Dissociation des Extensions Algébriques de Corps par les Extensions Galoisiennes ou Galsimples non Galoisiennes

Emmanuel Andréo

UNIVERSITÉ DE VALENCIENNES ET DU HAINAUT - CAMBRÉSIS

THÈSE

pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE VALENCIENNES

Discipline : **Mathématiques Pures**
présentée et soutenue publiquement par

Emmanuel ANDRÉO
le 15 juin 2004

Titre : *Dissociation des Extensions Algébriques de Corps par les Extensions Galoisiennes ou Galsimples non Galoisiennes*

Directeur de thèse : Richard MASSY Professeur,
Université de Valenciennes

JURY

Président : Christian U. JENSEN Professor,
University of Copenhagen

Rapporteurs : Jean-François JAULENT Professeur,
Université de Bordeaux I

John R. SWALLOW Kimbrough Associate Professor,
Davidson College

Arne LEDET Assistant Professor,
Texas University

Examinateurs : Pierre DÈBES Professeur,
Université de Lille I

Manfred HARTL Professeur,
Université de Valenciennes

REMERCIEMENTS

J'exprime d'abord toute ma gratitude à mon unique directeur de recherche, le Professeur Richard Massy, pour l'extraordinaire attention qu'il m'a procurée ces cinq années. C'est grâce à ses conseils que je me suis lancé dans cette formidable aventure. Qu'il soit également remercié pour la primeur qu'il me laisse de son "Théorème M".

Les Professeurs Jean-François Jaulent, Arne Ledet et John Swallow m'ont fait l'honneur d'accepter d'être les rapporteurs de ce travail. Merci à eux pour le temps qu'ils m'ont consacré et pour leurs remarques pertinentes.

Je rends hommage au Professeur Christian U. Jensen : il participa au cours de D.E.A. qui m'introduisit aux études doctorales, et je lui dois plusieurs de mes exemples. Qu'il figure dans mon Jury est pour moi un accomplissement.

Les Professeurs Pierre Dèbes et Manfred Hartl ont bien voulu être les examinateurs des sept chapitres qui suivent. Que la lecture de ceux-ci leur laisse le meilleur souvenir...

Ma reconnaissance va aussi au Lamath, pour les moyens mis à ma disposition et pour l'atmosphère chaleureuse que j'y ai trouvée.

Enfin merci à toute ma famille et à mes amis pour leurs encouragements constants.

INTRODUCTION

Le théorème fondamental de l'Arithmétique factorise tout nombre entier en produit de nombres premiers. En théorie des groupes, le théorème de Jordan-Hölder dévisse de nombreux groupes par leurs suites normales qui se raffinent en suites de composition. Le dernier théorème du chapitre 7 final de cette thèse dissocie toute extension de corps de degré fini par ses "tours d'élévation" qui se raffinent en "tours de composition".

Le thème central de ce travail est donc celui de la dissociation des extensions de corps. Nous prouvons que cette dissociation joue pour les extensions finies un rôle analogue à celui de la factorisation pour les entiers.

Détaillons maintenant ce point de vue. Pour les groupes, on connaît les deux célébres théorèmes suivants :

Théorème de Schreier Deux suites normales d'un même groupe admettent des raffinements équivalents.

Théorème de Jordan-Hölder Soit G un groupe admettant une suite de composition.
(1) Toute suite normale stricte de G admet un raffinement qui est une suite de composition de G.
(2) Deux suites de composition de G sont équivalentes.

La problématique, le questionnement de cette thèse est de se demander s'il existe pour les extensions de corps des analogues à ces deux profonds théorèmes qui révèlent la structure des groupes.

Et dans l'affirmative, peut-on obtenir ces analogues à l'instar de la théorie des groupes, c'est à dire de manière intrinsèque, en restant à l'intérieur des extensions considérées, par opposition à une approche extrinsèque faisant intervenir leurs clôtures galoisiennes ? Notre démarche se veut en effet effective, calculatoire, ce qui exclut de procéder via les clôtures galoisiennes, beaucoup trop grandes voire inconnues en général.

Les extensions non galoisiennes peuvent être considérées comme chaotiques. Est-il possible "d'approximer" les extensions algébriques par exemple, ou tout au moins certaines d'entre elles, par les extensions galoisiennes ? Peut-on dissocier ces extensions par leurs corps intermédiaires de façon à constituer une tour qui comporte le plus grand nombre possible de "marches galoisiennes" ?

Dans [**28**], Massy a introduit la notion de parallélogramme galoisien qui généralise celle d'extension galoisienne. Cependant, le théorème final ne s'énonce qu'en degrés finis. Pour ne pas limiter notre analogue du théorème de Schreier aux extensions finies, il a fallu, de manière déterminante, utiliser certaines propriétés des parallélogrammes galoisiens infinis. Leur étude est justement l'objet du chapitre 1, où nous présentons une théorie de Galois infinie en dimension 2 généralisant aux parallélogrammes de degré quelconque le théorème de Krull pour les extensions galoisiennes infinies.

Dès le chapitre 2, nous sommes amenés à définir précisément ce que sont les tours de corps, les marches d'une tour de corps, les tours galoisiennes :
Soit L/K une extension de corps. Une "tour (F) de L/K" est une suite finie croissante $\{F_i\}_{0\leq i\leq m}$ de corps intermédiaires entre K et L, telle que $F_0 = K$ et $F_m = L$:

$$(F) \qquad K = F_0 \leq F_1 \leq \cdots \leq F_i \leq F_{i+1} \leq \cdots \leq F_m = L.$$

Nous disons que les extensions F_{i+1}/F_i $(i = 0, \ldots, m-1)$ sont les "marches" de la tour (F). Nous appelons "tour galoisienne de L/K" une tour de L/K dont toutes les marches sont galoisiennes. En reprenant le symbole de théorie des groupes exprimant le fait d'être "normal dans", nous écrirons les tours galoisiennes

$$(F) \qquad K = F_0 \trianglelefteq F_1 \trianglelefteq \cdots \trianglelefteq F_i \trianglelefteq F_{i+1} \trianglelefteq \cdots \trianglelefteq F_m = L.$$

Le but du chapitre 2 est d'introduire une généralisation de la notion d'extension galoisienne : celle d'extension galtourable. Il existe des extensions qui ne peuvent se dissocier en une tour galoisienne : mis à part les extensions non galoisiennes de degré premier, c'est le cas par exemple pour $\mathbb{Q}(\sqrt[6]{2})/\mathbb{Q}$. Nous appelons "extension galtourable" une extension qui admet une tour galoisienne. Toute extension galoisienne est évidemment galtourable, la réciproque étant fausse. La classe des extensions galtourables contient donc strictement celle des extensions galoisiennes. Cependant nous parvenons à étendre aux extensions galtourables les propriétés essentielles de la théorie de Galois générale classique. Par exemple :

Soient K/J et L/J deux extensions algébriques. Sous la seule condition que K et L soient contenus dans un même corps, on a l'implication

$$(L/J \textit{ galtourable }) \qquad \Longrightarrow \qquad (KL/K \textit{ galtourable }).$$

De même, tout compositum d'extensions galtourables est galtourable. Précisément :
Quelles que soient les extensions galtourables K/J et L/J dont les sommets sont contenus dans un même corps, l'extension compositum KL/J est galtourable.

Quand on empile deux extensions galoisiennes, on obtient une extension galtourable non nécessairement galoisienne en général. La situation est différente

avec les extensions galtourables. Précisément :

Pour toute tour $K \leq L \leq M$, avoir L/K galtourable et M/L galtourable implique que M/K est galtourable.

Mentionnons que les extensions galtourables constituent une "généralisation maximale" des extensions galoisiennes : une extension admettant une tour galtourable est encore une extension galtourable.

Le chapitre 3, très technique, est nécessaire pour parvenir à des démonstrations rigoureuses dans la suite. Nous y introduisons, par analogie avec la théorie des groupes, la notion de raffinement de tour de corps :
Soient L/K une extension algébrique, et

$$(F) \qquad K = F_0 \leq F_1 \leq \cdots \leq F_i \leq F_{i+1} \leq \cdots \leq F_m = L$$

une tour de L/K.
(1) Nous appelons "raffinement de (F)" toute tour

$$(E) \qquad K = E_0 \leq E_1 \leq \cdots \leq E_j \leq E_{j+1} \leq \cdots \leq E_n = L$$

de L/K vérifiant les deux conditions suivantes :

(RAF1) $m \leq n$.
(RAF2) Il existe une suite finie d'indices
$0 \leq j_0 < j_1 < \cdots < j_m \leq n$

telle que

$$\forall i \in \{0, \ldots, m\} \quad F_i = E_{j_i} .$$

(2) Nous appelons "raffinement propre de (F)" tout raffinement (E) de (F) qui vérifie la condition supplémentaire

$$\text{(RAF3)} \qquad \exists j \in \{1, \ldots, n-1\} \quad \forall i \in \{0, \ldots, m\} \quad E_j \neq F_i .$$

(3) Nous disons que (E) est un "raffinement strict" de (F) si et seulement si c'est une tour stricte.
(4) Nous disons que (E) est un "raffinement trivial" de (F) si et seulement si c'est un raffinement de (F) non propre, autrement dit qui vérifie comme condition supplémentaire la négation de (RAF3) précédente, i.e.

$$\text{(RAFT)} \qquad \forall j \in \{1, \ldots, n-1\} \quad \exists i \in \{0, \ldots, m\} \quad E_j = F_i .$$

(5) Nous disons que (E) est un "raffinement galoisien" de (F) si et seulement si c'est un raffinement de (F) qui vérifie la condition supplémentaire

$$\text{(RAFG)} \quad \forall j \in \{1, \ldots, n-1\} \quad \Big(\forall i \in \{0, \ldots, m\} \quad E_j \neq F_i\Big) \Rightarrow E_{j-1} \trianglelefteq E_j .$$

Nous démontrons en particulier qu'un raffinement galoisien d'une tour galoisienne est encore une tour galoisienne (d'où la terminologie).

Le chapitre 4 énonce les premiers théorèmes de dissociation. Nous définissons tout d'abord les tours de composition galoisiennes et l'équivalence de deux tours galoisiennes :
Soient L/K une extension galtourable et

$$(F) \qquad K = F_0 \trianglelefteq \cdots \trianglelefteq F_i \trianglelefteq \cdots \trianglelefteq F_m = L$$

une tour galoisienne de L/K.
(1) Nous disons que (F) est "une tour de composition galoisienne de L/K" si et seulement si elle est stricte et n'admet aucun raffinement galoisien propre.

(2) Soit

$$(E) \qquad K = E_0 \trianglelefteq \cdots \trianglelefteq E_j \trianglelefteq \cdots \trianglelefteq E_n = L$$

une autre tour galoisienne de L/K. Nous disons que (E) et (F) sont "équivalentes", et nous notons $(E) \sim (F)$, si et seulement si elles ont même nombre de marches : $m = n$, et si, à permutation près, les groupes de Galois de ces marches sont isomorphes (topologiquement en degrés infinis) :

$$\exists \sigma \in S_m \quad \forall i \in \{1, \ldots, m = n\} \quad Gal(F_i/F_{i-1}) \xrightarrow{\sim} Gal(E_{\sigma(i)}/E_{\sigma(i)-1}) \; .$$

Avec ces définitions, nous énonçons et prouvons les analogues suivants, pour les extensions galtourables, des théorèmes de Schreier et de Jordan-Hölder :

Théorème. *(1^{er} théorème de dissociation)*
Si L/K est une extension galtourable, deux tours galoisiennes de L/K admettent des raffinements équivalents.

Scholie. L'extension L/K peut être ici de degré infini.

Théorème. *($3^{ème}$ théorème de dissociation)*
Soit L/K une extension galtourable de degré fini.
(1) Toute tour stricte de L/K admet un raffinement galoisien qui est une tour de composition galoisienne de L/K.
(2) Deux tours de composition galoisiennes de L/K sont équivalentes.

Le deuxième théorème de dissociation fournit une caractérisation des extensions admettant une tour de composition galoisienne. On sait qu'un groupe admet une suite de composition si et seulement s'il satisfait la condition de chaîne normale ; c'est en particulier le cas des groupes finis. Voici la version galoisienne de ce résultat :

Théorème. *($2^{ème}$ théorème de dissociation)*
Une extension de corps admet une tour de composition galoisienne si et seulement si elle est galtourable de degré fini.

Un autre parallèle avec les groupes est fourni par la notion de "galsimplicité". En terme de dissociation, les extensions galsimples jouent le rôle des groupes

simples en théorie des groupes. Nous appelons "extension galsimple" une extension L/K non triviale n'admettant aucune extension quotient galoisienne propre :

$$(L/K \text{ galsimple}) \quad \overset{\text{Déf.}}{\Longleftrightarrow} \quad \left(\begin{array}{c} L \neq K, \quad \forall F \quad K \leq F \leq L \\ (F/K \text{ galoisienne}) \Rightarrow (F = K \text{ ou } F = L) \end{array} \right).$$

On sait que pour qu'une suite normale de groupes soit de composition, il faut et il suffit que chacun de ses facteurs soit simple. Voici la version galoisienne de ce résultat :

Soit L/K une extension galtourable quelconque. Pour qu'une tour galoisienne de L/K soit de composition, il faut et il suffit que chacune de ses marches soit galsimple.

Le chapitre 5 est essentiellement constitué d'exemples des notions précédentes. Il comporte également quelques propriétés des extensions galsimples qui nous sont utiles dans les deux derniers chapitres.

Le coeur du chapitre 6 est le "théorème M", dû à Richard Massy. Celui-ci montre qu'à toute extension finie est attachée un invariant, son "corps d'intourabilité", au-delà duquel l'extension n'est plus galtourable :

Théorème. *($4^{ème}$ théorème de dissociation)*
Pour toute extension finie L/K , il existe un corps intermédiaire M et un seul entre K et L, vérifiant à la fois les deux propriétés suivantes :
(1) L'extension M/K est galtourable ;
(2) La sous-extension L/M est soit triviale, soit galsimple non galoisienne.

Nous mettons en évidence le rôle central du corps d'intourabilité, noté $M(L/K)$, en prouvant deux maximalités : pour une relation d'ordre canonique, l'extension $M(L/K)/K$ (resp. $L/M(L/K)$) se réalise comme l'extension quotient galtourable (resp. la sous-extension galsimple non galoisienne) maximale de L/K. Nous achevons le chapitre 6 en exhibant une large classe d'exemples de ce corps d'intourabilité en termes de corps cyclotomiques.

Le chapitre 7 final est l'aboutissement des précédents. Nous y introduisons, grâce au corps d'intourabilité, la notion de "tour d'élévation" associée à une tour de corps : elle fait correspondre canoniquement à toute tour de L/K une tour galtourable de l'extension quotient galtourable maximale $M(L/K)/K$ de L/K. Nous avons noté horizontalement $F \trianglelefteq E$ une extension galoisienne E/F ; notons $F \lesseqgtr E$ lorsque E/F n'est que galtourable. Ceci permet d'écrire les tours d'élévation de $M(L/K)/K$:

Soit L/K une extension finie quelconque. Toute tour

$$(F) \qquad K = F_0 \leq F_1 \leq \cdots \leq F_i \leq \cdots \leq F_m = L$$

de L/K induit une tour galtourable constituée des corps d'intourabilité sur K de chacun des corps de (F) :

$$K = M_0 := M(F_0/K) \lneqq M_1 := M(F_1/K) \lneqq \cdots \lneqq M_i := M(F_i/K) \lneqq \ldots \\ \cdots \lneqq M_m := M(F_m/K) = M(L/K) \ .$$

Nous l'appelons "tour d'élévation de $M(L/K)\nearrow K$ associée à (F)"

Les tours d'élévation de l'extension L/K elle-même s'obtiennent comme "tours induites" des tours d'élévation de $M(L/K)\nearrow K$. Précisément :
Soient M un corps d'intermédiaire entre K et L : $K \leq M \leq L$, et

$$(E) \qquad K = E_0 \leq E_1 \leq \cdots \leq E_m = M$$

une tour de M/K. Nous appelons "tour de L/K induite par (E)", et nous notons

$$((E) \dashrightarrow L) \ ,$$

la tour de L/K définie de la façon suivante

$$((E) \dashrightarrow L) := \begin{cases} (E) & \text{si } M = L \\ K = E_0 \leq E_1 \leq \cdots \leq E_m = M < L & \text{si } M \neq L \end{cases} \ .$$

Soient L/K une extension finie et (F) une tour quelconque de L/K. Nous appelons "tour d'élévation de L/K associée à (F)" la tour de L/K induite par la tour d'élévation associée à (F) de l'extension quotient galtourable maximale de $M(L/K)\nearrow K$ de L/K.

Ceci nous permet de définir des tours de compositions non nécessairement galoisiennes :
Soit L/K une extension finie quelconque. Nous appelons "tour de composition de L/K" toute tour d'élévation de L/K stricte qui n'admet aucun raffinement galoisien propre.
Une caractérisation de ces tours de composition est la suivante :

Soient L/K une extension finie et

$$(C) \qquad K = C_0 \leq \cdots \leq C_i \leq \cdots \leq C_m = L$$

une tour de L/K. On a l'équivalence :
(C) est une tour de composition si et seulement si elle est induite par une tour de composition galoisienne de l'extension quotient galtourable maximale de L/K.

Nous n'avons jusqu'ici défini l'équivalence de deux tours d'une même extension que lorsque ces tours sont galoisiennes. La définition ci-après de l'équivalence de deux tours induites implique en particulier celle de l'équivalence de deux tours de composition non galoisiennes :
Soient L/K une extension finie quelconque, (T) et (T') deux tours galoisiennes de l'extension quotient galtourable maximale $M(L/K)\nearrow K$ de L/K. Nous disons

que les tours induites de L/K par (T) et (T') sont équivalentes si et seulement si les tours galoisiennes (T) et (T') le sont au sens du chapitre 4 :

$$((T) \dashrightarrow L) \sim ((T') \dashrightarrow L) \quad \overset{\text{Déf.}}{\Longleftrightarrow} \quad (T) \sim (T') \,.$$

Ceci pour aboutir enfin à la généralisation aux extensions finies quelconques des théorèmes de dissociation obtenus au chapitre 4 pour des extensions galtourables :

Théorème. *($5^{ème}$ théorème de dissociation)*
Deux tours d'élévation d'une même extension finie quelconque admettent des raffinements galoisiens qui sont des tours d'élévation équivalentes de cette extension.

Théorème. *($6^{ème}$ théorème de dissociation)*
Soit L/K une extension finie quelconque.
(1) Toute tour d'élévation stricte de L/K admet un raffinement galoisien qui est une tour de composition de L/K.
(2) Deux tours de composition de L/K sont équivalentes.

Chapitre 1

PARALLÉLOGRAMMES GALOISIENS INFINIS

1. Introduction

Dans [**28**], 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 [**29**]. Le but de ce premier chapitre est d'étendre les résultats de [**28**] aux parallélogrammes de degré infini. Nous mettons en évidence section 5 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 6. 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 aux chapitres 3 et 4 pour développer en toute généralité une notion de "raffinement de tours galoisiennes" jouant pour les extensions galoisiennes un rôle analogue à celui du raffinement des suites normales de groupes.

2. Définitions

Plusieurs des démonstrations de [**28**] 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 5 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 2.1. Nous appelons "quadrilatère corporel" (ou "quadrilatère" en abrégé) 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) $KL = N$.

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

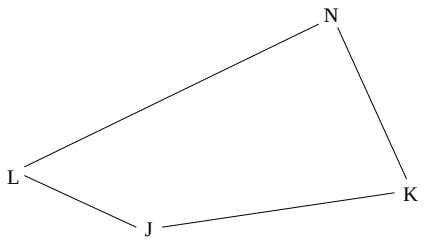

FIG. 1. *Quadrilatère corporel*

La définition suivante figure dans la section 3 de **[28]** pour des extensions galoisiennes qui justifient la terminologie.

Définition 2.2. (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 :

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

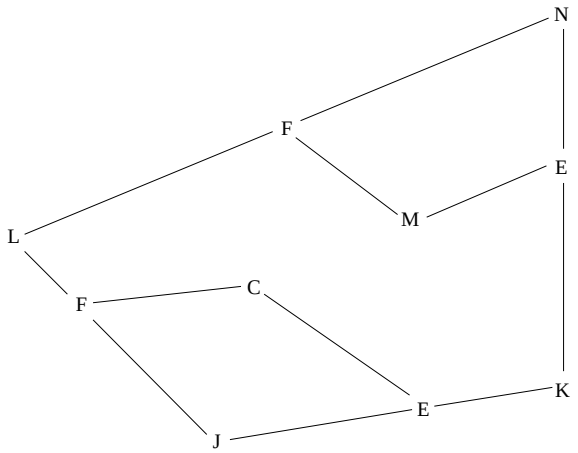

FIG. 2. *Sous-quadrilatère & quadrilatère quotient*

Nous aurons besoin du lemme immédiat suivant pour les monotonies des bijections de la section 5.

Lemme 2.3. *(1) Soit E/F une extension algébrique. Dans l'ensemble des sous-extensions (resp. des extensions quotients) de E/F, la relation définie par*

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

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

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

est une relation d'ordre.

Définition 2.4. 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 (où les flêches symbolisent les extensions galoisiennes)

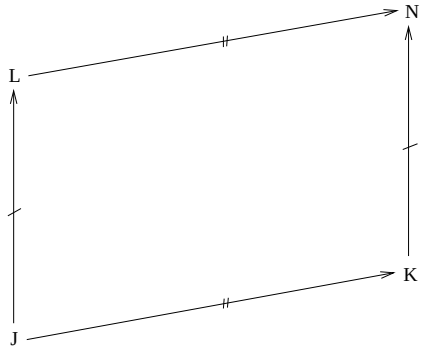

FIG. 3. *Parallélogramme galoisien*

Par composition, la "diagonale N/J" d'un parallélogramme $[J,K,N,L]$ est nécessairement galoisienne. Dans [**28**] , "le degré" d'un parallélogramme galoisien $[J,K,N,L]$ est défini comme étant le couple des degrés :

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

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 2.5. [**28**, 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. [**28**, 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 à 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. [**22**] ou [**19**, 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 [**7**, TG III.7]. C'est le groupe de Galois de E sur le corps des invariants de H dans E [**19**, p.344] i.e.

$$\overline{H} = Gal(E/E^H). \qquad (0)$$

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 :

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

Démonstration. (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_α est continue [**7**, 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_β, 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 (0) ci-dessus et le fait que la sous-extension E/E^H soit galoisienne, on a directement

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

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 $Gal(N/K)$.*

Démonstration. Posons $\Gamma := Gal(N/K)$, $A := Gal(N/E)$ et soit α un élément quelconque de A. Prouvons d'abord que tout voisinage V de α pour la topologie de Krull de A est aussi un voisinage de α pour la topologie induite sur A par celle de Γ. Par définition de la topologie de Krull de A, il existe une extension galoisienne finie M/E, avec $M \subseteq N$, telle que $V \supseteq \alpha\, Gal(N/M)$.

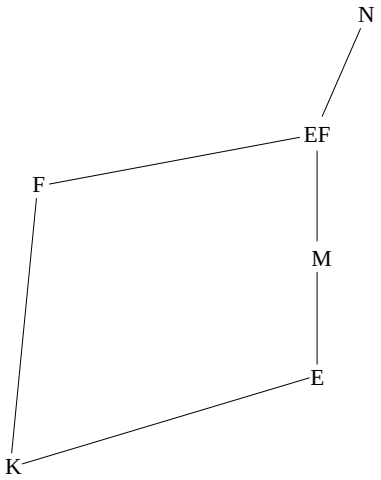

FIG. 4. *Topologie de Krull induite*

En vertu du théorème de l'élément primitif, il existe d'autre part un élément $x \in M$ 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 α pour la topologie de Krull de Γ puisque F/K est galoisienne finie. Ceci prouve que V est bien un voisinage de α pour la topologie induite sur A par celle de Γ.

La réciproque reprend certains des arguments précédents dans l'ordre inverse. Soit $V = U \cap A$ un voisinage de α dans lequel U est un voisinage de α pour la topologie de Krull de Γ. 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 α pour la topologie de Krull de A. □

Lemme 3.3. *Soient N/K une extension galoisienne et E/K, $E \subseteq N$, une extension galoisienne quotient de N/K. Soit ρ_E l'homomorphisme de restriction de $Gal(N/K)$ sur $Gal(E/K)$. Alors, pour toute extension galoisienne quotient F/K de N/K,*

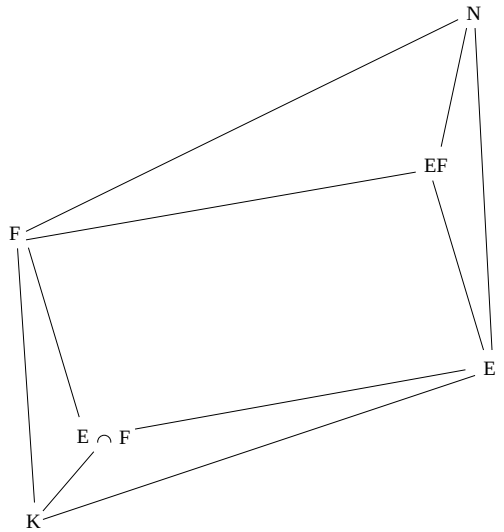

FIG. 5. *Parallélogramme galoisien inscrit*

on a

$$\rho_E(Gal(N/F)) = Gal(E/E \cap F).$$

Démonstration. En translatant l'extension galoisienne E/K par F/K, on obtient l'extension galoisienne EF/F et un isomorphisme de restriction $|_E$ du groupe $Gal(EF/F)$ sur $Gal(E/E \cap F)$. Soit donc $r \in Gal(E/E \cap F)$; il existe $s \in Gal(EF/F)$ tel que $s_{|_E} = r$. Et en considérant EF/F comme une extension galoisienne quotient de N/F, il existe $t \in Gal(N/F)$ tel que $t_{|_{EF}} = s$. Alors, pour tout $x \in E$,

$$(\rho_E(t))(x) = t_{|_{EF}}(x) = s_{|_E}(x) = r(x) \ ,$$

de sorte que $\rho_E(t) = r$, et $Gal(E/E \cap F) \subseteq \rho_E(Gal(N/F))$. L'autre inclusion est claire. □

Le lemme précédent nous permet d'énoncer un analogue de la proposition 3.2 en remplaçant topologie induite par topologie quotient.

Proposition 3.4. *Soit N/K une extension galoisienne. Pour tout corps intermédiaire E, $K \subseteq E \subseteq N$, tel que l'extension E/K soit galoisienne, la topologie de Krull de $Gal(E/K)$ est égale à la topologie quotient sur $Gal(E/K)$ de la topologie de Krull de $Gal(N/K)$.*

Démonstration. Soit

$$\begin{aligned} \rho_E \ : \quad \Gamma := Gal(N/K) &\longrightarrow G := Gal(E/K) \\ \gamma &\longmapsto \gamma_{|_E} \end{aligned}$$

l'homomorphisme de restriction à E. Considérons d'abord un voisinage V d'un élément $\gamma_{|_E} = \rho_E(\gamma)$, $\gamma \in \Gamma$, de G muni de sa topologie de Krull. Par définition de celle-ci, il existe une extension galoisienne finie E_γ/K , $E_\gamma \subseteq E$, telle que $V \supseteq \gamma_{|_E} Gal(E/E_\gamma)$. D'après le lemme 3.3,

$$\rho_E(\gamma\, Gal(N/E_\gamma)) = \gamma_{|_E}\, Gal(E/E \cap E_\gamma) = \gamma_{|_E}\, Gal(E/E_\gamma).$$

Il s'ensuit que

$$\rho_E^{-1}(V) \supseteq \rho_E^{-1}(\gamma_{|_E}\, Gal(E/E_\gamma)) = \rho_E^{-1}(\rho_E(\gamma\, Gal(N/E_\gamma))) \supseteq \gamma\, Gal(N/E_\gamma).$$

Comme $\gamma\, Gal(N/E_\gamma)$ est un ouvert pour la topologie de Krull de Γ, on obtient que $\rho_E^{-1}(V)$ est un voisinage de γ pour cette topologie. Autrement dit, la topologie de Krull sur G rend ρ_E continue. Or la topologie quotient sur G est par définition la plus fine de celles rendant la surjection ρ_E continue. Ceci signifie que toute partie ouverte pour la topologie de Krull de G est ouverte pour la topologie quotient sur G [**7**, TGI.11].

Considérons maintenant un ouvert Θ pour la topologie quotient sur G de la topologie de Krull de Γ. Par la continuité de ρ_E pour cette topologie, $\Omega := \rho_E^{-1}(\Theta)$ est un ouvert de Γ, donc voisinage de chacun de ses points. Par définition de la

topologie de Krull sur Γ, il existe, pour tout $\omega \in \Omega$, une extension galoisienne finie E_ω/K , $E_\omega \subseteq N$, telle que

$$\omega\, Gal(N/E_\omega) \subseteq \Omega\,.$$

Donc clairement

$$\Omega = \bigcup_{\omega\in\Omega} \omega\, Gal(N/E_\omega)\,.$$

Et comme ρ_E est surjective

$$\Theta = \rho_E(\rho_E^{-1}(\Theta)) = \rho_E(\Omega) = \bigcup_{\omega\in\Omega} \omega_{|_E}\, \rho_E(\, Gal(N/E_\omega)\,)\,.$$

En appliquant le lemme 3.3 à l'extension galoisienne quotient E_ω/K de N/K, on obtient donc que

$$\Theta = \bigcup_{\omega\in\Omega} \omega_{|_E}\, Gal(E/E\cap E_\omega)\,.$$

Or les extensions $E\cap E_\omega/K$ sont galoisiennes comme intersections d'extensions galoisiennes de K, et elles sont finies comme chaque E_ω/K. Par conséquent les $\omega_{|_E}\, Gal(E/E\cap E_\omega)\quad(\omega\in\Omega)$ sont des ouverts pour la topologie de Krull de G, et il en est de même de Θ par union. On a donc montré que toute partie ouverte pour la topologie quotient sur G est ouverte pour la topologie de Krull de G. D'où la conclusion. □

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 des sections 4 à 6.

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

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

Démonstration. 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 Γ et Λ sont normaux dans Δ. 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 [**28**]. Il est surprenant de constater qu'aucune propriété topologique (de fermeture) n'est exigée sur les groupes considérés.

Théorème 4.2. *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

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

Démonstration. (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

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

[**23**, 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

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

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 γ 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 KF/F 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 le (0) 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, κ 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 ρ_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

$$[L^{A_0}, KL^{A_0}, N, L] \quad (\text{resp. } [L^{A_{0|L}}, N^{A_0}, N, L] \text{ }).$$

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

(2-1) On a le sous-parallélogramme $[E \cap L, E, N, L]$.

(2-2) 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. 2.5) 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* $[J, K^{(B_{|K})}, N^{A\times B}, L^{(A_{|L})}]$.

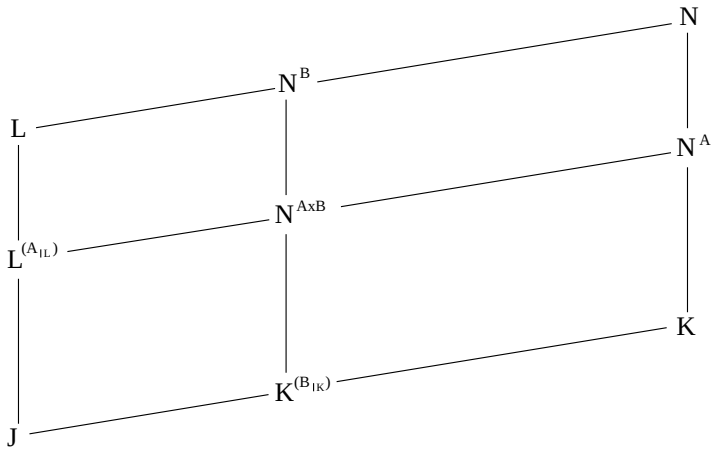

FIG. 6. *Sous-parallélogramme & parallélogramme quotient*

Démonstration. (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

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

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 4.2. 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 4.2, le fait que A (resp. B) soit normal dans $Gal(N/K)$ (resp. $Gal(N/L)$) induit le parallélogramme

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

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 6.7.

Proposition 5.2. *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. 2.5).
(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

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

Démonstration. (1) (1-1) Par la définition 2.5,

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

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 Φ_s est prouvée.

(1-2) L'application Ψ_s existe en vertu du (1) du théorème 5.1. Sa surjectivité résulte immédiatement du (1-3).

(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 (1-1) du corollaire 4.3, on a le parallélogramme $[F,KF,N,L]$ dans lequel $Gal(N/KF)_{|_L}=Gal(L/F)$. De plus, dans $[J,E,C,F]$, l'extension F/J est galoisienne et, d'après le (1-2) de ce même corollaire, 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 Φ_q résulte de l'unicité du sous-bigroupe normal (A,B) du (2-0). L'application Ψ_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 Φ_q est injective et Ψ_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 4.2 (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 au chapitre 4 avec la notion de tour galoisienne de composition. 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 5.5 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 5.3. (dit "de l'écartelé" [2])
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

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

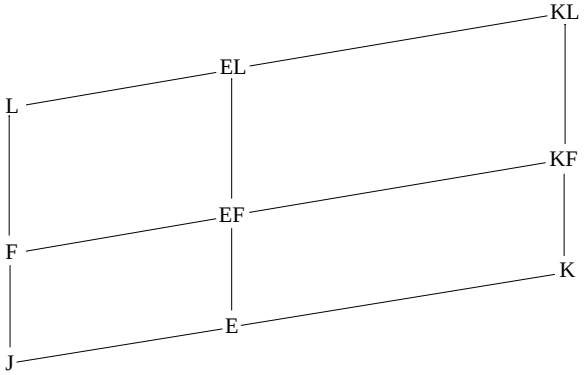

FIG. 7. *Ecartelé compositum*

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

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

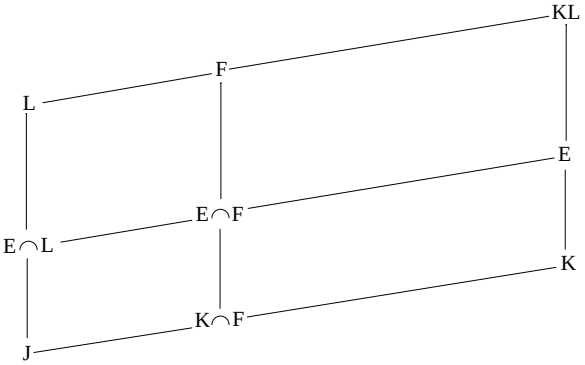

FIG. 8. *Ecartelé intersection*

[2] du nom du blason qu'évoquent, en héraldique, les figures correspondant au théorème.

Démonstration. 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 4.3, 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 (1-1) de la proposition 5.2, 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 4.2, 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 5.4. *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

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

Démonstration. (1) Le parallélogramme $[EF, KF, KL, EL]$ apparaît déjà dans la démonstration du (1) du théorème 5.3. 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 5.3 qui donne aussi le quadrilatère

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

Proposition 5.5. *Soit $[J, K, N, L]$ un parallélogramme galoisien de degré quelconque. Notons*

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

l'ensemble des sous-quadrilatères (resp. des quadrilatères quotients) de $[J, K, N, L]$. Pour les relations d'ordre du (2) du lemme 2.3 :
(1) L'application

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

est une bijection décroissante.

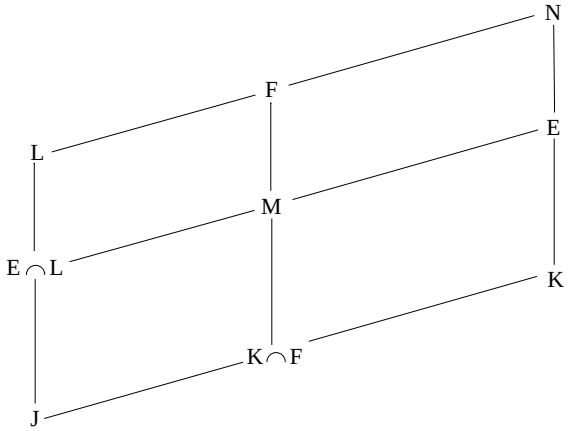

FIG. 9. *Bijection $\mathcal{R}$*

(2) L'application

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

est une bijection décroissante.

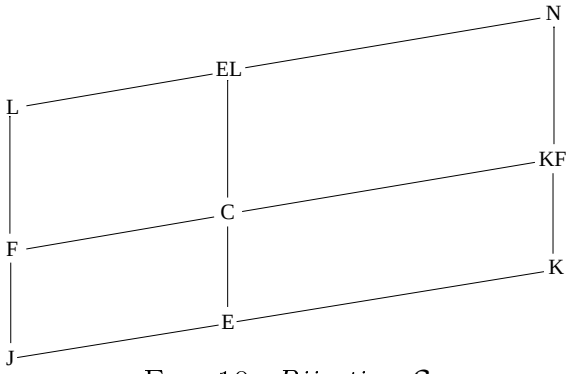

FIG. 10. *Bijection* $\mathcal{S}$

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

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

Démonstration. 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

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

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 2.3(2) car

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

implique que

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

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 2.3(2) car

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

implique que

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

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 $\mathcal{R} \circ \mathcal{S} = id_{\mathcal{R}quad}$. □

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

Dans cette section, nous enrichissons la proposition algébrique 5.2 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 Φ et Ψ de la proposition 5.2 deviennent des bijections. Le théorème 6.7 généralise ainsi, d'une part le théorème principal de la théorie de Galois finie en dimension 2 [**28**, Th.4-2] généralisant lui-même la bijection de Galois classique, d'autre part le théorème de Krull qui se retrouve en particularisant à des parallélogrammes galoisiens infinis plats.

Par définition dans [**33**, 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 6.1. (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 un 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 de la proposition 6.4 ci-dessous, sortons du contexte le fait général suivant.

Lemme 6.2. *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.*

Démonstration. Si B est fermée dans A, il existe un fermé F de X tel que $B = F \cap A$, et inversement, il suffit d'écrire $B = B \cap A$. □

Lemme 6.3. *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.

Démonstration. La première équivalence étant claire, il suffit de prouver la seconde et plus précisément le sens direct de celle-ci. Appliquons le lemme 6.2 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 6.4. *Lorsque E/F est une extension galoisienne, la relation d'ordre du lemme 2.3.(1) dans l'ensemble des sous-extensions de E/F (resp. des extensions galoisiennes quotients de E/F) s'écrit*

$$(E/M') \leq (E/M) \quad \Leftrightarrow \quad Gal(E/M') \leq_c Gal(E/M)$$
$$\Big(\textit{resp. } (M/F) \leq (M'/F) \quad \Leftrightarrow \quad Gal(E/M') \leq_c Gal(E/M) \Big) .$$

Démonstration. Immédiate par le lemme 6.3. □

Pour le généraliser en dimension 2, reformulons maintenant le théorème de Krull classique [**8**, AV.64,Th.4].

Théorème 6.5. (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 6.4 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

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

Démonstration. 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 6.4.
(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 6.4 à avoir $(N^{H_2}/K) \leq (N^{H_1}/K)$. □

Proposition 6.6. *Soit $[J,K,N,L]$ un parallélogramme galoisien. La relation d'ordre du lemme 2.3 dans l'ensemble des sous-parallélogrammes galoisiens (resp. des parallélogrammes galoisiens quotients) de $[J,K,N,L]$ s'écrit*

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

$$\Big(\textit{ resp.}$$

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

Démonstration. (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 2.3

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

(2) *Parallélogrammes quotients.* D'après la proposition 5.5, 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 6.7 qui suit généralise en degré quelconque le théorème principal de la théorie de Galois finie en dimension 2 (Th.4.2. de [**28**]). En se limitant à des sous-groupes fermés, il rend bijectives les injections Φ et les surjections Ψ de la proposition algébrique 5.2. De plus, en se limitant à des parallélogrammes plats, il redonne exactement la double bijection du théorème de Krull revisité. Ainsi, le théorème 6.7 suivant généralise en dimension 2 le théorème de Krull, tout comme le théorème 4.2. de [**28**] généralisait le théorème de Galois classique pour des extensions finies.

Théorème 6.7. *Soit $[J,K,N,L]$ un parallélogramme galoisien de degré quelconque, de groupe de Galois $Gal[J,K,N,L]$ (Déf. 2.5). 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 6.6. 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 :*

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

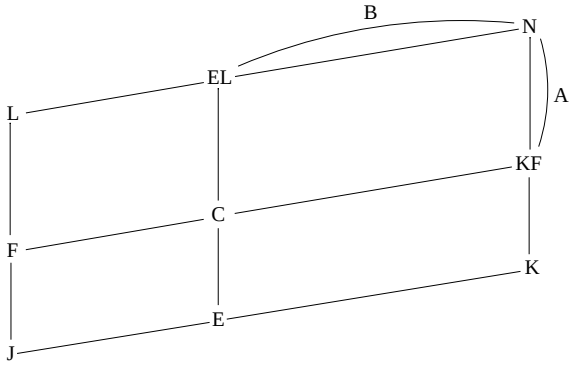

FIG. 11. *Sous-bigroupe associé à un parallélogramme quotient*

(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

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

Démonstration. On reprend les notations Φ et Ψ des applications de la proposition 5.2 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 Ψ_s du (1-2) de la proposition 5.2. 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

$$(A,B) \leq_c Gal[J,K,N,L] \quad \Rightarrow \quad \left\{ \begin{array}{l} A \leq_c Gal(N/K) \\ B \leq_c Gal(N/L) \end{array} \right.$$

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 6.6. Pour $\widetilde{\Psi}_s$, considérons deux sous-bigroupes profinis de $Gal[J,K,N,L]$

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

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 6.6, à $[M',E',N,F'] \leq [M,E,N,F]$.
(2) (2-0) Ce n'est que le (2-0) de la proposition 5.2 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 Ψ_q du (2-2) de la proposition 5.2. 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 $A'_{|_L} = Gal(L/L^{(A_{|L})})$ $\Big($ resp. $B'_{|_K} = Gal(K/K^{(B_{|K})})\Big)$. 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

6.6

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

et par définition

$$\Leftrightarrow \begin{cases} Gal(N/KF') \leq_c Gal(N/KF) \\ Gal(N/E'L) \leq_c Gal(N/EL) \end{cases} \Leftrightarrow \widetilde{\Phi}_q([J,E',C',F']) \leq_c \widetilde{\Phi}_q([J,E,C,F])\,.$$

Pour $\widetilde{\Psi}_q$, considérons deux sous-bigroupes profinis normaux de $Gal[J,K,N,L]$

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

Comme le composé $\widetilde{\Phi}_q \circ \widetilde{\Psi}_q$ est l'identité, on a d'après l'équivalence obtenue précedemment 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 du (2-4) de la proposition 5.2 sont topologiques. □

Chapitre 2

EXTENSIONS GALTOURABLES

Il s'agit ici d'introduire une notion nouvelle, celle d'extension galtourable, qui généralise celle d'extension galoisienne. Cette notion est la clef de notre démarche pour étudier les tours de corps (chapitre 3 et suivants).

On expose dans ce chapitre les premières propriétés des extensions galtourables. Nous examinons plus particulièrement les propriétés des extensions galoisiennes qui se généralisent aux extensions galtourables.

1. Définitions, notations, exemples

Formulons tout d'abord un certain nombre de définitions.

A l'instar de la notation de la théorie des groupes désignant les sous-groupes, nous remplaçons l'inclusion $\subseteq$ par un $\leq$ pour exprimer qu'il y a conservation de la structure de corps :

$$\forall E \text{ corps}, \quad F \leq E \quad \overset{\text{déf.}}{\Longleftrightarrow} \quad (F \text{ sous-corps de } E). \tag{1-0}$$

Définition & Convention 1.1. Soit L/K une extension quelconque.

(1) On appelle "tour (de corps) de L/K" une suite finie[1] croissante $\{F_i\}_{0\leq i\leq m}$ de corps intermédiaires de L/K dans laquelle $F_0 = K$ et $F_m = L$.
Nous notons une telle tour

$$(F) \qquad K = F_0 \leq F_1 \leq \ldots \leq F_i \leq F_{i+1} \leq \ldots \leq F_m = L\,.$$

Nous appelons
- "marche de la tour (F)" : toute extension $F_{i+1}/F_i \quad (i = 0, \ldots, m-1)$;
- "hauteur de la tour (F)" : l'entier m.

Nous disons que la tour (F) est "triviale" si et seulement si elle est de hauteur nulle : $m = 0$. Lorsque

$$\forall i \in \{0, \ldots, m-1\} \quad F_{i+1} \neq F_i$$

la tour

$$(F_<) := (F) \qquad K = F_0 < F_1 < \ldots < F_i < F_{i+1} < \ldots < F_m = L\,.$$

est dite "stricte". En particulier, la tour triviale est stricte.
Nous convenons que pour $m = 0$ la tour $(F_<)$ ci-dessus se réduit à

$$(F_<) \qquad K = F_0 = L\,.$$

[1] C'est le point de vue de cette thèse (à l'instar de la théorie des groupes), bien que des auteurs récents appellent "tour de corps" une suite infinie [**43**].

(2) Lorsque L/K est algébrique, nous appelons "tour galoisienne" de L/K toute tour

$$(T) \qquad K = T_0 \leq T_1 \leq \ldots \leq T_i \leq T_{i+1} \leq \ldots \leq T_m = L$$

dont toutes les marches $T_{i+1}/T_i \quad (i = 0, \ldots, m-1)$ sont des extensions galoisiennes.

(3) Deux tours de L/K

$$(F) \quad K = F_0 \leq F_1 \leq \ldots \leq F_i \leq \ldots \leq F_m = L$$

$$(E) \quad K = E_0 \leq E_1 \leq \ldots \leq E_j \leq \ldots \leq E_n = L$$

sont égales si et seulement si les deux suites $\{F_i\}_{0 \leq i \leq m}$ et $\{E_j\}_{0 \leq j \leq n}$ le sont ; autrement dit lorsque $m = n$ et

$$\forall i \in \{0, \ldots, m\} \qquad F_i = E_i \, .$$

Remarques 1.2. Les notations sont celles de la définition & convention 1.1.
(1) Pour une tour (F) triviale, on a nécessairement $L = K$. Mais on peut avoir $L = K$ et (F) non triviale, i.e. de hauteur non nulle : $m \neq 0$ (répétition de corps).

(2) Notons que la tour triviale est la seule tour stricte de L/K lorsque $L = K$, et qu'elle est toujours galoisienne.

(3) Il ne suffit pas d'avoir

$$\{E_0, \ldots, E_n\} = \{F_0, \ldots, F_m\}$$

pour que les tours (F) et (E) soient égales.

Fait 1.3. *La hauteur d'une tour stricte d'une extension finie L/K est au plus égale au nombre de diviseurs premiers, comptés avec leur multiplicité, du degré de L/K.*

Démonstration. Cela découle directement de la transitivité des degrés. □

De même que les extensions algébriques (même séparables) ne sont pas nécessairement galoisiennes, elles n'admettent pas nécessairement de tour galoisienne (cf. exemples 1.10), ce qui justifie la définition suivante.

Définition 1.4. Nous disons qu'une extension L/K est "galtourable" si et seulement si elle admet une tour galoisienne au sens de la définition & convention 1.1.(2).

Scholies. (1) Par la transitivité des notions d'algébricité et de séparabilité, une extension galtourable est toujours algébrique et séparable.

(2) Une extension galoisienne est évidemment galtourable. Mais une extension galtourable n'est pas nécessairement galoisienne vu la non transitivité de la normalité. La notion d'extension galtourable généralise donc celle d'extension galoisienne.

(3) Dans [**6**] est introduite la notion d' "extension radicale répétée". Il s'agit des extensions admettant une tour de corps dont chaque marche est une extension radicale. Nous dirions quant à nous que ce sont des extensions "radtourables".

Les tours galoisiennes introduites dans la définition & convention 1.1.(2) se généralisent en des tours dont les marches ne sont que galtourables.

Définition 1.5. Soit L/K une extension algébrique. Nous appelons "tour galtourable de L/K" toute tour

$$(F) \qquad K = F_0 \leq F_1 \leq \ \ldots \ \leq F_i \leq F_{i+1} \leq \ \ldots \ \leq F_m = L$$

dont toutes les marches $F_{i+1}/F_i \quad (i = 0, \ldots, m-1)$ sont des extensions galtourables.

Pour une extension donnée, l'existence d'une telle tour galtourable n'est pas automatique. Elle est discutée dans le corollaire 1.11 du chapitre 3.

Définition 1.6. (1) Nous appelons "extension simple" toute extension L/K non triviale n'admettant aucun corps intermédiaire propre :

$$\begin{array}{rcl} (L/K \text{ simple}) & \overset{\text{déf.}}{\Longleftrightarrow} & (L \neq K, \quad \forall F \quad K \leq F \leq L \ \Rightarrow \ (F = K \text{ ou } F = L)\ ) \\ & \Longleftrightarrow & (L \neq K, \quad \forall F \quad K \leq F < L \ \Rightarrow \ F = K)\,. \end{array}$$

(2) Nous appelons "extension galsimple" toute extension L/K non triviale n'admettant aucune extension quotient galoisienne propre :

$$\begin{array}{rcl} (L/K \text{ galsimple}) & \overset{\text{déf.}}{\Longleftrightarrow} & \left(\begin{array}{c} L \neq K, \quad \forall F \quad K \leq F \leq L \\ (F/K \text{ galoisienne}) \ \Rightarrow \ (F = K \text{ ou } F = L) \end{array} \right) \\ & \Longleftrightarrow & \left(\begin{array}{c} L \neq K, \quad \forall F \quad K \leq F < L \\ (F/K \text{ galoisienne}) \ \Rightarrow \ F = K \end{array} \right). \end{array}$$

Remarque 1.7. Dans la définition ci-dessus de la galsimplicité, aucune hypothèse n'est faite sur la sous-extension L/F : elle peut être galoisienne ou ne pas l'être.

Proposition 1.8. *(1) Toute extension simple est galsimple.*

(2) Une extension galsimple est galtourable si et seulement si elle est galoisienne.

Démonstration. Le (1) est clair. Prouvons le sens direct du (2). Soit L/K une extension galsimple galtourable. Par la définition 1.4, elle admet une tour galoisienne (définition & convention 1.1.(2))

$$(T) \qquad K = T_0 \leq T_1 \leq \ \ldots \ \leq T_i \leq T_{i+1} \leq \ \ldots \ \leq T_m = L \, .$$

Comme L/K est galsimple (Déf. 1.6.(2)), on tire de $K \leq T_1 \leq L$ l'implication

$$(T_1/K \text{ galoisienne}) \quad \Rightarrow \quad (T_1 = K \text{ ou } T_1 = L) \, .$$

Si $T_1 = L$, $(T_1/K) = (L/K)$ est bien galoisienne. Si $T_1 \neq L$, on a la tour

$$(T) \qquad K = T_0 = T_1 \leq T_2 \leq \ \ldots \ \leq T_i \leq T_{i+1} \leq \ \ldots \ \leq T_m = L \, .$$

En itérant le procédé sans avoir déjà conclu, on obtient

$$(T) \qquad K = T_0 = T_1 = \ \ldots \ = T_{m-2} \leq T_{m-1} \leq T_m = L \, .$$

Donc, ou bien $T_{m-1} = K$, ou bien $T_{m-1} = L$, et dans les deux cas L/K est galoisienne. □

Nous étudierons les extensions simples ou galsimples au chapitre 5. La galsimplicité nous permettra d'énoncer le "Théorème M" (Chap. 6) qui est le point crucial de la dissociation de toutes les extensions finies.

Afin d'alléger le texte qui suit, convenons de quelques notations. Elles concernent les définitions 1.1, 1.4, 1.5 et 1.6 précédentes, et ont été rassemblées ici pour y référer facilement.

Notations 1.9. (1) (Extension stricte L/K) $\quad \Leftrightarrow \quad K < L \quad \Leftrightarrow \quad L > K \, .$

(2) (Extension galoisienne L/K) $\quad \Leftrightarrow \quad L \nearrow K \quad \Leftrightarrow \quad K \trianglelefteq L \quad \Leftrightarrow \quad L \trianglerighteq K \, .$

(3) (Extension stricte galoisienne L/K) $\quad \Leftrightarrow \quad K \triangleleft L \quad \Leftrightarrow \quad L \triangleright K \, .$

(4) (Extension non galoisienne L/K) $\quad \Leftrightarrow \quad L \nwarrow\!\!\searrow K \, .$

(5) (Extension galtourable L/K) $\quad \Leftrightarrow \quad L \swarrow\!\!\nearrow K \quad \Leftrightarrow \quad K \leqslant L \quad \Leftrightarrow \quad L \geqslant K \, .$

(6) (Extension non galtourable L/K) $\quad \Leftrightarrow \quad L \nwarrow\!\!\searrow K \, .$

(7) (Extension galtourable non galoisienne L/K) $\quad \Leftrightarrow \quad L \swarrow\!\!\nearrow\!\!\nwarrow\!\!\searrow K \, .$

(8) (Extension simple L/K) $\quad \Leftrightarrow \quad L \not\phi K \, .$

(9) (Extension non simple L/K) $\quad\Leftrightarrow\quad L \not\backslash K$.

(10) (Extension galsimple L/K) $\quad\Leftrightarrow\quad L \not\nearrow K$.

(11) (Extension non galsimple L/K) $\quad\Leftrightarrow\quad L \nwarrow K$

(12) (Extension galsimple galoisienne L/K) $\quad\Leftrightarrow\quad L \not\nearrow\nearrow K$.

(13) (Extension galsimple non galoisienne L/K)

$$\Leftrightarrow\quad L \not\nearrow\nwarrow K \quad\Leftrightarrow\quad K \blacktriangleleft L \quad\Leftrightarrow\quad L \blacktriangleright K\,.$$

Les notations précédentes ne sont évidemment pas redondantes ; en voici quelques exemples.

Exemples 1.10. Pour un réel $r \in \mathbb{R}_+$ et un entier $n \in \mathbb{N}$, on note, $\sqrt[n]{r}$ la racine n-ième réelle de r : $\sqrt[n]{r} \in \mathbb{R}$.

(i) Il existe des extensions séparables non galtourables :

$$\mathbb{Q}(\sqrt[6]{2}) \nwarrow\!\!\searrow \mathbb{Q}\,.$$

(ii) Il existe des extensions galtourables non galoisiennes :

$$\mathbb{Q}(\sqrt[4]{2}) \swarrow\!\!\nwarrow \mathbb{Q}\,.$$

(iii)

- Toute extension cyclique de degré premier est simple.
- Quel que soit l'entier $n \geq 3$, l'extension $\mathbb{Q}(\theta)/\mathbb{Q}$ où

$$\theta^n - \theta - 1 = 0$$

est simple, mais non galoisienne :

$$\mathbb{Q}(\theta) \not\nwarrow\!\!\searrow \mathbb{Q}\,.$$

(iv) Il existe des extensions galsimples non simples non galoisiennes :

$$\mathbb{Q}(\sqrt[9]{2}) \not\nearrow\!\!\not\backslash\!\!\nwarrow\!\!\searrow \mathbb{Q}\,.$$

(v) Il existe des extensions galsimples non simples galoisiennes : soit L le corps de décomposition dans $\mathbb{C}$ du polynôme

$$X^5 + 20X + 16 \qquad (\text{resp. } \sum_{n=0}^{8} \frac{X^n}{n!}\ ).$$

On a :

$$Gal(L/\mathbb{Q}) \xrightarrow{\sim} A_5 \qquad (\text{resp. } Gal(L/\mathbb{Q}) \xrightarrow{\sim} A_8\ )$$
$$[L : \mathbb{Q}] = 60 \qquad (\text{resp. } [L : \mathbb{Q}] = 20160\ )\ ,$$

et $L/\mathbb{Q}$ est une extension galsimple non simple galoisienne :

$$L \nearrow\!\!\!\diagdown\!\!\!\nearrow \mathbb{Q} .$$

Démonstration. (i) On a $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$ par le critère d'Eisenstein. Supposons que l'extension $\mathbb{Q}(\sqrt[6]{2})/\mathbb{Q}$ soit galtourable, i.e. par définition qu'il existe une tour galoisienne

$$(T) \qquad \mathbb{Q} = T_0 \trianglelefteq \ldots \trianglelefteq T_i \trianglelefteq \ldots \trianglelefteq T_m = \mathbb{Q}(\sqrt[6]{2}) .$$

Prouvons qu'alors $\mathbb{Q}(\sqrt[6]{2})/\mathbb{Q}$ admet nécessairement une tour galoisienne stricte à deux marches (ceci est un cas particulier d'un résultat général démontré au corollaire 2.6 du chapitre 3). Posons :

$$j := min\{i \in \{0, \ldots, m\} \mid T_i \neq \mathbb{Q}\} , \quad k := max\{i \in \{0, \ldots, m\} \mid T_i \neq T_m\} .$$

De $j > k$ suivrait

$$\mathbb{Q}(\sqrt[6]{2}) = T_{k+1} \nearrow T_k = \mathbb{Q} \quad : \text{ absurde.}$$

Donc nécessairement $j \leq k$ et

$$(T) \quad \mathbb{Q} = T_0 = \ldots = T_{j-1} \lhd T_j \trianglelefteq \ldots \trianglelefteq T_k \lhd T_{k+1} = \ldots = T_m = \mathbb{Q}(\sqrt[6]{2}) .$$

On en déduit la tour à trois marches

$$\mathbb{Q} \lhd T_j \leq T_k \lhd \mathbb{Q}(\sqrt[6]{2})$$

qui ne peut pas être stricte, en vertu du Fait 1.3. C'est donc que $T_j = T_k$ et, dans notre hypothèse, on a ainsi prouvé l'existence d'une tour galoisienne stricte à deux marches

$$\mathbb{Q} = F_0 \lhd F_1 \lhd F_2 = \mathbb{Q}(\sqrt[6]{2}) .$$

Par ailleurs, on a la

Proposition. *Soient $n \in \mathbb{N}$ et $a \in \mathbb{Q}_+$ un rationnel positif. On suppose que pour tout diviseur d de n, $a \notin \mathbb{Q}^d$. Alors, pour tout corps intermédiaire F entre $\mathbb{Q}$ et $L := \mathbb{Q}(\sqrt[n]{a})$: $\mathbb{Q} \leq F \leq L$, il existe un entier d divisant n : $d \mid n$, tel que $F = \mathbb{Q}(\sqrt[d]{a})$.*

Démonstration. Conséquence directe du Théorème 2.1 de [**1**] ou du Théorème 2.2 de [**40**]. □

Avec ce qui précède, il résulte de la proposition ci-dessus que les seules tours strictes à deux marches de $\mathbb{Q}(\sqrt[6]{2})/\mathbb{Q}$ sont

$$\mathbb{Q} = F_0 \lhd F_1 = \mathbb{Q}(\sqrt{2}) < F_2 = \mathbb{Q}(\sqrt[6]{2})$$

et

$$\mathbb{Q} = F_0 < F_1 = \mathbb{Q}(\sqrt[3]{2}) \lhd F_2 = \mathbb{Q}(\sqrt[6]{2}) .$$

Or ni l'une ni l'autre n'est galoisienne, d'où la contradiction.

(ii) Il suffit de considérer la tour galoisienne

$$\mathbb{Q} \lhd \mathbb{Q}(\sqrt{2}) \lhd \mathbb{Q}(\sqrt[4]{2}) .$$

(iii) La première assertion est claire ; quant à la seconde, elle sera démontrée au chapitre 5.

(iv) Posons $L := \mathbb{Q}(\sqrt[9]{2})$. Clairement, l'extension $L/\mathbb{Q}$ est non simple et non galoisienne. Si elle n'était pas galsimple, il existerait un corps intermédiaire N tel que $\mathbb{Q} \lhd N < L$. Or, en vertu de la proposition de la démonstration du (i) ci-dessus, on a nécessairement $N = \mathbb{Q}(\sqrt[3]{2})$ qui n'est pas galoisien sur $\mathbb{Q}$.

(v) Pour $X^5 + 20X + 16$, on vérifie que $Gal(L/\mathbb{Q}) \xrightarrow{\sim} A_5$ par PARI [**10**]. Pour $\sum_{n=0}^{8} \frac{X^n}{n!}$, on a $Gal(L/\mathbb{Q}) \xrightarrow{\sim} A_8$ d'après un résultat de Schur ([**35**] ou [**11**]). Les sous-groupes de Sylow de A_5 (resp. A_8) assurent que $L/\mathbb{Q}$ n'est pas simple. Mais $L \nearrow \mathbb{Q}$ est galsimple puisque A_5 (resp. A_8) est un groupe simple (c'est un phénomène général : cf. Chap. 4, Prop. 2.7). □

2. Théorie générale des extensions galtourables

On dispose d'une théorie générale des extensions galoisiennes finies ou infinies. Nous allons montrer qu'il existe aussi une théorie générale des extensions galtourables. Rappelons d'abord le bien connu "théorème de l'extension galoisienne translatée" [**23**, p.266,Th.1.12] (dit "natural irrationalities" dans [**32**]).

Théorème 2.1. *Soient K/J et L/J deux extensions algébriques. Sous la seule hypothèse que K et L soient contenus dans un même corps, avoir L/J galoisienne implique que KL/K est galoisienne :*

$$(L \nearrow J) \qquad \Longrightarrow \qquad (KL \nearrow K) .$$

Corollaire 2.2. *La translatée d'une extension galoisienne par un corps donné est toujours une extension galoisienne.*
Précisément, soit L/J une extension galoisienne. Pour tout corps C contenu dans une clôture algébrique de J contenant L, l'extension CL/CJ est encore une extension galoisienne. Autrement dit, on a l'implication

$$(L \nearrow J) \qquad \Longrightarrow \qquad (CL \nearrow CJ) .$$

Démonstration. Il suffit d'appliquer le théorème 2.1 en translatant l'extension galoisienne L/J par CJ/J. □

Ces énoncés se généralisent aux extensions galtourables.

Théorème 2.3. *Soient K/J et L/J deux extensions algébriques. Sous la seule condition que K et L soient contenus dans un même corps, on a l'implication*

$$(L/J \text{ galtourable }) \qquad \Longrightarrow \qquad (KL/K \text{ galtourable }) .$$

Démonstration. Soit (F) une tour galoisienne de l'extension galtourable $L \nearrow J$:

$$(F) \qquad J = F_0 \trianglelefteq F_1 \trianglelefteq \ldots \trianglelefteq F_i \trianglelefteq F_{i+1} \trianglelefteq \ldots \trianglelefteq F_m = L .$$

Posons $E_i := KF_i \quad (i = 0, \ldots, m)$, et appliquons le théorème 2.1 en translatant chacune des marches galoisienne $F_{i+1} \nearrow F_i \quad (i = 0, \ldots, m-1)$ par l'extension algébrique E_i/F_i.

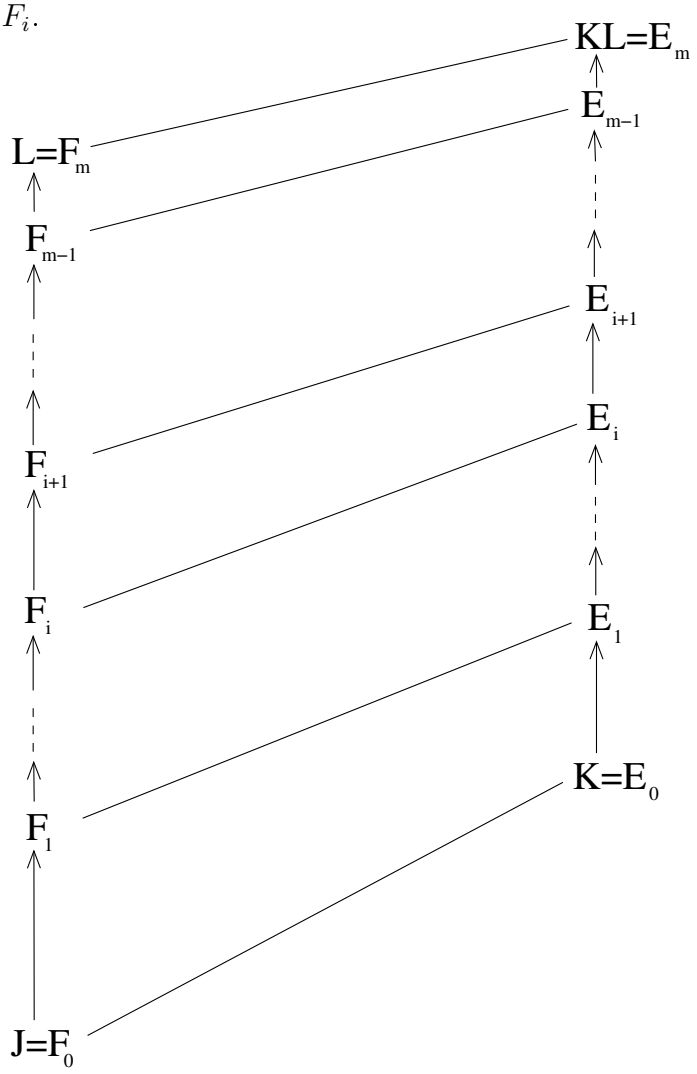

FIG. 12. *Translatée d'une tour galoisienne*

On en déduit que les extensions

$$E_i\, F_{i+1} = K\, F_{i+1} = E_{i+1} \,/\, E_i \qquad (i = 0, \ldots, m-1)$$

sont galoisiennes. On obtient donc la tour galoisienne

$$(E) \qquad K = KF_0 = E_0 \trianglelefteq \ldots \trianglelefteq E_i \trianglelefteq E_{i+1} \trianglelefteq \ldots \trianglelefteq E_m = KF_m = KL\,.$$

Or ceci n'exprime rien d'autre que la galtourabilité de KL/K. □

Enonçons maintenant trois corollaires au théorème 2.3.

Corollaire 2.4. *La translatée d'une extension galtourable par un corps donné est toujours une extension galtourable.*
Précisément, soit L/J une extension galtourable. Pour tout corps C contenu dans une clôture algébrique de J contenant L, l'extension CL/CJ est encore galtourable. Autrement dit on a l'implication

$$(L \swarrow J) \quad \Longrightarrow \quad (CL \swarrow CJ)\,.$$

Démonstration. On applique le théorème 2.3 avec $K := CJ$. □

Fait 2.5. *La réciproque du théorème 2.3 est fausse.*

Scholie. Il en est de même de la réciproque du théorème de l'extension galoisienne translatée 2.1.

Démonstration. Reprenons l'extension $L := \mathbb{Q}(\sqrt[6]{2})/\mathbb{Q}$ de l'exemple 1.10.(i) et translatons la par l'extension $K := \mathbb{Q}(j)/\mathbb{Q}$ où $j := e^{2i\pi/3}$. Comme K contient les racines $6^{\text{èmes}}$ de l'unité, l'extension $KL = K(\sqrt[6]{2})/K$ est kummérienne, donc galoisienne et a fortiori galtourable. Tandis que l'on a prouvé que l'extension $L := \mathbb{Q}(\sqrt[6]{2})/\mathbb{Q}$ n'est même pas galtourable.

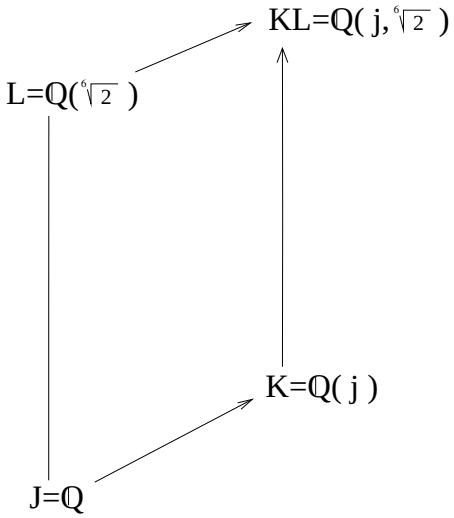

FIG. 13. *Descente non galtourable* □

Corollaire 2.6. *La translatée d'une tour galtourable par une extension algébrique est une tour galtourable.*
Précisément, soit L/J une extension admettant une tour galtourable (cf. Déf. 1.5)

$$(F) \qquad J = F_0 \leqslant \ldots \leqslant F_i \leqslant F_{i+1} \leqslant \ldots \leqslant F_m = L\,.$$

Alors, pour toute extension algébrique K/J telle que K et L soient contenus dans un même corps, on a la tour galtourable

$$(E) \qquad K = E_0 \leqslant \ldots \leqslant E_i \leqslant E_{i+1} \leqslant \ldots \leqslant E_m = KL$$

où l'on a posé $E_i := KF_i \quad (i = 0, \ldots, m)$.

Démonstration. Il suffit d'appliquer le théorème 2.3 aux extensions galtourables $F_{i+1}\nwarrow F_i$ en les translatant par les extensions algébriques E_i/F_i, pour $i \in \{0, \ldots, m-1\}$. □

Quand on empile deux extensions galoisiennes, on obtient une extension galtourable non nécessairement galoisienne en général (cf. exemple 1.10.(ii)). Les extensions galtourables n'ont pas ce défaut : quand on empile deux extensions galtourables, on obtient toujours une extension galtourable. Précisément :

Fait 2.7. *Pour toute tour $K \leq L \leq M$, avoir L/K galtourable et M/L galtourable implique que M/K est galtourable. Autrement dit on a l'implication*

$$(\, L\nwarrow K\,,\ M\nwarrow L\,) \quad \Longrightarrow \quad (M\nwarrow K)\,.$$

Scholie. Nous avons déjà prouvé que l'implication inverse est fausse en général : cf. 2.10.

Démonstration. Il suffit d'utiliser que la juxtaposition de tours galoisiennes est encore une tour galoisienne. Précisément, si

$$(F) \qquad F_0 \trianglelefteq F_1 \trianglelefteq \ldots \trianglelefteq F_i \trianglelefteq \ldots \trianglelefteq F_m$$

et

$$(E) \qquad F_m = E_0 \trianglelefteq E_1 \trianglelefteq \ldots \trianglelefteq E_j \trianglelefteq \ldots \trianglelefteq E_n$$

sont deux tours galoisiennes, la tour

$$\begin{aligned}(T) \quad F_0 =: T_0 \trianglelefteq \ldots \trianglelefteq T_i := F_i \trianglelefteq \ldots \trianglelefteq T_m := F_m = E_0 \trianglelefteq T_{m+1} := E_1 \trianglelefteq \ldots \\ \cdots \trianglelefteq T_{m+j} := E_j \trianglelefteq \ldots \trianglelefteq T_{m+n} = E_n\end{aligned}$$

est évidemment galoisienne. □

Corollaire 2.8. *Tout compositum d'extensions galtourables est galtourable. Précisément : quelles que soient les extensions galtourables K/J et L/J dont les sommets sont contenus dans un même corps, l'extension compositum KL/J est galtourable. Autrement dit, on a l'implication*

$$(\, K\nwarrow J\,,\ L\nwarrow J\,) \quad \Longrightarrow \quad (\, KL\nwarrow J\,)\,.$$

Démonstration. Le théorème 2.3 assure que $KL \nearrow K$. Comme de plus $K \nearrow J$, le Fait 2.7 précédent entraine que $KL \nearrow J$. □

Proposition 2.9. *Toute sous-extension d'une extension galtourable est galtourable. Précisément, soit $L \nearrow K$ une extension galtourable. Pour tout corps intermédiaire M, $K \leq M \leq L$, la sous extension L/M est galtourable.*

Démonstration. Il suffit d'appliquer le théorème 2.3 en translatant l'extension galtourable $L \nearrow K$ par l'extension algébrique M/K. □

La proposition précédente généralise une propriété analogue des extensions galoisiennes. Le fait suivant établit que la question "duale", c'est à dire pour les extensions quotients, trouve la même réponse dans le cas galtourable que dans le cas galoisien.

Fait 2.10. *En général, une extension quotient d'une extension galtourable n'est pas galtourable.*

Démonstration. Considérons la situation

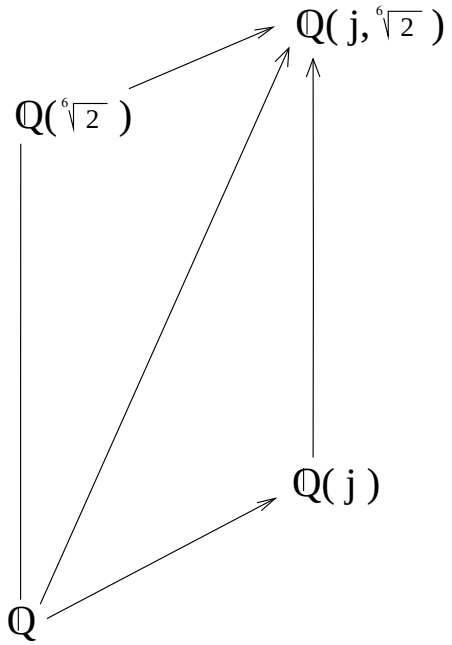

FIG. 14. *Extension quotient non galtourable*

L'extension $\mathbb{Q}(j, \sqrt[6]{2})/\mathbb{Q}$ est galoisienne (puisque son corps sommet est le corps de décomposition de $X^6 - 2$ sur $\mathbb{Q}$). Mais on a déjà vu que l'extension quotient $\mathbb{Q}(\sqrt[6]{2})/\mathbb{Q}$ n'est pas galtourable (cf. exemple 1.10.(i)). □

Les différentes propriétés précédentes constituent le début d'une théorie de la galtourabilité, similaire à la théorie de Galois générale. On peut numériquement décider si une extension donnée est galtourable ou non, de même que l'on peut décider si elle est galoisienne ou pas. Cependant il paraît illusoire de chercher une caractérisation "universelle" des extensions galtourables, ou même seulement des extensions galtourables finies. Rappelons qu'une telle caractérisation n'existe déjà pas pour la classe, plus restreinte, des extensions galoisiennes.

Un important problème de théorie de Galois est de conserver le caractère galoisien d'une extension en la faisant glisser sur un sous-corps de son corps de base. Ceci constitue le délicat

"Problème de la descente galoisienne".
Soient $N \nearrow K$ une extension galoisienne et K/J une extension algébrique. Existe-t-il un sous corps L de N : $L \leq N$, tel que les trois propriétés suivantes soient vérifiées :

(D_0) L/J est galoisienne : $L \nearrow J$;
(D_1) L'intersection de K et de L est égale à J : $K \cap L = J$;
(D_2) Le compositum de K et de L est égal à N : $KL = N$.

Ce problème, maintes fois abordé dans la littérature ([**30**], [**31**], [**29**], [**19**], [**9**], ...) se généralise en le problème suivant sur lequel tout reste à découvrir.

"Problème de la descente galtourable".
Soient $N \swarrow K$ une extension galtourable et K/J une extension algébrique. Existe-t-il un sous corps L de N tel que

(D_0) L/J est galtourable : $L \swarrow J$;
(D_1) $K \cap L = J$;
(D_2) $KL = N$.

Pour le problème de la descente galoisienne, Massy a introduit la notion de parallélogramme galoisien [**28**], essentiellement en degrés finis. Une généralisation en degrés infinis figure dans [**4**] (confer Chap. 1). Dans le cas galtourable introduisons la

Définition 2.11. Nous appellons "quadrilatère galtourable" tout quadrilatère corporel (J, K, N, L) (cf. Chap. 1, Déf. 1.1) dans lequel les quatre extensions sont galtourables :

$$K \swarrow J\ ,\ N \swarrow K\ ,\ N \swarrow L\ ,\ L \swarrow J\ .$$

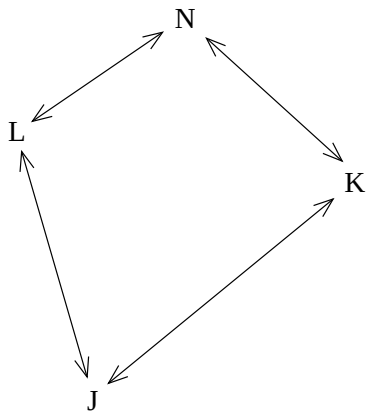

FIG. 15. *Quadrilatère galtourable*

Remarque 2.12. D'après le théorème 2.3, la galtourabilité de L/J (resp. K/J) implique celle de N/K (resp. N/L) :

$$(L \nearrow J) \Rightarrow (N \nearrow K) \quad \big(\text{ resp. } (K \nearrow J) \Rightarrow (N \nearrow L) \big) .$$

Proposition 2.13. *Soient (J, K, N, L) un quadrilatère galtourable, et F un corps intermédiaire entre J et L, $J \leq F \leq L$.*
(1) Si $KF \cap L = F$, on a le sous-quadrilatère galtourable (F, KF, N, L).
(2) Si F/J est galtourable, on a le quadrilatère quotient galtourable (J, K, KF, F).

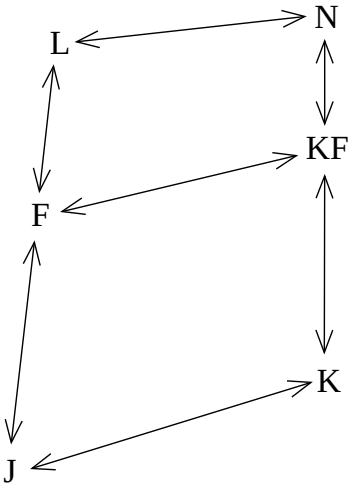

FIG. 16. *Sous galtourabilité & galtourabilité quotient*

Démonstration. (1) D'après le théorème 2.3,

$$(K \nearrow J) \quad \Rightarrow \quad (KF \nearrow F) \quad \Rightarrow \quad (N \nearrow L) .$$

D'après la proposition 2.9 et le théorème 2.3,

$$(L \nearrow J) \quad \Rightarrow \quad (L \nearrow F) \quad \Rightarrow \quad (N \nearrow KF)\,.$$

D'où le quadrilatère galtourable annoncé puisque $F = KF \cap L$ par hypothèse.

(2) Un nouvelle fois par le théorème 2.3

$$(F \nearrow J) \quad \Rightarrow \quad (KF \nearrow K)\,.$$

D'où la conclusion par la démonstration précédente du (1). □

Le lecteur qui se sera référé au théorème 1.3 de [**28**] et au théorème 4.2 du chapitre 1 aura noté que la proposition précédente est bien moins consistante que ceux-ci. En effet, plusieurs questions demeurent irrésolues. En voici un résumé.

Questions 2.14. On se donne un quadrilatère galtourable (J, K, N, L). Dans quels cas peut-on répondre par l'affirmative aux questions suivantes :
(1) Si F est un corps intermédiaire entre J et L, $J \leq F \leq L$,

$$KF \cap L = F \quad ?$$

(2) Si E est un corps intermédiaire entre K et N, $K \leq E \leq N$,

(2-1) $E/(E \cap L)$ est-elle galtourable : $E \nearrow (E \cap L)$?
(2-2) Pour E/K galtourable
(2-2-1) $K(E \cap L) = E$?
(2-2-2) $(E \cap L) \nearrow J$?

Lorsque $(J, K, N, L) = [J, K, N, L]$ est un parallélogramme galoisien, toutes les réponses sont affirmatives en vertu du corollaire 4.3 du chapitre 1.

3. Extensions galtourables définies par un polynôme

La galtourabilité d'une extension définie par une racine d'un polynôme irréductible dépend-elle de cette racine ? Nous allons prouver qu'il n'en est rien, bien qu'à deux racines différentes correspondent en général deux extensions différentes (contrairement au cas galoisien). La proposition suivante permet en particulier d'utiliser le logiciel PARI sur les extensions de corps définies par un polynôme pour prouver la galtourabilité d'une extension sans avoir d'état d'âme sur la racine considérée.

Proposition 3.1. *Soient J un corps quelconque et $\tilde{J}$ une clôture algébrique fixée de J. Soit $P(X)$ un polynôme séparable irréductible de $J[X]$. Quelles que soient les racines t_1 et t_2 de $P(X)$ dans $\tilde{J}$:*

$$P(t_1) = P(t_2) = 0\,,$$

l'extension $J(t_1)/J$ est galtourable si et seulement si l'extension $J(t_2)/J$ est galtourable :

$$(J(t_1)\nearrow\!\!\swarrow J) \quad \Longleftrightarrow \quad (J(t_2)\nearrow\!\!\swarrow J)\,.$$

Scholie. La séparabilité de $P(X)$ est exigée par la galtourabilité des extensions.

Démonstration. Supposons l'extension $L^1 := J(t_1)/J$ galtourable. Soit donc une tour galoisienne (T^1) de $L^1\nearrow\!\!\swarrow J$

$$(T^1) \qquad J = T_0^1 \trianglelefteq \ldots \trianglelefteq T_{i-1}^1 \trianglelefteq T_i^1 \trianglelefteq \ldots \trianglelefteq T_m^1 = L^1\,.$$

Montrons que (T^1) détermine canoniquement une tour galoisienne (T^2) de $L^2 := J(t_2)/J$. L'extension L^1/J est finie (de degré celui de $P(X)$) ; chacune des marches galoisiennes $T_i^1/T_{i-1}^1 \quad (i = 1, \ldots, m)$ est ainsi séparable de degré fini. Donc par le théorème de l'élément primitif

$$\forall i \in \{1, \ldots, m\} \quad \exists \theta_i \in T_i^1 \qquad T_i^1 = T_{i-1}^1(\theta_i)\,.$$

On sait que les corps $J(t_1)$ et $J(t_2)$ sont conjugués, i.e. il existe un J-isomorphisme Φ induit par $\Phi(t_1) = t_2$:

$$\begin{array}{rccc} \Phi\ : & L^1 & \xrightarrow{\sim} & L^2 \\ & t_1 & \longmapsto & t_2 \end{array}\,.$$

Posons alors

$$v_i := \Phi(\theta_i) \qquad (i = 1, \ldots, m)$$

et

$$T_0^2 := J\,, \quad T_i^2 := T_{i-1}^2(v_i)\,.$$

Il est clair par récurrence que

$$T_i^2 = \Phi(T_i^1) \qquad (i = 0, \ldots, m)$$

car

$$\begin{array}{ccccccc} \Phi(T_0^1) & = & \Phi(J) & = & J & & \\ \vdots & & \vdots & & \vdots & & \\ \Phi(T_i^1) & = & \Phi(T_{i-1}^1(\theta_i)) & = & \Phi(T_{i-1}^1)(\Phi(\theta_i)) & & \\ & & & = & T_{i-1}^2(v_i) & = T_i^2\,. & \end{array}$$

En prenant l'image de (T^1) par Φ, on obtient donc canoniquement la tour

$$\begin{array}{ccccccccccccc} (T^2) & \Phi(J) & = & \Phi(T_0^1) & \leq \cdots \leq & \Phi(T_{i-1}^1) & \leq & \Phi(T_i^1) & \leq \cdots \leq & \Phi(T_m^1) & = & \Phi(L^1) \\ & \| & & \| & & \| & & \| & & \| & & \| \\ & J & = & T_0^2 & \leq \cdots \leq & T_{i-1}^2 & \leq & T_i^2 & \leq \cdots \leq & T_m^2 & = & L^2 \end{array}$$

Il reste à prouver que la tour (T^2) est bien galoisienne. Posons :

$$P_i(X) := Irr(\theta_i, T_{i-1}^1, X) \quad (i = 1, \ldots, m)$$

et $\mathcal{R}_i := \{$ racines de $P_i(X)$ dans $\tilde{J}\}$. Puisque, par hypothèse, l'extension T_i^1/T_{i-1}^1 est galoisienne, on a

$$\mathcal{R}_i \subseteq T_i^1 \quad (i = 1, \ldots, m) .$$

Donc directement

$$\Phi(\mathcal{R}_i) \subseteq \Phi(T_i^1) = T_i^2 .$$

Or $\Phi(\mathcal{R}_i) = \{$ racines de $P_i^\Phi(X)$ dans $\tilde{J}\}$ car $P_i(X)$ se décompose en facteurs du premier degré dans T_i^1 :

$$P_i(X) = (X - z_{i\,1} = \theta_i) \ldots (X - z_{i\,d_i}) ,$$

et donc

$$P_i^\Phi(X) = (X - \Phi(\theta_i) = v_i) \ldots (X - \Phi(z_{i\,d_i})) .$$

On en déduit que T_i^2 est le corps de décomposition sur T_{i-1}^2 du polynôme $P_i^\Phi(X)$. En effet comme $\Phi(\mathcal{R}_i) \subseteq T_i^2$, on a trivialement

$$T_i^2 = T_i^2(\Phi(z_{i\,1}) = v_i, \ldots, \Phi(z_{i\,d_i})) ;$$

et puisque $T_i^2 = T_{i-1}^2(v_i)$,

$$T_i^2 = T_{i-1}^2(\Phi(z_{i\,1}) = v_i, \ldots, \Phi(z_{i\,d_i})) .$$

L'extension T_i^2/T_{i-1}^2 est donc normale, et par suite galoisienne. □

Chapitre 3

RAFFINEMENTS DE TOURS DE CORPS

Le chapitre précédent introduisait la notion de tour galoisienne jouant pour les corps un rôle analogue à celui des suites normales pour les groupes. Ce parallèle avec les groupes se poursuivra au chapitre 4 en un quasi-dictionnaire par des analogues, au départ inespérés, des célèbres théorèmes de Schreier et de Jordan-Hölder. Nous nous intéressons ici à la notion clef de ces futurs énoncés, celle de raffinement d'une tour (galoisienne) de corps qui nécessite, hélas, une mise au point technique assez lourde.

1. Définition d'un raffinement et d'un raffinement galoisien

Définition & Convention 1.1. Soient L/K une extension algébrique, et

$$(F) \qquad K = F_0 \leq F_1 \leq \cdots \leq F_i \leq F_{i+1} \leq \cdots \leq F_m = L$$

une tour de L/K (cf. définition & convention 1.1 du chapitre 2).
(1) Nous appelons "raffinement de (F)" toute tour

$$(E) \qquad K = E_0 \leq E_1 \leq \cdots \leq E_j \leq E_{j+1} \leq \cdots \leq E_n = L$$

de L/K vérifiant les deux conditions suivantes :

(RAF1) $m \leq n$
(RAF2) il existe une suite finie d'indices $0 \leq j_0 < j_1 < \cdots < j_m \leq n$

telle que

$$\forall i \in \{0, \ldots, m\} \quad F_i = E_{j_i} \, .$$

En particulier pour la tour triviale (F) (cf. Chap. 2, Déf. & Conv. 1.1), nous convenons que pour $m = 0$, la suite finie d'indices ci-dessus se réduit à

$$0 \leq j_0 \leq n \, .$$

(2) Nous appelons "raffinement propre de (F)" tout raffinement (E) de (F) qui vérifie la condition supplémentaire

$$\text{(RAF3)} \qquad \exists j \in \{1, \ldots, n-1\} \quad \forall i \in \{0, \ldots, m\} \quad E_j \neq F_i \, .$$

Scholie. Cette définition est un analogue exact, mutatis mutandis, de celle utilisée pour les suites normales de groupes qui figure clairement dans [**34**, p.120].

Remarques 1.2. (1) La condition (RAF1) est redondante : elle est impliquée par (RAF2), puisque l'on a clairement

$$\forall i \in \{0, \dots, m\} \quad i \leq j_i \, .$$

Cependant (RAF1) offre un moyen commode pour présélectionner les tours susceptibles d'être des raffinements.
(2) Le raffinement (E) de la définition & convention 1.1.(1) peut s'écrire

$$(E) \qquad K = E_0 \leq \cdots \leq E_{j_0} = F_0 = K \leq \cdots \leq E_{j_1} = F_1 \leq \cdots \leq E_{j_i} = F_i \leq \dots \\ \cdots \leq E_j \leq E_{j+1} \leq \cdots \leq E_{j_m} = F_m = L \leq \cdots \leq E_n = L \, .$$

(3) Toutes les répétitions de la tour (F) sont reproduites dans la tour (E). Il ne peut exister de raffinement supprimant des corps. Un raffinement qui ajoute un corps nouveau, distinct de tous ceux de la tour de départ (condition (RAF3)), est "propre".

La définition suivante précise la définition & convention générale 1.1 précédente, à l'instar de ce qui a été fait au chapitre 2 pour les tours strictes, galoisiennes, etc.

Définition 1.3. Soient L/K une extension algébrique, (F) une tour de L/K et (E) un raffinement de (F) (cf. Déf. & Conv. 1.1).
(1) Nous disons que (E) est un "raffinement strict" de (F) si et seulement si c'est une tour stricte (cf. Chap. 2, Déf. & Conv. 1.1.(1)).
(2) Nous disons que (E) est un "raffinement trivial" de (F) si et seulement si c'est un raffinement de (F) non propre, autrement dit qui vérifie comme condition supplémentaire la négation de (RAF3) dans la définition & convention 1.1.(2), i.e.

$$\text{(RAFT)} \qquad \forall j \in \{1, \dots, n-1\} \quad \exists i \in \{0, \dots, m\} \quad E_j = F_i \, .$$

(3) Nous appelons "raffinement identité" de (F), la tour (F) elle-même.
(4) Nous disons que (E) est un "raffinement galoisien" de (F) si et seulement si c'est un raffinement de (F) qui vérifie la condition supplémentaire

$$\text{(RAFG)} \quad \forall j \in \{1, \dots, n-1\} \quad \Big(\forall i \in \{0, \dots, m\} \quad E_j \neq F_i\Big) \Rightarrow \quad \begin{array}{c} E_{j-1} \trianglelefteq E_j \\ \Updownarrow \\ E_j \nearrow E_{j-1} \end{array} \, .$$

Scholie. Toutes ces notions sont évidemment cumulables : raffinement strict propre, raffinement galoisien strict, etc.

Remarques 1.4. (1) Une tour (F) non stricte (cf. Chap. 2, Déf. & Conv. 1.1) n'admet pas de raffinement strict.
(2) Le raffinement identité est un raffinement galoisien trivial.
(3) Un raffinement galoisien (E) d'une tour (F) n'est pas nécessairement une tour galoisienne : le raffinement identité d'une tour non galoisienne par exemple.

Fait 1.5. *(1) Tout raffinement trivial est galoisien.*
(2) Un raffinement qui est une tour galoisienne est un raffinement galoisien.

Démonstration. (1) Soient L/K une extension,

$$(F) \qquad K = F_0 \leq \cdots \leq F_i \leq \cdots \leq F_m = L$$

une tour de L/K, et

$$(E) \qquad K = E_0 \leq \cdots \leq E_j \leq \cdots \leq E_n = L$$

un raffinement trivial de (F). Dire que (E) est galoisien signifie que que dès qu'un corps E_j est distinct de tous les F_i, il est nécessairement galoisien sur E_{j-1} (condition (RAFG) de la définition 1.3). Mais la trivialité de (E) signifie que tous les E_j sont des F_i (condition (RAFT)). La condition (RAFG) est donc satisfaite puisqu'elle n'impose rien.
(2) Dire que la tour (E) est galoisienne revient à dire (cf. Chap. 2, Déf. & Conv. 1.1.(2)) que toutes les marches E_j/E_{j-1} $(j = 1, \ldots, n)$ sont galoisiennes. La condition (RAFG) est dès lors clairement vérifiée. □

Fait 1.6. *("Transitivité des notions de raffinement et de raffinement galoisien") Soient L/K une extension et*

$$(F) \qquad K = F_0 \leq \cdots \leq F_i \leq \cdots \leq F_m = L$$

une tour de L/K. Tout raffinement (resp. raffinement galoisien) (R) d'un raffinement (resp. d'un raffinement galoisien) (E) de (F) est un raffinement (resp. un raffinement galoisien) de (F).

Démonstration. En vertu de la remarque 1.2.(2)

$$(E) \qquad K = E_0 \leq \cdots \leq E_{j_0} = F_0 = K \leq \cdots \leq E_{j_i} = F_i \leq \cdots \leq E_j \leq \ldots \\ \cdots \leq E_{j_m} = F_m \leq \cdots \leq E_n = L$$

où $0 \leq j_0 < j_1 < \cdots < j_m \leq n$ et $F_i = E_{j_i}$ pour tout $i \in \{0, \ldots, m\}$. De même, comme (R) est un raffinement de (E), on a en particulier

$$(R) \qquad K = R_0 \leq \cdots \leq R_{k_0} = E_0 = K \leq \cdots \leq R_{k_{j_i}} = E_{j_i} \leq \cdots \leq R_k \leq \ldots \\ \cdots \leq R_{k_{j_m}} = E_{j_m} \leq \cdots \leq R_l = L$$

avec $0 \leq k_{j_0} < k_{j_1} < \cdots < k_{j_m} \leq l$ et $F_i = E_{j_i} = R_{k_{j_i}}$ pour tout $i \in \{0, \ldots, m\}$. Ceci suffit à établir que (R) est un raffinement de (F) elle-même.

Montrons maintenant que lorsque (E) (resp. (R)) est en fait un raffinement galoisien de (F) (resp. (E)), (R) est nécessairement un raffinement galoisien de (F), i.e. vérifie la condition (cf. Déf. 1.3.(4))

$$\text{(RAFG)} \quad \forall k \in \{1, \ldots, l-1\} \quad \big(\forall i \in \{0, \ldots, m\} \quad R_k \neq F_i\big) \;\Rightarrow\; R_{k-1} \trianglelefteq R_k \,.$$

Soit $k \in \{1, \ldots, l-1\}$ tel que $R_k \neq F_i$ pour tout $i \in \{0, \ldots, m\}$. De deux choses l'une :

- Ou bien R_k est distinct de tous les E_j, i.e.

$$\forall j \in \{0, \ldots, n\} \quad R_k \neq E_j \ ,$$

et alors la condition (RAFG) traduisant que (R) est un raffinement galoisien de (E) implique immédiatement $R_{k-1} \trianglelefteq R_k$.

- Ou bien R_k est déjà un corps de la tour (E), i.e.

$$\exists j \in \{0, \ldots, n\} \quad R_k = E_j \ .$$

Alors, par définition de k,

$$\forall i \in \{0, \ldots, m\} \quad R_k = E_j \neq F_i \ .$$

Si l'on traduit cette fois que (E) est un raffinement galoisien de (F), nous obtenons

$$R_{k_{j-1}} = E_{j-1} \trianglelefteq E_j = R_{k_j} \ .$$

Supposons que l'on ait choisi j minimal dans l'ensemble des indices j tels que $R_k = E_j$. Notons tout d'abord que $j \geq 1$, sans quoi $j = 0$ et $R_k = E_0 = K = F_0$ qui contredit notre hypothèse initiale sur k. Maintenant si l'on avait $k - 1 < k_{j-1}$, i.e. $k \leq k_{j-1}$, on aurait par croissance de la suite des R_k (Chap. 2, Déf. & Conv. 1.1)

$$E_j = R_k \leq R_{k_{j-1}} = E_{j-1} \leq E_j \ ;$$

d'où $R_k = E_{j-1}$, qui contredirait la minimalité de j. Donc nécessairement $k_{j-1} \leq k - 1$ et

$$\begin{array}{ccccc} R_{k_{j-1}} & \leq & R_{k-1} & \leq & R_k \\ || & & & & || \\ E_{j-1} & & \trianglelefteq & & E_j \ . \end{array}$$

L'extension R_k/R_{k-1} est ainsi bien galoisienne. □

On a déjà dit dans la remarque 1.4.(3) qu'un raffinement galoisien d'une tour quelconque n'est pas nécessairement une tour galoisienne. Cependant, nous disposons de la proposition suivante, que l'on peut regarder comme une justification de notre définition d'un raffinement galoisien.

Proposition 1.7. *Un raffinement galoisien d'une tour galoisienne est encore une tour galoisienne. Précisément, soit*

$$(T) \qquad K = T_0 \trianglelefteq T_1 \trianglelefteq \cdots \trianglelefteq T_i \trianglelefteq \cdots \trianglelefteq T_m = L$$

une tour galoisienne (cf. Chap. 2, Déf. & Conv. 1.1.(2)). Tout raffinement galoisien de (F)

$$(R) \qquad \begin{aligned} K = R_0 \leq \cdots \leq R_{j_0} = T_0 = K \leq \cdots \leq R_{j_1} = T_1 \leq \cdots \leq R_{j_i} = T_i \leq \ldots \\ \cdots \leq R_j \leq \cdots \leq R_{j_m} = T_m = L \leq \cdots \leq R_n = L \end{aligned}$$

est une tour galoisienne :

$$\forall j \in \{0, \ldots, n-1\} \quad R_j \trianglelefteq R_{j+1} \Leftrightarrow R_{j+1} \nearrow R_j \ .$$

Démonstration. Raisonnons par l'absurde en supposant que la tour (R) ne soit pas galoisienne, donc comporte au moins une marche non galoisienne :

$$\exists g \in \{0, \ldots, n-1\} \quad R_{g+1} \nwarrow R_g \, .$$

Considérons alors l'ensemble

$$J := \{j \in \{1, \ldots, n-1\} \mid \forall i \in \{0, \ldots, m\} \quad R_j \neq T_i\} \, .$$

L'indice $g+1$ ne peut être dans J, sans quoi l'on aurait

$$\forall i \in \{0, \ldots, m\} \quad R_{g+1} \neq T_i \, ,$$

et par la condition (RAFG) de (R) (cf. Déf. 1.3.(4))

$$R_g \trianglelefteq R_{g+1} \ : \text{ contradiction.}$$

Si $g+1 = n$, $R_{g+1} = L = T_m$. Si $g+1 \in \{1, \ldots, n-1\}$,

$$g+1 \notin J \iff (\exists i \in \{0, \ldots, m\} \quad R_{g+1} = T_i) \, .$$

Donc, dans tous les cas,

$$\exists i \in \{0, \ldots, m\} \quad R_{g+1} = T_i \, .$$

Soit i_p le plus petit des indices i tels que l'on ait $R_{g+1} = T_i$:

$$i_p := \min\{i \in \{0, \ldots, m\} \mid R_{g+1} = T_i\} \, .$$

Nécessairement $i_p \geq 1$, car sinon $i_p = 0$ et

$$K = T_0 = R_{g+1} \geq R_g \geq K$$

qui impliquerait $R_{g+1} = R_g = K$ et l'extension R_{g+1}/R_g serait galoisienne : contradiction. Donc $i_p - 1 \in \{0, \ldots, m\}$. La minimalité de i_p interdit que $R_{g+1} = T_{i_p-1}$. Ainsi $R_{g+1} \neq T_{i_p-1}$ et par la croissance de la suite $\{T_i\}_{0 \leq i \leq m}$,

$$\left.\begin{array}{c} T_{i_p-1} \leq T_{i_p} = R_{g+1} \\ T_{i_p-1} \neq R_{g+1} \end{array}\right\} \Rightarrow \ T_{i_p-1} < R_{g+1} \, .$$

Par ailleurs, comme (R) est un raffinement de (T), T_{i_p-1} est l'un des corps de la tour (R). Écrivons pour alléger la notation $j_p := j_{i_p-1}$; alors

$$R_{j_p} = T_{i_p-1} < R_{g+1} \ \Rightarrow \ j_p < g+1 \ \Leftrightarrow \ j_p \leq g$$

(puisque $j_p \geq g+1$ impliquerait $R_{j_p} \geq R_{g+1}$: contradiction). Donc

$$T_{i_p-1} = R_{j_p} \leq R_g \, .$$

Finalement

$$T_{i_p-1} \leq R_g \leq R_{g+1} = T_{i_p} \, .$$

L'hypothèse que (T) est une tour galoisienne nous assure en particulier que l'extension T_{i_p}/T_{i_p-1} est galoisienne. Il en est donc de même de sa sous-extension R_{g+1}/R_g, ce qui contredit notre hypothèse initiale $R_{g+1} \nwarrow R_g$. Cette dernière ne peut être faite ; c'est donc que la tour (R) est bien galoisienne. □

La proposition précédente admet un analogue galtourable.

Proposition 1.8. *Tout raffinement galoisien d'une tour galtourable est une tour galtourable.*

Démonstration. Celle de la proposition 1.7, mutatis mutandis, puisque l'on sait que toute sous-extension d'une extension galtourable est galtourable (cf. Prop. 2.9 du chapitre 2). □

Précisons maintenant le lien entre tours galtourables et tours galoisiennes.

Proposition 1.9. *Toute tour galtourable admet un raffinement galoisien qui est une tour galoisienne.*

Démonstration. Soit

$$(F) \qquad K = F_0 \lneqq F_1 \lneqq \ldots \lneqq F_i \lneqq \ldots \lneqq F_m = L$$

une tour galtourable (cf. Déf. 1.5 et Not. 1.9.(5) du chapitre 2). En tant qu'extension galtourable, chacune des marches F_{i+1}/F_i admet une tour galoisienne

$$(T_i) \qquad F_i = T_{j_i} \trianglelefteq T_{j_i+1} \trianglelefteq \cdots \trianglelefteq T_{j_{i+1}} = F_{i+1}$$

où

$$j_i < j_i + 1 \leq j_{i+1} \quad \Rightarrow \quad j_i < j_{i+1}\,.$$

En juxtaposant, c'est à dire en mettant bout à bout, les tours galoisiennes (T_i), on obtient la tour galoisienne

$$(T) \qquad K = F_0 = T_{j_0} \trianglelefteq T_{j_0+1} \trianglelefteq \cdots \trianglelefteq T_{j_1} = F_1 \trianglelefteq \cdots \trianglelefteq T_{j_m} = F_m = L$$

avec

$$0 \leq j_0 < j_1 < \cdots < j_m \leq j_m$$

et

$$F_i = T_{j_i} \quad (i = 0, \ldots, m)\,,$$

ce qui montre que (T) est un raffinement de (F). Comme c'est une tour galoisienne, c'est un raffinement galoisien de (F) (cf. Fait 1.5.(2)). □

Scholie. La démonstration précédente n'est qu'une généralisation de celle du Fait 2.7 du chapitre 2.

En contraste avec les extensions galoisiennes la proposition 1.9 admet le

Corollaire 1.10. *Soit L/K une extension admettant une tour galtourable. Alors L/K est une extension galtourable.*

Démonstration. D'après la proposition 1.9, cette tour galtourable admet un raffinement galoisien qui est une tour galoisienne (de L/K). Donc L/K admet une tour galoisienne, i.e. est galtourable (cf. Chap. 2, Déf. 1.4). □

A partir de la notion d'extension galoisienne, nous avons défini la classe plus large des extensions admettant une tour galoisienne. Le corollaire 1.10 précédent exprime que l'on ne peut pas aller plus loin dans cette direction : la classe des extensions admettant une tour galtourable n'est que celle des extensions galtourables elle-même. Précisément :

Corollaire 1.11. *Soit Ω un corps fixé. Dans Ω, l'ensemble des extensions galtourables est égal à celui des extensions admettant une tour galtourable.*

Démonstration. Toute extension galtourable $L\nearrow K$ admet la tour galtourable

$$K = F_0 \lesseqgtr F_1 = L \, .$$

L'autre inclusion est fournie par le corollaire 1.10. □

2. Tour stricte associée

La définition même d'un raffinement suppose la conservation des répétitions des corps dans une tour donnée. Le but de ce qui suit est d'introduire un moyen technique de "supprimer" ces répétitions, ce qui s'avérera nécessaire pour parler de tour de composition (cf. Chap. 4).

Proposition & Définition 2.1. *Soient L/K une extension quelconque et*

$$(F) \qquad K = F_0 \leq \cdots \leq F_i \leq \cdots \leq F_m = L$$

une tour de L/K. Il existe une tour stricte (S) de L/K (cf. Chap. 2, Déf. & Conv. 1.1.(1)) et une seule, telle que (F) soit un raffinement trivial de (S) (cf. Déf. 1.3.(2)). Nous appelons (S) "la tour stricte associée à (F)", et nous la notons

$$(F_<) := (S) \, .$$

Démonstration. (1) *Existence.* Il s'agit en fait d'effacer les répétitions de la tour (F). Précisément, notons $\mathcal{F}$ l'ensemble des corps de (F) :

$$\mathcal{F} := \{F_0, \ldots, F_i, \ldots, F_m\} \, ;$$

et soit

$$n := |\mathcal{F}| - 1 \leq m \, .$$

Renumérotons $\mathcal{F}$ de manière croissante en écrivant

$$\mathcal{F} = \{F_{j_0}, \ldots, F_{j_i}, \ldots, F_{j_n}\}$$

avec, donc,

$$\forall (k,l) \in \{0, \ldots, n\}^2 \quad k < l \Rightarrow F_{j_k} < F_{j_l} \, .$$

En posant $S_i := F_{j_i}$ $(i \in \{0, \ldots, n\})$, on obtient clairement la tour stricte

$$(S) \qquad S_0 = F_{j_0} = F_0 = K < \cdots < S_i = F_{j_i} < \cdots < S_n = F_{j_n} = F_m = L$$

de L/K, avec la suite finie d'indices

$$0 \leq j_0 < j_1 < \cdots < j_n \leq m \, .$$

En effet, on aurait dans le cas contraire l'existence d'un couple $(k,l) \in \{0,\dots,n\}^2$ avec $k < l$ et $j_l \leq j_k$, et par croissance de la suite $\{F_i\}_{0\leq i\leq m}$, $F_{j_l} \leq F_{j_k}$ qui contredit la croissance de la numérotation de $\mathcal{F}$.
Comme on a $S_i = F_{j_i}$ $(i \in \{0,\dots,n\})$ par construction, ceci prouve la condition (RAF2) de la définition & convention 1.1.(1), et (F) est un raffinement de (S). La condition (RAFT) de la définition 1.3.(2) étant évidemment vérifiée, il est de plus trivial.

(2) *Unicité*. Soit maintenant

$$(S') \qquad K = S'_0 < \cdots < S'_{i'} < \cdots < S'_{n'} = L$$

une autre tour stricte de L/K de raffinement trivial (F). On a aussi

$$\mathcal{F} = \{S'_0,\dots,S'_{n'}\}\,.$$

En effet soit $F_i \in \mathcal{F} = \{F_0,\dots,F_i,\dots,F_m\}$. Si l'on avait $F_i \notin \{S'_0,\dots,S'_{n'}\}$, la tour (F) serait un raffinement propre (cf. Déf. & Conv. 1.1.(2)), i.e. non trivial : contradiction avec la définition de (S'). L'inclusion inverse traduit simplement que (F) est un raffinement de (S'). L'égalité précédente implique que

$$n+1 = |\mathcal{F}| = |\{S'_0,\dots,S'_{n'}\}|\,.$$

Mais (S') étant stricte,

$$|\{S'_0,\dots,S'_{n'}\}| = n'+1\,,$$

de sorte que nécessairement $n' = n$. Raisonnons maintenant par l'absurde en supposant que $(S) \neq (S')$. Par le (3) de la définition & convention 1.1 du chapitre 2 cela équivaut à ce que

$$\{i \in \{0,\dots,n\} \mid S_i \neq S'_i\} \neq \emptyset\,.$$

Soit l le plus petit élément de cet ensemble non vide d'entiers. Comme d'après ce qui précède

$$\mathcal{F} = \{S_0,\dots,S_n\} = \{S'_0,\dots,S'_n\}\,,$$

il existe j dans $\{0,\dots,n\}$ tel que

$$j \neq l\,, \quad S_l = S'_j\,.$$

Si l'on avait $j < l$, on déduirait de la minimalité de l que $S_j = S'_j = S_l$ qui contredit que (S) est une tour stricte. Donc $j \geq l$, i.e. $j > l$ (puisque $j \neq l$ par définition). Comme (S') est stricte, on obtient alors $S'_l < S'_j$. De même, il existe k dans $\{0,\dots,n\}$ tel que $S'_l = S_k$. Mutatis mutandis, on montre que $k > l$ et $S_l < S_k$. Mais alors

$$\begin{array}{ccc} S_l & < & S_k \\ || & & || \\ S'_j & > & S'_l \end{array} \quad \text{contradiction.}$$

□

Remarques 2.2. (1) Lorsque (F) est stricte, on a clairement $(F_<) = (F)$. En particulier, la tour triviale est stricte (cf. Chap. 2, Déf. & Conv. 1.1.(1)) et

$$(F) = (F_<) \qquad K = F_0 = L\ .$$

(2) La démonstration de l'unicité de la tour stricte consiste en fait à montrer que celle-ci ne peut être obtenue que par renumérotation croissante de $\mathcal{F}$ (numérotation qui est unique).

La notion de tour stricte associée à une tour donnée est compatible avec celle de raffinement.

Proposition 2.3. *Soient L/K une extension quelconque et*

$$(F) \qquad K = F_0 \leq \cdots \leq F_i \leq \cdots \leq F_m = L$$

une tour de L/K. Pour tout raffinement

$$(E) \qquad K = E_0 \leq \cdots \leq E_j \leq \cdots \leq E_n = L$$

de (F), $(E_<)$ est un raffinement de $(F_<)$ (Prop.&Déf. 2.1).

Scholie. En général $(E_<)$ ne raffine pas (F), car les répétitions éventuelles de (F) ont disparu dans $(F_<)$, et ne peuvent se retrouver dans la tour stricte $(E_<)$.

Démonstration. Écrivons

$$(F_<) \qquad K = F_0 = F_{<0} < \cdots < F_{<m'} = F_m = L\,;$$
$$(E_<) \qquad K = E_0 = E_{<0} < \cdots < E_{<n'} = E_n = L\,.$$

Comme (F) est un raffinement trivial de $(F_<)$, on a

$$\mathcal{F} := \{F_0, \ldots, F_m\} = \{F_{<0}, \ldots, F_{<m'}\}\,;$$

de même

$$\mathcal{E} := \{E_0, \ldots, E_n\} = \{E_{<0}, \ldots, E_{<n'}\}\,.$$

L'hypothèse que (E) est un raffinement de (F) signifie qu'il existe une suite finie d'entiers

$$0 \leq j_0 < j_1 < \cdots < j_m \leq n$$

telle que

$$\forall i \in \{0, \ldots, m\} \qquad F_i = E_{j_i}\,.$$

Cela implique en particulier que $\mathcal{F} \subseteq \mathcal{E}$. Ainsi

$$\forall i' \in \{0, \ldots, m'\} \quad \exists j'_{i'} \in \{0, \ldots, n'\} \qquad F_{<i'} = E_{<j'_{i'}}\,.$$

Fixons une suite de tels entiers : $\{j'_{i'}\}_{0 \leq i' \leq m'}$. Elle est strictement croissante. En effet, raisonnons par l'absurde en supposant qu'il existe $0 \leq i'_1 < i'_2 \leq m'$ avec $j'_{i'_2} \leq j'_{i'_1}$. On a alors $E_{<j'_{i'_2}} \leq E_{<j'_{i'_1}}$ par croissance de toute tour de corps. Tandis que, comme la tour $(F_<)$ est stricte, l'inégalité $i'_1 < i'_2$ entraine

$$E_{<j'_{i'_1}} = F_{<i'_1} < F_{<i'_2} = E_{<j'_{i'_2}} \quad : \text{ contradiction.}$$

Par conséquent

$$0 \leq j'_0 < j'_1 < \cdots < j'_{m'} \leq n'$$

avec

$$\forall i' \in \{0, \ldots, m'\} \qquad F_{<i'} = E_{<j'_{i'}} .$$

Or ceci exprime précisément que $(E_<)$ est un raffinement de $(F_<)$ (Déf. & Conv. 1.1.(1)). □

Corollaire 2.4. *Pour toute tour stricte (F) de L/K et tout raffinement (E) de (F), $(E_<)$ est encore un raffinement de (F).*

Démonstration. Cela découle immédiatement de ce que $(F_<) = (F)$ (cf. Rem. 2.2.(1)) et de la proposition 2.3 précédente. □

Nous énonçons maintenant un fait bien intuitif, de démonstration élémentaire mais subtile. Il sera précisé davantage au chapitre 4. Nous le faisons figurer ici car il est indispensable pour généraliser la proposition 2.3 aux raffinements galoisiens.

Fait 2.5. *Soient L/K une extension quelconque,*

$$(F) \qquad K = F_0 \leq \cdots \leq F_i \leq \cdots \leq F_m = L$$

une tour de L/K, et

$$(F_<) \qquad K = F_0 = F_{<0} < \cdots < F_{<j} < \cdots < F_{<m'} = F_m = L$$

la tour stricte associée à (F) (cf. Prop. & Déf. 2.1). Alors toute marche de $(F_<)$ est une marche de (F).

Démonstration. Le résultat est trivial si $K = L$. Supposons $L \neq K$ de sorte que l'on puisse considérer $F_{<j+1}/F_{<j}$ ($j \in \{0, \ldots, m'-1\}$) une marche de $(F_<)$. Comme (F) est un raffinement de $(F_<)$, on sait

$$\exists i_j < i_{j+1} \quad F_{i_j} = F_{<j} < F_{<j+1} = F_{i_{j+1}} .$$

Considérons l'ensemble d'entiers

$$I_{j+1} := \{i \in \{0, \ldots, m\} \mid F_i = F_{<j+1}\} .$$

Comme l'ensemble $I_{j+1} \neq \emptyset$ puisque $F_{i_{j+1}} = F_{<j+1}$, il admet un plus petit élément, et nous pouvons considérer

$$l := (min\, I_{j+1}) - 1.$$

Avoir $l + 1 \leq i_j$ conduirait à $F_{l+1} \leq F_{i_j}$ qui contredit $F_{i_j} = F_{<j} < F_{<j+1} = F_{l+1}$. On a donc $0 \leq i_j < l + 1$ et en particulier $l \geq 0$. D'où l'existence de F_l. La minimalité de $l + 1$ dans I_{j+1} interdit que $F_l = F_{<j+1} = F_{l+1}$. Donc

$$F_l < F_{l+1} = F_{<j+1} .$$

Comme par ailleurs $F_{i_j} \leq F_l$ (puisque $i_j < l+1 \Leftrightarrow i_j \leq l$), on a la tour

$$F_{<j} = F_{i_j} \leq F_l < F_{l+1} = F_{<j+1}\,.$$

Or, par définition, (F) raffine trivialement $(F_<)$ et donc

$$\exists j' \in \{0, \ldots, m'\} \quad F_l = F_{<j'}\,.$$

Montrons maintenant que nécessairement $j' = j$. Si tel n'était pas le cas, on aurait :

- Ou bien $j' < j$ et $F_l = F_{<j'} < F_{<j}$; d'où

$$F_l < F_{<j} = F_{i_j} < F_{<j+1} = F_{l+1}\,.$$

Mais ceci pose un insurmontable problème à i_j, qui ne peut ni être inférieur ou égal à l (par l'inégalité stricte de gauche), ni supérieur ou égal à $l+1$ (par celle de droite) : contradiction.

- Ou bien $j+1 \leq j'$ et $F_{<j+1} \leq F_{<j'} = F_l$ qui contredit directement

$$F_l < F_{l+1} = F_{<j+1}\,.$$

Il est donc prouvé que $j' = j$. Finalement

$$(F_{<j+1}/F_{<j}) = (F_{l+1}/F_l)$$

et donc $(F_{<j+1}/F_{<j})$ est bien une marche de (F). □

Nous montrerons au chapitre 4, corollaire 1.6, que la réciproque est vraie : toute marche non triviale de (F) est une marche de $(F_<)$.

Tirons ici du Fait 2.5 précédent l'important

Corollaire 2.6. *Soit L/K une extension galtourable (Chap. 2, Déf. 1.4). Pour toute tour galoisienne*

$$(T) \qquad K = T_0 \trianglelefteq \cdots \trianglelefteq T_i \cdots \trianglelefteq T_m = L$$

de L/K, la tour stricte $(T_<)$ associée à (T) (Prop. & Déf. 2.1) est aussi galoisienne :

$$(T_<) \qquad K = T_0 = T_{<0} \lhd \cdots \lhd T_{<j} \lhd \cdots \lhd T_{<m'} = T_m = L\,.$$

Démonstration. Toute marche de $(T_<)$ est une extension galoisienne, en tant que marche de (T). □

On a vu que la notion de tour stricte associée est compatible avec celle de raffinement (Prop. 2.3). Voyons qu'il en est de même avec la notion de raffinement galoisien.

Proposition 2.7. *Soient L/K une extension quelconque, et*

$$(F) \qquad K = F_0 \leq \cdots \leq F_i \leq \cdots \leq F_m = L$$

une tour de L/K. Pour tout raffinement galoisien (Déf. 1.3.(4))

$$(E) \qquad K = E_0 \leq \cdots \leq E_k \leq \cdots \leq E_n = L$$

de (F), $(E_<)$ est un raffinement galoisien de $(F_<)$.

Démonstration. On sait déjà, par la proposition 2.3, que $(E_<)$ est un raffinement de

$$(F_<) \qquad K = F_0 = F_{<0} < \cdots < F_{<j} < \cdots < F_{<m'} = F_m = L\,.$$

Il reste à voir que

$$(E_<) \qquad K = E_0 = E_{<0} < \cdots < E_{<l} < \cdots < E_{<n'} = E_n = L$$

vérifie la condition (RAFG) du (4) de la définition 1.3. Notons que le Fait 2.5 assure que toutes les marches de $(E_<)$ sont des marches de (E) :

$$\forall l \in \{1, \ldots, n'\} \quad \exists k_l \in \{1, \ldots, n\} \quad (E_{<l}/E_{<l-1}) = (E_{k_l}/E_{k_l-1})\,.$$

Supposons qu'il existe $l \in \{1, \ldots, n'-1\}$ tel que

$$\forall j \in \{0, \ldots, m'\} \quad E_{<l} \neq F_{<j}\,.$$

(Si un tel l n'existe pas, le raffinement est trivial, donc galoisien (Fait 1.5.(1))). En vertu de la démonstration de la proposition & définition 2.1, on sait par ailleurs que

$$\{F_{<0}, \ldots, F_{<m'}\} = \{F_0, \ldots, F_m\}\,.$$

Dès lors on a

$$\forall i \in \{0, \ldots, m\} \quad E_{<l} \neq F_i\,.$$

Comme $E_{<l} = E_{k_l}$, c'est donc que

$$\forall i \in \{0, \ldots, m\} \quad E_{k_l} \neq F_i\,.$$

Par la condition (RAFG) du raffinement galoisien (E) de (F), on obtient finalement que

$$(E_{<l} = E_{k_l} \nearrow E_{k_l-1} = E_{<l-1})$$

ce que l'on voulait. □

Corollaire 2.8. *Pour toute tour stricte (F) de L/K et tout raffinement galoisien (E) de (F), $(E_<)$ est encore un raffinement galoisien de (F).*

Démonstration. Celle du corollaire 2.4 mutatis mutandis. □

L'introduction des tours strictes associées nous permet d'écrire la version stricte suivante de la proposition 1.9 :

Proposition 2.9. *Toute tour galtourable stricte admet un raffinement galoisien qui est une tour galoisienne stricte.*

Démonstration. Soit (F) une tour galtourable stricte

$$(F) \qquad K = F_0 \lneqq \cdots \lneqq F_i \lneqq \cdots \lneqq F_m = L\,.$$

La proposition 1.9 fournit une tour galoisienne

$$(T) \qquad K = F_0 = T_0 \trianglelefteq \cdots \trianglelefteq T_j \trianglelefteq \cdots \trianglelefteq T_n = L$$

qui est un raffinement (nécessairement galoisien par le Fait 1.5.(2)) de (F). La proposition 2.7 assure que la tour stricte associée $(T_<)$ est un raffinement galoisien de $(F_<) = (F)$ (Remarque 2.2.(1)). Et le corollaire 2.6 certifie que $(T_<)$ est encore une tour galoisienne. □

Notons enfin le fait suivant concernant les tours strictes.

Fait 2.10. *Soient L/K une extension et*

$$(F) \qquad K = F_0 < \cdots < F_i < \cdots < F_m = L$$

une tour stricte de L/K. Pour tout raffinement trivial strict

$$(E) \qquad K = E_0 = F_0 = E_{j_0} < \cdots < E_{j_i} = F_i < \cdots < E_{j_m} = F_m = L$$

de (F), on a nécessairement $(E) = (F)$ (Chap. 2, Déf. & Conv. 1.1.(3)).

Démonstration. La tour (F) est stricte de raffinement trivial (E). Par l'unicité de la Prop. & Déf. 2.1, c'est donc que $(F) = (E_<)$. Or (E) étant une tour stricte, on a $(E_<) = (E)$ d'après la remarque 2.2.(1). D'où la conclusion. □

3. Tour restreinte, tour ratio

L'obtention de raffinements de tours de corps sera notre objet dans les chapitres 4, 6 et 7. Nous voulons ici introduire une méthode de fragmentation qui sera utilisée au chapitre 7 final. La définition suivante précise la notion intuitive de suppression, à gauche ou à droite, des corps d'une tour donnée.

Définition 3.1. Soient L/K une extension quelconque et

$$(F) \qquad K = F_0 \leq \cdots \leq F_i \leq \cdots \leq F_m = L$$

une tour de L/K. Pour tout indice fixé $r \in \{0, \ldots, m\}$, nous appelons :

(1) "Tour restreinte de (F) à l'indice r", et nous notons

$$(res_r(F))$$

la tour obtenue en supprimant dans (F) les r premiers corps, i.e. $F_0, F_1, \ldots, F_{r-1}$:

$$(res_r(F)) \qquad F_r \leq \cdots \leq F_i \leq \cdots \leq F_m = L\,.$$

(2) "Tour ratio de (F) à l'indice r", et nous notons

$$(rat_r(F))$$

la tour obtenue en supprimant dans (F) les $m-r$ derniers corps, i.e. $F_{r+1}, \dots, F_m$:

$$(rat_r(F)) \qquad K = F_0 \leq \cdots \leq F_i \leq \cdots \leq F_r \, .$$

(3) "Tour inflatée à L de $(rat_r(F))$", et nous notons

$$\Big(inf_L(rat_r(F))\Big) \quad \text{ou} \quad (inf_{L,r}(F))$$

la tour obtenue en conservant tous les corps F_i de $(rat_r(F))$ sauf le dernier, que l'on remplace par L :

$$(inf_{L,r}(F)) \qquad K = F_0 \leq \cdots \leq F_i \leq \cdots \leq F_{r-1} \leq L \, .$$

(4) Lorsque la tour (F) est stricte (Chap. 2, Déf. & Conv. 1.1.(1)), on écrit par abus de notation $(res_{F_r}(F))$ (resp. $(rat_{F_r}(F))$) au lieu de $(res_r(F))$ (resp. $(rat_r(F))$).

Pour fixer les idées, donnons l'immédiat

Fait 3.2. *Dans les notations de la définition 3.1, et en convenant d'écrire (K) (resp. (L)) la tour réduite au seul corps K (resp. L), on a :*

$$\begin{array}{lll} (res_0(F)) = (F) & , & (res_m(F)) = (L) \, ; \\ (rat_0(F)) = (K) & , & (rat_m(F)) = (F) \, ; \\ (inf_{L,0}(F)) = (L) & , & (inf_{L,m}(F)) = (F) \, . \end{array}$$

La proposition suivante justifie les définitions qui précèdent.

Proposition 3.3. *Soient L/K une extension quelconque et*

$$(F) \qquad K = F_0 \leq \cdots \leq F_i \leq \cdots \leq F_m = L$$

une tour de L/K. Soit r un entier fixé quelconque dans $\{0, \dots, m\}$.

(1) Pour tout raffinement

$$(E) \qquad \begin{array}{l} K = E_0 \leq \cdots \leq E_{j_0} = F_0 = K \leq \cdots \leq E_{j_i} = F_i \leq \dots \\ \qquad \cdots \leq E_{j_r} = F_r \leq \cdots \leq E_{j_m} = F_m = L \leq \cdots \leq E_n = L \end{array}$$

de (F) (cf. Rem. 1.2.(2)), la tour restreinte (resp. ratio) à l'indice j_r de (E), i.e. $(res_{j_r}(E))$ $\Big($resp. $(rat_{j_r}(E))\Big)$, est un raffinement de $(res_r(F))$ $\Big($resp. $(rat_r(F))\Big)$.

(2) Réciproquement, pour tout raffinement (S) de $(res_r(F))$ et tout raffinement (R) de $(rat_r(F))$, il existe un unique raffinement (E) de (F) tel que l'on ait à la fois $(res_{j_r}(E)) = (S)$ et $(rat_{j_r}(E)) = (R)$.

Démonstration. (1) Puisque (E) raffine (F), on a par définition (Déf. & Conv. 1.1.(1))

$$0 \leq j_0 < \cdots < j_i < \cdots < j_r < \cdots < j_m \leq n$$

avec

$$\forall i \in \{0, \ldots, m\} \quad F_i = E_{j_i} \, .$$

Alors à l'évidence

$$j_r \leq j_r < \cdots < j_m \leq n \qquad (\text{resp.} \quad 0 \leq j_0 < \cdots < j_r \leq j_r \ )$$

avec

$$\forall i \in \{r, \ldots, m\} \quad F_i = E_{j_i} \qquad (\text{resp.} \quad \forall i \in \{0, \ldots, r\} \quad F_i = E_{j_i} \ ) \, .$$

Ceci établit directement que

$$(res_{j_r}(E)) \qquad F_r = E_{j_r} \leq \cdots \leq E_{j_i} = F_i \leq \cdots \leq E_j \leq \ldots$$
$$\cdots \leq E_{j_m} = F_m = L \leq \cdots \leq E_n = L$$

$$\Big(\text{ resp. } (rat_{j_r}(E)) \qquad K = E_0 = F_0 \leq \cdots \leq E_{j_0} = F_0 = K \leq \ldots$$
$$\cdots \leq E_{j_i} = F_i \leq \cdots \leq E_j \leq \cdots \leq E_{j_r} = F_r \quad \Big)$$

est un raffinement de

$$(res_r(F)) \qquad F_r \leq \cdots \leq F_i \leq \cdots \leq F_m = L$$

$$\Big(\text{ resp. } (rat_r(F)) \qquad K = F_0 \leq \cdots \leq F_i \leq \cdots \leq F_r \quad \Big) \, .$$

(2) Écrivons :

$$(S) \qquad F_r = S_0 \leq \cdots \leq S_k \leq \cdots \leq S_p = L$$
$$(R) \qquad K = R_0 \leq \cdots \leq R_l \leq \cdots \leq R_q = F_r \, .$$

Comme (S) (resp. (R)) raffine $(res_r(F))$ (resp. $(rat_r(F))$), on a par définition

$$0 \leq k_r < \cdots < k_m \leq p \qquad (\text{resp.} \quad 0 \leq l_0 < \cdots < l_r \leq q \ )$$

avec

$$\forall i \in \{r, \ldots, m\} \quad F_i = S_{k_i} \qquad (\text{resp.} \quad \forall i \in \{0, \ldots, r\} \quad F_i = R_{l_i} \ ) \, .$$

Posons :

$$\forall j \in \{0, \ldots, q\} \quad E_j := R_j \ , \quad \forall j \in \{q+1, \ldots, q+p\} \quad E_j := S_{j-q} \ ;$$
$$\forall i \in \{0, \ldots, r-1\} \quad j_i := l_i \ , \quad j_r := q \ , \quad \forall i \in \{r+1, \ldots, m\} \quad j_i := q + k_i \, .$$

On a la suite d'indices

$$0 \leq j_0 = l_0 < \cdots < j_{r-1} = l_{r-1} < j_r = q < j_{r+1} = q + k_{r+1} < \ldots$$
$$\cdots < j_m = q + k_m \leq q + p \, .$$

En effet

$$l_{r-1} < l_r \leq q \quad \Rightarrow \quad j_{r-1} < j_r$$

et

$$0 \leq k_r < k_{r+1} \quad \Rightarrow \quad j_r = q \leq q + k_r < q + k_{r+1} = j_{r+1} \, .$$

Tout ceci avec

$$\forall i \in \{0, \ldots, r-1\} \quad F_i = R_{l_i} = E_{l_i} = E_{j_i}$$
$$F_r = R_q = E_q = E_{j_r}$$
$$\forall i \in \{r+1, \ldots, m\} \quad F_i = S_{k_i} = E_{q+k_i} = E_{j_i}$$

(ce dernier cas car

$$0 \leq k_r < k_{r+1} \leq k_i \leq p \;\Rightarrow\; 1 \leq k_i \leq p \;\Rightarrow\; q+1 \leq q+k_i \leq q+p\ ).$$

Finalement, il est prouvé que

$$\forall i \in \{0, \ldots, m\} \quad F_i = E_{j_i}$$

ce qui exprime que (E) est un raffinement de (F).

Montrons enfin que cette tour (E) vérifie bien les conditions souhaitées. Posons $n := q + p$. D'après la définition 3.1

$$\begin{array}{lccccccccc} (res_{j_r}(E)) & F_r = & E_{j_r=q} & \leq & E_{q+1} & \leq \cdots \leq & E_j & \leq \cdots \leq & E_n & = L \\ & & || & & || & & || & & || & \\ & & S_0 & \leq & S_1 & \leq \cdots \leq & S_{k=j-q} & \leq \cdots \leq & S_p & \end{array}$$

ce qui exprime que $(res_{j_r}(E)) = (S)$. De même, trivialement

$$\begin{array}{lccccccc} (rat_{j_r}(E)) & K = & E_0 & \leq \cdots \leq & E_j & \leq \cdots \leq & E_{j_r=q} & = F_r \\ & & || & & || & & || & \\ & & R_0 & \leq \cdots \leq & R_j & \leq \cdots \leq & R_q & \end{array}$$

ce qui exprime que $(rat_{j_r}(E)) = (R)$.

Prouvons maintenant l'unicité de l'énoncé du (2). Soit (E') une tour de corps telle que $(res_{j_r}(E')) = (S)$ et $(rat_{j_r}(E')) = (R)$. Si l'on désigne par n' la hauteur de (E'), la première de ces deux égalités implique directement que

$$n' = j_r + p = n\ .$$

Il faut prouver que $E'_j = E_j$ pour tout $j \in \{0, \ldots, m\}$ (cf. Chap. 2, Déf. & Conv. 1.1.(3)).

- Si $j \in \{0, \ldots, q = j_r\}$

$$\begin{array}{ccccccc} (rat_{j_r}(E')) & E'_0 & \leq \cdots \leq & E'_j & \leq \cdots \leq & E'_{j_r} \\ || & || & & || & & || \\ (R) & R_0 & \leq \cdots \leq & R_j & \leq \cdots \leq & R_{j_r} \end{array}$$

d'où

$$\forall j \in \{0, \ldots, q\} \quad E'_j = R_j = E_j\ .$$

- Si $j \in \{q+1, \ldots, q+p = n\}$

$$\begin{array}{ccccccccc} (res_{j_r}(E')) & E'_{j_r} & \leq & E'_{j_r+1} & \leq \cdots \leq & E'_j & \leq \cdots \leq & E'_n \\ || & || & & || & & || & & || \\ (S) & S_0 & \leq & S_1 & \leq \cdots \leq & S_{j-q} & \leq \cdots \leq & S_p \end{array}$$

d'où

$$\forall j \in \{q+1, \dots, n\} \quad E'_j = S_{j-q} = E_j \ .$$

Ceci achève la démonstration de la proposition 3.3. □

Quelle est maintenant la version de la proposition 3.3 pour les raffinements propres ou les raffinements galoisiens ? Nous aurons besoin du

Lemme 3.4. *Soient L/K une extension quelconque,*

$$(F) \qquad K = F_0 \leq F_1 \leq \cdots \leq F_i \leq \cdots \leq F_m = L$$

une tour de L/K, et r un entier fixé dans $\{0, \dots, m\}$. Pour tout raffinement

$$(E) \qquad K = E_0 \leq \cdots \leq E_{j_0} = F_0 = K \leq \cdots \leq E_{j_i} = F_i \leq \cdots \leq E_j \leq \dots \\ \cdots \leq E_{j_m} = F_m = L \leq \cdots \leq E_n = L$$

de (F), on a les implications suivantes :

(1) $\forall j \in \{1, \dots, j_r - 1\} \quad (\exists\, i \in \{r+1, \dots, m\} \quad E_j = F_i) \quad \Rightarrow \quad E_j = F_r \ .$

(1-1) $\forall j \in \{1, \dots, j_r - 1\},$

$$(\forall i \in \{0, \dots, r\} \quad E_j \neq F_i) \ \Rightarrow \ (\forall i \in \{0, \dots, m\} \quad E_j \neq F_i) \ .$$

(1-2) $$\Big(\ \exists\, j \in \{1, \dots, j_r - 1\} \quad \forall i \in \{0, \dots, r\} \quad E_j \neq F_i \ \Big)$$
$$\Downarrow$$
$$\Big(\ \exists\, j \in \{1, \dots, n-1\} \quad \forall i \in \{0, \dots, m\} \quad E_j \neq F_i \ \Big) \ .$$

(2) $\forall j \in \{j_r + 1, \dots, n-1\} \quad (\exists\, i \in \{0, \dots, r-1\} \quad E_j = F_i) \quad \Rightarrow \quad E_j = F_r \ .$

(2-1) $\forall j \in \{j_r + 1, \dots, n-1\},$

$$(\forall i \in \{r, \dots, m\} \quad E_j \neq F_i) \ \Rightarrow \ (\forall i \in \{0, \dots, m\} \quad E_j \neq F_i) \ .$$

(2-2) $$\Big(\ \exists\, j \in \{j_r + 1, \dots, n-1\} \quad \forall i \in \{r, \dots, m\} \quad E_j \neq F_i \ \Big)$$
$$\Downarrow$$
$$\Big(\ \exists\, j \in \{1, \dots, n-1\} \quad \forall i \in \{0, \dots, m\} \quad E_j \neq F_i \ \Big) \ .$$

Démonstration. (1) Par la croissance des suites $\{F_i\}_{0 \leq i \leq m}$ et $\{E_j\}_{0 \leq j \leq n}$,

$$F_r \leq F_{r+1} \leq F_i = E_j \leq E_{j_r - 1} \leq E_{j_r} = F_r \quad \Rightarrow \quad E_j = F_r \ .$$

(1-1) Soit $j \in \{1, \dots, j_r - 1\}$ tel que $E_j \neq F_i$ pour tout $i \in \{0, \dots, r\}$. Raisonnons par l'absurde en supposant

$$\exists\, i \in \{0, \dots, m\} \quad E_j = F_i \ .$$

Comme $\{0, \dots, m\} = \{0, \dots, r\} \cup \{r+1, \dots, m\}$,
- ou bien

$(\exists\, i \in \{r+1, \dots, m\} \quad E_j = F_i)$ et $E_j = F_r$ d'après (1) : contradiction ;

- ou bien

$$(\exists\, i \in \{0,\dots,r\} \quad E_j = F_i) \quad \text{qui contredit notre hypothèse.}$$

D'où la conclusion voulue.
(1-2) Cela découle du (1-1) en prenant le même indice

$$j \in \{1,\dots,j_r-1\} \subseteq \{1,\dots,n-1\}$$

des deux côtés de l'implication.

$$(2) \qquad F_r = E_{j_r} \leq E_{j_r+1} \leq E_j = F_i \leq F_{r-1} \leq F_r \quad \Rightarrow \quad E_j = F_r\,.$$

(2-1) On raisonne par l'absurde comme dans la démonstration du (1-1) ci-dessus en considérant $j \in \{j_r+1,\dots,n-1\}$ tel que $E_j \neq F_i$ pour tout $i \in \{r,\dots,m\}$. Ne pas avoir le résultat annoncé conduit à une contradiction, ou bien par le (2) précédent, ou bien directement par hypothèse.
(2-2) Il découle quant à lui du (2-1) en prenant le même indice

$$j \in \{j_r+1,\dots,n-1\} \subseteq \{1,\dots,n-1\}$$

des deux côtés de l'implication. □

Avec la proposition 3.3 et le lemme 3.4 précédent, nous pouvons énoncer la

Proposition 3.5. *Soient L/K une extension quelconque et*

$$(F) \qquad K = F_0 \leq \cdots \leq F_i \leq \cdots \leq F_m = L$$

une tour de L/K. Soit r un entier fixé quelconque dans $\{0,\dots,m\}$.
(1) Pour tout raffinement propre (Déf. & Conv. 1.1.(2)) (E) de (F),
- ou la tour restreinte $(res_{j_r}(E))$ à l'indice j_r de (E) est un raffinement propre de $(res_r(F))$;
- ou la tour ratio $(rat_{j_r}(E))$ à l'indice j_r de (E) est un raffinement propre de $(rat_r(F))$.

(2) Réciproquement, pour tout raffinement (S) de $(res_r(F))$ et tout raffinement (R) de $(rat_r(F))$, tels que (R) ou (S) soit un raffinement propre, l'unique raffinement (E) induit par (R) et (S) (cf. Prop. 3.3.(2)) est un raffinement propre de (F).

Démonstration. (1) On se place dans les notations de la démonstration de la proposition 3.3. Notre hypothèse signifie que (Déf. & Conv. 1.1.(2))

$$\exists\, j \in \{1,\dots,n-1\} \quad \forall i \in \{0,\dots,m\} \quad E_j \neq F_i\,;$$

donc $E_j \neq F_i$ pour tout i dans $\{0,\dots,r\}$ ou $\{r,\dots,m\}$. Or $j \neq j_r$ car sinon $E_j = E_{j_r} = F_r$: contradiction. Donc
- ou bien

$$\exists\, j \in \{1,\dots,j_r-1\} \quad \forall i \in \{0,\dots,r\} \quad E_j \neq F_i$$

ce qui exprime que la tour ratio $(rat_{j_r}(E))$ est un raffinement propre de $(rat_r(F))$;
- ou bien

$$\exists\, j \in \{j_r+1,\dots,n-1\} \quad \forall i \in \{r,\dots,m\} \quad E_j \neq F_i$$

ce qui exprime que la tour restreinte $(res_{j_r}(E))$ est un raffinement propre de $(res_r(F))$.

(2) Les notations sont celles de la démonstration du (2) de la proposition 3.3 :

$$(S) \qquad F_r = S_0 \leq \cdots \leq S_k \leq \cdots \leq S_p = L$$
$$(R) \qquad K = R_0 \leq \cdots \leq R_l \leq \cdots \leq R_q = F_r\ .$$

- Dire que (S) est un raffinement propre de $(res_r(F))$ signifie

$$\exists\, k \in \{1,\dots,p-1\} \quad \forall i \in \{r,\dots,m\} \quad S_k \neq F_i\ .$$

Donc pour $j := q+k$,

$$\exists\, j \in \{q+1 = j_r+1,\dots,q+p-1 = n-1\} \quad \forall i \in \{r,\dots,m\} \quad S_{j-q} \neq F_i\ .$$

Mais, pour un tel j, on a posé $E_j := S_{j-q}$. Ainsi

$$\exists\, j \in \{j_r+1,\dots,n-1\} \quad \forall i \in \{r,\dots,m\} \quad E_j \neq F_i\ .$$

D'après le (2-2) du lemme 3.4, on en déduit que

$$\exists\, j \in \{1,\dots,n-1\} \quad \forall i \in \{0,\dots,m\} \quad E_j \neq F_i$$

ce qui exprime exactement que (E) est un raffinement propre de (F).

- De la même façon, dire que (R) est un raffinement propre de $(rat_r(F))$ signifie

$$\exists\, l \in \{1,\dots,q-1\} \quad \forall i \in \{0,\dots,r\} \quad R_l \neq F_i\ .$$

Donc pour $j := l$,

$$\exists\, j \in \{1,\dots,q-1 = j_r-1\} \quad \forall i \in \{0,\dots,r\} \quad E_j = R_j \neq F_i\ .$$

D'après le (1-2) du lemme 3.4, on en déduit que

$$\exists\, j \in \{1,\dots,n-1\} \quad \forall i \in \{0,\dots,m\} \quad E_j \neq F_i$$

ce qui exprime encore une fois que (E) est un raffinement propre de (F). □

Voici l'analogue galoisien de la proposition 3.3.

Proposition 3.6. *Dans les notations respectives de la proposition 3.3 :*
(1) Pour tout raffinement galoisien (E) de (F), la tour restreinte $(res_{j_r}(E))$ $\big($resp. la tour ratio $(rat_{j_r}(E))\big)$ est un raffinement galoisien de $(res_r(F))$ $\big($resp. $(rat_r(F))\big)$.

(2) Réciproquement, pour tout raffinement galoisien (S) de $(res_r(F))$ et tout raffinement galoisien (R) de $(rat_r(F))$, il existe un unique raffinement galoisien (E) de (F) tel que l'on ait à la fois $(res_{j_r}(E)) = (S)$ et $(rat_{j_r}(E)) = (R)$. Ce raffinement est celui de la proposition 3.3.

Démonstration. (1) Par définition d'un raffinement galoisien (Déf. 1.3.(4)), la tour (E) vérifie la condition

$$\text{(RAFG)} \quad \forall j \in \{1,\dots,n-1\} \ \Big(\ \forall i \in \{0,\dots,m\} \quad E_j \neq F_i \ \Big) \ \Rightarrow \ E_{j-1} \trianglelefteq E_j \ .$$

- Considérons $j \in \{1,\dots,j_r-1\}$ tel que $E_j \neq F_i$ pour tout $i \in \{0,\dots,r\}$. D'après le (1-1) du lemme 3.4,

$$\forall i \in \{0,\dots,m\} \quad E_j \neq F_i \ ,$$

d'où $E_{j-1} \trianglelefteq E_j$ par la condition (RAFG) ci-dessus. Ceci prouve que $(rat_{j_r}(E))$ est un raffinement galoisien de $(rat_r(F))$.

- Considérons $j \in \{j_r+1,\dots,n-1\}$ tel que $E_j \neq F_i$ pour tout $i \in \{r,\dots,m\}$. D'après le (2-1) du lemme 3.4,

$$\forall i \in \{0,\dots,m\} \quad E_j \neq F_i \ ,$$

d'où $E_{j-1} \trianglelefteq E_j$ par la condition (RAFG). Ceci prouve que $(res_{j_r}(E))$ est un raffinement galoisien de $(res_r(F))$.

(2) Les notations sont celles du (2) de la proposition 3.3 :

$$(S) \qquad F_r = S_0 \leq \cdots \leq S_k \leq \cdots \leq S_p = L$$

$$(R) \qquad K = R_0 \leq \cdots \leq R_l \leq \cdots \leq R_q = F_r \ .$$

Prouvons que le raffinement (E) qui y est construit est nécessairement galoisien. Soit $j \in \{1,\dots,n-1\} = \{1,\dots,j_r-1\} \cup \{j_r\} \cup \{j_r+1,\dots,n-1\}$ tel que $E_j \neq F_i$ pour tout $i \in \{0,\dots,m\}$. On ne peut pas avoir $j = j_r$ puisque $E_{j_r} = F_r$. Par conséquent :
- ou bien $j \in \{1,\dots,j_r-1 = q-1\}$ et l'on a en particulier

$$\forall i \in \{0,\dots,r\} \quad R_j = E_j \neq F_i \ .$$

La condition (RAFG) vérifiée par (R) assure alors que

$$E_{j-1} = R_{j-1} \trianglelefteq R_j = E_j \ ;$$

- ou bien $j \in \{j_r+1 = q+1,\dots,n-1 = q+p-1\}$ et pour $k := j-q$

$$\forall i \in \{r,\dots,m\} \quad S_k = E_j \neq F_i \ .$$

La condition (RAFG) vérifiée par (S) assure alors que

$$E_{j-1} = S_{k-1} \trianglelefteq S_k = E_j \ .$$

Dans tous les cas donc, $E_{j-1} \trianglelefteq E_j$ ce qui exprime que (E) est un raffinement galoisien de (F). □

Les propositions 3.5 et 3.6 se combinent en la proposition suivante pour les raffinements galoisiens propres.

Proposition 3.7. *Soient L/K une extension quelconque et*

$$(F) \qquad K = F_0 \leq \cdots \leq F_i \leq \cdots \leq F_m = L$$

une tour de L/K. Soit r un entier fixé quelconque dans $\{0, \ldots, m\}$.
(1) Pour tout raffinement galoisien propre (E) de (F) (Déf. & Conv. 1.1.(2))
- ou la tour restreinte $(res_{j_r}(E))$ à l'indice j_r de (E) est un raffinement galoisien propre de $(res_r(F))$;
- ou la tour ratio $(rat_{j_r}(E))$ à l'indice j_r de (E) est un raffinement galoisien propre de $(rat_r(F))$.

(2) Réciproquement, pour tout raffinement galoisien (S) de $(res_r(F))$ et tout raffinement galoisien (R) de $(rat_r(F))$, tels que (R) ou (S) soit un raffinement propre, l'unique raffinement (E) induit par (R) et (S) (cf. Prop. 3.3.(2)) est un raffinement galoisien propre de (F).

Démonstration. (1) Par le (1) de la proposition 3.6, $(res_{j_r}(E))$ et $(rat_{j_r}(E))$ sont des raffinements galoisiens. Le (1) de la proposition 3.5 assure que l'un ou l'autre est un raffinement propre. C'est donc que $(res_{j_r}(E))$ ou $(rat_{j_r}(E))$ est un raffinement galoisien propre.

(2) Par le (2) de la proposition 3.6, (E) est un raffinement galoisien de (F). Le (2) de la proposition 3.5 assure que (E) est un raffinement propre de (F). Autrement dit, (E) est un raffinement galoisien propre de (F) (cf. scholie de la Déf. 1.3). □

Chapitre 4

PREMIERS THÉORÈMES DE DISSOCIATION

En théorie des groupes, on connaît les deux célèbres théorèmes :

Théorème de Schreier ([**36**], [**16**])
Deux suites normales d'un même groupe admettent des raffinements équivalents.

Théorème de Jordan-Hölder ([**18**], [**15**], [**16**])
Soit G un groupe admettant une suite de composition.
(i) Toute suite normale stricte de G admet un raffinement qui est une suite de composition de G.
(ii) Deux suites de composition de G sont équivalentes.

En lieu et place d'un groupe G, nous considérons ici une extension galtourable L/K. Nous remplaçons les suites normales de G et ses suites de composition par les tours galoisiennes de L/K et ses "tours de composition". Notre but dans ce chapitre 4 est d'établir un analogue galoisien aux théorèmes de Schreier et de Jordan-Hölder. Pour cela, nous dévissons, nous dissocions les tours galoisiennes de L/K autant que nécessaire de façon à obtenir des "tours équivalentes" (de marches à groupes de Galois isomorphes à l'ordre près) qui n'admettent aucun raffinement galoisien propre. Nous appelons "théorèmes de dissociation" les théorèmes ainsi obtenus, et nous les généraliserons dans le chapitre 7 final à toutes les extensions algébriques finies.

1. Tours de composition galoisiennes, tours galoisiennes équivalentes

Définition 1.1. Soient L/K une extension galtourable et

$$(F) \qquad K = F_0 \trianglelefteq \cdots \trianglelefteq F_i \trianglelefteq \cdots \trianglelefteq F_m = L$$

une tour galoisienne de L/K.

(1) Nous disons que (F) est "une tour de composition galoisienne de L/K" si et seulement si elle est stricte et n'admet aucun raffinement galoisien propre.

(2) Soit

$$(E) \qquad K = E_0 \trianglelefteq \cdots \trianglelefteq E_j \trianglelefteq \cdots \trianglelefteq E_n = L$$

une autre tour galoisienne de L/K. Nous disons que (E) et (F) sont "équivalentes", et nous notons $(E) \sim (F)$, si et seulement si elles ont même nombre de

marches : $m = n$, et si, à permutation près, les groupes de Galois de ces marches sont isomorphes (topologiquement en degrés infinis) :

$$\exists \sigma \in S_m \quad \forall i \in \{1, \ldots, m = n\} \quad Gal(F_i/F_{i-1}) \xrightarrow{\sim} Gal(E_{\sigma(i)}/E_{\sigma(i)-1}) \ .$$

Un cas très particulier de cette définition est fourni par le

Fait 1.2. *L'extension triviale $L = K$ admet une tour de composition galoisienne et une seule, celle à zéro marche :*

$$(C) \qquad K = F_0 = L \ .$$

Démonstration. D'après le (1) de la définition & convention 1.1 du chapitre 2, la tour triviale (C) est stricte. Raisonnons par l'absurde en supposant que (C) admette un raffinement galoisien propre

$$(E) \qquad K = E_0 \trianglelefteq \cdots \trianglelefteq E_{j_0} = F_0 \trianglelefteq \cdots \trianglelefteq E_j \trianglelefteq \cdots \trianglelefteq E_n = L \ .$$

Par la condition (RAF3) de la définition & convention 1.1 du chapitre 3,

$$\exists j \in \{1, \ldots, n-1\} \quad \forall i \in \{0, \ldots, m\} \quad E_j \neq F_i \ .$$

En particulier $E_j \neq F_0 = K$. Dès lors, par la croissance de (E),

$$K = E_0 \leq E_j \leq E_n = L = K \ ;$$

d'où $E_j = K$: contradiction. Il est donc établi que (C) est une tour de composition galoisienne. Montrons que (C) est l'unique tour de composition de L/K. Soit (C') une tour de composition galoisienne de L/K de hauteur m'. Comme $[L : K] = 1$, on déduit du Fait 1.3 du chapitre 2 que nécessairement $m' = 0$. Donc (C') est la tour triviale et par conséquent $(C') = (C)$. □

La définition 1.1 précédente sera étendue au chapitre 7 aux tours quelconques d'une extension finie via la notion de "tour d'élévation". En particulier, il ne suffira pas d'y enlever les qualificatifs "galoisiens".

En théorie des groupes, on connaît la

Proposition. *Pour qu'une suite normale soit de composition, il faut et il suffit que chacun de ses facteurs soit simple.*

Voici son analogue galoisien :

Proposition 1.3. *Soit L/K une extension galtourable quelconque. Pour qu'une tour galoisienne de L/K soit de composition (cf. Déf. 1.1.(1)), il faut et il suffit que chacune de ses marches soit galsimple (Chap.2, Déf. 1.6.(2)).*

Démonstration. Montrons d'abord que l'équivalence est vraie pour l'extension triviale $L = K$. Par le Fait 1.2, celle-ci admet une tour de composition et une seule, celle à zéro marche :

$$(C) \qquad K = F_0 = L \ .$$

Soit donc (F) une tour de composition galoisienne de $L = K$. Comme $(F) = (C)$, la galsimplicité des marches de (F) est vérifiée puisqu'il n'y en a pas.

Inversement, soit (F) une tour de L/K dont toutes les marches sont galsimples. Si (F) était de hauteur non nulle, elle admettrait donc une marche stricte : contradiction. Finalement (F) est de hauteur nulle ; c'est la tour de composition galoisienne (C).

Supposons maintenant l'extension L/K non triviale, et soit

$$(F) \qquad K = F_0 \trianglelefteq \cdots \trianglelefteq F_i \trianglelefteq F_{i+1} \trianglelefteq \cdots \trianglelefteq F_m = L$$

une tour galoisienne de L/K. Supposons que (F) soit une tour de composition galoisienne et que l'une de ses marches $F_{i_0+1}\nearrow F_{i_0}$ ne soit pas galsimple. Par définition de la galsimplicité et le fait que la marche est galoisienne, il existe un corps F tel que

$$F_{i_0} \lhd F \lhd F_{i_0+1} \ .$$

Soit alors (E) la tour définie par

$$\begin{cases} \forall j \in \{0, \ldots, i_0\} & E_j = F_j \\ & E_{i_0+1} = F \\ \forall j \in \{i_0 + 2, \ldots, m+1\} & E_j = F_{j-1} \end{cases}$$

i.e.

$$(E) \quad K = E_0 \trianglelefteq \cdots \trianglelefteq E_{i_0} = F_{i_0} \trianglelefteq E_{i_0+1} = F \trianglelefteq E_{i_0+2} = F_{i_0+1} \trianglelefteq \cdots \trianglelefteq E_{m+1} = F_m = L \ .$$

Comme elle est galoisienne, cette tour (E) est un raffinement galoisien de (F) (cf. Chap. 3, Fait 1.5.(2)). De plus

$$\begin{cases} \forall i \in \{0, \ldots, i_0\} & (F_i \leq F_{i_0} < F) & \Rightarrow & F_i \neq F \\ \forall i \in \{i_0 + 1, \ldots, m\} & (F < F_{i_0+1} \leq F_i) & \Rightarrow & F_i \neq F \ . \end{cases}$$

Donc (E) est un raffinement propre de (F). On a ainsi construit un raffinement galoisien propre de (F) : contradiction, puisque (F) est de composition.

Inversement, supposons que toutes les marches de (F) soient galsimples. Elles sont donc en particulier toutes non triviales, et la tour (F) est stricte. Raisonnons par l'absurde en supposant l'existence d'un raffinement galoisien propre (E) de (F). D'après la proposition 1.7 du chapitre 3, c'est une tour galoisienne :

$$(E) \qquad K = E_0 = F_0 \trianglelefteq \cdots \trianglelefteq E_{j_i} = F_i \trianglelefteq \cdots \trianglelefteq E_j \trianglelefteq \cdots \trianglelefteq E_n = F_m = L \ .$$

De plus, par la définition et convention 1.1.(2) du chapitre 3, l'ensemble

$$\{j \in \{1, \ldots, n-1\} \quad | \quad \forall i \in \{0, \ldots, m\} \quad E_j \neq F_i\}$$

est non vide. Notons l son plus petit élément. Deux cas :
- ou bien $l-1=0$, $E_{l-1}=F_0$;
- ou bien $l-1\geq 1$ et par minimalité de l, il existe k dans $\{0,\dots,m\}$ tel que $E_{l-1}=F_k$.

Donc dans tous les cas

$$\exists k\in\{0,\dots,m\}\quad E_{l-1}=F_k\ .$$

On n'a pas $E_{l-1}=F_m$ car alors

$$F_m=E_{l-1}\leq E_l\leq L=F_m\quad\Rightarrow\quad E_l=F_m\text{ : contradiction.}$$

Donc

$$\exists k\in\{0,\dots,m-1\}\quad E_{l-1}=F_k\ .$$

Rappelons que $E_{j_{k+1}}=F_{k+1}$, et minorons à partir de là l'indice j_{k+1} :
- si $j_{k+1}\leq l-1$,

$$F_{k+1}=E_{j_{k+1}}\leq E_{l-1}=F_k<F_{k+1}\text{ (car }(F)\text{ est stricte) : absurde ;}$$

- si $j_{k+1}=l$, $F_{k+1}=E_l$: contradiction par définition de l.

On a donc nécessairement $j_{k+1}\geq l+1$, de sorte que

$$F_k=E_{l-1}<E_l\leq E_{l+1}\leq\cdots\leq E_{j_{k+1}}=F_{k+1}\ .$$

Retenons en particulier que

$$F_k=E_{l-1}<E_l<F_{k+1}\ .$$

Mais la marche E_l/E_{l-1} est galoisienne ((E) est une tour galoisienne) ; donc l'extension F_{k+1}/F_k n'est pas galsimple : contradiction. □

Le corollaire suivant prouve la compatibilité de la notion de tour de composition avec l'équivalence des tours galoisiennes.

Corollaire 1.4. *Soit L/K une extension galtourable et (T), (T') deux tours galoisiennes de L/K. On suppose que (T) et (T') sont équivalentes (cf. Déf. 1.1). Alors (T) est de composition si et seulement si (T') est de composition.*

Scholie. Nous montrerons qu'une extension galtourable n'admet une tour de composition galoisienne que lorsqu'elle est finie (cf. 2ème théorème de dissociation : Th. 4.2).

Démonstration. Posons

$$(T)\qquad K=T_0\trianglelefteq\cdots\trianglelefteq T_i\trianglelefteq T_{i+1}\trianglelefteq\cdots\trianglelefteq T_m=L\ ,$$

$$(T')\qquad K=T'_0\trianglelefteq\cdots\trianglelefteq T'_j\trianglelefteq T'_{j+1}\trianglelefteq\cdots\trianglelefteq T'_m=L\ .$$

Supposons que (T) ne soit pas de composition et prouvons qu'il en est ainsi de (T'). Par la proposition 1.3 précédente, au moins une marche de (T) n'est pas galsimple :

$$\exists i \in \{1, \ldots, m\} \qquad T_i \not\leftarrow T_{i-1} \ .$$

Ceci signifie, par définition de la galsimplicité (Chap. 2, Déf. 1.6.(2)),

- ou bien que $T_i = T_{i-1}$;
- ou bien qu'il existe un corps intermédiaire F tel que

$$T_{i-1} \lhd F < T_i \ ,$$

et donc, par la bijection de Krull classique,

$$Gal(T_i/T_{i-1}) \rhd_f Gal(T_i/F) \rhd \mathbb{1} \ .$$

On sait qu'il existe $\sigma \in S_m$ (Déf. 1.1) tel que

$$Gal(T_i/T_{i-1}) \xrightarrow{\sim} Gal(T'_{\sigma(i)}/T'_{\sigma(i)-1}) \ .$$

Donc

- ou bien, dans le premier cas, $T'_{\sigma(i)} = T'_{\sigma(i)-1}$;
- ou bien, dans le deuxième, l'image H de $Gal(T_i/F)$ par cet isomorphisme topologique est telle que

$$Gal(T'_{\sigma(i)}/T'_{\sigma(i)-1}) \rhd_f H \rhd \mathbb{1} \ .$$

On en déduit, par la réciproque de la bijection de Krull classique, la tour

$$T'_{\sigma(i)-1} \lhd T'^{H}_{\sigma(i)} < T'_{\sigma(i)} \ .$$

Dans les deux cas, (T') a une marche qui n'est pas galsimple, et par la proposition 1.3 précédente, (T') n'est pas de composition. □

Il arrive que l'on ne sache pas décider si une tour est stricte ou pas. Dans la quête de tours équivalentes strictes, la proposition suivante y remédie.

Proposition 1.5. *Soit L/K une extension galtourable. Pour toutes tours galoisiennes de L/K*

$$(F) \qquad K = F_0 \trianglelefteq \cdots \trianglelefteq F_i \trianglelefteq \cdots \trianglelefteq F_m = L$$

et

$$(E) \qquad K = E_0 \trianglelefteq \cdots \trianglelefteq E_k \trianglelefteq \cdots \trianglelefteq E_n = L$$

équivalentes, les tours strictes associées (Chap. 3, Prop. & Déf. 2.1)

$$(F_<) \qquad K = F_0 = F_{<0} \lhd \cdots \lhd F_{<j} \lhd \cdots \lhd F_{<m'} = F_m = L$$

et

$$(E_<) \qquad K = E_0 = E_{<0} \lhd \cdots \lhd E_{<l} \lhd \cdots \lhd E_{<n'} = E_n = L$$

sont équivalentes.

Démonstration. On sait déjà, par le corollaire 2.6 du chapitre 3, que $(E_<)$ et $(F_<)$ sont bien des tours galoisiennes (ce qui justifie leur notation dans l'énoncé). Il nous reste ainsi à montrer qu'elles sont équivalentes. Pour cela, prouvons que pour tout j dans $\{1,\dots,m'\}$, il existe un unique entier i_j dans $\{1,\dots,m\}$ tel que l'on ait

$$F_{<j} = F_{i_j} \qquad \text{et} \qquad F_{<j-1} = F_{i_j-1} \ .$$

L'existence d'entiers vérifiant l'une ou l'autre condition est claire. Examinons tout d'abord l'existence et l'unicité d'un entier vérifiant les deux conditions simultanément.

Soit $j \in \{1,\dots,m'\}$ quelconque mais fixé. Dans la démonstration du Fait 2.5 du chapitre 3, on a vu que l'entier

$$i_j := min\{i \in \{0,\dots,m\} \ \mid \ F_i = F_{<j}\}$$

(toujours ≥ 1) convient. Prenons un entier $i' \in \{1,\dots,m\}$ convenant également. La première condition assure que $F_{i'} = F_{<j}$, et la minimalité de i_j fournit alors

$$i_j \leq i' \ .$$

Dès lors, si $i_j \neq i'$, on a $i_j \leq i' - 1$; et par croissance de (F) et stricte croissance de $(F_<)$

$$F_{<j-1} < F_{<j} = F_{i_j} \leq F_{i'-1} \ .$$

Mais $F_{<j-1} < F_{i'-1}$ signifie en particulier que i' ne convient pas. C'est donc que $i_j = i'$. Comme par définition $F_{i_j-1} = F_{<j-1} < F_{<j} = F_{i_j}$, nous pouvons considérer l'application

$$\begin{array}{rccc} \Phi_F \ : & \{1,\dots,m'\} & \longrightarrow & \{i \in \{1,\dots,m\} \ \mid \ F_i \neq F_{i-1}\} \\ & j & \longmapsto & \Phi_F(j) := i_j \ . \end{array}$$

On a

$$\forall j \in \{1,\dots,m'\} \quad F_{\Phi_F(j)} = F_{<j} \ , \quad F_{\Phi_F(j)-1} = F_{<j-1} \ .$$

Montrons maintenant que Φ_F est une bijection.

∘ *Φ_F est injective :*

Comme l'ensemble de départ de Φ_F est totalement ordonné, il nous suffit de prouver que Φ_F est strictement croissante. Puisque la tour $(F_<)$ est stricte

$$\begin{array}{rcccc} j < j' & \Rightarrow & F_{<j} & < & F_{<j'} \\ & & || & & || \\ & \Leftrightarrow & F_{\Phi_F(j)} & < & F_{\Phi_F(j')}. \end{array}$$

Ceci implique

$$\Phi_F(j) < \Phi_F(j') \ .$$

En effet, si $\Phi_F(j') \leq \Phi_F(j)$, on aurait par la croissance de $\{F_i\}_{\{0\leq i\leq m\}}$,

$$F_{\Phi_F(j')} \leq F_{\Phi_F(j)} \quad : \quad \text{contradiction.}$$

En résumé

$$j < j' \quad \Rightarrow \quad \Phi_F(j) < \Phi_F(j') \ ,$$

ce qui prouve l'injectivité de Φ_F.

∘ Φ_F *est surjective :*
Soit un entier i quelconque mais fixé dans $\{1,\dots,m\}$ tel que $F_i \neq F_{i-1}$. Comme (F) raffine $(F_<)$ trivialement (Chap. 3, Prop. & Déf. 2.1), on a, par la condition (RAFT) (Chap. 3, Déf 1.3.(2))

$$\exists j \in \{0,\dots,m'\} \quad F_i = F_{<j} \ .$$

Observons tout d'abord que j ne peut être nul. En effet

$$j=0 \quad \Rightarrow \quad K = F_0 \leq F_{i-1} < F_i = F_{<0} = K \quad \Rightarrow \quad K < K \quad : \quad \text{contradiction.}$$

C'est donc que $j \in \{1,\dots,m'\}$. On peut ainsi considérer son image par Φ_F : soit $i_j := \Phi_F(j)$. Par définition de $\Phi_F(j)$, $F_{i_j} \neq F_{i_j-1}$ et $F_{i_j} = F_{<j} = F_i$. Supposons que les entiers i_j et i soient différents. Deux cas se présentent :

– ou bien

$$i_j < i \quad \Leftrightarrow \quad i_j \leq i-1 \quad \Rightarrow \quad F_{i_j} \leq F_{i-1} < F_i = F_{i_j} \ : \ \text{absurde} \, ;$$

– ou bien

$$i < i_j \quad \Leftrightarrow \quad i \leq i_j - 1 \quad \Rightarrow \quad F_i \leq F_{i_j-1} < F_{i_j} = F_i \ : \ \text{absurde.}$$

On vient bien de montrer que $i = i_j = \Phi_F(j)$. Ceci étant vrai pour tout i dans $\{1,\dots,m\}$ tel que $F_i \neq F_{i-1}$, on a prouvé la surjectivité de Φ_F.

Nous avons besoin pour la suite de l'analogue pour E de Φ_F, à savoir la bijection Φ_E définie par

$$\begin{array}{rccc} \Phi_E \ : & \{1,\dots,n'\} & \longrightarrow & \{k \in \{1,\dots,n\} \mid E_k \neq E_{k-1}\} \\ & l & \longmapsto & \Phi_E(l) := k_l \end{array}$$

où k_l est l'unique entier vérifiant

$$E_{k_l} = E_{<l} \qquad \text{et} \qquad E_{k_l-1} = E_{<l-1} \ .$$

Nous avons fait l'hypothèse que les tours galoisiennes (E) et (F) sont équivalentes : $(E) \sim (F)$, ce qui signifie (Déf. 1.1.(2)) que $m = n$ et

$$\exists \sigma \in S_m \quad \forall i \in \{1,\dots,m=n\} \quad Gal(F_i/F_{i-1}) \xrightarrow{\sim} Gal(E_{\sigma(i)}/E_{\sigma(i)-1}) \ .$$

Pour prouver que $(E_<) \sim (F_<)$, notons tout d'abord le banal, mais décisif, argument de théorie de Galois :

$$\begin{array}{rcl} F_i/F_{i-1} \text{ non triviale} & \Leftrightarrow & Gal(F_i/F_{i-1}) \neq \mathbb{1} \\ & \Leftrightarrow & Gal(E_{\sigma(i)}/E_{\sigma(i)-1}) \neq \mathbb{1} \\ & \Leftrightarrow & E_{\sigma(i)}/E_{\sigma(i)-1} \text{ non triviale.} \end{array}$$

Nous pouvons donc considérer la restriction $\sigma_|$ de σ aux marches non triviales :

$$\begin{array}{rccc} \sigma_| \ : & \{i \in \{1,\dots,m=n\} \mid F_i \neq F_{i-1}\} & \longrightarrow & \{k \in \{1,\dots,n\} \mid E_k \neq E_{k-1}\} \\ & i & \longmapsto & \sigma(i) \ . \end{array}$$

Puisque σ est surjective, l'équivalence ci-dessus assure que $\sigma_|$ est également surjective. L'injectivité de $\sigma_|$ est une conséquence directe de celle de σ. Par conséquent, $\sigma_|$ est aussi une bijection.

Considérons dès lors le composé des bijections

$$\begin{array}{rccc} \tau := \Phi_E^{-1} \circ \sigma_| \circ \Phi_F \ : & \{1,\dots,m'\} & \longrightarrow & \{1,\dots,n'\} \\ & j & \longmapsto & (\Phi_E^{-1} \circ \sigma_| \circ \Phi_F)(j) \ . \end{array}$$

Comme τ est encore une bijection, on a en particulier $m' = n'$ et $\tau \in S_{m'}$.
Ainsi, par les conditions que vérifie $\Phi_F(j)$ et la propriété de définition de σ, on a pour tout $j \in \{1,\dots,m'\}$

$$Gal(F_{<j} = F_{\Phi_F(j)}/F_{<j-1} = F_{\Phi_F(j)-1}) \xrightarrow{\sim} Gal(E_{\sigma(\Phi_F(j))}/E_{\sigma(\Phi_F(j))-1}) \ ,$$

et la marche étant non triviale

$$\begin{array}{rl} \xrightarrow{\sim} & Gal(E_{\sigma_|(\Phi_F(j))}/E_{\sigma_|(\Phi_F(j))-1}) \\ = & Gal(E_{\Phi_E(\Phi_E^{-1}\circ\sigma_|\circ\Phi_F(j))}/E_{\Phi_E(\Phi_E^{-1}\circ\sigma_|\circ\Phi_F(j))-1}). \end{array}$$

Enfin par les deux conditions que vérifie $\Phi_E(\Phi_E^{-1} \circ \sigma_| \circ \Phi_F(j))$

$$\begin{array}{rl} Gal(F_{<j}/F_{<j-1}) \xrightarrow{\sim} & Gal(E_{<\Phi_E^{-1}\circ\sigma_|\circ\Phi_F(j)}/E_{<\Phi_E^{-1}\circ\sigma_|\circ\Phi_F(j)-1}) \\ \xrightarrow{\sim} & Gal(E_{<\tau(j)}/E_{<\tau(j)-1}). \end{array}$$

Ceci prouve exactement que $(E_<) \sim (F_<)$. □

Corollaire 1.6. *Dans les notations de la proposition 1.5, toute marche non triviale de (F) est une marche de $(F_<)$.*

Démonstration. C'est ce qu'exprime la surjectivité de l'application Φ_F de la démonstration de la proposition 1.5. □

2. Le cas des extensions galoisiennes

Dans le cas particulier des extensions galoisiennes, les résultats auxquels nous voulons aboutir (cf. introduction du présent chapitre) sont des conséquences directes de leurs analogues pour les groupes. Les quatre propositions suivantes ne se limitent pas à des extensions finies.

Proposition 2.1. *Toute suite normale du groupe de Galois d'une extension galoisienne quelconque induit une tour galoisienne de cette extension. Précisément, soit $L \nearrow K$ une extension galoisienne de groupe $G := Gal(L/K)$. Pour tout suite normale*

$$(S) \qquad G = G_0 \trianglerighteq \cdots \trianglerighteq G_i \trianglerighteq G_{i+1} \trianglerighteq \cdots \trianglerighteq G_m = \mathbb{1} \ ,$$

posons $T_i := L^{G_i}$ $(i = 0, \ldots, m)$. *On a alors la tour galoisienne de* $L \nearrow K$

$$(T) \qquad K = T_0 \trianglelefteq \cdots \trianglelefteq T_i \trianglelefteq T_{i+1} \trianglelefteq \cdots \trianglelefteq T_m = L \ .$$

Nous disons que la tour galoisienne (T) *est induite par la suite normale* (S).

Démonstration. Que (T) soit une tour de L/K est trivial car

$$G_i \geq G_{i+1} \quad \Rightarrow \quad T_i = L^{G_i} \leq L^{G_{i+1}} = T_{i+1} \ .$$

Prouvons qu'elle est galoisienne. Par le (1) de la proposition 3.1 du chapitre 1

$$G_i \trianglerighteq G_{i+1} \quad \Rightarrow \quad \overline{G_i} \trianglerighteq \overline{G_{i+1}}$$

au sens de la topologie de Krull de G ; d'où

$$\overline{G_i} = Gal(L/L^{G_i}) \trianglerighteq Gal(L/L^{G_{i+1}}) = \overline{G_{i+1}}$$

i.e. $Gal(L/T_i) \trianglerighteq Gal(L/T_{i+1})$ ce qui signifie que l'extension T_{i+1}/T_i est galoisienne $(i = 0, \ldots, m-1)$. Toutes les marches de (T) étant galoisiennes, la tour (T) est galoisienne par définition (Chap. 2, Déf. & Conv. 1.1.(2)). □

Proposition 2.2. *Tout raffinement d'une suite normale du groupe de Galois d'une extension galoisienne induit un raffinement galoisien de la tour galoisienne correspondante de l'extension.*
Précisément, soient $L \nearrow K$ *une extension galoisienne quelconque de groupe* $G := Gal(L/K)$,

$$(S) \qquad G = G_0 \trianglerighteq \cdots \trianglerighteq G_i \trianglerighteq G_{i+1} \trianglerighteq \cdots \trianglerighteq G_m = \mathbb{1}$$

une suite normale de G, *et*

$$(T) \qquad K = T_0 \trianglelefteq \cdots \trianglelefteq T_i \trianglelefteq T_{i+1} \trianglelefteq \cdots \trianglelefteq T_m = L$$

la tour galoisienne de L/K *induite par* (S) *(Prop. 2.1). Pour tout raffinement*

$$(S') \qquad G = G'_0 \trianglerighteq \cdots \trianglerighteq G'_j \trianglerighteq G'_{j+1} \trianglerighteq \cdots \trianglerighteq G'_{m'} = \mathbb{1}$$

de (S) *(cf.* [**34**, p.120]*), la tour galoisienne*

$$(T') \qquad K = T'_0 \trianglelefteq \cdots \trianglelefteq T'_j \trianglelefteq T'_{j+1} \trianglelefteq \cdots \trianglelefteq T'_{m'} = L$$

induite par (S') *est un raffinement galoisien (cf. Chap. 3, Déf. 1.3.(4)) de* (T).

Démonstration. Par définition d'un raffinement d'une suite normale de groupe, on a $m \leq m'$ et l'existence d'une suite d'entiers

$$0 \leq j_0 < j_1 < \cdots < j_m \leq m'$$

telle que

$$\forall i \in \{0, \ldots, m\} \qquad G_i = G'_{j_i} \ .$$

Dès lors, on a directement

$$\begin{array}{rccc} \forall i \in \{0,\dots,m\} & L^{G_i} & = & L^{G'_{j_i}} \\ & || & & || \\ & T_i & ==== & T'_{j_i} \, . \end{array}$$

Donc (T') raffine (T). Le Fait 1.5.(2) du chapitre 3 nous permet de conclure : la tour galoisienne (T') est un raffinement galoisien de (T). □

Le résultat précédent vient de ce que l'on a posé la définition d'un raffinement de tour de corps (au chapitre 3) de manière compatible, dans le cas d'une extension galoisienne, avec la définition bien connue d'un raffinement d'une suite normale de groupes. Cette compatibilité permet d'énoncer les réciproques des propositions 2.1 et 2.2.

Proposition 2.3. *(1) Toute tour galoisienne de corps d'une extension galoisienne induit une suite normale du groupe de Galois de cette extension.*
Précisément, soit $L\nearrow K$ une extension galoisienne quelconque. Pour toute tour galoisienne

$$(T) \qquad K = T_0 \trianglelefteq \cdots \trianglelefteq T_i \trianglelefteq T_{i+1} \trianglelefteq \cdots \trianglelefteq T_m = L$$

de L/K, on a, en posant $G_i := Gal(L/T_i)$ $(i = 0,\dots,m)$, la suite normale de groupes

$$(S) \qquad Gal(L/K) = G_0 \trianglerighteq \cdots \trianglerighteq G_i \trianglerighteq G_{i+1} \trianglerighteq \cdots \trianglerighteq G_m = \mathbb{1} \, .$$

Nous disons que la suite normale (S) est "induite" par la tour galoisienne (T).
(2) La suite normale (S) induite par le (1) induit à son tour une tour galoisienne par la proposition 2.1, qui n'est autre que la tour (T) initiale.

Démonstration. (1) Le résultat est une conséquence immédiate de la théorie de Galois générale :

$$\forall i \in \{0,\dots,m-1\} \qquad T_i \leq T_{i+1} \quad \Leftrightarrow \quad Gal(L/T_{i+1}) \leq Gal(L/T_i)$$

et

$$T_i \trianglelefteq T_{i+1} \quad \Leftrightarrow \quad Gal(L/T_{i+1}) \trianglelefteq Gal(L/T_i) \quad \Leftrightarrow \quad G_{i+1} \trianglelefteq G_i \, .$$

(2) Pour tout entier i dans $\{0,\dots,m\}$, L/T_i est galoisienne, comme sous-extension de $L\nearrow K$; donc

$$T_i = L^{Gal(L/T_i)} = L^{G_i} \, .$$

□

Proposition 2.4. *Soit $L\nearrow K$ une extension galoisienne de groupe $G := Gal(L/K)$. Tout raffinement galoisien de $L\nearrow K$ induit un raffinement de la suite normale*

correspondante.
Précisément : soient

$$(T) \qquad K = T_0 \trianglelefteq \cdots \trianglelefteq T_i \trianglelefteq T_{i+1} \trianglelefteq \cdots \trianglelefteq T_m = L$$

une tour galoisienne de $L \nearrow K$ *et*

$$(T') \qquad K = T'_0 \trianglelefteq \cdots \trianglelefteq T'_j \trianglelefteq T'_{j+1} \trianglelefteq \cdots \trianglelefteq T'_{m'} = L$$

un raffinement galoisien de (T)*. Alors la suite normale*

$$(S') \qquad G = G'_0 \trianglerighteq \cdots \trianglerighteq G'_j \trianglerighteq G'_{j+1} \trianglerighteq \cdots \trianglerighteq G'_{m'} = \mathbb{1}$$

induite par (T') *(cf. Prop. 2.3.(1)) est un raffinement de*

$$(S) \qquad G = G_0 \trianglerighteq \cdots \trianglerighteq G_i \trianglerighteq G_{i+1} \trianglerighteq \cdots \trianglerighteq G_m = \mathbb{1}$$

induite par (T)*.*

Démonstration. D'après la proposition 1.7 du chapitre 3, (T') est une tour galoisienne de $L \nearrow K$. Par définition d'un raffinement d'une tour de corps (Chap. 3, Déf. & Conv. 1.1.(1)), on a $m \leq m'$ et l'existence d'une suite d'indices

$$0 \leq j_0 < j_1 < \cdots < j_m \leq m'$$

telle que

$$\forall i \in \{0, \ldots, m\} \qquad T_i = T'_{j_i} \ .$$

D'où par définition

$$\begin{array}{lccc} \forall i \in \{0, \ldots, m\} & Gal(L/T_i) & = & Gal(L/T'_{j_i}) \\ & \| & & \| \\ & G_i & ==== & G'_{j_i} \ . \end{array}$$

□

Corollaire 2.5. *Soit* $L \nearrow K$ *une extension galoisienne de groupe* $G := Gal(L/K)$*. Pour tout raffinement galoisien propre* (T') *d'une tour galoisienne* (T) *de* $L \nearrow K$*, la suite normale* (S') *de* G *induite par* (T') *(cf. Prop. 2.3.) est un raffinement propre de la suite normale* (S) *induite par* (T)*.*

Démonstration. La proposition 2.4 assure déjà que (S') est un raffinement de (S). De plus, dans les mêmes notations, on a, par définition d'un raffinement propre de tour de corps (Chap. 3, Déf. & Conv. 1.1.(2)), la condition

$$\exists j \in \{1, \ldots, m' - 1\} \quad \forall i \in \{0, \ldots, m\} \quad T'_j \neq T_i \ .$$

Or d'après le (1) de la proposition 2.3, $G_i := Gal(L/T_i)$, d'où

$$T_i = L^{G_i} \quad (i = 0, \ldots, m) \ .$$

De même

$$T'_j = L^{G'_j} \quad (j = 0, \ldots, m') \ .$$

Donc directement

$$\exists j \in \{1, \dots, m'-1\} \quad \forall i \in \{0, \dots, m\} \quad G'_j \neq G_i \ .$$

□

Dans le cas d'une extension galoisienne finie, on peut compléter les résultats précédents grâce à la bijection de Galois.

Proposition 2.6. *Soit $L \nearrow K$ une extension galoisienne finie de groupe $G := Gal(L/K)$.*

(1) Pour toute suite normale stricte

$$(S) \qquad G = G_0 \rhd \cdots \rhd G_i \rhd G_{i+1} \rhd \cdots \rhd G_m = \mathbb{1} \ ,$$

la tour galoisienne (T) induite par (S) (cf. Prop. 2.1) est stricte.

(2) Pour tout raffinement propre (S') d'une suite normale (S) de G, la tour (T') induite par (S') est un raffinement galoisien propre de la tour (T) induite par (S).

(3) Pour toute suite normale (S) de (G), la suite normale de G induite par la tour galoisienne de $L \nearrow K$ induite par (S) est égale à (S).

Démonstration. (1) Par la bijection classique de Galois :

$$G_i \neq G_{i+1} \quad \Rightarrow \quad T_i = L^{G_i} \neq L^{G_{i+1}} = T_{i+1} \qquad (i = 0, \dots, m-1) \ .$$

(2) D'après la proposition 2.2, (T') est un raffinement de (T). On a, par définition d'un raffinement propre d'une suite normale, la condition

$$\exists j \in \{1, \dots, n-1\} \quad \forall i \in \{0, \dots, m\} \quad G'_j \neq G_i \ .$$

Et par la bijection classique de Galois,

$$\begin{array}{lllll} \exists j \in \{1, \dots, n-1\} & \forall i \in \{0, \dots, m\} & L^{G'_j} & \neq & L^{G_i} \\ & & \| & & \| \\ & & T'_j & & T_i \ . \end{array}$$

Par définition et le théorème d'Artin dans l'extension finie $L \nearrow K$, on a

$$Gal(L/T_i) = Gal(L/L^{G_i}) = G_i \qquad (i = 0, \dots, m) \ .$$

□

Nous faisons maintenant le lien entre la notion de groupe simple et la notion d'extension galsimple, toujours dans le cas d'une extension galoisienne finie.

Proposition 2.7. *Pour qu'une extension galoisienne finie soit galsimple (cf. Chap. 2, Déf. 1.6.(2)), il faut et il suffit que son groupe de Galois soit simple.*

Démonstration. Soit $L \nearrow K$ une extension galoisienne finie de groupe de Galois $G := Gal(L/K)$. Supposons $L \nearrow K$ galsimple. Par définition, elle n'est pas triviale et $G \neq \mathbb{1}$ car sinon

$$K = L^{Gal(L/K)} = L^G = L^{\mathbb{1}} = L \ : \text{ contradiction .}$$

Raisonnons par l'absurde en supposant que G ne soit pas simple, i.e. qu'il existe un sous-groupe H de G tel que l'on ait la suite normale stricte $G \rhd H \rhd \mathbb{1}$. Le (1) de la proposition 2.6 ci-dessus nous assure alors que l'on a la tour galoisienne stricte

$$K \lhd L^H \lhd L$$

qui contredit la galsimplicité de L/K.

Inversement, si G est simple, on sait que $G \neq \mathbb{1}$ et donc que $L \neq K$. Raisonnons à nouveau par l'absurde en supposant que L/K ne soit pas galsimple. C'est qu'il existe un corps intermédiaire strict $K < M < L$ avec M/K galoisienne. Alors, par la théorie de Galois générale et la simplicité de G,

$$Gal(L/M) \trianglelefteq G \quad \Rightarrow \quad \Big(\ Gal(L/M) = G \text{ ou } Gal(L/M) = \mathbb{1} \ \Big) \ .$$

Mais, si $Gal(L/M) = G$, on a

$$M = L^{Gal(L/M)} = L^G = L^{Gal(L/K)} = K \ : \text{ contradiction ;}$$

et si $Gal(L/M) = \mathbb{1}$,

$$M = L^{Gal(L/M)} = L^{\mathbb{1}} = L \ : \text{ contradiction .}$$

C'est donc que l'extension L/K est galsimple. □

Dans le cas d'une extension galoisienne, les propositions précédentes font le lien entre tours galoisiennes de corps et suites normales de groupes, avec leurs raffinements. La correspondance se poursuit, dans le cas fini, entre tours de composition galoisiennes et suites de composition.

Proposition 2.8. *Toute extension galoisienne finie admet une tour de composition galoisienne.*

Démonstration. C'est clair pour l'extension triviale par le Fait 1.2. Soit L/K une extension galoisienne finie non triviale de groupe $G := Gal(L/K)$. En tant que groupe fini non trivial, il admet une suite normale de composition :

$$(C) \qquad G = G_0 \rhd \cdots \rhd G_i \rhd G_{i+1} \rhd \cdots \rhd G_m = \mathbb{1} \ .$$

Montrons que la tour galoisienne induite par (C) (Prop. 2.1)

$$(T) \qquad K = T_0 \trianglelefteq \cdots \trianglelefteq T_i \trianglelefteq T_{i+1} \trianglelefteq \cdots \trianglelefteq T_m = L$$

est une tour de composition de L/K. Le (1) de la proposition 2.6 nous assure que la tour (T) est stricte. Raisonnons par l'absurde en supposant l'existence d'un raffinement galoisien propre

$$(T') \qquad K = T'_0 \trianglelefteq \cdots \trianglelefteq T'_j \trianglelefteq T'_{j+1} \trianglelefteq \cdots \trianglelefteq T'_{m'} = L$$

de (T). Par le corollaire 2.5, il induit un raffinement propre (C') de (C), ce qui contredit le fait que (C) soit une suite normale de composition. □

Les propositions précédentes conduisent directement à un analogue galoisien du théorème de Schreier (cf. introduction de ce chapitre) pour une extension galoisienne finie. Cependant, comme cet analogue sera généralisé à toutes les extensions galtourables (cf. Th. 3.2), nous omettons ici sa démonstration dans ce cas particulier.

Proposition 2.9. *Deux tours galoisiennes d'une même extension galoisienne finie admettent des raffinements galoisiens équivalents.*

Remarque 2.10. Dans le cas particulier d'une extension abélienne, cette proposition 2.9 permet de retrouver la proposition 2.2 de [**13**] qui fournit en outre la hauteur des tours de composition.

3. Premier théorème de dissociation

Venons-en maintenant, pour les extensions galtourables, à l'analogue galoisien du théorème de Schreier (cf. introduction du présent chapitre). La démonstration moderne de l'équivalence des raffinements de Schreier utilise le lemme de Zassenhaus ("Butterfly lemma"). Nous allons montrer que ce sont les parallélogrammes galoisiens qui jouent, pour les extensions galtourables, le rôle du lemme de Zassenhaus pour les groupes. Ces parallélogrammes ont de plus l'avantage de rendre visuel l'esprit de la démonstration. Pour une meilleure lisibilité de celle-ci, nous avons sorti la proposition suivante qui est en fait un lemme technique.

Proposition 3.1. *Soient L/K une extension galtourable de degré quelconque, et*

$$(T^1) \qquad K = T^1_0 \trianglelefteq \cdots \trianglelefteq T^1_i \trianglelefteq T^1_{i+1} \trianglelefteq \cdots \trianglelefteq T^1_m = L$$

$$(T^2) \qquad K = T^2_0 \trianglelefteq \cdots \trianglelefteq T^2_j \trianglelefteq T^2_{j+1} \trianglelefteq \cdots \trianglelefteq T^2_n = L$$

deux tours galoisiennes de L/K. Alors nécessairement :
(1) Pour tous indices i, j, k tels que $0 \leq i \leq m-1$ et $0 \leq k < j \leq n-1$, on a le parallélogramme galoisien

$$[T^1_{i+1}T^2_k \cap T^1_i T^2_j, T^1_{i+1}T^2_{k+1} \cap T^1_i T^2_j, T^1_{i+1}T^2_{k+1} \cap T^1_i T^2_{j+1}, T^1_{i+1}T^2_k \cap T^1_i T^2_{j+1}] \,.$$

En particulier, on a les isomorphismes de restriction

$$Gal(T^1_{i+1}T^2_{k+1} \cap T^1_i T^2_{j+1}/T^1_{i+1}T^2_{k+1} \cap T^1_i T^2_j)$$

$$\downarrow \wr$$

$$Gal(T^1_{i+1}T^2_k \cap T^1_i T^2_{j+1}/T^1_{i+1}T^2_k \cap T^1_i T^2_j)\ .$$

(2) Pour tous i, j, k tels que $0 \leq k < i \leq m-1$ et $0 \leq j \leq n-1$, on a le parallélogramme

$$[T^1_k T^2_{j+1} \cap T^1_i T^2_j, T^1_{k+1}T^2_{j+1} \cap T^1_i T^2_j, T^1_{k+1}T^2_{j+1} \cap T^1_{i+1}T^2_j, T^1_k T^2_{j+1} \cap T^1_{i+1}T^2_j]\ .$$

En particulier on a les isomorphismes de restriction

$$Gal(T^1_{k+1}T^2_{j+1} \cap T^1_{i+1}T^2_j/T^1_{k+1}T^2_{j+1} \cap T^1_i T^2_j)$$

$$\downarrow \wr$$

$$Gal(T^1_k T^2_{j+1} \cap T^1_{i+1}T^2_j/T^1_k T^2_{j+1} \cap T^1_i T^2_j)\ .$$

Démonstration. (1) De l'extension galoisienne $T^1_{i+1} \nearrow T^1_i$, on déduit du corollaire 2.2 du chapitre 2 l'extension galoisienne $(T^1_{i+1}T^2_k \nearrow T^1_i T^2_k)$. Or

$$T^1_i T^2_k \leq T^1_{i+1}T^2_k \cap T^1_i T^2_{k+1} \leq T^1_{i+1}T^2_k\ ;$$

d'où la sous-extension galoisienne $(T^1_{i+1}T^2_k \nearrow T^1_{i+1}T^2_k \cap T^1_i T^2_{k+1})$. De même, on a les implications

$$(T^2_{k+1} \nearrow T^2_k) \ \Rightarrow\ (T^1_i T^2_{k+1} \nearrow T^1_i T^2_k) \ \Rightarrow\ (T^1_i T^2_{k+1} \nearrow T^1_{i+1}T^2_k \cap T^1_i T^2_{k+1})\ .$$

Comme $T^1_{i+1}T^2_k T^1_i T^2_{k+1} = T^1_{i+1}T^2_{k+1}$, on a donc le parallélogramme galoisien

$$P(i,k) := [T^1_{i+1}T^2_k \cap T^1_i T^2_{k+1}\ ,\ T^1_i T^2_{k+1}\ ,\ T^1_{i+1}T^2_{k+1}\ ,\ T^1_{i+1}T^2_k]\ .$$

Par ailleurs, de l'hypothèse $k < j$, i.e. $k+1 \leq j$, suit $T^2_{k+1} \leq T^2_j$, d'où $T^1_i T^2_{k+1} \leq T^1_i T^2_j$. Donc également

$$T^1_{i+1}T^2_k \cap T^1_i T^2_{k+1} \leq T^1_{i+1}T^2_k \cap T^1_i T^2_j\ .$$

Comme $T^1_i T^2_{k+1} \leq T^1_{i+1}T^2_{k+1}$, on en tire aussi

$$T^1_i T^2_{k+1} \leq T^1_{i+1}T^2_{k+1} \cap T^1_i T^2_j\ .$$

De plus

$$(T^1_{i+1}T^2_{k+1} \cap T^1_i T^2_j) \cap T^1_{i+1}T^2_k = T^1_{i+1}T^2_k \cap T^1_i T^2_j$$

$$\Big(\ \text{resp. } (T^1_{i+1}T^2_{k+1} \cap T^1_i T^2_{j+1}) \cap T^1_{i+1}T^2_k = T^1_{i+1}T^2_k \cap T^1_i T^2_{j+1}\ \Big).$$

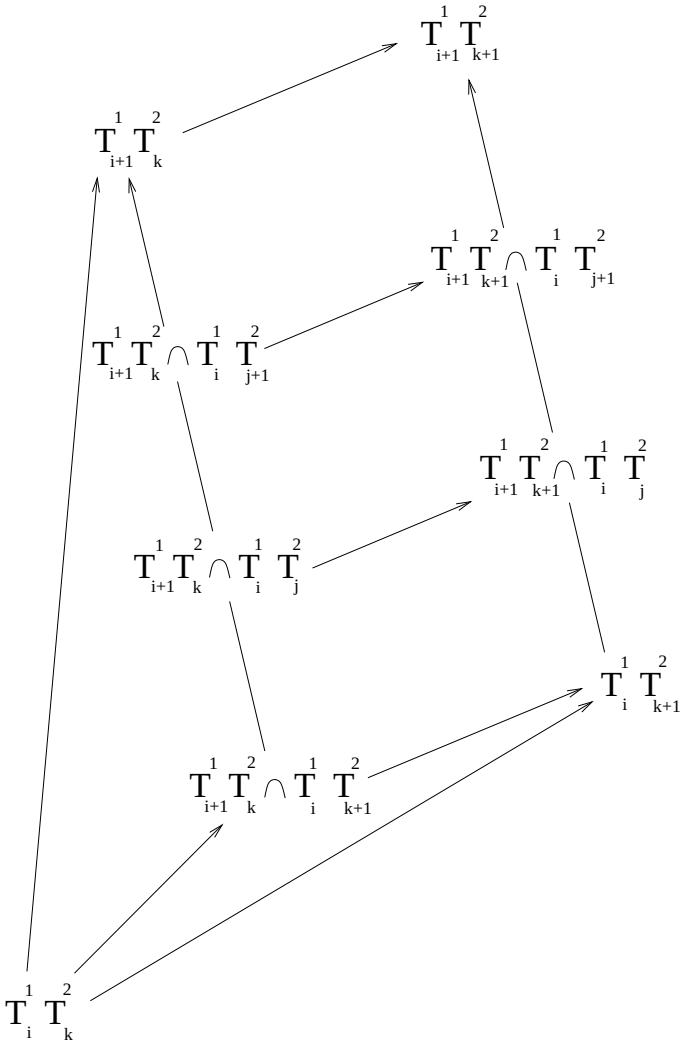

FIG. 17. *Parallélogrammes $P(i,j,k)$ et $Q(i,j,k)$*

On déduit alors du corollaire 4.3.(2-1) du chapitre 1 que l'on a le sous-parallélogramme galoisien de $P(i,k)$:

$$\begin{array}{c} P(i,j,k) \\ \vdots\vdots \\ \| \\ \left[T^1_{i+1}T^2_k \cap T^1_i T^2_j, T^1_{i+1}T^2_{k+1} \cap T^1_i T^2_j, T^1_{i+1}T^2_{k+1}, T^1_{i+1}T^2_k\right] \end{array}$$

$$\left(\text{ resp. } \begin{array}{c} P(i,j+1,k) \\ \vdots\vdots \\ \| \\ \left[T^1_{i+1}T^2_k \cap T^1_i T^2_{j+1}, T^1_{i+1}T^2_{k+1} \cap T^1_i T^2_{j+1}, T^1_{i+1}T^2_{k+1}, T^1_{i+1}T^2_k\right] \end{array} \right).$$

Prouvons maintenant, par récurrence descendante sur $k \in \{j-1, \ldots, 0\}$ que l'on a le parallégramme galoisien quotient

$$\begin{array}{c} Q(i,j,k) \\ \vdots \\ \| \\ \left[T^1_{i+1}T^2_k \cap T^1_i T^2_j, T^1_{i+1}T^2_{k+1} \cap T^1_i T^2_j, T^1_{i+1}T^2_{k+1} \cap T^1_i T^2_{j+1}, T^1_{i+1}T^2_k \cap T^1_i T^2_{j+1}\right] \end{array} .$$

Rang $k = j-1$.
Par le corollaire 2.2 du chapitre 2, on a l'implication

$$\left(\ (T^2_{j+1} = T^2_{k+2}) \nearrow T^2_{k+1} \right) \quad \Rightarrow \quad (T^1_i T^2_{j+1} \nearrow T^1_i T^2_{k+1}) \ .$$

De $T^1_{i+1}T^2_{k+1} \nearrow T^1_i T^2_{k+1}$ suit donc par intersection

$$(T^1_{i+1}T^2_{k+1} \cap T^1_i T^2_{j+1}) \nearrow (T^1_i T^2_{k+1} = T^1_{i+1}T^2_{k+1} \cap T^1_i T^2_j) \ .$$

Par le corollaire 4.3.(2-2) du chapitre 1, appliqué dans le sous-parallélogramme $P(i,j,k)$, on en déduit alors l'existence du parallélogramme galoisien quotient $Q(i,j,k)$.

Rang $k-1$.
Supposons l'existence du parallélogramme $Q(i,j,k)$ (avec $k \geq 1$) et prouvons celle de $Q(i,j,k-1)$. De la donnée de $Q(i,j,k)$ suit en particulier l'extension galoisienne

$$(T^1_{i+1}T^2_k \cap T^1_i T^2_{j+1}) \nearrow (T^1_{i+1}T^2_k \cap T^1_i T^2_j) \ .$$

L'existence de $Q(i,j,k-1)$ se déduit alors du corollaire 4.3.(2-2) du chapitre 1 appliqué cette fois dans le sous parallélogramme $P(i,j,k-1)$ de $P(i,k-1)$.

La récurrence établissant l'existence des parallélogrammes quotients $Q(i,j,k)$ est donc prouvée. On en déduit en particulier l'isomorphisme annoncé.

(2) Il s'agit du (1) mutatis mutandis, par la permutation

$$\begin{pmatrix} T^1 & T^2 & i & j & k & m & n \\ T^2 & T^1 & j & i & k & n & m \end{pmatrix} .$$

□

Nous sommes maintenant en mesure de prouver l'analogue galoisien suivant au théorème de Schreier pour les suites normales de groupes ([**34**, p.124], [**36**]).

Théorème 3.2. *(1er théorème de dissociation, dit "de Galschreier")*
Deux tours galoisiennes d'une même extension galtourable admettent des raffinements qui sont des tours galoisiennes équivalentes.

Scholies. (1) Les extensions galtourables sont ici quelconques, de degré fini ou infini.
(2) Ces raffinements sont nécessairement galoisiens en vertu du Fait 1.5.(2) du chapitre 3.

Démonstration. Nous allons prouver que les tours galoisiennes (T^1) et (T^2) de la proposition 3.1 admettent des raffinements équivalents. En faisant varier k de $j-1$ à 0 dans le (1) de cette proposition, on a

$$\forall i \in \{0,\dots,m-1\} \quad \forall j \in \{1,\dots,n-1\}$$

$$\begin{array}{ccc} Gal(T^1_{i+1}T^2_j \cap T^1_i T^2_{j+1}/T^1_{i+1}T^2_j \cap T^1_i T^2_j) & = & Gal(T^1_{i+1}T^2_j \cap T^1_i T^2_{j+1}/T^1_i T^2_j) \\ \downarrow\wr & & \\ Gal(T^1_{i+1}T^2_{j-1} \cap T^1_i T^2_{j+1}/T^1_{i+1}T^2_{j-1} \cap T^1_i T^2_j) & & \\ \downarrow\wr & & \\ \vdots & & \\ \downarrow\wr & & \\ Gal(T^1_{i+1}T^2_0 \cap T^1_i T^2_{j+1}/T^1_{i+1}T^2_0 \cap T^1_i T^2_j) & = & Gal(T^1_{i+1} \cap T^1_i T^2_{j+1}/T^1_{i+1} \cap T^1_i T^2_j)\,. \end{array}$$

Retenons que pour tous $i \in \{0,\dots,m-1\}$ et $j \in \{1,\dots,n-1\}$, on a l'isomorphisme

$$isom^1_{(i,j)} : Gal(T^1_{i+1} \cap T^1_i T^2_{j+1}/T^1_{i+1} \cap T^1_i T^2_j) \xrightarrow{\sim} Gal(T^1_{i+1}T^2_j \cap T^1_i T^2_{j+1}/T^1_i T^2_j)\,.$$

De même, en faisant varier k de $i-1$ à 0 dans le (2) de la proposition 3.1, on a

$$\forall i \in \{1,\dots,m-1\} \quad \forall j \in \{0,\dots,n-1\}$$

$$\begin{array}{ccc} Gal(T^1_i T^2_{j+1} \cap T^1_{i+1}T^2_j/T^1_i T^2_{j+1} \cap T^1_i T^2_j) & = & Gal(T^1_i T^2_{j+1} \cap T^1_{i+1}T^2_j/T^1_i T^2_j) \\ \downarrow\wr & & \\ Gal(T^1_{i-1}T^2_{j+1} \cap T^1_{i+1}T^2_j/T^1_{i-1}T^2_{j+1} \cap T^1_i T^2_j) & & \\ \downarrow\wr & & \\ \vdots & & \\ \downarrow\wr & & \\ Gal(T^1_0 T^2_{j+1} \cap T^1_{i+1}T^2_j/T^1_0 T^2_{j+1} \cap T^1_i T^2_j) & = & Gal(T^2_{j+1} \cap T^1_{i+1}T^2_j/T^2_{j+1} \cap T^1_i T^2_j)\,. \end{array}$$

Retenons que pour tous $i \in \{1,\dots,m-1\}$ et $j \in \{0,\dots,n-1\}$, on a l'isomorphisme

$$isom^2_{(i,j)} : Gal(T^2_{j+1} \cap T^1_{i+1}T^2_j/T^2_{j+1} \cap T^1_i T^2_j) \xrightarrow{\sim} Gal(T^1_i T^2_{j+1} \cap T^1_{i+1}T^2_j/T^1_i T^2_j)\,.$$

D'où l'isomorphisme composé

$$isom_{(i,j)} := \begin{cases} (isom^2_{(i,j)})^{-1} \circ isom^1_{(i,j)} & \text{si } (i,j) \neq (0,0) \\ isom^1_{(i,j)} & \text{si } i = 0\,,\ j \neq 0 \\ (isom^2_{(i,j)})^{-1} & \text{si } i \neq 0\,,\ j = 0 \\ id_{Gal(T^1_1 \cap T^2_1/K)} & \text{si } (i,j) = (0,0) \end{cases}$$

Dans tous les cas, on a

$$isom_{(i,j)} \ : \quad Gal(T^1_{i+1} \cap T^1_i T^2_{j+1} / T^1_{i+1} \cap T^1_i T^2_j) \xrightarrow{\sim} Gal(T^2_{j+1} \cap T^1_{i+1} T^2_j / T^2_{j+1} \cap T^1_i T^2_j)\ .$$

Remarquons par division euclidienne que, pour tout $l \in \{0, \ldots, mn-1\}$, il existe un unique couple $(q^1_l, r^1_l) \in \{0, \ldots, m-1\} \times \{0, \ldots, n-1\}$ et un unique $(q^2_l, r^2_l) \in \{0, \ldots, n-1\} \times \{0, \ldots, m-1\}$ tels que

$$l = q^1_l n + r^1_l = q^2_l m + r^2_l\ .$$

Soient maintenant (T'^1) et (T'^2) les deux tours de L/K définies par les formules

$$(\mathfrak{F}) \begin{cases} \forall l \in \{0, \ldots, mn-1\} & T'^1_l := T^1_{q^1_l+1} \cap T^1_{q^1_l} T^2_{r^1_l}\ ; \\ & T'^2_l := T^2_{q^2_l+1} \cap T^1_{r^2_l} T^2_{q^2_l}\ ; \\ T'^1_{mn} := T^1_m \cap T^1_{m-1} T^2_n = L\ ; & T'^2_{mn} := T^2_n \cap T^1_m T^2_{n-1} = L\ . \end{cases}$$

Notons que

$$\begin{cases} \forall i \in \{0, \ldots, m-1\} & T^1_i = T^1_{i+1} \cap T^1_i K = T^1_{i+1} \cap T^1_i T^2_0 = T'^1_{in}\ ; \\ T^1_m = L = T'^1_{mn}\ . \end{cases}$$

La suite d'indices

$$0 \leq l^1_0 := 0 < l^1_1 := n < \cdots < l^1_i := in < \cdots < l^1_{m-1} := (m-1)n < l^1_m := mn \leq mn$$

est donc telle que

$$\forall i \in \{0, \ldots, m\} \qquad T'^1_{l_i} = T^1_i\ ;$$

et

$$(T'^1) \qquad K = T'^1_0 \leq T'^1_1 \leq \cdots \leq T'^1_l \leq \cdots \leq T'^1_{mn-1} \leq T'^1_{mn} = L$$

est un raffinement de la tour (T^1) de l'énoncé au sens de la définition & convention 1.1 du chapitre 3. De même, notons que

$$\begin{cases} \forall j \in \{0, \ldots, n-1\} & T^2_j = T^2_{j+1} \cap K T^2_j = T^2_{j+1} \cap T^1_0 T^2_j = T'^2_{jm}\ ; \\ T^2_n = L = T'^2_{nm}\ . \end{cases}$$

La suite d'indices

$$0 \leq l_0^2 := 0 < l_1^2 := m < \cdots < l_j^2 := jm < \cdots < l_{n-1}^2 := (n-1)m < l_n^2 := nm \leq nm$$

est donc telle que

$$\forall j \in \{0, \ldots, n\} \qquad T'^2_{l_j} = T^2_j \ .$$

Et on vient de montrer que (T'^2) raffine (T^2).

Par le (1) (resp. le (2)) de la proposition 3.1 pour $j \neq 0$ (resp. $j = 0$), on a la tour galoisienne

$$\begin{array}{lcl}
(T'^1) \quad K = T'^1_0 = & T^1_1 \cap T^1_0 T^2_0 & \trianglelefteq T'^1_1 = T^1_1 \cap T^1_0 T^2_1 \trianglelefteq \cdots \trianglelefteq T'^1_{n-1} = T^1_1 \cap T^1_0 T^2_{n-1} \\
& \trianglelefteq T^1_1 \cap T^1_0 T^2_n & \\
& \| & \\
& T^1_1 & \\
& \| & \\
T'^1_n = & T^1_2 \cap T^1_1 T^2_0 & \trianglelefteq T'^1_{n+1} = T^1_2 \cap T^1_1 T^2_1 \trianglelefteq \cdots \trianglelefteq T'^1_{2n-1} = T^1_2 \cap T^1_1 T^2_{n-1} \\
& \trianglelefteq T^1_2 \cap T^1_1 T^2_n & \\
& \| & \\
& T^1_2 & \\
& \| & \\
T'^1_{2n} = & T^1_3 \cap T^1_2 T^2_0 & \trianglelefteq T'^1_{2n+1} = T^1_3 \cap T^1_2 T^2_1 \trianglelefteq \cdots \trianglelefteq T'^1_{3n-1} = T^1_3 \cap T^1_2 T^2_{n-1} \\
& \vdots & \\
& \vdots & \\
& \trianglelefteq T^1_i \cap T^1_{i-1} T^2_n & \\
& \| & \\
& T^1_i & \\
& \| & \\
T'^1_{in} = & T^1_{i+1} \cap T^1_i T^2_0 & \trianglelefteq T'^1_{in+1} = T^1_{i+1} \cap T^1_i T^2_1 \trianglelefteq \ldots \\
& & \cdots \trianglelefteq T'^1_{(i+1)n-1} = T^1_{i+1} \cap T^1_i T^2_{n-1} \\
& \vdots & \\
& \| & \\
& T^1_{m-1} & \\
& \| & \\
T'^1_{(m-1)n} = & T^1_m \cap T^1_{m-1} T^2_0 & \trianglelefteq T'^1_{(m-1)n+1} = T^1_m \cap T^1_{m-1} T^2_1 \trianglelefteq \ldots \\
& & \cdots \trianglelefteq T'^1_{mn-1} = T^1_m \cap T^1_{m-1} T^2_{n-1} \\
& \trianglelefteq T^1_m \cap T^1_{m-1} T^2_n & = T'^1_{mn} = L \ .
\end{array}$$

De même par le (2) (resp. le (1)) de la proposition 3.1 pour $i \neq 0$ (resp. $i = 0$), on a la tour galoisienne

$$
\begin{array}{lccl}
(T'^2) \quad K = T'^2_0 = & T_1^2 \cap T_0^1 T_0^2 & \trianglelefteq T'^2_1 = T_1^2 \cap T_1^1 T_0^2 \trianglelefteq \cdots \trianglelefteq T'^2_{m-1} = T_1^2 \cap T_{m-1}^1 T_0^2 \\
& \trianglelefteq T_1^2 \cap T_m^1 T_0^2 & \\
& \| & \\
& T_1^2 & \\
& \| & \\
T'^2_m = & T_2^2 \cap T_0^1 T_1^2 & \trianglelefteq T'^2_{m+1} = T_2^2 \cap T_1^1 T_1^2 \trianglelefteq \cdots \trianglelefteq T'^2_{2m-1} = T_2^2 \cap T_{m-1}^1 T_1^2 \\
& \trianglelefteq T_2^2 \cap T_m^1 T_1^2 & \\
& \| & \\
& T_2^2 & \\
& \| & \\
T'^2_{2m} = & T_3^2 \cap T_0^1 T_2^2 & \trianglelefteq T'^2_{2m+1} = T_3^2 \cap T_1^1 T_2^2 \trianglelefteq \cdots \trianglelefteq T'^2_{3m-1} = T_3^2 \cap T_{m-1}^1 T_2^2 \\
& \vdots & \\
& \vdots & \\
& \trianglelefteq T_j^2 \cap T_m^1 T_{j-1}^2 & \\
& \| & \\
& T_j^2 & \\
& \| & \\
T'^2_{jm} = & T_{j+1}^2 \cap T_0^1 T_j^2 & \trianglelefteq T'^2_{jm+1} = T_{j+1}^2 \cap T_1^1 T_j^2 \trianglelefteq \ldots \\
& & \cdots \trianglelefteq T'^2_{(j+1)m-1} = T_{j+1}^2 \cap T_{m-1}^1 T_j^2 \\
& \vdots & \\
& \| & \\
& T_{n-1}^2 & \\
& \| & \\
T'^2_{(n-1)m} = & T_n^2 \cap T_0^1 T_{n-1}^2 & \trianglelefteq T'^2_{(n-1)m+1} = T_n^2 \cap T_1^1 T_{n-1}^2 \trianglelefteq \ldots \\
& & \cdots \trianglelefteq T'^2_{nm-1} = T_n^2 \cap T_{m-1}^1 T_{n-1}^2 \\
& \trianglelefteq T_n^2 \cap T_m^1 T_{n-1}^2 & = T'^2_{mn} = L \, .
\end{array}
$$

Il reste à montrer que les tours (T'^1) et (T'^2) ainsi construites sont équivalentes (cf. Déf. 1.1). Elles ont même nombre de marches mn. Considérons ensuite l'application

$$
\begin{array}{rccl}
\sigma : & \{1, \ldots, mn\} & \longrightarrow & \{1, \ldots, mn\} \\
& l & \longmapsto & \sigma(l) := r_{l-1}^1 m + q_{l-1}^1 + 1
\end{array}
$$

où q^1_{l-1} et r^1_{l-1} sont définis, comme précédemment, par division euclidienne de $l-1$ par n :

$$l-1 = q^1_{l-1}n + r^1_{l-1} \qquad 0 \leq r^1_{l-1} \leq n-1 \ .$$

En particulier donc, $0 \leq q^1_{l-1} \leq m-1$, en sorte que $r^1_{l-1}m + q^1_{l-1}$ est une division euclidienne par m, ce qui assure l'injectivité, donc la bijectivité de l'application σ. Autrement dit, σ est un élément du groupe symétrique S_{mn}. Explicitement, σ est l'identité si $m=1$ ou $n=1$, et pour $m \geq 2$, $n \geq 2$:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n & n+1 & n+2 & \dots & 2n & \dots & mn \\ 1 & m+1 & \dots & (n-1)m+1 & 2 & m+2 & \dots & (n-1)m+2 & \dots & mn \end{pmatrix}.$$

Notons tout d'abord que $Gal(T'^1_{mn} = L/T'^1_{mn-1} = T^1_{m-1}T^2_{n-1}) = Gal(T'^2_{\sigma(mn)}/T'^2_{\sigma(mn)-1})$
Fixons-nous un $l \in \{1, \dots, mn-1\}$ avec toujours

$$l = q^1_l n + r^1_l \qquad (q^1_l, r^1_l) \in \{0, \dots, m-1\} \times \{0, \dots, n-1\} \ .$$

Envisageons deux cas.

1^{er} *cas :* $r^1_l = 0$.

Nécessairement $q^1_l \geq 1$ (sinon $l=0$: absurde). Alors de $l-1 = (q^1_l - 1)n + n - 1$ suit

$$q^1_{l-1} = q^1_l - 1, \quad r^1_{l-1} = n-1 \ .$$

d'où

$$\sigma(l) = (n-1)m + q^1_l \ .$$

On a déjà vu que

$$\forall i \in \{0, \dots, m-1\} \quad T'^1_{in} = T^1_i \ .$$

Donc, comme $T^2_n = L$,

$$T'^1_l = T'^1_{q^1_l n} = T^1_{q^1_l} = T^1_{q^1_l} \cap T^1_{q^1_l - 1}T^2_n \ .$$

Dès lors, par l'isomorphisme $isom_{(q^1_{l-1}, n-1)}$,

$$\begin{aligned} Gal(T'^1_l/T'^1_{l-1}) &= Gal(T^1_{q^1_l} \cap T^1_{q^1_l-1}T^2_n / T^1_{q^1_l} \cap T^1_{q^1_l-1}T^2_{n-1}) \\ &\xrightarrow{\sim} Gal(T^2_n \cap T^1_{q^1_l}T^2_{n-1} / T^2_n \cap T^1_{q^1_l-1}T^2_{n-1}) \\ &= Gal(T'^2_{(n-1)m+q^1_l} / T'^2_{(n-1)m+q^1_l-1}) \\ &= Gal(T'^2_{\sigma(l)} / T'^2_{\sigma(l)-1}) \ . \end{aligned}$$

2^{nd} *cas :* $r^1_l \geq 1$.

De $l-1 = q^1_l n + r^1_l - 1$ suit alors

$$q^1_{l-1} = q^1_l \ , \quad r^1_{l-1} = r^1_l - 1 \ ;$$

d'où

$$\sigma(l) = (r^1_l - 1)m + q^1_l + 1 \ .$$

On en déduit par l'isomorphisme $isom_{(q^1_{l-1},r^1_{l-1})}$ que

$$\begin{aligned} Gal(T'^1_l/T'^1_{l-1}) &= Gal(T^1_{q^1_l+1}\cap T^1_{q^1_l}T^2_{r^1_l}/T^1_{q^1_l+1}\cap T^1_{q^1_l}T^2_{r^1_l-1}) \\ &\xrightarrow{\sim} Gal(T^2_{r^1_l}\cap T^1_{q^1_l+1}T^2_{r^1_l-1}/T^2_{r^1_l}\cap T^1_{q^1_l}T^2_{r^1_l-1})\ . \end{aligned}$$

Pour $q^1_l+1\leq m-1$, ce dernier groupe est, par définition de la tour (T'^2), égal à

$$Gal(T'^2_{(r^1_l-1)m+q^1_l+1}/T'^2_{(r^1_l-1)m+q^1_l}) = Gal(T'^2_{\sigma(l)}/T'^2_{\sigma(l)-1})\ .$$

Enfin si $q^1_l+1=m$, on a $\sigma(l)=r^1_l m$, d'où

$$T^2_{r^1_l}\cap T^1_{q^1_l+1}T^2_{r^1_l-1} = T^2_{r^1_l}\cap LT^2_{r^1_l-1} = T^2_{r^1_l}\ .$$

Et l'on a déjà noté que $T^2_{r^1_l}=T'^2_{r^1_l m}=T'^2_{\sigma(l)}$.

Ainsi dans tous les cas, on a prouvé que

$$\forall l\in\{1,\dots,mn\}\quad Gal(T'^1_l/T'^1_{l-1})\xrightarrow{\sim} Gal(T'^2_{\sigma(l)}/T'^2_{\sigma(l)-1})\ ,$$

i.e. que $(T'^2)\sim(T'^1)$. Ceci achève la démonstration du 1^{er} théorème de dissociation. □

Dans le cas de tours strictes, le théorème 3.2 précédent peut être amélioré en le suivant :

Corollaire 3.3. *Deux tours galoisiennes strictes d'une même extension galtourable admettent des raffinements qui sont des tours galoisiennes strictes équivalentes.*

Démonstration. Dans les notations des proposition 3.1 et théorème 3.2, les tours (T^1) et (T^2), supposées strictes, admettent les raffinements équivalents (T'^1) et (T'^2), dont rien ne permet d'affirmer qu'ils sont stricts. La proposition 1.5 nous montre quant à elle que les tours galoisiennes strictes associées $(T'^1_<)$ et $(T'^2_<)$ sont équivalentes. Or le corollaire 2.4 du chapitre 3 conclut que $(T'^1_<)$ (resp. $(T'^2_<)$) est encore un raffinement de (T^1) (resp. (T^2)). □

Ce théorème 3.2 admet encore une généralisation aux tours galtourables :

Théorème 3.4. *(1^{er} théorème de dissociation bis)*
Deux tours galtourables d'une même extension galtourable admettent des raffinements qui sont des tours galoisiennes équivalentes.

Démonstration. Soient L/K une extension galtourable et (E^1), (E^2) deux tours galtourables de L/K. Par la proposition 1.9 du chapitre 3, (E^1) (resp. (E^2)) admet un raffinement qui est une tour galoisienne (T^1) (resp. (T^2)). Le théorème 3.2 assure alors que les tours galoisiennes (T^1) et (T^2) de L/K admettent des

raffinements équivalents (T'^1) et (T'^2). Or, par le Fait 1.6 du chapitre 3, (T'^1) (resp. (T'^2)) est encore un raffinement de (E^1) (resp. (E^2)). □

De même, le théorème précédent admet une version pour les tours strictes :

Corollaire 3.5. *Deux tours galtourables strictes d'une même extension galtourable admettent des raffinements qui sont des tours galoisiennes strictes équivalentes.*

Démonstration. Celle du corollaire 3.3 mutatis mutandis. □

4. Deuxième et troisième théorèmes de dissociation

Notons la proposition suivante, essentielle pour le théorème général 4.2 à suivre :

Proposition 4.1. *Une extension galoisienne infinie n'est jamais galsimple.*

Démonstration. Soit L/K une extension galoisienne infinie. Considérons $\{E_i\}_{i\in I}$ l'ensemble des corps intermédiaires entre K et L tels que l'extension quotient E_i/K soit galoisienne finie :

$$\forall i \in I \quad K \trianglelefteq E_i \leq L \qquad [E_i : K] < \infty \ .$$

On sait [**20**, p.16, Satz 2.3] (ou [**21**]) que

$$L = \bigcup_{i\in I} E_i \ .$$

Si l'on avait $E_i = K$ pour tout i dans I, on aurait donc $L = K$, ce qui contredirait l'hypothèse $[L : K] = \infty$. Par conséquent

$$\exists i_0 \in I \qquad E_{i_0} \neq K \ .$$

De plus

$$([E_{i_0} : K] < \infty \ , \quad [L : K] = \infty) \qquad \Rightarrow \qquad E_{i_0} \neq L \ .$$

Ainsi $K \lhd E_{i_0} < L$, et l'extension L/K n'est pas galsimple. □

En général, un groupe n'admet pas de suite de composition. Les groupes finis en admettent une, mais ce ne sont pas les seuls. Nous avons prouvé que les extensions de corps, même séparables, n'admettent pas nécessairement de tour galoisienne (Chap. 2, Ex. 1.10.(i)). Avec la notion d'extension galtourable, le théorème suivant répond à la question de savoir quelles sont exactement les extensions de corps admettant une tour de composition galoisienne.

Théorème 4.2. *($2^{ème}$ théorème de dissociation)*
Une extension de corps admet une tour de composition galoisienne si et seulement si elle est galtourable finie.

Scholie. En particulier, la proposition 2.8 se généralise donc aux extensions galtourables.

Démonstration. Soit L/K une extension admettant une tour de composition galoisienne

$$(F) \qquad K = F_0 \lhd \cdots \lhd F_i \lhd \cdots \lhd F_m = L \ .$$

Chacune des marches de (F) est galsimple en vertu de la proposition 1.3. Par définition (Chap. 2, Déf. 1.4), L/K est en particulier galtourable. Supposons qu'elle soit de degré infini. De $\infty = [L : K] = \prod_{i=0}^{m-1} [F_{i+1} : F_i]$ suit qu'au moins l'une des marches est infinie :

$$\exists i_0 \in \{0, \ldots, m-1\} \quad [F_{i_0+1} : F_{i_0}] = \infty \ .$$

Mais alors F_{i_0+1}/F_{i_0} est galoisienne infinie et galsimple, ce qui contredit la proposition 4.1 précédente.

Réciproquement, supposons l'extension L/K galtourable finie non triviale (le résultat est vrai pour l'extension triviale d'après le Fait 1.2). Soit

$$(F) \qquad K = F_0 \trianglelefteq \cdots \trianglelefteq F_i \trianglelefteq \cdots \trianglelefteq F_m = L$$

une tour galoisienne de L/K. Quitte à prendre sa tour stricte associée $(F_<)$, on peut supposer que (F) est une tour stricte en vertu du corollaire 2.6 du chapitre 3. L'extension L/K étant de degré fini, il en est de même de chacune de ses marches $F_{i+1} \nearrow F_i \quad (i = 0, \ldots, m-1)$. En tant qu'extensions galoisiennes finies, celles-ci admettent des tours de composition galoisiennes d'après la proposition 2.8 :

$$(T_i) \qquad F_i = T_{j_i} \lhd \cdots \lhd T_{j_{i+1}} = F_{i+1}$$

où $j_i < j_{i+1}$ puisque (F) est stricte. De même que dans la démonstration de la proposition 1.9 du chapitre 3, la juxtaposition des tours galoisiennes $(T_i) \quad (i = 0, \ldots, m-1)$ donne la tour galoisienne stricte

$$(T) \qquad K = F_0 = T_{j_0} \lhd \cdots \lhd T_{j_1} = F_1 \lhd \cdots \lhd T_{j_m} = F_m = L$$

de L/K. Chacune des marches de (T) est une marche de l'une des tours (T_i), donc est galsimple (cf. Prop. 1.3). Finalement la tour galoisienne (T) est elle-même de composition. □

Nous sommes maintenant en mesure de démontrer l'analogue galoisien au théorème de Jordan-Hölder annoncé dans l'introduction du présent chapitre.

Théorème 4.3. *($3^{ème}$ théorème de dissociation, dit "de Galjordanhölder")*
Soit L/K une extension finie galtourable.
(1) Toute tour galoisienne stricte de L/K admet un raffinement qui est une tour de composition galoisienne de L/K.
(2) Deux tours de composition galoisiennes de L/K sont équivalentes.

Scholie. Le raffinement du (1) est nécessairement un raffinement galoisien en vertu du Fait 1.5.(2) du chapitre 3.

Démonstration. (1) D'après le $2^{\text{ème}}$ théorème de dissociation (Th. 4.2), L/K admet une tour de composition galoisienne (C). Soit (T) une tour galoisienne stricte de L/K. D'après le théorème de Galschreier (Th. 3.2), (C) et (T) admettent des raffinements (C') et (T') qui sont des tours galoisiennes équivalentes. Ces raffinements sont galoisiens (Chap. 3, Fait 1.5.(2)). Comme la tour de composition (C) n'admet aucun raffinement galoisien propre, (C') est nécessairement un raffinement trivial de (C). Or (C) est stricte par définition. C'est donc la tour stricte associée à (C') (Chap. 3, Prop. & Déf. 2.1), d'où

$$(C) = (C'_<) \ .$$

Par la proposition 1.5, on en déduit que les tours galoisiennes $(C) = (C'_<)$ et $(T'_<)$ sont équivalentes. Comme (C) est de composition, il résulte alors du corollaire 1.4 que le raffinement $(T'_<)$ de (T) est une tour de composition galoisienne. De plus d'après le corollaire 2.8 du chapitre 3, $(T'_<)$ est encore un raffinement de (T).

(2) Dans le (1) précédent, lorsque (T) est une tour de composition galoisienne, le même argument que pour (C) conduit à $(T'_<) = (T)$. Et finalement $(T'_<) \sim (C'_<)$ signifie $(T) \sim (C)$. □

Comme le 1^{er} théorème de dissociation, ce théorème 4.3 admet une généralisation aux tours galtourables.

Théorème 4.4. *($3^{\text{ème}}$ théorème de dissociation bis)*
Soit L/K une extension finie galtourable.
(1) Toute tour galtourable stricte de L/K admet un raffinement qui est une tour de composition galoisienne de L/K.
(2) Deux tours de composition galoisiennes de L/K sont équivalentes.

Démonstration. (1) Soit (E) une tour galtourable stricte de L/K. Par la proposition 2.9 du chapitre 3, elle admet un raffinement (T) qui est une tour galoisienne stricte de L/K. Et d'après le théorème 4.3.(1) précédent, (T) admet un raffinement (C) qui est une tour de composition galoisienne de L/K. On déduit alors de la transitivité de la notion de raffinement (Chap. 3, Fait 1.6) que (C) est un raffinement de (E).
(2) Identique à celui du $3^{\text{ème}}$ théorème de dissociation. □

Chapitre 5

ILLUSTRATIONS ARITHMÉTIQUES ET GALSIMPLICITÉ

Ce chapitre 5 est un chapitre de transition, une respiration arithmétique avant les tours d'élévation qui nous permettrons de dissocier toutes les extensions finies et pas seulement les galtourables. La section 1 illustre les théorèmes de Galschreier et Galjordanhölder du chapitre 4 par une extension galtourable de degré 480 dont nous donnons deux tours galoisiennes différentes que l'on raffine en deux tours de composition galoisiennes équivalentes. La section 2 fournit, via un résultat de Selmer-Serre, une classe infinie d'extensions simples (au sens du (1) de la définition 1.6 du chapitre 2) mais non galoisiennes. La section 3 montre, via un contre-exemple, que le "Théorème M" du chapitre 6 suivant ne s'étend pas au cas d'une extension infinie. Ce contre-exemple justifie la finitude des extensions du chapitre 7 final. Enfin, la section 4 donne quelques propriétés des extensions galsimples non galoisiennes, notamment leur transitivité qui nous sera utile pour la maximalité des sous-extensions d'intourabilité.

1. Illustrations des théorèmes de Galschreier et Galjordanhölder par une extension de degré 480

On note génériquement $\zeta_n := e^{2i\pi/n} \quad (n \in \mathbb{N} \setminus \{0\})$. Dans toute cette section, on considère les tours

$$(T^1) \qquad K = T_0^1 := \mathbb{Q} < T_1^1 := T_0^1(i, \sqrt[4]{5}) < T_2^1 := T_1^1(\zeta_{15}, Y^{1/5}, Z^{1/3}) = L$$

et

$$(T^2) \qquad K = T_0^2 := \mathbb{Q} < T_1^2 := T_0^2(\zeta_{15}) < T_2^2 := T_1^2(i, Y^{1/5}) < T_3^2 = L\ ,$$

où l'on désigne par :

$$\begin{cases} - Y^{1/5} \text{ l'une quelconque des racines cinquièmes complexes de} \\ \qquad Y := (2-\zeta_5)^3(2-\zeta_5^4)^2\ ; \\ - Z^{1/3} \text{ l'une quelconque des racines troisièmes complexes de} \\ \qquad Z := 6-\sqrt{5}\ . \end{cases}$$

Fait 1.1. *L'extension $\mathbb{Q}(\zeta_5)(Y^{1/5})/\mathbb{Q}(\zeta_5)$ est cyclique de degré 5.*

Démonstration. Sinon, modulo $\mathbb{Q}(\zeta_5)^{\times 5}$,

$$\overline{Y} = \overline{\mathbb{1}} \qquad \Longleftrightarrow \qquad \overline{2-\zeta_5^4} = \overline{2-\zeta_5}\ .$$

En particulier, pour le corps local $C := \mathbb{Q}_5(\zeta_5)$, on a alors

$$\frac{2-\zeta_5^4}{2-\zeta_5} \in C^{\times 5} .$$

Prouvons que ceci n'est pas, grâce aux méthodes (et notations) de [**38**] et [**42**]. Tout d'abord, $2-\zeta_5^4$ est une unité principale de C :

$$2-\zeta_5^4 \in U_C^1 ,$$

car pour l'uniformisante $1-\zeta_5$, on a les valuations

$$\mathrm{ord}(1-(2-\zeta_5^4)) = \mathrm{ord}(\zeta_5^4(1-\zeta_5)) = 1 .$$

Comme il en est de même de $2-\zeta_5$, on a donc

$$\frac{2-\zeta_5^4}{2-\zeta_5} \in U_C^1 .$$

Calculons le défaut de cette unité principale :

$$\begin{array}{rcl} \mathrm{ord}(1-\frac{2-\zeta_5^4}{2-\zeta_5}) & = & \mathrm{ord}(-\zeta_5+\zeta_5^4) = \mathrm{ord}(\zeta_5^4(1-\zeta_5^2)) \\ & = & \mathrm{ord}(1-\zeta_5)+\mathrm{ord}(1+\zeta_5) \\ & = & 1+\mathrm{ord}(2-(1-\zeta_5)) \\ & = & 1 ; \end{array}$$

on en déduit que

$$\mathrm{def}\left(\frac{2-\zeta_5^4}{2-\zeta_5}\right) = 1 \qquad\qquad (\text{cf. } [\mathbf{42}]) .$$

D'où la conclusion puisque

$$\frac{2-\zeta_5^4}{2-\zeta_5} \in C^{\times 5} \quad \Longleftrightarrow \quad \mathrm{def}(\frac{2-\zeta_5^4}{2-\zeta_5}) = +\infty .$$

□

Fait 1.2. *(0) La tour (T^2) est galoisienne ;*

(1) $\sqrt[4]{5} \notin \mathbb{Q}(i,\zeta_3,\zeta_5)$;

(2) $T_1^1 \cap T_1^2 = \mathbb{Q}(\sqrt{5})$;

(3) $T_1^1 \cap \mathbb{Q}(\zeta_5) = \mathbb{Q}(\sqrt{5})$;

(4) $Gal(\mathbb{Q}(\zeta_{15})/\mathbb{Q}(\sqrt{5})) \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})^2$.

Démonstration. (0) La marche $L = T_2^2(\sqrt[4]{5}, Z^{1/3})/T_2^2$ est le compositum de deux extensions kummériennes.
(1) L'extension $\mathbb{Q}(i,\zeta_3,\zeta_5)\nearrow\mathbb{Q}$ est cyclotomique, donc abélienne. Si l'on avait $\sqrt[4]{5} \in \mathbb{Q}(i,\zeta_3,\zeta_5)$, l'extension $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}$ serait abélienne, comme quotient d'une

extension abélienne, ce qui n'est pas.

(2) D'après [**24**, p.74, Th.2], $i \notin T_1^2 = \mathbb{Q}(\zeta_{15})$, d'où

$$[T_1^2(i) : T_1^2] = 2 .$$

Par ailleurs

$$\zeta_5 + \zeta_5^4 = \frac{\sqrt{5}-1}{2}$$

(explicitement écrit dans [**14**, p.67-68] !). Donc

$$\mathbb{Q}(\sqrt{5}) < \mathbb{Q}(\zeta_5) < T_1^2 = \mathbb{Q}(\zeta_3, \zeta_5) .$$

En particulier, $\sqrt{5} \in T_1^2(i)$; tandis que par le (1), $\sqrt[4]{5} \notin T_1^2(i)$. Dès lors,

$$[T_1^1 T_1^2 = \mathbb{Q}(i, \zeta_3, \zeta_5, \sqrt[4]{5}) : T_1^2(i)] = 2 .$$

On a ainsi la figure

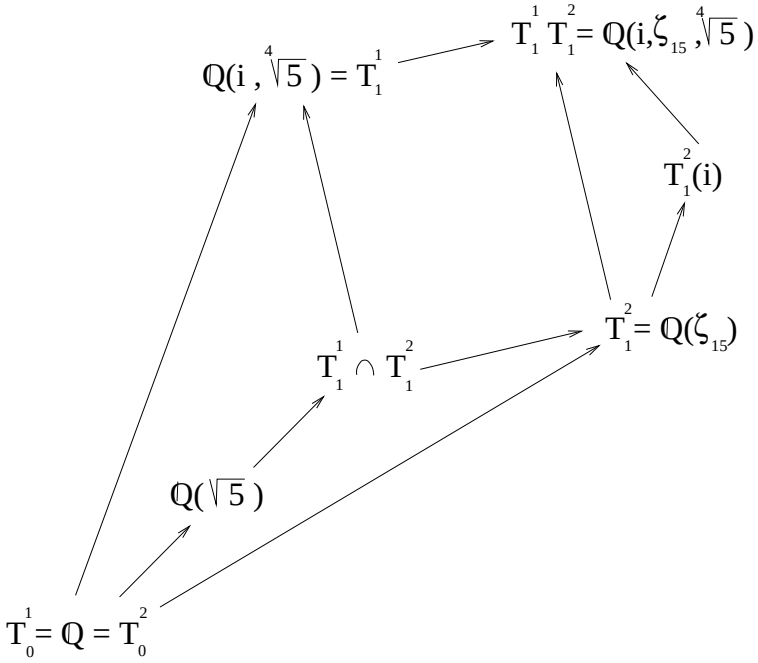

FIG. 18. *Parallélogramme* $[T_1^1 \cap T_1^2, T_1^2, T_1^1 T_1^2, T_1^1]$

dans laquelle le quadrilatère $(T_1^1 \cap T_1^2, T_1^2, T_1^1 T_1^2, T_1^1)$ est un parallélogramme galoisien. En effet, l'extension $T_1^1/T_1^1 \cap T_1^2$ (resp. $T_1^2/T_1^1 \cap T_1^2$) est galoisienne comme sous-extension de $T_1^1/\mathbb{Q}$ (resp. $T_1^2/\mathbb{Q}$) qui est galoisienne de degré 8 car $T_1^1 = \mathbb{Q}(i, \sqrt[4]{5})$ est le corps de décomposition du polynôme $X^4 - 5$ (resp. car

$[T_1^2 = \mathbb{Q}(\zeta_{15}) : \mathbb{Q}] = \varphi(15) = 8$). Par conséquent :

$$\begin{aligned} 8 = [T_1^1 : \mathbb{Q}] &= [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}][T_1^1 \cap T_1^2 : \mathbb{Q}(\sqrt{5})][T_1^1 : T_1^1 \cap T_1^2] \\ &= 2[T_1^1 \cap T_1^2 : \mathbb{Q}(\sqrt{5})][T_1^1 T_1^2 : T_1^2] \\ &= 2[T_1^1 \cap T_1^2 : \mathbb{Q}(\sqrt{5})][T_1^2(i) : T_1^2][T_1^1 T_1^2 : T_1^2(i)] \\ &= 8[T_1^1 \cap T_1^2 : \mathbb{Q}(\sqrt{5})] \\ \Leftrightarrow T_1^1 \cap T_1^2 &= \mathbb{Q}(\sqrt{5}) \ . \end{aligned}$$

(3) Comme $\sqrt{5} \in \mathbb{Q}(\zeta_5)$, on a par le (2)

$$\mathbb{Q}(\sqrt{5}) \leq T_1^1 \cap \mathbb{Q}(\zeta_5) \leq T_1^1 \cap \mathbb{Q}(\zeta_{15}) = T_1^1 \cap T_1^2 = \mathbb{Q}(\sqrt{5}) \ .$$

(4) Comme $T_1^2 = \mathbb{Q}(\zeta_{15})$, on a le parallélogramme $[\mathbb{Q}, \mathbb{Q}(\zeta_3), T_1^2, \mathbb{Q}(\zeta_5)]$.

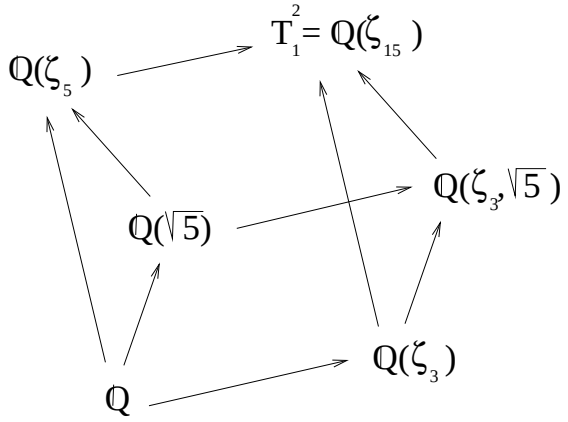

FIG. 19. *Un sous-parallélogramme de* $[\mathbb{Q}, \mathbb{Q}(\zeta_3), T_1^2, \mathbb{Q}(\zeta_5)]$

D'après le corollaire 4.3.(1-1) du chapitre 1, on a le sous-parallélogramme $[\mathbb{Q}(\sqrt{5}), \mathbb{Q}(\zeta_3, \sqrt{5}), T_1^2, \mathbb{Q}(\zeta_5)]$. On en déduit, par scindement de la diagonale (Chap. 1, Prop. 4.1) que

$$Gal(T_1^2/\mathbb{Q}(\sqrt{5})) \xrightarrow{\sim} Gal(T_1^2/\mathbb{Q}(\zeta_3, \sqrt{5})) \times Gal(T_1^2/\mathbb{Q}(\zeta_5)) \ .$$

Comme $[T_1^2 : \mathbb{Q}(\zeta_3, \sqrt{5})] = [T_1^2 : \mathbb{Q}(\zeta_5)] = 2$, on a bien le résultat annoncé :

$$Gal(T_1^2/\mathbb{Q}(\sqrt{5})) \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})^2 \ .$$

□

Nous avons déjà dit que la tour (T^2) est galoisienne $\big((0)$ du Fait précédent$\big)$, le lecteur aura deviné qu'il en est de même de la tour (T^1). Nous le démontrons maintenant, en utilisant deux fois un puissant outil introduit par Richard Massy dans [**26**] sous le nom de "moyenne galoisienne" ("Galois average").

Proposition 1.3. *L'extension* $L = T_2^1/T_1^1$ *est galoisienne, non abélienne, de degré 60.*

Démonstration. Soient v et w les générateurs de

$$Gal(T_1^2 = \mathbb{Q}(\zeta_{15})/\mathbb{Q}) = Gal(\mathbb{Q}(\zeta_3)/\mathbb{Q}) \times Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q})$$

définis par

$$v(\zeta_3) = \zeta_3^2\ ,\ v(\zeta_5) = \zeta_5\ ;\quad w(\zeta_5) = \zeta_5^2\ ,\ w(\zeta_3) = \zeta_3\ .$$

On a

$$w^2(\zeta_5 + \zeta_5^4) = \zeta_5^4 + \zeta_5 = \frac{\sqrt{5}-1}{2}\ ;$$

donc w^2 laisse fixe $\sqrt{5}$ et

$$Gal(T_1^2/\mathbb{Q}(\sqrt{5})) = \{1, v\} \times \{1, w^2\}\ .$$

Or, d'après le (2) du Fait 1.2, on a le parallélogramme galoisien

$$[\mathbb{Q}(\sqrt{5}), T_1^2, T_1^1T_1^2, T_1^1]\ .$$

En notant $\widetilde{v}$ et $\widetilde{w^2}$ les prolongements respectifs de v et w^2 à $T_1^1T_1^2$, on en déduit que

$$Gal(T_1^1T_1^2/T_1^1) = \{1, \widetilde{v}\} \times \{1, \widetilde{w^2}\}\ .$$

Soit η "l'homomorphisme cyclotomique" ([**26**]) de $Gal(T_1^1T_1^2/T_1^1)$ dans le groupe multiplicatif $\mathbb{F}_5^\times$ du corps à cinq éléments, défini par

$$\widetilde{w^2}(\zeta_5) = \zeta_5^4 \ \Leftrightarrow\ \eta(\widetilde{w^2}) = 4\ ;\qquad \widetilde{v}(\zeta_5) = \zeta_5 \ \Leftrightarrow\ \eta(\widetilde{v}) = 1\ .$$

Soient $y := 2-\zeta_5$ et $\overline{y}$ sa classe dans $(T_1^1T_1^2)^\times/(T_1^1T_1^2)^{\times 5}$. La moyenne galoisienne de $T_1^1T_1^2$ sur T_1^1 pour η en $\overline{y}$ est par définition [**26**, Sect. 2]

$$\begin{aligned}
ga^{\eta}_{T_1^1T_1^2/T_1^1}(\overline{y}) &= \Big(\prod_{\gamma\in Gal(T_1^1T_1^2/T_1^1)} \gamma(\overline{y})^{\eta(\gamma)^{-1}}\Big)^{4^{-1}}\\
&= \big(\overline{y}\,\widetilde{v}(\overline{y})\,\widetilde{w^2}(\overline{y})^4\,\widetilde{v}\widetilde{w^2}(\overline{y})^4\big)^{4^{-1}}\\
&= \overline{y}^4\,\widetilde{v}(\overline{y})^4\,\widetilde{w^2}(\overline{y})\,\widetilde{v}\widetilde{w^2}(\overline{y})\\
&= \overline{(2-\zeta_5)^4\,(2-\zeta_5)^4\,(2-\zeta_5^4)\,(2-\zeta_5^4)}\\
&= \overline{(2-\zeta_5)^3\,(2-\zeta_5^4)^2} = \overline{Y}\ .
\end{aligned}$$

D'après [**26**], l'extension $T_1^1T_1^2(Y^{1/5})/T_1^1$ est galoisienne. On a $T_1^2(Y^{1/5}) \cap T_1^1T_1^2 = T_1^2$ par primalité des degrés car $[T_1^1T_1^2 : T_1^2] = 4$ (cf. (2) de la démonstration du Fait 1.2) et $[T_1^2(Y^{1/5}) : T_1^2] \in \{1, 5\}$. On en déduit le parallélogramme galoisien $[T_1^2, T_1^1T_1^2, T_1^1T_1^2(Y^{1/5}), T_1^2(Y^{1/5})]$.

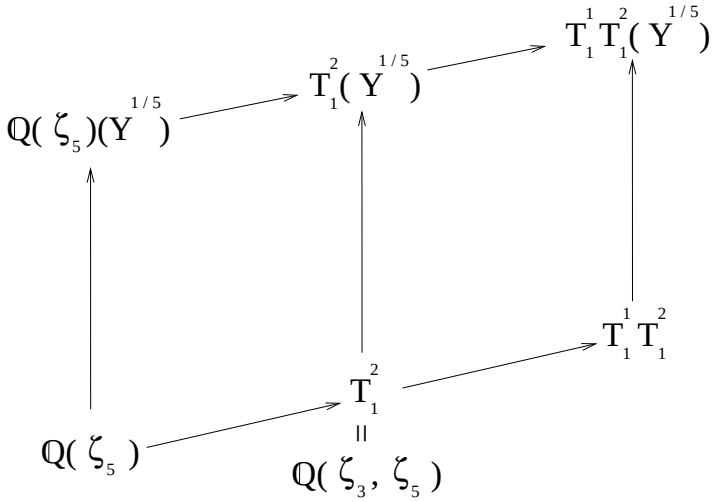

FIG. 20. *Deux parallélogrammes adjacents*

Or d'après le Fait 1.1, on a $[\mathbb{Q}(\zeta_5)(Y^{1/5}) : \mathbb{Q}(\zeta_5)] = 5$. A nouveau par primalité des degrés, on en déduit le parallélogramme

$$[\mathbb{Q}(\zeta_5), T_1^2, T_1^2(Y^{1/5}), \mathbb{Q}(\zeta_5)(Y^{1/5})] .$$

Par conséquent

$$5 = [T_1^2(Y^{1/5}) : T_1^2] = [T_1^1T_1^2(Y^{1/5}) : T_1^1T_1^2] .$$

On obtient ainsi le degré de l'extension galoisienne $T_1^1T_1^2(Y^{1/5})/T_1^1$:

$$[T_1^1T_1^2(Y^{1/5}) : T_1^1] = 5[T_1^1T_1^2 : T_1^1] = 20 .$$

Montrons que l'extension T_2^1/T_1^1 est obtenue par une 3-moyenne au dessus de l'extension $T_1^1T_1^2(Y^{1/5})/T_1^1$. Pour l'homomorphisme trivial

$$\mathbb{1} : \begin{array}{rccc} G := & Gal(T_1^1T_1^2(Y^{1/5})/T_1^1) & \to & \mathbb{F}_3^\times , \\ & \gamma & \mapsto & 1 \end{array}$$

on a

$$\begin{aligned} ga^1_{T_1^1T_1^2(Y^{1/5})/T_1^1}(\overline{Y}^{-1/5}) &= \Big(\prod_{\gamma\in G}\gamma(\overline{Y}^{-1/5})\Big)^{20^{-1}} = \Big(\prod_{\gamma\in G}\gamma(\overline{Y}^{-1/5})\Big)^{-1} \\ &= \overline{N_{T_1^1T_1^2(Y^{1/5})/T_1^1}(Y^{1/5})} . \end{aligned}$$

Notons que $T_1^1T_1^2(Y^{1/5}) = T_1^1T_2^2$, et

$$\begin{aligned} N_{T_1^1T_2^2/T_1^1}(Y^{1/5}) &= N_{T_1^1T_1^2/T_1^1}\Big(N_{T_1^1T_2^2/T_1^1T_1^2}(Y^{1/5})\Big) \\ &= N_{T_1^1T_1^2/T_1^1}(Y^{1/5}\,\zeta_5 Y^{1/5}\,\zeta_5^2 Y^{1/5}\,\zeta_5^3 Y^{1/5}\,\zeta_5^4 Y^{1/5}) \\ &= N_{T_1^1T_1^2/T_1^1}(Y) \\ &= Y\,\widetilde{v}(Y)\,\widetilde{w^2}(Y)\,\widetilde{v}\widetilde{w^2}(Y)\,. \end{aligned}$$

Comme $\widetilde{v}(\zeta_5) = \zeta_5$, on a $\widetilde{v}(Y) = Y$ et

$$\begin{aligned} ga^1_{T_1^1T_2^2/T_1^1}(\overline{Y}^{-1/5}) &= \overline{Y^2\,\widetilde{w^2}(Y)^2} \\ &= \overline{(2-\zeta_5)^6\,(2-\zeta_5^4)^4\,(2-\zeta_5^4)^6\,(2-\zeta_5)^4} \\ &= \overline{(2-\zeta_5)\,(2-\zeta_5^4)} \\ &= \overline{4-2(\zeta_5+\zeta_5^4)+1} \\ &= \overline{4-(\sqrt{5}-1)+1} \\ &= \overline{6-\sqrt{5}}\,. \end{aligned}$$

On en déduit, toujours par **[26]**, que l'extension L/T_1^1 est galoisienne, car on a :

$$\begin{aligned} L &= T_2^1 = T_1^1(\zeta_{15}, Y^{1/5}, Z^{1/3}) = T_1^1T_1^2(Y^{1/5}, Z^{1/3}) \\ &= T_1^1T_1^2(Y^{1/5})(Z^{1/3}) = T_1^1T_2^2(Z^{1/3})\,. \end{aligned}$$

Elle est de degré

$$[L : T_1^1] = [T_1^1T_2^2(Z^{1/3}) : T_1^1T_2^2][T_1^1T_2^2 : T_1^1] = 3 \times 20 = 60$$

car $Z = 6-\sqrt{5} \notin (T_1^1T_2^2)^{\times 3}$. En effet sinon on aurait $N_{T_1^1T_2^2/\mathbb{Q}}(6-\sqrt{5}) \in \mathbb{Q}^{\times 3}$, ce qui n'est pas, puisque

$$\begin{aligned} N_{T_1^1T_2^2/\mathbb{Q}}(6-\sqrt{5}) &= N_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(N_{T_1^1T_2^2/\mathbb{Q}(\sqrt{5})}(6-\sqrt{5})) \\ &= N_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(6-\sqrt{5})^{80} \\ &= 31^{80} \notin \mathbb{Q}^{\times 3}\,. \end{aligned}$$

Enfin L/T_1^1 est non abélienne, car soit $\check{v}$ un prolongement de $\widetilde{v}$ à $T_1^1T_2^2$:

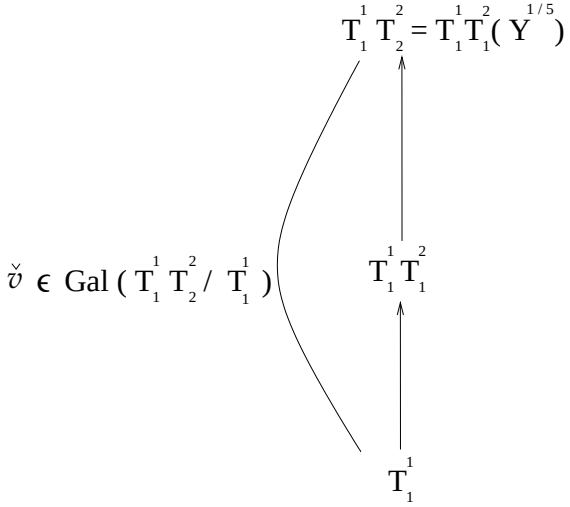

FIG. 21. *Extension galoisienne* $T_1^1T_2^2/T_1^1$

Clairement

$$\check{v}(\zeta_3) = \widetilde{v}(\zeta_3) = \zeta_3^2 \, .$$

L'homomorphisme cyclotomique de $Gal(T_1^1T_2^2/T_1^1)$ dans $\mathbb{F}_3^\times$ n'est donc pas trivial. Comme $\overline{Z} = \overline{6-\sqrt{5}}$ est dans l'image de la moyenne galoisienne $ga^1_{T_1^1T_2^2/T_1^1}$ pour cet homomorphisme trivial, il résulte du [**26**, Th.1.2.(3.2)] que l'extension L/T_1^1 ne peut être abélienne. □

Corollaire 1.4. *L'extension $L/\mathbb{Q}$ est de degré 480.*

Démonstration. C'est clair puisque

$$[L:\mathbb{Q}] = [L:T_1^1][T_1^1:\mathbb{Q}]$$

où $[L:T_1^1] = 60$ (Prop. 1.3) et $[T_1^1:\mathbb{Q}] = 8$ d'après la démonstration du (2) du Fait 1.2. □

La proposition suivante illustre le théorème de Galschreier (1er théorème de dissociation) pour une extension de degré 480.

Proposition 1.5. *On a les tours galoisiennes (strictes) équivalentes de L/K (Chap. 4, Déf. 1.1.(2)) $(T'^1) \sim (T'^2)$ où*

$$(T'^1) \qquad K = \mathbb{Q} =: T_0'^1 \lhd T_1'^1 := \mathbb{Q}(\sqrt{5}) \lhd T_2'^1 := \mathbb{Q}(i,\sqrt{5}) \lhd T_3'^1 := \mathbb{Q}(i,\sqrt[4]{5})$$

$$\lhd T_4'^1 := \mathbb{Q}(i,\sqrt[4]{5},\zeta_{15}) \lhd T_5'^1 := \mathbb{Q}(i,\sqrt[4]{5},\zeta_{15},Y^{1/5}) \lhd T_6'^1 := T_5'^1(Z^{1/3}) = L$$

et

$$(T'^2)\quad K=\mathbb{Q}=:T'^2_0 \lhd T'^2_1:=\mathbb{Q}(\sqrt{5}) \lhd T'^2_2:=\mathbb{Q}(\zeta_{15}) \lhd T'^2_3:=\mathbb{Q}(i,\zeta_{15})$$

$$\lhd T'^2_4:=\mathbb{Q}(i,\zeta_{15},Y^{1/5}) \lhd T'^2_5:=\mathbb{Q}(i,\sqrt[4]{5},\zeta_{15},Y^{1/5}) \lhd T'^2_6:=L\ .$$

Démonstration. Prouvons qu'elles sont obtenues à partir des tours (T^1) et (T^2) (cf. début de la présente section) par les formules $(\mathcal{F})$ de la démonstration du 1er théorème de dissociation (Chap. 4, Th. 3.2). On a :

$$\mathbb{Q}=T^1_1\cap T^1_0T^2_0=T^2_1\cap T^1_0T^2_0\ ;$$

$$\mathbb{Q}(\sqrt{5}) \overset{1.2.(2)}{=} T^1_1\cap T^2_1=T^1_1\cap T^1_0T^2_1=T^2_1\cap T^1_1T^2_0\ ;$$

$$\mathbb{Q}(\zeta_{15})=T^2_1=T^2_2\cap T^1_0T^2_1\ ;$$

$$\mathbb{Q}(i,\sqrt[4]{5})=T^1_1=T^1_2\cap T^1_1T^2_0\ .$$

D'après la démonstration de la proposition 1.3, on dispose du parallélogramme galoisien

$$[T^2_1,T^2_1(Y^{1/5}),T^1_1T^2_1(Y^{1/5}),T^1_1T^2_1]$$

dans lequel on peut utiliser le (1-1) du corollaire 4.3 du chapitre 1 : le corps intermédiaire $T^2_1(i)$ induit le sous-parallélogramme

$$[T^2_1(i),T^2_1(i,Y^{1/5}),T^1_1T^2_1(Y^{1/5}),T^1_1T^2_1]\ .$$

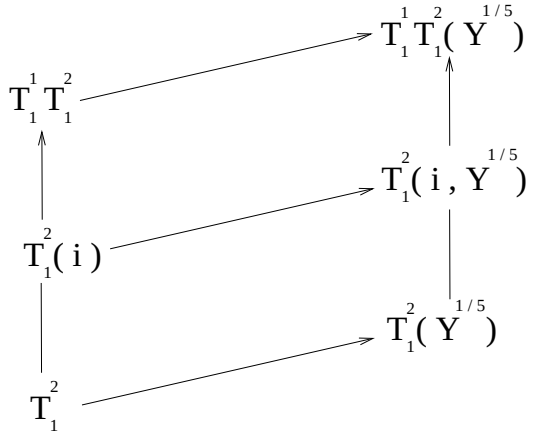

FIG. 22. *Sous-parallélogramme* $[T^2_1(i),T^2_1(i,Y^{1/5}),T^1_1T^2_1(Y^{1/5}),T^1_1T^2_1]$

On en déduit en particulier que

$$\mathbb{Q}(i,\zeta_{15})=T^2_1(i)=T^2_1(i,Y^{1/5})\cap T^1_1T^2_1=T^2_2\cap T^1_1T^2_1\ .$$

Par ailleurs

$$\mathbb{Q}(i,\sqrt[4]{5},\zeta_{15})=T^1_1T^2_1=T^1_2\cap T^1_1T^2_1\ ;$$

$$\mathbb{Q}(i,\zeta_{15},Y^{1/5})=T^2_2=T^2_3\cap T^1_0T^2_2\ ;$$

$$\mathbb{Q}(i, \sqrt[4]{5}, \zeta_{15}, Y^{1/5}) = T_1^1 T_2^2 = T_2^1 \cap T_1^1 T_2^2 = T_3^2 \cap T_1^1 T_2^2 \ .$$

Enfin dans le parallélogramme galoisien $[T_1^1 \cap T_1^2 \overset{1.2.(2)}{=} \mathbb{Q}(\sqrt{5}), T_1^2, T_1^1 T_1^2, T_1^1]$, on déduit du (1-1) du corollaire 4.3 du chapitre 1 appliqué au corps intermédiaire $\mathbb{Q}(i, \sqrt{5}) \leq T_1^1$, le sous-parallélogramme

$$[\mathbb{Q}(i, \sqrt{5}), T_1^2(i), T_1^1 T_1^2, T_1^1] \ .$$

En particulier

$$\begin{aligned} \mathbb{Q}(i, \sqrt{5}) &= T_1^1 \cap T_1^2(i) = T_1^1 \cap \mathbb{Q}(i, \zeta_{15}) \\ &= T_1^1 \cap (T_2^2 \cap T_1^1 T_1^2) = T_1^1 \cap T_2^2 \\ &= T_1^1 \cap T_0^1 T_2^2 \end{aligned}$$

□

Le corollaire suivant illustre le théorème de Galjordanhölder ($3^{\text{ème}}$ théorème de dissociation : Chap. 4, Th. 4.3) pour la même extension de degré 480.

Corollaire 1.6. *On a les tours de composition galoisiennes équivalentes de L/K $(T'^1) \sim (T'^2)$ où*

$$(T'^1) \quad K = \mathbb{Q} =: T'^1_0 \lhd T'^1_1 := \mathbb{Q}(\sqrt{5}) \lhd T'^1_2 := \mathbb{Q}(i, \sqrt{5})$$

$$\lhd T'^1_3 := \mathbb{Q}(i, \sqrt[4]{5}) \lhd T'^1_4 := \mathbb{Q}(i, \sqrt[4]{5}, \zeta_5) \lhd T'^1_5 := \mathbb{Q}(i, \sqrt[4]{5}, \zeta_{15})$$

$$\lhd T'^1_6 := \mathbb{Q}(i, \sqrt[4]{5}, \zeta_{15}, Y^{1/5}) \lhd T'^1_7 := \mathbb{Q}(i, \sqrt[4]{5}, \zeta_{15}, Y^{1/5}, Z^{1/3}) = L$$

et

$$(T'^2) \quad K = \mathbb{Q} =: T'^2_0 \lhd T'^2_1 := \mathbb{Q}(\sqrt{5}) \lhd T'^2_2 := \mathbb{Q}(\zeta_5)$$

$$\lhd T'^2_3 := \mathbb{Q}(\zeta_{15}) \lhd T'^2_4 := \mathbb{Q}(i, \zeta_{15}) \lhd T'^2_5 := \mathbb{Q}(i, \zeta_{15}, Y^{1/5})$$

$$\lhd T'^2_6 := \mathbb{Q}(i, \sqrt[4]{5}, \zeta_{15}, Y^{1/5}) \lhd T'^2_7 := \mathbb{Q}(i, \sqrt[4]{5}, \zeta_{15}, Y^{1/5}, Z^{1/3}) = L \ .$$

Démonstration. La tour (T'^1) est un raffinement galoisien de la tour galoisienne (T'^1) de la proposition 1.5 précédente, avec un seul nouveau corps T'^1_4. Par la proposition 1.7 du chapitre 3, (T'^1) est donc une tour galoisienne. Puisque $L/\mathbb{Q}$ est de degré 480 (Cor. 1.4), on a nécessairement :

$$\begin{array}{ll} [T'^1_7 : T'^1_6] = 3 \ , & [T'^1_6 : T'^1_5] = 5 \\ [T'^1_5 : T'^1_4] = 2 \ , & [T'^1_4 : T'^1_3] = 2 \\ [T'^1_3 : T'^1_2] = 2 \ , & [T'^1_2 : T'^1_1] = 2 \\ [T'^1_1 : T'^1_0] = 2 \ . & \end{array}$$

Toutes les marches de (T''^1) sont donc simples (Chap. 2, Ex. 1.10.(iii)) et a fortiori galsimples (Chap. 2, Prop. 1.8.(1)). On déduit alors de la proposition 1.3 du chapitre 4 que (T''^1) est une tour de composition galoisienne. Par un raisonnement identique, on établit que (T''^2) est aussi une tour de composition galoisienne.

Remarquons également que (T''^2) est un raffinement galoisien de (T'^2) avec un seul nouveau corps : (T''^2_2). D'après la proposition 1.5, les 1ère, 4ème, 5ème, 6ème, 7ème marches de (T''^2) sont équivalentes respectivement aux 1ère, 2ème, 6ème, 3ème, 7ème de (T''^1). De plus, on a le parallélogramme galoisien

$$[\mathbb{Q}(\sqrt{5}), \mathbb{Q}(\zeta_{15}), \mathbb{Q}(i, \zeta_{15}, \sqrt[4]{5}), \mathbb{Q}(i, \sqrt[4]{5})]$$

et la figure suivante :

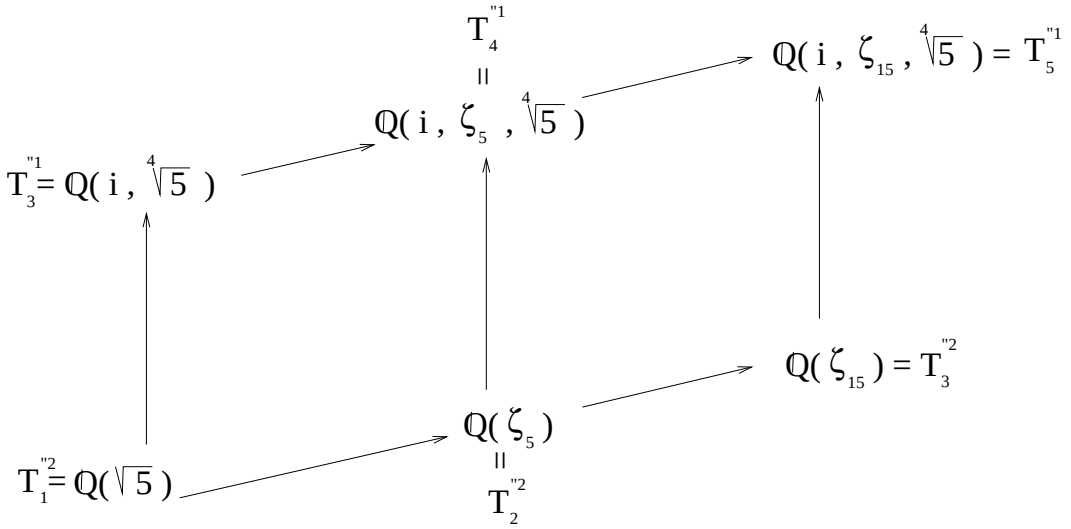

FIG. 23. *Parallélogramme* $[T''^2_1, T''^2_3, T''^1_5, T''^1_3]$

L'extension $\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5})$ est quadratique, donc galoisienne, et par le corollaire 4.3 du chapitre 1 on a les parallélogrammes

$$[\mathbb{Q}(\sqrt{5}), \mathbb{Q}(\zeta_5), \mathbb{Q}(i, \zeta_5, \sqrt[4]{5}), \mathbb{Q}(i, \sqrt[4]{5})]$$

et

$$[\mathbb{Q}(\zeta_5), \mathbb{Q}(\zeta_{15}), \mathbb{Q}(i, \zeta_{15}, \sqrt[4]{5}), \mathbb{Q}(i, \zeta_5, \sqrt[4]{5})] .$$

Donc en particulier

$$Gal(T''^1_4/T''^1_3) \xrightarrow{\sim} Gal(T''^2_2/T''^2_1)$$

et

$$Gal(T''^1_5/T''^1_4) \xrightarrow{\sim} Gal(T''^2_3/T''^2_2) .$$

Ceci achêve de prouver que les tours de composition galoisiennes (T''^1) et (T''^2) sont équivalentes. □

2. Exemple d'extensions simples

Nous exhibons ici une classe infnie d'extensions simples non galoisiennes : celles de l'exemple 1.10.(iii) du chapitre 2 : l'extension $\mathbb{Q}(\theta)/\mathbb{Q}$ où $\theta^n - \theta - 1 = 0$ $(n \geq 3)$ est simple mais non galoisienne.

Nous utilisons la propriété classique suivante des groupes de permutations :

Fait 2.1. *Pour tout entier $n \geq 3$, le groupe symétrique S_{n-1} s'identifie au stabilisateur d'un point quelconque dans S_n. Alors, S_{n-1} est un sous-groupe maximal (intransitif) de S_n.*

Démonstration. Cf. [**12**, p.268]. □

L'argument principal de notre démonstration est un résultat de Selmer-Serre[1] :

Proposition 2.2. *Pour tout entier $n \geq 2$, le polynôme*

$$P_n(X) := X^n - X - 1$$

est irréductible sur $\mathbb{Q}$, et l'on a

$$Gal(L_n/\mathbb{Q}) \xrightarrow{\sim} S_n$$

où L_n désigne le corps de décomposition dans $\mathbb{C}$ de $P_n(X)$.

Démonstration. Cf. [**37**] pour l'irréductibilité et [**38**] pour le reste. □

Corollaire 2.3. *Pour tout entier $n \geq 3$, l'extension $\mathbb{Q}(\theta)/\mathbb{Q}$ où*

$$\theta^n - \theta - 1 = 0$$

est simple et non galoisienne : $(\mathbb{Q}(\theta) \not\leftarrow \mathbb{Q})$.

Démonstration. Avec les notations de la proposition 2.2, soient d'une part $\mathcal{R} := \{\theta_1, \ldots, \theta_n\}$ l'ensemble des racines (nécessairement distinctes) de $P_n(X)$ dans L_n, et d'autre part $E_n := \mathbb{Q}(\theta_n)$, $H_n := Gal(L_n/E_n)$. La numérotation des racines de $P_n(X)$ induit un homomorphisme explicite

$$\begin{array}{rccc} \psi_n & : & Gal(L_n/\mathbb{Q}) & \to & S_n \\ & & \sigma & \mapsto & \psi_n(\sigma) \end{array}$$

défini par $\big(\psi_n(\sigma)\big)(i) = j$ quand $\sigma(\theta_i) = \theta_j$ $(1 \leq i, j \leq n)$. En vertu de la proposition 2.2, ψ_n est un isomorphisme. Il est clair que $\gamma(\theta_n) = \theta_n$ pour tout $\gamma \in H_n$, de sorte que

$$\forall \gamma \in H_n \quad \big(\psi_n(\gamma)\big)(n) = n \ ,$$

[1] Remerciements au Professeur C.U. Jensen de l'Université de Copenhague qui me le fit connaître lors d'un cours de D.E.A à Valenciennes en 1999.

ce qui exprime que $\psi_n(H_n)$ est inclus dans le stabilisateur de n dans S_n, lui même isomorphe à S_{n-1} par le Fait 2.1 :

$$\psi_n(H_n) \leq Stab_{S_n}(n) = S_{n-1} \ .$$

Ainsi :

$$|\psi_n(H_n)| = |H_n| = [L_n : E_n] = \frac{[L_n : \mathbb{Q}]}{[E_n : \mathbb{Q}]} = \frac{n!}{n} = |S_{n-1}| \ ,$$

d'où l'on déduit que

$$\psi_n(H_n) = S_{n-1}$$

est un sous-groupe maximal (Fait 2.1) de $\psi_n\big(Gal(L_n/\mathbb{Q})\big) = S_n$ (Prop. 2.2). Par conséquent, $H_n = Gal(L_n/E_n)$ est un sous-groupe maximal de $Gal(L_n/\mathbb{Q})$. Il résulte alors de la bijection de Galois que $E_n/\mathbb{Q}$ est une extension simple.

Par ailleurs, l'hypothèse $n \geq 3$ implique quant à elle que S_{n-1} n'est pas normal dans S_n (par exemple $(1\,2)^{(1\,n)} = (2\,n) \notin S_{n-1}$) ; donc $E_n/\mathbb{Q}$ n'est pas galoisienne. □

3. Un contre-exemple au "Théorème M" pour une extension infinie

Nous montrerons au chapitre 6 suivant, via le "Théorème M", que toute extension finie se dissocie canoniquement en une "extension quotient galtourable maximale" et une "sous-extension d'intourabilité maximale". Il est alors naturel de se demander si cette dissociation admet un analogue dans le cas d'une extension infinie. Le contre-exemple suivant de cette section, inséré dans le présent chapitre car indépendant de ce qui suit, nous prouve en particulier que, dans nos définitions, cet analogue n'existe pas.

Notations 3.1. Dans toute cette section, notons (E) la suite infinie de corps emboîtés

$$(E) \qquad E_0 \trianglelefteq E_1 \trianglelefteq \cdots \trianglelefteq E_n \trianglelefteq E_{n+1} \trianglelefteq \cdots \leq E_\infty$$

avec

$$\begin{cases} E_0 := \mathbb{Q} \ , \ x_0 := 2 \ ; \\ E_n := \mathbb{Q}(x_n) = E_{n-1}(x_n) \ , \ x_n := \sqrt[2^n]{2} \qquad (n \in \mathbb{N} \setminus \{0\}) \ ; \\ E_\infty := \bigcup_{n \in \mathbb{N}} E_n \ . \end{cases}$$

Scholie. Il ne s'agit pas d'une tour de corps au sens de notre définition & convention 1.1 du chapitre 2 , puisqu'il y a une infinité de corps.

Pour la démonstration du Fait 3.4 à suivre, nous aurons besoin des lemmes suivants :

Lemme 3.2. *Tout corps intermédiaire M entre E_0 et E_∞ : $E_0 \leq M \leq E_\infty$ induit l'ensemble non-vide*

$$I_M := \{n \in \mathbb{N} \mid x_n \in M\} = \{n \in \mathbb{N} \mid E_n \leq M\} ,$$

qui est infini si et seulement si $M = E_\infty$.

Démonstration. Notons tout d'abord que les deux définitions de I_M coïncident, puisque x_n est un élément primitif de E_n sur $\mathbb{Q}$ pour tout $n \in \mathbb{N}$.

Comme $x_0 = 2$, I_M contient toujours 0, et n'est donc jamais vide. Soit maintenant M un corps intermédiaire tel que I_M soit infini. Alors :

$$\forall n \in \mathbb{N} \quad \exists m \in \mathbb{N} \quad m \geq n \qquad m \in I_M ;$$

i.e.

$$\forall n \in \mathbb{N} \quad \exists m \geq n \quad E_m \leq M .$$

Par la croissance de la suite $(E_n)_{n\in\mathbb{N}}$, on a donc

$$\forall n \in \mathbb{N} \quad \exists m \geq n \quad E_n \leq E_m \leq M .$$

Ainsi

$$E_\infty = \bigcup_{n\in\mathbb{N}} E_n \leq M \leq E_\infty \qquad \text{i.e. } E_\infty = M .$$

La réciproque est immédiate puisque $I_{E_\infty} = \mathbb{N}$. □

Lemme 3.3. *Pour tout corps intermédiaire M entre E_0 et E_∞ : $E_0 \leq M \leq E_\infty$, vérifiant la propriété suivante*

$$\exists m \in \mathbb{N} \quad x_m \in M \quad x_{m+1} \notin M ,$$

le polynôme minimal de x_{m+2} sur M est

$$Irr(x_{m+2}, M, X) = X^4 - x_m .$$

Démonstration. Comme $x_m \in M$, $P_m(X) := X^4 - x_m \in M[X]$; et on a $P_m(x_{m+2}) = 0$ par définition des x_n. Donc $Irr(x_{m+2}, M, X)$ divise

$$P_m(X) = (X - x_{m+2})(X + x_{m+2})(X - i\, x_{m+2})(X + i\, x_{m+2}) .$$

Par ailleurs, l'extension $M(x_{m+1})/M$ est quadratique puisque $x_{m+1} = \sqrt{x_m} \notin M$. On en déduit que

$$[M(x_{m+2}) : M] = 2[M(\sqrt{x_{m+1}}) : M(x_{m+1})] \in \{2, 4\} .$$

Mais si le polynôme minimal de x_{m+2} sur M était de degré 2, il existerait un $l \in \{1, 2, 3\}$ tel que

$$Irr(x_{m+2}, M, X) = (X - x_{m+2})(X - i^l\, x_{m+2}) ;$$

et son terme constant serait $i^l\, x_{m+2}^2 = i^l\, x_{m+1} \in M$. Or ceci est imposible pour $l = 2$ car $x_{m+1} \notin M$; et pour $l = 1$ ou 3 car M est un corps réel.
Finalement $[M(x_{m+2}) : M] = 4$ et $P_m(X) = Irr(x_{m+2}, M, X)$. □

Fait 3.4. *L'extension E_∞/E_0 n'est pas galtourable : $E_\infty \nwarrow\!\!\searrow E_0$, et n'admet aucune sous-extension galsimple.*

Démonstration. Raisonnons par l'absurde en supposant que l'extension E_∞/E_0 soit galtourable, i.e. qu'elle admet une tour galoisienne

$$(T) \qquad E_0 = T_0 \trianglelefteq \cdots \trianglelefteq T_j \trianglelefteq \cdots \trianglelefteq T_p = E_\infty \ .$$

Comme E_∞/E_0 est clairement de degré infini, l'une au moins des marches de (T) est infinie :

$$\exists j \in \{0, \ldots, p-1\} \quad [T_{j+1} : T_j] = \infty.$$

Notons j le plus grand entier tel que la marche T_{j+1}/T_j soit infinie :

$$\forall k \in \{0, \ldots, p-1\} \quad k \geq j+1 \quad \Rightarrow \quad [T_{k+1} : T_k] < \infty \ .$$

Par transitivité du degré, l'extension E_∞/T_{j+1} est finie, et elle est séparable puisque nous sommes en caractéristique nulle. On peut donc lui appliquer le théorème de l'élément primitif :

$$\exists x \in E_\infty \quad E_\infty = T_{j+1}(x) \ .$$

Ainsi :

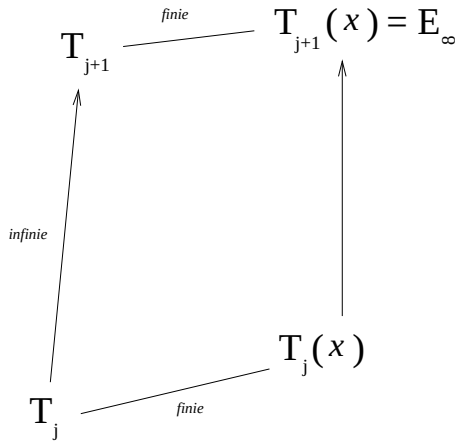

FIG. 24. *L'extension infinie $E_\infty/T_j(x)$*

d'où il résulte que $[E_\infty : T_j(x)] = \infty$. En particulier $T_j(x)$ est distinct de E_∞. On déduit alors du lemme 3.2 que l'ensemble $I_{T_j(x)}$ est fini. Notons m son plus grand élément :

$$m := max\ I_{T_j(x)} \ .$$

On a $m \in I_{T_j(x)}$ et $m+1 \notin I_{T_j(x)}$, i.e. $x_m \in T_j(x)$ et $x_{m+1} \notin T_j(x)$. Le lemme 3.3 nous assure alors que

$$Irr(x_{m+2}, T_j(x), X) = X^4 - x_m \ .$$

Mais par ailleurs, l'extension $E_\infty/T_j(x)$ est galoisienne en tant que translatée de la marche galoisienne $T_{j+1} \nearrow T_j$ de (T). Comme $x_{m+2} \in E_\infty$, toutes les racines du polynôme irréductible $X^4 - x_m$ doivent être dans E_∞ : absurde, puisque E_∞ est un corps réel tandis que deux des racines de $X^4 - x_m$ sont complexes non-réelles.Il est donc prouvé que E_∞/E_0 n'est pas galtourable.

Raisonnons encore une fois par l'absurde en supposant l'existence d'une sous-extension galsimple $E_\infty \nearrow M$ de E_∞/E_0. Par définition (cf. Chap. 2, Déf. 1.6), E_∞/M est non-triviale, et on déduit du lemme 3.2 que I_M est fini. Notons $m := max\ I_M$. On a :

$$x_m \in M \quad \text{et} \quad x_{m+1} \notin M \ ;$$

d'où par le lemme 3.3

$$Irr(x_{m+2}, M, X) = X^4 - x_m \ .$$

Ceci implique en particulier que $[M(x_{m+2}) : M] = 4$ et l'on a la tour

$$M \lhd M(x_{m+1}) < M(x_{m+2}) \leq E_\infty$$

qui contredit la galsimplicité de $E_\infty \nearrow M$. □

4. Extensions galsimples non galoisiennes

Nous utiliserons les résultats de cette section pour mettre en évidence le rôle central du corps d'intourabilité de toute extension finie.

La proposition suivante, vraie quant à elle pour un degré quelconque, montre que la galsimplicité passe toujours au quotient.

Proposition 4.1. *Toute extension quotient propre d'une extension galsimple est galsimple non galoisienne. Précisément :*

$$\forall (L \nearrow K) \qquad \forall M \qquad K < M < L \quad \Rightarrow \quad (M \nearrow\!\!\!\!\!\!\nwarrow K) \ .$$

Démonstration. La galsimplicité de L/K interdit que l'extension quotient propre M/K soit galoisienne. Et elle est nécessairement galsimple car s'il existait un corps F tel que $K \lhd F < M$, on en déduirait $K \lhd F < L$: contradiction. □

Prouvons maintenant qu'il y a transitivité de la galsimplicité non galoisienne.

Proposition 4.2. *Pour toute tour de corps $F_0 \leq F_1 \leq F_2$, le fait que les extensions F_1/F_0 et F_2/F_1 soient galsimples non galoisiennes implique qu'il en est de*

même de l'extension F_2/F_0. Précisément, dans nos notations (cf. Chap. 2, Not. 1.9) :

$$\big(\ (F_1 \nearrow\!\!\!\!\!\!\nwarrow F_0)\ ,\ (F_2 \nearrow\!\!\!\!\!\!\nwarrow F_1)\ \big) \quad \Rightarrow \quad (F_2 \nearrow\!\!\!\!\!\!\nwarrow F_0)\ .$$

Démonstration. On sait déjà que l'extension F_2/F_0 n'est pas galoisienne, sans quoi l'on aurait la sous-extension galoisienne $F_2 \nearrow F_1$. Raisonnons par l'absurde en supposant que l'extension F_2/F_0 ne soit pas galsimple. Comme elle n'est pas triviale puisque F_1/F_0 (et F_2/F_1) ne l'est pas, cela signifie qu'il existe un corps intermédiaire M tel que

$$F_0 \lhd M < F_2\ .$$

En translatant alors l'extension galoisienne $M \nearrow F_0$ par l'extension F_1/F_0, on obtient l'extension galoisienne MF_1/F_1, et donc

$$F_1 \trianglelefteq MF_1 \leq F_2\ .$$

Comme l'extension $(F_2 \nearrow\!\!\!\!\!\!\nwarrow F_1)$ est galsimple non galoisienne, son extension galoisienne quotient (MF_1/F_1) est nécessairement triviale :

$$MF_1 = F_1 \quad \text{i.e.} \qquad M \leq F_1\ .$$

De sorte que l'on a la tour

$$F_0 \lhd M \leq F_1\ .$$

Comme l'extension $F_1 \nearrow F_0$ est galsimple, on a donc $M = F_1$. Et finalement l'extension $(M \nearrow F_0) = (F_1 \nearrow F_0)$ est galoisienne : contradiction. □

La proposition 4.3 suivante fournit une classe infinie d'extensions galsimples non galoisiennes immédiatement utilisables car sur le corps $\mathbb{Q}$ des nombres rationnels. Nous nous en servirons dans les exemples du chapitre 6.

Rappelons d'abord le critère d'irréductibilité des polynômes $X^n - a$ que nous utiliserons également au chapitre 6

Theorem. [**23**, p.297, Th. 9.1]
Let K be a field and $n \geq 2$ an integer. Let $a \in K$, $a \neq 0$. Assume that for all prime numbers p such that $p|n$ we have $a \notin K^p$, and if $4|n$ then $a \notin -4K^4$. Then $X^n - a$ is irreducible in $K[X]$.

Proposition 4.3. *Soit $L = \mathbb{Q}(\alpha)/\mathbb{Q}$ une extension radicale où $\alpha^n = a \in \mathbb{Q}$ avec*
(1) a positif : $a \in \mathbb{Q}_+$, et $n \geq 3$ impair,
(2) pour tout diviseur d de n : $d \mid n$, $a \notin \mathbb{Q}^d$.
Alors l'extension $L/\mathbb{Q}$ est galsimple non galoisienne.

Démonstration. D'après le théorème précédent, le polynôme $X^n - a$ est irréductible sur $\mathbb{Q}$, d'où $X^n - a = Irr(\alpha, \mathbb{Q}, L)$ et $[L : \mathbb{Q}] = n$. Soit alors I un corps intermédiaire entre $\mathbb{Q}$ et L. D'après la proposition de la démonstration de

l'exemple 1.10 du chapitre 2, il existe nécessairement un diviseur δ de n tel que $I = \mathbb{Q}(\beta)$ avec $\beta^\delta = a$. Raisonnons par l'absurde en supposant que $I/\mathbb{Q}$ soit une extension galoisienne non triviale : $I \nearrow \mathbb{Q}$, $[I : \mathbb{Q}] \geq 2$. Le polynôme $X^\delta - a$ est aussi irréductible sur $\mathbb{Q}$ car

$$d|\delta \quad \Rightarrow \quad d|n \quad \Rightarrow \quad a \notin \mathbb{Q}^d$$

et le critère d'irréductibilité s'applique. Donc $X^\delta - a = Irr(\beta, \mathbb{Q}, X)$ et

$$2 \leq [I : \mathbb{Q}] = \delta \mid n \text{ impair.}$$

Or dire que $I = \mathbb{Q}(a^{1/\delta})/\mathbb{Q}$ est galoisienne implique que $\mu_\delta \subseteq I$.

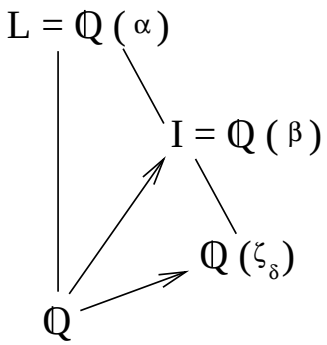

FIG. 25. *Galsimplicité de* $\mathbb{Q}(a^{1/n})/\mathbb{Q}$ *contredite*

Et on sait que $[\mathbb{Q}(\mu_\delta) : \mathbb{Q}] = \varphi(\delta)$ où $2 \leq \delta$ impair est divisible par un nombre premier impair p. Il en résulte que l'entier pair $p - 1$ divise $[I : \mathbb{Q}]$ impair : contradiction. Il est donc prouvé que $L/\mathbb{Q}$ est galsimple. □

Chapitre 6

THÉORÈME M

Ce chapitre 6 détaille un résultat non publié de Richard Massy (confer remerciements) que nous sommes convenus d'appeler le "théorème M" [1](Sect. 1). Ce théorème M est la clef de la généralisation à toutes les extensions finies des théorèmes de dissociation précédents pour les extensions galtourables. Il découvre qu'à toute extension finie L/K est attachée un invariant unique, son "corps d'intourabilité $M(L/K)$" qui est un corps intermédiaire au-delà duquel l'extension n'est plus galtourable. Le rôle central du corps d'intourabilité $M(L/K)$ est mis en lumière section 2 : il dissocie l'extension L/K en une extension quotient galtourable maximale $M(L/K)\nearrow K$ et une sous-extension d'intourabilité maximale $L/M(L/K)$, ou bien triviale, ou bien galsimple non galoisienne. Dans la dernière section, nous réalisons tous les corps cyclotomiques $\mathbb{Q}(\zeta_n)$ comme corps d'intourabilité d'une classe infinie d'extensions $L/\mathbb{Q}$ avec $L/\mathbb{Q}(\zeta_n)$ galsimple, donc non triviale, et non galoisienne : $(L\not\nearrow\mathbb{Q}(\zeta_n))$ (cf. Chap.2, Not. 1.9).

1. Quatrième théorème de dissociation

Il s'agit ici d'énoncer et de prouver le résultat central suivant pour généraliser les théorèmes de dissociation du chapitre 4, qui se limitaient au cas galtourable.

Théorème 1.1. *($4^{ème}$ théorème de dissociation, dit "Théorème M")*
Pour toute extension finie L/K , il existe un corps intermédiaire M et un seul entre K et L, vérifiant à la fois les deux propriétés suivantes :

(1) L'extension M/K est galtourable ;

(2) La sous-extension L/M est soit triviale, soit galsimple non galoisienne.

Scholie. Dans nos notations (Chap. 2, Not. 1.9), ce théorème M se symbolise comme suit :

$$\forall L/K \quad [L:K]<\infty\ ,\ \exists!\, M \quad K\le M\le L \quad (M\nearrow K\ ,\ L=M \text{ ou } (L\not\nearrow M))\ .$$

Démonstration. Existence. Le théorème est trivial pour $L=K$ car $K\nearrow K$ implique $K\swarrow K$ (Chap.2, Déf.1.4, Scholie (2)). Procédons par récurrence sur $n:=[L:K]\ge 2$ en supposant l'existence d'un corps intermédiaire de l'énoncé pour toute extension de degré $\le n-1$. Deux cas se présentent :

[1] plutôt que l'ambigu jeu de mots "corps de Massy"!

- Ou bien L/K est galsimple. Si elle est galoisienne (resp. non galoisienne) $M = L$ (resp. $M = K$) convient.
- Ou bien L/K n'est pas galsimple. Comme elle n'est pas triviale, cela signifie par définition (Chap. 2, Déf. 1.6.(2)) qu'il existe un corps K_1 tel que

$$K \lhd K_1 < L \ .$$

En particulier $[L : K_1] \leq n - 1$ et l'hypothèse de récurrence s'applique : il existe un corps M tel que

$$(M \nearrow K_1 \ , \ L = M \text{ ou } (L \not\nearrow M)) \ .$$

Or K_1/K est galtourable en tant qu'extension galoisienne, donc par le Fait 2.7 du chapitre 2,

$$(K_1 \nearrow K \ , \ M \nearrow K_1) \quad \Rightarrow \quad (M \nearrow K) \ ;$$

et le corps M remplit les conditions de l'énoncé.

Unicité. Soit M' un autre corps intermédiaire entre K et L satisfaisant les deux conditions de l'énoncé. Comme la translatée d'une extension galtourable est toujours une extension galtourable (cf. Chap. 2, Cor 2.4 ou Th. 2.3), avoir M/K galtourable implique que l'extension MM'/M' est galtourable.

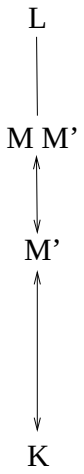

FIG. 26. *Translatée de M/K par M'*

Considérons une tour galoisienne (F) de MM'/M'

$$(F) \qquad M' = F_0 \trianglelefteq \cdots \trianglelefteq F_i \trianglelefteq \cdots \trianglelefteq F_m = MM' \ ,$$

et sa tour stricte associée $(F_<)$ (qui existe même pour une extension triviale : cf. Chap. 3, remarque. 2.2.(1)). D'après le corollaire 2.6 du chapitre 3, cette tour stricte associée $(F_<)$ est nécessairement galoisienne :

$$(F_<) \qquad M' = F_{<0} \lhd \cdots \lhd F_{<j} \lhd \cdots \lhd F_{<h} = MM' \ .$$

Supposons que l'on ait $h \geq 1$ de sorte que

$$M' \lhd F_{<1} \leq MM' \leq L \, .$$

En particulier $L \neq M'$, d'où $(L \not\nwarrow M')$ par définition de M'. Mais alors, on ne peut avoir $M' \lhd F_{<1} < L$ par la galsimplicité de L/M', ni $F_{<1} = L$ puisque L/M' n'est pas galoisienne. La seule possibilité est donc que $h = 0$, autrement dit $MM' = M'$ i.e. $M \leq M'$. En échangeant les rôles de M et M', on prouve de même que $M' \leq M$, et finalement $M = M'$. □

Remarque 1.2. Nous venons de démontrer que toute extension finie se dissocie en une extension galtourable et, éventuellement, une extension galsimple. Le théorème M justifie donc à lui seul l'introduction de la galtourabilité et de la galsimplicité.

Définition 1.3. Dans les notations du théorème M (Th. 1.1) précédent, nous appelons $M = M(L/K)$ "Le corps d'intourabilité de L/K".

Corollaire 1.4. *Une extension finie L/K est galtourable si et seulement si son corps d'intourabilité coïncide avec son corps sommet. Autrement dit, on a l'équivalence*

$$(L \not\nearrow K) \quad \Leftrightarrow \quad M(L/K) = L \, .$$

En particulier, on a toujours l'égalité $M(M(L/K)/K) = M(L/K)$.

Démonstration. Si L/K est galtourable, le corps L lui-même vérifie les deux conditions du théorème 1.1. Par unicité du corps d'intourabilité, on en déduit $M(L/K) = L$. Inversement dans ce cas, L/K est galtourable puisqu'il en est ainsi de $M(L/K)/K$ par définition. □

Exemple 1.5. Dans les notations 3.1 du chapitre 5 ;

$$E_0 = \mathbb{Q} \, , \quad E_\infty = \bigcup_{n \in \mathbb{N}} \mathbb{Q}(\sqrt[2^n]{2}) \, ,$$

il n'existe pas de corps intermédiaire entre E_0 et E_∞ tel que les conditions (1) et (2) du théorème 1.1 soient vérifiées.

Démonstration. C'est clair d'après le Fait 3.4 du chapitre 5. □

2. Le rôle central du corps d'intourabilité

Nous allons prouver que le corps d'intourabilité du théorème M commande la galtourabilité (resp. l'intourabilité) des extensions quotients (resp. des sous-extensions) de toute extension finie en induisant deux maximalités déterminantes.

Proposition & Définition 2.1. *Soient L/K une extension finie et $M(L/K)$ son corps d'intourabilité (Déf. 1.3).*

(1) Pour toute extension quotient galtourable $F\nearrow K$ de L/K : $K \leq F \leq L$, on a nécessairement $F \leq M(L/K)$.

(2) L'extension galtourable $M(L/K)\nearrow K$ est maximale dans l'ensemble des extensions quotients galtourables de L/K muni de la relation d'ordre du (1) du lemme 2.3 du chapitre 1.

(3) L'extension $M(L/K)\nearrow K$ est la seule extension quotient de L/K vérifiant la maximalité du (2).

Nous appelons $M(L/K)\nearrow K$ "l'extension quotient galtourable maximale de L/K."

Démonstration. Posons $M := M(L/K)$.

(1) Soit $F\nearrow K$ une extension quotient galtourable de L/K. D'après le corollaire 2.4 du chapitre 2, l'extension $FM\nearrow M$ est également galtourable. Elle admet ainsi une tour galoisienne que l'on peut supposer stricte (Chap. 3, Cor. 2.6) :

$$M = F_0 \lhd \cdots \lhd F_n = F\,M\ .$$

Raisonnons par l'absurde en supposant $M \neq FM$. Dès lors on a $n \geq 1$, et en particulier $M \lhd F_1 \leq L$. L'extension L/M est donc non triviale. C'est qu'elle est galsimple non galoisienne en vertu du théorème M. Or avoir $F_1 = L$ contredit le fait que L/M est non galoisienne, et avoir $F_1 \neq L$ contredit la galsimplicité de L/M. Ceci prouve que nécessairement $M = FM$, i.e. $F \leq M$.

(2) Pour toute extension quotient galtourable $F\nearrow K$, on a $F \leq M$ d'après le (1) précédent, ce qui signifie, par définition de la relation d'ordre, que

$$(F\nearrow K)\ \leq\ (M\nearrow K)\ .$$

(3) Si $(M'\nearrow K)$ est une extension quotient galtourable maximale de L/K, on a $M' \leq M$ d'après le (1), i.e. $(M'\nearrow K)\ \leq\ (M\nearrow K)$, d'où $M' = M$ par la maximalité de $M'\nearrow K$. □

La proposition suivante induira la notion de "tour d'élévation" du chapitre 7 final.

Proposition 2.2. *Soit L/K une extension finie. Pour tout corps intermédiaire $F : K \leq F \leq L$, le corps d'intourabilité de l'extension quotient F/K est inclus dans celui de l'extension L/K. Précisément :*

$$M(F/K) \ \leq \ F \cap M(L/K) \ .$$

Démonstration. L'extension $M(F/K)\nearrow\!\!\swarrow K$ est galtourable (Th. 1.1). D'après le (1) de la proposition & définition 2.1, on a donc nécessairement

$$M(F/K) \ \leq \ M(L/K) \ .$$

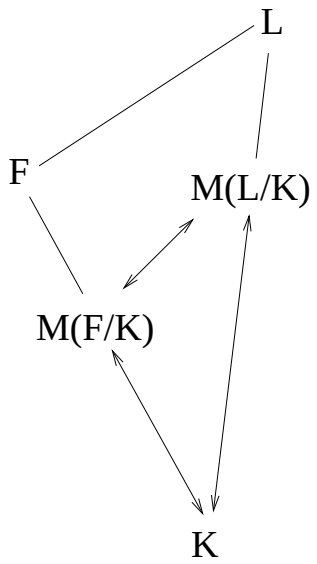

FIG. 27. *Corps d'intourabilité d'une extension quotient*

□

Proposition & Définition 2.3. *Soient L/K une extension finie et $M(L/K)$ son corps d'intourabilité (Déf. 1.3).*

(0) Nous appelons "sous-extension d'intourabilité de L/K" toute sous-extension L/F , $K \leq F \leq L$, ou bien triviale : $L = F$, ou bien galsimple non galoisienne : $(L\nearrow\!\!\nwarrow F)$.

(1) Pour toute sous-extension d'intourabilité L/F de L/K, on a nécessairement $M(L/K) \leq F$.

(2) L'extension $(L/M(L/K))$ est maximale dans l'ensemble des sous-extensions d'intourabilité de L/K muni de la relation d'ordre du (1) du lemme 2.3 du chapitre 1.

(3) L'extension $(L/M(L/K))$ est la seule sous-extension d'intourabilité de L/K vérifiant la maximalité du (2).

Nous appelons $(L/M(L/K))$ "la sous-extension d'intourabilité maximale de L/K".

Démonstration. (1) Soit L/F une sous-extension d'intourabilité de L/K. Quand $F = L$, le résultat est trivial. Supposons $F \neq L$. D'après le (0), c'est donc que L/F est une extension galsimple non galoisienne : $(L \nearrow\!\!\!\!\!\!\nwarrow F)$. Distinguons alors deux cas.
- Si F est égal au corps d'intourabilité de F/K, on déduit du théorème M (Th. 1.1) dans L/K que

$$\Big((F = M(F/K) \swarrow\!\!\!\!\!\!\nearrow K)\ ,\quad (L \nearrow\!\!\!\!\!\!\nwarrow F)\Big) \quad \Rightarrow \quad F = M(L/K)\ ,$$

et l'on a le résultat voulu.
- Si $F \neq M(F/K)$, on a l'extension galsimple non galoisienne $(F \nearrow\!\!\!\!\!\!\nwarrow M(F/K))$, et par la proposition 4.2 du chapitre 5 :

$$\Big((F \nearrow\!\!\!\!\!\!\nwarrow M(F/K))\ ,\quad (L \nearrow\!\!\!\!\!\!\nwarrow F)\Big) \quad \Rightarrow \quad \Big(L \nearrow\!\!\!\!\!\!\nwarrow M(F/K)\Big)\ .$$

On en déduit, une fois encore par le théorème M, que

$$\Big((M(F/K) \swarrow\!\!\!\!\!\!\nearrow K)\ ,\quad (L \nearrow\!\!\!\!\!\!\nwarrow M(F/K))\Big) \quad \Rightarrow \quad M(L/K) = M(F/K) \leq F\ .$$

(2) Soit L/F une sous-extension d'intourabilité de L/K. D'après le (1), on a $M(L/K) \leq F$, ce qui signifie $(L/F) \leq (L/M(L/K))$.

(3) Si L/M' est une sous-extension d'intourabilité maximale de L/K, on déduit du (1) que $M(L/K) \leq M'$, i.e. $(L/M') \leq (L/M(L/K))$, d'où $M' = M(L/K)$ par la maximalité de L/M'. □

Définition 2.4. Soient L/K une extension finie et $M(L/K)$ son corps d'intourabilité.

(1) Nous appelons "degré de galtourabilité de L/K", et nous notons $[L : K]_{gal}$, le degré de l'extension quotient galtourable maximale de L/K (Prop. & Déf. 2.1) :

$$[L : K]_{gal} := [M(L/K) : K]\ .$$

(2) Nous appelons "degré d'intourabilité de L/K", et nous notons $[L : K]_{int}$, le degré de la sous-extension d'intourabilité maximale de L/K (Prop. & Déf. 2.3) :

$$[L : K]_{int} := [L : M(L/K)]\ .$$

(3) Nous appelons "degré de tourabilité de L/K", et nous notons $[L : K]_{tour}$, le couple d'entiers formé par le degré de galtourabilité et le degré d'intourabilité de

L/K :

$$[L:K]_{tour} := ([L:K]_{gal}, [L:K]_{int}) .$$

3. Exemples de corps d'intourabilité

Nous avons déjà exhibé une classe infinie d'extensions simples non galoisiennes $\mathbb{Q}(\theta)/\mathbb{Q}$ où $n \geq 3$ et $\theta^n - \theta - 1 = 0$ (Chap. 2, Ex. 1.10.(iii)). Ceci prouve en particulier que :

Proposition 3.1. *Tout entier naturel distinct de* 0 *et* 2 *est un degré d'intourabilité (Déf. 2.4.(2)).*

Scholie. Une extension quadratique étant nécessairement galoisienne, 2 est exclu.

Cependant, le corps d'intourabilité des extensions induites par les polynômes $\theta^n - \theta - 1 = 0$ est toujours égal à $\mathbb{Q}$. Dans cette section, nous exhibons une classe infinie d'extensions finies où les extensions quotients galtourables maximales, ainsi que les sous-extensions d'intourabilité maximales, sont non triviales.

Nous utiliserons le Fait élémentaire suivant, dans lequel une racine primitive $\nu^{\text{ème}}$ de l'unité est notée génériquement $\zeta_\nu \quad (\nu \in \mathbb{N} \setminus \{0\})$.

Fait 3.2. *Pour tout couple d'entiers (m,n) premiers entre eux, on a le parallélogramme galoisien cyclotomique*

$$[\mathbb{Q}, \mathbb{Q}(\zeta_m), \mathbb{Q}(\zeta_{mn}), \mathbb{Q}(\zeta_n)] .$$

Démonstration. Écrivons $m = p_1^{e_1} \ldots p_r^{e_r}$ et $n = q_1^{f_1} \ldots q_s^{f_s}$ où les p_i et les q_j sont deux à deux étrangers. La décomposition en facteurs premier de mn est donc $mn = p_1^{e_1} \ldots p_r^{e_r} q_1^{f_1} \ldots q_s^{f_s}$, et d'après [**24**, p.74, Th.2]

$$\begin{aligned} \mathbb{Q}(\zeta_{mn}) &= \mathbb{Q}(\zeta_{p_1^{e_1}}) \ldots \mathbb{Q}(\zeta_{p_r^{e_r}}) \, \mathbb{Q}(\zeta_{q_1^{f_1}}) \ldots \mathbb{Q}(\zeta_{q_s^{f_s}}) \\ &= \mathbb{Q}(\zeta_m) \, \mathbb{Q}(\zeta_n) . \end{aligned}$$

De plus

$$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q} \qquad ([\mathbf{41}, \text{p.11}] \text{ ou } [\mathbf{24}, \text{p.75}]) .$$

D'où la conclusion. □

Lemme 3.3. *Soient deux entiers d et n tels que*

$$d \geq 2 , \quad 4 \nmid d , \quad n \geq 1 , \quad pgcd(d,n) = 1 .$$

Notons $E_n := \mathbb{Q}(\zeta_n)$ le $n^{ème}$ corps cyclotomique sur $\mathbb{Q}$. Pour tout nombre premier $l \in \mathbb{N}$ ne divisant pas n et tout $\rho \in \mathbb{C}$ tel que $\rho^d = l$, le polynôme minimal de ρ sur E_n est $X^d - l$ et $E_n(\rho)/E_n$ est de degré d :

$$Irr(\rho, E_n, X) = X^d - l , \quad [E_n(\rho) : E_n] = d .$$

Démonstration. Soit q l'un quelconque des nombres premiers divisant d (≥ 2). Raisonnons par l'absurde en supposant que $l \in E_n^q$, i.e. $l = e_n^q$ avec $e_n \in E_n$. A fortiori pour les idéaux engendrés dans l'anneau $\mathbb{Z}[\zeta_n]$ des entiers de E_n

$$l\,\mathbb{Z}[\zeta_n] = (e_n\,\mathbb{Z}[\zeta_n])^q\ ,$$

de sorte que, pour tout idéal premier $\mathcal{P}$ de $\mathbb{Z}[\zeta_n]$

$$\mathrm{ord}_{\mathcal{P}}(l\,\mathbb{Z}[\zeta_n]) = q\,\mathrm{ord}_{\mathcal{P}}(e_n\,\mathbb{Z}[\zeta_n])\ ,$$

d'où $\mathrm{ord}_{\mathcal{P}}(e_n\,\mathbb{Z}[\zeta_n]) \geq 0$. L'idéal $e_n\,\mathbb{Z}[\zeta_n]$ est donc entier, et se décompose en idéaux premiers dans l'anneau de Dedekind $\mathbb{Z}[\zeta_n]$

$$e_n\,\mathbb{Z}[\zeta_n] = \mathfrak{P}_1^{v_1} \ldots \mathfrak{P}_r^{v_r} \quad , \qquad v_i > 0 \quad (i = 1, \ldots, r)\ .$$

On en déduit

$$l\,\mathbb{Z}[\zeta_n] = \mathfrak{P}_1^{q\,v_1} \ldots \mathfrak{P}_r^{q\,v_r} \quad , \qquad v_i > 0 \quad (i = 1, \ldots, r)$$

avec $q \geq 2$. Ceci exprime que $l\,\mathbb{Z}$ se ramifie dans E_n. D'après [**24**, p.74, Th. 2], ceci implique $l \mid n$: contradiction. C'est donc que, pour tout q divisant d, $l \notin E_n^q$. Comme $4 \nmid d$, on déduit alors du critère d'irréductibilité rappelé avant la proposition 4.3 du chapitre 5 que $X^d - l$ est irréductible dans $E_n[X]$. D'où la conclusion. □

Remarque 3.4. Une autre démonstration du Lemme 3.3 est d'utiliser la galsimplicité de $\mathbb{Q}(\rho)/\mathbb{Q}$ (cf. Chap. 5, Prop. 4.3).

On en déduit le

Fait 3.5. *Dans les notations du lemme 3.3, supposons de plus que d soit impair. Pour tout entier $\delta \neq d$ divisant d : $\delta \mid d$, on a*

$$\mu_p \cap E_n(\rho^\delta) = \mathbb{1}$$

quel que soit le nombre premier p divisant $\frac{d}{\delta}$: $p \mid \frac{d}{\delta}$. En particulier, pour tout entier δ', multiple de δ, distinct de δ et divisant d : $\delta' \mid d$, l'extension $(E_n(\rho^\delta)/E_n(\rho^{\delta'}))$ n'est pas galoisienne.

Démonstration. Prouvons d'abord le résultat pour $\delta = 1$. Raisonnons par l'absurde en supposant que $\mu_p \cap E_n(\rho) \neq \mathbb{1}$. Comme $pgcd(d, n) = 1$ (cf. lemme 3.3), p ne divise pas n, et par le Fait 3.2, on a le parallélogramme galoisien

$$[\mathbb{Q}, \mathbb{Q}(\zeta_n), \mathbb{Q}(\zeta_{pn}), \mathbb{Q}(\zeta_p)] \quad (\text{cf. FIG. 28})\ .$$

Or $[E_n(\rho) : E_n] = d$ par lemme 3.3 précédent tandis que

$$[\mathbb{Q}(\zeta_{pn}) : E_n] = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1\ .$$

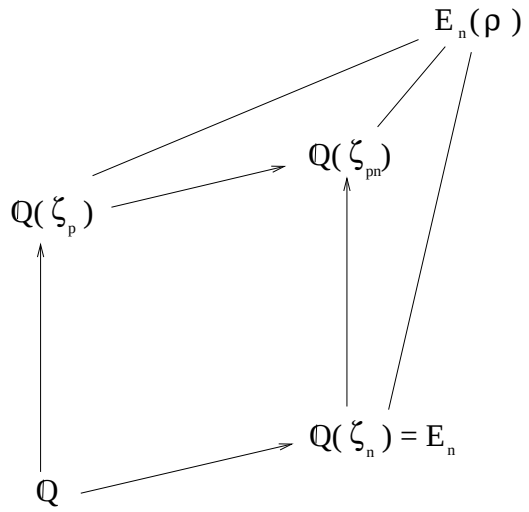

FIG. 28. *Parallélogramme* $[\mathbb{Q}, \mathbb{Q}(\zeta_n), \mathbb{Q}(\zeta_{pn}), \mathbb{Q}(\zeta_p)]$

Mais alors $p-1$ pair divise d impair : absurde. Ceci prouve l'égalité $\mu_p \cap E_n(\rho) = \mathbb{1}$. Soit maintenant δ' un entier différent de 1 divisant $d : 1 \neq \delta' \mid d$. Appliquons le lemme 3.3 à $\frac{d}{\delta'}$ et $\rho^{\delta'}$: comme $(\rho^{\delta'})^{\frac{d}{\delta'}} = \rho^d = l$, on a

$$[E_n(\rho^{\delta'}) : E_n] = \frac{d}{\delta'} .$$

On déduit alors de $[E_n(\rho^{\delta}) : E_n] = d$, que

$$[E_n(\rho) : E_n(\rho^{\delta'})] = \delta' .$$

Il en résulte que le polynôme minimal de ρ sur $E_n(\rho^{\delta'})$ est :

$$Irr(\rho, E_n(\rho^{\delta'}), X) = X^{\delta'} - \rho^{\delta'} = \prod_{j=0}^{\delta'-1} (X - \zeta_{\delta'}^j \rho) .$$

Avoir $E_n(\rho^{\delta})/E_n(\rho^{\delta'})$ galoisienne impliquerait donc que $\zeta_{\delta'} \in E_n(\rho^{\delta})$, et a fortiori que $\zeta_p \in E_n(\rho^{\delta})$ pour tout nombre premier p divisant $\delta' \neq 1$: contradiction d'après ce qui précède puisque par définition δ' divise d. Il est donc prouvé que $E_n(\rho^{\delta}) \nwarrow E_n(\rho^{\delta'})$ pour le cas $\delta = 1$.

Soit enfin δ un entier différent de d divisant $d : d \neq \delta \mid d$. Posons

$$P := \rho^{\delta} , \quad r := \frac{d}{\delta} , \quad \delta" := \frac{\delta'}{\delta} .$$

Clairement

$$P^r = \rho^d = l , \quad P^{\delta"} = \rho^{\delta'} .$$

De plus $\delta' \neq \delta$ i.e. $\delta" \neq 1$ et $\delta"$ divise r car δ' divise d. On peut donc appliquer le résultat précédent pour $\delta = 1$ avec la substitution

$$\begin{pmatrix} d & \rho & \delta' \\ r & P & \delta" \end{pmatrix}$$

qui nous dit que l'extension

$$(E_n(P)/E_n(P^{\delta"})) = (E_n(\rho^{\delta})/E_n(\rho^{\delta'}))$$

n'est pas galoisienne. □

Nous sommes maintenant en mesure de prouver le

Théorème 3.6. *Pour tous entiers : $d \geq 3$ impair et $n \geq 1$, tels que l'on ait $pgcd(d, n) = 1$, le couple $(\varphi(n), d)$ (où φ désigne l'indicateur d'Euler) est un degré de tourabilité (Déf. 2.4).*

Scholie . Cet énoncé sera amélioré au théorème 3.8 (cf. infra).

Démonstration. Comme dans le Fait 3.5, on se place dans les notations du lemme 3.3. Décomposons d en produit de nombres premiers p_i non nécessairement distincts : $d = \prod_{i=0}^{k} p_i$, et posons

$$\forall m \in \{1, \ldots, k+1\} \quad \delta_m := d/(\prod_{j=0}^{m-1} p_j) \ , \quad L_m := E_n(\rho^{\delta_m}) \ .$$

Prouvons, par récurrence finie sur m, que pour tout entier dans $\{1, \ldots, k+1\}$ l'extension L_m/E_n est galsimple non galoisienne :

$$\forall m \in \{1, \ldots, k+1\} \quad (L_m \nearrow\!\!\!\!\!\!\nwarrow E_n) \ .$$

Pour $m = 1$, on déduit directement du Fait 3.5 appliqué avec $\delta' = d$ que l'extension $L_1 := E_n(\rho^{\delta_1})/E_n$ n'est pas galoisienne. De plus, comme $(\rho^{\delta_1})^{p_0} = \rho^d = l$, on sait par le lemme 3.3 que

$$[L_1 : E_n] = p_0 \ ,$$

de sorte que L_1/E_n est une extension simple (Chap. 2, Ex. 1.10.(iii)), donc galsimple. Supposons maintenant le résultat vrai pour $m \in \{1, \ldots, k\}$ et démontrons le pour $m+1$. Par définition

$$\delta_m = p_m \, \delta_{m+1} \ .$$

D'autre part, en vertu du lemme 3.3 à nouveau

$$[L_m = E_n(\rho^{\delta_m}) : E_n] = \frac{d}{\delta_m} \ .$$

On en déduit

$$[L_{m+1} : E_n] = p_m \frac{d}{\delta_m} \ ,$$

et

$$[L_{m+1} : L_m] = p_m \ .$$

Ceci prouve que l'extension L_{m+1}/L_m est simple, donc galsimple. Et d'après le Fait 3.5, elle est non galoisienne :

$$L_{m+1} = E_n(\rho^{\delta_{m+1}}) \nwarrow\!\!\!\searrow E_n(\rho^{\delta_m}) = L_m \ .$$

De plus, par l'hypothèse de récurrence, on a $(L_m \not\nwarrow\!\!\!\searrow E_n)$. D'après la proposition 4.2 du chapitre 5, on en déduit l'extension galsimple non galoisienne $(L_{m+1} \not\nwarrow\!\!\!\searrow E_n)$. Ceci achève le raisonnement par récurrence.

En particulier pour $m = k + 1$, on a prouvé que l'extension $(E_n(\rho)/E_n)$ est galsimple non galoisienne. Finalement, comme l'extension $E_n = \mathbb{Q}(\zeta_n)/\mathbb{Q}$ est galoisienne, donc galtourable, il résulte du théorème M (Th. 1.1) que l'extension $(E_n(\rho)/E_n)$ est de degré de tourabilité $(\varphi(n), d)$. □

Pour généraliser le théorème 3.6 précédent, rappelons que

Proposition 3.7. [**8**, AVII.61, 5)]
Soit G un groupe commutatif fini. Pour tout entier q diviseur de l'ordre de G : $q \,|\, |G|$, il existe un sous-groupe de G d'ordre q.

Théorème 3.8. *Pour tous entiers : $d \geq 3$ impair et $n \geq 1$, tels que l'on ait $pgcd(d, n) = 1$, le couple (n, d) est un degré de tourabilité.*

Démonstration. Comme $pgcd(d, n^2) = 1$, on sait par le théorème 3.6 que le couple $(\varphi(n^2), d)$ est un degré de tourabilité. Précisément, le corps cyclotomique $E_{n^2} = \mathbb{Q}(\zeta_{n^2})$ est le corps d'intourabilité de l'extension $(E_{n^2}(\rho)/\mathbb{Q})$ où $\rho^d = l$ est un nombre premier ne divisant pas n (lemme 3.3). Retenons en particulier que

$$(E_{n^2}(\rho) \not\nwarrow\!\!\!\searrow E_{n^2}) \ , \quad [E_{n^2}(\rho) : E_{n^2}] = d \ .$$

Par ailleurs, il résulte directement de la formule explicitant l'indicateur d'Euler que n divise $\varphi(n^2)$. Appliquons la proposition 3.7 au groupe abélien $Gal(E_{n^2}/\mathbb{Q})$: comme n divise son ordre $\varphi(n^2)$, il existe un sous-groupe H d'ordre $\varphi(n^2)/n$:

$$|Gal(E_{n^2}/\mathbb{Q})| = \frac{\varphi(n^2)}{n}\, n = |H|\ n \ .$$

Considérons alors le corps des invariants dans E_{n^2} de H : $F_n := E_{n^2}^H$. Par le théorème d'Artin, $Gal(E_{n^2}/F_n) = H$, d'où

$$[F_n : \mathbb{Q}] = \frac{[E_{n^2} : \mathbb{Q}]}{[E_{n^2} : F_n]} = \frac{n \ | \ H \ |}{| \ H \ |} = n \ ;$$

et l'extension $F_n/\mathbb{Q}$ est galtourable (puisqu'elle est abélienne !). En adjoignant ρ à F_n, nous allons prouver que l'extension $F_n(\rho)/\mathbb{Q}$ est de degré de tourabilité

égal à (n, d). En translatant l'extension galoisienne $E_{n^2} \nearrow F_n$ par $F_n(\rho)/F_n$, nous obtenons l'extension galoisienne $E_{n^2}(\rho) \nearrow F_n(\rho)$ avec

$$Gal(E_{n^2}(\rho)/F_n(\rho)) \xrightarrow{\sim} Gal(E_{n^2}/(F_n(\rho) \cap E_{n^2}))$$

(cf. Chap. 2, Th. 2.1). On en déduit en particulier l'inégalité

$$[E_{n^2}(\rho) : F_n(\rho)] \leq [E_{n^2} : F_n] .$$

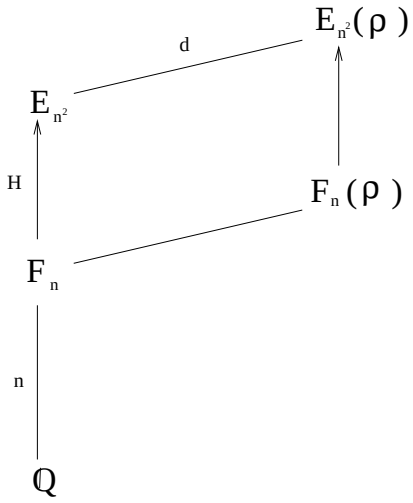

FIG. 29. (n, d) *degré de tourabilité*

Or

$$[E_{n^2}(\rho) : E_{n^2}][E_{n^2} : F_n] = [E_{n^2}(\rho) : F_n] = [E_{n^2}(\rho) : F_n(\rho)][F_n(\rho) : F_n] .$$

L'inégalité précédente oblige donc à avoir

$$[E_{n^2}(\rho) : E_{n^2}] \leq [F_n(\rho) : F_n] .$$

Mais ρ annule le polynôme $X^d - l \in F_n[X]$; donc $[F_n(\rho) : F_n] \leq d$. Comme on a rappelé que $[E_{n^2}(\rho) : E_{n^2}] = d$, ceci prouve que

$$[F_n(\rho) : F_n] = d .$$

Par ailleurs,

$$[E_{n^2}(\rho) : F_n(\rho)] = \frac{[E_{n^2}(\rho) : F_n]}{[F_n(\rho) : F_n]} = \frac{[E_{n^2}(\rho) : F_n]}{d} = \frac{[E_{n^2}(\rho) : F_n]}{[E_{n^2}(\rho) : E_{n^2}]} = [E_{n^2} : F_n] .$$

Mais aussi

$$[E_{n^2}(\rho) : F_n(\rho)] = [E_{n^2} : F_n(\rho) \cap E_{n^2}] .$$

Il en résulte donc que

$$F_n(\rho) \cap E_{n^2} = F_n .$$

Montrons maintenant que l'extension $F_n(\rho)/F_n$ est galsimple. Supposons qu'il existe un corps intermédiaire N galoisien sur F_n :

$$F_n \trianglelefteq N \leq F_n(\rho) \ .$$

En translatant l'extension galoisienne $N \nearrow F_n$ par E_{n^2}/F_n, on obtient l'extension galoisienne $N\,E_{n^2} \nearrow E_{n^2}$ qui est un quotient de l'extension galsimple non galoisienne $(E_{n^2}(\rho) \not\nwarrow E_{n^2})$ (cf. supra). Par conséquent

$$E_{n^2} \trianglelefteq N\,E_{n^2} \leq E_{n^2}(\rho) \quad \Rightarrow \quad \begin{cases} N\,E_{n^2} = E_{n^2}(\rho) \\ \text{ou} \\ E_{n^2} = N\,E_{n^2} \end{cases} .$$

Mais on ne peut avoir $N\,E_{n^2} = E_{n^2}(\rho)$ puisque $E_{n^2}(\rho)$ n'est pas galoisien sur E_{n^2}. C'est donc que $E_{n^2} = N\,E_{n^2}$, i.e. $N \leq E_{n^2}$. Ainsi

$$F_n \leq N = N \cap E_{n^2} \leq F_n(\rho) \cap E_{n^2} = F_n \ ,$$

d'où $N = F_n$, ce qui établit la galsimplicité de $F_n(\rho)/F_n$. De plus, si $F_n(\rho)/F_n$ était galoisienne, il en serait de même, par translation avec E_{n^2}/F_n, de l'extension $E_{n^2}(\rho) \nwarrow E_{n^2}$: contradiction. Finalement, $F_n(\rho)/F_n$ est galsimple non galoisienne : $(F_n(\rho) \not\nwarrow F_n)$, ce qui prouve que l'extension $F_n(\rho)/\mathbb{Q}$ est degré de tourabilité (n, d). □

Chapitre 7

TOURS D'ÉLÉVATION ET DISSOCIATION DES EXTENSIONS FINIES

Grâce au théorème M, détaillé au chapitre précédent, nous sommes en mesure de généraliser aux extensions finies quelconques les analogues aux théorèmes de Schreier et de Jordan-Hölder du chapitre 4 pour les extensions galtourables. Nous allons voir, grâce à la notion de tour d'élévation, que des définitions tout à fait canoniques conduisent à des énoncés très similaires, bien que leurs démonstrations soient différentes.

1. Tours d'élévation

Théorème & Définition 1.1. *(dit "de la tour d'élévation[1]")*
Soit L/K une extension finie quelconque. Toute tour

$$(F) \qquad K = F_0 \leq F_1 \leq \cdots \leq F_i \leq \cdots \leq F_m = L$$

de L/K induit une tour galtourable (cf. Chap. 2, Déf. 1.5) constituée des corps d'intourabilité (Chap. 6, Déf. 1.3) sur K de chacun des corps de (F) :

$$(M) \quad K = M_0 := M(F_0/K) \lneqq M_1 := M(F_1/K) \lneqq \cdots \lneqq M_i := M(F_i/K) \lneqq \ldots \\ \cdots \lneqq M_m := M(F_m/K) = M(L/K) \ .$$

Nous appelons la tour (M) "la tour d'élévation de $M(L/K)/K$ associée à la tour (F)", et la notons

$$(M) = (\mathcal{E}l[M(L/K)\swarrow K, (F)]) \ .$$

Nous disons en abrégé que "(E) est une tour d'élévation de $M(L/K)$" si et seulement s'il existe une tour (F) de L/K telle que $(E) = (\mathcal{E}l[M(L/K)\swarrow K, (F)])$.

Démonstration. D'après la proposition 2.2 du chapitre 6, on a

$$M(F_{i-1}/K) \ \leq \ F_{i-1} \cap M(F_i/K) \qquad (i = 1, \ldots, m)$$

et donc $M_{i-1} \leq M_i \quad (i = 1, \ldots, m)$. Or les extensions M_i/K étant galtourables, il en est de même des sous-extensions $M_i/M_{i-1} \quad (i = 1, \ldots, m)$ en vertu de la proposition 2.9 du chapitre 2. D'où la conclusion. □

[1] Le dictionnaire Le Robert donne la définition suivante : *Élévation. ◇ Géom. Projection sur un plan vertical parallélement à une des faces de l'objet.* On peut considérer que c'est ce qu'évoque la figure 30.

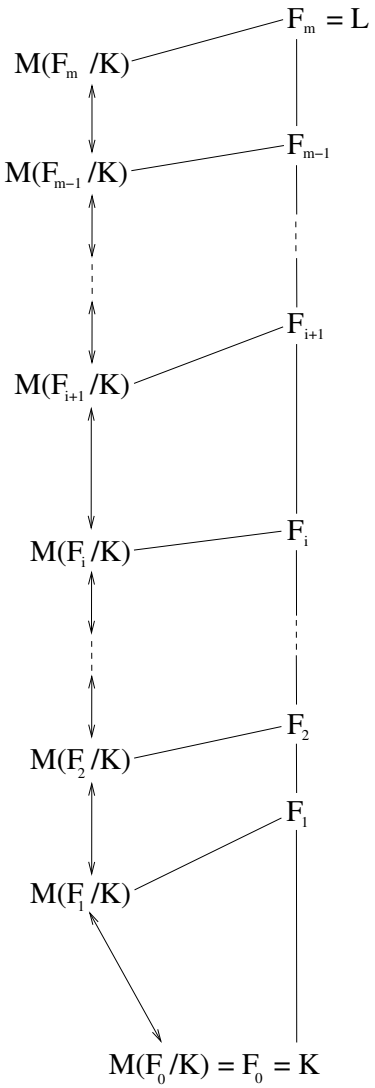

FIG. 30. *Tour d'élévation de $M(L/K)$ associée à (F)*

Nous voulons ensuite introduire, à partir de la définition précédente, les tours d'élévation de l'extension L/K elle-même, et plus seulement de son extension quotient galtourable maximale $M(L/K)\swarrow\!\!\nearrow K$. On sait, par le théorème M, que la sous-extension $L/M(L/K)$ peut être ou bien triviale, ou bien galsimple non galoisienne. Cette alternative pose une difficulté : rajouter systématiquement le corps L à une tour de $M(L/K)\swarrow\!\!\nearrow K$, c'est le répéter lorsque l'extension L/K est galtourable. Or une telle répétition rend impossible l'obtention de tours strictes, et par suite de tours de composition. Nous évitons cet écueil par la définition suivante

Définition 1.2. Soient L/K une extension et M un corps intermédiaire entre K et L : $K \leq M \leq L$. Soit de plus

$$(E) \qquad K = E_0 \leq E_1 \leq \cdots \leq E_m = M$$

une tour de M/K. Nous appelons "tour de L/K induite par (E)", et nous notons

$$((E) \dashrightarrow L)$$

la tour de L/K définie de la façon suivante

$$((E) \dashrightarrow L) := \begin{cases} (E) & \text{si } M = L \\ K = E_0 \leq E_1 \leq \cdots \leq E_m = M < L & \text{si } M \neq L \end{cases} .$$

Définition 1.3. Soient L/K une extension finie et

$$(F) \qquad K = F_0 \leq F_1 \leq \cdots \leq F_m = L$$

une tour quelconque de L/K.

Nous appelons "tour d'élévation de L/K associée à (F)", et nous notons $(\mathcal{E}l[L/K, (F)])$, la tour de L/K induite par la tour d'élévation associée à (F) de l'extension quotient galtourable maximale de L/K :

$$(\mathcal{E}l[L/K, (F)]) := ((\mathcal{E}l[M(L/K)\swarrow K, (F)]) \dashrightarrow L) .$$

Nous disons en abrégé que "(E) est une tour d'élévation de L/K", si et seulement s'il existe une tour (F) de L/K telle que $(E) = (\mathcal{E}l[L/K, (F)])$.

Remarque 1.4. Les définitions 1.1 et 1.3 coïncident lorsque l'extension L/K est galtourable. En particulier, il résulte du Th. & Déf. 1.1 que toute tour d'élévation d'une extension L/K galtourable est galtourable.

Tirons des définitions précédentes les résultats directs suivants

Fait 1.5. *Dans les notations de la définition 1.2, on a l'équivalence*

$$(E) \textit{ stricte} \qquad \Longleftrightarrow \qquad ((E) \dashrightarrow L) \textit{ stricte.}$$

Démonstration. Le résultat est évident si $M = L$. Si $M \neq L$, il est immédiat puisque la dernière marche de $((E) \dashrightarrow L)$ est toujours non triviale. □

Proposition 1.6. *Soit L/K une extension (galtourable) finie. Pour toute tour galtourable (T) de L/K, la tour d'élévation de L/K associée à (T) est égale à (T) :*

$$(\mathcal{E}l[L/K, (T)]) = (T) .$$

Démonstration. Notons

$$(T) \qquad K = T_0 \lneqq T_1 \lneqq \cdots \lneqq T_i \lneqq \cdots \lneqq T_m = L$$

une tour galtourable de L/K. Considérons les tours ratio (Chap. 3, Déf. 3.1.(2))

$$(T_r) \qquad K = T_0 \lneqq T_1 \lneqq \cdots \lneqq T_r \qquad (r = 0, \ldots, m)$$

Ce sont des tours galtourables. D'après le corollaire 1.10 du chapitre 3, les extensions T_r/K $(r = 0, \ldots, m)$ sont donc galtourables. Et l'on déduit du corollaire 1.4 du chapitre 6 que

$$\forall r \in \{0, \ldots, m\} \qquad M(T_r/K) = T_r \ .$$

D'où la conclusion. □

Lemme 1.7. *Soient L/K une extension quelconque et M un corps intermédiaire entre K et L : $K \leq M \leq L$. Pour tout entier r et toute tour*

$$(F) \qquad K = F_0 \leq F_1 \leq \cdots \leq F_r = M$$

de M/K, on a l'égalité

$$(rat_r((F) \dashrightarrow L)) = (F)$$

où $(rat_r((F) \dashrightarrow L))$ désigne la tour ratio à l'indice r (cf. Chap. 3, Déf. 3.1.(2)) de la tour de L/K induite par (F) (Déf. 1.2).

Démonstration. - Si $M = L$, $((F) \dashrightarrow L) = (F)$ et $(rat_r(F) = (F))$ (cf. Chap. 3, Fait 3.2).
- Si $M \neq L$, i.e. $M < L$, on a

$$((F) \dashrightarrow L) \qquad K = F_0 \leq F_1 \leq \cdots \leq F_r = M < L \ .$$

Il en découle, par définition d'une tour ratio, que

$$(rat_r((F) \dashrightarrow L)) \qquad K = F_0 \leq F_1 \leq \cdots \leq F_r = M$$

i.e. $(rat_r((F) \dashrightarrow L)) = (F)$. □

Le lemme précédent nous permet d'énoncer la proposition suivante, dont l'intérêt est de faire passer d'une tour de $M(L/K)\nearrow\!\!\swarrow K$ à une tour de L/K.

Proposition 1.8. *Soient L/K une extension finie et $M(L/K)$ son corps d'intourabilité (Chap. 6, Déf. 1.3). Pour toute tour*

$$(E) \qquad K = E_0 \leq E_1 \leq \cdots \leq E_i \leq \cdots \leq E_{m-1} \leq E_m = M(L/K)$$

de l'extension quotient galtourable maximale de L/K, on a

$$(E) = (rat_m((E) \dashrightarrow L))$$

et

$$(\mathcal{E}l[M(L/K)\nearrow\!\!\swarrow K, (inf_L(E))]) = (\mathcal{E}l[M(L/K)\nearrow\!\!\swarrow K, (E)])$$

où $(inf_L(E))$ désigne la tour inflatée à L de (E) (cf. Chap. 3, Déf. 3.1.(3)).

Démonstration. La première égalité est immédiate en vertu du lemme 1.7. Et par définition d'une tour inflatée

$$(inf_L(E)) \qquad K = E_0 \leq E_1 \leq \cdots \leq E_i \leq \cdots \leq E_{m-1} \leq L \ .$$

Par application directe du Th. & Déf. 1.1, on en déduit la tour d'élévation de $M(L/K)\nearrow K$:

$$(\mathcal{E}l[M(L/K)\nearrow K, (inf_L(E))]) \qquad K = M(E_0/K) \lneqq M(E_1/K) \lneqq \ldots \cdots \lneqq M(E_{m-1}/K) \lneqq M(L/K) \ .$$

D'autre part, on a vu au corollaire 1.4 du chapitre 6 que

$$M(M(L/K)/K) = M(L/K) \ .$$

Pour obtenir l'égalité des tours d'élévation de l'énoncé, il suffit alors d'appliquer à nouveau le Th. & Déf. 1.1 à la tour (E). □

Proposition 1.9. *Soient L/K une extension finie quelconque et*

$$(E) \qquad K = E_0 \leq \cdots \leq E_j \leq \cdots \leq E_n = L$$

une tour de L/K. On a l'équivalence :
(E) est une tour d'élévation de L/K si et seulement si (E) est induite par une tour galtourable de $M(L/K)\nearrow K$.

Démonstration. Supposons que (E) soit une tour d'élévation de L/K. Par la définition 1.3, elle est induite par une tour (M) d'élévation de $M(L/K)\nearrow K$; autrement dit il existe une tour (F) de L/K telle que (M) soit la tour d'élévation de $M(L/K)\nearrow K$ associée à (F). Et l'on a vu au Th. & Déf. 1.1 que (M) est une tour galtourable.

Inversement, supposons que (E) soit induite par une tour galtourable (T) de $M(L/K)\nearrow K$: $(E) = ((T) \dashrightarrow L)$. D'après la proposition 1.6

$$(T) = (\mathcal{E}l[M(L/K)\nearrow K, (T)]) \ ,$$

et par la proposition 1.8

$$(\mathcal{E}l[M(L/K)\nearrow K, (T)]) = (\mathcal{E}l[M(L/K)\nearrow K, (inf_L(T))]) \ .$$

Finalement

$$\begin{aligned} (E) &= (\mathcal{E}l[M(L/K)\nearrow K, (inf_L(T))]) \dashrightarrow L) \\ &= (\mathcal{E}l[L/K, (inf_L(T))]) \end{aligned}$$

(cf. Déf. 1.3). □

Prouvons enfin le résultat suivant.

Proposition 1.10. *Soient L/K une extension finie, et (F) une tour stricte de L/K telle que la tour d'élévation $(\mathcal{E}l[L/K,(F)])$ de L/K associée à (F) soit une tour stricte. Alors, tout raffinement galoisien strict de $(\mathcal{E}l[L/K,(F)])$ est encore une tour d'élévation de L/K.*

Démonstration. Distinguons deux cas.
(1) $M(L/K) = L$. Il résulte directement des définitions 1.3 & 1.2 que la tour d'élévation de L/K associée à (F) est une tour galtourable de L/K. Par la proposition 1.8 du chapitre 3, tout raffinement galoisien de celle-ci est encore une tour galtourable de L/K ; et donc une tour d'élévation de L/K en vertu de la proposition 1.6.
(2) $M(L/K) < L$. Pour

$$(F) \qquad K = F_0 < \cdots < F_i < \cdots < F_m = L \ ,$$

on a dans ce cas

$$(\mathcal{E}l[L/K,(F)]) \qquad K = M_0 := M(F_0/K) \lneqq \cdots \lneqq M_i := M(F_i/K) \lneqq \ldots \cdots \lneqq M_m := M(L/K) < M_{m+1} := L \ .$$

Soit (R) un raffinement galoisien strict de $(\mathcal{E}l[L/K,(F)])$. D'après la définition 1.3.(4) et la remarque 1.2.(2) du chapitre 3, il s'écrit

$$(R) \qquad K = R_0 < \cdots < R_{j_1} = M_1 < \cdots < R_j < \cdots < R_{j_i} = M_i < \ldots \cdots < R_{j_m} = M_m < \cdots < R_{j_{m+1}} = L$$

où

$$0 = j_0 < j_1 < \cdots < j_m < j_{m+1} \ .$$

D'autre part, il résulte de la proposition 3.6.(1) du chapitre 3 que la tour ratio de (R) à l'indice j_m (Chap. 3, Déf. 3.1.(2))

$$(rat_{j_m}(R)) \qquad K = R_0 < \cdots < R_{j_1} = M_1 < \cdots < R_j < \ldots \cdots < R_{j_i} = M_i < \cdots < R_{j_m} = M_m = M(L/K)$$

est un raffinement galoisien de la tour

$$(rat_m(\mathcal{E}l[L/K,(F)])) \qquad K = M_0 \lneqq \cdots \lneqq M_i \lneqq \cdots \lneqq M_m = M(L/K) \ .$$

Cette dernière étant galtourable, on déduit de la proposition 1.8 du chapitre 3 que $(rat_{j_m}(R))$ est aussi une tour galtourable de $M(L/K)\swarrow K$. En vertu de la proposition 1.9 précédente, il suffit maintenant pour conclure de prouver que la tour (R) est induite par la tour galtourable $(rat_{j_m}(R))$. Raisonnons par l'absurde en supposant que cela ne soit pas le cas. Comme par définition on a l'implication

$$j_m + 1 = j_{m+1} \quad \Rightarrow \quad (R) = ((rat_{j_m}(R)) \dashrightarrow L) \ ,$$

cela signifierait que

$$j_m + 1 \neq j_{m+1} \quad \Rightarrow \quad j_m + 1 < j_{m+1} \ ;$$

et le raffinement (R) étant strict,

$$M(L/K) = R_{j_m} < R_{j_m+1} < R_{j_{m+1}} = L \ .$$

Il est de plus galoisien ; donc par la condition (RAFG) de la définition 1.3 du chapitre 3, on en déduirait que R_{j_m+1} est galoisien sur R_{j_m}. Mais avoir

$$M(L/K) \lhd R_{j_m+1} < L$$

contredit la galsimplicité de $L/M(L/K)$ (cf. Théorème M du chapitre 6). □

2. Tour de composition et Théorèmes de dissociation

Nous avons introduit au chapitre 4 la notion de "tour de composition galoisienne" d'une extension galtourable. Nous allons maintenant définir sa généralisation à n'importe quelle extension finie.

Définition 2.1. Soit L/K une extension finie quelconque. Nous appelons "tour de composition de L/K" toute tour d'élévation de L/K stricte qui n'admet aucun raffinement galoisien propre.

Cette notion de tour de composition pour n'importe quelle extension finie généralise celle de tour de composition galoisienne pour les extensions galtourables (Chap. 4, Sect. 1). En effet :

Lemme 2.2. *Soit $L\nearrow K$ une extension galtourable finie. Toute tour de composition galoisienne de L/K est une tour de composition de L/K au sens de la définition 2.1 précédente.*

Démonstration. Soit (T) une tour de composition galoisienne de L/K (Chap. 4, Déf. 1.1.(1)). Il suffit de montrer que (T) est une tour d'élévation de L/K. Or (T) est a fortiori une tour galtourable ; donc par la proposition 1.6, $(T) = (\mathcal{E}l[L/K, (T)])$. □

Proposition 2.3. *Soit $L\nearrow K$ une extension galtourable finie. L'ensemble non-vide des tours de composition galoisiennes de L/K est égal à l'ensemble des tours de composition de L/K au sens de la définition 2.1.*

Démonstration. L'ensemble des tours de composition galoisiennes de L/K est non-vide en vertu du second théorème de dissociation (Chap. 4, Th. 4.2). Et par le lemme 2.2, il est inclus dans celui des tours de composition de L/K au sens de la définition ci-dessus.

Prouvons l'autre inclusion en considérant une tour de composition (C) de L/K comme définie au 2.1. C'est en particulier une tour d'élévation de L/K, et elle est galtourable parce que L/K l'est (remarque 1.4). Selon la proposition 1.9 du

chapitre 3, elle admet donc un raffinement galoisien (R) qui est une tour galoisienne. Or, en tant que tour de composition, (C) n'admet pas de raffinement galoisien propre. Ceci établit que le raffinement (R) de (C) est trivial (Chap. 3, Déf. 1.3.(2)). De plus, (C) est stricte en tant que tour de composition. Par définition d'une tour stricte associée (Chap. 3, Prop. & Déf. 2.1), on en déduit que $(C) = (R_<)$. Comme (R) est une tour galoisienne, le corollaire 2.6 du chapitre 3 assure finalement que (C) est une tour de composition galoisienne. □

Nous avons donné une caractérisation des tours d'élévation (Prop. 1.9) ; nous sommes maintenant en mesure de faire de même pour les tours de composition.

Proposition 2.4. *Soient L/K une extension finie et*

$$(C) \qquad K = C_0 \leq \cdots \leq C_i \leq \cdots \leq C_m = L$$

une tour de L/K. On a l'équivalence :
(C) est une tour de composition si et seulement si elle est induite par une tour de composition galoisienne de l'extension quotient galtourable maximale de L/K.

Démonstration. Supposons que (C) soit une tour de composition de L/K. C'est une tour d'élévation de L/K, donc par la proposition 1.9, elle est induite par une tour galtourable (T) de $M(L/K)\nearrow K$. Montrons que (T) est en fait une tour de composition galoisienne de $M(L/K)\nearrow K$. D'après le Fait 1.5, elle est stricte. Notons r la hauteur de (T). D'après le lemme 1.7,

$$(T) = (rat_r((T) \dashrightarrow L)) = (rat_r(C)) \ .$$

Raisonnons par l'absurde en supposant qu'il existe un raffinement galoisien propre (R) de (T). D'après la proposition 3.7.(2) du chapitre 3, $(res_r(C))$ et (R) induisent un raffinement galoisien propre de (C) : contradiction, puisque (C) n'en admet pas. Finalement, (T) est une tour stricte sans aucun raffinement galoisien propre. C'est de plus une tour d'élévation d'après la proposition 1.6, puisqu'elle est galtourable. C'est donc bien une tour de composition de L/K.

Réciproquement, supposons que (C) soit induite par une tour de composition galoisienne (T) de $M(L/K)\nearrow K$. D'après le Fait 1.5, (C) est stricte, tandis que par la proposition 1.9, c'est une tour d'élévation de L/K. Soit r la hauteur de (T). Raisonnons par l'absurde en supposant l'existence d'un raffinement galoisien propre de (C). Comme (T) n'admet pas de raffinement galoisien propre, on déduit alors du (1) de la proposition 3.7 du chapitre 3 qu'il existe un raffinement galoisien propre de la tour resteinte $(res_r(C))$. Or celle-ci est :
- Ou bien la tour triviale (Chap. 2, Déf. & Conv. 1.1.(1))

$$(res_r(C)) \qquad M(L/K) = F_0 = L$$

lorsque L/K est galtourable. Mais cette tour triviale est une tour de composition galoisienne (Chap. 4, Fait 1.2) et n'admet donc aucun raffinement galoisien

propre.
- Ou bien la tour stricte

$$(res_r(C)) \qquad M(L/K) < L \ .$$

Notons

$$(R) \qquad M(L/K) = R_0 \leq \cdots \leq R_j \leq \cdots \leq R_n = L$$

son raffinement galoisien susmentionné. Par définition d'un raffinement propre (Chap. 3, Déf. & Conv. 1.1.(2)), l'ensemble $\{j \in \{1, \ldots, n-1\} \mid R_0 < R_j < R_n\}$ est non vide, et l'on peut considérer son plus petit élément j_0. Alors, d'une part la minimalité de j_0 implique que $R_{j_0-1} = M(L/K)$, d'autre part la condition (RAFG) de définition d'un raffinement galoisien (Chap. 3, Déf. 1.3.(4)) conduit à

$$M(L/K) = R_{j_0-1} \lhd R_{j_0} < R_n = L \ .$$

Mais ceci contredit la galsimplicité de $L/M(L/K)$ (Chap. 6, Th. 1.1).

L'existence d'un raffinement galoisien propre de (C) est donc impossible, ce qui finit de prouver que (C) est une tour de composition de L/K au sens de la définition 2.1. □

Nous allons enfin pouvoir prouver les derniers théorèmes de dissociation qui sont les analogues pour les extensions finies quelconques des 1^{er} et $3^{\text{ème}}$ théorèmes de dissociation du chapitre 4 pour les extensions galtourables. Mais nous n'avons jusqu'ici défini l'équivalence de deux tours d'une même extension que lorsque ces tours sont galoisiennes. La définition suivante de l'équivalence de deux tours induites implique en particulier celle de l'équivalence de deux tours de composition non galoisiennes en vertu de la proposition 2.4 précédente.

Définition 2.5. Soient L/K une extension finie quelconque, (T) et (T') deux tours galoisiennes de l'extension quotient galtourable maximale $M(L/K)\nearrow K$ de L/K. Nous disons que les tours induites de L/K par (T) et (T') sont équivalentes si et seulement si les tours galoisiennes (T) et (T') le sont au sens de la définition 1.1.(2) du chapitre 4 :

$$((T) \dashrightarrow L) \sim ((T') \dashrightarrow L) \quad \overset{\text{Déf.}}{\Longleftrightarrow} \quad (T) \sim (T') \ .$$

Théorème 2.6. *($5^{ème}$ théorème de dissociation)*
Deux tours d'élévation d'une même extension finie quelconque admettent des raffinements galoisiens qui sont des tours d'élévation équivalentes de cette extension.

Démonstration. Soient L/K une extension finie et (E^1), (E^2) deux tours d'élévation de L/K. Lorsque L/K est galtourable, il en est de même de (E^1) et (E^2) par définition ; donc il suffit d'utiliser le 1^{er} théorème de dissociation bis (Chap. 4, Th. 3.4) avec la proposition 1.6.

Supposons désormais L/K non galtourable, i.e. telle que $M(L/K) < L$ (Chap. 6, Cor. 1.4). Les tours d'élévation (E^1) et (E^2) sont respectivement induites par des tours galtourables (T^1) et (T^2) de l'extension quotient galtourable maximale $M(L/K)\nearrow K$ (cf. Déf. 1.3 et Th. & Déf. 1.1). En notant $r_i \quad (i = 1, 2)$ la hauteur de la tour

$$(T^i) \qquad K = T_0^i \lesseqgtr \cdots \lesseqgtr T_{r_i}^i = M(L/K) \ ,$$

on a par le lemmme 1.7

$$(T^i) = (rat_{r_i}(E^i)) \ ,$$

et donc

$$(E^i) \qquad K = E_0^i = T_0^i \lesseqgtr \cdots \lesseqgtr E_{r_i}^i = T_{r_i}^i = M(L/K) < E_{r_i+1}^i = L \ .$$

Ceci permet d'appliquer le (2) de la proposition 3.6 du chapitre 3.
- D'une part, la tour restreinte $(res_{r_i}(E^i))$ est un raffinement galoisien d'elle-même en vertu du (2) de la remarque 1.4 du chapitre 3.
- D'autre part, on sait par le théorème 3.4 du chapitre 4 que (T^1) et (T^2) admettent des raffinements galoisiens (T'^1) et (T'^2) qui sont des tours galoisiennes équivalentes.

On déduit alors de la proposition 3.6 précitée qu'il existe un raffinement galoisien (E'^i) de (E^i) tel que

$$(res_{j_{r_i}}(E'^i)) = (res_{r_i}(E^i)) \quad \text{et} \quad (rat_{j_{r_i}}(E'^i)) = (T'^i) \ .$$

Par conséquent :

$$(E'^i) \quad K = E_0'^i \trianglelefteq \cdots \trianglelefteq E_{j_0}'^i = E_0^i \trianglelefteq \cdots \trianglelefteq E_{j_{r_i}}'^i = E_{r_i}^i = M(L/K) < E_{j_{r_i}+1}'^i = E_{r_i+1}^i = L \ .$$

En particulier (E'^i) est la tour de L/K induite par (T'^i)

$$(E'^i) = ((T'^i) \dashrightarrow L) \qquad (i = 1, 2) \ .$$

Comme (T'^1) et (T'^2) sont des tours galoisiennes, a fortiori galtourables, de $M(L/K)\nearrow K$, on déduit de la proposition 1.9 que les raffinements galoisiens (E'^1) et (E'^2) sont des tours d'élévation de L/K. Enfin, elles sont équivalences au sens de la définition 2.5 puisqu'il en est ainsi de (T'^1) et (T'^2). □

Théorème 2.7. *($6^{ème}$ théorème de dissociation)*
Soit L/K une extension finie quelconque.

(1) Toute tour d'élévation stricte de L/K admet un raffinement galoisien qui est une tour de composition de L/K.

(2) Deux tours de composition de L/K sont équivalentes.

Démonstration. (1) Si L/K est galtourable, i.e. si $L = M(L/K)$ (Chap. 6, Cor. 1.4), toute tour d'élévation de L/K est galtourable puisque

$$(\mathcal{E}l[L/K, (F)]) = (\mathcal{E}l[M(L/K)\nearrow K, (F)]) \quad \text{(Th. \& Déf. 1.1).}$$

D'après le 3ème théorème de dissociation bis (Chap. 4, Th. 4.4.(1)), une tour d'élévation stricte de L/K admet donc un raffinement qui est une tour de composition galoisienne de L/K. Par le Fait 1.5.(2) du chapitre 3, ce raffinement est galoisien, et c'est une tour de composition de L/K en vertu de la proposition 2.3.

Plaçons-nous maintenant dans le cas nouveau où $M(L/K) < L$. Soit (E) une tour d'élévation stricte de L/K. Elle est induite par une tour d'élévation (T) de $M(L/K)\swarrow K$ (Déf. 1.3) qui est stricte d'après le Fait 1.5 du présent chapitre, et galtourable (Th. & Déf. 1.1) :

$$(T) \qquad K = T_0 \lneqq \cdots \lneqq T_i \lneqq \cdots \lneqq T_r = M(L/K) \ ;$$

d'où

$$(E) = ((T) \dashrightarrow L) \qquad \begin{array}{l} K = E_0 := T_0 \lneqq \cdots \lneqq E_i := T_i \lneqq \dots \\ \qquad \cdots \lneqq E_r := T_r = M(L/K) < E_{r+1} := L \ . \end{array}$$

En particulier, par définition (Chap. 3, Déf. 3.1),

$$(T) = (rat_r(E))$$

et

$$(res_r(E)) \qquad E_r = M(L/K) < E_{r+1} = L \ .$$

Nous allons raffiner les tours $(rat_r(E))$ et $(res_r(E))$. D'une part, il est clair que $(res_r(E))$ est un raffinement galoisien de lui-même (Chap. 3, remarques 1.4.(2)). D'autre part (T) étant une tour galtourable stricte, on déduit du (1) du théorème 4.4 du chapitre 4 que $(rat_r(E))$ admet un raffinement galoisien (C) qui est une tour de composition galoisienne de $M(L/K)\swarrow K$. Il résulte alors du (2) de la proposition 3.6 du chapitre 3 qu'il existe un raffinement galoisien (E') de (E) tel que l'on ait à la fois

$$(res_{j_r}(E')) = (res_r(E)) \quad , \quad (rat_{j_r}(E')) = (C) \ .$$

Par conséquent, la tour (E') s'écrit

$$(E') \qquad \begin{array}{l} K = E'_0 = C_0 \lhd \cdots \lhd E'_{j_i} = C_{j_i} = E_i \lhd \cdots \lhd E'_j = C_j \lhd \dots \\ \qquad \cdots \lhd E'_{j_r} = C_{j_r} = E_r = M(L/K) < E'_{j_r+1} = E_{r+1} = L \ . \end{array}$$

On constate en particulier que la tour (E') est induite par la tour de composition galoisienne (C) de $M(L/K)\swarrow K$:

$$(E') = ((C) \dashrightarrow L) \ .$$

En vertu de la proposition 2.4, (E') est donc une tour de composition de L/K. □

Bibliographie

[1] M. Acosta de Orozco and W.Y. Vélez, The lattice of subfields of a radical extension, *J. Number Theory* **15** (1982), 388–405.

[2] E. Andréo et R. Massy, Dissociation d'extensions de corps II, Raffinements de tours galoisiennes, en préparation.

[3] E. Andréo et R. Massy, Dissociation of field extensions III, Elevation towers, in preparation.

[4] E. Andréo et R. Massy, Parallélogrammes galoisiens infinis, *Annales Math. Blaise Pascal* **8** (2001), 21–45.

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

[6] F. Barrera-Mora and P. Lam-Estrada, Radical extensions and crossed homomorphisms, *Bull. Austral. Math. Soc.* **64** (2001), 107–119.

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

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

[9] H. Cohen, *Advanced Topics in Computational Number Theory*, Grad. Texts in Math. **193**, Springer-Verlag, New-York, 2000.

[10] H. Cohen et al. *Users'guide for PARI / GP*, http ://pari.math.u-bordeaux.fr/doc.html

[11] R.F. Coleman, On the Galois groups of the exponential Taylor polynomials, *L'Enseignement Mathématique* **33** (1987), 183–189.

[12] J.D. Dixon and B. Mortimer, *Permutation Groups*, Grad. Texts in Math. **163**, Springer-Verlag, New York, 1996.

[13] D.E. Dobbs and B. Mullins, On the lengths of maximal chains of intermediate fields in a field extension, *Commun. in Algebra.* **29** (2001), 4487–4507.

[14] J.-P. Escofier, *Théorie de Galois*, Masson, Paris, 1997.

[15] B. Hölder, Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen, *Math. Ann.* **34** (1889), 26–56.

[16] B. Huppert, *Endliche Gruppen I*, Grundlehren der mathematischen Wissenschaften **134**, Springer-Verlag, Berlin, 1983.

[17] C.U. Jensen, A. Ledet and N. Yui, *Generic Polynomials. Constructive Aspects of the Inverse Galois Problem*, MSRI Publ., Vol. **45**, Cambridge University Press, Cambridge, 2002.

[18] C. Jordan, Commentaire sur Galois, *Math. Ann.* **1** (1869), 141–160, (Oeuvres Gauthier-Villars 1961, Vol.1, pp.211-230).

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

[20] H. Koch, *Galoissche Theorie der p-Erweiterungen*, Springer-Verlag, Berlin, 1970.

[21] H. Koch, *Galois Theory of p-Extensions*, Springer Monographs in Math., Berlin, 2002.

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

[23] S. Lang, *Algebra,* 3^{rd} *revised ed.*, Addison-Wesley, Reading, MA, 2002.

[24] S. Lang, *Algebraic Number Theory*, Grad. Texts in Math. **110**, Springer-Verlag, Berlin, 1986.

[25] R. Massy, Une construction algorithmique des p-extensions cycliques de corps, de caractéristique différente de p, contenant les racines p-ièmes de l'unité, *Acta Arithmetica* **103** (2002), 21–26.

[26] R. Massy, Galois averages, en préparation.

[27] R. Massy, Dissociation of field extensions I, The field of intowerability, in preparation.

[28] R. Massy et S. Monier-Derviaux, Parallélogrammes galoisiens, *J. Algebra* **217** (1999), 229–248.

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

[30] S. Monier, Descente de p-extensions galoisiennes kummériennes, *Math. Scand.* **79** (1996), 5–24.

[31] S. Monier-Derviaux, *Le Problème de la Descente Galoisienne Finie*, Thèse de Doctorat, Univ. Valenciennes (1997).

[32] P. Morandi, *Field and Galois Theory*, Grad. Texts in Math. **167**, Springer-Verlag, New York, 1996.

[33] L.S. Pontryagin, *Topological Groups*, Gordon and Breach, New York, 1986.

[34] J.S. Rose, *A Course on Group Theory*, Cambridge University Press, Cambridge, 1978.

[35] I. Schur, Gleichungen ohne Affekt , *Gesammelte Abhandlungen*, Band III **67** (1930), 191–197, Springer-Verlag, Berlin, 1973.

[36] O. Schreier, Über den Jordan-Hölderschen Satz, *Abh. Math. Sem. Univ. Hamburg* **6** (1928), 300–302.

[37] E.S. Selmer, On the irreducibility of certain trinomials, *Math. Scand.* **4** (1956), 287–302.

[38] J.-P. Serre, *Topics in Galois Theory*, Jones and Bartlett, Boston, 1992.

[39] J.-P. Serre, *Corps Locaux,* $3^{ème}$ *édition*, Hermann, Paris, 1980.

[40] F. Viviani, Ramification groups and Artin conductors of radical extensions of $\mathbb{Q}$, *J. Théorie des Nombres Bordeaux*, à paraître.

[41] L.C. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. **83**, Springer-Verlag, New York, 1997.

[42] B.F. Wyman, Wildly ramified gamma extensions, *Amer. J. Math.* **91** (1969), 135–152.

[43] E. Yoshida, On the 3-class field tower of some biquadratic fields, *Acta Arithmetica* **107** (2003), 327–336.

Table des figures

Index

Table des matières