J) \simeq (K/J) \qquad \text{(resp. } (K, K, N, N) \simeq (N/K)\text{)}.$$

Remarque 1.2. Tout corps K s’identifie au parallélogramme plat (K, K, K, K).

Le théorème suivant regroupe les principales propriétés générales des parallélogrammes galoisiens. Pour abréger, on emploie partout le terme “parallélogramme” au lieu de parallélogramme galoisien. Dans la première partie, nous simplifions en supposant les parallélogrammes de degrés finis bien que certaines propriétés soient vraies pour un degré quelconque.

THÉORÈME 1.3. *I. Soit (J, K, N, L) un parallélogramme de degré fini.*

(1) *Pour tout corps intermédiaire E entre J et L, $J \subseteq E \subseteq L$:*

(1.1) *On a le parallélogramme (E, KE, N, L).*

(1.2) *Si E/J est une extension galoisienne, on a le parallélogramme (J, K, KE, E).*

(2) *Pour tout corps intermédiaire E entre K et N, $K \subseteq E \subseteq N$:*

(2.1) *On a le parallélogramme $(L^{(A_{|L})}, E, N, L)$ où $L^{(A_{|L})}$ désigne le corps des invariants dans L de l’image par la restriction à L du groupe $A := \mathrm{Gal}(N/E)$.*

(2.2) *Si E/K est une extension galoisienne, on a le parallélogramme $(J, K, E, L^{(A_{|L})})$.*

(3) *Pour toute extension galoisienne intermédiaire E_1/E_0 de L/J (resp. N/K), $J \subseteq E_0 \subseteq E_1 \subseteq L$ (resp. $K \subseteq E_0 \subseteq E_1 \subseteq N$), on a le parallélogramme (E_0, KE_0, KE_1, E_1) (resp. $(L^{(A_{0|L})}, E_0, E_1, L^{(A_{1|L})})$) où $A_i := \mathrm{Gal}(N/E_i)$ $(i = 0, 1)$:*

$$\begin{tikzcd}[arrows=dash]
 & N \arrow[d] \\
L \arrow[ur] \arrow[d] & KE_1 \arrow[d] \\
E_1 \arrow[ur] \arrow[d] & KE_0 \arrow[d] \\
E_0 \arrow[ur] \arrow[d] & K \\
J \arrow[ur] &
\end{tikzcd}
\qquad \text{(resp.} \qquad
\begin{tikzcd}[arrows=dash]
 & N \arrow[d] \\
L \arrow[ur] \arrow[d] & E_1 \arrow[d] \\
L^{(A_{1|L})} \arrow[ur] \arrow[d] & E_0 \arrow[d] \\
L^{(A_{0|L})} \arrow[ur] \arrow[d] & K \\
J \arrow[ur] &
\end{tikzcd}
\quad)$$

(4) *Pour tout parallélogramme* (J, K, E, F) *où* $K \subseteq E \subseteq N$ *et* $J \subseteq F \subseteq L$, *on a le parallélogramme* (F, E, N, L).

II. (1) *Soit* (J, K, N, L) *un parallélogramme de degré quelconque*.

(1.1) *"Parallélogramme translaté"*:

— *Pour toute extension algébrique* E/J, *telle que* N *et* E *soient contenus dans un même corps* C, *on a le parallélogramme*

$$(KE \cap LE, KE, NE, LE).$$

— *Si de plus* (J, K, N, L) *est de degré fini et séparé*, *on a le parallélogramme*

$$(E, KE, NE, LE).$$

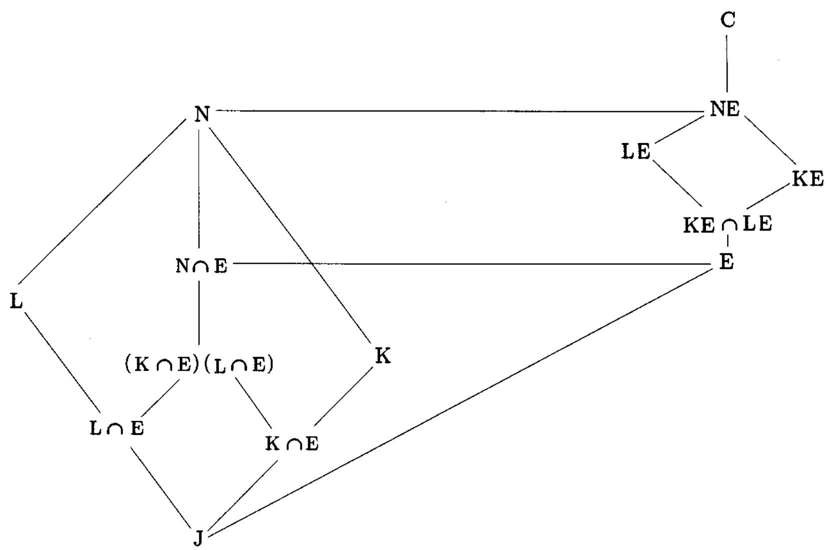
(1.2) *"Quotient d'un parallélogramme par une extension galoisienne"*:

— *Pour toute extension galoisienne* E/J, *on a le parallélogramme*

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

— *Si de plus* (J, K, N, L) *est de degré fini et séparé*, *on a le parallélogramme*

$$(J, K \cap E, N \cap E, L \cap E).$$



(2) *Soient* (J, K_i, N_i, L_i) $(i = 1, 2)$ *deux parallélogrammes de degrés quelconques.*

(2.1) *“Parallélogramme compositum”*:

— *Si les corps* N_1 *et* N_2 *sont contenus dans un même corps* C, *on a le parallélogramme*

$$(K_1K_2 \cap L_1L_2, K_1K_2, N_1N_2, L_1L_2).$$

— *De plus, les degrés* $[K_1K_2 : J]$, $[L_1L_2 : J]$ *sont finis et premiers entre eux si et seulement si les degrés* $[K_i : J]$, $[L_j : J]$ $(1 \leq i, j \leq 2)$ *sont finis et premiers deux à deux. Dans ce cas, on a le parallélogramme*

$$(J, K_1K_2, N_1N_2, L_1L_2).$$

(2.2) *“Parallélogramme intersection”*:

— *On a le parallélogramme*

$$\big(J, K_1 \cap K_2, (K_1 \cap K_2)(L_1 \cap L_2), L_1 \cap L_2\big).$$

— *De plus, quand les degrés* $\deg(J, K_i, N_i, L_i)$ $(i = 1, 2)$ *sont finis et séparés, on a l'égalité*

$$\big[N_1 \cap N_2 : (K_1 \cap K_2)(L_1 \cap L_2)\big] = \big[K_1 \cap L_2 : J\big]\,\big[K_2 \cap L_1 : J\big].$$

En conséquence, si $K_1 \cap L_2 = J$ *et* $K_2 \cap L_1 = J$, *par exemple si les degrés* $[K_i : J]$, $[L_j : J]$ $(1 \leq i, j \leq 2)$ *sont premiers deux à deux, on a le parallélogramme*

$$\big(J, K_1 \cap K_2, N_1 \cap N_2, L_1 \cap L_2\big).$$

Remarques 1.4. (0) Tous les parallélogrammes de l'énoncé précédent sont transposables au sens de la définition 1.1(2).

(1) On peut voir le (1.1) et le (2.1) de la partie I du théorème 1.3 comme une généralisation “en dimension 2” de la propriété usuelle que toute sous-extension d'une extension galoisienne est galoisienne. En effet, dans le cas d'un parallélogramme plat (K, K, N, N), qui s'identifie à l'extension galoisienne N/K, on obtient que l'extension N/E est galoisienne. De la même façon, dans la partie II, le (1.1) généralise le théorème de l'extension galoisienne translatée [2, p. 266, th. 1.12], tandis que le (2.1) (resp. le (2.2) ou le (1.2)) généralise(nt) le fait que le compositum (resp. l'intersection) de deux extensions galoisiennes d'un même corps est une extension galoisienne de ce corps.

(2) Même dans le cas d'une extension galoisienne E/J, un parallélogramme translaté n'est pas en général un parallélogramme compositum. En effet, le compositum de $(J, K_1, N_1, L_1)=(J, K, N, L)$ par $(J, K_2, N_2, L_2)=(J, E, E, J) \simeq (E/J)$ n'est que le parallélogramme $(KE \cap L, KE, NE, L)$. Pareillement, le quotient d'un parallélogramme par une extension galoisienne n'est pas en général un parallélogramme intersection. C'est un "parallélogramme quotient" au sens de la définition 3.3(2).

La démonstration du théorème 1.3 est reportée à la dernière section.

2. PROPRIÉTÉS ARITHMÉTIQUES

Dans cette section, nous considérons des parallélogrammes galoisiens de corps de nombres. Pour un tel corps F, O_F désignera l'anneau des entiers de F et Spec O_F l'ensemble des idéaux premiers de O_F.

Le théorème suivant montre que dans un parallélogramme galoisien de degré séparé, il y a une parfaite similitude de la décomposition d'un idéal premier dans les extensions parallèles. Nous déduisons alors des propriétés du théorème 1.3 que la notion de parallélogramme galoisien existe arithmétiquement: en effet, elle respecte le dévissage canonique d'une extension galoisienne par les corps des invariants du groupe de décomposition et du groupe d'inertie d'un diviseur d'un idéal premier du corps de base [8, chap. I, sect. 7]. Nous achevons cette section en montrant que, comme une extension galoisienne, un parallélogramme galoisien se localise, ce qui ouvre tout un champ d'investigations futures.

THÉORÈME 2.1. *Soit* (J, K, N, L) *un parallélogramme galoisien de corps de nombres, de degré fini et séparé* (*cf. déf.*1.1(3)). *Soient* $\mathscr{L} \in \operatorname{Spec} O_J$ *un idéal premier de* O_J *et* $\mathfrak{N} \in \operatorname{Spec} O_K$ *un diviseur premier de* $\mathscr{L}$ *dans* O_K: $\mathfrak{N} \cap O_J = \mathscr{L}$.

(1) *Il y a égalité des indices de ramification, des degrés résiduels et du nombre de facteurs, de la décomposition de* $\mathscr{L}$ *dans* L *et de celle de* $\mathfrak{N}$ *dans* N:

$$e_L(\mathscr{L}) = e_N(\mathfrak{N}), \qquad f_L(\mathscr{L}) = f_N(\mathfrak{N}), \qquad g_L(\mathscr{L}) = g_N(\mathfrak{N}).$$

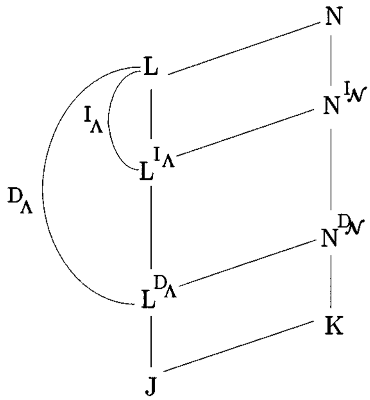
(2) *Soient* $\mathscr{N} \in \operatorname{Spec} O_N$ *l'un quelconque des diviseurs premiers de* $\mathfrak{N}$ *dans* O_N: $\mathscr{N} \cap O_K = \mathfrak{N}$, *et* $\Lambda := \mathscr{N} \cap O_L$ *sa trace sur* L. *Les groupes de décomposition* $D_{\mathscr{N}}$ *et* D_Λ (*resp. d'inertie* $I_{\mathscr{N}}$ *et* I_Λ) *de* $\mathscr{N}$ *dans* $\operatorname{Gal}(N/K)$ *et* Λ *dans* $\operatorname{Gal}(L/J)$ *sont isomorphes via la restriction à* L.

(3) *On a les parallélogrammes galoisiens*

$$(L^{D_\Lambda}, N^{D_{\mathscr{N}}}, N, L), \qquad (L^{I_\Lambda}, N^{I_{\mathscr{N}}}, N, L), \qquad (L^{D_\Lambda}, N^{D_{\mathscr{N}}}, N^{I_{\mathscr{N}}}, L^{I_\Lambda}).$$

Si de plus, le sous-groupe $D_{\mathcal{N}}$ (*resp.* $I_{\mathcal{N}}$) *est normal dans* $\mathrm{Gal}(N/K)$, *on a le parallélogramme galoisien*

$$(J, K, N^{D_{\mathcal{N}}}, L^{D_\Lambda}) \qquad (\textit{resp. } (J, K, N^{I_{\mathcal{N}}}, L^{I_\Lambda})):$$



Remarque 2.2. Cet énoncé généralise le théorème 3 de [5].

Démonstration du Théorème 2.1. Dans le parallélogramme (J, K, N, L), on a $\Lambda \cap O_J = \mathscr{L}$.

(1) Par multiplicativité des indices de ramification, on sait que

$$e(\mathcal{N}/\mathscr{L}) = e(\mathcal{N}/\mathfrak{N})e(\mathfrak{N}/\mathscr{L}) = e(\mathcal{N}/\Lambda)\, e(\Lambda/\mathscr{L})$$

où $e(\Lambda/\mathscr{L}) = e_L(\mathscr{L})$ et $e(\mathcal{N}/\mathfrak{N}) = e_N(\mathfrak{N})$ divisent $[N : K]$, tandis que $e(\mathfrak{N}/\mathscr{L})$ et $e(\mathcal{N}/\Lambda)$ divisent $[K : J]$. Comme le degré de (J, K, N, L) est séparé, on en déduit que $e_L(\mathscr{L}) = e_N(\mathfrak{N})$. Même démarche pour les degrés résiduels.

(2) La restriction à L induit un homomorphisme injectif de $D_{\mathcal{N}}$ dans D_Λ (resp. de $I_{\mathcal{N}}$ dans I_Λ) qui est surjectif en vertu de l'égalité

$$e_N(\mathfrak{N})\, f_N(\mathfrak{N}) = e_L(\mathscr{L})\, f_L(\mathscr{L}) \qquad (\text{resp. } e_N(\mathfrak{N}) = e_L(\mathscr{L}))$$

déduite du (1).

(3) Les parallélogrammes de l'énoncé se déduisent du (2) précédent combiné respectivement avec les propriétés fonctorielles du (2.1), du (3) et du (2.2) du théorème 1.3.I. ∎

COROLLAIRE 2.3. *Dans les notations du théorème* 2.1, *on a le parallélogramme galoisien local* $(J_{\mathscr{L}}, K_{\mathfrak{N}}, N_{\mathcal{N}}, L_\Lambda)$.

Démonstration. Par le (2) du théorème 2.1,

$$[L_\Lambda : J_{\mathscr{L}}] = |D_\Lambda| = |D_{\mathscr{N}}| = [N_{\mathscr{N}} : K_{\mathfrak{R}}]$$

qui divise $[N : K]$, et clairement $[K_{\mathfrak{R}} : J_{\mathscr{L}}] \mid [K : J]$. Comme le degré de (J, K, N, L) est séparé, on en déduit que $K_{\mathfrak{R}} \cap L_\Lambda = J_{\mathscr{L}}$. Par suite

$$[K_{\mathfrak{R}}\, L_\Lambda : J_{\mathscr{L}}] = [K_{\mathfrak{R}} : J_{\mathscr{L}}]\,[L_\Lambda : J_{\mathscr{L}}] = [K_{\mathfrak{R}} : J_{\mathscr{L}}]\,[N_{\mathscr{N}} : K_{\mathfrak{R}}] = [N_{\mathscr{N}} : J_{\mathscr{L}}],$$

en sorte que $N_{\mathscr{N}} = K_{\mathfrak{R}}\, L_\Lambda$. Il est ainsi prouvé que $L_\Lambda/J_{\mathscr{L}}$ est une descendue de $N_{\mathscr{N}}/K_{\mathfrak{R}}$, d'où le parallélogramme local $(J_{\mathscr{L}}, K_{\mathfrak{R}}, N_{\mathscr{N}}, L_\Lambda)$. ∎

3. GROUPE DE GALOIS D'UN PARALLÉLOGRAMME

Soit N/K une extension galoisienne. Appelons "sous-extension de N/K" (resp. "extension galoisienne quotient de N/K") toute extension N/E (resp. toute extension galoisienne E/K) où E est un corps intermédiaire entre K et N: $K \subseteq E \subseteq N$. Dans l'ensemble des sous-extensions de N/K, la relation induite par l'inclusion des sous-groupes de $\mathrm{Gal}(N/K)$,

$$\begin{aligned}(N/E') \le (N/E) \quad &\Leftrightarrow \quad \mathrm{Gal}(N/E') \le \mathrm{Gal}(N/E)\\ &\Leftrightarrow \quad E \subseteq E',\end{aligned} \tag{3.1}$$

est clairement une relation d'ordre. Nous ordonnons les extensions galoisiennes quotient de N/K par la même inclusion. Précisément, par définition

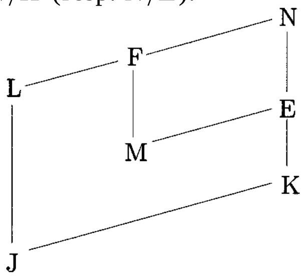
$$(E/K) \le (E'/K) \quad \Leftrightarrow \quad E \subseteq E'. \tag{3.2}$$

D'après la théorie de Galois classique, toute sous-extension (resp. toute extension galoisienne quotient) de N/K de degré fini a pour groupe de Galois un sous-groupe (resp. un groupe quotient) du groupe de Galois de N/K. Avec les définitions qui suivent, nous allons montrer qu'il en est de même "en dimension 2" pour les parallélogrammes galoisiens.

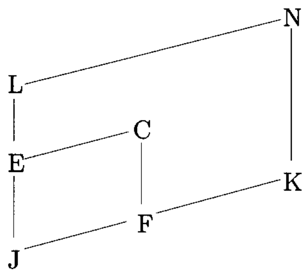
Définition 3.3. Soit (J, K, N, L) un parallélogramme galoisien.

(1) Nous appelons "sous-parallélogramme (galoisien) de (J, K, N, L)" tout parallélogramme galoisien (M, E, N, F) où N/E (resp. N/F) est

une sous-extension de N/K (resp. N/L):



(2) Nous appelons "parallélogramme (galoisien) quotient de (J, K, N, L)" tout parallélogramme galoisien (J, F, C, E) où F/J (resp. E/J) est une extension galoisienne quotient de K/J (resp. (L/J):



Remarquons que dans le cas plat, par exemple $(J, K, N, L) = (J, K, K, J)$, le sous-parallélogramme $(M, E, N, F) = (F, K, K, F)$ (resp. le parallélogramme quotient $(J, F, C, E) = (J, F, F, J)$) s'identifie à la sous-extension K/F (resp. à l'extension galoisienne quotient F/J) de K/J (cf. déf.1.1(4)).

Pour définir le groupe de Galois d'un parallélogramme, nous allons nous placer, non pas dans la catégorie des groupes **Gr** comme en théorie classique, mais dans la catégorie produit $\mathbf{Gr}^2 = \mathbf{Gr} \times \mathbf{Gr}$.

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.

Nous appelons "sous-bigroupe" (resp. "sous-bigroupe normal") d'un bigroupe (G_1, G_2), tout bigroupe (H_1, H_2) où $H_i \leq G_i$ (resp. $H_i \trianglelefteq G_i$) $(i = 1, 2)$. On écrira

$$(H_1, H_2) \leq (G_1, G_2) \qquad (\text{resp. } (H_1, H_2) \trianglelefteq (G_1, G_2)). \tag{3.4}$$

Nous appelons "bigroupe quotient du bigroupe (G_1, G_2) par son sous-bigroupe normal (H_1, H_2)", le bigroupe $(G_1/H_1, G_2/H_2)$. On écrira

$$(G_1, G_2)/(H_1, H_2) := (G_1/H_1, G_2/H_2). \tag{3.5}$$

Les "homomorphismes de bigroupes" $(f_1, f_2)\colon (G_1, G_2) \to (G_1', G_2')$ sont les morphismes de $\mathbf{Gr}^2$, et ils sont injectifs (resp. surjectifs, bijectifs) selon qu'il en est ainsi de f_1 et de f_2.

DÉFINITION 3.6. Soit (J, K, N, L) un parallélogramme galoisien.

(1) Nous appelons “groupe de Galois de (J, K, N, L)”, et nous notons $\mathrm{Gal}(J, K, N, L)$, le bigroupe

$$\mathrm{Gal}(J, K, N, L) := (\mathrm{Gal}(N/K),\ \mathrm{Gal}(N/L)).$$

(2) Nous appelons “sous-groupe” (resp. “sous-groupe normal”; resp. “groupe quotient”) du groupe de Galois de (J, K, N, L), tout sous-bigroupe (resp. sous-bigroupe normal; resp. bigroupe quotient) de $\mathrm{Gal}(J, K, N, L)$.

Il est immédiat que le groupe de Galois d'un sous-parallélogramme de (J, K, N, L) est un sous-groupe du groupe de Galois de (J, K, N, L). Nous prouverons que le groupe de Galois de tout parallélogramme quotient de (J, K, N, L) est un groupe quotient de $\mathrm{Gal}(J, K, N, L)$.

Fait 3.7. Soit (J, K, N, L) un parallélogramme galoisien de degré fini.

(1) Dans l'ensemble des sous-parallélogrammes galoisiens de (J, K, N, L) (déf. 3.3(1)), la relation induite par l'inclusion des sous-groupes de $\mathrm{Gal}(J, K, N, L)$,

$$\begin{aligned} & (M', E', N, F') \le (M, E, N, F) \\ \Leftrightarrow\quad & \mathrm{Gal}(M', E', N, F') \le \mathrm{Gal}(M, E, N, F) \\ \Leftrightarrow\quad & (E \subseteq E',\ F \subseteq F'), \end{aligned}$$

est une relation d'ordre.

(2) Dans l'ensemble des parallélogrammes galoisiens quotient de (J, K, N, L) (déf. 3.3(2)), la relation définie par

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

est une relation d'ordre.

C'est clair en invoquant, pour le (1) que $M = E \cap F \subseteq E' \cap F' = M'$, et pour le (2) que $C = EF \subseteq E'F' = C'$.

Remarque 3.8. Nous verrons que la relation d'ordre du (2) précédent est, comme celle du (1), induite par l'inclusion des sous-groupes de Gal (J, K, N, L) (confer la décroissance de la démonstration du théorème 4.2).

4. ANALOGUE DE LA BIJECTION DE GALOIS POUR LES PARALLÉLOGRAMMES GALOISIENS

Le but de cette section est d'élaborer un début de “théorie de Galois en dimension 2”, en généralisant aux parallélogrammes galoisiens la bijection classique de Galois que nous réénonçons sous la forme suivante.

Théorème 4.1 (Théorème de Galois Revisité). *Soit* N/K *une extension galoisienne finie de groupe de Galois* $\mathrm{Gal}(N/K)$. *On munit l'ensemble des sous-extensions* (*resp. des extensions galoisiennes quotient*) *de* N/K *de la relation d'ordre induite par l'inclusion des sous-groupes de* $\mathrm{Gal}(N/K)$ (*cf.* (3.1) *et* (3.2)). *Alors*:

(1) *L'application*

$$(N/E) \mapsto \mathrm{Gal}(N/E)$$

est une bijection croissante de l'ensemble des sous-extensions de N/K *sur l'ensemble des sous-groupes de* $\mathrm{Gal}(N/K)$, *dont la réciproque est l'application*

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

(2) *L'application*

$$(E/K) \mapsto \mathrm{Gal}(N/E)$$

est une bijection décroissante de l'ensemble des extensions galoisiennes quotient de N/K *sur l'ensemble des sous-groupes normaux de* $\mathrm{Gal}(N/K)$, *dont la réciproque est l'application*

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

De plus,

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

Cette double bijection sur les extensions se généralise en une double bijection sur les parallélogrammes.

THÉORÈME 4.2. *Soit* (J, K, N, L) *un parallélogramme galoisien de degré fini de groupe de Galois* $\mathrm{Gal}(J, K, N, L)$. *On munit l'ensemble des sous-parallélogrammes galoisiens* (*resp. des parallélogrammes galoisiens quotient*) *de* (J, K, N, L) *de la relation d'ordre induite par l'inclusion des sous-groupes de* $\mathrm{Gal}(J, K, N, L)$ (*cf. fait* 3.7). *Alors*:

(1) *L'application*

$$(M, E, N, F) \mapsto \operatorname{Gal}(M, E, N, F)$$

est une bijection croissante de l'ensemble des sous-parallélogrammes galoisiens de (J, K, N, L) *sur l'ensemble des sous-groupes de* $\operatorname{Gal}(J, K, N, L)$, *dont la réciproque est l'application*

$$(A, B) \mapsto (N^{A\times B}, N^A, N, N^B).$$

(2) *L'application*

$$(J, F, C, E) \mapsto \operatorname{Gal}(N^{A\times B}, N^A, N, N^B) = (A, B),$$

où A (*resp.* B) *est l'unique sous-groupe de* $\operatorname{Gal}(N/K)$ (*resp.* $\operatorname{Gal}(N/L)$) *de restriction* $A_{|L} = \operatorname{Gal}(L/E)$ (*resp.* $B_{|K} = \operatorname{Gal}(K/F)$), *est une bijection décroissante de l'ensemble des parallélogrammes galoisiens quotient de* (J, K, N, L) *sur l'ensemble des sous-groupes normaux de* $\operatorname{Gal}(J, K, N, L)$, *dont la réciproque est l'application*

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

De plus,

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

Remarque 4.3. Dans le cas d'un parallélogramme plat, cette double bijection "en dimension 2" redonne exactement la double bijection classique de Galois. Le théorème 4.1 n'est donc qu'un cas particulier du théorème 4.2. En effet, plaçons-nous dans le parallélogramme $(J, K, N, L) = (K, K, N, N)$ qui s'identifie à l'extension galoisienne N/K.

(1) *Sous-parallélogramme* (M, E, N, F). On a $L{=}F{=}N$ et $M = E \cap F = E$, de sorte que $(M, E, N, F) = (E, E, N, N)$ qui s'identifie à la sous-extension N/E de N/K, et

$$\operatorname{Gal}(M, E, N, F) = (\operatorname{Gal}(N/E), \mathbf{1}) \xrightarrow{\sim} \operatorname{Gal}(N/E).$$

On retrouve donc bien la bijection $(N/E) \mapsto \operatorname{Gal}(N/E)$. De même, la réciproque $(A, B) \mapsto (N^{A\times B}, N^A, N, N^B)$ où $B \leq \operatorname{Gal}(N/L) = \mathbf{1}$, devient

$$A \xrightarrow{\sim} (A, \mathbf{1}) \mapsto (N^A, N^A, N, N) \simeq (N/N^A).$$

(2) *Parallélogramme quotient* (J, F, C, E). On a $K = J \subseteq E \subseteq L = N$, $F = K$ et $C = EF = E$, de sorte que $(J, F, C, E) = (K, K, E, E)$ s'identifie à l'extension galoisienne quotient E/K de N/K. La bijection $(J, F, C, E) \mapsto$

(A, B), dans laquelle $A = \mathrm{Gal}(N/E)$ et $B = \mathbf{1}$, redonne donc la bijection classique $(E/K) \mapsto \mathrm{Gal}(N/E)$. De même, la réciproque $(A, B) \mapsto (J, K^{(B_{|K})}, N^{A\times B}, L^{(A_{|L})})$ devient

$$A \xrightarrow{\sim} (A, \mathbf{1}) \mapsto (K, K, N^A, N^A) \simeq (N^A/K).$$

Enfin

$$\begin{array}{ccc} \mathrm{Gal}(J, F, C, E) & \xrightarrow{\sim} & \mathrm{Gal}(J, K, N, L)/(A, B) \\ \downarrow\wr & & \downarrow\wr \\ \mathrm{Gal}(E/K) & \xrightarrow{\sim} & \mathrm{Gal}(N/K)/\mathrm{Gal}(N/E). \end{array}$$

Démonstration du théorème 4.2. (1) *Injectivité.* Avoir $\mathrm{Gal}(M', E', N, F') = \mathrm{Gal}(M, E, N, F)$ s'exprime par une égalité entre couples qui conduit à

$$E' = N^{\mathrm{Gal}(N/E')} = N^{\mathrm{Gal}(N/E)} = E,$$

et de même $F' = F$; d'où $M' = E' \cap F' = E \cap F = M$.

Surjectivité. Soit $(A,\ B) \leq \mathrm{Gal}(J,\ K,\ N,\ L)$ (cf. (3.4)). La sous-extension $N/N^{A\times B}$ de l'extension galoisienne N/J admet les extensions galoisiennes quotient $N^A/N^{A\times B}$ et $N^B/N^{A\times B}$. On a

$$N^A \cap N^B = N^{\langle A,\, B\rangle} = N^{A\times B}, \qquad N^A N^B = N^{A\cap B} = N.$$

Ceci prouve que l'extension $N^B/N^{A\times B}$ est une descendue de N/N^A, d'où le sous-parallélogramme galoisien $(N^{A\times B}, N^A, N, N^B)$. La surjectivité s'en déduit par le théorème d'Artin:

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

Croissance. Par définition de la relation d'ordre du fait 3.7(1).

Réciproque. Dans le parallélogramme galoisien (M, E, N, F), on a l'égalité $\mathrm{Gal}(N/E) \times \mathrm{Gal}(N/F) = \mathrm{Gal}(N/M)$. Ainsi

$$\begin{aligned} (M, E, N, F) &\mapsto (\mathrm{Gal}(N/E), \mathrm{Gal}(N/F)) \\ &\mapsto (N^{\mathrm{Gal}(N/M)}, N^{\mathrm{Gal}(N/E)}, N, N^{\mathrm{Gal}(N/F)}) = (M, E, N, F). \end{aligned}$$

L'identité de la composition dans l'ordre inverse est claire.

(2) *Injectivité.* Soit $(J,\ F,\ C,\ E)$ (resp. $(J,\ F',\ C',\ E')$) un parallélogramme quotient d'image (A, B) (resp. (A', B')). Avoir $(A, B) = (A', B')$ implique par restriction à L que $\mathrm{Gal}(L/E) = \mathrm{Gal}(L/E')$, d'où $E = E'$. De même $F = F'$, et donc $C = EF = E'F' = C'$.

Surjectivité. Soit $(A, B) \trianglelefteq \mathrm{Gal}(J, K, N, L)$ (cf. (3.4)). Comme l'extension N^A/K est galoisienne, on sait d'après le théorème 1.3.I(2.2) que l'on a le parallélogramme galoisien $(J, K, N^A, L^{(A_{|L})})$. En particulier, l'extension $L^{(A_{|L})}/J$ est galoisienne, de groupe

$$\mathrm{Gal}(L^{(A_{|L})}/J) \xrightarrow{\sim} \mathrm{Gal}(N/K)/A.$$

De même, l'extension N^B/L est galoisienne dans le parallélogramme transposé (J, L, N, K) (cf. déf. 1.1(2)), donc l'extension $K^{(B_{|K})}/J$ est galoisienne, de groupe

$$\mathrm{Gal}(K^{(B_{|K})}/J) \xrightarrow{\sim} \mathrm{Gal}(N/L)/B.$$

Il est clair que $L^{(A_{|L})} \subseteq N^{A\times B}$ et $K^{(B_{|K})} \subseteq N^{A\times B}$. Prouvons que l'on a le parallélogramme galoisien $(J, K^{(B_{|K})}, N^{A\times B}, L^{(A_{|L})})$. Comme dans le parallélogramme (J, K, N, L)

$$A \times B \trianglelefteq \mathrm{Gal}(N/K) \times \mathrm{Gal}(N/L) = \mathrm{Gal}(N/J),$$

l'extension $N^{A\times B}/J$ est galoisienne, et il en est de même de sa sous-extension $N^{A\times B}/K^{(B_{|K})}$. A montrer que l'extension galoisienne $L^{(A_{|L})}/J$ est une descendue de $N^{A\times B}/K^{(B_{|K})}$. On a, d'une part

$$J \subseteq K^{(B_{|K})} \cap L^{(A_{|L})} \subseteq K \cap L = J,$$

d'où $K^{(B_{|K})} \cap L^{(A_{|L})} = J$; d'autre part, en vertu de ce qui précède,

$$\left|\mathrm{Gal}(K^{(B_{|K})}L^{(A_{|L})}/J)\right| = \left|\mathrm{Gal}(N/L)/B\right| \left|\mathrm{Gal}(N/K)/A\right|.$$

Or

$$\mathrm{Gal}(N^{A\times B}/J) \xrightarrow{\sim} \mathrm{Gal}(N/J)/A \times B \xrightarrow{\sim} (\mathrm{Gal}(N/K)/A) \times (\mathrm{Gal}(N/L)/B),$$

d'où $K^{(B_{|K})}L^{(A_{|L})} = N^{A\times B}$ par finitude des extensions. En posant $F := K^{(B_{|K})}$, $C := N^{A\times B}$, $E := L^{(A_{|L})}$, on déduit alors la surjectivité voulue du théorème d'Artin.

Surjectivité inverse. Pour tout parallélogramme galoisien quotient (J, F, C, E) de (J, K, N, L), il existe un unique sous-groupe normal (A, B) de $\mathrm{Gal}(J, K, N, L)$ tel que

$$A_{|L} = \mathrm{Gal}(L/E), \qquad B_{|K} = \mathrm{Gal}(K/F),$$
$$(J, F, C, E) = \left(J, K^{(B_{|K})}, N^{A\times B}, L^{(A_{|L})}\right).$$

En effet, E/J étant une extension galoisienne quotient de L/J, l'image par la réciproque de la restriction à L: $A := |_L{}^{-1}(\mathrm{Gal}(L/E))$ est un sous-groupe normal de $\mathrm{Gal}(N/K)$. De même, $B := |_K{}^{-1}(\mathrm{Gal}(K/F)) \trianglelefteq \mathrm{Gal}(N/L)$. Le bigroupe (A, B) est donc normal dans $\mathrm{Gal}(J, K, N, L)$. D'après la surjectivité précédente, on sait donc lui associer le parallélogramme quotient $(J, K^{(B_{|K})}, N^{A\times B}, L^{(A_{|L})})$ qui répond à la question.

Décroissance. Par définition (cf. fait 3.7(2))

$$(J, F_1, C_1, E_1) \leq (J, F_2, C_2, E_2) \Leftrightarrow (E_1 \subseteq E_2, F_1 \subseteq F_2).$$

Or d'après la surjectivité inverse

$$\exists!(A_i, B_i) \trianglelefteq \mathrm{Gal}(J, K, N, L),$$
$$(J, F_i, C_i, E_i) = (J, K^{(B_{i|K})}, N^{A_i \times B_i}, L^{(A_{i|L})})$$

où $A_{i|L} = \mathrm{Gal}(L/E_i)$ et $B_{i|K} = \mathrm{Gal}(K/F_i)$ $(i = 1, 2)$. Comme

$$E_1 \subseteq E_2 \quad \Leftrightarrow \quad A_2 \leq A_1, \qquad F_1 \subseteq F_2 \quad \Leftrightarrow \quad B_2 \leq B_1,$$

on a donc bien $(A_2, B_2) \leq (A_1, B_1)$ (cf. (3.4)).

Réciproque. Par ce qui précède, notamment la surjectivité inverse ci-dessus, la composition des applications de l'énoncé donne deux fois l'identité.

Groupe de Galois. Dans le parallélogramme quotient $(J, F, C, E) = (J, K^{(B_{|K})}, N^{A\times B}, L^{(A_{|L})})$, on a par définition (cf. déf. 3.6(1))

$$\begin{aligned}
\mathrm{Gal}(J, F, C, E) &= (\mathrm{Gal}(C/F), \mathrm{Gal}(C/E)) \\
&\xrightarrow{\sim} (\mathrm{Gal}(L^{(A_{|L})}/J), \mathrm{Gal}(K^{(B_{|K})}/J)) \\
&\xrightarrow{\sim} (\mathrm{Gal}(N/K)/A, \mathrm{Gal}(N/L)/B) \qquad \text{(voir la surjectivité)} \\
&= (\mathrm{Gal}(N/K), \mathrm{Gal}(N/L))/(A, B) \qquad \text{par (3.5)} \\
&= \mathrm{Gal}(J, K, N, L)/(A, B).
\end{aligned}$$

Ceci achève la démonstration du théorème 4.2. ∎

5. DÉMONSTRATION DU THÉORÈME 1.3

I. (1) (1.1) L'extension KE/E est galoisienne en vertu du théorème de l'extension galoisienne translatée [2, p. 266, th. 1.12] appliqué à K/J. Comme $J \subseteq K \cap E \subseteq K \cap L = J$ d'où $K \cap E = J$, on sait par ce même théorème que

$$\mathrm{Gal}(KE/E) \xrightarrow{\sim} \mathrm{Gal}(K/J);$$

autrement dit, dans le parallélogramme (J, K, N, L),

$$\mathrm{Gal}(KE/E) \xrightarrow{\sim} \mathrm{Gal}(N/L).$$

De plus, $KEL = KL = N$. Donc, en translatant l'extension galoisienne KE/E par l'extension L/E, on a

$$\mathrm{Gal}(N/L) \xrightarrow{\sim} \mathrm{Gal}(KE/KE \cap L).$$

On en déduit que $KE \cap L = E$, de sorte que L/E est une descendue de N/KE, d'où le parallélogramme (E, KE, N, L).

(1.2) Il suffit d'ajouter que l'extension KE/K est galoisienne comme translatée de E/J par K/J.

(2) (2.1) Clairement, $L^{(A_{|L})} \subseteq N^A \cap L \subseteq L^{(A_{|L})}$ d'où $E \cap L = L^{(A_{|L})}$, et $N = KL \subseteq EL \subseteq N$ d'où $EL = N$, ce qui prouve que $L/L^{(A_{|L})}$ est une descendue de N/E. Observons par ailleurs que $\mathrm{Gal}(N/L^{(A_{|L})}) = A \times V$ où $V := \mathrm{Gal}(N/L)$. En effet, dans le parallélogramme (J, K, N, L), on a $\mathrm{Gal}(N/J) = \mathrm{Gal}(N/K) \times V$, d'où $A \cap V = \mathbf{1}$; de plus,

$$\left[N : L^{(A_{|L})}\right] = \left[L : L^{(A_{|L})}\right][N : L] = |A|\,|V|$$

d'où $\mathrm{Gal}(N/L^{(A_{|L})}) = AV$, et les éléments de A et de V commutent dans le produit direct $\mathrm{Gal}(N/J)$. En particulier, A est normal dans $\mathrm{Gal}(N/L^{(A_{|L})})$, donc l'extension $E/L^{(A_{|L})}$ est galoisienne; d'où le parallélogramme galoisien $(L^{(A_{|L})}, E, N, L)$.

(2.2) La normalité de $A = \mathrm{Gal}(N/E)$ dans $\mathrm{Gal}(N/K)$ implique celle de $A_{|L}$ dans $\mathrm{Gal}(L/J)$, et l'extension $L^{(A_{|L})}/J$ est galoisienne. Prouvons que c'est une descendue de E/K. De $K \cap L = J$ suit $K \cap L^{(A_{|L})} = J$. Ainsi

$$[KL^{(A_{|L})} : J] = [K : J]\,[L^{(A_{|L})} : J].$$

De plus, d'après le (2.1),

$$[L^{(A_{|L})} : J] = [L : J]/[L : L^{(A_{|L})}] = [N : K]/[N : E] = [E : K].$$

Donc

$$[KL^{(A_{|L})} : J] = [K : J]\,[E : K] = [E : J],$$

et par suite $E = KL^{(A_{|L})}$; d'où le parallélogramme $(J, K, E, L^{(A_{|L})})$.

(3) Il suffit d'appliquer le (1.2) (resp. (2.2)) à l'extension galoisienne E_1/E_0 dans le parallélogramme (E_0, KE_0, N, L) (resp. $(L^{(A_{0|L})}, E_0, N, L)$) qui résulte du (1.1) (resp. (2.1)).

(4) On a le parallélogramme (F, KF, N, L) en vertu du (1.1), et $KF = E$ dans (J, K, E, F).

II. (1) (1.1) En translatant les extensions galoisiennes K/J (resp. L/J, N/J) par l'extension E/J, on obtient les sous-extensions galoisiennes $KE/KE \cap LE$ (resp. $LE/KE \cap LE$, NE/KE) (cf. [2, p. 266, th. 1.12]). Or $KELE = NE$ puisque $KL = N$ dans (J, K, N, L); d'où le parallélogramme $(KE \cap LE, KE, NE, LE)$.

De plus, lorsque les degrés sont finis, on a les divisibilités suivantes:

$$[KE \cap LE : E] \mid [KE : E] = [K : K \cap E] \mid [K : J],$$
$$[KE \cap LE : E] \mid [LE : E] = [L : L \cap E] \mid [L : J].$$

Si donc (J, K, N, L) est de degré séparé, on a bien $KE \cap LE = E$.

(1.2) L'hypothèse E/J galoisienne implique que l'extension intersection $K \cap E/J$ est galoisienne. De même, l'extension $L \cap E/J$ est galoisienne, et il suffit de la translater par $K \cap E/J$ pour voir que $(K \cap E)(L \cap E)/K \cap E$ est galoisienne. Comme $(K \cap E) \cap (L \cap E) = J$, on obtient donc directement le parallélogramme $(J, K \cap E, (K \cap E)(L \cap E), L \cap E)$.

Supposons de plus (J, K, N, L) de degré séparé. D'après le (1.1) précédent, on dispose du parallélogramme (E, KE, NE, LE). Alors, en translatant l'extension galoisienne N/J par E/J,

$$\begin{aligned}
[N : N \cap E] &= [NE : E] = [KE : E]\,[LE : E] \\
&= [K : K \cap E]\,[L : L \cap E] \\
&= \frac{[K : J]}{[K \cap E : J]}\,\frac{[L : J]}{[L \cap E : J]} \\
&= \frac{[N : J]}{[(K \cap E)(L \cap E) : J]} \\
&= [N : (K \cap E)(L \cap E)],
\end{aligned}$$

ce qui prouve que $(K \cap E)(L \cap E) = N \cap E$.

(2) (2.1) L'existence du parallélogramme $(K_1K_2 \cap L_1L_2,\ K_1K_2,\ N_1N_2,\ L_1L_2)$ est claire par composition d'extensions galoisiennes de J.

Lorsque les degrés sont finis, on a par le théorème de l'extension galoisienne translatée

$$[K_1K_2 : J] = [K_1 : K_1 \cap K_2]\,[K_2 : J] = [K_2 : K_1 \cap K_2]\,[K_1 : J],$$
$$[L_1L_2 : J] = [L_1 : L_1 \cap L_2]\,[L_2 : J] = [L_2 : L_1 \cap L_2]\,[L_1 : J].$$

On en déduit que les degrés $[K_1K_2 : J]$, $[L_1L_2 : J]$, sont premiers entre eux si et seulement s'il en est ainsi, deux à deux, des degrés $[K_i : J]$, $[L_j : J]$ $(1 \leq i, j \leq 2)$; et dans ce cas, il est évident que $K_1K_2 \cap L_1L_2 = J$.

(2.2) L'existence du parallélogramme $(J, K_1 \cap K_2, (K_1 \cap K_2)(L_1 \cap L_2), L_1 \cap L_2)$ est claire par intersection d'extensions galoisiennes de J.

Supposons les degrés finis. En quotientant le parallélogramme de degré séparé (J, K_1, N_1, L_1) par l'extension galoisienne N_2/J (confer le (1.2) du II (1) de l'énoncé), on a

$$N_1 \cap N_2 = (K_1 \cap N_2)(L_1 \cap N_2).$$

Les extensions $K_1 \cap N_2/J$ et $L_1 \cap N_2/J$ sont galoisiennes, avec $K_1 \cap N_2 \cap L_1 \cap N_2 = J$; donc

$$\begin{aligned}[N_1 \cap N_2 : J] &= [K_1 \cap N_2 : J]\,[L_1 \cap N_2 : J]\\ &= [K_1 \cap N_2 : K_1 \cap K_2]\,[K_1 \cap K_2 : J]\\ &\quad \times [L_1 \cap N_2 : L_1 \cap L_2]\,[L_1 \cap L_2 : J].\end{aligned}$$

D'autre part

$$\big[N_1 \cap N_2 : J] = [N_1 \cap N_2 : (K_1 \cap K_2)\,(L_1 \cap L_2)]\,[K_1 \cap K_2 : J]\;[L_1 \cap L_2 : J].$$

On voit donc que

$$\begin{aligned}&[N_1 \cap N_2 : (K_1 \cap K_2)\,(L_1 \cap L_2)]\\ &\quad = [K_1 \cap N_2 : K_1 \cap K_2]\,[L_1 \cap N_2 : L_1 \cap L_2].\end{aligned}$$

Quotientons maintenant le parallélogramme de degré séparé $(J,\ K_2, N_2, L_2)$ par les extensions galoisiennes K_1/J et L_1/J successivement; il vient

$$K_1 \cap N_2 = (K_1 \cap K_2)\;(K_1 \cap L_2),$$
$$L_1 \cap N_2 = (K_2 \cap L_1)\;(L_1 \cap L_2).$$

De plus, en translatant l'extension galoisienne $K_1 \cap L_2/J$ (resp. $K_2 \cap L_1/J$) par l'extension $K_1 \cap K_2/J$ (resp. $L_1 \cap L_2/J$), on a

$$[(K_1 \cap K_2)(K_1 \cap L_2) : K_1 \cap K_2] = [K_1 \cap L_2 : J]$$
$$\big(\text{resp. } [(K_2 \cap L_1)(L_1 \cap L_2) : L_1 \cap L_2] = [K_2 \cap L_1 : J]\big).$$

Finalement, par conjonction des égalités précédentes, on obtient que

$$[N_1 \cap N_2 : (K_1 \cap K_2)(L_1 \cap L_2)] = [K_1 \cap L_2 : J]\;[K_2 \cap L_1 : J],$$

ce qui achève la démonstration du théorème 1.3. ∎

REFERENCES

1. G. Brattström, On p-groups as Galois groups, *Math. Scand.* **65** (1989), 165–174.
2. S. Lang, "Algebra," 3ème éd., Addison–Wesley, Reading, MA, 1995.
3. A. Ledet, Subgroups of Hol Q_8 as Galois groups, *J. Algebra* **181** (1996), 478–506.
4. R. Massy, Construction de p-extensions galoisiennes d'un corps de caractéristique différente de p, *J. Algebra* **109** (1987), 508–535.
5. R. Massy et S. Monier-Derviaux, Descente et parallélogramme galoisiens, *J. Théorie des Nombres Bordeaux (Actes J. A. 97)*, à paraître.
6. S. Monier-Derviaux, "Le Problème de la Descente Galoisienne Finie," Thèse de Doctorat, Univ. Valenciennes, 1997.
7. S. Monier, Descente de p-extensions galoisiennes kummériennes, *Math. Scand.* **79** (1996), 5–24.
8. J.-P. Serre, "Corps Locaux," 3ème éd., Hermann, Paris, 1980.
9. J. R. Swallow, Central p-extensions of $(p, p, \ldots, p)$-type Galois groups, *J. Algebra* **186** (1996), 277–298.