Boolean FIP ring extensions
Gabriel Picavet, Martine Picavet-L’hermitte

To cite this version:
Gabriel Picavet, Martine Picavet-L’hermitte. Boolean FIP ring extensions. Communications in Algebra, Taylor & Francis, 2020, 48 (5), pp.1821-1852. 10.1080/00927872.2019.1708088. hal-02982795

HAL Id: hal-02982795
https://hal.archives-ouvertes.fr/hal-02982795
Submitted on 28 Oct 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
BOOLEAN FIP RING EXTENSIONS

GABRIEL PICAVET AND MARTINE PICAVET-L’HERMITTE

ABSTRACT. We characterize extensions of commutative rings $R \subseteq S$ whose sets of subextensions $[R, S]$ are finite (i.e. $R \subseteq S$ has the FIP property) and are Boolean lattices, that we call Boolean FIP extensions. Some characterizations involve “factorial” properties of the poset $[R, S]$. A non-trivial result is that each subextension of a Boolean FIP extension is simple (i.e. $R \subseteq S$ is a simple pair).

1. Introduction and Notation

We consider the category of commutative and unital rings, whose epimorphisms will be involved. If $R \subseteq S$ is a (ring) extension, we denote by $[R, S]$ the set of all $R$-subalgebras of $S$ and set $]R, S]:=[R, S]\setminus\{R, S\}$ (with a similar definition for $[R, S]$ or $]R, S]$).

A lattice is a poset $L$ such that every pair $a, b \in L$ has a supremum and an infimum. For an extension $R \subseteq S$, the poset $([R, S], \subseteq)$ is a complete lattice where the supremum of any non-void subset is the compositum which we call product from now on and denote by $\Pi$ when necessary, and the infimum of any non-void subset is the intersection. We are aiming to study some lattice properties of the poset $([R, S], \subseteq)$, mainly the Boolean property. As a general rule, an extension $R \subseteq S$ is said to have some property of lattices if $[R, S]$ has this property.

The extension $R \subseteq S$ is said to have FIP (for the “finitely many intermediate algebras property”) or an FIP extension if $[R, S]$ is finite. A chain of $R$-subalgebras of $S$ is a set of elements of $[R, S]$ that are pairwise comparable with respect to inclusion. When $[R, S]$ is a chain, the extension $R \subseteq S$ is called a $\lambda$-extension by Gilbert [18]. We will say that $R \subseteq S$ is chained. We also say that the extension $R \subseteq S$ has FCP (or is an FCP extension) if each chain in $[R, S]$ is finite. Clearly, each extension that satisfies FIP must also satisfy FCP. Dobbs and the authors characterized FCP and FIP extensions [11].

2010 Mathematics Subject Classification. Primary: 13B02, 13B21, 13B22, 06E05, 06C10; Secondary: 13B30, 12F10, 06E25.

Key words and phrases. FIP, FCP extension, minimal extension, integral extension, support of a module, lattice, Boolean lattice, algebraic field extension, Galois extension.
Let $R \subseteq S$ be an FCP extension, then $[R, S]$ is a complete Noetherian Artinian lattice, with $R$ as the least element and $S$ as the largest element. We use lattice definitions and properties described in [25].

Our main tool is minimal (ring) extensions, a concept that was introduced by Ferrand-Olivier [17]. Recall that an extension $R \subseteq S$ is called minimal if $[R, S] = \{R, S\}$. An extension $R \subseteq S$ is called a simple extension if $S = R[t]$ for some $t \in S$ and a simple pair if $R \subseteq T$ is a simple extension for each $T \in [R, S]$. A minimal extension is simple. The key connection between the above ideas is that if $R \subseteq S$ has FCP, then any maximal (necessarily finite) chain of $R$-subalgebras of $S$, $R = R_0 \subset R_1 \subset \cdots \subset R_{n-1} \subset R_n = S$, with length $n < \infty$, results from juxtaposing $n$ minimal extensions $R_i \subset R_{i+1}$, $0 \leq i \leq n - 1$. An FCP extension is finitely generated, and (module) finite if integral. For any extension $R \subseteq S$, the length $\ell[R, S]$ of $[R, S]$ is the supremum of the lengths of chains of $R$-subalgebras of $S$. Notice that if $R \subseteq S$ has FCP, then there does exist some maximal chain of $R$-subalgebras of $S$ with length $\ell[R, S]$ [12, Theorem 4.11].

1.1. **A summary of the main results.** Any undefined material is explained at the end of the section or in the next sections.

Section 2 is devoted to some general properties of lattices $[R, S]$, mainly in the context of FCP and FIP extensions. Since Boolean extensions are distributive, we evidently have to work on distributive extensions, which is done in this section. We discuss the decomposition of elements of $[R, S]$ into irreducible elements. When $[R, S]$ has finitely many atoms and each element of $[R, S]$ is a product of atoms, then Proposition 2.18 shows that $R \subseteq S$ has FIP and is almost-Prüfer, and Theorem 2.11 shows that $R \subseteq S$ is a simple pair. Section 3 is devoted to the study of arbitrary FIP extensions.

The canonical decomposition of a ring extension is crucial. It consists of the tower $R \subseteq \hat{\circ} S R \subseteq ^t \circ S R \subseteq \overline{R} \subseteq S$, where $\hat{\circ} S R$ (resp. $^t \circ S R$) is the seminormalization (resp. $t$-closure) of $R$ in $S$ (see Section 3, Definition 3.23). This decomposition allows us to only consider special extensions:
subintegral, seminormal infra-integral, t-closed and integrally closed. The t-closed case is reduced to the context of field extensions and is the subject of Section 4. In particular, for a field extension \( k \subset L \) with separable closure \( T \) and radicial closure \( U \) such that \( U, T \notin \{ k, L \} \), Theorem 4.2 shows that \( k \subset L \) is Boolean if and only if \( k \subset U \) and \( T \subset L \) are minimal, \( [k, L] = [k, T] \cup [U, L] \), \( k \subset T \) and \( k \subset U \) are linearly disjoint and \( [k, T] \) is a Boolean lattice. Boolean separable field extensions need special study. A striking result is Theorem 4.19: A Galois finite extension (hence FIP) \( k \subset L \) is Boolean if and only if \( k \subset L \) is a cyclic extension whose dimension is square free.

1.2. Some conventions and notation. A local ring is here what is called elsewhere a quasi-local ring. As usual, \( \text{Spec}(R) \) and \( \text{Max}(R) \) are the set of prime and maximal ideals of a ring \( R \). The support of an \( R \)-module \( E \) is \( \text{Supp}_R(E) := \{ P \in \text{Spec}(R) \mid E_P \neq 0 \} \), and \( \text{MSupp}_R(E) := \text{Supp}_R(E) \cap \text{Max}(R) \). When \( R \subseteq S \) is an extension, we will set \( \text{Supp}_R(T/R) := \text{Supp}(T/R) \) and \( \text{Supp}_R(S/T) := \text{Supp}(S/T) \) for each \( T \in [R, S] \), unless otherwise specified.

If \( R \subseteq S \) is a ring extension and \( P \in \text{Spec}(R) \), then \( S_P \) is both the localization \( S_{R \setminus P} \) as a ring and the localization at \( P \) of the \( R \)-module \( S \). We denote by \( \kappa_R(P) \) the residual field \( R_P/PR_P \) at \( P \). An extension \( R \subset S \) is called locally minimal if \( R_P \subset S_P \) is minimal for each \( P \in \text{Supp}(S/R) \) or equivalently for each \( P \in \text{MSupp}(S/R) \).

We denote by \( (R : S) \) the conductor of \( R \subseteq S \). The integral closure of \( R \) in \( S \) is denoted by \( \widetilde{R}^S \) (or by \( \overline{R} \) if no confusion can occur).

Recall ([23, Theorem 5.2, page 47]) that an extension \( R \subseteq S \) is Prüfer (or a normal pair) if \( R \subseteq T \) is a flat epimorphism for each \( T \in [R, S] \). The Prüfer hull of an extension \( R \subseteq S \) is the greatest Prüfer subextension \( \widetilde{R} \) of \( [R, S] \) [29]. An extension \( R \subseteq S \) is called almost-Prüfer if \( \widetilde{R} \subseteq S \) is integral, or equivalently, when \( R \subseteq S \) is FIP, if \( S = \widetilde{R} \overline{R} \) [31, Theorem 4.6].

A poset \( (X, \leq) \) is called a tree if \( x_1, x_2 \leq x_3 \) in \( X \) implies that \( x_1 \) and \( x_2 \) are comparable (with respect to \( \leq \)). We also say that \( (X, \leq) \) is treed. A subset \( Y \) of \( X \) is called an antichain if no two distinct elements of \( Y \) are comparable.

Finally, \( |X| \) is the cardinality of a set \( X \), \( \subset \) denotes proper inclusion and, for a positive integer \( n \), we set \( \mathbb{N}_n := \{1, \ldots, n\} \). The characteristic of an integral domain \( k \) is denoted by \( c(k) \). For \( a, b, c \) in a ring \( R \), if \( c \) divides \( a - b \), we write \( a \equiv b (c) \).
2. Lattices properties of the poset $[R, S]$

2.1. Some definitions on the lattice $[R, S]$. In the context of a lattice $[R, S]$, some definitions and properties of lattices have the following formulations.

An element $T \in [R, S]$ is called $\cap$-irreducible (resp.; $\Pi$-irreducible) (see [25]) if $T = T_1 \cap T_2$ (resp.; $T = T_1 T_2$) implies either $T = T_1$ or $T = T_2$.

An element $T$ of $[R, S]$ is an atom (resp.; co-atom) if and only if $R \subset T$ (resp.; $T \subset S$) is a minimal extension. Therefore, an atom (resp.; co-atom) is $\Pi$-irreducible (resp.; $\cap$-irreducible). We denote by $A$ the set of atoms of $[R, S]$ and by $\mathcal{CA}$ the set of co-atoms of $[R, S]$.

Now $R \subset S$ is called:

(a) atomic (resp.; atomistic) if each $T \in [R, S]$ contains some atom (resp.; is the product of atoms (contained in $T$)) [33, page 80].

(b) co-atomic (resp.; co-atomistic) if each $T \in [R, S]$ is contained in some co-atom (resp.; is the intersection of co-atoms (containing $T$)).

(c) distributive if intersection and product are each distributive with respect to the other. Actually, each distributivity implies the other [25, Exercise 5, page 33].

(d) factorial (resp.; co-factorial) if each element of $[R, S]$ has a unique irredundant representation by a finite product of atoms (resp.; a unique irredundant representation by a finite intersection of co-atoms.)

An FCP extension is both atomic and co-atomic.

We introduce a definition reminiscent of arithmetic rings [30].

Definition 2.1. A ring extension $R \subseteq S$ is called arithmetic if $[R_P, S_P]$ is a chain for each $P \in \text{Spec}(R)$.

Example 2.2. The extension $R \subset S$ is arithmetic in the following cases ([30, Example 5.13] for (2), (3) and (4)). See Section 3, Definition 3.23 for (3) and (4):

1. $R \subset S$ is locally minimal.
2. $R \subset S$ has FCP and is integrally closed.
3. $R \subset S$ is FIP subintegral and $|R/M| = \infty$ for each $M \in \text{MSupp}(S/R)$.
4. $R \subset S$ is FIP t-closed integral such that $R_M/MR_M \subset S_M/MS_M$ is radicial for each $M \in \text{MSupp}(S/R)$.
5. We also have examples in [32, Theorem 6.1] of arithmetic extensions $R \subset S$ of length 2, when $|[R, S]| = 3$.

We proved in [30, Proposition 5.18]:

Proposition 2.3. An arithmetic extension is distributive.
The following proposition will make easier many proofs.

**Proposition 2.4.** Let $R \subseteq S$ be a ring extension. The following statements are equivalent:

1. $R \subseteq S$ is distributive;
2. $R_M \subseteq S_M$ is distributive for each $M \in \text{MSupp}(S/R)$;
3. $R_P \subseteq S_P$ is distributive for each $P \in \text{Supp}(S/R)$;
4. $R/I \subseteq S/I$ is distributive for each ideal $I$ shared by $R$ and $S$;
5. $R/I \subseteq S/I$ is distributive for some ideal $I$ shared by $R$ and $S$.

**Proof.** We have obviously (1) $\Rightarrow$ (3) $\Rightarrow$ (2). Conversely, assume that $R_M \subseteq S_M$ is distributive for each $M \in \text{MSupp}(S/R)$. Then, $R_M \subseteq S_M$ is distributive for each $M \in \text{Max}(R)$. It follows that the distributivity property holds in $[R, S]$ since it holds in any $[R_M, S_M]$.

We recall that a lattice isomorphism is nothing but a bijective lattice morphism. An ideal $I$ shared by $R$ and $S$ also is an ideal of any $T \in [R, S]$. The map $\varphi : [R, S] \to [R/I, S/I]$ defined by $\varphi(T) := T/I$ is a bijection and a lattice morphism. Indeed, for any $T, U \in [R, S]$, we have $(T/I) \cap (U/I) = (T \cap U)/I$ and $(T/I)(U/I) = (TU)/I$. Then, we get the equivalence between (1), (4) and (5). $\Box$

**Proposition 2.5.** [21, Theorem 1, p. 172] In a distributive lattice of finite length, all maximal chains between two comparable elements have the same length (the Jordan-Hölder chain condition or condition (JH)).

**Proposition 2.6.** [8, Remarks, page 9 and Theorem 1.7] A distributive extension $R \subset S$ satisfies the upper covering condition (UCC), which means that for each $T, U \in [R, S]$ such that $T \cap U \subset T$ is minimal, then $U \subset TU$ is minimal.

2.2. Some distributive extensions are simple. We are going to show that some special subextensions of an FCP distributive extension are simple. Before doing so, the next lemma is needed.

**Lemma 2.7.** If $R \subset S$ is a distributive extension, then $R[x, y] = R[x + y]$ whenever $y \in S \setminus R$, $x \in S \setminus R[y]$ and $R \subset R[x]$ is minimal.

**Proof.** Consider the diagram

```
R[x, y]  \\
|       |       |
R[x]    R[y]  \\
|       |       |
R       R[y]  \\
```

Since $R[x]R[y] = R[x, y]$ and $R \subset R[x]$ is minimal, we get that $R[y] \subset R[x, y]$ is minimal by UCC. There is another diagram
where $R[x] \cap (R[y] \cap R[x + y]) = R$ and $R \subseteq R[x]$ is minimal. Using again UCC, we get that $R[y] \cap R[x + y] \subseteq R[x](R[y] \cap R[x + y])$ is minimal. But $R[x](R[y] \cap R[x + y]) = R[x]R[y] \cap R[x]R[x + y] = R[x,y]$ by distributivity, so that $R[y] \cap R[x + y] \subseteq R[x,y]$ is minimal. From $R[y] \cap R[x + y] \subseteq R[y] \subset R[x,y]$, we deduce $R[y] = R[y] \cap R[x + y]$, which implies $R[y] \subset R[x + y] \subseteq R[x,y]$ because $x \not\in R[y]$, and then $R[x + y] = R[x,y]$.

\textbf{Proposition 2.8.} Let $R \subseteq S$ be a distributive extension. Let $T \in [R,S]$ be a product of finitely many atoms. Then, $R \subseteq T$ is simple. More precisely, if $T = \prod_{i=1}^{n} R[x_{i}]$, where the $R \subseteq R[x_{i}]$ are minimal distinct extensions, then, $T = R[\sum_{i=1}^{n} x_{i}]$.

\textbf{Proof.} We prove the two statements by induction on $n$. There is nothing to prove when $n = 1$. Assume that the induction hypothesis holds for $n - 1$ and set $T' := \prod_{i=1}^{n-1} R[x_{i}] \neq R$, so that $T' = R[x]$ with $x := \sum_{i=1}^{n-1} x_{i}$. Then, $T = R[x]R[x_{n}]$, with $x \not\in R$ and $x_{n} \in S \setminus R[x]$. Deny. Then $R[x_{n}] \subseteq R[x] = T'$ would imply $T = T'$, a contradiction [33, Theorem 4.30] with the uniqueness of the product of atoms [33, Theorem 4.30]. Now, use Lemma 2.7 to get the result. \hfill \Box

\subsection{2.3. The lattice $[R,S]$ for an FCP or FIP extension.}

\textbf{Proposition 2.9.} [25, Proposition 1.4.4] If $R \subseteq S$ has FCP, then any $T \in [R,S]$ is a finite intersection (resp.; product) of $\cap$-irreducible (resp.; $\Pi$-irreducible) elements of $[R,S]$.

\textbf{Lemma 2.10.} Let $R \subseteq S$ be a distributive extension.

1. Assume that $T \in [R,S]$ has an irredundant representation $T = T_{1} \cdots T_{m}$ by $\Pi$-irreducible elements $T_{1}, \ldots, T_{m}$ of $[R,S]$. (resp.; $T = U_{1} \cap \cdots \cap U_{r}$ by $\cap$-irreducible elements $U_{1}, \ldots, U_{r}$ of $[R,S]$) (for example by atoms (resp.; co-atoms)). Then the representation is unique.

2. If in addition $R \subseteq S$ has FCP, then $[R,S]$ has exactly $n$ $\Pi$-irreducible (resp.; $\cap$-irreducible) elements if and only if $\ell([R,S] = n$. In particular, $R \subseteq S$ has FIP.

\textbf{Proof.} (1) By [16, Theorem 146], if an element of a distributive lattice has an irredundant representation by $\Pi$-irreducible elements, the representation is unique. The same holds with $\cap$-irreducible elements.
Then, \( UV \) over, \[16, \text{Theorem 148}\] gives that \( |UV| \) has exactly \( T \)

Write \( \{ \alpha | \alpha \in I \} \), \( \{ \alpha | \beta \in J \} \) and \( \{ \alpha | \gamma \in K \} \) of \( \mathcal{A} \).

Then, \( UV = \prod_{\beta \in J} A_{\alpha} \), so that \( T \cap UV = (\prod_{\alpha \in I} A_{\alpha}) \cap (\prod_{\beta \in J} A_{\beta}) \).

Write \( T \cap UV =: \prod_{\beta \in J} A_{\delta} = (\prod_{\alpha \in I} A_{\alpha}) \cap (\prod_{\beta \in J} A_{\beta}) \).

Then, for any \( \delta \in I \), we have \( A_{\delta} \subseteq T \) and \( A_{\delta} \subseteq \prod_{\beta \in J} A_{\beta} \), so that there exist some \( \alpha \in I \) such that \( A_{\delta} = A_{\alpha} \) and some \( \beta \in J \cup K \) such that \( A_{\delta} = A_{\beta} \). If \( \beta \in J \), then \( A_{\delta} \subseteq U \), so that \( A_{\delta} \subseteq T \cap U \subseteq (T \cap U)(T \cap V) \).

If \( \beta \in K \), then \( A_{\delta} \subseteq V \), so that \( A_{\delta} \subseteq T \cap V \subseteq (T \cap U)(T \cap V) \). In both cases, \( A_{\delta} \subseteq (T \cap U)(T \cap V) \), which yields \( T \cap UV \subseteq (T \cap U)(T \cap V) \), and then \( T \cap UV = (T \cap U)(T \cap V) \). Therefore, \( R \subset S \) is distributive. Moreover, \( R \subset S \) has FIP since \( \mathcal{A} \) is finite (\( S \) is the product of all elements of \( \mathcal{A} \)).

Now, let \( R \subset S \) be factorial, whence distributive. Set \( n := |\mathcal{A}| \), and for \( A_{\alpha} \in \mathcal{A} \), set \( B_{\alpha} := \prod_{\beta \neq \alpha} A_{\beta} \). Obviously, \( \mathcal{A} = \{ B_{\alpha} | \alpha \in \mathbb{N}_n \} \).

Let \( T \in [R,S] \), with \( T = \prod_{\alpha \in I} A_{\alpha} \). For \( J = \mathbb{N}_n \setminus I \), an easy calculation shows that \( T = \cap_{\beta \in J} B_{\beta} \) in a unique way. Hence, \( R \subset S \) is co-factorial.

To end, assume that \( R \subset S \) is co-factorial. We get that \( R \subset S \) is factorial and distributive, mimicking the previous proof. It is enough to exchange product and intersection, and atoms and co-atoms. In fact, we use the fact that \( R \subset S \) is co-atomistic. If these conditions hold, then \( R \subset S \) is a simple pair by Proposition 2.8.

The following notions and results are deeply involved in the sequel.

**Definition 2.12.** [7, Theorem 4.5] An extension \( R \subset S \) is called crucial if \( |\text{Supp}(S/R)| = 1 \). For such an extension, there is some unique \( M \in \text{Max}(R) \), called the crucial (maximal) ideal \( \mathcal{C}(R,S) \) of \( R \subset S \), such that \( RP = SP \) for each \( P \in \text{Spec}(R) \setminus \{M\} \). We will say that \( R \subset S \) is \( M \)-crucial.

**Theorem 2.13.** [17, Théorème 2.2] A minimal extension is crucial and is either integral (finite) or a flat epimorphism.
Lemma 2.14. [11, Corollary 3.2] If there exists a maximal chain $R = R_0 \subset \cdots \subset R_i \subset \cdots \subset R_n = S$ of extensions, where $R_i \subset R_{i+1}$ is minimal, then $\text{Supp}(S/R) = \{ \mathcal{C}(R_i, R_{i+1}) \cap R \mid i = 0, \ldots, n-1 \}$.

Lemma 2.15. [32, Lemma 1.8] Let $R \subset S$ be an FCP extension and $M \in \text{MSupp}(S/R)$. There is some $T \in [R, S]$ such that $R \subset T$ is minimal and $\mathcal{C}(R, T) = M$.

If $R \subseteq S$ has FCP, we set $\mathcal{T} := \{ T \in [R, S] \mid R \subset T \text{ crucial} \}$ and $\mathcal{T}_M := \{ T \in \mathcal{T} \mid R \subset T \text{ M-crucial} \}$. We are able to give dual results with $\mathcal{T}^* := \{ T \in [R, S] \mid |\text{MSupp}_R(S/T)| = 1 \}$, but they do not appear in this paper because they are not used in the sequel. The sets $\mathcal{T}_M$ give a partition of $\mathcal{T}$ associated to the equivalence relation $\mathcal{R}$ on $\mathcal{T}$, defined by $T \mathcal{R} T'$ if and only if $\text{Supp}(T/R) = \text{Supp}(T'/R)$. They play a significant role in factorizations properties in $[R, S]$.

Proposition 2.16. A subextension $R \subset T$ of an FCP extension $R \subset S$ is $M$-crucial when $T \in \mathcal{T}_M$ is such that $\text{Supp}(T/R) \subseteq \text{Max}(R)$. Moreover, $\mathcal{A}$ is the set of all minimal elements of $\mathcal{T}$.

In case $R \subset S$ has FIP, $\mathcal{T}_M$ has a greatest element $s(M) := \prod_{T \in \mathcal{T}_M} T$.

Proof. Let $T \in \mathcal{T}_M$ be such that $\text{Supp}(T/R) \subseteq \text{Max}(R)$. It follows that $\text{Supp}_R(T/R) = \text{MSupp}(T/R) = \{ M \}$ and $R_P = T_P$ for each $P \in \text{Spec}(R) \setminus \{ M \}$. Hence $R \subset T$ is $M$-crucial. If $U \in [R, S]$ is an atom, $R \subset U$ is minimal and $M := \mathcal{C}(R, U)$ with $\text{MSupp}(U/R) = \{ M \}$, whence $U \in \mathcal{T}$. Since $R \subset U$ is minimal, $U$ is a minimal element of $\mathcal{T}$. Conversely, let $U$ be a minimal element of $\mathcal{T}$. If $U$ is not an atom, there is $U' \in [R, S]$ with $R \subset U' \subset U$. Then, $\emptyset \neq \text{MSupp}(U'/R) \subseteq \text{MSupp}(U/R) = \{ M \}$ implies $\text{MSupp}(U'/R) = \{ M \}$ giving $U' \in \mathcal{T}$, contradicting the minimality of $U$ in $\mathcal{T}$. Therefore, $U$ is an atom.

Since $s(M) := \prod_{T \in \mathcal{T}_M} T$, we get that $T \subseteq s(M)$ for each $T \in \mathcal{T}_M$ and $R \subset s(M)$, whence $\text{MSupp}(s(M)/R) \neq \emptyset$. Since $R_P = T_P$ for each $T \in \mathcal{T}_M$ and $P \in \text{Spec}(R) \setminus \{ M \}$, we get $s(M)_P = R_P$, so that $\text{MSupp}(s(M)/R) = \{ M \}$ and $s(M)$ is the greatest element of $\mathcal{T}_M$. □

Lemma 2.17. Let $R \subset S$ be a ring extension and $T, T_1, \ldots, T_n \in [R, S]$ be such that $T = \prod_{i=1}^n T_i$. Then, $\text{Supp}(T/R) = \bigcup_{i=1}^n \text{Supp}(T_i/R)$.

Proof. Obvious, since $T_M = \prod_{i=1}^n (T_i)_M$ for any $M \in \text{Spec}(R)$. □

Proposition 2.18. Let $R \subset S$ be an FCP atomistic extension such that $|\mathcal{A}| < \infty$, with $\text{MSupp}(S/R) = \{ M_1, \ldots, M_n \}$. Set $\mathcal{A}_M = \mathcal{A} \cap \mathcal{T}_M$, $V_0 := R$, and, for each $k \in \mathbb{N}_n$, $V_k := \prod_{i=1}^k s(M_i)$.

Then, the following statements hold.

1. $R \subset S$ has FIP.
Proof. (1) Since $|\mathcal{A}| < \infty$ and any element of $[R, S]$ is a product of atoms, then $|[R, S]| < \infty$ and $R \subset S$ has FIP.

(2) Let $M \in \text{MSupp}(S/R)$. Any element of $\mathcal{T}_M$ is a product of atoms, which are necessarily in $V_s$ since $|\text{Supp}(M)| = \prod_{A \in \mathcal{A}} A$.

(3) Let $M_k \in \text{MSupp}(S/R)$ be such that $\text{Supp}(M_k) = \prod_{A \in \mathcal{A}} A$. Since $V_k = \prod_{i=1}^k s(M_i)$ and $V_{k-1} = \prod_{i=1}^{k-1} s(M_i)$, we have $(V_{k-1})M_j = (V_k)m_j = R_{M_j}$ if $j > k$, so that $M_j \notin \text{Supp}(V_k/V_{k-1})$. If $j = k > k-1$, then $(V_{k-1})M_k = R_{M_k}$ and $(V_k)m_k = s(M_k)m_k \neq R_{M_k}$, so that $M_k \notin \text{Supp}(V_k/V_{k-1})$. At last, if $j < k$, then $(V_{k-1})M_j = (V_k)m_j = s(M_j)m_j$, so that $M_j \notin \text{Supp}(V_k/V_{k-1})$. Hence, $\text{Supp}(V_k/V_{k-1}) = \{M_k\}$. If $k \in \{1, n\}$, the same reasoning holds. The end of (3) is obvious.

(4) If $T \in [R, S]$, then $T = \prod_{\alpha \in J} A_{\alpha}$, where $A_{\alpha} \in \mathcal{A}$ and $|J| \leq |\mathcal{A}|$, because $R \subset S$ is atomistic. There is some subset $I \subset \mathbb{N}_n$, such that $\text{Supp}(T/R) = \{M_i \mid i \in I\} = \text{MSupp}(T/R) = \bigcup_{\alpha \in J} \text{MSupp}(A_{\alpha}/R)$ by Lemma 2.17. Indeed, since $\text{Supp}(A_{\alpha}/R) \subseteq \text{Max}(R)$ for each $A_{\alpha}$, it follows that $\text{Supp}(T/R) \subseteq \text{Max}(R)$. For each $i \in I$, set $T_i = \prod[A_{\alpha} \mid A_{\alpha} \in \mathcal{T}_M]$. Then, $T_i \in \mathcal{T}_M$, and $T = \prod_{M_i \in \text{MSupp}(T/R)} T_i$.

(5) Since $R \subset A$ is minimal for any $A \in \mathcal{A}$, either $R \subset A$ is integral or $R \subset A$ is integrally closed. Moreover, by [32, Lemma 1.5], for a given $M \in \text{MSupp}(S/R)$, minimal extensions $R \subset A$, for $A \in \mathcal{T}_M$, are either all integral, or all integrally closed. Reorder $\text{MSupp}(S/R)$ such that for some $k \in \mathbb{N}_n$, $R \subset A$ is integrally closed for all $A \in \mathcal{T}_M$ and for any $i \leq k$ and $R \subset A$ is integral for all $A \in \mathcal{T}_M$ and for any $i > k$. Then, $R \subset V_k$ is Prüfer and $V_k \subset S$ is integral, so that $R \subset S$ is almost-Prüfer. Hence, $V_k$ is the Prüfer hull of $R \subset S$. $\square$

Proposition 2.19. Let $R \subset S$ be an FCP extension, such that $(\mathcal{T}, \subseteq)$ is a tree. Then,

1. The elements of $\mathcal{T}$ are $\Pi$-irreducible in $[R, S]$.
2. For each $M \in \text{MSupp}(S/R)$, $\mathcal{T}_M$ is a chain, whose least element $i(M)$ is the only $T \in [R, S]$ satisfying $R \subset T$ is minimal and $M = \mathcal{C}(R, T)$.
3. Let $M \in \text{MSupp}(S/R)$. For each $T \in [R, S]$ such that $M \in \text{MSupp}(T/R)$, we have $i(M) \subseteq T$. 

BOOLEAN FIP 9
Proof. (1) Let \( T \in \mathcal{T} \) and \( M \in \text{MSupp}(S/R) \) such that \( \text{MSupp}(T/R) = \{ M \} \). It follows that \( R_M \neq T_M \) and \( R_{M'} = T_{M'} \) for each \( M' \in \text{Max}(R) \setminus \{ M \} \). Let \( T_1, T_2 \in [R, S] \) be such that \( T = T_1 T_2 \). Then we have \( R \subseteq T_i \subseteq T \) for \( i \in \mathbb{N}_2 \), giving \( (T_i)_M' = R_{M'} = T_{M'} \) for each \( M' \in \text{Max}(R) \setminus \{ M \} \), and \( R_M \subseteq (T_i)_M \subseteq T_M \) for \( i \in \mathbb{N}_2 \), giving, for each \( i \in \mathbb{N}_2 \), either \( R = T_i \) (a), or \( \text{MSupp}(T_i/R) = \{ M \} \) (b). Fix \( i \) and let \( j \in \mathbb{N}_2 \setminus \{ i \} \). Case (a) gives \( T = T_j \). Case (b) gives that \( T_i \in \mathcal{T} \). In this case, either \( T_j = R \), giving \( T = T_i \), or \( T_j \in \mathcal{T} \). Hence \( T_i \) and \( T_j \) are comparable, because \( \mathcal{T} \) is a tree. Therefore, \( T \) is equal to the greatest element of \( \{ T_1, T_2 \} \) and \( T \) is II-irreducible.

(2) Let \( M \in \text{MSupp}(S/R) \) and \( T_1, T_2 \in \mathcal{T}_M \). Set \( U := T_1 T_2 \), so that \( T_i \subseteq U \) for \( i \in \mathbb{N}_2 \) and then \( (T_i)_M' = R_{M'} = U_{M'} \) for each \( M' \in \text{Max}(R) \setminus \{ M \} \), and \( R_M \subseteq (T_i)_M \subseteq U_M \). Then, \( \text{MSupp}(U/R) = \{ M \} \). Therefore, \( U \in \mathcal{T} \), so that \( T_1 \) and \( T_2 \) are comparable and \( \mathcal{T}_M \) is a chain.

By Lemma 2.15, there is \( T \in [R, S] \) such that \( R \subset T \) is minimal with \( M = \mathcal{C}(R, T) \). Obviously, we have \( \text{MSupp}(T/R) = \{ M \} \), so that \( T \in \mathcal{T}_M \). Since \( \mathcal{T}_M \) is a chain, \( T \) is the least element of \( \mathcal{T}_M \), because any \( U \in \mathcal{T}_M \) is comparable to \( T \), and we cannot have \( U \subset T \). Moreover, since any \( T' \in [R, S] \) such that \( R \subset T' \) is minimal with \( M = \mathcal{C}(R, T') \) satisfies \( T' \in \mathcal{T}_M \), we have just proved that there is only one \( T' \in [R, S] \) such that \( R \subset T' \) is minimal with \( M = \mathcal{C}(R, T') \). We set \( i(M) := T' \).

(3) Let \( T \in [R, S] \) with \( M \in \text{MSupp}(T/R) \). For each \( M' \in \text{Max}(R) \setminus \{ M \} \), we have \( R_{M'} = i(M)_{M'} \subseteq T_{M'} \) and a maximal chain \( R = R_0 \subset \cdots \subset R_i \subset \cdots \subset R_n = T \), where \( R_{i-1} \subset R_i \) is minimal for each \( i \in \mathbb{N}_n \). Since \( M \in \text{MSupp}(T/R) \), there is some \( i \in \mathbb{N}_n \) such that \( M = \mathcal{C}(R_{i-1}, R_i) \cap R \), by Lemma 2.14. Let \( k \in \mathbb{N}_n \) be the least \( i \) satisfying this property. Assume \( k \neq 1 \), so that \( M \notin \text{MSupp}(R_{k-1}/R) \). Again by Lemma 2.15, there is \( R_{k}' \in [R, R_k] \) such that \( R \subset R_{k}' \) is minimal with \( M = \mathcal{C}(R, R_{k}') \). From (2), we deduce that \( R_{k}' = i(M) \), so that \( i(M) \subseteq T \). If \( k = 1 \), then \( R_{k-1} = R \) and \( R_k = i(M) \subseteq T \). \( \square \)

We will see in Proposition 2.22, that, under some conditions, for an FCP extension \( R \subset S \), any element of \( [R, S] \) can be written in a unique way, as a product of elements of \( \mathcal{T} \). But Remark 2.25 shows that this property does not always hold.

Now, we look at some properties of arithmetic FCP extensions.

**Theorem 2.20.** Let \( R \subset S \) be an arithmetic FCP extension. Then,

1. \( R \subset S \) has FIP and \( ||[R, S]|| \leq \prod_{M \in \text{MSupp}(S/R)} (1 + \ell[R_M, S_M]) \).
2. \( \mathcal{T}_M \) is a chain for each \( M \in \text{MSupp}(S/R) \) and \( (\mathcal{T}, \subseteq) \) is treed.
Proof. Since $R \subset S$ is an FCP extension, we have $|\text{MSupp}(S/R)| \leq \infty$ by [11, Corollary 3.2]. Clearly, $R_M \subset S_M$ has FCP for each $M \in \text{MSupp}(S/R)$ ([11, Proposition 3.7(a)]).

(1) Therefore, $|\{R_M, S_M\}| < \infty$ follows, since $[R_M, S_M]$ is a finite chain and $R_M \subset S_M$ has FIP for each $M \in \text{MSupp}(S/R)$. Hence, $R \subset S$ has FIP [11, Proposition 3.7(b)]. By [11, Theorem 3.6 (a)], we have $|[R, S]| \leq \prod_{M \in \text{MSupp}(S/R)} |[R_M, S_M]|$ because the map $\varphi : [R, S] \to \prod_{M \in \text{MSupp}(S/R)} [R_M, S_M]$ defined by $\varphi(T) := (T_M)_{M \in \text{MSupp}(S/R)}$ is injective. But $|[R_M, S_M]| = 1 + \ell[R_M, S_M]$ holds since $[R_M, S_M]$ is a chain, giving the requested inequality.

(2) Let $T_1, T_2 \in \mathcal{T}_M$, so that $\{M\} = \text{MSupp}(T_i/R)$ for $i \in \mathbb{N}_2$. Then, $(T_1)_{M'} = (T_2)_{M'} = R_{M'}$ for each $M' \in \text{MSupp}(S/R) \setminus \{M\}$. Moreover, $(T_1)_{M} \in [R_M, S_M]$ for $i \in \mathbb{N}_2$, so that $(T_1)_M$ and $(T_2)_M$ are comparable since $[R_M, S_M]$ is a chain, and so are $T_1$ and $T_2$. Then, $\mathcal{T}_M$ is a chain.

Let $T_1, T_2, T \in \mathcal{T}$ be such that $T_i \subseteq T$ for $i \in \mathbb{N}_2$ and $M \in \text{MSupp}(S/R)$ such that $\text{MSupp}(T/R) = \{M\}$ since $|\text{MSupp}(T/R)| = 1$. Moreover, for $i = 1, 2$, we have $|\text{MSupp}(T_i/R)| = 1$ since $T_i \in \mathcal{T}$, which implies that $R \subset T_i \subset T$. Then, we get, for $i \in \mathbb{N}_2$, that $\emptyset \neq \text{MSupp}(T_i/R) \subseteq \text{MSupp}(T/R) = \{M\}$, so that $\text{MSupp}(T_i/R) = \{M\}$. It follows that $T_1, T_2 \in \mathcal{T}_M$, which is a chain, and then $T_1$ and $T_2$ are comparable as we have just seen. Therefore, $\mathcal{T}$ is a tree. \hfill \Box

Let $R \subset S$ be an FCP extension and $\text{MSupp}(S/R) := \{M_1, \ldots, M_n\}$. We will use the maps $\varphi : [R, S] \to \prod_{i=1}^{n} [R_{M_i}, S_{M_i}]$ defined in [11, Theorem 3.6] by $\varphi(T) := (T_{M_i}, \ldots, T_{M_n})$ and $\varphi_M : [R, S] \to [R_M, S_M]$ defined by $\varphi_M(T) := T_M$, for each $M \in \text{MSupp}(S/R)$. Then $\varphi$ is injective. If $\varphi$ is bijective, $R \subset S$ is called a $\mathcal{B}$-extension ($\mathcal{B}$ stands for bijective).

Proposition 2.21. An FCP extension $R \subset S$ is a $\mathcal{B}$-extension if and only if $R/P$ is local for each $P \in \text{Supp}(S/R)$.

The above “local” condition on the factor domains $R/P$ holds in case $\text{Supp}(S/R) \subseteq \text{Max}(R)$, and, in particular, if $R \subset S$ is integral.

Proof. One implication appears in the proof of [11, Theorem 3.6(b)] which uses [11, Lemma 3.5].

Conversely, assume that $\varphi$ is bijective and that there is some $P \in \text{Supp}(S/R)$ contained in two elements $M_1, M_2 \in \text{Max}(R)$. Consider a maximal chain $\mathcal{C} : R = R_0 \subset \cdots \subset R_i \subset \cdots \subset R_n = S$, where $R_{i-1} \subset R_i$ is minimal for each $i \in \mathbb{N}_n$. Since $P \in \text{Supp}(S/R)$, there exists some $i \in \mathbb{N}_n$ such that $P = N \cap R$, where $N := \mathcal{C}(R_{i-1}, R_i)$ by Lemma 2.14. In particular, $P \in \text{Supp}(R_i/R)$, which implies that $M_j \in \text{Supp}(R_i/R)$ for $j \in \mathbb{N}_2$. Since $\varphi$ is surjective, there is $T \in [R, S]$ such
that $T_{M_1} = (R_i)_{M_1}$ and $T_M = R_M$ for each $M \in \text{MSupp}(S/R) \setminus \{M_1\}$. In particular, $M_2 \notin \text{Supp}(T/R)$. Localizing $E$ at $M_1$, we get that $P_{M_1} \in \text{Supp}((R_i)_{M_1}/R_{M_1}) = \text{Supp}(T_{M_1}/R_{M_1})$ so that $P \in \text{Supp}(T/R)$, Now $M_2 \in \text{Supp}(T/R)$ is absurd. Then, $R/P$ is a local ring for each $P \in \text{Supp}(S/R)$.

If $\text{Supp}(S/R) \subseteq \text{Max}(R)$, it follows from Lemma 2.14 that each $E(R_{i-1}, R_i)$ lies over a maximal ideal of $R$ (and so $R/P$ is a field, hence local for each $P \in \text{Supp}(S/R)$). Finally, it is standard that maximal ideals lie over maximal ideals in any integral extension (cf. [22, Theorem 44]).

Under an additional assumption, next proposition gives a converse to Theorem 2.20. Set $\text{MSupp}(S/R) := \{M_1, \ldots, M_n\}$ for an FCP extension $R \subset S$. It follows that the elements of $\text{MSupp}(T/R)$ are some $M_i$ when $T \in ]R, S]$.

**Proposition 2.22.** Let $R \subset S$ be an FCP $B$-extension.

1. For each $M \in \text{MSupp}(S/R)$, we have $[R_M, S_M] = \varphi_M(T) \cup \{R_M\} = \varphi_M(T_M) \cup \{R_M\}$.
2. Any $T \in ]R, S]$ is a product of $|\text{MSupp}(T/R)|$ distinct elements $E_i \in T$ in a unique way such that $E_i \in T_M$, for each $M_i \in \text{MSupp}(T/R)$.
3. $R \subset S$ is arithmetic if and only if $T$ is a tree.
4. Assume that $R \subset S$ is arithmetic. Then, $T$ is the set of $\Pi$-irreducible elements of $]R, S]$. Moreover, $|[R, S]| = \prod_{M \in \text{MSupp}(S/R)} (1 + \ell[R_M, S_M])$.

**Proof.** (1) The following inclusions are obvious: $\varphi_M(T_M) \cup \{R_M\} \subseteq \varphi_M(T) \cup \{R_M\} \subseteq [R_M, S_M]$. Let $E \in ]R_M, S_M]$. Since $\varphi$ is a bijection, there exists $T \subseteq ]R, S]$ such that $T_M = E$ and $T_{M'} = R_{M'}$ for each $M' \in \text{MSupp}(S/R) \setminus \{M\}$. The result follows from $E = \varphi_M(T)$ and $T \in T_M$.

2. Let $T \in ]R, S]$. From $\text{MSupp}(T/R) \neq \emptyset$, we infer that some $M_i \in \text{MSupp}(T/R)$. Since $\varphi$ is a bijection, there exists a unique $E_i \in [R, S]$ such that $(E_i)_{M_i} = T_{M_i}$ and $(E_i)_{M} = R_{M}$ for $M \neq M_i$. It follows that $E_i \in T_M$, for each $M_i \in \text{MSupp}(T/R)$. Set $E_j = R$ when $M_j \notin \text{MSupp}(T/R)$ and $E := E_1 \cdots E_n$. For each $j \in \mathbb{N}_n$, we get that $E_{M_j} = T_{M_j}$, so that $E = T$ is the product of $|\text{MSupp}(T/R)|$ distinct elements of $T$. The uniqueness of these elements is obvious.

3. One implication is Theorem 2.20. Assume that $T$ is a tree. Let $M \in \text{MSupp}(S/R)$. By Proposition 2.19, $T_M$ is a chain. Since $\varphi_M$ preserves order, (1) implies that $[R_M, S_M]$ is a chain.
(4) Assume that \( R \subset S \) is arithmetic. Then, \( \mathcal{T} \) is a tree. It results from Proposition 2.19 that the elements of \( \mathcal{T} \) are \( \cap \)-irreducible. Conversely, let \( T \subseteq [R,S] \) be \( \cap \)-irreducible. In view of (2), \( T \) is a product of elements \( E_i \in \mathcal{T}_{M_i} \), where \( M_i \in \text{MSupp}(T/R) \), and then, of only one element of \( \mathcal{T} \), so that \( T \in \mathcal{T} \).

Now \( \prod_{M \in \text{MSupp}(S/R)} |[R_M, S_M]| = \prod_{M \in \text{MSupp}(S/R)} (1 + \ell[R_M, S_M]) = \prod_{\ell[M, S]} \), since \( \varphi \) is bijective and each \( R_M \subset S_M \) a chain. \( \square \)

For the definition of the Goldie dimension of a distributive lattice, the reader may look at [25, p. 14 and Exercise 8, p. 33]. We will use the following results.

**Proposition 2.23.** [25, Theorem 1.5.9] If \( R \subseteq S \) is an FCP arithmetic extension, its Goldie dimension is the integer \( n \) such that \( R = B_1 \cap \cdots \cap B_n \) is an irredundant representation of \( R \) by \( \cap \)-irreducible elements.

**Proposition 2.24.** Let \( R \subset S \) be an FCP arithmetic \( \mathcal{B} \)-extension. Then, the Goldie dimension of \( [R, S] \) is \( n := |\text{MSupp}(S/R)| \).

**Proof.** For each \( M_i \in \text{MSupp}(S/R) \) there exists a unique \( E_i' \in [R, S] \) such that \((E_i')_M = R_M \) and \((E_i')_M = S_M \) for \( M \neq M_i \). Set \( E' := E_1' \cap \ldots \cap E_n' \). For each \( i \), we get that \( E'_{M_i} = R_{M_i} \), so that \( E' = R \) is the intersection of \( |\text{MSupp}(S/T)| \) distinct elements of \( [R, S] \). The uniqueness of these elements is obvious.

We claim that the \( E_i' \) are \( \cap \)-irreducible. Let \( T, T' \in [R, S] \) be such that \( E_i' = T \cap T' \). Then we have \( R \subseteq E_i' \subseteq T, T' \), giving \((E_i')_M = S_M = T_M = T_i' \) for each \( M \in \text{Max}(R) \setminus \{M_i\} \), and \( R_{M_i} = (E_i')_{M_i} \subseteq T_{M_i} = T_i' \). Since \( R \subset S \) is arithmetic, \( T_{M_i} \) and \( T_i' \) are comparable, and so are \( T \) and \( T' \) by (\(*\)). It follows that \( E_i' \) is the least element of \( \{T, T'\} \), and then is \( \cap \)-irreducible so that \( n \) is the Goldie dimension of \([R, S]\) by Proposition 2.23. \( \square \)

**Remark 2.25.** Using [11, Remark 3.4(b)], we exhibit a non-\( \mathcal{B} \)-extension, for which some statements of Proposition 2.22 do not hold.

We now summarize the context of the above quoted remark.

Let \( R \) be a two-dimensional Prüfer domain with exactly two height-2 maximal ideals, \( N \) and \( N' \), each of which contains the unique height 1 prime ideal \( P \) of \( R \). Set \( R_0 := R, R_1 := R_N, R_1' := R_{N'}, R_2 := R_P \) and \( R_3 := K \), the quotient field of \( R \). Since each overring of a Prüfer domain is an intersection of localizations [19, Theorem 26.2], it is easy to check that \( R_0 \subseteq R_1, R_0 \subseteq R_1', R_1 \subseteq R_2, R_1' \subseteq R_2 \) and \( R_2 \subseteq R_3 \) are Prüfer minimal extensions.

Moreover, \( \mathcal{C}(R_0, R_1) = N', \mathcal{C}(R_1, R_2) = NR_N \) and \( \mathcal{C}(R_2, R_3) = P \), which is an ideal of \( R_2 \) because \( P = (R_0 : R_2) \). It follows that
Supp($K/R$) = \{P, N, N'\} and MSupp($K/R$) = \{N, N'\}. By Proposition 2.21, the map $\varphi$ is not bijective, since $R/P$ is not local. The poset $\mathcal{T} = \{R_1, R'_1\}$ is a tree. Moreover, $[R_N, K_N] = \{R_N, R_P, K\} = \{R_1, R_2, R_3\}$ and $[R_{N'}, K_{N'}] = \{R_{N'}, R_P, K\} = \{R'_1, R_2, R_3\}$ are chains. However, $\varphi_N(\mathcal{T}) = \{R_1, R_2\}$, because $(R_{N'})_N = R_P$. Then, Proposition 2.22(1) is not satisfied. In the same way, Proposition 2.22(2) is not satisfied, because $K$ is not a product of elements of $\mathcal{T}$. In particular, some $\Pi$-irreducible element as $R_3 = K$ of $[R, S]$ is not in $\mathcal{T}$.

The conditions of Proposition 2.22 hold in the following context and provide us a structure of Boolean lattices in Proposition 3.15.

**Proposition 2.26.** Let $R \subset S$ be an FCP extension. Assume that Supp($T/R$) ∩ Supp($S/T$) = $\emptyset$ for all $T \in [R, S]$. Then:

1. Supp($S/R$) ⊆ Max($R$) and $R \subset S$ is a $\mathcal{B}$-extension.
2. $\mathcal{T}$ is an antichain.

**Proof.** (1) Assume that Supp($T/R$) ∩ Supp($S/T$) = $\emptyset$ for all $T \in [R, S]$. We use Proposition 2.21 to show that $\varphi$ is a bijection. Let $P \in$ Supp($S/R$). Consider a maximal chain $\mathcal{C} : R = R_0 \subset \cdots \subset R_i \subset \cdots \subset R_n = S$, where $R_{i-1} \subset R_i$ is minimal for each $i \in \mathbb{N}_n$. Since $P \in$ Supp($S/R$), there exists some $k \in \mathbb{N}_n$ such that $P = N \cap R$, where $N := \mathcal{C}(R_{k-1}, R_k)$, in view of Lemma 2.14. In particular, $P \in$ Supp($R_k/R_k$), and, more precisely, $P \in$ Supp($R_k/R_{k-1}$) ⊆ Supp($S/R_{k-1}$). Assume that $P$ is not a maximal ideal, and let $M \in$ Max($R$) be such that $P \subset M$. Then, $M \in$ Supp($R_k/R_k$) ∩ Supp($S/R_{k-1}$). Moreover, there is some $j < k$ such that $M = N' \cap R$, where $N' := \mathcal{C}(R_{j-1}, R_j)$. Indeed, $j \neq k$ because $N \cap R = P \neq M$. Therefore $M \in$ Supp($R_j/R_j$) ⊆ Supp($R_{k-1}/R$), since $j \leq k-1$ and $M \in$ Supp($R_{k-1}/R$) ∩ Supp($S/R_{k-1}$) is absurd. Hence, Supp($S/R$) ⊆ Max($R$), and $\varphi$ is a bijection by Proposition 2.21.

(2) Let $T, T' \in \mathcal{T}$ be such that $T' \subset T$ and $M \in$ Max($R$) such that Supp($T/R$) = $\{M\}$. Since $T' \subset T$, we get that Supp($T'/R$) ⊆ Supp($T/R$), giving Supp($T'/R$) = $\{M\}$. But, $\emptyset \neq$ Supp($T/T'$) ⊆ Supp($T/R$) = $\{M\}$ implies that $\{M\} =$ Supp($T/T'$) ⊆ Supp($S/T'$). Therefore, $M \in$ Supp($T'/R$) ∩ Supp($S/T'$) = $\emptyset$, a contradiction. Then, two distinct elements of $\mathcal{T}$ are incomparable, and $\mathcal{T}$ is an antichain. \qed

Let $R \subset S$ be an FCP extension. In the following, we will meet the condition that Supp($T/R$) ∩ Supp($S/T$) = $\emptyset$ for some $T \in [R, S]$. Here is a theorem which gives a stronger result.

**Theorem 2.27.** If $R \subset S$ has FCP, then Supp($T/R$) ∩ Supp($S/T$) = $\emptyset$ for all $T \in [R, S]$ if and only if $R \subset S$ is locally minimal. In this case, $R \subset S$ is an FIP factorial extension.
Proof. Assume that \( \text{Supp}(T/R) \cap \text{Supp}(S/T) = \emptyset \) for all \( T \in [R, S] \). By Propositions 2.26 and 2.22, \( R \subseteq S \) is arithmetic because an antichain is treed. Let \( T \in [R, S] \), there is \( U \in [R, S] \) such that \( U \cap T = R \) and \( UT = S \) [29, Lemma 3.7], which gives \( U_M \cap T_M = R_M \) and \( U_M T_M = S_M \) for each \( M \in \text{MSupp}(S/R) \), so that \( \{U_M, T_M\} = \{R_M, S_M\} \), whence, \( R_M \subseteq S_M \) is minimal.

Conversely, if there exists some \( N \in \text{MSupp}(T/R) \cap \text{MSupp}(S/T) \) for some \( T \in [R, S] \), we get that \( T_N \neq R_N, S_N \), so that \( |[R_N, S_N]| \geq 2 \). But \( R_N \subseteq S_N \) is minimal, a contradiction.

If these conditions hold, then \( R \subseteq S \) has FIP by Theorem 2.20, and is factorial by Propositions 2.26, 2.22 and 2.16. Indeed, \( R \subseteq S \) is a \( \mathcal{B} \)-extension such that \( \mathcal{T} \) is an antichain, so that \( \mathcal{T} = \mathcal{A} \) and any element of \([R, S]\) is a product of atoms in a unique way. \( \square \)

3. Boolean FCP extensions

3.1. General properties of Boolean extensions. Let \( R \subseteq S \) be an extension and \( T \in [R, S] \). Then, \( T' \in [R, S] \) is called a complement of \( T \) if \( T \cap T' = R \) and \( TT' = S \). If \( R \subseteq S \) is distributive, then \( T \) has at most one complement [25, Exercise 9, page 33]. We denote this complement by \( T^o \) when it exists.

We recall that \( R \subseteq S \) is Boolean if and only if \( R \subseteq S \) is distributive and each \( T \in [R, S] \) has a (unique) complement \( T^o \) [33, Definition page 129]. In a Boolean FIP extension \( R \subseteq S \), any \( T \in [R, S] \) is, in a unique way, a product of finitely many atoms and the intersection of finitely many co-atoms. To see this, use Lemma 2.10, Proposition 2.9, [33, Theorems 5.1 and 6.3], and the fact that \([R, S]\) is a complete Boolean lattice. Indeed, the \( \Pi \)-irreducible (resp. \( \cap \)-irreducible) elements are the atoms (resp. co-atoms). In particular, if \( A \) is an atom, then \( A^o \) is a co-atom [33, Theorem 3.43]. Next Theorem characterizes Boolean FCP extensions amid distributive FCP extensions. Before, we translate in the context of ring extensions the equivalences of [34, page 392] that characterize a Boolean lattice, a result often used in the following.

Proposition 3.1. Let \( R \subseteq S \) be an FIP distributive extension. Then, the following conditions are equivalent:

1. \( R \subseteq S \) is a Boolean extension;
2. \( S \) is the product of atoms of \([R, S]\);
3. Any \( \Pi \)-irreducible element is an atom;
4. If \( \ell([R, S]) = n \), then \( |[R, S]| = 2^n \);
5. If \([R, S]\) has \( n \) \( \Pi \)-irreducible elements, then \( |[R, S]| = 2^n \).

Theorem 3.2. Let \( R \subseteq S \) be an FCP distributive extension and set \( n := \ell([R, S]) \). Then, the following conditions are equivalent:
(1) $R \subseteq S$ is a Boolean extension;
(2) $n = |\mathcal{A}|$, where $\mathcal{A}$ is the set of atoms of $[R, S]$;
(3) $|[R, S]| = 2^n$.

If these conditions hold, then $R \subseteq S$ is FIP factorial and a simple pair. Moreover, for each $T, U \in [R, S]$ with $T \subseteq U$, all maximal chains of $[T, U]$ have the same length.

Proof. To begin with, $R \subseteq S$ has FIP by Lemma 2.10. Moreover, $[R, S]$ has exactly $n$ $\Pi$-irreducible element by Lemma 2.10. Since any atom is $\Pi$-irreducible, the equivalences of (1), (2) and (3) are gotten by the equivalences of Proposition 3.1.

If these conditions hold, then $R \subseteq S$ is factorial and a simple pair by Theorem 2.11. Since a Boolean lattice is a distributive lattice, the last results comes from Proposition 2.5. □

Example 3.3. (1) An extension $R \subseteq S$ is Boolean and chained if and only if it is minimal. One implication is obvious. Conversely, assume that $[R, S]$ is chained and a Boolean lattice. If there is some $T \in [R, S]$, it has a complement $T'$. Then, $T \cap T' = R$ and $TT' = S$ implies $\{T, T'\} = \{R, S\}$ since $T$ and $T'$ are comparable, a contradiction.

(2) Let $R \subseteq S$ be a Boolean FCP extension and $x \in S \setminus R$. We intend to compute $R[x]^\circ$. Let $\mathcal{A} := \{B_1, \ldots, B_n\}$. Then $R[x] = \cap [B_\alpha \in Y]$ for a unique family $Y := \{B_\alpha\}$ of co-atoms ([33, Theorem 6.3]), so that $x \in B_\alpha$ for each $B_\alpha \in Y$. Let $B_\beta \in \mathcal{A}$ which does not contain $x$. Then $R[x] \not\subseteq B_\beta$ and $Y$ is the set of co-atoms containing $x$. Now, $(R[x])^\circ = (\cap [B_\alpha \in Y])^\circ = \Pi[(B_\alpha)^\circ \cap B_\alpha \in Y]$, where the $(B_\alpha)^\circ$ are atoms. Then, $(R[x])^\circ$ is the product of atoms which are complements of the co-atoms containing $x$. But we also have $(R[x])^\circ = \cap [B_\beta \in \mathcal{A} \setminus Y]$. Indeed, set $T := \cap [B_\beta \in \mathcal{A} \setminus Y]$. Obviously, $R[x] \cap T = R$ and assume that $R[x]T \neq S$, so that $R[x]T = \cap [B_\gamma \in X]$ for some $X \subseteq \mathcal{A}$. Let $B_\gamma \in X$. Then, $R[x] = \cap [B_\alpha \in Y] \subseteq B_\gamma$ implies $B_\alpha = B_\gamma$ for some $B_\alpha \in Y$. In the same way, $B_\beta = B_\gamma$ for some $B_\beta \in \mathcal{A} \setminus Y$, a contradiction. Then, $R[x]T = S$ and $T = (R[x])^\circ$.

(3) By Theorem 3.2, an FCP Boolean extension $R \subseteq S$ verifies $|[R, S]| = 2^n$, where $n = \ell[R, S]$. But an extension $R \subseteq S$ may be distributive with $|[R, S]| = 2^n$ for some integer $n$ without being Boolean. It is enough to consider a chained extension of length $2^n - 1$.

The following lemma is needed for the next proposition. See the close notion of patching due to Dobbs-Shapiro [15].

Lemma 3.4. Let $R \subseteq S$ be an FCP extension and $M \in MSupp(S/R)$. For any $T' \in [R_M, S_M]$ such that $R_M \subseteq T'$ is minimal, there exists $T \in [R, S]$ such that $R \subseteq T$ is minimal with $T_M = T'$. 

Proof. Let $\varphi : S \to S_M$ be the canonical ring morphism and set $T'' := \varphi^{-1}(T')$. Then $T'' \in [R, S]$ is such that $T' = T'' - M$, so that $M \in MSupp(T''/R)$. From Lemma 2.15 we deduce the existence of some $T \in [R, T''] \subseteq [R, S]$ such that $R \subseteq T$ is minimal with $M = \mathfrak{C}(R, T)$. Hence, $R_M \subseteq T_M \subseteq T''_M = T'$. \hfill \Box

Proposition 3.5. Let $R \subseteq S$ be an FCP extension. The following statements are equivalent:

1. $R \subseteq S$ is Boolean;
2. $R_M \subseteq S_M$ is Boolean for each $M \in MSupp(S/R)$;
3. $R_P \subseteq S_P$ is Boolean for each $P \in Supp(S/R)$;
4. $R/I \subseteq S/I$ is Boolean for each ideal $I$ shared by $R$ and $S$;
5. $R/I \subseteq S/I$ is Boolean for some ideal $I$ shared by $R$ and $S$.

Proof. We have obviously $(1) \Rightarrow (3) \Rightarrow (2)$. Conversely, assume that $R_M \subseteq S_M$ is Boolean, and then distributive, for each $M \in MSupp(S/R)$. Then $R \subseteq S$ is distributive by Proposition 2.4. It remains to show that any $T \in [R, S]$ has a complement. Let $M \in MSupp(S/R)$. Then, $T_M$ has a complement $(T_M)^\circ$ in $[R_M, S_M]$ satisfying $T_M \cap (T_M)^\circ = R_M$ (*), and $T_M(T_M)^\circ = S_M$ (**). Since $[R_M, S_M]$ is Boolean, any of its elements is a product of its atoms [33, Theorem 5.2]. Then, $(T_M)^\circ = \prod_{i \in I_M} R'_i,M_i$.

By Lemma 3.4, for each atom $R'_i,M_i \in [R_M, S_M]$, there is $R_i,M \in [R, S]$ such that $R \subseteq R_i,M$ is minimal, with $R'_i,M = (R_i,M)_M$. In particular, $(R_i,M)_{M'} = R'_i,M'$ for each $M' \in MSupp(S/R) \setminus \{M\}$. Setting $T' := \prod_{M \in MSupp(S/R)} (\prod_{i \in I_M} R_i,M)$, we get, for each $M \in MSupp(S/R)$ that $T'_M = \prod_{i \in I_M} R'_i,M = (T_M)^\circ$, so that (*) and (**) give $T_M \cap T'_M = R_M$ and $T_M T'_M = S_M$, and, to end, $T \cap T' = R$ and $TT' = S$, showing that $T'$ is the complement of $T$. Therefore, $R \subseteq S$ is Boolean.

For the equivalences of (1), (4) and (5), and for an ideal $I$ shared by $R$ and $S$, use the lattice isomorphism $\varphi : [R, S] \to [R/I, S/I]$ defined by $T \mapsto T/I$ in the proof of Proposition 2.4. For $T, T' \in [R, S]$, we see easily that $T'$ is a complement of $T$ in $[R, S]$ if and only if $T'/I$ is a complement of $T/I$ in $[R/I, S/I]$. \hfill \Box

Corollary 3.6. Let $R \subseteq S$ be an FIP extension. The following statements are equivalent:

1. $R \subseteq S$ is atomistic and arithmetic;
2. $R \subseteq S$ is Boolean and arithmetic;
3. $R \subseteq S$ is locally minimal.

Assume that these conditions hold and let $A = \{A_1, \ldots, A_a\}$ be the set of atoms of $[R, S]$ where $a$ is some integer. Then, the complement of
any \( T = \prod_{i \in I} A_i \in [R, S] \), where \( I \subseteq \mathbb{N}_a \), is \( T^\circ := \prod_{j \in J} A_j \), where \( J := \mathbb{N}_a \setminus I \). If in addition \( R \subset S \) is integral, then \( \ell[R, S] = |\text{MSupp}(S/R)| \).

**Proof.** Since an arithmetic extension is distributive by Proposition 2.3, we get (1) \( \Rightarrow \) (2) by Proposition 3.1 and (2) \( \Rightarrow \) (1) by Theorem 3.2 because \( R \subset S \) is factorial. Moreover, a locally minimal extension is distributive. Then, (2) \( \Leftrightarrow \) (3) holds by Proposition 3.5 and Example 3.3(1).

Assume that these equivalent conditions hold. We observe that \( S \) is the product of all atoms. Let \( T = \prod_{i \in I} A_i \in [R, S] \), where \( I \subseteq \mathbb{N}_a \). Since \( T^\circ \) is a product of atoms, the relations \( T \cap T^\circ = R \) and \( TT^\circ = S \) give \( T^\circ := \prod_{j \in J} A_j \), where \( J := \mathbb{N}_a \setminus I \).

In case \( R \subset S \) is integral, we use \( \ell[R, S] = \sum_{M \in \text{MSupp}(S/R)} \ell[R_M, S_M] \). \( \Box \)

The next proposition uses the notation of [4, Proposition 10, p.52].

**Proposition 3.7.** Let \( R \subset S \) be a ring extension, \( f : R \rightarrow R' \) a faithfully flat ring morphism and \( S' := R' \otimes_R S \). Assume that \( R' \subset S' \) is distributive. Then,

1. \( R \subset S \) is distributive.
2. Let \( T \in [R, S] \) be such that \( R'T \) is \( \Pi \)-irreducible (resp. an atom) in \( [R', S'] \). Then, \( T \) is \( \Pi \)-irreducible (resp. an atom) in \( [R, S] \).
3. In case \( R'T \) is \( \Pi \)-irreducible for any \( \Pi \)-irreducible \( T \in [R, S] \) and \( R' \subset S' \) is an FIP Boolean extension, so is \( R \subset S \).

**Proof.** (1) The ring morphism \( \varphi : S \rightarrow S' \) defines a map \( \theta : [R', S'] \rightarrow [R, S] \) while there is a map \( \psi : [R, S] \rightarrow [R', S'] \), defined by \( \psi(T) = R' \otimes_R T \) and such that \( \theta \circ \psi \) is the identity of \( [R, S] \) by [4, Proposition 10, p.52] (it is enough to take \( F = S \) and to observe that if \( M \) is an \( R \)-submodule of \( S \), then with the notation of the above reference, \( R'M \) identifies to \( M \otimes_R R' \)). In particular, \( \psi \) is injective. The same reference shows that \( \psi(T \cap U) = \psi(T) \cap \psi(U) \) for \( U, T \in [R, S] \). It is easy to show that \( \psi(TU) = \psi(T)\psi(U) \). If \( R' \subset S' \) is distributive, it follows that for \( T, U, V \in [R, S] \), we get \( \psi[T(U \cap V)] = \psi(T)[\psi(U) \cap \psi(V)] = [\psi(T)\psi(U)]\cap[\psi(T)\psi(V)] = \psi[(TU)\cap(TV)] \), giving \( T(U \cap V) = (TU) \cap (TV) \). Then, \( R \subset S \) is distributive.

(2) Let \( T \in [R, S] \) be such that \( R'T \) is \( \Pi \)-irreducible in \( [R', S'] \) and let \( U, V \in [R, S] \) be such that \( T = UV \). Then, \( R'T = (R'U)(R'V) \), so that either \( R'T = R'U \), or \( R'T = R'V \), which implies either \( T = U \), or \( T = V \) and \( T \) is \( \Pi \)-irreducible in \( [R, S] \).

Let \( T \in [R, S] \) be such that \( R'T \) is an atom in \( [R', S'] \). Assume that \( T \) is not an atom in \( [R, S] \). There exists \( U \in [R, T] \) which yields \( R' \subset R'U \subset R'T \), a contradiction. Then, \( T \) is an atom in \( [R, S] \).
(3) Assume that \( R'T \) is \( \Pi \)-irreducible in \([R', S']\) for any \( \Pi \)-irreducible \( T \in [R, S] \). This holds if \( \theta \) (or \( \psi \)) is bijective. If \( R' \subset S' \) is an FIP Boolean extension, any \( \Pi \)-irreducible element of \([R', S']\) is an atom in \([R', S']\) by Proposition 3.1. Moreover, \( R \subset S \) is also an FIP extension since \( \theta \) is surjective. Let \( T \in [R, S] \) be \( \Pi \)-irreducible in \([R, S]\). Then, \( R'T \) is \( \Pi \)-irreducible in \([R', S']\). Then \( R'T \) is an atom in \([R', S']\), so that \( T \) is an atom in \([R, S]\) by (2). Since \( \Pi \)-irreducible elements of \([R, S]\) are atoms, the same reference shows that \( R \subset S \) is Boolean. \( \square \)

**Proposition 3.8.** An FIP extension \( R \subset S \), whose Nagata extension \( R(X) \subset S(X) \) has FIP and is Boolean, is Boolean.

**Proof.** According to ([12, Corollary 3.5]), \( R \subset S \) is an FCP extension implies that \( S(X) = R(X) \otimes_R S \), so that we can use Proposition 3.7 because \( R(X) \subset S(X) \) is distributive since Boolean. As \( R(X) \subset S(X) \) has FIP, the map \( \psi : [R, S] \rightarrow [R(X), S(X)] \) defined by \( \psi(T) = T(X) = TR(X) \) is \( \Pi \)-irreducible. Deny, and assume that \( T(X) = T_1' T_2' \) (\( * \)) for \( T_i' \in [R(X), S(X)] \), \( T_i' \neq T' \), \( i = 1, 2 \). There exists \( T_i \in [R, S], i = 1, 2 \), such that \( T_i' = T_i(X) \), so that \( T_i \neq T, i = 1, 2 \), and (\( * \)) gives \( T(X) = T_1(X)T_2(X) \). Then, \( T = T_1T_2 \), a contradiction. It follows that \( R \subset S \) is Boolean by Proposition 3.7. \( \square \)

**Proposition 3.9.** Let \( R \subset S \) be a ring extension, \( f : R \rightarrow R' \) a flat ring epimorphism and \( S' := R' \otimes_R S \). If \( R \subset S \) is a distributive extension (resp. a FIP Boolean extension), then so is \( R' \subset S' \).

**Proof.** The proof is a consequence of the following facts. Let \( f : R \rightarrow R' \) be a flat epimorphism and \( Q \in \text{Spec}(R') \), lying over \( P \) in \( R \), then \( R_P \rightarrow R'_Q \) is an isomorphism. Moreover, we have \( (R' \otimes_R S)_Q \cong R'_Q \otimes_{R_P} S_P \), so that \( R_P \rightarrow S_P \) identifies to \( R'_Q \rightarrow (R' \otimes_R S)_Q = S'_Q \).

Assume that \( R \subset S \) is distributive (resp.: FIP Boolean). Then, so is \( R_P \rightarrow S_P \) for each \( P \in \text{Spec}(R) \) by Proposition 2.4 (resp. Proposition 3.5 and [11, Proposition 3.7]). Let \( Q \in \text{Spec}(R') \) and \( P := f^{-1}(Q) \in \text{Spec}(R) \). Since \( R_P \rightarrow S_P \) identifies to \( R'_Q \rightarrow S'_Q \), we get that \( R'_Q \subset S'_Q \) is distributive (resp.; FIP Boolean) for each \( Q \in \text{Spec}(R') \). It follows that \( R' \subset S' \) is distributive (resp.: FIP Boolean) by the same references. Indeed, in the FIP Boolean case, since \( R \subset S \) has FIP, so has \( R' \subset S' \), because \( \text{Spec}(R') \rightarrow \text{Spec}(R) \) is injective. \( \square \)

**Proposition 3.10.** Let \( R \subset S \) be an FCP distributive extension. The following statements are equivalent:

1. \( R \subset S \) is Boolean;
Any $\Pi$-irreducible element is an atom;

Any $\cap$-irreducible element is a co-atom.

Proof. $R \subset S$ has FIP by Lemma 2.10.

(1) $\iff$ (2) by Proposition 3.1.

(1) $\Rightarrow$ (3) Assume that $R \subset S$ is Boolean. By (2) and using complements, we deduce that any $\cap$-irreducible element of $[R, S]$ is a co-atom of $[R, S]$.

(3) $\Rightarrow$ (1) Use Lemma 2.10 and Proposition 3.1.

Theorem 3.11. Let $R \subset S$ be an FCP extension. The following statements are equivalent, each of them implying that $R \subset S$ has FIP:

(1) $R \subset S$ is Boolean;

(2) $R \subset S$ is factorial;

(3) $R \subset S$ is co-factorial.

Proof. (1) $\Rightarrow$ (2) by Theorem 3.2 and (1) $\Rightarrow$ (3) because, by Proposition 2.9, any $T \in [R, S]$ is a finite intersection of $\cap$-irreducible elements, and then a finite intersection of co-atoms of $[R, S]$ by Proposition 3.10.

(2) $\Rightarrow$ (1). By Theorem 2.11, $R \subset S$ is an atomistic distributive FIP extension. Then, use Proposition 3.1.

(3) $\Rightarrow$ (2) It is enough to exchange products and intersections, and atoms and co-atoms.

Proposition 3.12. [16, Theorems 107, 158 and 159] Let $R \subset S$ be a Boolean extension. Then, $U \subset T$ is Boolean for any $U, T \in [R, S]$ such that $U \subseteq T$ and the complement of $V \in [U, T]$ in $[U, T]$ is $U(T \cap V^\circ)$.

We can now generalize Ayache’s result [3, Theorem 7] in case of an arbitrary ring extension.

Proposition 3.13. When $R \subset S$ has a maximal chain of length $n$ from $R$ to $S$ such that $|\text{Supp}(S/R)| = |\text{MSupp}(S/R)| = n$, then $R \subset S$ is FIP, Boolean, any maximal chain of $[R, S]$ has length $n$ and $|[R, S]| = 2^n$.

Proof. Let $R_0 := R \subset \ldots \subset R_i \subset \ldots \subset R_n := S$ be a maximal chain of $R$-subalgebras of length $n$. For each $i \in \mathbb{N}_n$, set $M_{i-1} := \mathcal{E}(R_{i-1}, R_i) \cap R$. Then, $\text{Supp}(S/R) = \{M_i\}_{i=0}^{n-1} \subseteq \text{Max}(R)$ in view of Lemma 2.14. It follows that $M_i \neq M_j$ for each $i \neq j$, so that $R_{M_i} = (R_i)_{M_i} \subset (R_{i+1})_{M_i} = S_{M_i}$ is minimal (and then has FIP), so that $R \subset S$ has FIP by [11, Proposition 3.7]. Now, $R_{M_i} \subseteq S_{M_i}$ is Boolean (see Example 3.3(1)), and so is $R \subseteq S$ by Proposition 3.5. The last results follow from Theorem 3.2.
Let $R \subset S$ be an FCP Boolean extension and let $R_0 := R \subset \ldots \subset R_i \subset \ldots \subset R_n := S$ be a maximal chain of $R$-subalgebras of $S$. By Proposition 3.12, $R \subset R_{n-1}$ is a Boolean FCP extension and $R_{n-1} \subset S$ is minimal. Next theorem gives a kind of converse which allows us to check by induction that an FIP extension is Boolean.

**Theorem 3.14.** An FIP extension $R \subset S$, which is not minimal, is Boolean if and only if there exist $U,T \in R,S$ such that the conditions (1), (2), (3) and (4) hold, if and only if there exist $U,T \in R,S$ such that the conditions (1), (4) and (5) hold:

1. $[R,S] = [R,T] \cup [U,S]$.
2. $[U,S] = \{UL \mid L \in [R,T]\}$.
3. $L \subset UL$ is a minimal extension for each $L \in [R,T]$.
4. $[R,T]$ is a Boolean lattice.
5. The map $\varphi : [R,T] \to [U,S]$ defined by $\varphi(L) = UL$, for $L \in [R,T]$, is bijective.

Moreover, if these conditions hold, $U$ is an atom, $T = U^\circ$ is a co-atom. In fact, these conditions hold for any atom $U'$ and its complement $T'$, and $[R,T'] \cap [U',S] = \emptyset$.

**Proof.** Assume that $R \subset S$ has FIP and is not minimal. Set $A := \{A_1, \ldots, A_n\}$. We will prove the theorem in four steps:

(a) $R \subset S$ is Boolean $\Rightarrow (1)+(2)+(3)+(4)$.
(b) $(1)+(2)+(3)+(4) \Rightarrow (1)+(4)+(5)$.
(c) $(1)+(4)+(5) \Rightarrow (1)+(2)+(3)+(4)$.
(d) $(1)+(2)+(3)+(4)+(5) \Rightarrow R \subset S$ is Boolean.

(a) Assume that $R \subset S$ is Boolean. Set $U := A_1 \in [R,S]$ and $T := U^\circ \in [R,S]$, the complement of $U$, so that $U \cap T = R$ and $UT = S$. Moreover, $T = \prod_{i=2}^n A_i$, since $T$ is a product of atoms of $[R,S]$ [33, Theorems 3.43 and 5.1].

(1) Let $L \in [R,S]$ and assume that $L \not\subset [U,S]$. We have $U \subset L^\circ$, the complement of $L$ [33, Theorem 5.1] because $U \not\subset L$, and $U \subset L^\circ$ implies $L \subset U^\circ = T$ by [33, Theorem 5.1], so that $L \in [R,T]$. Hence (1) is proved. Moreover, $[R,T] \cap [U,S] = \emptyset$ because $U \subset L \subset T$, for some $L \in [R,T] \cap [U,S]$ leads to the contradiction $U \cap T = R$.

(2) Each element of $[R,S]$ is a product of some $A_i$s by Theorem 3.11. Let $L' := \prod_{i \in I} A_i \in [U,S]$ for some $I \subset \mathbb{N}_n$. Then, $1 \in I$ because $U \subset L'$ (if not, $U \cap L' = R = U$ which is absurd). In particular, $L' = UL$, where $L := \prod_{i \in I \setminus \{1\}} A_i \subset T$ and (2) follows since $UL \in [U,S]$.

(3) Let $L := \prod_{i \in I} A_i \in [R,T]$, so that $1 \notin I$ by (1). Then, $UL = \prod_{i \in I \setminus \{1\}} A_i$. Let $L' \in [L,UL]$. There exists some $J \subset \mathbb{N}_n$ such that $L' := \prod_{i \in J} A_i$. By the uniqueness of this writing, $I \subset J \subset I \cup \{1\}$,
so that we have either $I = J$ or $J = I \cup \{1\}$, giving either $L' = L$ or $L' = UL$. It follows that $L \subseteq UL$ is minimal and (3) holds.

(4) By Proposition 3.12, $R \subseteq T$ is Boolean. Remark that (1), (2), (3) and (4) hold for any atom $U''$ with complement $T'$.

$$R \to L \to T$$

In fact, we have the following diagram: $\downarrow \quad \downarrow \quad \downarrow$

$$U \to UL \to S$$

(b) Assume that (1)+(2)+(3)+(4) holds. Then $\varphi$ is surjective by (2). Let $L, L' \in [R, T]$ be such that $\varphi(L) = \varphi(L')$, that is $UL = UL'$. Since $L, L' \subseteq T$, we get that $LL' \in [R, T]$. Moreover, $U(UL') = (UL)(UL') = UL$. Then, $L, L' \subseteq LL' \subseteq UL = UL'$ gives by (3) either $LL' \neq UL = UL'$, so that $LL' = L = L'$ or $LL' = UL \in [U, S]$. But, in this last case, $UL = LL' \subset ULL' = UL$ is minimal, a contradiction, because $LL' \in [R, T]$. Then, $\varphi$ is bijective and (5) holds.

(c) Assume that (1)+(4)+(5) holds. Then (2) holds by (5). Let $L \in [R, T]$. Since $UL \in [U, S]$, we get $L \neq UL$. Deny, so that $U \subseteq L \subseteq T$ yields $S = UT = T$, a contradiction. Assume that there exists some $L' \in L, UL]$. If $L' \in [R, T]$, we get $UL \subseteq UL' \subset U(UL) = UL$ by (5), a contradiction. If $L' \in [U, S]$, then $L' = UL''$ for some $L'' \in [R, T]$, so that $UL \subseteq UL' = U^2L'' = UL'' = L' \subset UL$, also a contradiction. Then, $L \subset UL$ is minimal, giving (3).

(d) Assume that (1)+(2)+(3)+(4)+(5) holds for some $U, T \in [R, S]$ and that $[R, T] \cap [U, S] \neq \emptyset$. If $L \in [R, T] \cap [U, S]$, then $L = UL$ is a contradiction with (3). So, $[R, T] \cap [U, S] = \emptyset$. We are going to prove that $[R, S]$ is a complemented distributive lattice. We first show that $T$ is the complement of $U$. We get that $R \subset U$ is minimal by (3), so that $R = U \cap T$, because $U \cap T = U$ would imply $U \subseteq T$, a contradiction. Indeed, $UT = S$ by (2) because the map $[R, T] \to [U, S]$ defined by $L \mapsto UL$ is increasing. Then, $T$ is a complement of $U$.

Now, conditions (1), (2) and (5) show that $[R, S]$ is a decomposable lattice, which means that there exist $T, U \in [R, S]$, $T \neq U$, such that for any $L \in [R, S]$, there is a unique pair $(L_1, L_2) \in [R, T] \times [R, U]$ satisfying $L = L_1L_2$ (see [37, p.57]). Set $L_1 := L$ and $L_2 := R$ when $L \in [R, T]$. Set $L_2 := U$ and take $L_1 \in [R, T]$ such that $L = \varphi(L_1)$ when $L \in [U, S]$. The uniqueness of such $(L_1, L_2)$ is obvious in each case. Then, $[R, S]$ is isomorphic as a lattice to $[R, T] \times [R, U]$. In particular, since $[R, T]$ and $[R, U]$ are each Boolean, and then distributive, so is $[R, S]$ by [37, Proposition 3.5.1].

To end, we show that any $L \in [R, S] = [R, T] \cup [U, S]$ has a complement in $[R, S]$. Assume first that $L \in [R, T]$ with complement $L''$ in $[R, T]$ because $R \subseteq T$ is Boolean, so that $L \cap L'' = R$ and
$LL'' = T$. Setting $L' := L''U$, we get $LL' = LL''U = TU = S$. Moreover $L \cap L' = L \cap L''U = (L \cap L'')(L \cap U) = R$. Then, $L'$ is a complement of $L$ in $[R, S]$.

Now, assume that $L \in [U, S]$. Set $L'' := L \cap T \in [R, T]$, and let $L' \in [R, T]$ be its complement in $[R, T]$. Then, $L \cap L' = L \cap L' \cap T = L'' \cap L' = R$. Moreover, $LL' = LUL' \supseteq UUL' = UT = S$ gives that $LL' = S$. Then, $L$ has a complement in $[R, S]$.

So, any element of $[R, S]$ has a complement in $[R, S]$, which is unique by distributivity. To conclude, $R \subset S$ is Boolean.

We are now in position to generalize and improve Ayache’s result [2, Theorem 38] for an arbitrary FIP extension, using a completely different method. This is done in the next subsection. We will need the following results.

**Proposition 3.15.** An FCP extension $R \subset S$, such that $\text{Supp}(T/R) \cap \text{Supp}(S/T) = \emptyset$ for all $T \in [R, S]$, is a Boolean extension.

**Proof.** By Theorem 2.27, $R_M \subset S_M$ is minimal, whence Boolean for any $M \in \text{MSupp}(S/R)$, so that $R \subset S$ is Boolean by Proposition 3.5. □

**Proposition 3.16.** Let $R \subset S$ be an FCP extension and let $T \in [R, S]$ be such that $\text{MSupp}(S/T) \cap \text{MSupp}(T/R) = \emptyset$. Then $R \subset S$ is Boolean if and only if $R \subset T$ and $T \subset S$ are Boolean.

**Proof.** Assume first that $R \subset T$ and $T \subset S$ are Boolean. Let $M \in \text{MSupp}(S/R)$. Then either $M \in \text{MSupp}(S/T)$ (\*) or $M \in \text{MSupp}(T/R)$ (\**). In case (\*), $M \not\in \text{MSupp}(T/R)$, so that $T_M = R_M$. Hence, $[R_M, S_M] = [T_M, S_M]$ is Boolean by Proposition 3.5. In case (\**), $M \not\in \text{MSupp}(S/T)$, so that $T_M = S_M$. Then, $[R_M, S_M] = [R_M, T_M]$ is Boolean by Proposition 3.5. Therefore, $[R_M, S_M]$ is Boolean for each $M \in \text{MSupp}(S/R)$, and Proposition 3.5 gives that $R \subset S$ is Boolean.

The converse is given by Proposition 3.12. □

### 3.2. Characterization of Boolean extensions.

**Theorem 3.17.** An FIP extension $R \subset S$ is Boolean if and only if the following conditions (1) and (2) hold, in which case $\bar{R}$ is the complement of $\bar{R}$:

1. $\text{Supp}((R/R) \cap \text{Supp}(S/R) = \emptyset$.
2. $[\bar{R}, \bar{R}]$ and $[\bar{R}, S]$ are Boolean lattices.

**Proof.** If $[R, S]$ is Boolean, set $T := (\bar{R})^\circ$. Then $\bar{R} \cap T = R$ and $\bar{RT} = S$, so that $\text{Supp}((R/R) \cap \text{Supp}(S/R) = \emptyset$ [29, Proposition 3.6],
and (1) holds. The same proposition shows that \( \tilde{R} = (\overline{R})^\circ \). Now (2) results from Proposition 3.16.

Conversely, assume that (1) and (2) hold. Then, Proposition 3.16 implies that \([R, S]\) is Boolean. \(\square\)

We get a generalization of Ayache’s result [2, Theorem 38] as a corollary thanks to the following lemma.

**Lemma 3.18.** Let \( R \subset S \) be an FCP extension. Set \( X := \{(T', T'') \in [R, \overline{R}] \times [\overline{R}, S] \mid \text{Supp}_{T'}(\overline{R}/T') \cap \text{Supp}_{T''}(\overline{T''}/\overline{R}) = \emptyset\} \). There is a bijection \( \varphi : [R, S] \to X \) defined by \( \varphi(T) := (T \cap \overline{R}, \overline{RT}) \) for each \( T \in [R, S] \).

In particular, if \( R \subset S \) has FIP, then \([|R, S]| \leq |[R, \overline{R}]|([\overline{R}, S]|\)

**Proof.** Let \((T', T'') \in [R, \overline{R}] \times [\overline{R}, S] \). Then, \( \overline{R} \) is also the integral closure \( T' \) of \( T' \) in \( T'' \) (and in \( S \)).

Let \( T \in [R, S] \). Set \( T' := T \cap \overline{R} \) and \( T'' := \overline{RT} \). Then \((T', T'') \in [R, \overline{R}] \times [\overline{R}, S] \). If \( T' = T'' \), then \( T' = T'' = \overline{T} \) implies \( T = \overline{T} \) and \( \text{Supp}_{T'}(\overline{T}/T') = \text{Supp}_{T''}(\overline{T''}/\overline{T}) = \emptyset \). Now assume that \( T' \neq T'' \), then \( \text{Supp}_{T'}(\overline{T}/T') \cap \text{Supp}_{T''}(\overline{T''}/\overline{T}) = \emptyset \) [29, Proposition 3.6]; so that, \((T', T'') \in X \). Hence we can define \( \varphi : [R, S] \to X \) by \( \varphi(T) := (T \cap \overline{R}, \overline{RT}) \) for each \( T \in [R, S] \).

Now, let \( T_1, T_2 \in [R, S] \) be such that \( \varphi(T_1) = \varphi(T_2) = (T', T'') \). Assume \( T' \neq T'' \). An application of [29, Lemma 3.7] to the extension \( T' \subseteq T'' \) gives that \( T_1 = T_2 \). If \( T' = T'' \), then \( T' = T'' = \overline{T} \), so that \( T_1 = T_2 = \overline{T} \). It follows that \( \varphi \) is injective. The same reference gives that \( \varphi \) is bijective, which yields \([|R, S]| \leq |[R, \overline{R}]|([\overline{R}, S]|\)

**Corollary 3.19.** The extension \( R \subset S \) is FIP Boolean if and only if the two following conditions hold:

1. \( R \subset \overline{R} \) and \( \overline{R} \subset S \) are FIP Boolean extensions.
2. \([|R, S]| = |[R, \overline{R}]|([\overline{R}, S]|\]

**Proof.** If \( R \subset S \) is FIP Boolean, Proposition 3.12 implies that so are \( R \subset \overline{R} \) and \( \overline{R} \subset S \), giving (1). Since \( \text{Supp}(\overline{R}/R) \cap \text{Supp}(S/\overline{R}) = \emptyset \) by Theorem 3.17, we infer that \([|R, S]| = |[R, \overline{R}]|([\overline{R}, S]|\) [29, Lemma 3.7].

Conversely, assume that conditions (1) and (2) hold. Then \( R \subset S \) has FIP by (2) and (1) is condition (2) of Theorem 3.17. The map \( \varphi \) defined in Lemma 3.18 being condition (2) of Theorem 3.17. The map \( \varphi \) defined in Lemma 3.18 being injective, condition (2) shows that \( \varphi([R, S]) = [R, \overline{R}] \times [\overline{R}, S] \). Therefore, there is \( T \in [R, S] \) such that \( \varphi(T) = (R, S) \), inducing by the properties of \( \varphi \) that \( \text{Supp}_{R}(\overline{R}/R) \cap \text{Supp}_{R}(S/\overline{R}) = \emptyset \), (actually, the condition of Theorem 3.17(1), asserting that \( R \subset S \) is Boolean). To conclude, \( R \subset S \) is Boolean. \(\square\)
Corollary 3.20. Let $R \subseteq S$ be an FIP Boolean extension, where $R$ is a local ring. Then, $R \subseteq S$ is either Prüfer, or integral.

Proof. Use Theorem 3.17 and [31, Proposition 4.16]. □

By Corollary 3.20 and Proposition 3.5, the characterization of Boolean FIP extension $R \subseteq S$ can be reduced to those that are either Prüfer or integral, with $R$ local.

For the Prüfer case, we recover and generalize some Ayache’s results on extensions of integral domains [2, Proposition 35].

Proposition 3.21. An integrally closed extension $R \subseteq S$ is Boolean and FIP if and only if $R \subseteq S$ is a Prüfer extension and $\lvert \Supp(S/R) \rvert = \lvert \MSupp(S/R) \rvert < \infty$. If these conditions hold, $\lvert [R, S] \rvert = 2^{\lvert \Supp(S/R) \rvert}$.

Proof. Assume first that $\lvert \Supp(S/R) \rvert = \lvert \MSupp(S/R) \rvert < \infty$ and that $R \subseteq S$ is Prüfer. From [11, Proposition 6.9], we infer that $R \subseteq S$ has FIP. Moreover, we proved in [11, Proposition 6.12], that, under these conditions, $\lvert [R_M, S_M] \rvert = 2$ for each $M \in \Supp(S/R)$, so that $R_M \subseteq S_M$ is Boolean for each $M \in \Supp(S/R)$ by Example 3.3(1), since minimal, and then $[R, S]$ is Boolean by Proposition 3.5. From [11, Proposition 6.12], we deduce that $\lvert [R, S] \rvert = 2^{\lvert \Supp(S/R) \rvert}$.

Conversely, suppose that $R \subseteq S$ is Boolean and has FIP. Then, [11, Proposition 6.9] implies that $R \subseteq S$ is Prüfer and $\Supp(S/R)$ is finite. Since $R \subseteq S$ is Boolean, so is $R_M \subseteq S_M$ for each $M \in \Supp(S/R)$ by Proposition 3.5. But, $\lvert [R_M, S_M] \rvert$ is chained [11, Theorem 6.10]. It follows that $R_M \subseteq S_M$ is minimal for each $M \in \Supp(S/R)$ by Example 3.3(1), so that $\lvert \Supp(R_M/S_M) \rvert = 1$ for each $M \in \Supp(S/R)$ by [11, Proposition 6.12], and then $\Supp(S/R) \subseteq \MSupp(S/R)$ completes the proof. □

Corollary 3.22. A Prüfer FIP extension $R \subseteq S$ is Boolean if and only if $R \subseteq S$ is locally minimal. In this case, $R \subseteq S$ is a $B$-extension.

Proof. The two properties are equivalent by the proof of the above proposition. Since $\Supp(S/R) = \MSupp(S/R)$ holds in this case, [11, Theorem 3.6] shows that $\varphi$ is a bijection. □

The following definitions are needed for the sequel.

Definition 3.23. An integral extension $R \subseteq S$ is called infra-integral [27] (resp.; subintegral [35]) if all its residual extensions $\kappa_R(P) \to \kappa_S(Q)$, (with $Q \in \Spec(S)$ and $P := Q \cap R$) are isomorphisms (resp.;and the natural map $\Spec(S) \to \Spec(R)$ is bijective). An extension $R \subseteq S$ is called $t$-closed (cf. [27]) if the relations $b \in S$, $r \in R$, $b^2 - rb \in R$, $b^3 - rb^2 \in R$ imply $b \in R$. The $t$-closure $t_S R$ of $R$ in $S$ is the smallest
Three types of minimal integral extensions exist, characterized in the next theorem, (a consequence of the fundamental lemma of Ferrand-Olivier), so that there are four types of minimal extensions.

**Theorem 3.24.** [11, Theorems 2.2 and 2.3] Let $R \subseteq T$ be an extension and $M := (R : T)$. Then $R \subseteq T$ is minimal and finite if and only if $M \in \text{Max}(R)$ and one of the following three conditions holds:

(a) **inert case:** $M \in \text{Max}(T)$ and $R/M \rightarrow T/M$ is a minimal field extension.

(b) **decomposed case:** There exist $M_1, M_2 \in \text{Max}(T)$ such that $M = M_1 \cap M_2$ and the natural maps $R/M \rightarrow T/M_1$ and $R/M \rightarrow T/M_2$ are both isomorphisms; or, equivalently, there exists $q \in T \setminus R$ such that $T = R[q]$, $q^2 - q \in M$, and $Mq \subseteq M$.

(c) **ramified case:** There exists $M' \in \text{Max}(T)$ such that $M'^2 \subseteq M \subseteq M'$, $[T/M : R/M] = 2$, and the natural map $R/M \rightarrow T/M'$ is an isomorphism; or, equivalently, there exists $q \in T \setminus R$ such that $T = R[q]$, $q^2 \in M$, and $Mq \subseteq M$.

It remains to solve [2, Problem 45]: under which conditions an integral extension $R \subseteq S$ is Boolean and has FIP? The study is quite complicated. We are going to use the canonical decomposition of an integral ring extension and Proposition 3.5 which allows us to only consider local rings $R$.

**Proposition 3.25.** Let $R \subseteq S$ be an integral FIP Boolean extension where $R$ is local. Then, $R \subseteq S$ is either infra-integral or t-closed.

**Proof.** Let $T := \ell_S R$ be the t-closure of the local ring $(R, M)$ in $S$, and let $T^\circ \in [R, S]$ be its complement. Let $T'$ be the t-closure of $R$ in $T^\circ$, so that $R \subseteq T'$ is infra-integral, and then $T' \subseteq T$. It follows that $T' \subseteq T^\circ \cap T = R$. Then $T' = R$ and $R \subseteq T^\circ$ is t-closed. In the same way, let $T''$ be the t-closure of $T^\circ$ in $S$, so that $T^\circ \subseteq S$ is t-closed and then $T \subseteq T''$. Hence $S = T^\circ T \subseteq T''$, so that $T'' = S$ and $T^\circ \subseteq S$ is infra-integral.

Assume that $R \subseteq S$ is neither t-closed, nor infra-integral, so that $T, T^\circ \neq R, S$. Then, there are $R_1 \in [R, T]$ and $R'_1 \in [R, T^\circ]$ such
that $R \subset R_1$ is minimal infra-integral, and $R \subset R'_1$ is minimal inert, with both the same crucial maximal ideal $M$. By [14, Propositions 7.1 and 7.4], there are two maximal chains from $R$ to $R_1R'_1$ with different lengths, and the same statement holds for $R \subset S$. This contradicts Condition (JH) of Proposition 2.5 since $R \subset S$ is distributive. Then, $R \subset S$ is either infra-integral, or t-closed.

\[ \square \]

**Remark 3.26.** Proposition 3.25 is no longer true if $R$ is not local. Take a ring $R$ with two distinct maximal ideals $M_1$ and $M_2$, and two minimal extensions $R \subset T_1$ ramified and $R \subset T_2$ inert with $M_1 := \mathfrak{c}(R, T_1)$ and $M_2 := \mathfrak{c}(R, T_2)$. Assume that $S := T_1T_2$ exists, so that $R_{M_1} \subset S_{M_1} = (T_1)_{M_1}$ is minimal ramified, and then Boolean and $R_{M_2} \subset S_{M_2} = (T_2)_{M_2}$ is minimal inert, and then Boolean. It follows from Proposition 3.5 that $R \subset S$ is Boolean although being neither infra-integral nor t-closed. To get such a situation, we may take $S := \mathbb{Z}[i]$, $T_2 := \mathbb{Z} + 2S$, $T_1 := \mathbb{Z} + 3S$ and $R := T_1 \cap T_2 = \mathbb{Z} + 6S$. It is well known that 2 is ramified in $S$ and 3 is inert in $S$. If $p$ is a prime integer, the extension $\mathbb{Z} + pS \subset S$ is minimal of the same type as $\mathbb{Z}/p\mathbb{Z} \subset \mathbb{Z}/pS$, which is of the same type as the decomposition of $p$ in $S$. Then, $T_2 \subset S$ is a minimal ramified extension with conductor 2S and $T_1 \subset S$ is a minimal inert extension with conductor 3S. Moreover, 2S and 3S are incomparable. Setting $M_1 := 2S \cap R = 2T_1$ and $M_2 := 3S \cap R = 3T_2$, [14, Proposition 6.6(a)] shows that $R \subset T_1$ is minimal ramified and $R \subset T_2$ is minimal inert with $M_1 := \mathfrak{c}(R, T_1)$, $M_2 := \mathfrak{c}(R, T_2)$ and $S = T_1T_2$.

We first consider the infra-integral case for which we need the next lemma.

**Lemma 3.27.** A subintegral FIP extension (resp. seminormal and infra-integral) $R \subset S$, where $(R, M)$ is local, is Boolean if and only if $R \subset S$ is minimal ramified (resp. decomposed).

**Proof.** One implication is Example 3.3 (1).

Conversely, assume that $[R, S]$ is a Boolean lattice. The atoms of $[R, S]$ are of the form $R_i := R + Rx_i$, for $i \in I := \mathbb{N}_n$, $n := |A|$, where $x_i \in S$ is such that $x_i^2 \in M$ (resp. $x_i^2 - x_i \in M$) and $x_i M \subseteq M$, because $R \subset R_i$ is minimal ramified (resp.; decomposed), with $M = (R : R_i)$. Then, $S = \prod_{i \in I} R_i$ by Theorem 3.2. Let $M_i := M + Rx_i$ be the (resp.; one) maximal ideal of $R_i$. Assume that $n > 1$. Let $i, j \in I$ be such that $i \neq j$, so that $R = R_i \cap R_j$, with $x_ix_j \in R_iR_j$. But, $R_i \subseteq R_iR_j$ and $R_j \subseteq R_iR_j$ are minimal by Theorem 3.2 because $[R, R_iR_j]$ is Boolean with 2 atoms. It follows that $x_i \in M_i = (R_i : R_iR_j)$ and $x_j \in M_j = (R_j : R_iR_j)$. In the decomposed case, we may choose $x_i$ and $x_j$ in order that $M_i$ and $M_j$ are the needed conductors. It follows that $M_i$
and $M_j$ are ideals of $R_i R_j$, and so is $M_i \cap M_j$, which contains $M_i M_j$.
But $M_i \cap M_j \subseteq R_i \cap R_j = R$. This implies that $x_i x_j \in M_i \cap M_j = M_i \cap R \cap M_j = M$, the maximal ideal of $R$. Then, $x_i x_j \in M$, giving $S = R + \sum_{i \in I} R x_i$. Set $x := x_i + x_j \not\in R$ and $R_x := R + Rx \not= R_i R_j$.
We get that $x^2 = x_i + x_j + m = x + m$, where $m \in M$). Moreover, $x M \subseteq x_i M + x_j M \subseteq M$, so that $R \subset R_x$ is minimal by Theorem 3.24, and $R_x$ is an atom of $[R, S]$. But we have $R_x \subseteq R_i R_j$, so that $R_x = R_x \cap R_i R_j = (R_x \cap R_i)(R_x \cap R_j) = R$, a contradiction. Then, $n = 1$, $S = R_1$ and $R \subset S$ is minimal.

It may be asked if extensions of Boolean rings and Boolean extensions are linked. The next result shows that they are almost never linked.

**Proposition 3.28.** Let $S$ be a Boolean ring and $R$ a subring of $S$ such that $R \subset S$ is a finite extension. Then $R \subset S$ is seminormal infra-integral and $R \subset S$ is Boolean if and only if $R \subset S$ is locally minimal.

**Proof.** Since $S$ is a Boolean ring, $R \subset S$ is seminormal integral. Because a Boolean local ring is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, the residual extensions of $R \subset S$ are isomorphisms, so that $R \subset S$ is infra-integral. Now, $R \subset S$ is finite implies that it has FCP by [11, Theorem 4.2].

Assume that $R \subset S$ is Boolean. Then, $R \subset S$ has FIP by Theorem 3.2 because FCP distributive. Moreover, an appeal to Lemma 3.27 shows that $R \subset S$ is locally minimal.

Conversely, if $R \subset S$ is locally minimal, then $R \subset S$ is Boolean in view of Corollary 3.6. Indeed, $R \subset S$ has FIP [11, Proposition 3.7].

Next proposition gives a characterization of arbitrary infra-integral Boolean FIP extensions.

**Proposition 3.29.** An infra-integral FIP extension $R \subset S$, where $(R, M)$ is local, is Boolean if and only if there exist $x, y \in S$ such that $S = R[x, y]$, where $x^2, xy, y^2 - y \in M$ and $x M, y M \subseteq M$.

If these conditions hold, then $R[x, y] = R[x + y]$.

**Proof.** If $R \subset S$ is subintegral, we choose $y = 0$, if $R \subset S$ is seminormal, we choose $x = 0$. In both cases, we use Lemma 3.27 to get the equivalence. From now on, we assume that $R \subset S$ is neither subintegral, nor seminormal.

Assume that $R \subset S$ is Boolean and set $T := \frac{R}{S} R \not= R, S$. From Proposition 3.12, we deduce that $[R, T]$ and $[T, S]$ are Boolean. Then, $R \subset T$ is minimal ramified, which implies that $T$ is also local. It follows that $T \subset S$ is minimal decomposed by Lemma 3.27, so that $\ell[R, S] = 2$, because all maximal chains of $[R, S]$ have the same length.
Theorem 3.30. An FIP extension \( R \subset S \) is Boolean if and only if, for each \( M \in \text{MSupp}(S/R) \), one of the following conditions holds:

1. \( R_M \subset S_M \) is a minimal extension.
2. There exist \( U, T \in [R_M, S_M] \) such that \( R_M \subset T \) is minimal ramified, \( R_M \subset U \) is minimal decomposed and \( [R_M, S_M] = \{R_M, T, U, S_M\} \).
3. \( R_M \subset S_M \) is a Boolean t-closed extension (equivalently, \( R_M \subset S_M \) is t-closed and \( \kappa_R(M) \subset \kappa_S(N) \) is a Boolean field extension, where \( N \) is the only maximal ideal of \( S \) lying above \( M \)).

Proof. From Proposition 3.5, we deduce that \([R, S]\) is Boolean if and only if, for each \( M \in \text{MSupp}(S/R) \), \([R_M, S_M]\) is Boolean. An appeal to Corollary 3.20 shows that this statement is equivalent to the following: for each \( M \in \text{MSupp}(S/R) \), either \( R_M \subset S_M \) is Boolean and integrally closed (\(*\)), or \( R_M \subset S_M \) is Boolean integral (\(**\)). In case (\(*\)) Corollary 3.22 gives that \( R_M \subset S_M \) is Boolean integrally closed if and only if \( R_M \subset S_M \) is Prüfer minimal. In case (\(**\)), when \( R_M \subset S_M \) is integral, Proposition 3.25 says that \( R_M \subset S_M \) is Boolean if and only if either
$R_M \subseteq S_M$ is infra-integral Boolean (a), or $R_M \subseteq S_M$ is t-closed Boolean (b). To sum up, if $[R,S]$ is Boolean, for each $M \in \text{MSupp}(S/R)$, either $(\ast)$ or $(\ast\ast)$ (a) or $(\ast\ast)$ (b) holds. Case $(\ast)$ implies (1). Case $(\ast\ast)$ (a) implies either (1) or (2). Indeed, by Proposition 3.29, there exist $x,y \in S_M$ such that $S_M = R_M[x,y]$, where $x^2, xy, y^2 - y \in MR_M$ and $xMR_M, yMR_M \subseteq MR_M$. Since $M \in \text{MSupp}(S/R)$, we have $R_M \neq S_M$, so that either $x \notin R_M$ or $y \notin R_M$. If both $x, y \notin R_M$, setting $T := R_M[x]$ and $U := R_M[y]$, we get (2). If only one of $x, y \notin R_M$, we get (1). Case $(\ast\ast)$ (b) is (3). Conversely, if (1) holds, then $R_M \subseteq S_M$ is Boolean by Example 3.3(1). If (2) holds, then $R_M \subseteq S_M$ is Boolean by Proposition 3.29, setting $T := R_M[x]$ and $U := R_M[y]$ for some $x \in T$, $y \in U$ such that $x^2, xy, y^2 - y \in MR_M$ and $xMR_M, yMR_M \subseteq MR_M$. At last, (3) is $(\ast\ast)$ (b).

We now show that, for some $M \in \text{MSupp}(S/R)$, $R_M \subseteq S_M$ is Boolean t-closed is equivalent to $R_M \subseteq S_M$ is t-closed and $\kappa(M) \subseteq \kappa(N)$ is a Boolean field extension, where $N$ is the only maximal ideal of $S$ lying above $M$. Set $R' := R_M$, $M' := MR_M$ and $S' := S_M$. Since $R' \subseteq S'$ is t-closed, $M' = (R': S')$ and $(S', M')$ is local, [12, Lemma 3.17]. It follows that there is only one maximal ideal $N$ in $S$ lying over $M$, so that $S_M = S_N$ ([5, Proposition 2, page 40]) and $\kappa_S(N) = S'/M'$. Then $\kappa_R(M) = R'/M' \subseteq S'/M' = \kappa_S(N)$ is an FIP field extension. Now, $R' \subseteq S'$ is Boolean if and only if $R'/M' \subseteq S'/M'$ is Boolean by Proposition 3.5. \hfill \Box

It follows that the remaining t-closed case can be reduced to the case of FIP field extensions. The case of fields is the subject of the next section, because of its complexity.

**Proposition 3.31.** A ring extension $R \subseteq S$ has FIP and is Boolean if and only if $R(X) \subseteq S(X)$ has FIP and is Boolean.

**Proof.** One part of the proof is Proposition 3.8. So, assume that $R \subseteq S$ has FIP and is Boolean. Then, $R(X) \subseteq S(X)$ has FIP if and only if $R \subseteq \hat{S} R$ is arithmetic [30, Corollary 4.3]. If this conditions holds, the map $\psi : [R, S] \to [R(X), S(X)]$ defined by $T \mapsto T(X)$ is an order-isomorphism [13, Theorem 32]. It follows that $R(X) \subseteq S(X)$ is Boolean since Boolean conditions are preserved through $\psi$. To complete the proof, we need only to show that $R(X) \subseteq S(X)$ has FIP. It follows from Proposition 3.12 that $[R, \hat{S} R]$ is finite and Boolean. But, under these conditions, Theorem 3.30 yields that either $R_M = (\hat{S} R)_M$ or $R_M \subseteq (\hat{S} R)_M$ is minimal, for each $M \in \text{MSupp}(S/R)$. This means that $R \subseteq \hat{S} R$ is arithmetic, so that $R(X) \subseteq S(X)$ has FIP. \hfill \Box
4. Boolean FIP field extensions

The characterization of a Boolean extension of fields is quite different from those obtained in Theorem 3.14 and needs a special study.

4.1. FIP non-separable field extensions. We will call in this paper *radicial* any purely inseparable field extension. We recall that a minimal field extension is either separable or radicial ([28, p. 371]). We will use the separable closure of a FIP algebraic field extension. In this subsection, we only consider FIP field extensions. Indeed, a finite algebraic field extension is not necessarily FIP. For instance a radicial extension $k \subseteq L$ has not FIP, when $p := c(k), L := k[x, y]$, with $x \in k$, $y \in L$ and $[L : k] = p^2$.

Lemma 4.1. An FIP radicial field extension $k \subseteq K$ is chained.

*Proof.* Since $k \subseteq K$ has FIP, there exists $\alpha \in K$ such that $K = k[\alpha]$ by the Primitive Element Theorem. Moreover, $c(k) = p$ is a prime integer because $k \subseteq K$ is radicial. Then, the monic minimal polynomial of $\alpha$ over $k$ is of the form $f(X) := X^{p^n} - a = (X - \alpha)^{p^n}$, where $a := \alpha^{p^n}$ for some positive integer $n$.

The map $\varphi : \{0, \ldots, n\} \to [k, K]$ defined by $\varphi(m) := k[\alpha^{p^m}]$ is strictly decreasing. Let $L \in [k, K]$ and $g(X)$ be the monic minimal polynomial of $\alpha$ over $L$. Then, $g(X)$ divides $f(X)$ in $K[X]$ and is of the form $g(X) = (X - \alpha)^{p^m}$ for some $m \in \{0, \ldots, n\}$ because $L \subseteq K = L[\alpha]$ is radicial and then the degree of $g(X)$ is a power of $p$. It follows that $g(X) = X^{p^n} - \alpha^{p^m} = X^{p^n} - \beta$, where $\beta := \alpha^{p^m} \in L$. By the proof of the Primitive Element Theorem, $L$ is generated over $k$ by the coefficients of $g(x)$, so that $L = k[\beta] = k[\alpha^{p^m}] = \varphi(m)$. Then, $\varphi$ is a bijection and $[k, K]$ is chained. □

We here take the opportunity to correct a miswriting in the proof of [30, Proposition 2.3]. The sentence: “It follows that there is only one maximal chain composing $K \subseteq L$, and it has length $n$” has to be replaced with “It follows that any maximal chain composing $K \subseteq L$ has length $n$”.

Theorem 4.2. An FIP field extension $k \subset K$, with separable closure $T$ and radicial closure $U$ such that $U, T \not\subseteq \{k, K\}$, is Boolean if and only if the following conditions hold:

1. $k \subset U$ and $T \subset K$ are minimal.
2. $[k, K] = [k, T] \cup [U, K]$.
3. $k \subset T$ and $k \subset U$ are linearly disjoint.
4. $[k, T]$ is a Boolean lattice.

If these conditions hold, then $[k, T] \cap [U, K] = \emptyset$ and $U = T^\circ$. 
Proof. Since $k \subseteq U$ is radicial, $c(k) = p$ is a prime integer.

Assume that $k \subseteq K$ is Boolean. If $T^\circ$ is the complement of $T$ and $T'$ the separable closure of $k$ in $T^\circ$, then $T' \subseteq T^\circ \cap T = k$ entails that $k \subseteq T^\circ$ is radical, so that $T^\circ \subseteq U$. But $K = T^\circ T \subseteq UT$ gives $UT = K$. Moreover, $k = U \cap T$ shows that $T^\circ = U$.

We claim that $k \subseteq U$ is minimal. Deny, and let $U_1 \in [k, U]$ be such that $k \subseteq U_1$ is minimal. Since $k \subseteq U$ is radicial, $[k, U]$ is a chain by Lemma 4.1. Let $U_1^\circ \in [T, K]$ be the complement of $U_1$ in $[k, K]$. Then, $K = U_1 U_1^\circ \subseteq UU_1^\circ$ implies $K = UU_1^\circ$. Moreover, $k \subseteq U \cap U_1^\circ \subseteq U \Rightarrow U \cap U_1^\circ \in [k, U]$. If $k \neq U \cap U_1^\circ$, then $U_1 \subseteq U \cap U_1^\circ \subseteq U_1^\circ \Rightarrow U_1 U_1^\circ = U_1^\circ = K$ is absurd because $U_1 \neq k$. Hence, $U \cap U_1^\circ = k$, so that $U_1^\circ$ is also the complement of $U$, which is absurd. It follows that $k \subseteq U$ is minimal. Then (1), (2) and (4) hold by Theorem 3.14 (3),(1),(4). We get that $[U : k] = [K : T] = p$ since $k \subseteq U$ and $T \subseteq K$ are minimal radicial. But, $K = TU \Rightarrow [TU : T] = [U : k]$; so that, $[TU : k] = [T : k][U : k]$, and then $k \subseteq T$ and $k \subseteq U$ are linearly disjoint [6, Proposition 5, A V.13].

Conversely, assume that (1), (2), (3) and (4) hold. Then, the above conditions (2) and (4) on $T$ and $U$ coincide with Theorem 3.14 (1),(4), so that we can use the diagram appearing in its proof, where $L \in [k, T]$:

$$
\begin{array}{c}
k \\
\downarrow \\
U
\end{array} \quad \begin{array}{c}
L \to T \\
\downarrow \\
UL \to K
\end{array}
$$

Moreover, (3) implies that $L \subseteq LU$ and $L \subseteq T$ are linearly disjoint [6, Proposition 8, A V.14]. In particular, $[LU : L] = [K : T] = p$ shows that $L \subseteq LU$ is minimal as in Theorem 3.14 (3). Let $L \in [U, K]$, and set $L' := L \cap T$, which is the separable closure of $k \subseteq L$. Then, $L' \subseteq L$ is radicial. But, $UL' \subseteq L$ is both separable (because so is $U \subseteq K$ by [6, A V.45, Proposition 16] since $k \subseteq T$ and $k \subseteq U$ are linearly disjoint) and radicial, because $L' \subseteq L$ is radicial, so that $L'U = L = U(L \cap T)$. Then, $[U, K] = \{UL' \mid L' \in [k, T]\}$ implies Theorem 3.14 (2). Finally, $[k, K]$ is Boolean by Theorem 3.14. The missing statement $[k, T] \cap [U, K] = \emptyset$ hold by Theorem 3.14.

Hence, we need only to consider either radicial or separable Boolean field extensions to have a complete answer. We recall [20] that a finite field extension $k \subseteq L$ is said to be exceptional if $k$ is the radicial closure and $L$ is not the separable closure. Then, a finite exceptional field extension $k \subseteq L$ is never Boolean. Deny. Using notation of Theorem 4.2, $U = k = T^\circ$ implies $T = L$, a contradiction.
Proposition 4.3. An FIP radical field extension $k \subset K$ is Boolean if and only if $k \subset K$ is minimal if and only if $c(k) = [K : k]$.

Proof. Use Example 3.3 (1) since $[k, K]$ is a chain by Lemma 4.1 for the first equivalence, the second comes from [28, Proposition 2.2]. □

A Galois extension $k \subset K$ is minimal if and only if $[K : k]$ is a prime integer [28, Proposition 2.2]. But this equivalence does not always hold for an arbitrary finite separable extension. Theorem 4.5 characterizes minimal separable extensions, independently of Galois Theory, contrary to Philippe’s methods [26]. She proved that a separable extension $k \subset k(x)$ is minimal if and only if the Galois group of the minimal polynomial of $x$ is primitive [28, Proposition 2.2(3)]. See also Cox [9, page 414] for the characterization and links between primitive groups and “primitive” separable polynomials, a non-trivial theory.

4.2. Finite separable field extensions. Let $k \subset L$ be a finite separable field extension, (whence FIP). Then any $T \in [k, L]$ is an intersection of finitely many $\cap$-irreducible elements of $[k, L]$ by Proposition 2.9. We give an upper bound of $|[k, L]|$ and recall a result from Dobbs-Mullins.

Proposition 4.4. [10, Theorem 2.7] Let $k \subset L$ be a finite field extension of degree $n$, where $k$ is an infinite field, then, $|[k, L]| \leq 2^{n-2} + 1$.

Following the referee’s advice, we remark that a simple result for finite fields holds. If $k$ is a finite field, there exists a prime integer $p$ such that $p = c(k)$ and $k \cong \mathbb{F}_q$, where $q$ is a power of $p$. If $k \subset L$ is a finite (separable) extension, then $L \cong \mathbb{F}_{q^m}$, where $m$ is a positive integer. It is well known that $|[k, L]| = m$ [6, A V.90, Proposition 3.].

If $k \subset L$ is Boolean, any $\cap$-irreducible element is a co-atom by Proposition 3.10. In fact, Theorem 3.11 says that $k \subset L$ is Boolean if and only if any $T \in [k, L]$ is an intersection in a unique way of finitely many co-atoms. Thanks to principal subfields introduced in [36] and some of their properties we studied in [32], we are able to characterize co-atoms of a finite separable field extension, and then give a characterization of a finite separable Boolean field extension by using [36], from van Hoeij, Klüners and Novocin, that gives an algorithm to compute subextensions of a finite separable field extension. We recall the notation of [32], $(k_u[X]$ is the set of monic polynomials of $k[X])$.

From now on, our riding hypotheses for the subsection will be: $L := k[x]$ is a finite separable (whence FIP) field extension of $k$ with degree $n$ and $f(X) \in k_u[X]$ is the minimal polynomial of $x$ over $k$. If $g(X) \in L_u[X]$ divides $f(X)$, we denote by $K_g$ the $k$-subalgebra of $L$ generated by the coefficients of $g$. For any $K \in [k, L]$, we denote by $f_K(X) \in$
$K_u[X]$ the minimal polynomial of $x$ over $K$. The proof of the Primitive Element Theorem shows that $K = K_{f_K}$ (*). Of course, $f_K(X)$ divides $f(X)$ in $K[X]$ (and in $L[X]$). If $f(X) := (X - x)f_1(X) \cdots f_r(X)$ is the decomposition of $f(X)$ into irreducible factors of $L_u[X]$, we set $\mathcal{F} := \{f_1, \ldots, f_r\}$ because the $f_\alpha$’s are different by separability. For each $\alpha \in \mathbb{N}_r$, we set $L_\alpha := \{g(x) \in L \mid g(x) \in k[X], \ g(X) \equiv g(x) \ (f_\alpha(X)) \ \text{in} \ L[X]\}$. The $L_\alpha$’s are called the principal subfields of $k \subset L$. It may be that $L_\alpha = L_\beta$ for some $\alpha \neq \beta$ (see [32, Example 5.17 (1)]). To get rid of this situation, we defined in [32] $\Phi : \mathcal{F} \to [k, L]$ by $\Phi(f_\alpha) = L_\alpha$.

Proof. The inequality comes from that any $n$ not Galois and of degree $|k, L|$ is minimal if and only if $t = 1$.

Theorem 4.5. [32, Theorem 5.5] Let $K \in [k, L[$. Then, $f_K(X) = (X - x) \prod_{\alpha \in I(K)} f_\alpha(X)$ and $K = \{g(x) \in L \mid g(X) \in k[X], g(X) \equiv g(x) \ (f_K(X)) \ \text{in} \ K[X]\} = \bigcap_{\beta \in J(K)} E_\beta = \bigcap_{\alpha \in I(K)} L_\alpha$. In particular, $|[k, L[| \leq 2^t$ and $k \subset L$ is minimal if and only if $t = 1$.

Proof. The inequality comes from that any $K \in [k, L]$ is an intersection of some principal subfields and gives the equivalence.

In case $k \subset L$ is not a Galois extension, we get a better bound than the bound of [10, Theorem 2.7].

Corollary 4.6. Let $k \subset L$ be a finite separable field extension which is not Galois and of degree $n$. Then, $|[k, L]| \leq 2^{n-2}$.

Proof. Let $f(X)$ be the minimal polynomial of the extension $k \subset L$ and set $f(X) := (X - x)f_1(X) \cdots f_r(X)$ the decomposition of $f(X)$ into irreducible factors of $L_u[X]$. Since $k \subset L$ is not Galois, at least one $f_i$ is not of degree 1, so that $n = 1 + \sum_{i=1}^{r'} \text{deg}(f_i) \geq 1 + 2 + (r - 1) = r + 2$.

It follows that $t \leq r \leq n - 2$ implies $|[k, L]| \leq 2^t \leq 2^{n-2}$. In case $k \subset L$ is Galois and $k$ is an infinite field, Dobbs-Mullins proved in [10, Proposition 2.8] that there exist Galois extensions such that $|[k, L]| = 2^{n-2} + 1$ when either $n = 2$ or $n = 4$. The same Proposition shows that for $n \neq 2, 4$, then $|[k, L]| < 2^{n-2} + 1$, so that we recover the bound of Corollary 4.6.

In the following, we write $K_\alpha := K_{g_\alpha}$, where $g_\alpha(X) := (X - x)f_\alpha(X)$.

Lemma 4.7. For $K, K' \in [k, L], K \subset K' \iff f_{K'}(X)|f_K(X)$ in $L[X]$. 
Proof. Assume that \( K \subseteq K' \). Then, \( f_K(X) \in K'[X] \) satisfies \( f_K(x) = 0 \), so that \( f_{K'}(X) \) divides \( f_K(X) \) in \( K'[X] \), and also in \( L[X] \).

Conversely, assume that \( f_{K'} \) divides \( f_K \) in \( L[X] \). Since Theorem 4.5 implies \( K = \cap_{\alpha \in I(K)} L_\alpha \), \( K' = \cap_{\alpha \in I(K')} L_\alpha \) and \( f_{K'} \) divides \( f_K \) in \( L[X] \), any \( f_\alpha \) which divides \( f_{K'} \) divides \( f_K \), so that \( I(K') \subseteq I(K) \) and then \( K = \cap_{\alpha \in I(K)} L_\alpha \subseteq \cap_{\alpha \in I(K')} L_\alpha = K' \).

\[ \square \]

**Proposition 4.8.** If \( K, K' \in [k, L] \), then \( \text{lcm}(f_K, f_{K'}) \) divides \( f_{K \cap K'} \), and \( f_{KK'} \) divides \( \text{gcd}(f_K, f_{K'}) \) in \( L[X] \).

**Proof.** Use Lemma 4.7 applied to \( K \cap K' \subseteq K, K' \subseteq KK' \). \[ \square \]

We set \( \mathcal{D} := \{ f_K \mid K \in [k, L] \} \). Then, \( (\mathcal{D}, \leq) \) is a poset for the order \( \leq \) defined as follows: if \( f_K, f_{K'} \in \mathcal{D} \), then \( f_K \leq f_{K'} \) if and only if \( f_K|f_{K'} \) in \( L[X] \), which is equivalent to \( K' \subseteq K \) by Lemma 4.7. In particular, sup and inf are respectively lcm and gcd in \( \mathcal{D} \).

**Corollary 4.9.** The map \( \varphi : [k, L] \to \mathcal{D} \) defined by \( K \mapsto f_K \) is a reversing order bijection such that \( \text{sup}(f_K, f_{K'}) = f_{K \cap K'} \) and \( f_{KK'} = \text{inf}(f_K, f_{K'}) \) for \( K, K' \in [k, L] \).

**Proof.** \( \varphi \) is obviously surjective and is injective since \( K = K_{f_K} \) by (\(^*\)). It is reversing order by Lemma 4.7. Let \( K, K' \in [k, L] \), we deduce from Proposition 4.8 that \( f_{KK'} \leq f_K, f_{K'} \leq f_{K \cap K'} \). Let \( K_1 \in [k, L] \) be such that \( f_{K_1} \leq f_K, f_{K'} \). It follows that \( K, K' \subseteq K_1 \) so that \( KK' \subseteq K_1 \), whence \( f_{K_1} \leq f_{K \cap K'} \) and then, \( f_{KK'} = \text{inf}(f_K, f_{K'}) \). A similar proof shows that \( \text{sup}(f_K, f_{K'}) = f_{K \cap K'} \) \[ \square \]

We denote by \( \mathcal{CA} := \{ K \in [k, L] \mid K \subseteq L \text{ minimal} \} \) the set of co-atoms of \( [k, L] \).

**Proposition 4.10.** Assume that \( k \subseteq L \) is not minimal and let \( K \in [k, L] \). If \( K \in \mathcal{CA} \), there is some \( \beta \in \mathbb{N}_t \) such that \( K = E_\beta \). Moreover, for any \( \beta \in \mathbb{N}_t \), the following conditions are equivalent:

1. \( E_\beta \in \mathcal{CA} \);
2. \( \mathcal{F}_\beta \) is a minimal element in the set \( \{ \mathcal{F}_\gamma \mid \gamma \in \mathbb{N}_t \} \);
3. \( \varphi(E_\beta) \) is a minimal element in \( \mathcal{D} \setminus \{ X - x \} \).

**Proof.** By [32, Lemma 5.10], \( K = E_\beta \) for some \( \beta \in \mathbb{N}_t \) since \( K \) is \( \cap \)-irreducible. Moreover, \( m_\beta(X) = (X - x) \prod_{f_\alpha \in \mathcal{F}_\beta} f_\alpha(X) \) by the definition of \( \mathcal{F}_\beta \).

(1) \( \Rightarrow \) (2) Assume that \( E_\beta \subseteq L \) is minimal. We claim that \( \mathcal{F}_\beta \) is minimal in the poset \( \{ \mathcal{F}_\gamma \mid \gamma \in \mathbb{N}_t \} \). Deny, then there is some \( \beta' \in \mathbb{N}_t \) such that \( \mathcal{F}_\beta' \subseteq \mathcal{F}_\beta \), so that \( m_\beta' \) divides strictly \( m_\beta \). We get \( E_\beta \subseteq E_{\beta'} \subseteq L \), contradicting \( E_\beta \subseteq L \) minimal and (2) holds.
(2) ⇒ (3) Let \( E_\beta \) for some \( \beta \in \mathbb{N}_t \) satisfying (2) and assume that \( \varphi(E_\beta) \) is not minimal in \( D \setminus \{X - x\} \). Then, there is some \( K \in [k, L] \) such that \( f_K \) divides strictly \( m_\beta \). It follows that \( E_\beta \subset K \) by Lemma 4.7. But \( K \) is an intersection of some \( E_\gamma \)'s by Theorem 4.5. In particular, we have \( E_\beta \subset K \subset E_\gamma \) which implies that \( m_\gamma \) divides strictly \( m_\beta \), so that \( \mathcal{F}_\gamma \subset \mathcal{F}_\beta \), a contradiction with (2).

(3) ⇒ (1) Let \( E_\beta \) for some \( \beta \in \mathbb{N}_t \) satisfying (3). Assume that \( E_\beta \subset L \) is not minimal, so that there exists some \( K \in [k, L] \) such that \( E_\beta \subset K \subset L \). Using again Theorem 4.5, we exhibit some \( E_\gamma \) such that \( K \subset E_\gamma \subset L \), giving \( E_\beta \subset K \subset E_\gamma \). Then, \( m_\gamma \) divides strictly \( m_\beta \), contradicting (3) and then, \( E_\beta \in \mathcal{C}A \). \( \square \)

In case \( k \subset L \) is Galois, we can give a characterization of \( \mathcal{C}A \) from the Galois group of the extension.

**Proposition 4.11.** Let \( k \subset L \) be a finite Galois extension with Galois group \( G \) and \( n := [L : k] = \prod_{i \in \mathbb{N}_m} p_i^{\alpha_i} \), the factorization into prime integers \( p_i \).

1. Let \( K \in [k, L] \). Then \( K \in \mathcal{C}A \Leftrightarrow \) there exists some \( i \in \mathbb{N}_m \) such that \( [L : K] = p_i \Leftrightarrow \) there exists some subgroup \( H \) of \( G \) of order \( p_i \) such that \( K \) is the fixed field of \( H \) in \( L \).
2. \( |\mathcal{C}A| \geq m \).

**Proof.** (1) An appeal to the Fundamental Theorem of Galois Theory shows that \( K \in \mathcal{C}A \Leftrightarrow \) the group \( H \) of \( K \)-automorphisms of \( L \) has no proper subgroup \( \Leftrightarrow |H| = p_i \) for some \( i \in \mathbb{N}_m \) since \( |G| = n \Leftrightarrow \) there exists some \( i \in \mathbb{N}_m \) such that \( [L : K] = |H| = p_i \) because \( K \) is the fixed field of \( H \).

(2) For each \( i \in \mathbb{N}_m \), there exists a subgroup of \( G \) of order \( p_i \) and therefore an element of \( \mathcal{C}A \) by (1), which yields \( |\mathcal{C}A| \geq m \). \( \square \)

Since each element of \( \mathcal{C}A \) is some \( E_\beta \), we can reorder them so that \( \mathcal{C}A = \{E_1, \ldots, E_s\} \) with \( s \leq t \).

If \( k \subset L \) is a finite separable field extension, Theorem 4.5 tells us that any \( K \in [k, L] \) is an intersection of some \( E_\beta \)'s, that we can suppose \( \cap \)-irreducible. In order to have a Boolean extension, any irreducible \( E_\beta \) must belong to \( \mathcal{C}A \).

**Remark 4.12.** An \( \cap \)-irreducible element is not necessarily a co-atom. It is enough to take a Galois cyclic extension \( k \subset L \) such that \( [L : k] = p^n, \ n \geq 3 \), where \( p \) is a prime integer. Then the Galois group of the extension is a chain, and so is \( [k, L] \), with \( \ell[k, L] = n \). Any \( K \in [k, L] \) such that \( \ell[k, K] \in \{1, \ldots, n - 2\} \) is \( \cap \)-irreducible but not a co-atom.
We have seen in Lemma 4.7 that for each $K \in [k, L]$, there exists $g(X) = (X - x)g'(X)$, where $g'(X) \in L[X]$ is a product of some of the $f_{\alpha}(X)$, and satisfying $g = f_K$. Conversely, let $g(X) = (X - x)g'(X)$, where $g'(X) \in L[X]$ is a product of some of the $f_{\alpha}(X)$. A necessary and sufficient condition in order that there is $K \in [k, L]$ such that $g = f_K$ is gotten for $k = \mathbb{Q}$ in [36, Remark 6], a result without proof that we supply for an arbitrary field $k$.

**Proposition 4.13.** If $g(X) \in L_a[X]$, there exists $K \in [k, L]$ such that $g = f_K \iff g \in \mathcal{D} \iff g(x) = 0$ and $[L : K_g] = \deg(g)$.

**Proof.** The first equivalence comes from the definition of $\mathcal{D}$. If $g = f_K$ for some $K \in [k, L]$, then, $K = K_g$ by (*). Obviously, $g(x) = 0$. Moreover, $[L : K] = \deg(f_K) = \deg(g) = [L : K_g]$.

Conversely, if $g(x) = 0$ and $[L : K_g] = \deg(g)$ hold, set $K := K_g$. Then, $f_K(X)$ divides $g(X)$ in $K[X]$ since $g(x) = 0$. Moreover, $[L : K] = \deg(f_K) = [L : K_g] = \deg(g)$, so that $g = f_K$.

If $g(X) = X - x$, we get that $L = K$. \qed

This result allows to characterize Boolean and finite separable extensions using only polynomials with the following result.

**Theorem 4.14.** Let $k \subset L := k[x]$ be a finite separable field extension. The following conditions are equivalent:

1. $k \subset L$ is a Boolean extension;
2. For any $K \in [k, L]$, there is a unique subset $T$ of $\mathcal{C}A$ such that $f_K = \sup\{m_\beta \mid E_\beta \in T\}$;
3. For any $g \in \mathcal{D} \setminus \{X - x\}$, there is a unique subset $I \subseteq \mathbb{N}_s$ such that $g = \sup\{m_\beta \mid \beta \in I\}$.

**Proof.** Theorem 3.11, states that $k \subset L$ is Boolean if and only if each $K \in [k, L]$ is of the form $K = \cap_{E_\beta \in T} E_\beta$ for some unique $T \subseteq \mathcal{C}A$.

1. $\Rightarrow$ (2) Assume that $k \subset L$ is a Boolean extension. Let $K \in [k, L]$ and $T := \{E_\gamma \in \mathcal{C}A \mid K = \cap_{E_\gamma \in T} E_\gamma\}$, which is unique. Corollary 4.9 yields that $f_K = \sup\{m_\beta \mid E_\beta \in T\}$. Let $T' \subseteq \mathcal{C}A$ be such that $f_K = \sup\{m_\gamma \mid E_\gamma \in T'\}$. Then, $K = \cap_{E_\gamma \in T'} E_\gamma$ and $T = T'$ follows from the uniqueness property.

2. (2) $\Rightarrow$ (1) Assume that for any $K \in [k, L]$, there is a unique subset $T$ of $\mathcal{C}A$ such that $f_K = \sup\{m_\gamma \mid E_\gamma \in T\}$. This implies that $K = \cap_{E_\gamma \in T} E_\gamma$ by Corollary 4.9. Assume that there is some $T' \neq T$ such that $K = \cap_{E_\gamma \in T'} E_\gamma$ with $T' \subseteq \mathcal{C}A$. It follows that $f_K = \sup\{m_\gamma \mid E_\gamma \in T'\}$ and $T = T'$ because of the assumption on $T$. Therefore, $k \subset L$ is Boolean by Theorem 3.11.

2. $\iff$ (3) Use Corollary 4.9 and the bijection $\varphi$. \qed
Scholium. Here are the different steps in order to check that a finite separable extension \( k \subset L \), with minimal polynomial \( f(X) \), is Boolean according to Theorem 4.14:

1. Decompose \( f(X) \) into irreducible elements of \( L[X] \).
2. Determine the set \( \mathcal{E} \) of principal subfields.
3. Determine \( \mathcal{CA} \) using Proposition 4.10.
4. Determine \( D \) using Proposition 4.13.
5. Check if condition (3) of Theorem 4.14 holds.

Remark 4.15. Let \( k \subset L := k[x] \) be a finite separable Boolean field extension and let \( \mathcal{CA} = \{ E_1, \ldots, E_s \} \) be the set of co-atoms of the extension. Let \( K := k[z] \in k, K \). Then Example 3.3 implies that, if \( K = \bigcap \{ E_\alpha \in Y \} \), where \( Y \subseteq \mathcal{CA} \), we have \( Y = \{ E_\alpha \in \mathcal{CA} \mid z \in E_\alpha \} \). Moreover, \( K^\circ = \bigcap \{ E_\beta \in \mathcal{CA} \setminus Y \} \). But, since the extension is finite separable, there exists \( y \in L \) such that \( K^\circ = k[y] \). Then, \( \mathcal{CA} \setminus Y = \{ E_\beta \in \mathcal{CA} \mid y \in E_\beta \} = \{ E_\beta \in \mathcal{CA} \mid z \notin E_\beta \} \). It follows that \( f_K = \sup(m_\alpha \mid E_\alpha \in Y) \) and \( f_{k[y]} = \sup(m_\beta \mid E_\beta \in \mathcal{CA} \setminus Y) \). We recall that the sup is considered in \( D \), the set of the minimal polynomials of the elements of \( [R,S] \).

Proposition 4.16. A finite separable field extension \( k \subset L := k[x] \) such that \( D = \{ g(X) \in L_u[X] \mid g(x) = 0, \ g(X)|f(X) \text{ in } L[X] \} \) is Boolean. If, in addition \( k \subset L \) is Galois and \( k \) an infinite field, then \( k \subset L \) is minimal of degree 2.

Proof. For \( \alpha \in \mathbb{N}_r \), we have \( g_\alpha(X) = (X - x)f_\alpha(X) \in D \), giving that there exists some \( K \in [k, L] \) such that \( g_\alpha = f_K \) with \( L \neq K \) because \( f_L(X) = X - x \). It follows that \( K \subset L \) is minimal by [32, Lemma 5.7]. Hence, \( K = E_\gamma \) for some \( \gamma \in \mathbb{N}_s \). Let \( K' \in [k, L] \) and set \( f_{K'}(X) := (X - x) \prod_{\alpha \in I} f_\alpha(X) \) for some \( I \subseteq \mathbb{N}_r \). Moreover, \( f_{K'} = \text{lcm}_{\alpha \in I}(\{ m_\alpha \}) \), for a unique \( I \), and then a unique subset \( T = \{ L_\alpha \}_{\alpha \in I} \) of \( \mathcal{CA} \) satisfying the hypotheses of Theorem 4.14. (In fact, the \( L_\alpha \) are all distinct and are the \( E_\beta \).) Therefore, \( k \subset L \) is Boolean and \( \ell[k, L] = r \) by Theorem 3.2, because \( |\mathcal{CA}| = |A| = r \).

Now if \( k \subset L \) is Galois, any \( f_\alpha \) has degree 1. Set \( n := \deg(f) \), so that \( r = n - 1 \), with the previous notation. Then \( \ell[k, L] = n - 1 \) and \( ||k, L|| = 2^{n-1} \) by Theorem 3.2. But \( k \) is infinite, which implies that \( 2^{n-1} = ||k, L|| \leq 2^{n-2} + 1 \) by Proposition 4.4, which gives \( n = 2 \). \( \square \)

There exist finite separable Boolean extensions \( k \subset L \) such that \( D = \{ g(X) \in L_u[X] \mid g(x) = 0, \ g(X)|f(X) \text{ in } L[X] \} \) and \( k \subset L \) is not Galois. Take \( k := \mathbb{Q} \) and \( L := k[x] \), where \( x := \sqrt{2} \). Then \( k \subset L \) is finite separable and not Galois, because not normal. Indeed, the minimal polynomial of \( x \) is \( f(X) = X^3 - 2 = (X - x)(X^2 + xX + x^2) \),
with $X^2 + xX + x^2$ irreducible in $L[X]$. Then, $k \subset L$ is Boolean by Proposition 4.16, in fact minimal by [32, Lemma 5.7].

Here is an example of Boolean extension where we show how the irreducible divisors of the minimal polynomial provides the subextensions of a finite separable extension of fields.

**Example 4.17.** [30, Remark 5.19] Let $k := \mathbb{Q}$, $x := \sqrt[3]{2}$ and set $L := k[x]$, which is a finite separable extension of $k$, but not Galois.

The monic minimal polynomial of $x$ over $k$ is $f(x) := X^6 - 2 = (X-x)(X+x)(X^2+xX+x^2)(X^2-xX+x^2)$, which is its decomposition into irreducible polynomials over $L$. Set $f_1(X) := X + x$, $f_2(X) := X^2 + xX + x^2$, $f_3(X) := X^2 - xX + x^2$ and $g_\alpha(X) := (X - x)f_\alpha(X)$, for $\alpha = 1, 2, 3$. Then, $g_1(X) = X^2 - x^2 = X^2 - \sqrt[3]{2}$, $g_2(X) = X^3 - x^3 = X^3 - \sqrt[3]{2}$ and $g_3(X) = X^3 - 2xX^2 + 2x^2X - x^3$. It follows that $K_1 = k[\sqrt[3]{2}]$, $K_2 = k[\sqrt[2]{2}]$ and $K_3 = L$. Then, $L_1 = K_1$ and $L_2 = K_2$ by [32, Lemma 5.10]. Moreover, no subextension $K \in [k, L]$ is such that $g_3 = f_K$ since $K_3 = L$. Let $K \in [k, L]$ be such that $g_3$ divides strictly $f_K$ in $L[X]$. Then, $[L : K] = \deg(f_K) > 3$ gives that $[L : K] = 6$, so that $K = k = L_3$ because $f_{L_3} = f$ [32, Proposition 5.8]. To end, $L_1 \cap L_2 = k = L_3$. Hence, $[k, L] = \{k, L_1, L_2, K\}$ is a Boolean lattice by Theorem 3.14, and we get the following diagram:

\[ L \]
\[ \rightarrow \quad \leftarrow \quad \rightarrow \]
\[ L_1 \]
\[ \leftarrow \quad \rightarrow \quad \leftarrow \]
\[ k = L_3 \]

**Remark 4.18.** [32, Example 5.17 (2)] Let $k := \mathbb{Q}$ and $L = k[x]$, where $x := \sqrt[3]{2} + \sqrt[3]{3}$. The monic minimal polynomial of $x$ over $k$ is $f(X) = X^4 - 10X^2 + 1 = (X-x)(X+x)(X-x^{-1})(X+x^{-1})$. Set $f_1(X) := X + x$, $f_2(X) := X - x^{-1}$, $f_3(X) := X + x^{-1}$. We get $K_1 = L_1 = k[\sqrt{6}]$, $K_2 = L_2 = k[\sqrt{3}]$ and $K_3 = L_3 = k[\sqrt{2}]$. In particular, $L_\alpha = E_\alpha$ for each $\alpha$ and $L_\alpha \cap L_\beta = k$ for $\alpha \neq \beta$, $\alpha$, $\beta \in \mathbb{N}_3$, which shows that $[k, L] = \{k, L_1, L_2, L_3, L\}$ is not Boolean because $\ell[k, L] = 2$ and $||[k, L]| = 5 \neq 2^2$, but $k \subset L$ is Galois. Therefore, although $k \subset L_\alpha$ is Boolean for $\alpha \in \mathbb{N}_2$, the product $k \subset L_1L_2 = L$ is not Boolean. We also observe that despite the fact that $k \subset L_\alpha$ and $L_\alpha \subset L$ are Boolean for $\alpha \in \mathbb{N}_3$, $k \subset L$ is not Boolean.

However, we are able to characterize Boolean Galois extensions.

**Theorem 4.19.** Let $k \subset L$ be a finite separable extension with normal closure $N$. If $k \subset N$ is a cyclic extension with a square free degree, then $k \subset L$ is a Boolean extension.
In particular, a finite Galois extension \( k \subset L \) with Galois group \( G \) is Boolean if and only if \( k \subset L \) is cyclic whose degree is square free.

Proof. We begin to prove the second part of the Theorem and assume that \( k \subset L \) is Galois. Let \( \mathcal{G} \) be the set of subgroups of \( G \). For \( H, H' \in \mathcal{G} \), we denote by \( <H, H'> \) the subgroup of \( \mathcal{G} \) generated by \( H \) and \( H' \). Define \( \varphi : [k, L] \rightarrow \mathcal{G} \) by \( \varphi(K) := \text{Aut}_K(L) \), the group of \( K \)-automorphisms of \( L \), for each \( K \in [k, L] \). We define \( \psi : \mathcal{G} \rightarrow [k, L] \) by \( \psi(H) := \text{Fix}(H) \), the fixed field of \( H \) in \( L \), for each \( H \in \mathcal{G} \). The Fundamental Theorem of Galois Theory for finite extensions shows that \( \varphi \) and \( \psi \) are reversing order isomorphisms of lattices, with \( \varphi = \psi^{-1} \). Therefore, \([k, L]\) is a Boolean lattice if and only if \( \mathcal{G} \) is a Boolean lattice. To conclude, use [38, Corollary 2] which says that for a finite group \( G \), the lattice of its subgroups is a Boolean lattice if and only if \( G \) is a cyclic group whose order is square free.

Now, if \( k \subset L \) is a finite separable extension whose normal closure is \( N \) such that \( k \subset N \) is a cyclic extension with a square free degree, then \( k \subset L \) is Boolean by Proposition 3.12 because \( k \subset N \) is Boolean. \( \square \)

Remark 4.20. The last part of the Theorem has no converse, unless adding some new assumptions as in Theorem 3.14. Consider Example 4.17. The normal closure \( N \) of the extension \( k \subset L \) is generated over \( k \) by \( x \) and its conjugates, which are the zeroes \( \{\pm x, \pm jx, \pm j^2x\} \), of \( f(X) = X^6 - 2 \), where \( j = (1 + i\sqrt{3})/2 \). Then, \( N = k[x, jx, j^2x] \). Moreover, \( k \subset N \) is Galois. Assume that \( k \subset N \) is Boolean. Then, \( k \subset N \) is a cyclic extension by Theorem 4.19. Set \( K_1' := k[j^2x^2] \subset N \). Since \( (j^2x^2)^3 = 2 \), we get that \([K_1' : k] = 3 = [K_1 : k]\), and we have two subextensions of \( k \subset N \) of degree 3, a contradiction for a cyclic extension (see [6, A V, page 81]). Then, \( k \subset N \) is not Boolean.

The two next examples exhibit Galois Boolean field extensions.

Example 4.21. (1) Let \( n \) be a positive integer, \( n \geq 2 \). In view of [6, A V.152, Exercice 3)], there exists a cyclic extension of \( \mathbb{Q} \) of degree \( n \). It is enough to take a square free integer \( n \) and to use Theorem 4.19 to get a Boolean extension.

(2) Let \( k = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} \) be the finite field with two elements, and let \( K_n \) be the cyclic extension of \( k \) of degree \( n \). Set \( L := K_{30} \). The subfields of \( L \) are the \( K_n \), where \( n \) divides 30. In view of Theorem 4.19, \( k \subset L \) is a Boolean extension, because cyclic of degree a square free integer, and \([k, L] = \{K_n \mid n = 1, 2, 3, 5, 6, 10, 15, 30\}\).

Proposition 4.22. Let \( k \subset L \) be a finite Galois Boolean extension and let \( T, U \in \mathbb{R}, S \). Then \( U = T^\circ \) if and only if \( k \subset T \) and \( k \subset U \) are linearly disjoint with \( L = TU \).
**Proof.** If $k \subset T$ and $k \subset U$ are linearly disjoint, then $T \cap U = k$, so that $U = T^\circ$ since $TU = L$.

Conversely, assume that $U = T^\circ$. We are going to show how $U$ is built from $T$. Since $k \subset L$ is a finite Galois Boolean extension, Theorem 4.19 shows that $k \subset L$ is cyclic, $n := [L : k]$ is square free, and so is $[T : k]$. Set $n = p_1 \cdots p_k p_{k+1} \cdots p_r$ where the $p_i$'s are distinct prime integers ordered such that $m := [T : k] = p_1 \cdots p_k$, and set $l := n/m$. Since $k \subset L$ is cyclic, there exists $V \in [k, L]$ such that $[V : k] = l$. It follows that $(m, l) = ([T : k], [V : k]) = 1$, so that $V \cap T = k$ and $TV := L$. Indeed, $T, V \subset TV \subseteq L$ shows that $m, l$ dividing $[TV : k]$, gives that $[L : k] = n = ml$ divides $[TV : k]$, which leads to $TV = L$. Then, $V = T^\circ = U$. Under these conditions, we have $[TU : k] = [L : k] = ml = [T : k][U : k]$, which shows that $k \subset T$ and $k \subset U$ are linearly disjoint. \hfill $\Box$

We can say more about distributive Galois extension not necessarily Boolean, involving a result from Dobbs-Mullins.

**Proposition 4.23.** Let $k \subset L$ be a finite Galois extension with degree $n(= \prod_{i=1}^{m} p_i^{e_i}$ the factorization into prime integers).

1. [10, Proposition 2.2] If $k \subset L$ is Abelian, then $\ell [k, L] = \sum_{i=1}^{m} e_i$.
2. If $k \subset L$ is distributive, then $k \subset L$ is cyclic, $\ell [k, L] = \sum_{i=1}^{m} e_i$ and $|[k, L]| = \tau(n)$, where $\tau(n)$ is the number of divisors of $n$.
3. If $k \subset L$ is Boolean, $e_i = 1$ for each $i \in \mathbb{N}_m$, $\ell [k, L] = m$ and $|[k, L]| = 2^m$.

**Proof.** (2) Let $G$ be the Galois group of $k \subset L$ and $\mathcal{G}$ be the set of subgroups of $G$. Since $k \subset L$ is distributive, so is $\mathcal{G}$. Then, $G$ is cyclic by [33, Page 97], and so is the extension $k \subset L$. The first part of (2) comes from (1) since a cyclic extension is Abelian. Moreover, there is a bijection between the subgroups of a cyclic group of order $n$ and the divisors of $n$, as there is a bijection between $\mathcal{G}$ and $[k, L]$. This gives the last equality.

(3) Assume that $k \subset L$ is Boolean, then cyclic and $n$ is square free by Theorem 4.19; so that, $e_i = 1$ for each $i$. Hence, $\ell [k, L] = m$ and $|[k, L]| = 2^m$, by Theorem 3.2 since $k \subset L$ is Boolean. \hfill $\Box$

In a recent paper [32], we characterized ring extensions $R \subset S$ of length 2 and gave the value of $|[R, S]|$. It is then easy to characterize an extension of length 2 which is Boolean.

**Proposition 4.24.** Let $R \subset S$ be an FIP extension of length 2. Then $R \subset S$ is Boolean if and only if $|[R, S]| = 4$, and, if and only if one of the following conditions holds:
(1) \(|\text{Supp}(S/R)| = 2\) and \(\text{Supp}(S/R) \subseteq \text{Max}(R)\).

(2) \(R \subset S\) is infra-integral such that \(\text{Supp}(S/R) = \{M\}, \, s^*_R \neq R, S\) and \((R : S) = M\).

(3) \(R \subset S\) is \(t\)-closed integral such that \(\text{Supp}(S/R) = \{M\}, \, M = (R : S) \in \text{Max}(S)\), and one of the following conditions holds:

(a) \(R/M \subset S/M\) is neither radicial nor separable, nor exceptional.

(b) \(R/M \subset S/M\) is a finite separable field extension and \(t = 2\), where \(t\) is the number of principal subfields of \(S/M\) different from \(R/M\).

Proof. Assume that \(R \subset S\) is Boolean. Then \(|[R, S]| = 4\) by Theorem 3.2. Conversely, if \(|[R, S]| = 4\), then \([R, S] = \{R, T, U, S\}\) for some \(U, T \in ]R, S[,\) where \(T\) and \(U\) are incomparable, so that \(R \subset S\) is Boolean by Theorem 3.14. Now the second equivalence comes from [32, Theorem 6.1] which gives the different cases for a length 2 extension \(R \subset S\) to satisfy \(|[R, S]| = 4\). \(\Box\)

Acknowledgments. The authors wish to thank the referee for giving suggestions that improve the paper.

References

[1] A. Ayache, When is the set of intermediate rings a finite boolean algebra?, \textit{Inter. Elec. J. Algebra}, \textbf{8}, (2010), 129–139.

[2] A. Ayache, A constructive study about the set of intermediate rings, \textit{Comm. Algebra}, \textbf{41} (2013), 4637–4661.

[3] A. Ayache, The set of intermediate rings as a boolean algebra, \textit{Comm. Algebra}, \textbf{43} (2015), 1377–1386.

[4] N. Bourbaki; Algèbre Commutative, Chs. 1–2, Hermann, Paris, 1961.

[5] N. Bourbaki, Algèbre Commutative, Chs. 5–6, Hermann, Paris, 1964.

[6] N. Bourbaki, Algèbre, Chs. 4–7, Masson, Paris, 1981.

[7] P.-J. Cahen, D. E. Dobbs and T.G. Lucas, Valuative domains, \textit{J. Algebra Appl.}, \textbf{9} (2010), 43–72.

[8] G. Calugareanu, Lattice concepts of module theory, Springer, New York, 2000.

[9] D. A. Cox, Galois theory, Wiley/Interscience, 2004.

[10] D. E. Dobbs and B. Mullins, On the lengths of maximal chains of intermediate fields in a field extension, \textit{Comm. Algebra}, \textbf{29} (2001), 4487–4507.

[11] D. E. Dobbs, G. Picavet and M. Picavet-L’Hermitte, Characterizing the ring extensions that satisfy FIP or FCP, \textit{J. Algebra}, \textbf{371} (2012), 391–429.

[12] D. E. Dobbs, G. Picavet and M. Picavet-L’Hermitte, Transfer results for the FIP and FCP properties of ring extensions, \textit{Comm. Algebra}, \textbf{43} (2015), 1279–1316.

[13] D. E. Dobbs, G. Picavet and M. Picavet-L’Hermitte, When an extension of Nagata rings has only finitely many intermediate rings, each of those
is a Nagata ring?, *Int. J. Math. Math. Sci.*, **Vol 2014** (2012), Article ID 315919, 13 pp..

[14] D. E. Dobbs, G. Picavet, M. Picavet-L’Hermitte and J. Shapiro, On intersections and composites of minimal ring extensions, *JPJANTA*, **26** (2012), 103–158.

[15] D. E. Dobbs and J. Shapiro, Patching together a minimal overring, *Houston J. Math.*, **36** (2010), 985–995.

[16] T. Donnellan, Lattice Theory, Pergamon Press, Oxford, 1968.

[17] D. Ferrand and J.-P. Olivier, Homomorphismes minimaux d’anneaux, *J. Algebra*, **16** (1970), 461–471.

[18] M. S. Gilbert, Extensions of commutative rings with linearly ordered intermediate rings, Ph. D. dissertation, University of Tennessee, Knoxville, (1996).

[19] R. Gilmer, Multiplicative Ideal Theory, Dekker, New York, 1972.

[20] R. Gilmer and W. Heinzer, On the existence of exceptional field extensions, *Bull. Amer. Math. Soc.*, **74** (1968), 545–547.

[21] G. Grätzer, General Lattice Theory, Academic Press, New York (1978).

[22] I. Kaplansky, Commutative Rings, rev. ed., Univ. Chicago Press, Chicago, 1974.

[23] M. Knebusch and D. Zhang, Manis Valuations and Prüfer Extensions I, Springer, Berlin (2002).

[24] S. Mac Lane, G. Birkhoff, Algebra, American Mathematical Soc., 1999.

[25] C. Nastăsescu and F. Van Oystaeyen, Dimensions of Ring Theory, Mathematics and its applications, D. Reidel Publishing Co., Dordrecht, 1987.

[26] A. Philippe, Extension minimale de corps, Mémoire de D.E.A., Paris (1969), unpublished.

[27] G. Picavet and M. Picavet-L’Hermitte, T-Closedness, pp. 369–386, in: *Non-Noetherian Commutative Ring Theory*, Math. Appl. **520**, Kluwer, Dordrecht, 2000.

[28] G. Picavet and M. Picavet-L’Hermitte, About minimal morphisms, pp. 369–386, in: *Multiplicative Ideal Theory in Commutative Algebra*, Springer, New York, 2006.

[29] G. Picavet and M. Picavet-L’Hermitte, Prüfer and Morita hulls of FCP extensions, *Comm. Algebra*, **43** (2015), 102–119.

[30] G. Picavet and M. Picavet-L’Hermitte, Some more combinatorics results on Nagata extensions, *Palestine J. of Maths*, **5** (2016), 1–15.

[31] G. Picavet and M. Picavet-L’Hermitte, Quasi-Prüfer extensions of rings, pp. 307–336, in: *Rings, Polynomials and Modules*, Springer, 2017.

[32] G. Picavet and M. Picavet-L’Hermitte, Ring extensions of length two, JAA, DOI: 10.1142/S0219498819501743.

[33] S. Roman, Lattices and ordered sets, Springer, New York, 2008.

[34] R. P. Stanley, Enumerative combinatorics, Vol. 1, Second edition, Version of 15 July 2011.

[35] R. G. Swan, On seminormality, *J. Algebra*, **67** (1980), 210–229.

[36] M. van Hoeij, J. Klüners and A. Novocin, Generating subfields, *Journal of Symbolic Computation*, **52** (2013), 17–34.

[37] N. White, Theory of Matroids, Cambridge University Press, London, New York, 1986.
[38] G. Whitson, Finite groups whose subgroup, composition subgroup, or normal subgroup lattice is an ortholattice, *Algebra Universalis*, 8 (1978), 123–127.

Université Clermont Auvergne, CNRS, LMBP, F-63000 CLERMONT-FERRAND, FRANCE

*E-mail address*: gabriel.picavet@uca.fr

*E-mail address*: picavet.mathu (at) orange.fr