Polynesian Journal of Mathematics

Volume 2, Issue 3

A finiteness theorem for 2-towers of number fields

Xavier Vidaux Carlos Rodolfo Videla

Received 2 Jan 2025
Accepted 18 Mar 2025
Published 5 May 2025
Communicated by Gaetan Bisson

DOI: `10.69763/polyjmath.2.3`

Polynesian Journal of Mathematics
Volume 2, Issue 3 (May 2025)

A finiteness theorem for 2-towers of number fields

Xavier Vidaux[1] Carlos Rodolfo Videla[2]

[1]Departamento de Matemática, Universidad de Concepción, Chile
[2]Department of Mathematics and Computing, Mount Royal University, Calgary, Canada

À la mémoire de Jacques Savariau. *

Abstract

We show that if a 2-tower $(F_n)_{n\geqslant 0}$ of number fields does not contain infinitely many Galois quartic extensions, then the structure of the lattice of subfields of the union F of the F_n is completely determined by studying the subfields of F up to some degree.

Keywords: Towers of number fields, 2-towers, lattice of subfields.

1 Introduction

We call a sequence $(F_n)_{n\geqslant 0}$ of number fields a 2-*tower* if $F_n \subseteq F_{n+1}$ and the degrees $[F_{n+1} : F_n]$ are exactly 2 for every n. A 2-tower $(F_n)_{n\geqslant 0}$ of number fields is *thin (from F_0)* if the F_n are the only subfields of $F = \bigcup_{n\geqslant 0} F_n$ containing F_0 which have finite degree over F_0 — see [4], and [5, Prop. 13.1] in the context of cyclotomic fields. Given a 2-tower $\mathcal{F} = (F_n)_{n\geqslant 0}$ such that $(F_n)_{n\geqslant m}$ is thin for some $m \geqslant 1$, with $F = \bigcup_{n\geqslant 0} F_n$, for each $\ell \geqslant m + 1$, we let $\Phi(\mathcal{F}, \ell)$ denote the set of intermediate fields of degree 2^ℓ that are different from F_ℓ, namely,

$$\Phi(\mathcal{F}, \ell) = \left\{L : F_0 \subseteq L \subseteq F \text{ and } [L : F_0] = 2^\ell \text{ and } L \neq F_\ell\right\}.$$

We prove (note that the third statement is trivially equivalent to the second one):

---

*Jacques Savariau était professeur à l'université de la Polynésie française lorsque le premier auteur y était étudiant. Il lui a transmis sa passion pour les mathématiques.

The two authors have been partially supported by the first author's ANID Fondecyt research project 1210329, Chile. Part of this work was done during visits in April 2022 and December 2023 to Mount Royal University, Canada. The first author thanks Mount Royal University for its hospitality during the stay. We thank the two referees for their comments, which helped to improve the presentation of this work.

Theorem 1.1. *Let F_0 be a number field. Let $\mathcal{F} = (F_n)_{n\geqslant 0}$ be a 2-tower and $F = \bigcup_{n\geqslant 0} F_n$. Assume that the tower $(F_n)_{n\geqslant m}$ is thin for some $m \geqslant 1$. Let $\ell \geqslant m+1$.*

1. *All fields in $\Phi(\mathcal{F},\ell)$ are subfields of $F_{\ell+m}$.*
2. *If some $\Phi(\mathcal{F},\ell)$ is non-empty but each of $\Phi(\mathcal{F},m+1),\dots,\Phi(\mathcal{F},2m)$ is empty, then there is some $n \geqslant 2m$ such that F_{n+2}/F_n is Galois, hence cyclic.*
3. *If for every $n \geqslant 2m$ the extension F_{n+2}/F_n is not cyclic and each of $\Phi(\mathcal{F},m+1),\dots,$ $\Phi(\mathcal{F},2m)$ is empty, then for every $\ell \geqslant m+1$, $\Phi(\mathcal{F},\ell)$ is empty.*

Motivated by a problem of Julia Robinson, we studied thin 2-towers in [4]. There we prove that a 2-tower is thin if and only if there is no quartic extension within it which is Galois with Galois group the Klein group V_4 of 4 elements — see [4, Thm. 2.4]. It is easy to see that, for a thin tower, the only subfield of infinite degree of F is F itself — see [4, Rem. 2.2]. Nevertheless, this need not be true if $(F_n)_{n\geqslant m}$ is thin for some $m \geqslant 1$, while $(F_n)_{n\geqslant m-1}$ is not — see [4, Thm. 1.4-3] for an example with $m = 1$:

$$K^{2,0} = \mathbb{Q}(\sqrt{2}) \cup \mathbb{Q}(\sqrt{2+\sqrt{2}}) \cup \cdots \qquad \text{is a subfield of}$$

$$K^{2,1} = \mathbb{Q}(\sqrt{3}) \cup \mathbb{Q}(\sqrt{2+\sqrt{3}}) \cup \mathbb{Q}(\sqrt{2+\sqrt{2+\sqrt{3}}}) \cup \cdots$$

that has infinite degree over $\mathbb{Q}$ and $K^{2,1}$ is thin from $\mathbb{Q}(\sqrt{3})$ but not from $\mathbb{Q}$. Intermediate fields of finite degree over F_0 that are different from any F_n also can appear in this case. In that paper, we developed some tools for $m = 1$ that eventually allowed us to determine the structure of subfields of F for infinitely many towers — this is a contribution to the study of the lattice of subfields of infinite extensions of $\mathbb{Q}$ beyond the cyclotomic case. Nevertheless, for $m \geqslant 2$, the situation is much more involved. In this work, we generalize some of these tools to any $m \geqslant 1$ and produce two infinite families of examples with $m = 2$ for which we completely determine the structure of subfields.

For 2-towers that are thin from some point on, as it is written, the second statement of Theorem 1.1 gives a finiteness criterion for having a cyclic quartic extension within the 2-tower. Note that the first and third statements together give the finiteness result the title refers to. Indeed, if one knows that a 2-tower as in Theorem 1.1 has no cyclic quartic subextension after some point, then by the third statement it says that if there is no intermediate subfield in a finite piece of the tower, then every $\Phi(\mathcal{F},\ell)$ must be empty, reducing the problem of determining the lattice of subfields of F to the problem of studying the subfields of F up to some degree (by the first statement). The proof is given in Section 2. Note that, in the second statement, proving that F_{n+2}/F_n is Galois is the same as proving that it is cyclic, because if it were Klein this would contradict the thinness from m.

Finally, Section 3 is dedicated to the construction of concrete infinite families of towers for which Theorem 1.1 applies and for which we compute the lattice of subfields — see Figure 1.

For basic facts on lattices of subfields in the abelian case, see for instance [5, Ch. 14].

2 Proof of the theorem

We will often use without explanation the fact that if M/K and M/L are Galois extensions of number fields, then $M/K \cap L$ is Galois (apply [1, Ch. 11, Ex. 11.10, p. 98], taking into account that, in our case, M is always finite over $K \cap L$).

The following lemma generalizes [4, Lem. 2.6]. It implies Item 1 of Theorem 1.1.

Lemma 2.1. *Let $m \geqslant 1$ and $k \geqslant m+1$ be integers. Let $(F_n)_{n\geqslant 0}$ be a 2-tower and $F = \bigcup_{n\geqslant 0} F_n$. If the tower $(F_n)_{n\geqslant m}$ is thin and L is a subfield of F which contains F_0, then either L is a subfield of F_k or $[L : F_0] \geqslant 2^{k-m+1}$. So, if L has degree 2^ℓ over F_0 for some $\ell \geqslant 1$, then L is a subfield of $F_{\ell+m}$.*

Proof. Assume that L is not a subfield of F_k. If L has infinite degree over F_0, there is nothing to prove. Assume that L has finite degree over F_0, so also F_mL has finite degree over F_0, hence F_mL has finite degree over F_m. Since $(F_n)_{n\geqslant m}$ is thin, there is some $j \geqslant m$ such that $F_mL = F_j$. Since L is not a subfield of F_k, we have $j \geqslant k+1$. Since

$$2^m[L : F_0] = [F_m : F_0][L : F_0] \geqslant [F_mL : F_0] = [F_j : F_0] = 2^j,$$

we have $[L : F_0] \geqslant 2^{j-m} \geqslant 2^{k-m+1}$. □

Definition 2.2. *If $\mathcal{F} = (F_n)_{n\geqslant 0}$ is a 2-tower and $c \geqslant 1$ and $u \geqslant c+1$ are integers, we say that the property $H_c(\mathcal{F}, u)$ is true if at least one of the following extensions (whenever the indices are non-negative integers) is Galois:*

$$\begin{array}{cccc}
F_{u+1}/F_{2c} & & & \\
F_{u+1}/F_{2c-1} & F_{u+2}/F_{2c-1} & & \\
\vdots & \vdots & \ddots & \\
F_{u+1}/F_{c+1} & F_{u+2}/F_{c+1} & \cdots & F_{u+c}/F_{c+1}
\end{array}$$

Note that there are c rows and c columns if and only if $u \geqslant 2c-1$, otherwise some of the listed extensions (e.g. F_{u+1}/F_{2c}) do not make sense. Nevertheless, since $u \geqslant c+1$, there is always at least the whole last line of extensions remaining in the list and, since $c \geqslant 1$, there is at least one extension remaining in this line, namely F_{u+1}/F_{c+1} (note that, if $c \geqslant 2$, then the last line has at least two distinct extensions remaining).

Remark 2.3. If the property $H_c(\mathcal{F}, u)$ is true for some $u \geqslant 2c+1$, then there exists $n \geqslant 2c+1$ such that F_{n+1}/F_{n-1} is Galois.

Lemma 2.4. *Let $\mathcal{F} = (F_n)_{n\geqslant 0}$ be a 2-tower and $c \geqslant 2$ and $u \geqslant c+1$ be integers. Consider the shifted sequence $\mathcal{G} = (G_n)_{n\geqslant 0}$ where $G_n = F_{n+1}$. If $H_{c-1}(\mathcal{G}, u-1)$ is true, then $H_c(\mathcal{F}, u)$ is true.*

Proof. Indeed, the list of possible extensions for $H_{c-1}(\mathcal{G}, u-1)$ is

$$\begin{array}{cccc}
G_u/G_{2c-2} & & & \\
G_u/G_{2c-3} & G_{u+1}/G_{2c-3} & & \\
\vdots & \vdots & \ddots & \\
G_u/G_c & G_{u+1}/G_c & \cdots & G_{u+c-2}/G_c
\end{array}
=
\begin{array}{cccc}
F_{u+1}/F_{2c-1} & & & \\
F_{u+1}/F_{2c-2} & F_{u+2}/F_{2c-2} & & \\
\vdots & \vdots & \ddots & \\
F_{u+1}/F_{c+1} & F_{u+2}/F_{c+1} & \cdots & F_{u+c-1}/F_{c+1},
\end{array}$$

which is a subset of the options for $H_c(\mathcal{F}, u)$ (taking out the longest diagonal), which is non-empty because $c \geqslant 2$. □

Lemma 2.5. *Let* $\mathcal{F} = (F_n)_{n\geqslant 0}$ *be a* 2*-tower and* $c \geqslant 2$ *and* $u \geqslant c+1$ *be integers. Consider the shifted sequence* $\mathcal{G} = (G_n)_{n\geqslant 0}$*, where* $G_n = F_{n+1}$*. If* $H_{c-1}(\mathcal{G}, u)$ *is true, then* $H_c(\mathcal{F}, u)$ *is true.*

Proof. Indeed, the list of possible extensions for $H_{c-1}(\mathcal{G}, u)$ is

$$\begin{array}{cccc} G_{u+1}/G_{2c-2} & & & \\ G_{u+1}/G_{2c-3} & G_{u+2}/G_{2c-3} & & \\ \vdots & \vdots & \ddots & \\ G_{u+1}/G_c & G_{u+2}/G_c & \cdots & G_{u+c-1}/G_c \end{array} = \begin{array}{cccc} F_{u+2}/F_{2c-1} & & & \\ F_{u+2}/F_{2c-2} & F_{u+3}/F_{2c-2} & & \\ \vdots & \vdots & \ddots & \\ F_{u+2}/F_{c+1} & F_{u+3}/F_{c+1} & \cdots & F_{u+c}/F_{c+1}, \end{array}$$

which is a subset of the options for $H_c(\mathcal{F}, u)$ (taking out the first column), which is non-empty because $c \geqslant 2$. □

Recall that, for a tower $\mathcal{F}$ thin from $m = 1$ and $\ell \geqslant m + 1$, we have

$$\Phi(\mathcal{F}, \ell) = \left\{L : F_0 \subseteq L \subseteq F_{\ell+m} \text{ and } [L : F_0] = 2^{\ell} \geqslant 2^{m+1} \text{ and } L \neq F_{\ell}\right\}.$$

If some $\Phi(\mathcal{F}, \ell)$ is non-empty, we denote by $\ell_{\mathcal{F}}$ the minimum of the set of ℓ such that $\Phi(\mathcal{F}, \ell)$ is non-empty.

Lemma 2.6. *Let* F_0 *be a number field. Let* $\mathcal{F} = (F_n)_{n\geqslant 0}$ *be a* 2*-tower and* $F = \bigcup_{n\geqslant 0} F_n$*. Assume that the tower* $(F_n)_{n\geqslant 1}$ *is thin. If some* $\Phi(\mathcal{F}, \ell)$ *is non-empty, then* $F_{\ell_{\mathcal{F}}+1}/F_2$ *is Galois (namely, the property* $H_1(\mathcal{F}, \ell_{\mathcal{F}})$ *is true).*

Proof. Let $\ell = \ell_{\mathcal{F}}$. Let $L \in \Phi(\mathcal{F}, \ell)$. We first prove that the field $L \cap F_{\ell}$ is not any of the F_n for $1 \leqslant n \leqslant \ell$. Assume the contrary. We then have $F_1 \subseteq F_n = L \cap F_{\ell} \subseteq L$. Therefore, since the tower is thin from $n = 1$, L is one of the F_j and, since L has degree 2^{ℓ}, we have $L = F_{\ell}$. This contradicts the fact that L lies in $\Phi(\mathcal{F}, \ell)$.

In particular, $L \cap F_{\ell} \neq F_{\ell}$ is a proper subfield of F_{ℓ}, hence it has degree 2^k for some $k < \ell$. If $k \geqslant 2$, then $L \cap F_{\ell} \in \Phi(\mathcal{F}, k)$ for $k < \ell$, contradicting the minimality of ℓ. Hence we have $k \leqslant 1$ and $L \cap F_{\ell}$ is a subfield of F_2 by Lemma 2.1. Also by Lemma 2.1, L is a subfield of $F_{\ell+1}$. Since the extensions $F_{\ell+1}/L$ and $F_{\ell+1}/F_{\ell}$ are quadratic, they are Galois, hence $F_{\ell+1}/L \cap F_{\ell}$ is Galois, hence $F_{\ell+1}/F_2$ is Galois. □

Lemma 2.7. *Let* F_0 *be a number field. Let* $\mathcal{F} = (F_n)_{n\geqslant 0}$ *be a* 2*-tower and* $F = \bigcup_{n\geqslant 0} F_n$*. Assume that the tower* $(F_n)_{n\geqslant m}$ *is thin for some* $m \geqslant 1$*. Consider the shifted sequence* $\mathcal{G} = (G_n)_{n\geqslant 0}$*, where* $G_n = F_{n+1}$*. If for some* $\ell \geqslant m + 1$ *there is a field* L *in* $\Phi(\mathcal{F}, \ell)$ *that contains* F_1*, then* $\ell_{\mathcal{G}} \geqslant m$ *exists and we have* $\ell_{\mathcal{F}} \leqslant \ell_{\mathcal{G}} + 1$*.*

Proof. Note that $\mathcal{G} = (G_n)_{n\geqslant m-1}$ is thin. Since $\ell - 1 \geqslant (m-1) + 1$, $\Phi(\mathcal{G}, \ell - 1)$ exists and we have $L \in \Phi(\mathcal{G}, \ell - 1)$, so in particular $\ell_{\mathcal{G}}$ exists (and is $\geqslant m$) and $\Phi(\mathcal{G}, \ell_{\mathcal{G}}) \neq \varnothing$

by definition of $\ell_{\mathcal{G}}$. Since

$$\begin{aligned}\Phi(\mathcal{G},\ell_{\mathcal{G}}) &= \left\{L : G_0 \subseteq L \subseteq G \text{ and } [L : G_0] = 2^{\ell_{\mathcal{G}}} \geqslant 2^m \text{ and } L \neq G_{\ell_{\mathcal{G}}}\right\}\\ &= \left\{L : F_1 \subseteq L \subseteq G \text{ and } [L : F_1] = 2^{\ell_{\mathcal{G}}} \geqslant 2^m \text{ and } L \neq F_{\ell_{\mathcal{G}}+1}\right\}\\ &\subseteq \left\{L : F_0 \subseteq L \subseteq F \text{ and } [L : F_0] = 2^{\ell_{\mathcal{G}}+1} \geqslant 2^{m+1} \text{ and } L \neq F_{\ell_{\mathcal{G}}+1}\right\}\\ &= \Phi(\mathcal{F},\ell_{\mathcal{G}}+1),\end{aligned}$$

where the last equality makes sense because $\ell_{\mathcal{G}} + 1 \geqslant m + 1$, and, since $\Phi(\mathcal{G},\ell_{\mathcal{G}}) \neq \varnothing$, we deduce that $\Phi(\mathcal{F},\ell_{\mathcal{G}}+1) \neq \varnothing$ and we then have $\ell_{\mathcal{F}} \leqslant \ell_{\mathcal{G}} + 1$ by minimality of $\ell_{\mathcal{F}}$. ◻

Lemma 2.8. *Let F_0 be a number field. Let $\mathcal{F} = (F_n)_{n\geqslant 0}$ be a 2-tower and $F = \bigcup_{n\geqslant 0} F_n$. Assume that the tower $(F_n)_{n\geqslant m}$ is thin for some $m \geqslant 1$. If some $\Phi(\mathcal{F},\ell)$ is non-empty, then the property $H_m(\mathcal{F},\ell_{\mathcal{F}})$ is true.*

Proof. We prove the lemma by induction on m. It is true for $m = 1$ by Lemma 2.6. Assume that it is true up to $m - 1$ for some $m \geqslant 2$. Let $\mathcal{F} = (F_n)_{n\geqslant 0}$ be a 2-tower and $F = \bigcup_{n\geqslant 0} F_n$ such that the tower $(F_n)_{n\geqslant m}$ is thin and $\Phi(\mathcal{F},\ell)$ is non-empty for some ℓ (hence $\ell_{\mathcal{F}} \geqslant m + 1$ and $\Phi(\mathcal{F},\ell_{\mathcal{F}})$ is non-empty). Let $L \in \Phi(\mathcal{F},\ell_{\mathcal{F}})$. Consider the tower $\mathcal{G} = (G_n)_{n\geqslant 0}$ defined by $G_n = F_{n+1}$. Since $(F_n)_{n\geqslant m}$ is thin, $(G_n)_{n\geqslant m-1}$ is thin. Let $G = \bigcup_{n\geqslant 0} G_n$. The proof will be done in two steps, depending whether or not L contains F_1.

Case 1: L contains F_1 (hence G_0). On the one hand, we have $\ell_{\mathcal{F}} \leqslant \ell_{\mathcal{G}} + 1$ by Lemma 2.7. On the other hand, we have $[L : G_0] = 2^{\ell_{\mathcal{F}}-1} \geqslant 2^m$ and $L \neq F_{\ell_{\mathcal{F}}} = G_{\ell_{\mathcal{F}}-1}$, so we have $L \in \Phi(\mathcal{G},\ell_{\mathcal{F}} - 1)$, hence $\ell_{\mathcal{G}} \leqslant \ell_{\mathcal{F}} - 1$ by minimality of $\ell_{\mathcal{G}}$. So in that case, we have $\ell_{\mathcal{F}} = \ell_{\mathcal{G}} + 1$. By hypothesis of induction applied to the tower $\mathcal{G}$, the property $H_{m-1}\big(\mathcal{G},(\ell_{\mathcal{G}} + 1) - 1\big)$ is true and, since $m \geqslant 2$ and $\ell_{\mathcal{G}} + 1 \geqslant m + 1$, the property $H_m(\mathcal{F},\ell_{\mathcal{G}} + 1)$ is true by Lemma 2.4, so we can conclude because $\ell_{\mathcal{G}} + 1 = \ell_{\mathcal{F}}$.

Case 2: L does not contain F_1. We have then

$$2^{\ell_{\mathcal{F}}} < [LF_1 : F_0] \leqslant [L : F_0][F_1 : F_0] = 2^{\ell_{\mathcal{F}}+1},$$

hence $[LF_1 : F_0] = 2^{\ell_{\mathcal{F}}+1}$.

If $LF_1 \neq F_{\ell_{\mathcal{F}}+1}$, then by Lemma 2.7, since LF_1 lies in some $\Phi(\mathcal{F},\ell)$ and contains F_1, we know that $\ell_{\mathcal{G}}$ exists and $\ell_{\mathcal{F}} \leqslant \ell_{\mathcal{G}} + 1$. Since $[LF_1 : G_0] = 2^{\ell_{\mathcal{F}}} \geqslant 2^{m+1} \geqslant 2^m$ and $LF_1 \neq F_{\ell_{\mathcal{F}}+1} = G_{\ell_{\mathcal{F}}}$, we have $LF_1 \in \Phi(\mathcal{G},\ell_{\mathcal{F}})$, hence $\ell_{\mathcal{G}} \leqslant \ell_{\mathcal{F}}$ by minimality of $\ell_{\mathcal{G}}$. For the sake of contradiction, assume $\ell_{\mathcal{G}} < \ell_{\mathcal{F}}$. Since $\ell_{\mathcal{F}} \leqslant \ell_{\mathcal{G}} + 1$ we have $\ell_{\mathcal{F}} = \ell_{\mathcal{G}} + 1$. By definition of $\ell_{\mathcal{G}}$, there exists a field $L' \subseteq G$ which contains G_0, such that $[L' : G_0] = 2^{\ell_{\mathcal{G}}} \geqslant 2^m$ and $L' \neq G_{\ell_{\mathcal{G}}}$, namely, $L' \subseteq F$ contains F_1, $[L' : F_0] = 2^{\ell_{\mathcal{G}}+1} \geqslant 2^{m+1}$ and $L' \neq F_{\ell_{\mathcal{G}}+1}$. But we have $\ell_{\mathcal{F}} = \ell_{\mathcal{G}} + 1$, hence $L' \subseteq F$ contains F_1, $[L' : F_1] = 2^{\ell_{\mathcal{F}}} \geqslant 2^{m+1}$ and $L' \neq F_{\ell_{\mathcal{F}}}$. Hence $L' \in \Phi(\mathcal{F},\ell_{\mathcal{F}})$, but this contradicts the fact that no field in $\Phi(\mathcal{F},\ell_{\mathcal{F}})$ contains F_1. Hence we have $\ell_{\mathcal{F}} = \ell_{\mathcal{G}}$. By hypothesis of induction applied to the tower $\mathcal{G}$, the property $H_{m-1}(\mathcal{G},\ell_{\mathcal{G}})$ is true and, since $m \geqslant 2$ and $\ell_{\mathcal{G}} = \ell_{\mathcal{F}} \geqslant m + 1$, the property $H_m(\mathcal{F},\ell_{\mathcal{G}})$ is true by Lemma 2.5, so we can conclude because $\ell_{\mathcal{G}} = \ell_{\mathcal{F}}$.

Otherwise, we have $[F_{\ell_{\mathcal{F}}+1} : L] = [LF_1 : L] = 2$ and, therefore, the extension $F_{\ell_{\mathcal{F}}+1}/(L \cap F_{\ell_{\mathcal{F}}})$ is Galois.

If $L \cap F_{\ell_{\mathcal{F}}} = F_n$ for some $m \leqslant n \leqslant \ell_{\mathcal{F}}$, then $F_m \subseteq F_n = L \cap F_{\ell_{\mathcal{F}}} \subseteq L$, hence $L = F_{\ell_{\mathcal{F}}}$ because the tower is thin from m, but this contradicts our hypothesis on L. Therefore, $L \cap F_{\ell_{\mathcal{F}}}$ is different from F_n for each $n \geqslant m$, hence it is a proper subfield of $F_{\ell_{\mathcal{F}}}$, hence it has degree $< 2^{\ell_{\mathcal{F}}}$, hence it is a proper subfield of L and, by minimality of $\ell_{\mathcal{F}}$, it has degree at most 2^m. Therefore, $L \cap F_{\ell_{\mathcal{F}}}$ is a subfield of F_{2m} by Lemma 2.1. Since $F_{\ell_{\mathcal{F}}+1}/(L \cap F_{\ell_{\mathcal{F}}})$ is Galois, we deduce that $F_{\ell_{\mathcal{F}}+1}/F_{2m}$ is Galois and, since $\ell_{\mathcal{F}} \geqslant m+1$, the property $H_m(\mathcal{F}, \ell_{\mathcal{F}})$ is true. ☐

Under the hypothesis of Item 2 of Theorem 1.1, the property $H_m(\mathcal{F}, \ell_{\mathcal{F}})$ is true by Lemma 2.8 and we have $\ell_{\mathcal{F}} \geqslant 2m + 1$ because each of $\Phi(\mathcal{F}, m + 1), \dots, \Phi(\mathcal{F}, 2m)$ is empty. Therefore, there exists $n \geqslant 2m$ such that F_{n+1}/F_n is Galois by Remark 2.3, which concludes the proof of Item 2 of Theorem 1.1.

3 Examples

Let $P = X^4 + cX^2 + d$ be a polynomial over a field F, with roots $\pm\alpha$ and $\pm\beta$. It is irreducible over F if and only if α^2 and $\alpha\beta$ are not in F (see [2, Thm. 2] and its proof) — note that the irreducibility condition $\alpha\beta \notin F$ is equivalent to the condition that d is not a square in F. The splitting field of P has Galois group V_4 if and only if d is a square in F, the cyclic group C_4 if and only if $d(c^2 - 4d)$ is a square in F, and the dihedral group with eight elements D_4 otherwise, namely for neither d nor $d(c^2 - 4d)$ a square in F. See [2, Thm. 3].

We now give two examples where we can apply the main theorem. Both consider 2-towers $(\mathbb{Q}(\alpha_n))_{n\geqslant 0}$ that are *nested* in the sense that $\alpha_{n+1}^2 \in \mathbb{Q}(\alpha_n) \setminus \mathbb{Q}(\alpha_{n-1})$. In a third example, we give a nested 2-tower in which no finite portion of the tower can contain all the quadratic extensions of $\mathbb{Q}$ which are in the tower, so this tower is not thin from any level and the conclusion of Item 3 of Theorem 1.1 is false. Hence to be nested is not the point in the previous two examples, but thinness.

3.1 Examples 1 and 2

We first prove a lemma.

Lemma 3.1. *Let F be a number field. Let $L = F(\sqrt{b})$ be a quadratic extension of F, with b a cube and an algebraic integer in F. There exist infinitely many $a \in F$ such that the splitting field of $L(\sqrt{a + \sqrt{b}})/F$ is Galois with Galois group D_4.*

Proof. Note that the roots of the polynomial $X^4 - 2aX^2 + a^2 - b$ are $\alpha = \sqrt{a + \sqrt{b}}$, $\beta = \sqrt{a - \sqrt{b}}$, and their opposites. This polynomial is irreducible over F if and only if b and $a^2 - b$ are not squares in F by [2, Thm. 2] and the observation made at the beginning of this section. We know that b is not a square by hypothesis. Furthermore, for the group to be D_4, we need $(a^2 - b)b$ to be a non-square in F.

Consider the elliptic curve $Y^3 - b = X^2$. By Siegel's theorem it has finitely many integral points over F, so it has only finitely many points of the form (x, a^2), even with

$x \in F$. So among the a that are cubes, there can only be finitely many of them such that $a^2 - b$ is a square.

Similarly, consider the elliptic curve $Y^3 - b^2 = X^2$. Again this curve has finitely many points of the form $(x, \sqrt[3]{b}a^2)$. So among the a that are cubes, there can only be finitely many of them such that $b(a^2 - b)$ is a square. $\square$

Given integers v and x_0, write $x_n = \sqrt{v + x_{n-1}}$ for $1 \leqslant n \leqslant 6$ (choose any root) and $K_n = \mathbb{Q}(x_n)$. Thanks to the above Lemma, we can extend the tower to a 2-tower $(K_n)_{n \geqslant 0}$ so that none of the extensions K_{n+1}/K_{n-1} is Galois for $n \geqslant 6$. Indeed, we have $K_6 = K_5(\sqrt{v + x_5})$. If $v + x_5$ is a cube in K_5, then we just apply the lemma to get a K_7. If $v + x_5$ is not a cube in K_5, then we apply the lemma with $b = (v + x_5)^3$, noting that $K_6 = K_5(b)$. Next steps are done similarly.

The following list of commands defines a function in SageMath [3] that takes as entry v and x_0 and returns a list that says for each K_{n+2}/K_n whether it is or not Galois and then the number of subfields of K_2, K_3 and K_6 respectively. More specifically, with the notation of the program below:

- The letter a stands for a square root of $v + x_0$, so $K_1 = \mathbb{Q}(a) = \mathbb{Q}(\sqrt{v + x_0}) = \mathbb{Q}(x_1)$, and R_1 is the polynomial ring in the variable X_1 over K_1.
- The letter b stands for a root of $X_1^2 - v - a$, so $K_2 = K_1(b) = K_1(x_2)$. Etc.
- Line 7, K_6 is defined as a quartic extension of K_4.
- Lines 8 and 9, we ask whether $K_2/\mathbb{Q}$ is Galois, whether K_3/K_1 is Galois, and so on up to K_6/K_4.
- Finally, on the last line, we ask for the length of the sequence of subfields (i.e. the number of subfields) of K_2, K_3 and K_6.

```
nu=3; x0=17;
K1.<a> = QuadraticField(nu+x0); R1.<X1>=K1[];
K2.<b> = K1.extension(X1^2-nu-a); R2.<X2>=K2[];
K3.<c> = K1.extension(X1^4-2*nu*X1^2+nu^2-nu-a); R3.<X3>=K3[];
K4.<d> = K2.extension(X2^4-2*nu*X2^2+nu^2-nu-b); R4.<X4>=K4[];
K5.<e> = K3.extension(X3^4-2*nu*X3^2+nu^2-nu-c);
K6.<f> = K4.extension(X4^4-2*nu*X4^2+nu^2-nu-d);
[K2.is_galois_absolute(),K3.is_galois_relative(),K4.is_galois_relative(),
K5.is_galois_relative(),K6.is_galois_relative(),
len(K2.subfields()),len(K3.subfields()),len(K6.subfields())]
```

Example 1. For $v = 3$ and $x_0 = 17$, as above, the program returns `[False, True, False, False, False, 3, 6, 9]` and the command `K3.subfields()` lists 2 subfields of degree 4, so:

- Except for K_3/K_1, none of the quartic extensions is Galois, so they are of D_4 type.

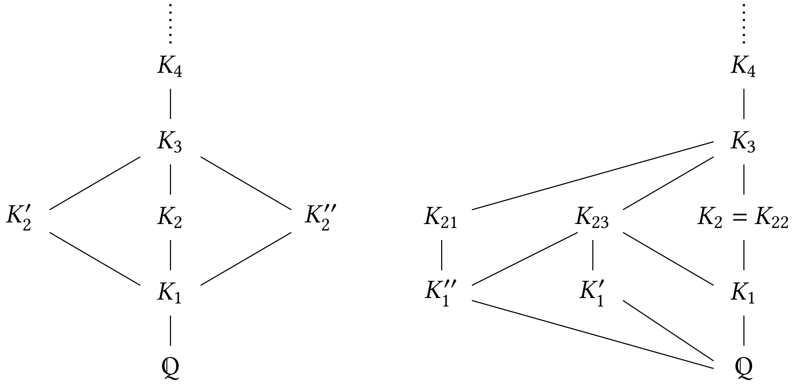

Figure 1: Using Theorem 1.1 to determine the structure of subfields.

- K_3/K_1 is Galois and K_3 has 2 subfields of degree 4 over $\mathbb{Q}$, hence K_3/K_1 is of V_4 type. In particular the tower $(K_n)_{n\geqslant 1}$ is not thin.
- The tower $(K_n)_{n\geqslant 2}$ is thin because all its quartic extensions are non-Galois by construction, so in particular they are not of V_4 type — see [4, Thm. 2.4].
- Since K_6 has 9 subfields, there is no field in the tower with degree 2^3 or 2^4, except for K_3 and K_4. We conclude by Item 3 of Theorem 1.1 that the lattice of subfields is as in Figure 1, left graph.

Example 2. The same program with $v = 9$ and $x_0 = 2259$ returns `[False, True, False, False, False, 3, 8, 11]`, so all the quartic extensions are of D_4 type, except for K_3/K_1. Among the 8 subfields of K_3, there are three of degree 2, one of which being K_1, and three of degree 4, one of which being K_2, with minimal polynomials $x^4+8x^3-126x^2-1072x+757$, $x^4+32x^3+366x^2+1760x+757$ and $x^4-16x^3-78x^2+632x+757$. The following commands return `[3, 3, 5]`, meaning that one of the three fields of degree 4 has 5 subfields and the other two have 3 subfields (K_2 is one of them).

```
x = polygen(ZZ, 'x');
K21.<a> = NumberField(x^4 + 8*x^3 - 126*x^2 - 1072*x + 757);
K22.<b> = NumberField(x^4 + 32*x^3 + 366*x^2 + 1760*x + 757);
K23.<c> = NumberField(x^4 - 16*x^3 - 78*x^2 + 632*x + 757);
[len(K21.subfields()), len(K22.subfields()), len(K23.subfields())]
```

Since K_6 has 11 subfields, there is no field in the tower with degree 2^3 or 2^4, except for K_3 and K_4. We conclude by Theorem 1.1 that the lattice of subfields is as in Figure 1, right graph.

We finish this section with the nested counter-example announced above.

3.2 Example 3

Write p_n for the n^{th} prime, $p_0 = 1$, and $\alpha_n = \sqrt{p_0 p_n} + \cdots + \sqrt{p_{n-1} p_n}$. So we have $\alpha_1 = \sqrt{2}$, $\alpha_2 = \sqrt{3} + \sqrt{6}$, $\alpha_3 = \sqrt{5} + \sqrt{10} + \sqrt{15}$, etc. Let $K = \bigcup_n K_n$, where $K_n = \mathbb{Q}(\alpha_n)$. Let $L_n = \mathbb{Q}(\sqrt{p_j p_n} : 0 \leqslant j \leqslant n-1)$. Observe that $L_n/\mathbb{Q}$ is an abelian extension of $\mathbb{Q}$ of degree 2^n — indeed the union of the L_n is the field $\mathbb{Q}(\sqrt{p_n} : n \geqslant 1)$. Therefore, its subextension K_n is a Galois extension of $\mathbb{Q}$. Let σ_j be the automorphism of L_n that sends $\sqrt{p_j p_n}$ to $-\sqrt{p_j p_n}$ and fixes $\sqrt{p_i p_n}$ for every $i \neq j$ (in particular we have $\sigma_j(K_n) = K_n$ because $K_n/\mathbb{Q}$ is Galois). So $2\sqrt{p_j p_n} = \alpha_n - \sigma_j(\alpha_n) \in K_n$. Hence $K_n = L_n$. Note that $\sqrt{p_i p_n}\sqrt{p_j p_n} = p_n\sqrt{p_i p_j}$, so we have $K_{n-1} \subseteq K_n$. Moreover, we have

$$\begin{aligned}
\alpha_n^2 &= (\sqrt{p_0 p_n} + \cdots + \sqrt{p_{n-1} p_n})^2 \\
&= p_n(p_0 + \cdots + p_{n-1}) + 2p_n \sum_{0 \leqslant j < k \leqslant n-1} \sqrt{p_j p_k} \\
&= p_n(p_0 + \cdots + p_{n-1}) + 2p_n(\alpha_{n-1} + \alpha_{n-2} + \cdots + \alpha_1) \in K_{n-1}.
\end{aligned}$$

We also deduce that α_n^2 is not in K_{n-2}: otherwise, the latter would give $\alpha_{n-1} \in K_{n-2}$, which is a contradiction since, if that were false, we would have $L_{n-1} = K_{n-1} = K_{n-2} = L_{n-2}$ yet L_{n-1} and L_{n-2} have different degree. We have therefore proved that the field

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5} \ldots)$$

is the union of a nested 2-tower and, for all natural numbers n, $\sqrt{n}$ lies in it.

References

[1] David J. H. Garling. *A course in Galois theory.* Cambridge University Press, 1986. ISBN: 9780521312493.

[2] Luise-Charlotte Kappe and Bette Warren. An elementary test for the Galois group of a quartic polynomial. *The American Mathematical Monthly*, 96(2):133–137, 1989. DOI: 10.2307/2323198.

[3] The Sage Developers. SageMath, the Sage Mathematics Software System. https://www.sagemath.org/, version 9.1, 2020.

[4] Xavier Vidaux and Carlos Rodolfo Videla. An approach to Julia Robinson numbers through the lattice of subfields. https://arxiv.org/abs/2401.14492, 2024.

[5] Lawrence Washington. *Introduction to Cyclotomic Fields.* Volume 83 of *Graduate Texts in Mathematics.* Springer, 1997. ISBN: 9780387947624.