**Journal of Algebra, Number Theory: Advances and Applications**
Volume 6, Number 1-2, 2011, Pages 29-56

# TRANSLATION INTO GALOIS THEORY OF THEOREMS IN GROUP THEORY

**EMMANUEL ANDRÉO and RICHARD MASSY**

Université Lille Nord de France
Le Mont Houy
F-59313 Valenciennes
France
e-mail: Richard.Massy@univ-valenciennes.fr

## Abstract

We develop the theory of algebraic field extensions in a way similar to normal series of subgroups in group theory. Is it possible, by dissociating algebraic extensions through their intermediate fields, to "approximate" them by Galois extensions, in order to construct a tower with as many Galois steps as possible? We describe the obstruction to this Galois dissociation by proving a fundamental difference between groups and extensions: Every finite group admits a normal series, whereas a finite extension, even if separable, does not necessarily admit a Galois tower. For those extensions that are analogous in nature to groups, we establish a complete dictionary between groups and extensions by giving the Galois analogues of the most famous classical results of group theory.

## 1. Introduction

What are the relations between field extensions and groups? From classical Galois theory to the inverse Galois problem, the history is full of major results. However, in this paper, we interpret the question in the

2010 Mathematics Subject Classification: 12F10, 11R32, 11S20.

Keywords and phrases: field towers, refinements, composition Galois towers, semi-abelian extensions, solvable extensions.

Received October 13, 2011

© 2011 Scientific Advances Publishers

following way: Does there exist a dictionary between properties of groups and of extensions? For instance, do there exist Galois analogues of the theorems of Schreier, Jordan-Hölder, Feit-Thompson …? We shall see that the answer is yes and how these analogues illuminate the extension theory.

The classical point of view is to embed the given extension in its Galois closure. But in our opinion, this approach is essentially formal: Except for very small degrees, the Galois closure is in general beyond computation. By contrast, the method described here "delves into" the extension; this allows us, as is explained in the last section, to deal with degrees up to $10^4$.

Our point of view answers the following natural question: Is it possible to "approximate" algebraic extensions, or at last some of them, via Galois extensions? By analogy with groups, which can be unraveled by way of subgroups into a normal series, can we "dissociate" algebraic extensions into intermediate fields, constructing a tower with the greatest possible number of Galois steps?

By a "Galois tower" of a separable extension $L/K$, we mean a finite increasing sequence between $K$ and $L$ inducing a tower, all the steps of which are Galois extensions. If $L/K$, which is of arbitrary degree, dissociates into a Galois tower, we say that it is "galtowerable". The notion of a galtowerable extension strictly generalizes that of a Galois extension and allows us to discover a fundamental difference between groups and extensions: Any finite group admits a normal series, but a finite separable extension is not necessarily galtowerable. The obstruction to the Galois dissociation of a finite extension $L/K$ is what we call the "field of untowerability[1]" (or the "untowerable field") of $L/K$. In Theorem 3.7, we prove (without any Galois closure) that it always exists and is unique.

---

[1] In French "corps d'intourabilité".

Classifying finite groups is a problem that has been dealt with for almost two centuries now. We suggest to classify finite and separable extensions. As far back as 1959, Artin [3] introduces "halbabelsche Erweiterungen" (that can be translated by "semi-abelian extensions") as those dissociating into an abelian tower. Since 1965, Lang [16] calls "solvable" any finite separable extension that embeds into a Galois extension with solvable Galois group. However, with this definition, even a solvable extension may not be galtowerable. In this paper, we prove that being both galtowerable and solvable is equivalent with being a semi-abelian extension. Further, thanks to the "Galois Feit-Thompson theorem" (4.10), we obtain that any galtowerable finite extension of odd degree is semi-abelian. Then, via the orders of the first sixteen finite non-abelian simple groups, we set the table of all possible degrees $\leq 10080$ for a galtowerable nonsemi-abelian extension. Therefore, a galtowerable extension with degree $d \leq 10080$ not in this table is necessarily semi-abelian, and its "composition towers" are induced by the prime power decomposition of $d$.

To conclude the construction of finite solvable extensions, it now remains to build those which are not galtowerable. One of the main problems is how to describe their "Galois entropy", i.e., their galsimple non-Galois subextensions (Theorem 3.7(INT2))?

## 2. Galtowerable Extensions

Recall the

**Definition 2.1** ([4, p.23], [11, p.308])**.** Let $G$ be a group. We say that a subgroup $H \leq G$ is subnormal in $G$, if there exists a series from $H$ to $G$, i.e., a finite increasing sequence $(G_i)_{0\leq i\leq n}$ of subgroups of $G$ such that

$$H = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_i \trianglelefteq G_{i+1} \trianglelefteq \ldots \trianglelefteq G_n = G.$$

The following properties are well known (e.g., [21, Chapter 7]):

**Proposition 2.2.** *Let $H_1$, $H_2$ be two subgroups of $G$.*

(1) *If $H_2$ is subnormal in $G$, then $H_1 \cap H_2$ is subnormal in $H_1$.*

(2) *Assume that* $H_2 \leq H_1 \leq G$. *If* $H_2$ *is subnormal in* $G$, *then* $H_2$ *is subnormal in* $H_1$.

(3) *If* $H_1$ *and* $H_2$ *are both subnormal in* $G$, *then* $H_1 \cap H_2$ *is subnormal in* $G$.

**Definition 2.3.** Let $L / K$ be a field extension.

(1) By a "tower (of fields) of $L / K$", we mean a finite increasing sequence (Definition 2.1) $(F_i)_{0 \leq i \leq m}$ of intermediate fields of $L / K$ with $F_0 = K$ and $F_m = L$. We denote such a tower by

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

We call the extensions $F_{i+1} / F_i$ $(i = 0, \ldots, m-1)$ (resp., the integer $m$) the "steps" (resp., the "height") of the tower $(F)$. A tower with height 0 is said to be "trivial". When $F_{i+1} \neq F_i$ for each $i \in \{0, \ldots, m-1\}$, the tower $(F)$ is "strict" (i.e., without repetitions). For instance, a trivial tower is strict.

(2) When $L / K$ is an algebraic extension, a "Galois tower of $L / K$" is a tower of $L / K$ all whose steps are Galois extensions. Then we write

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

(where $F_i \trianglelefteq F_{i+1}$ means $F_{i+1} / F_i$ a Galois extension).

From the transitivity of the degree, we immediately deduce the

**Lemma 2.4.** *Let* $L / K$ *be a finite extension. If* $[L : K] = p_1^{m_1} \cdots p_r^{m_r}$ *is the prime decomposition of its degree, then the height* $m$ *of any strict tower of* $L / K$ *satisfies* $m \leq m_1 + \cdots + m_r$.

The translation of Definition 2.1 for field extensions is the following:

**Proposition 2.5.** *Let $N / K$ be a Galois extension. For any intermediate field $L$ of $N / K$, the extension $L / K$ dissociates into a Galois tower, if and only if the subgroup $Gal(N / L)$ is subnormal in $Gal(N / K)$.*

**Proof.** The only if part is clear. Conversely, we use that in a group $G$, the normality of a subgroup in some other one implies the normality of their topological closure (for the Krull topology)

$$\forall A \leq G; \quad \forall B \leq G; \quad A \trianglelefteq B \Rightarrow \overline{A} \trianglelefteq \overline{B},$$

(cf. [1, Proposition 3.1(1)]). □

**Corollary 2.6.** *Let $L / K$ be an algebraic extension of arbitrary (finite or infinite) degree. The following conditions are equivalent*:

(1) *$L / K$ dissociates into a Galois tower.*

(2) *There exists a Galois extension $N / K$, $L \leq N$, such that $Gal(N / L)$ is subnormal in $Gal(N / K)$.*

(3) *For any Galois extension $M / K$, $L \leq M$, $Gal(M / L)$ is subnormal in $Gal(M / K)$.*

To dissociate into a Galois tower is therefore an intrinsic property: It only depends upon the given extension and not of the Galois extension in which it is embedded. This justifies the

**Definition 2.7.** We say that a separable field extension $L / K$ is "galtowerable", if and only if it dissociates into a Galois tower (Definition 2.3(2)).

Any Galois extension is obviously galtowerable, the converse being false by the lack of transitivity of normality. Therefore, the notion of a galtowerable extension strictly generalizes that of a Galois extension.

**Proposition 2.8.** (0) *Transitivity. Let $J \leq K \leq L$ be a tower of fields. If $K / J$ and $L / K$ are galtowerable, then $L / J$ is galtowerable as well.*

(1) *Translation. Let* $K/J$ *and* $L/J$ *be two algebraic extensions. Assume only that K and L are subfields of a common field. Then, we have the following implication*:

$$(L/J \text{ galtowerable}) \Rightarrow (KL/K \text{ galtowerable}).$$

(2) *Subextension* (*cf. Definition* 3.2). *Let* $L/J$ *be galtowerable. For any intermediate field K of* $L/J$, *the subextension* $L/K$ *is galtowerable.*

(3) *Compositum. The compositum of two galtowerable extensions* (*with top fields in a common field*) *is a galtowerable extension.*

**Proof.** (0) Trivial with Definition 2.7. For (1) (resp., (3)), use Corollary 2.6 and Proposition 2.2(1) (resp., 2.2(3)) with classical Galois theory. For (2) use (1) with $K \leq L$. □

**Corollary 2.9.** *The translation of a galtowerable extension by a given field is always galtowerable. More precisely, let* $L/J$ *be an algebraic extension. For any field* $C \leq \widetilde{J}$, $\widetilde{J}$ *an algebraic closure of J containing L, we have the following implication*:

$$(L/J \text{ galtowerable}) \Rightarrow (CL/CJ \text{ galtowerable}).$$

**Proof.** Apply Proposition 2.8(1) with $K = CJ$. □

**Remark 2.10.** In particular, Corollary 2.9 is true when we replace "galtowerable extension" by "Galois extension".

## 3. The Field of Untowerability

The concept of a galtowerable extension makes it possible to shed light upon a fundamental difference between groups and extensions. We know that any finite group admits a normal series. By contrast, we shall see that, in general, a finite separable extension does not dissociate into a Galois tower; hence a finite extension is not necessarily galtowerable.

**Proposition 3.1.** *Let* $L/K$ *be a finite separable extension. There exists a unique intermediate field M of* $L/K$ *such that* $M/K$ *is a galtowerable*

*extension with the following property*: *For any intermediate field* $I$ *of* $L / K$, *we have* $I \leq M$, *whenever* $I / K$ *is a galtowerable extension*.

**Proof.** Let $N$ be the Galois closure of $L$ over $K$ in an algebraic closure of $K$ containing $L$. Then, with Proposition 2.2(3) and Proposition 2.5, take for $M$, the fixed field into $N$ of the intersection of all subnormal subgroups of $Gal(N / K)$ containing $Gal(N / L)$. □

Unfortunately, the use in the former proof of the Galois closure $N / K$ makes the definition of the field $M$ ineffective. In our opinion, to make computations, we have to stay into the extension: This is what we do now by introducing for extensions the analogue of the notion of a simple group.

**Definition 3.2.** Let $E / F$ be an algebraic extension. We call "subextension" (resp., "quotient extension") of $E / F$ any extension $E / M$ (resp., $M / F$), where $M$ is an intermediate field of $E / F$ : $F \leq M \leq E$.

**Remark 3.3.** To speak, as in literature, of the "subextension $M / F$" is a Galois inconsistency. Indeed, if $M / F$ is a Galois extension in a Galois extension $E / F$, $Gal(M / F)$ is not a subgroup of $Gal(E / F)$!

**Definition 3.4.** A "galsimple extension" is a nontrivial extension that has no proper Galois quotient extension:

$$(L / K \text{ galsimple}) \overset{\text{def.}}{\Leftrightarrow} (L \neq K, \quad \forall F \quad K \trianglelefteq F \leq L \Rightarrow (F = K \text{ or } F = L)).$$

**Example 3.5.** A finite Galois extension is galsimple, if and only if its Galois group is simple.

Let us emphasize here another difference between groups and extensions. There exists infinite simple groups; but the group of an infinite Galois extension $L / K$ is never simple because $L / K$ is never galsimple (cf. Proposition 4.7).

**Example 3.6.** For any integer $n \geq 3$, the extension $\mathbb{Q}(\theta)/\mathbb{Q}$ with $\theta^n - \theta - 1 = 0$ is galsimple and non-Galois.

This follows from the fact that the polynomial $P_n(x) := X^n - X - 1$ $(n \geq 2)$ is irreducible over $\mathbb{Q}$ [24] and from the isomorphism $Gal(P_n(X)) \tilde{\to} S_n$ ([25] or [12]).

**Theorem 3.7.** *For any finite extension $L/K$, there exists a unique intermediate field $M$ of $L/K$ satisfying the following two conditions*:

(INT1) *The quotient extension $M/K$ is galtowerable.*

(INT2) *The subextension $L/M$ is either trivial or both galsimple and non-Galois.*

*We call this unique field $M$ the "field of untowerability"* (*or the "untowerable field"*) *of $L/K$ and we denote it by $M(L/K)$.*

**Proof.** (Without using any Galois closure.) If $L = K$, the theorem is true with $K = M = L$. In what follows, let $L \neq K$.

(1) Existence. Assume that $L/K$ is not a galsimple extension. This means that it dissociates into a field tower of the form

$$K =: M_0 \lhd M_1 \lhd \ldots \lhd M_m < L.$$

Since the degree of $L/K$ is finite, there exists an integer $m \in \mathbb{N} \setminus \{0\}$ such that $L/M_m$ is a galsimple extension. Then, either $M_m \lhd L$ and we take $M = L$, or $L/M_m$ is non-Galois and we take $M = M_m$.

(2) Uniqueness. Assume that there exist two intermediate fields $M' \neq M$ satisfying conditions (INT1) and (INT2).

• First case: For instance, $K \leq M < M' \leq L$. The subextension $M'/M$ is galtowerable as $M'/K$ by Proposition 2.8(2). Then there exists a field $F$ such that $M \lhd F < L$, which contradicts the galsimplicity of $L/M$.

• Second case: We do not have $M < M'$ nor $M' < M$. Since $M / K$ is galtowerable, so is the subextension $M / M \cap M'$ and there exists a field $F$ such that $M \cap M' \lhd F \leq M$. Then we translate the Galois extension $F / M \cap M'$ by $M' / M \cap M'$. We get the Galois extension $FM' / M'$. It is nontrivial because $M' = FM'$ would lead to $F = M \cap M'$, a contradiction. Moreover, if $FM' = L$, then $L / M'$ would be a Galois extension contradicting condition (INT2). Hence $M' \lhd FM' < L$, which contradicts the galsimplicity of $L / M'$. □

The identity of the following proposition should make it possible to develop an algorithm to determine the untowerable field of a given extension.

**Proposition 3.8.** *Let $L / K$ be a finite extension. For any intermediate extension $E / F$, $K \leq F \leq E \leq L$, we have the identity*

$$M(L / K) = M(M(L / F) / M(E / K)).$$

It is not the goal of this paper to show this kind of results; we will return there.

One draws, for instance, the following example from it:

**Example 3.9.** Let $a \in \mathbb{N}$ be an integer such that there exists a prime $p$ for which $p \| a$ (i.e., $p \mid a$ but $p^2 \nmid a$). For any $n \in \mathbb{N} \setminus \{0\}$, the untowerable field of the real extensions $\mathbb{Q}(\sqrt[n]{a}) / \mathbb{Q}$ is given by

$$M(\mathbb{Q}(\sqrt[n]{a}) / \mathbb{Q}) = \mathbb{Q}(\sqrt[2^d]{a}),$$

where $n = 2^d(2m + 1)(m \in \mathbb{N})$. In particular,

$$\forall n = 2m + 1 \quad (m \in \mathbb{N}); \qquad M(\mathbb{Q}(\sqrt[n]{a}) / \mathbb{Q}) = \mathbb{Q}.$$

In other words, for $n$ odd, the real extensions $\mathbb{Q}(\sqrt[n]{a}) / \mathbb{Q}$ are all galsimple and non-Galois. And for $n$ even, we get for instance that the usual extension $\mathbb{Q}(\sqrt[6]{2}) / \mathbb{Q}$ is not even galtowerable because $M(\mathbb{Q}(\sqrt[6]{2}) / \mathbb{Q}) = \mathbb{Q}(\sqrt{2})$.

## 4. Galois Analogues of the Theorems of Schreier and Jordan-Hölder

Suppose now that the extensions dissociate in a way similar to groups, i.e., admit Galois towers, in other words are galtowerable. In this case, we are able to prove very close analogues of major theorems in group theory. On the contrary, we are not able to provide a satisfactory theory for dealing with the nongaltowerable extensions.

To begin, let us translate for any field tower, the usual definitions for normal series of groups (which appear clearly, e.g., in [21, Chapter 7]).

**Definition 4.1.** Let $L / K$ be an extension and

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

a tower of $L / K$.

(1) We call "refinement of ($F$)" a tower of $L / K$

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

satisfying the following condition: There exist integers

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

such that

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

In particular, $m \leq n$.

(2) A refinement of ($F$) is said to be "proper" when, in addition, the following condition holds:

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

(3) We say that ($E$) is a "Galois refinement of ($F$)" when ($E$) is a refinement of ($F$) satisfying the following additional condition:

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

(4) Let $L / K$ be a galtowerable extension. Two Galois towers of $L / K$

$$(F) \quad K = F_0 \trianglelefteq \ldots \trianglelefteq F_{i-1} \trianglelefteq F_i \trianglelefteq \ldots \trianglelefteq F_m = L,$$

$$(E) \quad K = E_0 \trianglelefteq \ldots \trianglelefteq E_{j-1} \trianglelefteq E_j \trianglelefteq \ldots \trianglelefteq E_n = L,$$

are said to be "equivalent", if and only if

(4.1) they have the same height (Definition 2.3(1)): $m = n$;

(4.2) up to permutation, the Galois groups of their steps are isomorphic (topologically in infinite degrees)

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

**Lemma 4.2.** *A Galois refinement of a Galois tower is still a Galois tower.*

**Proof.** Cf. [2, p.58, Proposition 1.7]. □

We can now state a perfect Galois analogue of the Schreier's theorem for normal series of groups [22].

**Theorem 4.3.** *Let $L / K$ be a galtowerable* (*not necessarily finite*) *extension. Any two Galois towers of $L / K$ have equivalent Galois refinements.*

**Proof.** A formal proof, using a Galois closure of $L / K$, is obtained while transporting, via the bijections of Galois-Krull, the construction of the subgroups made for Schreier's theorem. Another proof, much more interesting because remaining inside $L / K$, was given in [2, p.93, Theorem 3.2]. □

**Definition 4.4.** Let $L / K$ be a galtowerable extension and (*F*) be a Galois tower of $L / K$. We say that (*F*) is a "composition Galois tower of $L / K$", when it is strict and such that there does not exist a proper Galois refinement of (*F*) (Definition 4.1(3)).

**Example 4.5.** Any finite Galois extension has a composition Galois tower (induced by a composition series of its group).

In group theory, we know that a normal series of a given group is a composition series, if and only if each factor of the series is a simple group. Here is the Galois analogue of this equivalence.

**Proposition 4.6.** *Let* $L / K$ *be a galtowerable extension* (*finite or infinite*). *A Galois tower* (*F*) *of* $L / K$ *is a composition Galois tower of* $L / K$, *if and only if each step of* (*F*) *is a galsimple extension* (*Definition* 3.4).

**Proof.** (Let us give it in details, because it is very representative of the arguments used in this section.) For $L = K$, the equivalence is true. Now, let $L / K$ be a nontrivial extension and

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

be a Galois tower of $L / K$.

Assume that (*F*) is composition Galois tower of $L / K$ with one step $F_{i_0+1} / F_{i_0}$, which is not a galsimple extension: There exists a field *F* such that $F_{i_0} \lhd F \lhd F_{i_0+1}$. Then, the tower defined by

$$\forall j \in \{0, \ldots, i_0\}; \quad E_j := F_j, E_{i_0+1} := F, \forall j \in \{i_0 + 2, \ldots, m+1\}; E_j := F_{j-1}$$

is a proper Galois refinement of (*F*): a contradiction since (*F*) is a composition tower.

Conversely, if each step of (*F*) is a galsimple extension, then (*F*) is strict (Definition 3.4). Assume that there exists a proper Galois refinement (*E*) of (*F*). Following Lemma 4.2, (*E*) is still a Galois tower:

$$(E) \quad K = E_0 = F_0 \trianglelefteq \ldots \trianglelefteq E_{j_i} = F_i \trianglelefteq \ldots \trianglelefteq E_j \trianglelefteq \ldots \leq E_n = F_m = L,$$

with $\{j \in \{1, \ldots, n-1\} \mid \forall i \in \{0, \ldots, m\}; E_j \neq F_i\} \neq \emptyset$. Let $l$ be the smallest element of this set. There exists $k \in \{0, \ldots, m-1\}$ such that $E_{l-1} = F_k$. Therefore,

• if $j_{k+1} \leq l-1$, then $F_{k+1} = E_{j_{k+1}} \leq E_{l-1} = F_k < F_{k+1}$ : a contradiction;

• if $j_{k+1} = l$, then $F_{k+1} = E_l$ : a contradiction by definition of $l$.

Thus, necessarily, we have $j_{k+1} \geq l+1$, and

$$F_k = E_{l-1} < E_l \leq E_{l+1} \leq \cdots \leq E_{j_{k+1}} = F_{k+1} \neq E_l.$$

But in the Galois tower ($E$), the step $E_l / E_{l-1}$ is a Galois extension, which contradicts the galsimplicity of $F_{k+1} / F_k$. □

**Proposition 4.7.** *An infinite Galois extension is never galsimple.*

**Proof.** Let $L / K$ be an infinite Galois extension. We know that for the family $\{E_i\}_{i \in I}$ of intermediate fields of $L / K$ such that

$$\forall i \in I; \quad K \trianglelefteq E_i \leq L; \quad [E_i : K] < \infty,$$

we have $L = \bigcup_{i \in I} E_i$ ([5, AV.54, Corollary 2] or [15, p.16, Satz 2.3]). □

In general, a group does not admit a composition series. The finite groups do, but they are not the only ones. We saw that the field extensions, even finite and separable, do not necessarily admit a Galois tower. With the notion of a galtowerable extension, the following theorem allows to determine precisely the field extensions admitting a composition Galois tower.

**Theorem 4.8.** *A field extension admits a composition Galois tower, if and only if it is finite and galtowerable.*

**Proof.** For any infinite extension admitting a composition Galois tower ($T$), there necessarily exists a step of ($T$), which is both of infinite degree and a galsimple extension in view of Proposition 4.6, contradicting the previous proposition. Conversely, it is enough to concatenate composition towers of each Galois step of a tower of the extension (they exist by Example 4.5) and to apply Proposition 4.6 again. □

**Proposition 4.9.** *Let $L / K$ be a nontrivial finite galtowerable extension. A Galois tower of $L / K$ is a composition Galois tower, if and only if each of its steps has a Galois group that is finite and simple.*

**Proof.** Use Proposition 4.6 and Example 3.5. □

**Corollary 4.10.** *A field extension is nontrivial finite and galtowerable, if and only if it dissociates into a Galois tower, each step of which having a finite simple Galois group.*

**Proposition 4.11.** *Notations are those of Definitions* 2.3 *and* 4.1.

(1) *We say that* (*E*) *is a "trivial refinement of* (*F*)", *if and only if it is a nonproper refinement of* (*F*), *i.e., such that*

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

(2) *There exists one and only one strict tower* (*S*) *of $L / K$ such that* (*F*) *is a trivial refinement of* (*S*). *We call* (*S*) "*the strict tower associated to* (*F*)", *and we denote it by* $(F_<) := (S)$.

(3) *The strict tower associated to a Galois tower is still a Galois tower.*

**Proof.** Cf. [2, Chapter 3]. □

**Proposition 4.12.** *Let $L / K$ be a galtowerable extension.*

(1) *Let* (*F*) *and* (*E*) *be two Galois towers of $L / K$. Assume that* (*F*) *and* (*E*) *are equivalent* (*Definition* 4.1(4)). *Then*

(1-1) (*E*) *is a composition Galois tower, if and only if* (*F*) *is a composition Galois tower.*

(1-2) *The associated strict towers* $(F_<)$ *and* $(E_<)$ *are equivalent.*

(2) *For any strict tower* (*F*) *of $L / K$ and any Galois refinement* (*E*) *of* (*F*), $(E_<)$ *is still a Galois refinement of* (*F*).

**Proof.** Cf. [2, Chapter 3]. □

Let us note that the functional aspect of the previous Proposition 4.12 shows, a posteriori, the good choice of the refinements definitions.

We are now able to state a perfect Galois analogue of the Jordan-Hölder theorem ([14], [10]).

**Theorem 4.13.** *Let $L / K$ be a finite galtowerable extension.*

(1) *Any strict Galois tower of $L / K$ admits a refinement, which is a composition Galois tower of $L / K$.*

(2) *Any two composition Galois towers of $L / K$ are equivalent.*

**Proof.** (1) Following Theorem 4.8, $L / K$ admits a composition Galois tower ($C$). Let ($T$) be a strict Galois tower of $L / K$. Following Theorem 4.3, ($C$) and ($T$) have equivalent Galois refinements $(C')$ and $(T')$, respectively. Since there does not exist a proper Galois refinement of the composition Galois tower ($C$), $(C')$ is necessarily a trivial refinement of ($C$) (Proposition 4.11(1)). But ($C$) is strict by Definition 4.4, so ($C$) is the strict tower associated to $(C') : (C) = (C'_<)$. Now, let us use the three points of Proposition 4.12. By the (1.2), one obtains that ($C$) is equivalent to the associated strict tower $(T'_<)$ (it is a Galois tower by Proposition 4.11(3)). At last, following Proposition 4.12(2), $(T'_<)$ is a (Galois) refinement of ($T$).

(2) In part (1), when ($T$) is a composition Galois tower, the same argument as for ($C$) leads to $(T) = (T'_<)$. The equivalence of $(C'_<)$ and $(T'_<)$ is thus that of ($C$) and ($T$). □

Point (2) of the previous Theorem 4.13 with (4) of Definition 4.1 enable us to highlight an invariant of the construction of each finite galtowerable extension.

**Definition 4.14.** For a finite galtowerable extension $L / K$, we call "composition height of $L / K$", and we denote by $h(L / K)$, the number of steps of any one of its composition Galois towers.

**Example 4.15.** Let $\zeta_n := e^{2i\pi/n} (n \in \mathbb{N} \setminus \{0\})$. Let us consider the following two towers of the same extension $L / K$:

$$(T^1)\ K = \mathbb{Q} =: T_0^1 < T_1^1 := T_0^1(i, \sqrt[4]{5}) < T_2^1 := T_1^1(\zeta_{15}, Y^{1/5}, Z^{1/3}) = L,$$

$$(T^2)\ K = \mathbb{Q} =: T_0^2 < T_1^2 := T_0^2(\zeta_{15}) < T_2^2 := T_1^2(i, Y^{1/5}) < T_3^2 := L,$$

where we denote by $Y^{1/5}$ (resp., $Z^{1/3}$) any of the complex fifth (resp., third) roots of

$$Y := (2 - \zeta_5)^3(2 - \zeta_5^4)^2; \qquad (\text{resp.}, Z := 6 - \sqrt{5}).$$

These towers are Galois towers (for $(T^1)$, this can be proven via the notion of Galois averages introduced in [19] and [13], or even by [18] and [20]).

The degree of $L / K$ is $[L : K] = 480$. We illustrate:

• the Galois Schreier theorem (Theorem 4.3) by the following two equivalent strict Galois towers of $L / K$:

$$(T'^1)\ \ K = \mathbb{Q} =: T_0'^1 \lhd T_1'^1 := \mathbb{Q}(\sqrt{5}) \lhd T_2'^1 := T_1'^1(i) \lhd T_3'^1 := T_2'^1(\sqrt[4]{5})$$

$$\lhd T_4'^1 := T_3'^1(\zeta_{15}) \lhd T_5'^1 := T_4'^1(Y^{1/5}) \lhd T_6'^1 := T_5'^1(Z^{1/3}) = L,$$

$$(T'^2)\ \ K = \mathbb{Q} =: T_0'^2 \lhd T_1'^2 := \mathbb{Q}(\sqrt{5}) \lhd T_2'^2 := T_1'^2(\zeta_{15}) \lhd T_3'^2 := T_2'^2(i)$$

$$\lhd T_4'^2 := T_3'^2(Y^{1/5}) \lhd T_5'^2 := T_4'^2(\sqrt[4]{5}) \lhd T_6'^2 := L;$$

• the Galois Jordan-Hölder theorem (Theorem 4.13) by the equivalent composition Galois towers of $L / K$, with seven steps, obtained by refining the fourth (resp., the second) step of $(T'^1)$ (resp., $(T'^2)$) by the following one:

$$T_3'^1 \lhd T_3'^1(\zeta_5) \lhd T_3'^1(\zeta_{15}) = T_4'^1$$

$$(\text{resp., } T_1'^2 \lhd T_1'^2(\zeta_5) \lhd T_1'^2(\zeta_{15}) = T_2'^2).$$

The composition height (Definition 4.14) of $L / K$ is thus $h(L / K) = 7$.

## 5. Semi-Abelian Extensions and Galois Analogue of the Feit-Thompson Theorem

Due to the degree barrier (cf. Section 7, final table), almost all the galtowerable extensions that one uses normally are semi-abelian.

**Definition 5.1** [3, p.73]**.** We say that a field extension $L / K$ is "semi-abelian", when it dissociates into an abelian tower

$$(T) \quad K = T_0 \trianglelefteq T_1 \trianglelefteq \ldots \trianglelefteq T_i \trianglelefteq T_{i+1} \trianglelefteq \ldots \trianglelefteq T_m = L;$$

$$\forall i \in \{0, \ldots, m-1\}; \quad Gal(T_{i+1} / T_i) \text{ abelian.}$$

In particular, semi-abelian extensions are galtowerable and they enjoy the same properties as the latter.

**Proposition 5.2.** *Proposition* 2.8 *and Corollary* 2.9 *remain true when replacing everywhere "galtowerable" by "semi-abelian".*

**Proof.** In the notations of Proposition 2.8:

(1) Clear by translation of an abelian tower of $L / J$.

(2) Apply (1) by translating $L / J$ by $K / J$.

(3) Following (1), $(KL / K)$ is a semi-abelian extension, and since it is the same for $K / J$, we conclude by transitivity of (0). □

**Lemma 5.3.** (1) *Any refinement of an abelian tower is still an abelian tower.*

(2) *The strict tower associated to an abelian tower* (*Proposition* 4.11(2)) *is still an abelian tower.*

**Proof.** Straightforward from the definitions. □

Following Theorem 4.8, a finite semi-abelian extension admits composition Galois towers.

**Proposition 5.4.** *All composition Galois towers of a finite semi-abelian extension are abelian towers.*

**Proof.** Let $L/K$ be a finite semi-abelian extension. Let ($A$) (resp., ($C$)) be an abelian tower (resp., a composition Galois tower) of $L/K$. Following Theorem 4.3, ($A$) and ($C$) have equivalent Galois refinements $(A')$ and $(C')$. From Lemma 5.3(1), we deduce immediately that $(C')$ is an abelian tower. Moreover, $(C')$ is necessarily a trivial refinement of the composition Galois tower ($C$), and we have $(C) = (C'_<)$ (Proposition 4.11(2)). Then, the conclusion follows from Lemma 5.3(2). □

In group theory, we know that a (nontrivial) finite group is solvable, if and only if it admits a composition series, the factors of which are cyclic of prime orders. The following theorem gives a Galois analogue of this characterization:

**Theorem 5.5.** *A finite nontrivial extension is semi-abelian, if and only if it admits a composition Galois tower, the steps of which are cyclic extensions of prime degrees.*

**Proof.** Propositions 5.4 and 4.9 suffice since the only abelian simple groups are cyclic of prime orders. □

**Corollary 5.6.** *Let $L/K$ be a finite nontrivial semi-abelian extension. Let $[L:K] = p_1^{m_1} \cdots p_r^{m_r}$ be the prime decomposition of its degree. Then, the composition height of $L/K$ (Definition 4.14) is $h(L/K) = m_1 + \cdots + m_r$.*

**Proof.** Use Theorem 5.5 and Lemma 2.4. □

There are many semi-abelian extensions.

**Proposition 5.7.** *There exists only one galtowerable extension of degree $\leq 119$, which is not semi-abelian: The non-abelian Galois extension with simple Galois group $A_5$.*

**Proof.** Since $|A_5| = 60$, Corollary 4.10 suffices. □

Here is an easy criterion to detect semi-abelian extensions by means of the orders of finite non-abelian simple groups.

**Proposition 5.8.** *Let $L/K$ be a finite galtowerable extension of degree $d := [L : K]$. Suppose that the following two conditions hold*:

(i) *The integer d is not the order of a finite non-abelian simple group.*

(ii) *For any non-abelian simple group S of order $|S| \leq \frac{d}{2}$,*

$$d \not\equiv 0 \bmod(|S|).$$

*Then $L/K$ is necessarily a semi-abelian extension.*

**Proof.** Thanks to Corollary 4.10, if $L/K$ is a not a semi-abelian extension, there exists a non-abelian simple group $S$, whose order divides $d$, say $d = q|S|$, with $q \geq 2$ by (i), which contradicts (ii). □

**Example 5.9.** Any galtowerable extension of degree 1010 is semi-abelian.

Indeed, it is enough to check the former criterion with the following orders:

$$|A_5| = 60, \quad |PSL_2(7)| = 168, \quad |A_6| = 360, \quad |PSL_2(8)| = 504.$$

A version of the Feit-Thompson theorem [9] is as follows:

**Odd Order Theorem** [4, p.260]. *Groups of odd order are solvable.*

Here is its Galois analogue:

**Theorem 5.10.** *Any finite galtowerable extension of odd degree is semi-abelian.*

**Remark 5.11.** Once again, the assumption of galtowerability is due to the fact that a finite extension is not necessarily galtowerable (Theorem 3.7 or Example 3.9), whereas any finite group does admit a normal series.

**Proof.** The trivial extension (of degree 1) is abelian, whence semi-abelian. Let $L/K$ be a nontrivial finite galtowerable extension of odd degree. According to Corollary 4.10, it dissociates into a Galois tower, each step of which has a simple group as its Galois group. Now, following the Feit-Thompson theorem, any finite non-abelian simple group is of even order. Then $L/K$ is necessarily a semi-abelian extension. □

The galtowerable extensions of odd degree are thus classified.

**Corollary 5.12.** *A finite extension of odd degree is galtowerable, if and only if it is semi-abelian.*

## 6. Solvable Extensions

One classifies groups since almost two centuries now; we suggest to classify finite and separable extensions.

In Lang's terminology [16, p.291], a finite separable extension $L/K$ is said to be "solvable", when it is a quotient (Definition 3.2) of a Galois extension $N/K$ with $Gal(N/K)$ a solvable group. (For an equivalent definition, see also [8, p.197].)

**Proposition 6.1.** *A finite semi-abelian extension is always a solvable extension. The converse is not true.*

**Proof.** Any $p$-group is solvable and solvable extensions form a distinguished class [16, p.291, Proposition 7.1]. Then use Theorem 5.5. Lack of a converse is proven by counterexample 6.2 below: □

A solvable extension is not necessarily semi-abelian.

**Example 6.2.** Let $f(X)$ be a quartic polynomial in $\mathbb{Q}[X]$, whose Galois group over $\mathbb{Q}$ is $\mathbb{S}_4$ or $\mathbb{A}_4$ (for instance, $X^4+X+1$ or $X^4+8X+12$ [12, p.38]). Let $\theta$ be a root of $f(X)$; then $\mathbb{Q}(\theta)/\mathbb{Q}$ is solvable. If $N$ is the splitting field of $f(X)$, then $Gal(N/\mathbb{Q}(\theta))$ is a maximal subgroup of $Gal(N/\mathbb{Q})$, so there is no field lying strictly between $\mathbb{Q}(\theta)$ and $\mathbb{Q}$. Since

$\mathbb{Q}(\theta)/\mathbb{Q}$ is not Galois, $\mathbb{Q}(\theta)$ is definitely not a galtowerable extension of $\mathbb{Q}$ and a fortiori $\mathbb{Q}(\theta)/\mathbb{Q}$ is not a semi-abelian extension.

The previous counterexample raises the question of determining, which extensions are both solvable and galtowerable.

**Theorem 6.3.** *A finite extension is solvable and galtowerable, if and only if it is semi-abelian.*

**Proof.** According to Proposition 6.1, it is enough to prove that an extension $L/K$, which is both solvable and galtowerable is necessarily semi-abelian. Let us fix a field $N$, containing $L$, such that $N/K$ is a Galois extension with $Gal(N/K)$ a solvable group. Any composition series of $Gal(N/K)$ (resp., of its solvable subgroup $Gal(N/L)$) clearly induces a composition Galois tower (*C*) (resp., (*D*)) of $N/K$ (resp., $N/L$), whose steps are cyclic of prime degrees. Moreover, following Theorem 4.8, the finite galtowerable extension $L/K$ admits a Galois composition tower, say (*B*), and by Proposition 4.9, all the steps of (*B*) have a simple group as Galois group. Then, still by the same proposition, we deduce that the juxtaposition of (*B*) and (*D*) (in other words, "the amalgamated tower (*B*)⨿(*D*) of (*B*) and (*D*) at *L*") is a Galois composition tower of $N/K$. Now, according to the Galois Jordan-Hölder theorem (Theorem 4.13), the composition towers (*C*) and (*B*)⨿(*D*) are necessarily equivalent. It follows that (*B*) is abelian, therefore that $L/K$ is semi-abelian. □

The galtowerable solvable extensions are thus classified (Theorems 6.3 and 5.5).

**Question 6.4.** How to build the nongaltowerable finite solvable extensions?

## 7. Finite Galtowerable Nonsemi-Abelian Extensions

**Definition 7.1.** Let $L/K$ be a nontrivial finite galtowerable extension.

(1) We call "composition group of $L/K$" any Galois group of a step into a composition Galois tower of $L/K$ (Theorem 4.8).

(2) Let $\{S_1, \ldots, S_n\}$ be a family of finite simple groups. We say that $L/K$ is an $\{S_1, \ldots, S_n\}$-extension, if and only if each $S_i$ is a composition group of $L/K$ (Proposition 4.9).

Note that the extension $L/K$ may contain composition groups other than the $S_i$.

By the Galois Jordan-Hölder theorem (Theorem 4.13), the groups $S_i$ do not depend on the considered composition Galois towers of $L/K$; they are unique up to permutation.

**Example 7.2.** According to Theorem 5.5, a semi-abelian extension is a $(\mathbb{Z}/p_1\mathbb{Z}, \ldots, \mathbb{Z}/p_{h(L/K)}\mathbb{Z})$-extension, where the $p_i (i = 1, \ldots, h(L/K))$ are prime numbers. In particular, this is the case for a galtowerable extension that is solvable (Theorem 6.3) or of odd degree (Theorem 5.10).

As often as not in practice, we omit simple composition groups when they are abelian, to mention only the non-abelian ones, whenever there exist.

**Definition 7.3.** Let $\{S_1, \ldots, S_n\}$ be a family of finite non-abelian simple groups. We say that $L/K$ is "a strict $\{S_1, \ldots, S_n\}$-extension", if and only if any composition group of $L/K$ different from all $S_i (i = 1, \ldots, n)$ is necessarily abelian.

**Proposition 7.4.** *Let* $L / K$ *be a finite galtowerable extension with composition height* $h(L / K) \geq 1$. *If the following inequality holds for the degree of L over K*:

$$[L : K] \leq 119 \times 2^{h(L/K)-1},$$

*then*

- *either* $[L : K] \equiv 0 \mod 60$ *and* $L / K$ *is a strict* $A_5$*-extension*;
- *or* $[L : K] \not\equiv 0 \mod 60$ *and* $L / K$ *is a semi-abelian extension.*

**Proof.** According to Proposition 5.7, this is true for $h(L / K) = 1$. This allows us to proceed by induction: Assume the result for all galtowerable extensions of composition height $h$. Let $L / K$ be an extension admitting a composition Galois tower

$$(C) \quad K = C_0 \lhd C_1 \lhd \ldots \lhd C_h \lhd C_{h+1} = L,$$

and suppose that $[L : K] \leq 119 \times 2^h$. Since $2 \leq [L : C_h]$ (Definition 4.4), we have $[C_h : K] \leq 119 \times 2^{h-1}$. But clearly $h(C_h / K) = h$, so by induction over $h$, the proposition holds for $C_h / K$. Furthermore,

$$2^h \leq [C_h : K] \Rightarrow 2^h [L : C_h] \leq [L : K] \Rightarrow [L : C_h] \leq 119.$$

Then Proposition 5.7 completes the proof. □

**Lemma 7.5.** *Any nontrivial galtowerable extension of degree* $\leq 335$ *is*

- *either a strict* $A_5$*-extension*;
- *or a Galois extension with* $PSL_2(7)$ *Galois group.*

**Proof.** Let $L / K$ be a nontrivial galtowerable extension of degree $\leq 335$. We know by Corollary 4.10 that it dissociates into a Galois tower

$$(C) \quad K = C_0 \lhd C_1 \lhd \ldots \lhd C_i \lhd C_{i+1} \lhd \ldots \lhd C_h = L,$$

each step of which having a simple Galois group. According to the table of the orders of finite non-abelian simple groups [17], the only possible non-

abelian groups $Gal(C_{i+1} / C_i)$ are isomorphic to $A_5$ or $PSL_2(7)$. In this latter case, 168 divides $[L : K] \leq 335$, therefore $[L : K] = 168$ and

$$K = C_i \lhd C_{i+1} = L.$$

□

**Proposition 7.6.** *Let $L / K$ be a finite galtowerable extension with composition height $h(L / K) \geq 1$. Assume that the degree of $L / K$ satisfies the inequality*

$$[L : K] \leq 335 \times 2^{h(L/K)-1}.$$

*Then $L / K$ necessarily falls into one, and only one, of the following four cases*:

$$([L : K] \equiv 0 \mod 60, \quad [L : K] \equiv 0 \mod 168)$$

(i) $$\Downarrow$$

$$(L / K \text{ is a strict } \{A_5, PSL_2(7)\}\text{- extension}).$$

*In that case*,

$$[L : K] \equiv 0 \mod 840.$$

$$([L : K] \equiv 0 \mod 60, \quad [L : K] \not\equiv 0 \mod 168)$$

(ii) $$\Downarrow$$

$$(L / K \text{ is a strict } A_5\text{- extension}).$$

$$([L : K] \not\equiv 0 \mod 60, \quad [L : K] \equiv 0 \mod 168)$$

(iii) $$\Downarrow$$

$$(L / K \text{ is a strict } PSL_2(7)\text{- extension}).$$

$$([L : K] \not\equiv 0 \mod 60, \quad [L : K] \not\equiv 0 \mod 168)$$

(iv) $$\Downarrow$$

$$(L / K \text{ is a semi-abelian extension}).$$

**Proof.** In the same way as in the proof of Proposition 7.4, we argue by induction over $h(L/K)$ using Lemma 7.5 instead of Proposition 5.7.

□

We can multiply, at will, statements generalizing Propositions 7.4 and 7.6.

As a matter of conclusion, we set the table of possible degrees ≤ 10080 for finite galtowerable nonsemi-abelian extensions. It is obtained by negation of Theorem 5.5 and by using the orders of the first sixteen finite non-abelian simple groups as they appear for instance in [17]. A galtowerable extension $L/K$ of degree not appearing in this table is necessarily semi-abelian. Its composition height $h(L/K)$ is equal to the number of prime factors of $[L:K]$, counted with their multiplicities (Corollary 5.6). And all of its composition Galois towers (Theorem 4.13(2)) consist of cyclic steps with degrees equal to these prime factors.

**Table of Degrees** $\leq$ 10080
**of Galtowerable Nonsemi-Abelian Extensions**

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 60 | 120 | 168 | 180 | 240 | 300 | 336 | 360 | 420 | 480 | 504 | 540 | 600 | 660 | 672 |
| 720 | 780 | 840 | 900 | 960 | 1008 | 1020 | 1080 | 1092 | 1140 | 1176 | 1200 | 1260 | 1320 | 1344 |
| 1380 | 1440 | 1500 | 1512 | 1560 | 1620 | 1680 | 1740 | 1800 | 1848 | 1860 | 1920 | 1980 | 2016 | 2040 |
| 2100 | 2160 | 2184 | 2220 | 2280 | 2340 | 2352 | 2400 | 2448 | 2460 | 2520 | 2580 | 2640 | 2688 | 2700 |
| 2760 | 2820 | 2856 | 2880 | 2940 | 3000 | 3024 | 3060 | 3120 | 3180 | 3192 | 3240 | 3276 | 3300 | 3360 |
| 3420 | 3480 | 3528 | 3540 | 3600 | 3660 | 3696 | 3720 | 3780 | 3840 | 3864 | 3900 | 3960 | 4020 | 4032 |
| 4080 | 4140 | 4200 | 4260 | 4320 | 4368 | 4380 | 4440 | 4500 | 4536 | 4560 | 4620 | 4680 | 4704 | 4740 |
| 4800 | 4860 | 4872 | 4896 | 4920 | 4980 | 5040 | 5100 | 5160 | 5208 | 5220 | 5280 | 5340 | 5376 | 5400 |
| 5460 | 5520 | 5544 | 5580 | 5616 | 5640 | 5700 | 5712 | 5760 | 5820 | 5880 | 5940 | 6000 | 6048 | 6060 |
| 6072 | 6120 | 6180 | 6216 | 6240 | 6300 | 6360 | 6384 | 6420 | 6480 | 6540 | 6552 | 6600 | 6660 | 6720 |
| 6780 | 6840 | 6888 | 6900 | 6960 | 7020 | 7056 | 7080 | 7140 | 7200 | 7224 | 7260 | 7320 | 7344 | 7380 |
| 7392 | 7440 | 7500 | 7560 | 7620 | 7644 | 7680 | 7728 | 7740 | 7800 | 7860 | 7896 | 7920 | 7980 | 8040 |
| 8064 | 8100 | 8160 | 8220 | 8232 | 8280 | 8340 | 8400 | 8460 | 8520 | 8568 | 8580 | 8640 | 8700 | 8736 |
| 8760 | 8820 | 8880 | 8904 | 8940 | 9000 | 9060 | 9072 | 9120 | 9180 | 9240 | 9300 | 9360 | 9408 | 9420 |
| 9480 | 9540 | 9576 | 9600 | 9660 | 9720 | 9744 | 9780 | 9792 | 9828 | 9840 | 9900 | 9912 | 10020 | 10080 |

In our intention to classify finite separable extensions (Section 6), the objective is far from being reached. Via Corollary 4.10 and the classification of finite non-abelian simple groups, we may consider that the problem is solved for galtowerable extensions. But how to build the ones which are not? The nature of the obstruction to the Galois dissociation is elucidated by means of the untowerable field in Theorem 3.7. We are thus reduced to the following problem (which generalizes Question 6.4 for solvable extensions):

**Question 7.7.** How to classify galsimple (Definition 3.4) non-Galois extensions?

## References


[1] E. Andréo and R. Massy, Parallélogrammes Galoisiens infinis, Annales Math. Blaise Pascal 8 (2001), 21-45.

[2] E. Andréo, Dissociation des Extensions Algébriques de Corps par les Extensions Galoisiennes ou Galsimples non Galoisiennes, Thèse de Doctorat, Univ. Valenciennes (2004), arXiv:0905.4385.

[3] E. Artin, Galoissche Theorie, B. G. Teubner-Verlag, Leipzig, 1959.

[4] M. Aschbacher, Finite Group Theory, 2nd Edition, Cambridge Studies in Advanced Math. 10, Cambridge University Press, New York, 2000.

[5] N. Bourbaki, Algèbre, Chapteres 4 à 7, Hermann, Paris, 1971.

[6] H. Cohen et al., Users guide for PARI/GP.

http://pari.math.u-bordeaux.fr/doc.html

[7] R. F. Coleman, On the Galois groups of the exponential Taylor polynomials, L'Enseignement Mathématique 33 (1987), 183-189.

[8] D. Cox, Galois Theory, Wiley-Interscience, New Jersey, 2004.

[9] W. Feit and J. G. Thompson, Solvability of groups of odd order, Pacific J. Math. 13 (1963), 775-1029.

[10] O. Hölder, Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen, Math. Ann. 34 (1889), 26-56.

[11] B. Huppert, Endliche Gruppen I, Grundlehren der Mathematischen Wissenschaften 134, Springer-Verlag, Berlin, 1983.

[12] C. U. Jensen, A. Ledet and N. Yui, Generic Polynomials, Constructive Aspects of the Inverse Galois Problem, MSRI Publication 45, Cambridge University Press, New York, 2002.

[13] C. U. Jensen and R. Massy, Some remarks on Hilbertian fields (An appendix to the paper "Galois averages" by Massy), J. Number Theory 120 (2006), 229-233.

[14] C. Jordan, Commentaire sur Galois, Math. Ann. 1 (1869), 141-160 (Oeuvres Gauthier-Villars 1 (1961), 211-230).

[15] H. Koch, Galois Theory of $p$-Extensions, Springer Monographs in Math., Berlin, 2002, or Galoissche Theorie der $p$-Erweiterungen, Springer-Verlag, Berlin, 1970.

[16] S. Lang, Algebra, 3rd Edition, Graduate Texts in Math. 211, Springer, New York, 2002.

[17] D. Madore, Orders of non abelian simple groups, Ecole Normale Supérieure.

http://www.madore.org/~david/math/simplegroups.html

[18] 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(1) (2002), 21-26.

[19] R. Massy, Galois averages, J. Number Theory 113 (2005), 244-275.

[20] R. Massy, An algorithmic construction of cyclic $p$-extensions of fields, with characteristic different from $p$, not containing the $p$-th roots of unity, Acta Arithmetica 139(1) (2009), 9-16.

[21] J. S. Rose, A Course on Group Theory, Cambridge University Press, Cambridge, 1978.

[22] O. Schreier, Über den Jordan-Hölderschen Satz, Abh. Math. Sem. Univ. Hamburg 6 (1928), 300-302.

[23] I. Schur, Gleichungen ohne Affekt, Gesammelte Abhandlungen, Band III 67 (1930), 191-197, Springer-Verlag, Berlin, 1973.

[24] E. S. Selmer, On the irreducibility of certain trinomials, Math. Scand. 4 (1956), 287-302.

[25] J.-P. Serre, Topics in Galois Theory, Jones and Bartlett, Boston, 1992.

■