Tel Aviv University
The Raymond and Beverly Sackler Faculty of Exact Sciences
School of Mathematical Sciences

Decidability of Large Fields of Algebraic Numbers

Thesis submitted for the degree 'Doctor of Philosophy'

by
Arno Fehm

under the supervision of
Prof. Moshe Jarden

Submitted to the senate of Tel Aviv University
April 2010

This work was done under the supervision of Prof. Moshe Jarden.

Acknowledgements

I want to express my gratitude to my advisor Moshe Jarden for his constant and enduring guidance, and in particular for suggesting to work on this specific topic, for determining the broad framework by proposing to start from the proof of the well known special case $S = \emptyset$ of Theorem I, and for sharing the idea to use Proposition 5.1.2 in the proof of Theorem 5.2.5.

I also thank Bijan Afshordel, Lior Bary-Soroker, Luck Darnière, Ido Efrat, Dan Haran, Martin Hils, Jochen Koenigsmann, Elad Paran, Alexander Prestel, and Martin Ziegler for inspiring and helpful questions and comments.

Most of the writing was done in April 2009 while I was a guest at K. U. Leuven. I thank Jan Denef and the whole algebra section for their hospitality. The Hebrew part would not have been completed without the help of Elad Paran whom I thank for his time and efforts.

My work on this thesis was funded by the European Union FP6 Marie Curie network 'Galois Theory and Explicit Methods' (MRTN-CT-2006-035495). I thank in particular our network coordinator Bart de Smit and the scientist in charge of the Tel Aviv node Moshe Jarden for their efforts in struggling with the bureaucracy, and my fellow ESRs María Teresa Aranés, Florian Heiderich, Mirjam Jöllenbeck, Jan Tuitman, and Michael Wibmer for our many enjoyable meetings.

Finally, for the overwhelming support and friendship that I received from them during my stay in Israel I am deeply indebted and grateful to Dan, Elad, Eli, and Lior.

Contents

Introduction

Historical Overview

It is a central question in mathematics whether a given mathematical task that is known to have a solution can be solved *effectively*. For example, one can ask if it is possible to effectively factor an integer into its prime factors, that is, if there exists an algorithm that takes an integer as input and gives its list of prime factors as output. One easily sees that such an algorithm exists, but this is not so clear in other cases. For example, the tenth problem of Hilbert's list of 23 open problems from 1900 proposed the following task.

> *Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlenkoeffizienten sei vorgelegt: man soll ein Verfahren angeben, nach welchem sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

In other words, Hilbert asks for an algorithm that decides whether a polynomial equation (in several variables) with coefficients in the ring of integers $\mathbb{Z}$ has a solution in $\mathbb{Z}$. It took 70 years until Matijasevich could show that the task posed by Hilbert cannot be solved: There exists no such algorithm. It is an important unsolved question until today, whether this remains true if we replace the ring $\mathbb{Z}$ by its quotient field $\mathbb{Q}$, i.e. if we ask for rational solutions of polynomial equations with rational coefficients.

Instead of considering equations over a ring or field R, and asking which of these equations have a solution in R, one may more generally consider first-order formulas in the language of rings and ask which of these are satisfied in R. One says that R is *decidable*, or that the complete theory of R is decidable, if there exists an algorithm that determines whether a given first-order sentence holds in R or not.

In 1949, J. Robinson proved that the field $\mathbb{Q}$ of rational numbers is undecidable. A few years later, she generalized this result to number fields, i.e. finite extensions of $\mathbb{Q}$. On the other end, results of Tarski from 1948 show that the field $\mathbb{C}$ of complex numbers and the field $\mathbb{R}$ of real numbers have a decidable theory. In 1965, Ax-Kochen and Ershov

independently presented the – at that time surprising – result that also the theory of the field of p-adic numbers $\mathbb{Q}_p$ is decidable.

Let us now focus on results about algebraic fields, that is, fields lying between $\mathbb{Q}$ and the algebraic closure $\tilde{\mathbb{Q}}$ of $\mathbb{Q}$. The results mentioned above also show that the field of algebraic numbers $\tilde{\mathbb{Q}}$, the field of real algebraic numbers

$$\mathbb{R}_{\mathrm{alg}} = \mathbb{R} \cap \tilde{\mathbb{Q}},$$

and the field of p-adic algebraic numbers

$$\mathbb{Q}_{p,\mathrm{alg}} = \mathbb{Q}_p \cap \tilde{\mathbb{Q}}$$

are decidable. So, roughly speaking, fields 'close to $\mathbb{Q}$' are undecidable, whereas fields 'close to $\tilde{\mathbb{Q}}$' tend to be decidable. Therefore, it is a challenge to find decidable algebraic fields which are as 'far away from $\tilde{\mathbb{Q}}$' (or as 'close to $\mathbb{Q}$') as possible.

Each of the following four theorems makes use of what is called a *geometric local-global principle*, or Hasse principle. Roughly speaking, a field K satisfies a (geometric) local-global principle if a variety over K has a K-rational point if and only if it has a rational point over each field in a family of localizations of K. These localizations can be, for example, completions of K with respect to a family of absolute values on K. If one can decide whether an equation over K has solutions in these localizations, then a local-global principle may allow to decide whether an equation over K has a solution in K. For an extensive survey on the use of local-global principles in decidability proofs see [Dar00a].

A number field K is called totally real if every embedding of K into $\mathbb{C}$ maps K into $\mathbb{R}$. Thus the field of totally real algebraic numbers

$$\mathbb{Q}_{\mathrm{tr}} = \bigcap_{\tau \in \mathrm{Gal}(\mathbb{Q})} (\mathbb{R}_{\mathrm{alg}})^{\tau},$$

where $\mathrm{Gal}(\mathbb{Q}) = \mathrm{Aut}(\tilde{\mathbb{Q}}/\mathbb{Q})$ is the absolute Galois group of $\mathbb{Q}$, is the maximal Galois extension of $\mathbb{Q}$ in $\mathbb{R}$.

Fried-Haran-Völklein combined their results on the absolute Galois group of $\mathbb{Q}_{\mathrm{tr}}$ with the fact that the field $\mathbb{Q}_{\mathrm{tr}}$ satisfies a local-global principle (a result of Moret-Bailly and Green-Pop-Roquette) to prove the following:

THEOREM A ([FHV94]). *The complete theory of the field of totally real algebraic numbers $\mathbb{Q}_{\mathrm{tr}}$ is decidable.*

Ershov proved a p-adic analogue of this. Let

$$\mathbb{Q}_{\mathrm{tot},p} = \bigcap_{\tau \in \mathrm{Gal}(\mathbb{Q})} (\mathbb{Q}_{p,\mathrm{alg}})^{\tau}$$

be the maximal Galois extension of $\mathbb{Q}$ in $\mathbb{Q}_p$. If S is a set of prime numbers, let

$$\mathbb{Q}_{\mathrm{tot},S} = \bigcap_{p\in S} \mathbb{Q}_{\mathrm{tot},p}.$$

Using the same results of Moret-Bailly and Green-Pop-Roquette, and a result of Pop on the absolute Galois groups of the fields $\mathbb{Q}_{\mathrm{tot},S}$, Ershov was able to prove decidability of these fields.

THEOREM B ([Ers96b]). *Let S be a finite set of prime numbers. Then the complete theory of the field $\mathbb{Q}_{\mathrm{tot},S}$ is decidable.*

A different line of research on decidable theories of algebraic fields started much earlier. Instead of investigating the complete theory of a single field, one can try to determine the probability that a given first-order sentence holds in a randomly chosen member of a certain class of algebraic fields. Let K be a number field, and let e be a nonnegative integer. For an e-tuple

$$\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$$

of elements of the absolute Galois group $\mathrm{Gal}(K) = \mathrm{Aut}(\tilde{K}/K)$ of K, denote by

$$\tilde{K}(\boldsymbol{\sigma}) = \left\{ x \in \tilde{K} \colon \sigma_1(x) = \cdots = \sigma_e(x) = x \right\}$$

the fixed field of $\boldsymbol{\sigma}$ in $\tilde{K}$. Since $\mathrm{Gal}(K)^e$ is a compact group, it admits a unique normalized Haar measure. Thus one can ask for the probability that a given sentence holds in $\tilde{K}(\boldsymbol{\sigma})$, where $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$. The set of sentences which hold in $\tilde{K}(\boldsymbol{\sigma})$ with probability one is called the theory of almost all $\tilde{K}(\boldsymbol{\sigma})$.

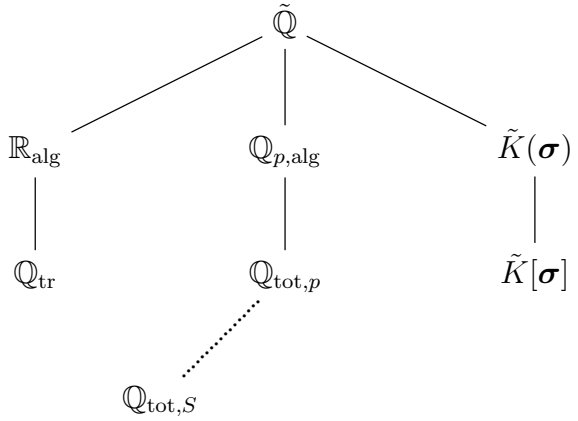
Using a result on the absolute Galois groups of these fields and a (degenerated) local-global principle they satisfy (both by Jarden), Jarden-Kiehne proved the following:

THEOREM C ([JK75]). *The theory of almost all fields $\tilde{K}(\boldsymbol{\sigma})$, $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, is decidable.*

Denote by $\tilde{K}[\boldsymbol{\sigma}]$ the maximal Galois extension of K contained in $\tilde{K}(\boldsymbol{\sigma})$. After determining the absolute Galois groups of these fields, and showing that they satisfy a local-global principle, Jarden was also able to prove the following:

THEOREM D ([Jar97]). *The theory of almost all fields $\tilde{K}[\boldsymbol{\sigma}]$, $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, is decidable.*

The decidable theories of algebraic fields mentioned so far can be summarized in the following diagram.



The Present Work

In this work we combine and generalize the four theorems mentioned above. Let S be a finite set of absolute values on a number field K. For $\mathfrak{p} \in S$ we denote by $K_{\mathrm{tot},\mathfrak{p}}$ the maximal Galois extension of K in a completion $\hat{K}_{\mathfrak{p}}$ of K with respect to the absolute value $\mathfrak{p}$, and we let

$$K_{\mathrm{tot},S} = \tilde{K} \cap \bigcap_{\mathfrak{p} \in S} K_{\mathrm{tot},\mathfrak{p}}$$

be the field of *totally S-adic numbers* over K. If $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, let

$$K_{\mathrm{tot},S}(\boldsymbol{\sigma}) = K_{\mathrm{tot},S} \cap \tilde{K}(\boldsymbol{\sigma})$$

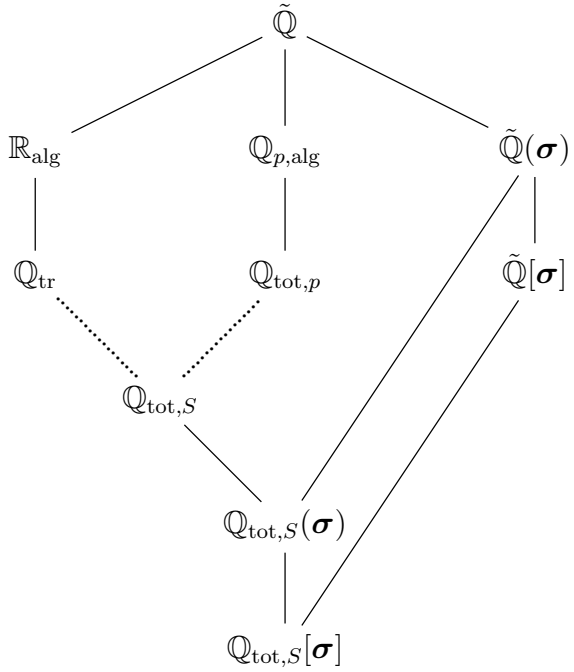
be the fixed field of $\boldsymbol{\sigma}$ in $K_{\mathrm{tot},S}$, and let

$$K_{\mathrm{tot},S}[\boldsymbol{\sigma}] = K_{\mathrm{tot},S} \cap \tilde{K}[\boldsymbol{\sigma}]$$

be the maximal Galois extension of K in $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$. Note the following special cases of these definitions, and compare with the corresponding theorems above.

(A) If $K = \mathbb{Q}$, $e = 0$, and $S = \{|\cdot|\}$ consists of the archimedean absolute value on $\mathbb{Q}$ only, then $K_{\mathrm{tot},S}(\boldsymbol{\sigma}) = \mathbb{Q}_{\mathrm{tr}}$.
(B) If $K = \mathbb{Q}$, $e = 0$, and S consists of finitely many non-archimedean absolute values on $\mathbb{Q}$, then $K_{\mathrm{tot},S}(\boldsymbol{\sigma}) = \mathbb{Q}_{\mathrm{tot},S}$.
(C) If $S = \emptyset$, then $K_{\mathrm{tot},S}(\boldsymbol{\sigma}) = \tilde{K}(\boldsymbol{\sigma})$.
(D) If $S = \emptyset$, then $K_{\mathrm{tot},S}[\boldsymbol{\sigma}] = \tilde{K}[\boldsymbol{\sigma}]$.

The special case $K = \mathbb{Q}$ can be pictured as follows.



In a series of papers, Haran-Jarden-Pop recently determined the structure of the absolute Galois groups of the fields $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$ and $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ (for almost all $\boldsymbol{\sigma}$) as a free product of a free profinite group and an infinite free product of local factors. Moreover, Jarden-Razon and Geyer-Jarden proved that these fields satisfy a certain geometric local-global principle – they are PSC. Making use of these two algebraic results, we prove the following two theorems.

THEOREM I. *Let S be a finite set of absolute values on a number field K, and let e be a nonnegative integer. Then the theory of almost all fields $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$, $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, is decidable.*

THEOREM II. *Let S be a finite set of absolute values on a number field K, and let e be a nonnegative integer. Then the theory of almost all fields $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$, $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, is decidable.*

In fact, in both cases we prove more, cf. Theorem 4.6.7 and Theorem 5.5.4. We show that the probability that a given sentence holds in $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$ resp. $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ can be recursively computed, and we prove Theorem I in a more general setting with K replaced by a countable Hilbertian field of characteristic zero satisfying some recursivity assumptions.

Our proof follows the pattern of the proof of Jarden-Kiehne mentioned above. A key step is to find an axiomatization of the theories in question. That is, to give some algebraic properties that characterize the models of the theory among all fields, and to show that these properties can be formulated by first-order sentences.

One of these algebraic properties is the PSC property. Therefore, in Chapter 2 we develop a model theory of a quite general class of PSC fields, which we call PSCC. In particular, we show that the class of PSCC fields is elementary.

A second algebraic property we use in our axiomatization is concerned with the absolute Galois groups. We construct 'group piles' by adding local objects to the absolute Galois groups. The main difference between our treatment and the work of Haran-Jarden-Pop is that in our model-theoretic situation only the 'local part' of the group pile is accessible, while the 'free part' is not. This causes some difficulties, which we overcome by working with certain characteristic quotients of the group piles. This is done in Chapter 3.

The proofs of Theorem I and Theorem II are carried out in Chapter 4 and Chapter 5, respectively. Chapter 1 summarizes some basic results on real closed fields, p-adically closed fields, and profinite groups.

CHAPTER 1

Preliminaries and Notation

1.1. Notation

By $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\hat{\mathbb{Q}}_p$, $\mathbb{F}_q$ we denote the field of rational numbers, the field of real numbers, the field of complex numbers, the field of p-adic numbers, and the finite field with q elements, respectively. By $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_{\geq 0}$ we denote the set of positive integers, the ring of integers and the set of nonnegative integers, respectively. Every ring and every semiring is commutative with 1. If R is a ring, we denote by $R^\times$ the group of invertible elements of R.

If K is a field, we denote by $\tilde{K}$ a fixed algebraic closure of K, by K_s the separable closure of K in $\tilde{K}$, and by $\mathrm{Gal}(K) = \mathrm{Gal}(K_s/K)$ its absolute Galois group.

The cardinality of a set X is denoted by $|X|$. A set is countable if and only if it is countably infinite or finite. By ω we denote both the smallest infinite ordinal number and the smallest infinite cardinal number. By $\cup$ we denote the disjoint union of sets, and also the direct sum (i.e. coproduct) of topological spaces. We use the term compact as a synonym for quasi-compact.

Varieties are geometrically irreducible and geometrically reduced. If V is a variety defined over a field K, we denote by $K(V)$ the function field of V over K.

1.2. Model Theory of Fields and Recursion Theory

We recall some notions from model theory and fix the logical setting we are working in.

We only consider classical first-order logic. The structures we consider are only fields, and expansions of fields by additional structure. For basic model theoretic notions like language, structure, formula, model, and satisfaction, see for example [Mar02] or [FJ08, Chapter 7].

The **language of rings** is

$$\mathcal{L}_{\mathrm{ring}} = \{+, -, \cdot, 0, 1\},$$

where $+$ and $\cdot$ are binary function symbols, $-$ is a unary function symbol, and 0 and 1 are constant symbols.

Let $\mathcal{L}$ be a language containing $\mathcal{L}_{\mathrm{ring}}$. If K is an $\mathcal{L}$-structure (i.e. a field with possibly some extra structure), and C is a subset of K, denote

by

$$\mathcal{L}(C) = \mathcal{L} \cup \{c_x \colon x \in C\}$$

the language $\mathcal{L}$ augmented by constant symbols for the elements in C. Every $\mathcal{L}$-structure F containing K is then naturally an $\mathcal{L}(C)$-structure, and K is naturally embedded into every $\mathcal{L}(K)$-structure that is a model of the positive diagram of K, [FJ08, 7.3.1]. We write $\equiv_C$ for elementary equivalence of $\mathcal{L}(C)$-structures.

If $\varphi(x_1, \ldots, x_n)$ is an $\mathcal{L}$-formula in n free variables, and K is an $\mathcal{L}$-structure, we denote by

$$\varphi(K) = \{\mathbf{a} \in K^n \colon K \models \varphi(\mathbf{a})\}$$

the subset **defined** by φ in K.

An $\mathcal{L}$-theory T has **quantifier elimination** if every $\mathcal{L}$-formula is equivalent modulo T to a quantifier free formula. It is **complete** if for every $\mathcal{L}$-sentence φ it holds that $T \models \varphi$ or $T \models \neg\varphi$. It is **model complete** if every extension $K \leq L$ of models of T is elementary, i.e. $K \prec L$. An $\mathcal{L}$-structure K is **$\aleph_1$-saturated** if for every countable subset $C \subseteq K$ the following holds: If Σ is a set of $\mathcal{L}(C)$-formulas in countably many free variables such that every finite subset of Σ is satisfied in K, then Σ is satisfied in K.

Lemma 1.2.1 (Löwenheim-Skolem downwards). *Let $\mathcal{L}$ be a countable language, and let K be an $\mathcal{L}$-structure. If $C \subseteq K$ is a countable subset, then there exists a countable elementary substructure $K_0 \prec K$ with $C \subseteq K_0$.*

Proof. See [FJ08, 7.4.2]. □

If $\mathcal{D}$ is an ultrafilter on a set I, and K_i is an $\mathcal{L}$-structure for each $i \in I$, then the **ultraproduct**

$$\prod_{i \in I} K_i/\mathcal{D}$$

is an $\mathcal{L}$-structure with universe the Cartesian product $\prod_{i\in I} K_i$ modulo the relation $\sim$ given by $(x_i)_{i\in I} \sim (y_i)_{i\in I}$ if and only if $\{i \in I \colon x_i = y_i\} \in \mathcal{D}$, c.f. [FJ08, Chapter 7.7].

Lemma 1.2.2 (Łoś's theorem). *If φ is an $\mathcal{L}$-sentence, then*

$$\prod_{i \in I} K_i/\mathcal{D} \models \varphi$$

if and only if

$$\{i \in I \colon K_i \models \varphi\} \in \mathcal{D}.$$

Proof. See [FJ08, 7.7.1]. □

A set $X \subseteq \mathbb{N}^n$ is **recursive** if the characteristic function of X is a recursive function in the usual sense, see for example [FJ08, Chapter

8.5]. If $\mathcal{L}$ is a countable language with a fixed embedding $\mathcal{L} \to \mathbb{N}$, then an $\mathcal{L}$-theory T is **decidable** (or recursive) if the set T, identified with a subset of $\mathbb{N}$ via a Gödel numbering, is recursive, [FJ08, Chapter 8.6].

A **presented field** is a countable field K together with an injection $\rho\colon K \to \mathbb{N}$ such that the images of the graphs of addition and multiplication are recursive.[1] If $\mathcal{L}$ is a finite language containing $\mathcal{L}_{\mathrm{ring}}$, then the injection $\rho\colon K \to \mathbb{N}$ induces an injection $\mathcal{L}(K) \to \mathbb{N}$. We refer to this injection when we call an $\mathcal{L}(K)$-theory decidable.

If K is a presented field, one can inject the ring of polynomials $K[X]$ into $\mathbb{N}$ via a recursive pairing function $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$. We say that K has a **splitting algorithm** if the set of irreducible polynomials in $K[X]$ is a recursive subset of $K[X]$. If K has a splitting algorithm, then one can recursively factor elements of $K[X]$ into irreducible factors.[2]

1.3. Profinite Groups and Profinite Spaces

A **profinite group** G is a topological group with a totally disconnected compact Hausdorff topology. Equivalently, it is an inverse limit of finite groups, [RZ00, 2.1.3]. A subgroup of G is open if and only if it is closed and of finite index in G, [FJ08, 1.2.1(a)], and each closed subgroup is the intersection of open subgroups, [FJ08, 1.2.3]. The category of profinite groups is closed under quotients, direct products, inverse limits, [FJ08, 1.2.6], and fibre products, [FJ08, 22.2.1]. Note: We always consider profinite groups as topological groups, so in particular homomorphisms between profinite groups are continuous homomorphisms. By $H \leq G$ (resp. $H \lhd G$) we indicate that H is a closed (resp. normal closed) subgroup of G. If $X \subseteq G$, we denote by $\langle X \rangle$ the closed subgroup generated by X in G. We use the symbol 1 to denote both the unit element of G, and the trivial subgroup $\{1\} \leq G$.

A subset $X \subseteq G$ **converges to 1** if $X \smallsetminus H$ is finite for each open normal subgroup $H \lhd G$. We denote by $\mathrm{rank}(G)$ the (profinite) **rank** of G, that is, the minimal cardinality of a set of (topological) generators converging to 1, cf. [FJ08, 17.1.3]. If $G \to H$ is an epimorphism of profinite groups, then $\mathrm{rank}(H) \leq \mathrm{rank}(G)$, [FJ08, 17.1.4]. We say that G is **finitely generated** if $\mathrm{rank}(G) < \infty$.

Proposition 1.3.1 (Gaschütz). *Let $\pi\colon G \to H$ be an epimorphism of profinite groups with $\mathrm{rank}(G) \leq e \in \mathbb{Z}_{\geq 0}$. Let $h_1, \ldots, h_e$ be a system of generators of H. Then there exists a system of generators $g_1, \ldots, g_e$ of G such that $\pi(g_i) = h_i$, $i = 1, \ldots, e$.*

Proof. See [FJ08, 17.7.2]. □

[1] Note that our definition differs from [FJ08, 19.1.1] as we do not assume the images of the graphs to be *primitive* recursive. Furthermore, we refrain from using meta-mathematical concepts like 'explicitly given'.

[2] So this definition coincides with [FJ08, 19.1.2], except that also here we replace *primitive recursive* by *recursive* and drop properties like 'explicitly given'.

LEMMA 1.3.2. *Let G, H be profinite groups, and assume that G is finitely generated.*

(1) *If G and H have the same finite quotients, then $G \cong H$.*
(2) *If every finite quotient of H is a quotient of G, then H is a quotient of G.*
(3) *If $G \cong H$, then any epimorphism $G \to H$ is an isomorphism.*

PROOF. See [FJ08, 16.10.7, 16.10.8]. □

A profinite group F is **free** on a set of generators $X \subseteq F$ if $\langle X \rangle = F$, X converges to 1, and for each map $\varphi\colon X \to G$ into a profinite group G for which $\langle \varphi(X) \rangle = G$ and $X \smallsetminus \varphi^{-1}(H)$ is finite for each open normal subgroup $H \triangleleft G$, there exists a unique epimorphism $\hat{\varphi}\colon F \to G$ extending φ. If κ is a cardinal number, we denote by $\hat{F}_\kappa$ the free profinite group on a set of κ generators. It exists and is unique up to isomorphism, [FJ08, 17.4.7]. In particular, $\hat{F}_\omega$ is the free profinite group on a countably infinite set of generators.

If G, H are profinite groups, the **free product** $G * H$ is a profinite group determined up to isomorphism by the following properties: G and H are closed subgroups of $G * H$ with $G * H = \langle G, H \rangle$, and each pair $\alpha\colon G \to C$, $\beta\colon H \to C$ of homomorphisms of profinite groups extends uniquely to a homomorphism $\gamma\colon G * H \to C$, [FJ08, 22.4.9].

LEMMA 1.3.3. *If $x \in G * H$ and $G^x \cap G \neq 1$, then $x \in G$.*

PROOF. See [RZ00, 9.1.12]. □

If L/K is a Galois extension, then $\mathrm{Gal}(L/K)$ is a profinite group in the **Krull topology**. A basis for the neighbourhoods of 1 is given by the open subgroups $\mathrm{Gal}(L/N)$, where N/K is a finite Galois subextension of L/K, [FJ08, Chapter 1.3]. Galois correspondence establishes a bijection between the closed subgroups of $\mathrm{Gal}(L/K)$ and the intermediate fields of L/K, [FJ08, 1.3.1]. If F/K is an extension, then the restriction map $\mathrm{res}_{F_s/K_s}\colon \mathrm{Gal}(F) \to \mathrm{Gal}(K)$ is continuous.

LEMMA 1.3.4. *If $K \equiv L$ are elementarily equivalent fields and $\mathrm{Gal}(K)$ is finitely generated, then $\mathrm{Gal}(K) \cong \mathrm{Gal}(L)$.*

PROOF. See [FJ08, 20.4.6]. □

Like any compact group, a profinite group admits a unique normalized **Haar measure**, i.e. a (left and right) invariant complete regular probability measure, cf. [FJ08, Chapter 18].

A **profinite space** is a totally disconnected compact Hausdorff space. Profinite spaces can be characterized as inverse limits of finite discrete spaces, or as zero-dimensional compact Hausdorff spaces, [RZ00, 1.1.12]. Here, a topological space is called **zero-dimensional** if it has a basis for its topology consisting of open-closed sets. For

example, the underlying space of a profinite group is a profinite space. Any product or finite direct sum (i.e. coproduct) of profinite spaces is a profinite space, and a subspace of a profinite space is profinite if and only if it is closed. Since profinite spaces are compact Hausdorff, any continuous map between profinite spaces is closed, and any continuous bijection of profinite spaces is a homeomorphism.

LEMMA 1.3.5. *Let X be a profinite space with a subbasis $\mathcal{B}$ which is closed under complements. Then the following are equivalent.*

(1) *$\mathcal{B}$ is closed under finite intersections.*
(2) *For all $U, V \in \mathcal{B}$, $U \cap V \in \mathcal{B}$.*
(3) *Every open-closed subset of X is in $\mathcal{B}$.*

PROOF. See [Pre84, 6.6]. □

LEMMA 1.3.6. *If a profinite group G acts continuously on a profinite space X, then the quotient space X/G is profinite and the quotient map $X \to X/G$ is continuous and closed.*

PROOF. By [Bou98, III.4 Prop. 2, Prop. 3], X/G is compact Hausdorff. Moreover, it is zero-dimensional, since if $U \subseteq X$ is open-closed, then the G-closure $U^G \subseteq X$ is also open-closed. Indeed, U^G is the union of homeomorphic copies of U, so it is open, and it is the image of the closed map $U \times G \to X$ given by $(x, g) \mapsto x^g$, so it is closed. □

A **Cantor space** is a perfect second-countable profinite space. Here, a topological space is called **perfect** if it has no isolated points, and **second-countable** if it has a countable basis for its topology. A finite direct sum of Cantor spaces is a Cantor space, and a closed subspace of a Cantor space is a Cantor space if and only if it is perfect. All Cantor spaces are homeomorphic to each other, [Kec94, 7.4], so we also talk about *the* Cantor space C.

LEMMA 1.3.7. *Let $\varphi\colon X \to A$, $\alpha\colon B \to A$ be continuous surjections of topological spaces, where A is discrete, α has finite fibres, and X is zero-dimensional perfect Hausdorff. Then there exists a continuous surjection $\lambda\colon X \to B$ with $\alpha \circ \lambda = \varphi$.*

PROOF. Let $a \in A$. Since A is discrete, $X_a = \varphi^{-1}(a)$ is a nonempty open-closed subset of X. Since X is Hausdorff and has no isolated points, X_a is infinite. The fibre $B_a = \alpha^{-1}(a)$ is finite by assumption. Let $B_a = \{b_1, \dots, b_n\}$, and choose distinct elements $x_1, \dots, x_n \in X_a$. Since X is zero-dimensional Hausdorff, there are open-closed subsets $X_{a,1}, \dots, X_{a,n}$ of X_a with $x_i \in X_{a,i}$ and $X_a = \bigcup_{i=1}^n X_{a,i}$.

Now define λ on X_a by $\lambda|_{X_{a,i}} = b_i$, and do this for all $a \in A$. Since $x_i \in X_{a,i}$ for every i, λ is surjective. Since each $X_{a,i}$ is open-closed, λ is continuous. Since for $x \in X_{a,i}$, $\varphi(x) = a$ and $\alpha(\lambda(a)) = \alpha(b_i) = a$, $\alpha \circ \lambda = \varphi$. □

1.4. Real Closed Fields

We recall the notion of real closed fields and quote some well known results from [Pre84].

Let K be a field. A **positive cone** of K is a semiring $P \subseteq K$ such that $P \cup (-P) = K$ and $P \cap (-P) = \{0\}$. An **ordering** of K is a total order $\leq$ on K such that $\{x \in K : x \geq 0\}$ is a positive cone. The map that assigns to an ordering the corresponding positive cone induces a natural bijection between the orderings of K and the positive cones of K. An **ordered field** is a field K together with an ordering. A **pre-positive cone** of K is a semiring $P \subseteq K$ such that $K^2 \subseteq P$ and $-1 \notin P$.

LEMMA 1.4.1. *Each pre-positive cone of K is the intersection of the positive cones of K containing it. In particular, each pre-positive cone of K is contained in a positive cone of K.*

PROOF. See [Pre84, 1.6]. □

An ordering $\leq$ of K is **archimedean** if for every $x \in K$ there exists $y \in \mathbb{N} \subseteq K$ with $x < y$. Any archimedean ordered field can be embedded into $\mathbb{R}$ (as an ordered field), [Pre84, 1.23], hence the ordering of an ordered algebraic extension of an archimedean ordered field is archimedean.

A field is **real closed** if it has an ordering but each proper algebraic extension has no ordering. A real closed field K has a unique ordering, given by the positive cone K^2, [Pre84, 3.2]. A real closed field F is a **real closure** of an ordered field K if F is an algebraic extension of K and the unique ordering of F extends the ordering of K. Any ordered field K has a real closure, which is unique up to K-isomorphism, [Pre84, 3.10]. If L is a finite extension of an ordered field K, then the extensions of the ordering of K to L bijectively correspond to the K-embeddings of L into a fixed real closure of K, [Pre84, 3.12].

LEMMA 1.4.2. *A field which is algebraically closed in a real closed field is real closed.*

PROOF. See [Pre84, 3.13]. □

PROPOSITION 1.4.3 (Artin-Schreier). *A field K is real closed if and only if* $\mathrm{Gal}(K) \cong \mathbb{Z}/2\mathbb{Z}$.

PROOF. This follows from [Lan02, VI.9.3] and [Pre84, 3.3]. □

LEMMA 1.4.4. *Let V be an affine variety defined over a real closed field K. Then V has a simple K-rational point if and only if the ordering of K extends to an ordering of $K(V)$.*

PROOF. See [Lan02, XI.3.1, XI.3.6] or [Pre81, 0.4]. □

The **language of ordered rings**

$$\mathcal{L}_{\leq} = \mathcal{L}_{\text{ring}} \cup \{\leq\}$$

is the language of rings augmented by a binary relation symbol $\leq$, which is interpreted as the ordering of an ordered field.

PROPOSITION 1.4.5 (Tarski). *The $\mathcal{L}_{\leq}$-theory of real closed ordered fields has quantifier elimination, is model complete, complete, and decidable.*

PROOF. See [Mar02, 3.3.15, 3.3.16]. □

1.5. Valued Fields

We recall some basic notions from valuation theory. For more details see [FJ08, Chapter 2], [Efr06], or [EP05].

A **valuation** on K is a Krull valuation on K, i.e. an epimorphism $v\colon K^\times \to \Gamma$ from the (multiplicative) abelian group $K^\times$ onto an ordered (additive) abelian group Γ that satisfies $v(a+b) \geq \min\{v(a), v(b)\}$ for all $a, b \in K^\times$. We let $v(0) = \infty$ and $\gamma < \infty$ for all $\gamma \in \Gamma$. The group Γ is the **value group** of v. The **valuation ring** of v is $\mathcal{O}_v = \{x \in K\colon v(x) \geq 0\}$. Two valuations are **equivalent** if their valuation rings are equal. The valuation ring $\mathcal{O}_v$ is a local ring with maximal ideal $\mathfrak{m}_v = \{x \in K\colon v(x) > 0\}$, and $\bar{K}_v = \mathcal{O}_v/\mathfrak{m}_v$ is the **residue field** of v.

An ordered abelian group Γ is of **rank one** if it has no non-trivial proper convex subgroup, and **discrete** if it has a smallest positive element, i.e. if Γ is discrete in the order topology. A valuation v on K is of rank one resp. discrete if the value group $v(K^\times)$ has this property. We normalize every discrete valuation v such that $\mathbb{Z}$ is a convex subgroup of the value group. In particular, 1 denotes the smallest positive element of the value group.

LEMMA 1.5.1 (Artin-Whaples, Weak Approximation Theorem). *Let $v_1, \ldots, v_n$ be pairwise inequivalent discrete rank one valuations on K, and let $\leq_1, \ldots, \leq_m$ be pairwise distinct archimedean orderings of K. Let $x_1, \ldots, x_n, y_1, \ldots, y_m \in K$, $\epsilon \in (K^\times)^2$, and $n \in \mathbb{Z}$. Then there exists $x \in K$ such that for $1 \leq i \leq n$,*

$$v_i(x - x_i) > n,$$

and, for $1 \leq j \leq m$,

$$x_j - \epsilon^2 \leq x \leq x_j + \epsilon^2.$$

PROOF. See [EP05, 1.1.3]. □

Let v be a valuation on K and F/K a field extension. Then v can be extended to a valuation w on F, [EP05, 3.1.1]. One calls $e_{w/v} = (w(F^\times) : v(K^\times))$ the **ramification index** and $f_{w/v} = [\bar{F}_w : \bar{K}_v]$ the **residue degree**. If F/K is algebraic, then $w(F^\times)$ is contained in

the divisible hull of $v(K^\times)$, [EP05, 3.2.4]. If F/K is Galois, then the extensions of v to F are conjugate over K, [EP05, 3.2.15].

LEMMA 1.5.2 (Fundamental inequality). *Let v be a valuation on K, and let $w_1, \ldots, w_n$ be all inequivalent extensions of v to a finite extension L of K. Then the following inequality holds.*

$$\sum_{i=1}^{n} e_{w_i/v} f_{w_i/v} \leq [L : K].$$

If v is discrete of rank one and L/K is separable, then equality holds.

PROOF. See [EP05, 3.3.4, 3.3.5]. □

If v is a valuation on K, we say that (K, v) is a **valued field**. A valued field (K, v) is **Henselian** if v extends uniquely to $\tilde{K}$. Every valued field (K, v) has a minimal algebraic extension which is Henselian, its **Henselization**. It is unique up to K-isomorphism, [EP05, 5.2.2]. If (F, w) is the Henselization of (K, v), then the extension w/v is **immediate**, i.e. $e_{w/v} = f_{w/v} = 1$, [EP05, 5.2.5].

LEMMA 1.5.3 (Hensel-Rychlik). *Let v be a Henselian valuation on K. If $f \in \mathcal{O}_v[X]$ and $a \in \mathcal{O}_v$ with $v(f(a)) > 2v(f'(a))$, then there exists $\alpha \in \mathcal{O}_v$ with $f(\alpha) = 0$ and $v(a - \alpha) > v(f'(a))$.*

PROOF. See [EP05, 4.1.3(5)]. □

LEMMA 1.5.4 (Hensel's lemma). *Let v be a Henselian valuation on K. If $f \in \mathcal{O}_v[X]$ and $a \in \mathcal{O}_v$ with $f(a) \in \mathfrak{m}_v$ and $f'(a) \notin \mathfrak{m}_v$, then there exists $\alpha \in \mathcal{O}_v$ with $f(\alpha) = 0$ and $a - \alpha \in \mathfrak{m}_v$.*

PROOF. This follows from Lemma 1.5.3. □

The **language of valued fields**

$$\mathcal{L}_R = \mathcal{L}_{\text{ring}} \cup \{R\}$$

is the language of rings augmented by a unary predicate symbol R, which is interpreted as the valuation ring of a valued field.

1.6. p-adically Closed Fields

We recall the notion of p-adically closed fields, and quote some well known results from [PR84] and some properties of the absolute Galois group of a p-adically closed field.

A valuation v on a field K of characteristic zero with residue field of characteristic $p > 0$ and corresponding valuation ring $\mathcal{O}$ is a **p-valuation of p-rank** $d \in \mathbb{N}$ if

$$\dim_{\mathbb{F}_p} \mathcal{O}/p\mathcal{O} = d.$$

We also say that the valued field (K, v) is a **p-valued** field.

The residue field $\bar{K}_v$ of a p-valued field (K, v) is finite, and the value group $v(K^\times)$ is discrete and $v(p) \in \mathbb{Z}$. If $e = v(p)$ and $f = [\bar{K}_v : \mathbb{F}_p]$, then $d = ef$, [PR84, p. 15]. We call (p, e, f) the **type** of (K, v). Thus, if two p-valued fields have the same type, then they have the same p-rank. If L/K is an extension of p-valued fields, then L and K have the same p-rank if and only if they have the same type. In that case, this type is also the type of each intermediate extension of L/K.

A p-valued field is **p-adically closed** if it has no proper p-valued algebraic extension of the same p-rank. Every p-adically closed valued field (K, v) has a unique p-valuation, [PR84, 6.15]. We therefore also call K p-adically closed. A **p-adic closure** of a p-valued field (K, v) is an algebraic extension of (K, v) which is p-adically closed of the same p-rank as (K, v). A p-valued field (K, v) is p-adically closed if and only if it is Henselian and the value group $v(K^\times)$ is a $\mathbb{Z}$-group, [PR84, 3.1]. Here, an ordered abelian group Γ is a **$\mathbb{Z}$-group** if it is discrete and $(\Gamma : n\Gamma) = n$ for each $n \in \mathbb{N}$. Any p-valued field (K, v) has a p-adic closure. A p-adic closure of (K, v) is unique up to K-isomorphism if and only if $v(K^\times)$ is a $\mathbb{Z}$-group, [PR84, 3.2].

LEMMA 1.6.1. *If a field is algebraically closed in a p-adically closed field K, then it is p-adically closed of the same p-rank as K.*

PROOF. See [PR84, 3.4]. □

LEMMA 1.6.2. *Let V be an affine variety defined over a p-adically closed field K. Then V has a simple K-rational point if and only if the unique p-valuation of K extends to a p-valuation of $K(V)$ of the same p-rank.*

PROOF. See [PR84, 7.8]. □

The language

$$\mathcal{L}_{P,d} = \mathcal{L}_R \cup \{c_1, \ldots, c_d\} \cup \{P_n : n \in \mathbb{N}\}$$

is the language of valued fields augmented by d constant symbols $c_1, \ldots, c_d$ interpreting a fixed $\mathbb{F}_p$-basis of $\mathcal{O}/p\mathcal{O}$, and unary predicate symbols P_n, $n \in \mathbb{N}$, interpreting the subset of n-th powers of a p-valued field of p-rank d. The class of p-adically closed valued fields of p-rank d is elementary in the language $\mathcal{L}_R$, [PR84, p. 86].

PROPOSITION 1.6.3. *The $\mathcal{L}_R$-theory of p-adically closed valued fields of p-rank d is model complete and decidable, and it has quantifier elimination in the language $\mathcal{L}_{P,d}$. The $\mathcal{L}_R$-theory of p-adically closed valued fields of type $(p, 1, d)$ is complete.*

PROOF. See [PR84, 5.1, 5.2, 5.6, 5.4]. □

A **p-adic field** is the completion of a p-valued number field, i.e. a finite extension of $\hat{\mathbb{Q}}_p$. A p-adic field F is p-adically closed of p-rank $[F : \hat{\mathbb{Q}}_p]$, [PR84, p. 21].

LEMMA 1.6.4. *Every p-adically closed field is elementarily equivalent to a p-adic field.*

PROOF. Let E be p-adically closed, and let $K = \tilde{\mathbb{Q}} \cap E$, $K_0 = \tilde{\mathbb{Q}} \cap \hat{\mathbb{Q}}_p$. By Lemma 1.6.1, K is p-adically closed of the same p-rank as E, so $K_0 = \tilde{\mathbb{Q}} \cap \hat{\mathbb{Q}}_p \subseteq K$. Then $[K : K_0] < \infty$, c.f. [PR84, 2.9], so $F := K\hat{\mathbb{Q}}_p$ is a p-adic field. Since K is algebraically closed in F, K and F have the same p-rank by Lemma 1.6.1. Therefore, $E \equiv K \equiv F$ by model completeness (Proposition 1.6.3). □

LEMMA 1.6.5. *Let K be p-adically closed. Then* $\mathrm{Gal}(K)$ *is finitely generated, prosolvable, torsion-free, and* $\mathrm{cd}_l(\mathrm{Gal}(K)) = 2$ *for every prime number l.*

PROOF. First, if K is a p-adic field, then $\mathrm{Gal}(K)$ is finitely generated and prosolvable, and $\mathrm{cd}_l(\mathrm{Gal}(K)) = 2$ for every l, [NSW08, 7.4.1, p. 409, 7.1.8(i)], so in particular it is torsion-free. Since every p-adically closed field K is elementarily equivalent to a p-adic field K_0 (Lemma 1.6.4), and $\mathrm{Gal}(K_0)$ is finitely generated, $\mathrm{Gal}(K) \cong \mathrm{Gal}(K_0)$ has all the asserted properties (Lemma 1.3.4). □

PROPOSITION 1.6.6 (Neukirch-Pop[3]-Efrat[4]-Koenigsmann). *Let K be p-adically closed, and let L be a field. If* $\mathrm{Gal}(K) \cong \mathrm{Gal}(L)$*, then L is p-adically closed of the same type as K.*

PROOF. By Lemma 1.6.4, K is elementarily equivalent to a p-adic field K_0, and $\mathrm{Gal}(K) \cong \mathrm{Gal}(K_0)$ by Lemma 1.6.5 and Lemma 1.3.4. By [Koe95, Theorem 4.1], if $\mathrm{Gal}(K_0) \cong \mathrm{Gal}(L)$, then L is p-adically closed. But $\mathrm{Gal}(L)$ determines the type of L, see for example [JR79, Lemma 1]. □

[3] see [Pop88]
[4] see [Efr95]

CHAPTER 2

Local-Global Principles for Fields

The aim of this chapter is to develop basic model theoretic properties of fields satisfying a certain local-global principle, which we call PSCC. For subfields of the fields $K_{\mathrm{tot},S}$ we are interested in, the PSCC property coincides with the PSC property of [JR98], [GJ02], and [HJP09a]. A PSCC field F satisfies a local-global principle with respect to p-adic closures and real closures belonging to primes of F that lie over a given finite set of local primes S of some fixed base field K, and have the same type as their restrictions to K.

Previous works in this direction are [Pre81], [Ers82] and [Pre85] on PRC fields, [Gro87] and [Kün89b] on PpC fields, and [Kün89a] on PC_M fields. Furthermore, the work [Ers92] on RC_π fields, and [Dar00b], [Dar01] and [Ers01] on local-global principles for rings are related to the subject. We make use of ideas from some of these works.

The three main goals for the PSCC fields under consideration are: First-order definition of the holomorphy domains (Sections 2.3-2.4), axiomatization of the PSCC property (Sections 2.5-2.7), and describing totally S-adic extensions (Sections 2.8-2.9).

For the rest of this work, let K be a field of characteristic zero.

2.1. Classical Primes

We start this chapter by introducing the notion of a classical prime. This notion generalizes the notion of a place of a number field and unifies considerations about orderings and p-valuations.

Definition 2.1.1. A **prime** $\mathfrak{p}$ of K is either an equivalence class of valuations on K ($\mathfrak{p}$ is a **non-archimedean** prime) or an ordering of K ($\mathfrak{p}$ is an **archimedean** prime). The **characteristic**

$$\mathrm{char}(\mathfrak{p})$$

of $\mathfrak{p}$ is defined as follows: If $\mathfrak{p}$ is an equivalence class of valuations, then $\mathrm{char}(\mathfrak{p}) = \mathrm{char}(\bar{K}_\mathfrak{p})$, the characteristic of the **residue field** $\bar{K}_\mathfrak{p} = \bar{K}_v,\ v \in \mathfrak{p}$; if $\mathfrak{p}$ is an ordering, then $\mathrm{char}(\mathfrak{p}) = \infty$.

Remark 2.1.2. The reader may have noticed that our definition of primes does not include the classical so called 'complex primes', i.e. ab-

solute values for which the corresponding completion is isomorphic to $\mathbb{C}$. The reason for this is that both for the PSCC property and for the definition of the fields $K_{\mathrm{tot},S}$ we are interested in, the 'complex primes' in S can be disregarded.

DEFINITION 2.1.3. Let $\mathfrak{p}$ be a prime of K.

If $\mathrm{char}(\mathfrak{p}) \neq \infty$, let $v_\mathfrak{p}$ be a fixed valuation in the class $\mathfrak{p}$, and denote by

$$\mathcal{O}_\mathfrak{p} = \{x \in K \colon v_\mathfrak{p}(x) \geq 0\}$$

the corresponding valuation ring.

If $\mathrm{char}(\mathfrak{p}) = \infty$, denote the ordering $\mathfrak{p}$ by $\leq_\mathfrak{p}$, and by

$$\mathcal{O}_\mathfrak{p} = \{x \in K \colon x \geq_\mathfrak{p} 0\}$$

the corresponding positive cone.

DEFINITION 2.1.4. Let F/K be an extension of fields. A prime $\mathfrak{P}$ of F **lies over** a prime $\mathfrak{p}$ of K if

$$\mathcal{O}_\mathfrak{P} \cap K = \mathcal{O}_\mathfrak{p}.$$

We write this as

$$\mathfrak{P}|_K = \mathfrak{p}.$$

REMARK 2.1.5. If F/K is finite of degree n, then there are at most n primes of F lying over a given prime $\mathfrak{p}$ of K. This motivates the following definition.

DEFINITION 2.1.6. Let $\mathfrak{p}$ be a prime of K. We say that $\mathfrak{p}$ **totally splits** in a finite extension F/K if there are exactly $[F : K]$ many primes of F lying over $\mathfrak{p}$. We say that $\mathfrak{p}$ totally splits in an algebraic extension of K if it totally splits in every finite subextension.

DEFINITION 2.1.7. Let $\mathfrak{p}$ be a prime of K. The **localization**

$$K_\mathfrak{p}$$

of K with respect to $\mathfrak{p}$ is a Henselization of $(K, v_\mathfrak{p})$ (if $\mathrm{char}(\mathfrak{p}) \neq \infty$) resp. a real closure of $(K, \leq_\mathfrak{p})$ (if $\mathrm{char}(\mathfrak{p}) = \infty$). It is unique up to K-isomorphism.

EXAMPLE 2.1.8. *The field $\mathbb{Q}$ has one archimedean prime, which we denote by ∞, and one non-archimedean prime for each prime number p, which we simply denote by p. Note that in our notation, $\mathbb{Q}_p$ is now the field of p-adic* algebraic *numbers, whereas the field of p-adic numbers is denoted by $\hat{\mathbb{Q}}_p$.*

REMARK 2.1.9. If F/K is an extension and $\mathfrak{P}$ is a prime of F lying over a prime $\mathfrak{p}$ of K, we can and will assume that $K_\mathfrak{p} \subseteq F_\mathfrak{P}$.

DEFINITION 2.1.10. If $\mathfrak{p}$ is a prime of K and $\sigma \in \mathrm{Aut}(K)$ is an automorphism of K, then the **conjugate**

$$\sigma\mathfrak{p}$$

of $\mathfrak{p}$ is the unique prime of K with $\mathcal{O}_{\sigma\mathfrak{p}} = \sigma(\mathcal{O}_\mathfrak{p})$.

LEMMA 2.1.11. *If F/K is a Galois extension and $\mathfrak{P}, \mathfrak{Q}$ are primes of F with $\mathfrak{P}|_K = \mathfrak{Q}|_K = \mathfrak{p}$, then there exists $\sigma \in \mathrm{Gal}(F/K)$ with $\sigma\mathfrak{P} = \mathfrak{Q}$.*

PROOF. If $\mathrm{char}(\mathfrak{p}) = \infty$, then both $F_\mathfrak{P}$ and $F_\mathfrak{Q}$ are real closed fields, and thus real closures of K with respect to $\leq_\mathfrak{p}$, so they are conjugate over K, cf. Section 1.4. If $\mathrm{char}(\mathfrak{p}) \neq \infty$, then the claim follows from the fact that $v_\mathfrak{P}$ and $v_\mathfrak{Q}$ are conjugate over K, cf. Section 1.6. □

DEFINITION 2.1.12. If S is a set of primes of K,

$$R(S) = \bigcap_{\mathfrak{p} \in S} \mathcal{O}_\mathfrak{p}$$

is the **holomorphy domain** of S.

REMARK 2.1.13. Note that if S contains archimedean primes, then $R(S)$ is only a semiring but not a ring.

DEFINITION 2.1.14. A **classical** prime $\mathfrak{p}$ of K is either an equivalence class of p-valuations, for some prime number p, or an ordering of K.

DEFINITION 2.1.15. For a classical prime $\mathfrak{p}$ of K, a **classical closure** of $(K, \mathfrak{p})$ is a p-adic closure of $(K, v_\mathfrak{p})$ resp. a real closure of $(K, \leq_\mathfrak{p})$. Let

$$\mathrm{CC}(K, \mathfrak{p})$$

denote the set of all classical closures of $(K, \mathfrak{p})$ contained in $\tilde{K}$. We say that $(K, \mathfrak{p})$ is **classically closed** if $K \in \mathrm{CC}(K, \mathfrak{p})$, i.e. if K is p-adically closed resp. real closed.

DEFINITION 2.1.16. A prime $\mathfrak{p}$ of K is **local** if it is classical and the value group of $v_\mathfrak{p}$ is isomorphic to $\mathbb{Z}$ resp. the ordering $\leq_\mathfrak{p}$ is archimedean.

REMARK 2.1.17. Note that this definition of local primes essentially coincides with the definition of local primes in [GJ02] and [HJP09a], and the 'classical P-adic valuations and orderings' in [HJP09b]. Indeed, an ordering of K is archimedean if and only if there is an embedding of K into $\mathbb{R}$ (see Section 1.4), and since a field complete with respect to an archimedean absolute value is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$ by Gelfand-

Mazur (cf. [Lan02, XII.2.4]), embeddings of K into $\mathbb{R}$ correspond to 'non-complex' archimedean absolute values on K, cf. Remark 2.1.2. If a p-valuation v on K is discrete of rank one, then the completion of K with respect to v is a p-adic field, cf. [Ser79, Chapter II §5], and rank one valuations on K correspond to non-archimedean absolute values on K, cf. [End72, 7.6, 3.5].

Definition 2.1.18. A classical prime $\mathfrak{p}$ of K is **quasi-local** if $K_{\mathfrak{p}} \in \mathrm{CC}(K, \mathfrak{p})$, i.e. if the localization is a classical closure.

Remark 2.1.19. Note that each prime of a number field is local, and each local prime is quasi-local. If $\mathfrak{p}$ is quasi-local, then all $K' \in \mathrm{CC}(K, \mathfrak{p})$ are K-conjugate. A non-archimedean classical prime is quasi-local if and only if its value group is a $\mathbb{Z}$-group, cf. Section 1.6. If F/K is an algebraic extension and $\mathfrak{P}$ is a classical prime of F lying over a local prime $\mathfrak{p}$ of K, then $\mathfrak{P}$ is local.

Definition 2.1.20. The **type**

$$\mathrm{tp}(\mathfrak{p})$$

of a classical prime $\mathfrak{p}$ of K is the type (p, e, f) of the p-valuation $v_{\mathfrak{p}}$ if $\mathrm{char}(\mathfrak{p}) = p$, and $(\infty, 1, 1)$ if $\mathrm{char}(\mathfrak{p}) = \infty$.

Definition 2.1.21. We say that a field F is $\mathbf{P\mathcal{F}C}$ with respect to a family $\mathcal{F}$ of algebraic extensions of F if every absolutely irreducible smooth variety V defined over F has an F-rational point, provided it has an F'-rational point for each $F' \in \mathcal{F}$, cf. [Jar91, §7].

If $\mathcal{S}$ is a set of primes of F, then F is **pseudo-$\mathcal{S}$-closed with respect to localizations** ($\mathbf{P\mathcal{S}CL}$) if it is P$\mathcal{F}$C with respect to the family

$$\mathcal{F} = \{F_{\mathfrak{P}} \colon \mathfrak{P} \in \mathcal{S}\}$$

of localizations.

If $\mathcal{S}$ is a set of classical primes of F, then F is **pseudo-$\mathcal{S}$-closed with respect to classical closures** ($\mathbf{P\mathcal{S}CC}$) if it is P$\mathcal{F}$C with respect to the family

$$\mathcal{F} = \bigcup_{\mathfrak{P} \in \mathcal{S}} \mathrm{CC}(F, \mathfrak{P})$$

of classical closures.

Remark 2.1.22. Since every classical closure is Henselian resp. real closed, if F is P$\mathcal{S}$CC, then F is P$\mathcal{S}$CL. However, the converse does not hold, as the example of a p-valued Henselian but not p-adically closed field shows, cf. Remark 2.1.19 and Proposition 2.2.11 below.

2.2. PSCC and PSCL Fields

In this section we define the class of fields we are working with. For the rest of this chapter, we work in the following setting.

Setting 2.2.1.

- **K is a fixed base field of characteristic 0.**
- **S is a finite set of local primes of K.**
- **F is an extension of K.**

Definition 2.2.2. For $\mathfrak{p} \in S$ denote by

$$\mathcal{S}_{\mathfrak{p}}(F)$$

the set of all *classical* primes $\mathfrak{P}$ of F that satisfy the following conditions:

(1) $\mathfrak{P}|_K = \mathfrak{p}$.
(2) $\mathrm{tp}(\mathfrak{P}) = \mathrm{tp}(\mathfrak{p})$.

Definition 2.2.3. Let

$$\mathcal{S}_S(F) = \bigcup_{\mathfrak{p}\in S} \mathcal{S}_{\mathfrak{p}}(F),$$

$$R_{\mathfrak{p}}(F) = R(\mathcal{S}_{\mathfrak{p}}(F)),$$

cf. Definition 2.1.12,

$$\mathrm{CC}(F, \mathfrak{p}) = \bigcup_{\mathfrak{P}\in\mathcal{S}_{\mathfrak{p}}(F)} \mathrm{CC}(F, \mathfrak{P}),$$

cf. Definition 2.1.15, and

$$\mathrm{CC}(F, S) = \bigcup_{\mathfrak{p}\in S} \mathrm{CC}(F, \mathfrak{p}).$$

Remark 2.2.4. If $\mathfrak{p} \in S$ with $\mathrm{char}(\mathfrak{p}) \neq \infty$ and $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$, then $v_{\mathfrak{P}}$ extends $v_{\mathfrak{p}}$. Indeed, first note that by our convention of identifying $\mathbb{Z}$ with a convex subgroup of the value group, the value group of $v_{\mathfrak{p}}$ is a subgroup of the value group of $v_{\mathfrak{P}}$. Let $\pi_{\mathfrak{p}} \in K$ such that $v_{\mathfrak{p}}(\pi_{\mathfrak{p}}) = 1$. If $\mathrm{tp}(\mathfrak{P}) = \mathrm{tp}(\mathfrak{p}) = (p, e, f)$, then $p\pi_{\mathfrak{p}}^{-e} \in \mathcal{O}_{\mathfrak{p}}^{\times} \subseteq \mathcal{O}_{\mathfrak{P}}^{\times}$, so $e = v_{\mathfrak{P}}(p) = ev_{\mathfrak{P}}(\pi_{\mathfrak{p}})$, and therefore $v_{\mathfrak{P}}(\pi_{\mathfrak{p}}) = 1 = v_{\mathfrak{p}}(\pi_{\mathfrak{p}})$. Since $v_{\mathfrak{p}}(K^{\times}) = \mathbb{Z}$, this implies that $v_{\mathfrak{P}}(x) = v_{\mathfrak{p}}(x)$ for all $x \in K^{\times}$.

Definition 2.2.5. We say that F is **pseudo-S-closed with respect to localizations** (**PSCL**) resp. **pseudo-S-closed with respect to classical closures** (**PSCC**) if F is P$\mathcal{S}$CL resp. P$\mathcal{S}$CC with respect to

$$\mathcal{S} = \mathcal{S}_S(F).$$

REMARK 2.2.6. Note that F is PSCC if and only if F is P$\mathcal{F}$C with respect to the family

$$\mathcal{F} = \mathrm{CC}(F, S).$$

If F is PSCC, then F is PSCL, cf. Remark 2.1.22.

REMARK 2.2.7. Note that for $K = \mathbb{Q}$ and $|S| = 1$, our notion of PSCC fields coincides with the classical notions of PpC resp. PRC fields. For $K = \mathbb{Q}$ and S a finite set of prime numbers, the notion of PSCC fields coincides with the notion of PC$_M$ fields of [Kün89a] and [Kün92]. For $K = \mathbb{Q}$ and $S = \emptyset$, a PSCC field is just a PAC field (cf. [FJ08, Chapter 11]).

REMARK 2.2.8. Note that there is a related notion of PSC fields in the literature. However, in [JR98] and [GJ02] this property is only defined for algebraic extensions of K, and in [JR01], [Raz02] and [HJP09a] only for subextensions of $K_{\mathrm{tot},S}/K$ (cf. Definition 4.1.1 below). For subextensions of $K_{\mathrm{tot},S}/K$, the three notions PSC, PSCL, and PSCC coincide, but both the PSCL property and the PSCC property are defined for arbitrary extensions of K. The reason for our focus on the PSCC property is that, as we show, it is elementary.

DEFINITION 2.2.9. We say that F is **S-quasi-local** if every $\mathfrak{P} \in \mathcal{S}_S(F)$ is quasi-local (cf. Definition 2.1.18).

LEMMA 2.2.10. *If F/K is algebraic, then F is S-quasi-local.*

PROOF. Since S consists of local primes, every $\mathfrak{P} \in \mathcal{S}_S(F)$ is local, and thus quasi-local, cf. Remark 2.1.19. □

PROPOSITION 2.2.11. *If F is* PSCC*, then F is S-quasi-local.*

PROOF. If F is PSCC, then F is P$\mathcal{F}$C with respect to $\mathcal{F} = \mathrm{CC}(F, S)$, cf. Remark 2.2.6. Hence, the claim follows from [HJP09c, Proposition 2.3(a)]. Indeed, this proposition implies that if $F' \in \mathrm{CC}(F, S)$, then F is dense in F' if two conditions are satisfied.

The first condition is that $\mathrm{CC}(F, S)$ is 'étale-compact'. This is in particular the case if $\mathrm{CC}(F, S)$ is 'strictly compact', see [HJP07, Section 1]. The second condition is that F' is minimal in $\mathrm{CC}(F, S)$. This always holds if there are no non-trivial inclusions among elements of $\mathrm{CC}(F, S)$.

In Lemma 3.5.3 below we prove properties of the absolute Galois group of an arbitrary extension F of K, which via Galois correspondence imply that $\mathrm{CC}(F, S)$ is 'strictly compact' and that there are no non-trivial inclusions among elements of $\mathrm{CC}(F, S)$. Therefore, if $\mathfrak{P} \in \mathcal{S}_S(F)$ and $F' \in \mathrm{CC}(F, \mathfrak{P})$, then F is dense in F', and hence $\mathfrak{P}$ is quasi-local. □

2.3. Defining Holomorphy Domains in a General Setting

This section contains the technical first-order definition of the holomorphy domains. We consider the following setting.

SETTING 2.3.1.

- F is a field of characteristic zero.
- $\mathcal{S}$ is a set of classical primes of F.
- $\mathcal{S}$ is partitioned as $\mathcal{S} = \bigcup_{i=1}^{n} \mathcal{S}_i$, such that for every i, if $\mathfrak{P}, \mathfrak{Q} \in \mathcal{S}_i$, then $\mathrm{char}(\mathfrak{P}) = \mathrm{char}(\mathfrak{Q})$.
- For each i, π_i is an element of $F^\times$ that satisfies the following conditions:
  (S1) If $\mathfrak{P} \in \mathcal{S}_i$ and $\mathrm{char}(\mathfrak{P}) \neq \infty$, then $v_{\mathfrak{P}}(\pi_i) = 1$.
  (S2) If $\mathfrak{P} \in \mathcal{S} \setminus \mathcal{S}_i$ and $\mathrm{char}(\mathfrak{P}) \neq \infty$, then $v_{\mathfrak{P}}(\pi_i - 1) > 0$.
  (S3) If $\mathfrak{P} \in \mathcal{S}_i$ and $\mathrm{char}(\mathfrak{P}) = \infty$, then $\pi_i <_{\mathfrak{P}} -1$.
  (S4) If $\mathfrak{P} \in \mathcal{S} \setminus \mathcal{S}_i$ and $\mathrm{char}(\mathfrak{P}) = \infty$, then $\pi_i >_{\mathfrak{P}} 0$.

DEFINITION 2.3.2. We write

$$\mathrm{char}(\mathcal{S}_i)$$

for $\mathrm{char}(\mathfrak{P})$, $\mathfrak{P} \in \mathcal{S}_i$, and we let

$$\pi = \prod_{i=1}^{n} \pi_i.$$

Our first goal is to give a first-order definition of the holomorphy domain $R(\mathcal{S}_i)$ of $\mathcal{S}_i$ in the case that F is P$\mathcal{S}$CL. The case $n = m = 1$ of the following lemma can be found in [HP84].

LEMMA 2.3.3. *Let $f \in F[X_1, \ldots, X_n]$ and $g \in F[Y_1, \ldots, Y_m]$ be non-constant polynomials, and let $c \in F^\times$. If g is square-free in $\tilde{F}[\mathbf{Y}]$, then*

$$h(\mathbf{X}, \mathbf{Y}) = f(\mathbf{X})g(\mathbf{Y}) + c \quad \in F[\mathbf{X}, \mathbf{Y}]$$

is absolutely irreducible.

PROOF. Without loss of generality assume that $F = \tilde{F}$. We prove the lemma by induction on n.

First assume that $n = 1$. Let $r(\mathbf{Y})$ be any prime factor of $g(\mathbf{Y})$. Since g is square-free, $r | g$ but $r^2 \nmid g$. Write h as a polynomial in X_1. Then r divides all coefficients of h except the constant one. Thus, by Eisenstein's criterion (cf. [FJ08, Lemma 2.3.10(b)]), h is irreducible in $F(\mathbf{Y})[\mathbf{X}]$. Therefore, if h decomposes in $F[\mathbf{X}, \mathbf{Y}]$, then one of the factors must be in $F[\mathbf{Y}]$. But then, since $c \neq 0$, this factor must be in F, and thus h is irreducible in $F[\mathbf{X}, \mathbf{Y}]$.

Now assume that $n > 1$ and $f \notin F[X_1]$. Assume that h decomposes as $h = h_1 h_2$ with $h_1, h_2 \in F[\mathbf{X}, \mathbf{Y}] \setminus F$. Since $c \neq 0$, we have $h_1, h_2 \notin F[X_1]$. Hence, there exists $x \in F$ such that $h_1(x, X_2, \ldots, X_n, \mathbf{Y}) \notin F$,

$h_2(x, X_2, \ldots, X_n, \mathbf{Y}) \notin F$, and $f(x, X_2, \ldots, X_n) \notin F$. Consequently,

$$f(x, X_2, \ldots, X_n)g(\mathbf{Y}) + c = h_1(x, X_2, \ldots, X_n, \mathbf{Y})h_2(x, X_2, \ldots, X_n, \mathbf{Y})$$

decomposes in $F[X_2, \ldots, X_n, \mathbf{Y}]$, contradicting the induction hypothesis. □

LEMMA 2.3.4. *Let $f \in F[X_1, \ldots, X_n]$ be non-constant, and let $g \in F[Y]$ be non-constant and square-free in $\tilde{F}[Y]$ with $g(1) \neq 0$ and $g'(1) \neq 0$. Then the polynomial*

$$G(\mathbf{X}, Y) = g(Y)(1 + f(\mathbf{X})) - g(1) \quad \in F[\mathbf{X}, Y]$$

is absolutely irreducible, and for every root $\mathbf{x}$ of f, $(\mathbf{x}, 1)$ is a non-singular point on the hypersurface defined by G.

PROOF. Since f is non-constant, also $1 + f$ is non-constant. Since in addition g is square-free in $\tilde{F}[Y]$ and $g(1) \neq 0$, Lemma 2.3.3 implies that G is absolutely irreducible. If $f(\mathbf{x}) = 0$, then $G(\mathbf{x}, 1) = g(1)(1 + f(\mathbf{x})) - g(1) = 0$ and $\frac{\partial G}{\partial Y}(\mathbf{x}, 1) = g'(1) \neq 0$. Therefore, $(\mathbf{x}, 1)$ is non-singular on the hypersurface $G = 0$. □

Our formula defining $R(\mathcal{S}_i)$ makes use of a polynomial of the form $G(X, Y)$ in Lemma 2.3.4. More precisely, we let $f(X)$ depend on a parameter $a \in F$ such that $R(\mathcal{S}_i)$ consists of all $a \in F$ for which $G(X, Y)$ has a zero in F (in the case $\mathrm{char}(\mathcal{S}_i) \neq \infty$). We construct $f(X)$ as a product of several polynomials, each of which has a zero in a certain class of localizations of F, so that the hypersurface $G = 0$ has a simple point in every localization. The basic idea for this 'modular' approach appears in Künzi's work [Kün89a].

LEMMA 2.3.5. *Under Setting 2.3.1, the polynomial*

$$A_i(X) = X^2 - \pi_i$$

satisfies the following conditions:

- (A1) *If $\mathfrak{P} \in \mathcal{S} \smallsetminus \mathcal{S}_i$ and $\mathrm{char}(\mathfrak{P}) \neq 2$, then A_i has a zero in $F_{\mathfrak{P}}$.*
- (A2) *If $\mathfrak{P} \in \mathcal{S}_i$ and $\mathrm{char}(\mathfrak{P}) \neq \infty$, then for all $x \in F$, $v_{\mathfrak{P}}(A_i(x)) \leq 1$.*
- (A3) *If $\mathfrak{P} \in \mathcal{S}_i$ and $\mathrm{char}(\mathfrak{P}) \neq \infty$, then $v_{\mathfrak{P}}(A_i(1)) = 0$.*
- (A4) *$A_i(X)$ is square-free in $\tilde{F}[X]$, and $A_i'(1) \neq 0$.*
- (A5) *If $\mathfrak{P} \in \mathcal{S}_i$ and $\mathrm{char}(\mathfrak{P}) = \infty$, then for all $x \in F$, $A_i(x) >_{\mathfrak{P}} 1$.*

PROOF. Let $\mathfrak{P} \in \mathcal{S} \smallsetminus \mathcal{S}_i$ with $\mathrm{char}(\mathfrak{P}) \notin \{2, \infty\}$. The reduction $\bar{A}_i$ of A_i with respect to $\mathfrak{P}$ is $\bar{A}_i(X) = X^2 - 1$ by (S2). Thus, since $\bar{A}_i(1) = 0$ and $\bar{A}_i'(1) = 2 \neq 0$ (since $\mathrm{char}(\mathfrak{P}) \neq 2$), Hensel's lemma (Lemma 1.5.4) gives a zero of A_i in $F_{\mathfrak{P}}$. Now let $\mathfrak{P} \in \mathcal{S} \smallsetminus \mathcal{S}_i$ with $\mathrm{char}(\mathfrak{P}) = \infty$. Since $\pi_i >_{\mathfrak{P}} 0$ by (S4), A_i has a zero in the real closed field $F_{\mathfrak{P}}$. This proves (A1).

Now let $\mathfrak{P} \in \mathcal{S}_i$ with $\mathrm{char}(\mathfrak{P}) \neq \infty$ and $x \in F$. If $v_{\mathfrak{P}}(x) > 0$, then $v_{\mathfrak{P}}(x^2) \geq 2 > v_{\mathfrak{P}}(\pi_i)$ by (S1), so $v_{\mathfrak{P}}(A_i(x)) = v_{\mathfrak{P}}(\pi_i) = 1$. If $v_{\mathfrak{P}}(x) \leq 0$,

then $v_{\mathfrak{P}}(x^2) < v_{\mathfrak{P}}(\pi_i)$ by (S1), so $v_{\mathfrak{P}}(A_i(x)) = v_{\mathfrak{P}}(x^2) \leq 1$. This proves (A2).

Furthermore, $v_{\mathfrak{P}}(A_i(1)) = v_{\mathfrak{P}}(1 - \pi_i) = 0$ by (S1). This proves (A3).

Condition (A4) follows from $\mathrm{char}(F) = 0$ and $\pi_i \neq 0$.

Finally let $\mathfrak{P} \in \mathcal{S}_i$ with $\mathrm{char}(\mathfrak{P}) = \infty$, and $x \in F$. Then $\pi_i <_{\mathfrak{P}} -1$ by (S3) and $x^2 \geq_{\mathfrak{P}} 0$, so $A_i(x) \geq_{\mathfrak{P}} -\pi_i >_{\mathfrak{P}} 1$. This proves (A5). □

LEMMA 2.3.6. *Under Setting 2.3.1, the polynomial*

$$B_i(X) = X^2 + \pi_i X + \pi$$

satisfies the following conditions:

(B1) *If $\mathfrak{P} \in \mathcal{S} \setminus \mathcal{S}_i$ and $\mathrm{char}(\mathfrak{P}) = 2$, then B_i has a zero in $F_{\mathfrak{P}}$.*
(B2) *If $\mathfrak{P} \in \mathcal{S}_i$ and $\mathrm{char}(\mathfrak{P}) \neq \infty$, then for all $x \in F$, $v_{\mathfrak{P}}(B_i(x)) \leq 1$.*

PROOF. Let $\mathfrak{P} \in \mathcal{S} \setminus \mathcal{S}_i$ with $\mathrm{char}(\mathfrak{P}) = 2$. Then the reduction $\bar{B}_i$ of B_i with respect to $\mathfrak{P}$ is $\bar{B}_i(X) = X^2 + X$ (by (S1) and (S2)), and $\bar{B}_i'(X) = 1$. Therefore, by Hensel's lemma, B_i has a root in $F_{\mathfrak{P}}$. This proves (B1).

Now let $\mathfrak{P} \in \mathcal{S}_i$ with $\mathrm{char}(\mathfrak{P}) \neq \infty$ and $x \in F$. If $v_{\mathfrak{P}}(x) > 0$, then (S1) and (S2) imply that $v_{\mathfrak{P}}(x^2) \geq 2 > v_{\mathfrak{P}}(\pi)$ and $v_{\mathfrak{P}}(\pi_i x) > v_{\mathfrak{P}}(\pi_i) = v_{\mathfrak{P}}(\pi)$, so $v_{\mathfrak{P}}(B_i(x)) = v_{\mathfrak{P}}(\pi) = 1$. If $v_{\mathfrak{P}}(x) \leq 0$, then (S1) and (S2) imply that $v_{\mathfrak{P}}(x^2) \leq v_{\mathfrak{P}}(x) < v_{\mathfrak{P}}(\pi_i x)$ and $v_{\mathfrak{P}}(x^2) \leq 0 < v_{\mathfrak{P}}(\pi)$, so $v_{\mathfrak{P}}(B_i(x)) = v_{\mathfrak{P}}(x^2) \leq 1$. This proves (B2). □

LEMMA 2.3.7. *Under Setting 2.3.1, if $\mathrm{char}(\mathcal{S}_i) \neq \infty$, then for every $a \in F$, the polynomial*

$$D_{i,a}(X) = a\pi_i X^2 - X + a$$

satisfies the following conditions:

(D1) *If $\mathfrak{P} \in \mathcal{S}_i$ and $v_{\mathfrak{P}}(a) \geq 0$, then $D_{i,a}$ has a zero in $F_{\mathfrak{P}}$.*
(D2) *If $\mathfrak{P} \in \mathcal{S}_i$ and $v_{\mathfrak{P}}(a) < 0$, then $v_{\mathfrak{P}}(D_{i,a}(x)) \leq v_{\mathfrak{P}}(a)$ for all $x \in F$. Thus, if $v_{\mathfrak{P}}(D_{i,a}(x)) \geq 0$ for some $x \in F$, then $v_{\mathfrak{P}}(a) \geq 0$.*

PROOF. Let $\mathfrak{P} \in \mathcal{S}_i$ with $v_{\mathfrak{P}}(a) \geq 0$. Then $D_{i,a}(X) \in \mathcal{O}_{\mathfrak{P}}[X]$ by (S1). The reduction $\bar{D}_{i,a}$ of $D_{i,a}$ with respect to $\mathfrak{P}$ is $\bar{D}_{i,a}(X) = -X + \bar{a}$, and $\bar{D}_{i,a}'(X) = -1$. Therefore, $D_{i,a}$ has a zero in $F_{\mathfrak{P}}$ by Hensel's lemma (Lemma 1.5.4). This proves (D1).

Now let $\mathfrak{P} \in \mathcal{S}_i$ with $v_{\mathfrak{P}}(a) < 0$, and let $x \in F$. If $v_{\mathfrak{P}}(x) \geq 0$, then $v_{\mathfrak{P}}(a\pi_i x^2) > v_{\mathfrak{P}}(a)$ and $v_{\mathfrak{P}}(x) \geq 0 > v_{\mathfrak{P}}(a)$, so $v_{\mathfrak{P}}(D_{i,a}(x)) = v_{\mathfrak{P}}(a)$. If $v_{\mathfrak{P}}(x) < 0$, then $v_{\mathfrak{P}}(a\pi_i x^2) < 2v_{\mathfrak{P}}(x) + v_{\mathfrak{P}}(\pi_i) \leq -1 + v_{\mathfrak{P}}(x) + v_{\mathfrak{P}}(\pi_i) = v_{\mathfrak{P}}(x)$ by (S1); and $v_{\mathfrak{P}}(a\pi_i x^2) = v_{\mathfrak{P}}(a) + v_{\mathfrak{P}}(\pi_i) + 2v_{\mathfrak{P}}(x) \leq v_{\mathfrak{P}}(a) + 1 - 2 < v_{\mathfrak{P}}(a)$, so $v_{\mathfrak{P}}(D_{i,a}(x)) = v_{\mathfrak{P}}(a\pi_i x^2) < v_{\mathfrak{P}}(a)$. This proves (D2). □

LEMMA 2.3.8. *Under Setting 2.3.1 and* $\mathrm{char}(\mathcal{S}_i) \neq \infty$*, let* $a \in F$*. If* A_i *satisfies* (A1)-(A4)*,* B_i *satisfies* (B1)-(B2)*, and* $D_{i,a}$ *satisfies* (D1)-(D2)*, then the polynomial*

$$G_{i,a}(X,Y) = A_i(Y)(1 + \pi_i^{-4} A_i(X) B_i(X) D_{i,a}(X)) - A_i(1)$$

satisfies the following conditions:

(1) *If* $G_{i,a}$ *has a zero in* F*, then* $v_{\mathfrak{P}}(a) \geq 0$ *for all* $\mathfrak{P} \in \mathcal{S}_i$*.*
(2) *If* F *is* P$\mathcal{S}$CL *and* $v_{\mathfrak{P}}(a) \geq 0$ *for all* $\mathfrak{P} \in \mathcal{S}_i$*, then* $G_{i,a}$ *has a zero in* F*.*

PROOF. Let $x, y \in F$ with $G_{i,a}(x,y) = 0$ and let $\mathfrak{P} \in \mathcal{S}_i$. Then

$$v_{\mathfrak{P}}(1 + \pi_i^{-4} A_i(x) B_i(x) D_{i,a}(x)) = v_{\mathfrak{P}}(A_i(1)) - v_{\mathfrak{P}}(A_i(y)) \geq -1$$

by (A2) and (A3). Thus,

$$v_{\mathfrak{P}}(\pi_i^{-4} A_i(x) B_i(x) D_{i,a}(x)) \geq -1,$$

so

$$v_{\mathfrak{P}}(D_{i,a}(x)) \geq -1 + 4v_{\mathfrak{P}}(\pi_i) - v_{\mathfrak{P}}(A_i(x)) - v_{\mathfrak{P}}(B_i(x)) > 0$$

by (S1), (A2), and (B2). Therefore, $v_{\mathfrak{P}}(a) \geq 0$ by (D2).

Now assume that F is P$\mathcal{S}$CL and $v_{\mathfrak{P}}(a) \geq 0$ for all $\mathfrak{P} \in \mathcal{S}_i$. If $A_i(1) = 0$, then $G_{i,a}(0,1) = 0$. Hence, assume without loss of generality that $A_i(1) \neq 0$. Let $\mathfrak{P} \in \mathcal{S}$. We claim that $A_i(X)B_i(X)D_{i,a}(X)$ has a zero in $F_{\mathfrak{P}}$. If $\mathfrak{P} \in \mathcal{S} \smallsetminus \mathcal{S}_i$ and $\mathrm{char}(\mathfrak{P}) \neq 2$, this follows from (A1). If $\mathfrak{P} \in \mathcal{S} \smallsetminus \mathcal{S}_i$ and $\mathrm{char}(\mathfrak{P}) = 2$, this follows from (B1). If $\mathfrak{P} \in \mathcal{S}_i$, this follows from (D1). Therefore, by Lemma 2.3.4 and (A4), $G_{i,a}$ is absolutely irreducible and has a simple zero in $F_{\mathfrak{P}}$ for all $\mathfrak{P} \in \mathcal{S}$. Since F is P$\mathcal{S}$CL, $G_{i,a}$ has a zero in F. □

This almost concludes the proof of the definability of $R(\mathcal{S}_i)$ for $\mathrm{char}(\mathcal{S}_i) \neq \infty$. We now turn to the case $\mathrm{char}(\mathcal{S}_i) = \infty$.

LEMMA 2.3.9. *Under Setting 2.3.1, if* $\mathrm{char}(\mathcal{S}_i) = \infty$*, then the polynomial*

$$C(X) = X^2 + X + 2$$

satisfies the following conditions:

(C1) *If* $\mathfrak{P} \in \mathcal{S} \smallsetminus \mathcal{S}_i$ *and* $\mathrm{char}(\mathfrak{P}) = 2$*, then* C *has a zero in* $F_{\mathfrak{P}}$*.*
(C2) *If* $\mathfrak{P} \in \mathcal{S}_i$*, then* $C(x) >_{\mathfrak{P}} 1$ *for every* $x \in F$*.*

PROOF. If $\mathrm{char}(\mathfrak{P}) = 2$, then C has a zero in $F_{\mathfrak{P}}$ by Hensel's lemma, and this implies (C1). If $x \in F$, then $x^2 + x + 2 = (x + \frac{1}{2})^2 + \frac{7}{4} >_{\mathfrak{P}} 1$, so (C2) holds. □

LEMMA 2.3.10. *Under Setting 2.3.1, if* $\mathrm{char}(\mathcal{S}_i) = \infty$*, then for every* $a \in F$*, the polynomial*

$$E_a(X) = X^2 - a$$

satisfies the following conditions:

(E1) *If* $\mathfrak{P} \in \mathcal{S}_i$ *and* $a \geq_{\mathfrak{P}} 0$*, then* E_a *has a zero in* $F_{\mathfrak{P}}$*.*
(E2) *If* $\mathfrak{P} \in \mathcal{S}_i$*,* $x, \epsilon \in F$*, and* $E_a(x) \leq_{\mathfrak{P}} \epsilon$*, then* $a \geq_{\mathfrak{P}} -\epsilon$*.*

PROOF. Let $\mathfrak{P} \in \mathcal{S}_i$ with $a \geq_{\mathfrak{P}} 0$. Then a has a square root in the real closed field $F_{\mathfrak{P}}$, and this implies (E1).

Now let $\mathfrak{P} \in \mathcal{S}_i$, and $x, \epsilon \in F$ with $E_a(x) \leq_{\mathfrak{P}} \epsilon$. Then $x^2 - a \leq_{\mathfrak{P}} \epsilon$, and therefore $a \geq_{\mathfrak{P}} -\epsilon$, since $x^2 \geq_{\mathfrak{P}} 0$. This implies (E2). □

LEMMA 2.3.11. *Under Setting 2.3.1, if* $\operatorname{char}(\mathcal{S}_i) = \infty$*, then for every* $u \in F^\times$*, the polynomial*

$$H_u(X) = X^2 + u^2$$

satisfies the following conditions:

(H1) *If* $\mathfrak{P} \in \mathcal{S}_i$*, then for all* $x \in F$*,* $H_u(x) \geq_{\mathfrak{P}} u^2$*.*
(H2) *If* $\mathfrak{P} \in \mathcal{S}_i$*, then* $H_u(1) = 1 + u^2 >_{\mathfrak{P}} 0$*.*
(H3) $H_u(X)$ *is square-free in* $\tilde{F}[X]$*, and* $H_u'(1) \neq 0$*.*

PROOF. (H1) follows from $x^2 \geq_{\mathfrak{P}} 0$. (H2) follows from $H_u(1) = 1 + u^2 \geq_{\mathfrak{P}} 1 >_{\mathfrak{P}} 0$. (H3) follows from $u \neq 0$ and $\operatorname{char}(F) = 0$. □

LEMMA 2.3.12. *Under Setting 2.3.1 and* $\operatorname{char}(\mathcal{S}_i) = \infty$*, let* $a \in F$ *and* $u \in F^\times$*. If* A_i *satisfies* (A1) *and* (A5)*,* C *satisfies* (C1)-(C2)*,* E_a *satisfies* (E1)-(E2)*, and* H_u *satisfies* (H1)-(H3)*, then the polynomial*

$$G_{i,a,u}(X, Y) = H_u(Y)(1 + A_i(X)C(X)E_a(X)) - H_u(1)$$

satisfies the following conditions:

(1) *If* $G_{i,a,u}$ *has a zero in* F*, then* $a \geq_{\mathfrak{P}} -\frac{1}{u^2}$ *for all* $\mathfrak{P} \in \mathcal{S}_i$*.*
(2) *If* F *is* P$\mathcal{S}$CL *and* $a \geq_{\mathfrak{P}} 0$ *for all* $\mathfrak{P} \in \mathcal{S}_i$*, then* $G_{i,a,u}$ *has a zero in* F*.*

PROOF. Let $x, y \in F$ such that $G_{i,a,u}(x, y) = 0$ and let $\mathfrak{P} \in \mathcal{S}_i$. Then

$$1 + A_i(x)C(x)E_a(x) = \frac{H_u(1)}{H_u(y)} \leq_{\mathfrak{P}} \frac{1 + u^2}{u^2} = 1 + \frac{1}{u^2}$$

by (H1), (H2). Thus, $E_a(x) \leq_{\mathfrak{P}} \frac{1}{u^2}$ by (A5) and (C2). Therefore, $a \geq_{\mathfrak{P}} -\frac{1}{u^2}$ by (E2).

Now assume that F is P$\mathcal{S}$CL and $a \geq_{\mathfrak{P}} 0$ for all $\mathfrak{P} \in \mathcal{S}_i$. If $H_u(1) = 0$, then $G_{i,a,u}(0, 1) = 0$. Hence, assume without loss of generality that $H_u(1) \neq 0$. Let $\mathfrak{P} \in \mathcal{S}$. We claim that $A_i(X)C(X)E_a(X)$ has a zero in $F_{\mathfrak{P}}$. If $\mathfrak{P} \in \mathcal{S} \setminus \mathcal{S}_i$ and $\operatorname{char}(\mathfrak{P}) \neq 2$, this follows from (A1). If $\operatorname{char}(\mathfrak{P}) = 2$, it follows from (C1). If $\mathfrak{P} \in \mathcal{S}_i$, it follows from (E1). Therefore, by Lemma 2.3.4, (H3), and the assumption that F is P$\mathcal{S}$CL, it follows that $G_{i,a,u}$ has a zero in F. □

For the following proposition, let A_i, B_i, C, $D_{i,a}$, E_a, H_u be the concrete polynomials defined above.

PROPOSITION 2.3.13. *Under Setting 2.3.1, for* $\mathrm{char}(\mathcal{S}_i) \neq \infty$ *let* $\varphi_i(a)$ *be the* $\mathcal{L}_{\mathrm{ring}}(\pi_1, \ldots, \pi_n)$*-formula*

$$(\exists x, y)(A_i(y)(1 + \pi_i^{-4} A_i(x) B_i(x) D_{i,a}(x)) - A_i(1) = 0),$$

and for $\mathrm{char}(\mathcal{S}_i) = \infty$ *let* $\varphi_i(a)$ *be the* $\mathcal{L}_{\mathrm{ring}}(\pi_i)$*-formula*

$$(\forall u \neq 0)(\exists x, y)(H_u(y)(1 + A_i(x) C(x) E_a(x)) - H_u(1) = 0).$$

Then the following holds for the subset $\varphi_i(F) \subseteq F$ *defined by* φ_i*:*

(1) $\varphi_i(F) \subseteq R(\mathcal{S}_i)$.
(2) *If* F *is* P$\mathcal{S}$CL*, then* $\varphi_i(F) = R(\mathcal{S}_i)$.

PROOF.

PART A: CASE $\mathrm{char}(\mathcal{S}_i) \neq \infty$. Note that the left hand side of the equation in $\varphi_i(a)$ is $G_{i,a}(x, y)$, where $G_{i,a}$ is the polynomial defined in Lemma 2.3.8. By Lemma 2.3.5, Lemma 2.3.6, and Lemma 2.3.7, A_i, B_i, and $D_{i,a}$ satisfy (A1)-(A4), (B1)-(B2), (D1)-(D2). Therefore, if $G_{i,a}(x, y) = 0$, then $v_{\mathfrak{P}}(a) \geq 0$ for all $\mathfrak{P} \in \mathcal{S}_i$ by Lemma 2.3.8(1), so $a \in R(\mathcal{S}_i)$. This proves (1). Conversely, if $a \in R(\mathcal{S}_i)$ and F is P$\mathcal{S}$CL, then $\varphi_i(a)$ holds in F by Lemma 2.3.8(2). This proves (2).

PART B: CASE $\mathrm{char}(\mathcal{S}_i) = \infty$. By Lemma 2.3.5, Lemma 2.3.9, Lemma 2.3.10 and Lemma 2.3.11, A_i, C, E_a, H_u satisfy (A1), (A5), (C1)-(C2), (E1)-(E2), (H1)-(H3). First assume that $\mathfrak{P} \in \mathcal{S}_i$ and $a \in \varphi_i(F)$, i.e. the polynomial $G_{i,a,u}$ of Lemma 2.3.12 has a zero for all $u \in F^\times$. By Lemma 2.3.12(1), $a \geq_{\mathfrak{P}} -1/u^2$ for all $\mathfrak{P} \in \mathcal{S}_i$ and $u \in F^\times$. If $a <_{\mathfrak{P}} 0$, then $a <_{\mathfrak{P}} -1/(2^2)$ or $a <_{\mathfrak{P}} -1/(1/a)^2$, since otherwise $a \geq_{\mathfrak{P}} -1/4$ and $a \leq_{\mathfrak{P}} -1$. Thus, $a \geq_{\mathfrak{P}} 0$ for all $\mathfrak{P} \in \mathcal{S}_i$, i.e. $a \in R(\mathcal{S}_i)$. This proves (1). Now assume that F is P$\mathcal{S}$CL and $a \in R(\mathcal{S}_i)$. By Lemma 2.3.12(2), $G_{i,a,u}$ has a zero in F for each $u \in F^\times$, i.e. $\varphi_i(a)$ is satisfied in F. This proves (2). □

REMARK 2.3.14. Note that in the case $\mathrm{char}(\mathcal{S}_i) \neq \infty$, our definition of $R(\mathcal{S}_i)$ is existential. With a little more effort, it is possible to give an existential definition of $R(\mathcal{S}_i)$ also in the case $\mathrm{char}(\mathcal{S}_i) = \infty$.

2.4. Defining Holomorphy Domains in P*S*CL Fields

Now we apply the general construction of the previous section to the fields we are interested in. For the rest of this chapter, we continue to work in Setting 2.2.1 and make the following additional assumptions:

- **For** $\mathfrak{p} \in S$ **non-archimedean,** $\pi_{\mathfrak{p}} \in K$ **with** $v_{\mathfrak{p}}(\pi_{\mathfrak{p}}) = 1$ **is fixed.**
- **For** $\mathfrak{p} \in S$ **archimedean, let** $\pi_{\mathfrak{p}} = -1$**.**

LEMMA 2.4.1. *Let* $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, $\mathcal{S}_i = \mathcal{S}_{\mathfrak{p}_i}(F)$, *and* $\mathcal{S} = \bigcup_{i=1}^n \mathcal{S}_i$. *Then there exist* $\pi_1, \ldots, \pi_n \in K$ *that satisfy the conditions of Setting 2.3.1.*

PROOF. Let $i \in \{1, \dots, n\}$.

PART A: $\mathrm{char}(\mathfrak{p}_i) \neq \infty$. By the weak approximation theorem (Lemma 1.5.1), there exists $\pi_i \in K$ with $v_{\mathfrak{p}_i}(\pi_i - \pi_{\mathfrak{p}_i}) > 1$, $v_{\mathfrak{p}_j}(\pi_i - 1) > 1$ for $j \neq i$ with $\mathrm{char}(\mathfrak{p}_j) \neq \infty$, and $0 <_{\mathfrak{p}_j} \pi_i <_{\mathfrak{p}_j} 2$ for $j \neq i$ with $\mathrm{char}(\mathfrak{p}_j) = \infty$. In particular, $v_{\mathfrak{p}_i}(\pi_i) = v_{\mathfrak{p}_i}(\pi_{\mathfrak{p}_i}) = 1$. So π_i satisfies (S1), (S2), and (S4), cf. Remark 2.2.4.

PART B: $\mathrm{char}(\mathfrak{p}_i) = \infty$. By Lemma 1.5.1, there exists $\pi_i \in K$ with $-3 <_{\mathfrak{p}_i} \pi_i <_{\mathfrak{p}_i} -1$, $v_{\mathfrak{p}_j}(\pi_i - 1) > 1$ for $j \neq i$ with $\mathrm{char}(\mathfrak{p}_j) \neq \infty$, and $0 <_{\mathfrak{p}_j} \pi_i <_{\mathfrak{p}_j} 2$ for $j \neq i$ with $\mathrm{char}(\mathfrak{p}_j) = \infty$. Thus, π_i satisfies (S2), (S3) and (S4). □

So in particular, Proposition 2.3.13 applies under our current setting. We write

$$\varphi_{\mathrm{holom},\mathfrak{p}}$$

for the corresponding $\mathcal{L}_{\mathrm{ring}}(K)$-formula constructed there. More precisely, if $\mathfrak{p} \in S$, then $\varphi_{\mathrm{holom},\mathfrak{p}}(a)$ is the formula $\varphi_i(a)$, where i is chosen such that $\mathfrak{p} = \mathfrak{p}_i$ in Lemma 2.4.1. This way we proved the following.

PROPOSITION 2.4.2. *Let $\mathfrak{p} \in S$. Then the following holds:*

(1) $\varphi_{\mathrm{holom},\mathfrak{p}}(F) \subseteq R_{\mathfrak{p}}(F)$.
(2) *If F is* P*S*CL*, then* $\varphi_{\mathrm{holom},\mathfrak{p}}(F) = R_{\mathfrak{p}}(F)$.

DEFINITION 2.4.3. Let $\mathfrak{p} \in S$. If $\mathrm{char}(\mathfrak{p}) \neq \infty$, let $q = |\bar{K}_{\mathfrak{p}}|$, and define the **$\mathfrak{p}$-adic Kochen operator** (of type $(1,1)$ over K) by

$$\gamma_{\mathfrak{p}}(x) = \frac{1}{\pi_{\mathfrak{p}}} \cdot ((x^q - x) - (x^q - x)^{-1})^{-1}$$

if this expression is well defined, and $\gamma_{\mathfrak{p}}(x) = 0$ otherwise. Define the **$\mathfrak{p}$-adic Kochen ring** (of type $(1,1)$ over K) of F by

$$\Gamma_{\mathfrak{p}}(F) = \left\{ \frac{b}{1 + \pi_{\mathfrak{p}} c} : b, c \in \mathcal{O}_{\mathfrak{p}}[\gamma_{\mathfrak{p}}(F)],\ 1 + \pi_{\mathfrak{p}} c \neq 0 \right\}.$$

If $\mathrm{char}(\mathfrak{p}) = \infty$, let

$$\gamma_{\mathfrak{p}}(x) = \gamma(x) = x^2$$

and

$$\Gamma_{\mathfrak{p}}(F) = \mathcal{O}_{\mathfrak{p}}[\gamma(F)],$$

the *semiring* generated by $\gamma(F)$ over $\mathcal{O}_{\mathfrak{p}}$.

LEMMA 2.4.4. *Let $\mathfrak{p} \in S$. Then $\mathcal{S}_{\mathfrak{p}}(F) \neq \emptyset$ if and only if $\pi_{\mathfrak{p}}^{-1} \notin \Gamma_{\mathfrak{p}}(F)$. In that case, $R_{\mathfrak{p}}(F) = \Gamma_{\mathfrak{p}}(F)$.*

PROOF. For the case $\mathrm{char}(\mathfrak{p}) \neq \infty$ see [PR84, 6.4, 6.8, 6.9, 6.14]. For the case $\mathrm{char}(\mathfrak{p}) = \infty$, first note that $\Gamma_{\mathfrak{p}}(F) \subseteq R_{\mathfrak{p}}(F)$. Assume that there exists $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$. Then $\Gamma_{\mathfrak{p}}(F) \subseteq R_{\mathfrak{p}}(F) \subseteq \mathcal{O}_{\mathfrak{P}}$, so $-1 \notin \Gamma_{\mathfrak{p}}(F)$. Conversely, if $-1 \notin \Gamma_{\mathfrak{p}}(F)$, then $\Gamma_{\mathfrak{p}}(F)$ is a pre-positive cone. By

Lemma 1.4.1, $\Gamma_{\mathfrak{p}}(F) = R_{\mathfrak{p}}(F)$. So $\Gamma_{\mathfrak{p}}(F) \neq F$ implies that $\mathcal{S}_{\mathfrak{p}}(F) \neq \emptyset$. □

LEMMA 2.4.5. *Let $\mathfrak{p} \in S$ and let L/F be an extension. If $\mathcal{S}_{\mathfrak{p}}(L) = \emptyset$, then there exists a finitely generated subextension L_0/F of L/F with $\mathcal{S}_{\mathfrak{p}}(L_0) = \emptyset$.*

PROOF. By Lemma 2.4.4, $\pi_{\mathfrak{p}}^{-1} \in \Gamma_{\mathfrak{p}}(L)$, so by the definition of $\Gamma_{\mathfrak{p}}(L)$ there exists a finitely generated extension L_0/F contained in L such that $\pi_{\mathfrak{p}}^{-1} \in \Gamma_{\mathfrak{p}}(L_0)$. Thus, $\mathcal{S}_{\mathfrak{p}}(L_0) = \emptyset$ by Lemma 2.4.4. □

DEFINITION 2.4.6. Let $T_{\mathrm{holom},\mathfrak{p}}$ be the $\mathcal{L}_{\mathrm{ring}}(K)$-theory consisting of the following sentences.

(1) A finite number of sentences stating that $\varphi_{\mathrm{holom},\mathfrak{p}}$ defines a ring (if $\mathrm{char}(\mathfrak{p}) \neq \infty$) resp. a semiring (if $\mathrm{char}(\mathfrak{p}) = \infty$).
(2) For every $a \in \mathcal{O}_{\mathfrak{p}}$ the sentence
$$\varphi_{\mathrm{holom},\mathfrak{p}}(a).$$
(3) The sentence
$$(\forall x)(\varphi_{\mathrm{holom},\mathfrak{p}}(\gamma_{\mathfrak{p}}(x))).$$
(4) If $\mathrm{char}(\mathfrak{p}) \neq \infty$, the sentence
$$(\forall x)(\varphi_{\mathrm{holom},\mathfrak{p}}(x) \wedge 1 + \pi_{\mathfrak{p}} x \neq 0 \to \varphi_{\mathrm{holom},\mathfrak{p}}((1 + \pi_{\mathfrak{p}} x)^{-1})).$$
(5) The sentence
$$\varphi_{\mathrm{holom},\mathfrak{p}}(\pi_{\mathfrak{p}}^{-1}) \to (\forall x)(\varphi_{\mathrm{holom},\mathfrak{p}}(x)).$$

PROPOSITION 2.4.7. *The field F satisfies $T_{\mathrm{holom},\mathfrak{p}}$ if and only if the formula $\varphi_{\mathrm{holom},\mathfrak{p}}$ defines the holomorphy domain $R_{\mathfrak{p}}(F)$ in F.*

PROOF. First suppose that $\varphi_{\mathrm{holom},\mathfrak{p}}(F) = R_{\mathfrak{p}}(F)$. Since a holomorphy domain is a ring resp. a semiring, F satisfies (1). If $R_{\mathfrak{p}}(F) = F$, then F satisfies (2)-(5), so assume that $\mathcal{S}_{\mathfrak{p}}(F) \neq \emptyset$. By Lemma 2.4.4, $\pi_{\mathfrak{p}}^{-1} \notin \Gamma_{\mathfrak{p}}(F)$ and $\Gamma_{\mathfrak{p}}(F) = R_{\mathfrak{p}}(F)$. So since $\mathcal{O}_{\mathfrak{p}} \subseteq \Gamma_{\mathfrak{p}}(F)$ and $\gamma_{\mathfrak{p}}(F) \subseteq \Gamma_{\mathfrak{p}}(F)$, F satisfies (2) and (3). If $\mathrm{char}(\mathfrak{p}) \neq \infty$, $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$ and $x \in \mathcal{O}_{\mathfrak{P}}$, then $v_{\mathfrak{P}}(1 + \pi_{\mathfrak{p}} x) = 0$, so $v_{\mathfrak{P}}((1 + \pi_{\mathfrak{p}} x)^{-1}) = 0$. Hence, if $x \in F$ and F satisfies $\varphi_{\mathrm{holom},\mathfrak{p}}(x)$, then F satisfies $\varphi_{\mathrm{holom},\mathfrak{p}}((1+\pi_{\mathfrak{p}} x)^{-1})$. Therefore, F satisfies also (4). Since $\pi_{\mathfrak{p}}^{-1} \notin \Gamma_{\mathfrak{p}}(F)$, F does not satisfy $\varphi_{\mathrm{holom},\mathfrak{p}}(\pi_{\mathfrak{p}}^{-1})$, and hence satisfies (5).

Conversely suppose that F satisfies $T_{\mathrm{holom},\mathfrak{p}}$. It follows from Proposition 2.4.2(1) that $\varphi_{\mathrm{holom},\mathfrak{p}}(F) \subseteq R_{\mathfrak{p}}(F)$. By (1), $\varphi_{\mathrm{holom},\mathfrak{p}}(F)$ is a ring resp. a semiring. Moreover, by (2) and (3), it contains $\mathcal{O}_{\mathfrak{p}}$ and $\gamma_{\mathfrak{p}}(F)$. If $\mathrm{char}(\mathfrak{p}) \neq \infty$, then $\varphi_{\mathrm{holom},\mathfrak{p}}(F)$ is closed under the map $x \mapsto (1+\pi_{\mathfrak{p}} x)^{-1}$ for x with $1+\pi_{\mathfrak{p}} x \neq 0$. Therefore, $\Gamma_{\mathfrak{p}}(F) \subseteq \varphi_{\mathrm{holom},\mathfrak{p}}(F)$. If $\pi_{\mathfrak{p}}^{-1} \in \Gamma_{\mathfrak{p}}(F)$, then $\pi_{\mathfrak{p}}^{-1} \in \varphi_{\mathrm{holom},\mathfrak{p}}(F)$, so $\varphi_{\mathrm{holom},\mathfrak{p}}(F) = F$ by (5), and thus $\varphi_{\mathrm{holom},\mathfrak{p}}(F) = R_{\mathfrak{p}}(F)$. If $\pi_{\mathfrak{p}}^{-1} \notin \Gamma_{\mathfrak{p}}(F)$, then $\Gamma_{\mathfrak{p}}(F) = R_{\mathfrak{p}}(F)$ by Lemma 2.4.4, so $\varphi_{\mathrm{holom},\mathfrak{p}}(F) = R_{\mathfrak{p}}(F)$. □

2.5. Quantification over Classical Primes

In this section we translate first-order statements concerning the classical primes of F to statements about F and the corresponding holomorphy domains.

LEMMA 2.5.1. *Let $\mathfrak{p} \in S$ with $\operatorname{char}(\mathfrak{p}) \neq \infty$. For $a \in F$ let*

$$H_{\mathfrak{p}}(a) = \{\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F) \colon a \in \mathcal{O}_{\mathfrak{P}}\}.$$

Then the following holds:

(1) *If $a, b \in F$, then $H_{\mathfrak{p}}(a) \cap H_{\mathfrak{p}}(b) = H_{\mathfrak{p}}(a^2 + \pi_{\mathfrak{p}} b^2)$.*
(2) *If $a \in F^\times$, then $\mathcal{S}_{\mathfrak{p}}(F) \setminus H_{\mathfrak{p}}(a) = H_{\mathfrak{p}}((\pi_{\mathfrak{p}} a^2)^{-1})$.*
(3) *If $P(Z_1, \dots, Z_n)$ is a boolean polynomial[1], then there exists a rational function*

$$r(\mathbf{X}) \in \mathbb{Q}(\pi_{\mathfrak{p}})(X_1, \dots, X_n)$$

such that for all $a_1, \dots, a_n \in F$,

$$P(H_{\mathfrak{p}}(a_1), \dots, H_{\mathfrak{p}}(a_n)) = H_{\mathfrak{p}}(r(a_1, \dots, a_n)). \tag{2.1}$$

PROOF.

PROOF OF (1). Let $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$ and $a, b \in F$. If $v_{\mathfrak{P}}(a) \geq 0$ and $v_{\mathfrak{P}}(b) \geq 0$, then $v_{\mathfrak{P}}(a^2 + \pi_{\mathfrak{p}} b^2) \geq 0$ since $v_{\mathfrak{P}}(\pi_{\mathfrak{p}}) \geq 0$. Conversely, if $v_{\mathfrak{P}}(a) < 0$ or $v_{\mathfrak{P}}(b) < 0$, then, since $v_{\mathfrak{P}}(\pi_{\mathfrak{p}}) = 1$, $2v_{\mathfrak{P}}(a) \neq 2v_{\mathfrak{P}}(b) + v_{\mathfrak{P}}(\pi_{\mathfrak{p}})$, and thus $v_{\mathfrak{P}}(a^2 + \pi_{\mathfrak{p}} b^2) = \min\{v_{\mathfrak{P}}(a^2), v_{\mathfrak{P}}(\pi_{\mathfrak{p}} b^2)\} < 0$.

PROOF OF (2). Let $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$ and $a \in F^\times$. If $v_{\mathfrak{P}}(a) \geq 0$, then $v_{\mathfrak{P}}(\pi_{\mathfrak{p}} a^2) \geq v_{\mathfrak{P}}(\pi_{\mathfrak{p}}) > 0$, so $v_{\mathfrak{P}}((\pi_{\mathfrak{p}} a^2)^{-1}) < 0$. Conversely, if $v_{\mathfrak{P}}(a) < 0$, then $v_{\mathfrak{P}}(\pi_{\mathfrak{p}} a^2) \leq -1$, so $v_{\mathfrak{P}}((\pi_{\mathfrak{p}} a^2)^{-1}) \geq 0$.

PROOF OF (3). First note that for $a \in F$, $H_{\mathfrak{p}}(a) = H_{\mathfrak{p}}(a) \cap H_{\mathfrak{p}}(1) = H_{\mathfrak{p}}(a^2 + \pi_{\mathfrak{p}})$ by (1), and $a^2 + \pi_{\mathfrak{p}} \neq 0$. Hence, the set of boolean polynomials $P(\mathbf{Z})$ for which there exists a rational function $r(\mathbf{X}) \in \mathbb{Q}(\pi_{\mathfrak{p}})(X_1, \dots, X_n)$ such that $r(\mathbf{a}) \notin \{0, \infty\}$ and (2.1) hold for all $a_1, \dots, a_n \in F$ contains the boolean polynomials $Z_1, \dots, Z_n$. By (1), it is closed under intersections. By (2), it is closed under complements. Therefore, it is also closed under unions, and hence contains all boolean polynomials. □

REMARK 2.5.2. In what comes, the predicate symbol R of the language $\mathcal{L}_R$ will be used in two different ways. It will interpret either a valuation ring resp. positive cone $\mathcal{O}_{\mathfrak{P}}$, or a holomorphy domain $R_{\mathfrak{p}}(F)$. We write $(F, \mathcal{O}_{\mathfrak{P}})$ and $(F, R_{\mathfrak{p}}(F))$, respectively, for the corresponding structures.

NOTATION 2.5.3. For convenience, we introduce the $\mathcal{L}_R$-formula

$$x \in R^\times$$

[1] see [FJ08, Chapter 7.6]

as an abbreviation for the formula

$$x \in R \wedge x^{-1} \in R.$$

REMARK 2.5.4. Note that formally we work in the language $\mathcal{L}_{\text{ring}}$ of rings, i.e. there is no function $\cdot^{-1}$ in our language. However, it is common to use this function in first-order formulas when working in fields, knowing that it can always be eliminated by introducing a new quantifier. More precisely, if $\varphi(x)$ is a formula, then $\varphi(x^{-1})$ is equivalent in the theory of fields to

$$(\exists y)(xy = 1 \wedge \varphi(y))$$

or

$$x \neq 0 \wedge (\forall y)(xy = 1 \to \varphi(y)).$$

In other words, the function $\cdot^{-1}$ can always be eliminated either by introducing an existential or a universal quantifier. Therefore, we will *not* make use of the function $\cdot^{-1}$ in formulas we claim to be quantifier free, but we will eventually use this function in universal or existential formulas.

PROPOSITION 2.5.5. *Let* $\mathfrak{p} \in S$.

(1) *There exists a recursive map* $\varphi(\mathbf{x}) \mapsto \varphi_{\mathfrak{p},\exists}(\mathbf{x})$ *from existential* $\mathcal{L}_R$*-formulas to* $\mathcal{L}_R(\pi_{\mathfrak{p}})$*-formulas such that for every extension* F/K *and elements* $a_1, \dots, a_n \in F$ *the following statements are equivalent:*
   (1a) *There exists* $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$ *such that* $(F, \mathcal{O}_{\mathfrak{P}}) \models \varphi(\mathbf{a})$.
   (1b) $(F, R_{\mathfrak{p}}(F)) \models \varphi_{\mathfrak{p},\exists}(\mathbf{a})$.

(2) *There exists a recursive map* $\varphi(\mathbf{x}) \mapsto \varphi_{\mathfrak{p},\forall}(\mathbf{x})$ *from universal* $\mathcal{L}_R$*-formulas to* $\mathcal{L}_R(\pi_{\mathfrak{p}})$*-formulas such that for every extension* F/K *and elements* $a_1, \dots, a_n \in F$ *the following statements are equivalent:*
   (2a) $(F, \mathcal{O}_{\mathfrak{P}}) \models \varphi(\mathbf{a})$ *for all* $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$.
   (2b) $(F, R_{\mathfrak{p}}(F)) \models \varphi_{\mathfrak{p},\forall}(\mathbf{a})$.

PROOF. First of all, note that we can get $\varphi_{\mathfrak{p},\forall}$ from $\varphi_{\mathfrak{p},\exists}$ via $\varphi_{\mathfrak{p},\forall} :\Leftrightarrow \neg(\neg\varphi)_{\mathfrak{p},\exists}$. Thus, it suffices to prove (1). For $x \in F$, let $H_{\mathfrak{p}}(x) = \{\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F) \colon x \in \mathcal{O}_{\mathfrak{P}}\}$.

PART A1: CASE $\operatorname{char}(\mathfrak{p}) \neq \infty$. First assume that $\varphi(\mathbf{x})$ is of the simple form

$$\bigwedge_i (f_i(\mathbf{x}) \in R) \wedge \bigwedge_i (g_i(\mathbf{x}) \notin R),$$

where $f_i, g_i \in \mathbb{Z}[\mathbf{X}]$ for all i.

Assume that (1a) holds. Then there exists $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$ with $f_i(\mathbf{a}) \in \mathcal{O}_{\mathfrak{P}}$ and $g_i(\mathbf{a}) \notin \mathcal{O}_{\mathfrak{P}}$ for all i. Hence,

$$\bigcap_i H_{\mathfrak{p}}(f_i(\mathbf{a})) \cap \bigcap_i (\mathcal{S}_{\mathfrak{p}}(F) \smallsetminus H_{\mathfrak{p}}(g_i(\mathbf{a}))) \neq \emptyset,$$

or, equivalently,

$$(\mathcal{S}_{\mathfrak{p}}(F) \smallsetminus \bigcap_i H_{\mathfrak{p}}(f_i(\mathbf{a}))) \cup \bigcup_i H_{\mathfrak{p}}(g_i(\mathbf{a})) \neq \mathcal{S}_{\mathfrak{p}}(F). \tag{2.2}$$

By Lemma 2.5.1(3), applied to the left hand side of inequality (2.2), there exists a rational function $r \in \mathbb{Q}(\pi_{\mathfrak{p}})(\mathbf{X})$ independent of $\mathbf{a}$ such that

$$H_{\mathfrak{p}}(r(\mathbf{a})) = (\mathcal{S}_{\mathfrak{p}}(F) \smallsetminus \bigcap_i H_{\mathfrak{p}}(f_i(\mathbf{a}))) \cup \bigcup_i H_{\mathfrak{p}}(g_i(\mathbf{a})).$$

But if $H_{\mathfrak{p}}(r(\mathbf{a})) \neq \mathcal{S}_{\mathfrak{p}}(F)$ then $r(\mathbf{a}) \notin R_{\mathfrak{p}}(F)$. Therefore, if we let $\varphi_{\mathfrak{p},\exists}(\mathbf{x})$ be the formula

$$\neg(r(\mathbf{x}) \in R),$$

then (1a) implies (1b).

Conversely, suppose that (1b) holds. Then $r(\mathbf{a}) \notin R_{\mathfrak{p}}(F)$, and hence $H_{\mathfrak{p}}(r(\mathbf{a})) \neq \mathcal{S}_{\mathfrak{p}}(F)$. Therefore there exists $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$ with $f_i(\mathbf{a}) \in \mathcal{O}_{\mathfrak{P}}$ and $g_i(\mathbf{a}) \notin \mathcal{O}_{\mathfrak{P}}$ for all i, i.e. (1a) holds.

Part A2: Conclusion of the proof for $\mathrm{char}(\mathfrak{p}) \neq \infty$. Now assume that $\varphi(\mathbf{x})$ is an arbitrary existential $\mathcal{L}_R$-formula in prenex disjunctive normal form, i.e. $\varphi(\mathbf{x})$ is of the form

$$(\exists y_1, \ldots, y_m) \bigvee_j \quad [\bigwedge_i (f_{ij}(\mathbf{x},\mathbf{y}) \in R) \wedge \bigwedge_i (g_{ij}(\mathbf{x},\mathbf{y}) \notin R) \wedge$$
$$\wedge \bigwedge_i (h_{ij}(\mathbf{x},\mathbf{y}) = 0) \wedge \bigwedge_i (k_{ij}(\mathbf{x},\mathbf{y}) \neq 0)],$$

where $f_{ij}, g_{ij}, h_{ij}, k_{ij} \in \mathbb{Z}[\mathbf{X},\mathbf{Y}]$. Let $\varphi_j(\mathbf{x},\mathbf{y})$ be the formula

$$\bigwedge_i (f_{ij}(\mathbf{x},\mathbf{y}) \in R) \wedge \bigwedge_i (g_{ij}(\mathbf{x},\mathbf{y}) \notin R).$$

Then φ_j is of the special form considered in Part A1. Let $\varphi_{\mathfrak{p},\exists}(\mathbf{x})$ be the formula

$$(\exists y_1, \ldots, y_m) \bigvee_j [(\varphi_j)_{\mathfrak{p},\exists}(\mathbf{x},\mathbf{y}) \wedge \bigwedge_i (h_{ij}(\mathbf{x},\mathbf{y}) = 0) \wedge \bigwedge_i (k_{ij}(\mathbf{x},\mathbf{y}) \neq 0)].$$

Then $\varphi_{\mathfrak{p},\exists}$ satisfies the claim. This follows from the fact that existential quantifiers commute with each other (even first and second order quantifiers, as in our case), and with disjunctions. Furthermore, $F \models \bigwedge_i (h_{ij}(\mathbf{x},\mathbf{y}) = 0) \wedge \bigwedge_i (k_{ij}(\mathbf{x},\mathbf{y}) \neq 0)$ if and only if $(F, R_{\mathfrak{p}}(F)) \models \bigwedge_i (h_{ij}(\mathbf{x},\mathbf{y}) = 0) \wedge \bigwedge_i (k_{ij}(\mathbf{x},\mathbf{y}) \neq 0)$.

Part B1: Case $\mathrm{char}(\mathfrak{p}) = \infty$. First of all, assume that $\varphi(\mathbf{x})$ is of the form

$$\bigwedge_i (f_i(\mathbf{x}) \in R)$$

where $f_1, \ldots, f_m \in \mathbb{Z}[\mathbf{X}]$.

Assume that (1a) holds. Then there exists an ordering $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$ with $f_1(\mathbf{a}) \geq_{\mathfrak{P}} 0, \ldots, f_m(\mathbf{a}) \geq_{\mathfrak{P}} 0$. Hence, $R_{\mathfrak{p}}(F)[f_1(\mathbf{a}), \ldots, f_m(\mathbf{a})]$, the semiring generated by $f_1(\mathbf{a}), \ldots, f_m(\mathbf{a})$ over $R_{\mathfrak{p}}(F)$, is contained in $\mathcal{O}_{\mathfrak{P}}$. In particular,

$$R_{\mathfrak{p}}(F)[f_1(\mathbf{a}), \ldots, f_m(\mathbf{a})] \cap (-R_{\mathfrak{p}}(F)) \quad \subseteq \quad \mathcal{O}_{\mathfrak{P}} \cap (-\mathcal{O}_{\mathfrak{P}}),$$

so

$$R_{\mathfrak{p}}(F)[f_1(\mathbf{a}), \ldots, f_m(\mathbf{a})] \cap (-R_{\mathfrak{p}}(F)) \quad = \quad \{0\}. \tag{2.3}$$

Equality (2.3) says that all possible non-zero finite sums

$$\sum_{j=1}^{r} s_j f_1(\mathbf{a})^{k_{j,1}} \cdots f_m(\mathbf{a})^{k_{j,m}},$$

where $s_j \in R_{\mathfrak{p}}(F)$ and $k_{j,l} \geq 0$ for all j, l, are not in $-R_{\mathfrak{p}}(F)$. Hence, if $\varphi_{\mathfrak{p},\exists}(\mathbf{x})$ is the formula

$$\begin{aligned}(\forall s_1, \ldots, s_r \in R) \qquad & (-\sum_{j=1}^{r} s_j f_1(\mathbf{x})^{k_{j,1}} \cdots f_m(\mathbf{x})^{k_{j,m}} \in R_{\mathfrak{p}}(F) \\ & \rightarrow \sum_{j=1}^{r} s_j f_1(\mathbf{x})^{k_{j,1}} \cdots f_m(\mathbf{x})^{k_{j,m}} = 0),\end{aligned}$$

where $r = 2^m$, and $(k_{j,1}, \ldots, k_{j,m})$ ranges over $\{0,1\}^m$, then (1a) implies (1b).

Conversely, suppose that (1b) holds. Then

$$\begin{aligned}(\forall s_1, \ldots, s_r \in R_{\mathfrak{p}}(F)) \qquad & (\sum_{j=1}^{r} s_j f_1(\mathbf{a})^{k_{j,1}} \cdots f_m(\mathbf{a})^{k_{j,m}} \neq 0 \\ & \rightarrow \sum_{j=1}^{r} s_j f_1(\mathbf{a})^{k_{j,1}} \cdots f_m(\mathbf{a})^{k_{j,m}} \notin -R_{\mathfrak{p}}(F)),\end{aligned}$$

where $r = 2^m$, and $(k_{j,1}, \ldots, k_{j,m})$ ranges over $\{0,1\}^m$, holds. Since $F^2 \subseteq R_{\mathfrak{p}}(F)$, this remains true if $r \in \mathbb{N}$ and the $(k_{j,1}, \ldots, k_{j,m})$ are taken from $(\mathbb{Z}_{\geq 0})^m$. Hence, (2.3) holds. Since $-1 \in -R_{\mathfrak{p}}(F)$, $-1 \notin R_{\mathfrak{p}}(F)[f_1(\mathbf{a}), \ldots, f_m(\mathbf{a})]$, so $R_{\mathfrak{p}}(F)[f_1(\mathbf{a}), \ldots, f_m(\mathbf{a})]$ is a pre-positive cone. By Lemma 1.4.1, there exists an ordering $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$ with $f_1(\mathbf{a}) \geq_{\mathfrak{P}} 0, \ldots, f_m(\mathbf{a}) \geq_{\mathfrak{P}} 0$, and hence (1a) holds.

PART B2: CONCLUSION OF THE PROOF FOR $\mathrm{char}(\mathfrak{p}) = \infty$. Now assume that $\varphi(\mathbf{x})$ is an arbitrary existential $\mathcal{L}_R$-formula in prenex disjunctive normal form. Replace $x \notin R$ by $(-x \in R) \wedge (x \neq 0)$ to assume that $\varphi(\mathbf{x})$ is of the form

$$(\exists \mathbf{y}) \bigvee_j [\bigwedge_i (f_{ij}(\mathbf{x}, \mathbf{y}) \in R) \wedge \bigwedge_i (h_{ij}(\mathbf{x}, \mathbf{y}) = 0) \wedge \bigwedge_i (k_{ij}(\mathbf{x}, \mathbf{y}) \neq 0)],$$

where $f_{ij}, h_{ij}, k_{ij} \in \mathbb{Z}[\mathbf{X}, \mathbf{Y}]$. Now conclude the proof as in PART A2.

PART C: RECURSIVITY. Everything in the construction of $\varphi_{\mathfrak{p},\exists}$, like finding the prenex normal form of a formula, or finding the rational function $r \in \mathbb{Q}(\pi_{\mathfrak{p}})(\mathbf{X})$, can be done explicitly. Therefore, the map $\varphi(\mathbf{x}) \mapsto \varphi_{\mathfrak{p},\exists}(\mathbf{x})$ can be chosen to be recursive. □

REMARK 2.5.6. We borrowed the idea for the case $\mathrm{char}(\mathfrak{p}) = \infty$ from Prestel's work [Pre81, p. 154]. The idea for the case $\mathrm{char}(\mathfrak{p}) \neq \infty$ appears in Grob's thesis [Gro87, proof of Theorem 4.01].

2.6. Quantification over Classical Closures

We use the quantification over classical primes of the previous section to quantify over classical closures.

DEFINITION 2.6.1. For $\mathfrak{p} \in S$ with $\mathrm{char}(\mathfrak{p}) \neq \infty$, we fix a finite set $C_{\mathfrak{p}} \subseteq K$ of representatives of $\bar{K}_{\mathfrak{p}}$.

LEMMA 2.6.2. *Let $\mathfrak{p} \in S$ with $\mathrm{char}(\mathfrak{p}) \neq \infty$, and let $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$ be quasi-local (see Definition 2.1.18). Let $n \in \mathbb{N}$ and $r = 2v_{\mathfrak{P}}(n)$. Then the following holds for each $x \in F^{\times}$:*

(1) *$x \notin (F_{\mathfrak{P}}^{\times})^n$ if and only if for all $y \in F$, $v_{\mathfrak{P}}(y^n x - 1) \leq r$.*
(2) *$x \in (F_{\mathfrak{P}}^{\times})^n$ if and only if for all $y \in F$, the following two conditions hold:*
   (2a) *$v_{\mathfrak{P}}(y^n x/\pi_{\mathfrak{p}}^k) \neq 0$ for $1 \leq k < n$.*
   (2b) *If $v_{\mathfrak{P}}(y^n x) = 0$, then*

$$v_{\mathfrak{P}}\left(y^n \left(\sum_{0 \leq j \leq r} c_j \pi_{\mathfrak{p}}^j\right)^n x - 1\right) > r$$

for some $c_0, \ldots, c_r \in C_{\mathfrak{p}}$.

PROOF. Let $\mathcal{O} = R_{\mathfrak{p}}(F_{\mathfrak{P}})$ be the unique valuation ring of $F_{\mathfrak{P}}$ lying over $\mathcal{O}_{\mathfrak{P}}$. Note that $\mathcal{O}^{\times} \cap (F_{\mathfrak{P}}^{\times})^n = (\mathcal{O}^{\times})^n$.

PROOF OF (1). First suppose that $x = z^n$, where $z \in F_{\mathfrak{P}}^{\times}$. We want to show that there exists $y \in F$ such that $v_{\mathfrak{P}}(y^n x - 1) > r$. Since $\mathcal{O}/\mathcal{O}_{\mathfrak{P}}$ is immediate, there exists $u \in F^{\times}$ with $uz \in \mathcal{O}^{\times}$, and thus $u^n x \in \mathcal{O}^{\times}$. Therefore assume without loss of generality that $x \in \mathcal{O}^{\times}$, i.e. $x = z^n$ for some $z \in \mathcal{O}^{\times}$. Since $\pi_{\mathfrak{p}}$ is a uniformizer for $\mathcal{O}$, and $C_{\mathfrak{p}}$ is a set of representatives of $\mathcal{O}/\pi_{\mathfrak{p}}\mathcal{O}$,

$$z^{-1} = c_0 + c_1 \pi_{\mathfrak{p}} + \cdots + c_r \pi_{\mathfrak{p}}^r + w \pi_{\mathfrak{p}}^{r+1},$$

where $c_0, \dots, c_r \in C_\mathfrak{p}$ and $w \in \mathcal{O}$. Then $y := c_0 + c_1\pi_\mathfrak{p} + \dots + c_r\pi_\mathfrak{p}^r \in F$ and

$$\begin{aligned} v_\mathfrak{P}(y^n x - 1) &= v_\mathfrak{P}\left((z^{-1} - w\pi_\mathfrak{p}^{r+1})^n x - 1\right) \\ &= v_\mathfrak{P}\left(\sum_{i=0}^{n} \binom{n}{i} z^{i-n}(-w\pi_\mathfrak{p}^{r+1})^i z^n - 1\right) = \\ &= v_\mathfrak{P}\left(\sum_{i=1}^{n} \binom{n}{i} z^{i}(-w\pi_\mathfrak{p}^{r+1})^i\right) > \\ &> r. \end{aligned}$$

Conversely, suppose there is $y \in F$ with $v_\mathfrak{P}(y^n x - 1) > r$. Then $v_\mathfrak{P}(y^n x) \geq 0$ and the polynomial $f(Z) = Z^n - y^n x \in \mathcal{O}[Z]$ satisfies

$$v_\mathfrak{P}(f(1)) = v_\mathfrak{P}(1 - y^n x) > r = 2v_\mathfrak{P}(n) = 2v_\mathfrak{P}(f'(1)).$$

Therefore, f has a zero in $F_\mathfrak{P}$ by Hensel-Rychlik (Lemma 1.5.3), i.e. $x \in (F_\mathfrak{P}^\times)^n$.

Proof of (2). Suppose that (2a) holds for all $y \in F$. Then $n \nmid v_\mathfrak{P}(x) - k$ for $k = 1, \dots, n-1$. Since $\mathfrak{P}$ is quasi-local, $v_\mathfrak{P}(F^\times)$ is a $\mathbb{Z}$-group (cf. Remark 2.1.19), so $n | v_\mathfrak{P}(x)$. Therefore there is some $y \in F$ such that $v_\mathfrak{P}(y^n x) = 0$. By (2b), there are $c_0, \dots, c_r \in C_\mathfrak{p}$ such that $v_\mathfrak{P}(y^n(\sum_j c_j\pi_\mathfrak{p}^j)^n x - 1) > r$. By (1), $x \in (F_\mathfrak{P}^\times)^n$.

Conversely suppose that $x \in (F_\mathfrak{P}^\times)^n$. Then for all $y \in F$, $n | v_\mathfrak{P}(y^n x)$, so $v_\mathfrak{P}(y^n x/\pi_\mathfrak{p}^k) \neq 0$ for $1 \leq k < n$, i.e. (2a) holds. If $v_\mathfrak{P}(y^n x) = 0$, then there is $z \in \mathcal{O}^\times$ such that $z^n = y^n x$. Write z^{-1} as

$$z^{-1} = c_0 + c_1\pi_\mathfrak{p} + \dots + c_r\pi_\mathfrak{p}^r + w\pi_\mathfrak{p}^{r+1},$$

with $c_0, \dots, c_r \in C_\mathfrak{p}$ and $w \in \mathcal{O}$. Then $y^n(\sum_j c_j\pi_\mathfrak{p}^j)^n x = z^n(z^{-1} - w\pi_\mathfrak{p}^{r+1})^n$, so $v_\mathfrak{P}(y^n(\sum_j c_j\pi_\mathfrak{p}^j)^n x - 1) > r$, and thus (2b) holds. □

Lemma 2.6.3. *Let $\mathfrak{p} \in S$ with $\mathrm{char}(\mathfrak{p}) \neq \infty$, and let $\mathfrak{P} \in \mathcal{S}_\mathfrak{p}(F)$ be quasi-local. Let $n \in \mathbb{N}$ and $r = 2v_\mathfrak{p}(n)$, and write $\mathcal{O} = R_\mathfrak{p}(F_\mathfrak{P})$. Define $\mathcal{L}_R(K)$-formulas*

$$\varphi_n(x, y) \;:\Leftrightarrow\; \pi_\mathfrak{p}^r(y^n x - 1)^{-1} \in R$$

and

$$\begin{aligned} \psi_n(x, y) \;:\Leftrightarrow\; & \Big(\bigwedge_{k=1}^{n-1} y^n x\pi_\mathfrak{p}^{-k} \notin R^\times \wedge (y^n x \in R^\times \rightarrow \\ & \rightarrow \bigvee_{c_0,\dots,c_r \in C_\mathfrak{p}} (y^n(\sum_{0 \leq j \leq r} c_j\pi_\mathfrak{p}^j)^n x - 1)\pi_\mathfrak{p}^{-r-1} \in R)\Big) \end{aligned}$$

Then for $x \in F^\times$ the following are equivalent:

(1) $x \notin (F_\mathfrak{P}^\times)^n$.
(2) $(F_\mathfrak{P}, \mathcal{O}) \models (\forall y)(\varphi_n(x, y))$.

(3) $(F, \mathcal{O}_{\mathfrak{P}}) \models (\forall y)(\varphi_n(x, y))$.

Furthermore, the following are equivalent:

(1′) $x \in (F_{\mathfrak{P}}^{\times})^n$.
(2′) $(F_{\mathfrak{P}}, \mathcal{O}) \models (\forall y)(\psi_n(x, y))$.
(3′) $(F, \mathcal{O}_{\mathfrak{P}}) \models (\forall y)(\psi_n(x, y))$.

PROOF. Note that $(F, \mathcal{O}_{\mathfrak{P}}) \models \varphi_n(x, y)$ if and only if $v_{\mathfrak{P}}(y^n x - 1) \leq r$. By Lemma 2.6.2(1), applied to the field $F_{\mathfrak{P}}$, (1) implies (2). Since the formula $(\forall y)(\varphi_n(x, y))$ is universal, (2) implies (3). By Lemma 2.6.2(1), applied to the field F, (3) implies (1).

Note that $(F, \mathcal{O}_{\mathfrak{P}}) \models \psi_n(x, y)$ if and only if properties (2a) and (2b) of Lemma 2.6.2(2) hold. By Lemma 2.6.2(2), applied to the field $F_{\mathfrak{P}}$, (1′) implies (2′). Since the formula $(\forall y)(\psi_n(x, y))$ is universal, (2′) implies (3′). Finally, by Lemma 2.6.2(2), applied to the field F, (3′) implies (1′). □

REMARK 2.6.4. One could imagine a different approach and define ψ_n from φ_n by using a set of representatives of $F_{\mathfrak{P}}^{\times}/(F_{\mathfrak{P}}^{\times})^n$ as parameters. But since these representatives depend on n, this would imply the use of infinitely many parameters, and would force us in the following lemma to make stronger recursivity assumptions on K – which we wish to avoid at this point. The approach we chose uses only a finite set of parameters for all of the ψ_n.

LEMMA 2.6.5. *Let $\mathfrak{p} \in S$. There exists a recursive map $\varphi(\mathbf{x}) \mapsto \hat{\varphi}_{\mathfrak{p},\forall,R}(\mathbf{x})$ from $\mathcal{L}_{\mathrm{ring}}$-formulas to $\mathcal{L}_R(K)$-formulas such that for every extension F/K and elements $a_1, \ldots, a_m \in F$ the following holds:*

(1) *If $F' \models \varphi(\mathbf{a})$ holds for all $F' \in \mathrm{CC}(F, \mathfrak{p})$, then $(F, R_{\mathfrak{p}}(F)) \models \hat{\varphi}_{\mathfrak{p},\forall,R}(\mathbf{a})$.*
(2) *If $(F, R_{\mathfrak{p}}(F)) \models \hat{\varphi}_{\mathfrak{p},\forall,R}(\mathbf{a})$ and $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$ is quasi-local, then $F_{\mathfrak{P}} \models \varphi(\mathbf{a})$.*

PROOF.

PART A: CASE $\mathrm{char}(\mathfrak{p}) = p \neq \infty$. Recall that the theory of p-adically closed fields of fixed p-rank d has quantifier elimination in the language

$$\mathcal{L}_{P,d} = \mathcal{L}_R \cup \{c_1, \ldots, c_d\} \cup \{P_n \colon n \in \mathbb{N}\},$$

which is the language of rings augmented by a predicate R for the p-valuation ring $\mathcal{O}$, constants $c_1, \ldots, c_d$ for an $\mathbb{F}_p$-basis of $\mathcal{O}/p\mathcal{O}$, and predicates P_n for the n-th powers (Proposition 1.6.3).

In our case, we may choose $c_1, \ldots, c_d$ from K, since for $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$, $v_{\mathfrak{P}}$ and $v_{\mathfrak{p}}$ have the same p-rank, and hence $\mathcal{O}_{\mathfrak{P}}/p\mathcal{O}_{\mathfrak{P}} = \mathcal{O}_{\mathfrak{p}}/p\mathcal{O}_{\mathfrak{p}}$. Therefore, there exists a quantifier free formula $\psi(\mathbf{x})$ in the language $\mathcal{L}_R(K) \cup \{P_n \colon n \in \mathbb{N}\}$ such that for each $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$ and each p-adic closure F' of $(F, v_{\mathfrak{P}})$ with p-valuation ring $\mathcal{O}_{F'}$, and every $\mathbf{a} \in F^m$, $F' \models \varphi(\mathbf{a})$ if and only if $F' \models \psi(\mathbf{a})$. Here $F' \models \psi(\mathbf{a})$ means that R

and P_n are interpreted, respectively, by the p-valuation ring $\mathcal{O}_{F'}$ of F', and the subset $(F')^n$ of n-th powers.

Let $\eta(\mathbf{x})$ be the universal $\mathcal{L}_R(K)$-formula obtained from the disjunctive normal form of $\psi(\mathbf{x})$ by replacing all occurrences of $x \in P_n$ resp. $x \notin P_n$ by the universal $\mathcal{L}_R(K)$-formulas $(\forall y)(\psi_n(x,y))$ resp. $(\forall y)(\varphi_n(x,y))$ constructed in Lemma 2.6.3. If F' is as above, then the prime of F' belonging to $\mathcal{O}_{F'}$ is quasi-local, and hence (1) $\Leftrightarrow$ (2) and (1′) $\Leftrightarrow$ (2′) of Lemma 2.6.3 imply that $F' \models \psi(\mathbf{a})$ if and only if $(F', \mathcal{O}_{F'}) \models \eta(\mathbf{a})$. Let $\hat{\varphi}_{\mathfrak{p},\forall,R}(\mathbf{x})$ be the formula $\eta_{\mathfrak{p},\forall}(\mathbf{x})$ that Proposition 2.5.5 attaches to $\eta(\mathbf{x})$. Then the following are equivalent for every $\mathbf{a} \in F^m$.

(a) $(F, \mathcal{O}_{\mathfrak{P}}) \models \eta(\mathbf{a})$ for all $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$.
(b) $(F, R_{\mathfrak{p}}(F)) \models \hat{\varphi}_{\mathfrak{p},\forall,R}(\mathbf{a})$.

We claim that $\hat{\varphi}_{\mathfrak{p},\forall,R}(\mathbf{x})$ satisfies (1) and (2).

Part A1: Proof of (1). Assume that $F' \models \varphi(\mathbf{a})$ for all $F' \in \mathrm{CC}(F, \mathfrak{P})$, $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$. Then $F' \models \psi(\mathbf{a})$, and hence $(F', \mathcal{O}_{F'}) \models \eta(\mathbf{a})$. Since η is universal, this implies that $(F, \mathcal{O}_{\mathfrak{P}}) \models \eta(\mathbf{a})$ for all $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$. By (a) $\Rightarrow$ (b), $(F, R_{\mathfrak{p}}(F)) \models \hat{\varphi}_{\mathfrak{p},\forall,R}(\mathbf{a})$.

Part A2: Proof of (2). Assume that $(F, R_{\mathfrak{p}}(F)) \models \hat{\varphi}_{\mathfrak{p},\forall,R}(\mathbf{a})$ and $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$ is quasi-local, and let $\mathcal{O} = R_{\mathfrak{p}}(F_{\mathfrak{P}})$. By (b) $\Rightarrow$ (a), $(F, \mathcal{O}_{\mathfrak{P}}) \models \eta(\mathbf{a})$. Recall that η was built from the quantifier free $\mathcal{L}_R(K) \cup \{P_n \colon n \in \mathbb{N}\}$-formula ψ by replacing all atomic formulas $x \in P_n$ resp. $x \notin P_n$ by the universal formulas constructed in Lemma 2.6.3. By (2) $\Leftrightarrow$ (3) and (2′) $\Leftrightarrow$ (3′) of that lemma, these universal formulas are satisfied in $(F, \mathcal{O}_{\mathfrak{P}})$ if and only if they are satisfied in $(F_{\mathfrak{P}}, \mathcal{O})$. Therefore, since $(F, \mathcal{O}_{\mathfrak{P}})$ is a substructure of $(F_{\mathfrak{P}}, \mathcal{O})$, $(F, \mathcal{O}_{\mathfrak{P}}) \models \eta(\mathbf{a})$ implies that $(F_{\mathfrak{P}}, \mathcal{O}) \models \eta(\mathbf{a})$. As mentioned above, this implies that $F_{\mathfrak{P}} \models \psi(\mathbf{a})$. Therefore, $F_{\mathfrak{P}} \models \varphi(\mathbf{a})$, as claimed.

Part B: Case $\mathrm{char}(\mathfrak{p}) = \infty$. The theory of real closed fields has quantifier elimination in the language $\mathcal{L}_{\leq} = \mathcal{L}_{\mathrm{ring}} \cup \{\leq\}$, see Proposition 1.4.5. Thus, replacing $x \leq y$ by by $y - x \in R$, we get a quantifier free $\mathcal{L}_R$-formula $\psi(\mathbf{x})$ such that for every $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$ and $\mathbf{a} \in F^m$, $F_{\mathfrak{P}} \models \varphi(\mathbf{a})$ if and only if $(F_{\mathfrak{P}}, \mathcal{O}) \models \psi(\mathbf{a})$, where $\mathcal{O} = R_{\mathfrak{p}}(F_{\mathfrak{P}})$ is the positive cone (i.e. the set of squares) of $F_{\mathfrak{P}}$. Since the ordering of $F_{\mathfrak{P}}$ extends $\leq_{\mathfrak{P}}$, $(F_{\mathfrak{P}}, \mathcal{O}) \models \psi(\mathbf{a})$ if and only if $(F, \mathcal{O}_{\mathfrak{P}}) \models \psi(\mathbf{a})$. Proposition 2.5.5 gives an $\mathcal{L}_R(K)$-formula $\psi_{\mathfrak{p},\forall}(\mathbf{x})$ such that $(F, R_{\mathfrak{p}}(F)) \models \psi_{\mathfrak{p},\forall}(\mathbf{a})$ if and only if $(F, \mathcal{O}_{\mathfrak{P}}) \models \psi(\mathbf{a})$ for all $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$. Therefore, the $\mathcal{L}_R(K)$-formula $\hat{\varphi}_{\mathfrak{p},\forall,R}(\mathbf{x}) :\Leftrightarrow \psi_{\mathfrak{p},\forall}(\mathbf{x})$ satisfies (1) and (2).

Part C: Recursivity. The formula $\hat{\varphi}_{\mathfrak{p},\forall,R}(\mathbf{x})$ is constructed from φ via quantifier elimination, the formulas φ_n, ψ_n from Lemma 2.6.3, and the map $\eta \mapsto \eta_{\mathfrak{p},\forall}$ of Proposition 2.5.5. The map $\eta \mapsto \eta_{\mathfrak{p},\forall}$ is recursive by Proposition 2.5.5, and since the theory of real closed fields

and the theory of p-adically closed fields of a fixed p-rank are decidable (Proposition 1.6.3 and Proposition 1.4.5), the quantifier elimination can be carried out recursively. Since the formulas φ_n and ψ_n involve only parameters from the finite set $\bigcup_{\mathfrak{p}\in S} C_{\mathfrak{p}} \cup \{\pi_{\mathfrak{p}}\}$, independent of n, replacing $x \in P_n$ and $x \notin P_n$ by the formulas $(\forall y)(\psi_n(x,y))$ resp. $(\forall y)(\varphi_n(x,y))$ from Lemma 2.6.3 can be done recursively. Therefore, the map $\varphi(\mathbf{x}) \mapsto \hat{\varphi}_{\mathfrak{p},\forall,R}(\mathbf{x})$ can be chosen to be recursive. □

PROPOSITION 2.6.6. *Let $\mathfrak{p} \in S$. There exists a recursive map $\varphi(\mathbf{x}) \mapsto \hat{\varphi}_{\mathfrak{p},\forall}(\mathbf{x})$ from $\mathcal{L}_{\mathrm{ring}}$-formulas to $\mathcal{L}_{\mathrm{ring}}(K)$-formulas such that for every extension F/K that satisfies $T_{\mathrm{holom},\mathfrak{p}}$, and for all elements $a_1, \ldots, a_m \in F$ the following holds:*

(1) *If $F' \models \varphi(\mathbf{a})$ for all $F' \in \mathrm{CC}(F,\mathfrak{p})$, then $F \models \hat{\varphi}_{\mathfrak{p},\forall}(\mathbf{a})$.*
(2) *If $F \models \hat{\varphi}_{\mathfrak{p},\forall}(\mathbf{a})$ and $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$ is quasi-local, then $F_{\mathfrak{P}} \models \varphi(\mathbf{a})$.*

PROOF. Combine Lemma 2.6.5 with Proposition 2.4.7. □

2.7. Axiomatization of PSCC Fields

We use the results of the previous section to axiomatize the PSCC property.

LEMMA 2.7.1. *Let $\mathfrak{p} \in S$ and $F' \in \mathrm{CC}(F,\mathfrak{p})$, and let V be a smooth absolutely irreducible variety defined over F. Then $V(F') = \emptyset$ if and only if $\mathcal{S}_{\mathfrak{p}}(F'(V)) = \emptyset$.*

PROOF. This follows from Lemma 1.4.4 and Lemma 1.6.2. □

DEFINITION 2.7.2. Construct an $\mathcal{L}_{\mathrm{ring}}(K)$-theory $T_{\mathrm{P}SCC}$ as follows:

Let

$$f_n(\mathbf{T},\mathbf{Z}) = \sum_{\boldsymbol{\alpha}} T_{\boldsymbol{\alpha}} Z_1^{\alpha_1} \cdots Z_n^{\alpha_n} \in \mathbb{Z}[\mathbf{T},\mathbf{Z}]$$

be the general polynomial in n variables $Z_1, \ldots, Z_n$ of degree n with coefficients $\mathbf{T}$. Here $\boldsymbol{\alpha}$ runs over all n-tuples $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$, $\alpha_i \in \mathbb{Z}_{\geq 0}$, $\sum_{i=1}^n \alpha_i \leq n$.

For $n \in \mathbb{N}$, let $\psi_n(\mathbf{x},\mathbf{y})$ be an $\mathcal{L}_{\mathrm{ring}}$-formula stating that the polynomial $f_n(\mathbf{x},\mathbf{Z})$ with coefficients $\mathbf{x}$ is absolutely irreducible, see for example [FJ08, Chapter 11.3], and all singular points on the affine hypersurface defined by this polynomial lie on the subvariety defined by the polynomial $f_n(\mathbf{y},\mathbf{Z})$ with coefficients $\mathbf{y}$.

Let $\eta_n(\mathbf{x},\mathbf{y})$ be the $\mathcal{L}_{\mathrm{ring}}$-formula

$$(\exists \mathbf{z})(f_n(\mathbf{x},\mathbf{z}) = 0 \wedge f_n(\mathbf{y},\mathbf{z}) \neq 0)$$

stating that the polynomial with coefficients $\mathbf{x}$ has a zero which is not a zero of the polynomial with coefficients $\mathbf{y}$. By Proposition 2.6.6 there exists an $\mathcal{L}_{\mathrm{ring}}(K)$-formula $(\hat{\eta}_n)_{\mathfrak{p},\forall}(\mathbf{x},\mathbf{y})$ such that if F satisfies $T_{\mathrm{holom},\mathfrak{p}}$, then the following holds for all tuples $\mathbf{a},\mathbf{b}$ from F.

(a) If $F' \models \eta_n(\mathbf{a},\mathbf{b})$ for all $F' \in \mathrm{CC}(F,\mathfrak{p})$, then $F \models (\hat{\eta}_n)_{\mathfrak{p},\forall}(\mathbf{a},\mathbf{b})$.

(b) If $F \models (\hat{\eta}_n)_{\mathfrak{p},\forall}(\mathbf{a},\mathbf{b})$ and $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$ is quasi-local, then $F_{\mathfrak{P}} \models \eta_n(\mathbf{a},\mathbf{b})$.

Let φ_n be the $\mathcal{L}_{\mathrm{ring}}(K)$-sentence

$$(\forall \mathbf{x},\mathbf{y})[(\psi_n(\mathbf{x},\mathbf{y}) \wedge \bigwedge_{\mathfrak{p}\in S}(\hat{\eta}_n)_{\mathfrak{p},\forall}(\mathbf{x},\mathbf{y})) \to \eta_n(\mathbf{x},\mathbf{y})].$$

Let $T_{\mathrm{P}S\mathrm{CC}}$ consist of the following sentences.

(1) For every $\mathfrak{p} \in S$, the theory $T_{\mathrm{holom},\mathfrak{p}}$.
(2) For every $n \in \mathbb{N}$, the sentence φ_n.

PROPOSITION 2.7.3. *The field F satisfies $T_{\mathrm{P}S\mathrm{CC}}$ if and only if F is* PSCC.

PROOF. First assume that F is PSCC. Then F is also PSCL (cf. Remark 2.2.6). Hence, if $\mathfrak{p} \in S$, then $\varphi_{\mathrm{holom},\mathfrak{p}}$ defines $R_{\mathfrak{p}}(F)$ in F by Proposition 2.4.2. Therefore, by Proposition 2.4.7, F satisfies $T_{\mathrm{holom},\mathfrak{p}}$. Thus, F satisfies (1).

By Proposition 2.2.11, each $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$ is quasi-local. By (b), for all tuples $\mathbf{a},\mathbf{b}$ from F, if $F \models (\hat{\eta}_n)_{\mathfrak{p},\forall}(\mathbf{a},\mathbf{b})$ then $F_{\mathfrak{P}} \models \eta_n(\mathbf{a},\mathbf{b})$ for every $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$. Therefore, if $F \models \psi_n(\mathbf{a},\mathbf{b}) \wedge \bigwedge_{\mathfrak{p}\in S}(\hat{\eta}_n)_{\mathfrak{p},\forall}(\mathbf{a},\mathbf{b})$, then the conditions

$$f_n(\mathbf{a},\mathbf{Z}) = 0, \quad f_n(\mathbf{b},\mathbf{Z}) \neq 0 \tag{2.4}$$

define a non-singular variety V which has an $F_{\mathfrak{P}}$-rational point for every $\mathfrak{P} \in \mathcal{S}_S(F)$. Therefore, since F is PSCL, V has an F-rational point, so $F \models \eta_n(\mathbf{a},\mathbf{b})$. Consequently, F satisfies (2).

Conversely, assume that F satisfies $T_{\mathrm{P}S\mathrm{CC}}$. Then, for all $\mathfrak{p} \in S$, F satisfies $T_{\mathrm{holom},\mathfrak{p}}$. Let V be any absolutely irreducible smooth variety over F that has an F'-rational point for every $F' \in \mathrm{CC}(F,S)$. Then the F'-rational points are Zariski-dense on V, as follows from Lemma 2.7.1. Therefore, assume without loss of generality that V is given by tuples $\mathbf{a}$ resp. $\mathbf{b}$ from F as in (2.4). Thus, $F' \models \eta_n(\mathbf{a},\mathbf{b})$ for every $F' \in \mathrm{CC}(F,S)$. Therefore, by (a), $F \models (\hat{\eta}_n)_{\mathfrak{p},\forall}(\mathbf{a},\mathbf{b})$. Since F satisfies (2), $F \models \eta_n(\mathbf{a},\mathbf{b})$, i.e. V has an F-rational point, and so F is PSCC. □

REMARK 2.7.4. Note that Proposition 2.7.3 gives an $\mathcal{L}_{\mathrm{ring}}$-axiomatization of P$p$C, PRC, and PC_M fields, cf. Remark 2.2.7.

REMARK 2.7.5. We can use our results to prove the conjecture posed by Darnière in [Dar01, Remark 11]: If $\mathcal{F}$ is a finite family of fields taken among $\mathbb{R}$ and the finite extensions of the fields $\hat{\mathbb{Q}}_p$, and $\mathbf{Q}_{\mathcal{F}}$ is the maximal Galois extension of $\mathbb{Q}$ contained in every $F \in \mathcal{F}$, then there exists a finite extension $K/\mathbb{Q}$ contained in $\mathbf{Q}_{\mathcal{F}}$ and a finite set of primes S of K such that $\mathbf{Q}_{\mathcal{F}}$ is PSCC. Hence, $\mathbf{Q}_{\mathcal{F}}$ is 'restricted RC-local' by Proposition 2.7.3, and $R_{\mathcal{F}}$ is $\mathcal{L}_{\mathrm{ring}}(K)$-definable in $\mathbf{Q}_{\mathcal{F}}$ by Proposition 2.4.2.

REMARK 2.7.6. If fact, with a little more effort, our method can be extended to allow finite initial ramification and finite residue field extension of the p-valuations, and hence to cover all 'PCC' fields of [Pop03].

COROLLARY 2.7.7. *Let $\mathfrak{p} \in S$ and let $\varphi(\mathbf{x})$ be an $\mathcal{L}_{\mathrm{ring}}$-formula. The $\mathcal{L}_{\mathrm{ring}}(K)$-formula $\hat{\varphi}_{\mathfrak{p},\forall}(\mathbf{x})$ of Proposition 2.6.6 satisfies the following: For every* PSCC *field $F \supseteq K$ and for all elements $a_1, \ldots, a_m \in F$ the following are equivalent:*

(1) $F \models \hat{\varphi}_{\mathfrak{p},\forall}(\mathbf{a})$.
(2) $F' \models \varphi(\mathbf{a})$ *for all* $F' \in \mathrm{CC}(F, \mathfrak{p})$.

PROOF. By Proposition 2.7.3, F satisfies $T_{\mathrm{holom},\mathfrak{p}}$. Furthermore, by Proposition 2.2.11, every $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$ is quasi-local. Thus, the equivalence of (1) and (2) follows from Proposition 2.6.6. □

2.8. The Strong Approximation Property

In this section we discuss the 'strong approximation property' and prove that every PSCC field satisfies this property. We need the strong approximation property for the characterization of totally S-adic extensions in terms of holomorphy domains, which follows in the next section.

DEFINITION 2.8.1. Let $\tilde{\mathcal{S}}(F)$ be the set of *all* primes of F, and let $\tilde{\mathcal{S}}_{\mathfrak{p}}(F)$ be the subset of those lying over $\mathfrak{p} \in S$. We equip $\tilde{\mathcal{S}}(F)$ with the following **Zariski-topology**: A subbasis is given by sets of the form

$$H(a) = \{\mathfrak{P} \in \tilde{\mathcal{S}}(F) \colon a \in \mathcal{O}_{\mathfrak{P}}\},$$

where $a \in F$. A set $\mathcal{S} \subseteq \tilde{\mathcal{S}}(F)$ is **profinite** if $\mathcal{S}$, as a subspace of $\tilde{\mathcal{S}}(F)$, is a profinite space. We say that $\mathcal{S}$ satisfies **SAP** (the Strong Approximation Property) if $\mathcal{S}$ is profinite and the family $H(a) \cap \mathcal{S}$, $a \in F$, is closed under finite intersections.

Let $\tilde{\mathcal{S}}_{\mathcal{P}}(F) = \tilde{\mathcal{S}}(F) \setminus \tilde{\mathcal{S}}_{\infty}(F)$ be the set of non-archimedean primes of F. We also consider the following (finer) **patch topology** on $\tilde{\mathcal{S}}_{\mathcal{P}}(F)$: A subbasis is given by sets of the form

$$H_{\mathcal{P}}(a) = \{\mathfrak{P} \in \tilde{\mathcal{S}}_{\mathcal{P}}(F) \colon v_{\mathfrak{P}}(a) \geq 0\}$$

and

$$H'_{\mathcal{P}}(a) = \{\mathfrak{P} \in \tilde{\mathcal{S}}_{\mathcal{P}}(F) \colon v_{\mathfrak{P}}(a) > 0\},$$

where $a \in F$.

LEMMA 2.8.2. *For every $\mathfrak{p} \in S$, $\mathcal{S}_{\mathfrak{p}}(F)$ is profinite, and the family $H(a) \cap \mathcal{S}_{\mathfrak{p}}(F)$, $a \in F$, is closed under complements (in $\mathcal{S}_{\mathfrak{p}}(F)$).*

PROOF.

PART A: CASE $\mathrm{char}(\mathfrak{p}) \neq \infty$. First note that for $a \in F^{\times}$,

$$H_{\mathcal{P}}(a) = \tilde{\mathcal{S}}_{\mathcal{P}}(F) \setminus H'_{\mathcal{P}}(a^{-1}),$$

so $H_{\mathcal{P}}(a)$ is open-closed in the patch topology. By Lemma 2.5.1(2),

$$\mathcal{S}_{\mathfrak{p}}(F) \setminus H_{\mathcal{P}}(a) = H_{\mathcal{P}}((\pi_{\mathfrak{p}} a^2)^{-1}) \cap \mathcal{S}_{\mathfrak{p}}(F),$$

so the family $H_{\mathcal{P}}(a) \cap \mathcal{S}_{\mathfrak{p}}(F)$, $a \in F$, is closed under complements and the patch topology on $\mathcal{S}_{\mathfrak{p}}(F)$ coincides with the Zariski-topology. By [HJP07, Proposition 8.2], the patch topology on $\tilde{\mathcal{S}}_{\mathcal{P}}(F)$ is profinite. Hence, also the closed subset

$$\tilde{\mathcal{S}}_{\mathfrak{p}}(F) = \bigcap_{a \in \mathcal{O}_{\mathfrak{p}}} H_{\mathcal{P}}(a) \cap \bigcap_{a \in K \setminus \mathcal{O}_{\mathfrak{p}}} (\tilde{\mathcal{S}}_{\mathcal{P}}(F) \setminus H_{\mathcal{P}}(a))$$

is profinite. Therefore, it suffices to show that $\mathcal{S}_{\mathfrak{p}}(F)$ is closed in $\tilde{\mathcal{S}}_{\mathfrak{p}}(F)$.

Claim A1. The set

$$\mathcal{S}_1 := \{\mathfrak{P} \in \tilde{\mathcal{S}}_{\mathfrak{p}}(F) \colon v_{\mathfrak{P}} \text{ is discrete and } v_{\mathfrak{P}}(\pi_{\mathfrak{p}}) = 1\}$$

is closed in $\tilde{\mathcal{S}}_{\mathfrak{p}}(F)$.

Indeed, for $\mathfrak{P} \in \tilde{\mathcal{S}}_{\mathfrak{p}}(F)$, $v_{\mathfrak{P}}(\pi_{\mathfrak{p}})$ is the smallest positive element of the value group $v_{\mathfrak{P}}(F^\times)$ if and only if for all $a \in F^\times$, $v_{\mathfrak{P}}(a) \leq 0$ or $v_{\mathfrak{P}}(a) \geq v_{\mathfrak{P}}(\pi_{\mathfrak{p}})$. Thus,

$$\mathcal{S}_1 = \tilde{\mathcal{S}}_{\mathfrak{p}}(F) \cap \bigcap_{a \in F^\times} (H_{\mathcal{P}}(a^{-1}) \cup H_{\mathcal{P}}(\pi_{\mathfrak{p}}^{-1} a))$$

is closed.

Claim A2. The set $\mathcal{S}_{\mathfrak{p}}(F) = \{\mathfrak{P} \in \mathcal{S}_1 \colon \bar{F}_{\mathfrak{P}} = \bar{K}_{\mathfrak{p}}\}$ is closed in $\mathcal{S}_1$.

Indeed, let $\mathcal{F} = \{f \in \mathcal{O}_{\mathfrak{p}}[X] \colon \bar{f} \in \bar{K}_{\mathfrak{p}}[X] \text{ has no zero in } \bar{K}_{\mathfrak{p}}\}$. Then for $\mathfrak{P} \in \mathcal{S}_1$, $\bar{F}_{\mathfrak{P}} = \bar{K}_{\mathfrak{p}}$ if and only if no $f \in \mathcal{F}$ has a zero in $\bar{F}_{\mathfrak{P}}$. That is,

$$\mathcal{S}_{\mathfrak{p}}(F) \;=\; \mathcal{S}_1 \cap \bigcap_{f \in \mathcal{F}} \bigcap_{a \in F^\times} H(\pi_{\mathfrak{p}}^{-1} a^{-1}) \cup H(f(a)^{-1}),$$

and this proves the claim.

Part B: Case $\operatorname{char}(\mathfrak{p}) = \infty$. Since for $a \in F^\times$, $\mathcal{S}_{\mathfrak{p}}(F) \setminus H(a) = H(-a) \cap \mathcal{S}_{\mathfrak{p}}(F)$, the family $H(a) \cap \mathcal{S}_{\mathfrak{p}}(F)$ is closed under complements. By [Pre84, 6.5], the Zariski-topology on the space $\mathcal{S}_\infty(F)$ of orderings is profinite. Since each of the sets $H(a) \cap \mathcal{S}_\infty(F)$ is closed in $\mathcal{S}_\infty(F)$,

$$\mathcal{S}_{\mathfrak{p}}(F) = \bigcap_{a \in \mathcal{O}_{\mathfrak{p}}} H(a) \cap \mathcal{S}_\infty(F)$$

is closed in $\mathcal{S}_\infty(F)$, and hence profinite. □

Lemma 2.8.3. *If* $\operatorname{char}(\mathfrak{p}) \neq \infty$, *then* $\mathcal{S}_{\mathfrak{p}}(F)$ *satisfies* SAP.

Proof. By Lemma 2.8.2, $\mathcal{S}_{\mathfrak{p}}(F)$ is profinite. By Lemma 2.5.1(1), the family $H(a) \cap \mathcal{S}_{\mathfrak{p}}(F)$, $a \in F$, is closed under finite intersections. Hence, $\mathcal{S}_{\mathfrak{p}}(F)$ satisfies SAP. □

DEFINITION 2.8.4. We say that F is **S-SAP** if $\mathcal{S}_\mathfrak{p}(F)$ satisfies SAP for each $\mathfrak{p} \in S$.

LEMMA 2.8.5. *If F/K is algebraic, then F is S-SAP.*

PROOF. Let $\mathfrak{p} \in S$. If $\mathrm{char}(\mathfrak{p}) \neq \infty$, then $\mathcal{S}_\mathfrak{p}(F)$ satisfies SAP by Lemma 2.8.3. If $\mathrm{char}(\mathfrak{p}) = \infty$, let $a, b \in F$. Then, since F/K is algebraic, there exists a finite subextension L/K of F/K such that $a, b \in L$. Since L/K is finite, $\mathcal{S}_\mathfrak{p}(L)$ is finite and every $\mathfrak{P} \in \mathcal{S}_\mathfrak{p}(L)$ is local. Therefore, Lemma 1.5.1 gives $c \in L$ such that for $\mathfrak{P} \in \mathcal{S}_\mathfrak{p}(L)$, $1 \leq_\mathfrak{P} c \leq_\mathfrak{P} 3$ if $a, b \in \mathcal{O}_\mathfrak{P}$, and $-3 \leq_\mathfrak{P} c \leq_\mathfrak{P} -1$ otherwise. If $\mathfrak{P} \in \mathcal{S}_\mathfrak{p}(F)$, then $\mathfrak{P}|_L \in \mathcal{S}_\mathfrak{p}(L)$, hence $c \in \mathcal{O}_\mathfrak{P}$ if and only if $a, b \in \mathcal{O}_\mathfrak{P}$, i.e. $H(a) \cap H(b) \cap \mathcal{S}_\mathfrak{p}(F) = H(c) \cap \mathcal{S}_\mathfrak{p}(F)$. Thus, $\mathcal{S}_\mathfrak{p}(F)$ satisfies SAP. □

If F is PRC, then $\mathcal{S}_\infty(F)$ satisfies SAP, see [Pre81, Proposition 1.3]. In fact this holds for every PSCC field. We prove this by combining the construction of Section 2.3 with the specific polynomial constructed by Prestel.

LEMMA 2.8.6. *For $a, b \in F^\times$, let*

$$f_{a,b}(X, Y) = abX^2Y^2 + aX^2 + bY^2 - 1 \in F[X, Y].$$

If $\mathfrak{p} \in S$ with $\mathrm{char}(\mathfrak{p}) = \infty$, and $\mathfrak{P} \in \mathcal{S}_\mathfrak{p}(F)$, then the following holds:

1. *$f_{a,b}$ has a zero in $F_\mathfrak{P}$.*
2. *If $x, y \in F$ and $f_{a,b}(x, y) >_\mathfrak{P} -1$, then $ab(ax^2 + by^2) \geq_\mathfrak{P} 0$ if and only if $a \geq_\mathfrak{P} 0$ and $b \geq_\mathfrak{P} 0$.*

PROOF.

PROOF OF (1). First note that

$$f_{a,b}(X, Y) = aX^2(bY^2 + 1) + (bY^2 - 1).$$

One can choose $y \in F$ such that $(-\frac{1}{a})\frac{by^2-1}{by^2+1} >_\mathfrak{P} 0$. Indeed, if $a >_\mathfrak{P} 0$, let $y = 0$. If $a <_\mathfrak{P} 0$ and $b >_\mathfrak{P} 0$, let $y = 1 + b^{-1}$. If $a <_\mathfrak{P} 0$ and $b <_\mathfrak{P} 0$, let $y = 1 - b^{-1}$. Since $F_\mathfrak{P}$ is real closed, there exists $x \in F_\mathfrak{P}$ such that $x^2 = (-\frac{1}{a})\frac{by^2-1}{by^2+1}$, hence $f_{a,b}(x, y) = 0$.

PROOF OF (2). First note that $f_{a,b}(0, 0) = -1$, so $x \neq 0$ or $y \neq 0$. Furthermore, $f_{a,b}(x, y) >_\mathfrak{P} -1$ implies that

$$ax^2 + by^2 >_\mathfrak{P} -abx^2y^2. \tag{2.5}$$

If $a >_\mathfrak{P} 0$ and $b >_\mathfrak{P} 0$, then $ab(ax^2 + by^2) \geq_\mathfrak{P} 0$. If $a <_\mathfrak{P} 0$ and $b <_\mathfrak{P} 0$, then $ab >_\mathfrak{P} 0$ and $ax^2 + by^2 <_\mathfrak{P} 0$ (since $x \neq 0$ or $y \neq 0$), so $ab(ax^2 + by^2) <_\mathfrak{P} 0$. If $a >_\mathfrak{P} 0$ and $b <_\mathfrak{P} 0$, or $a <_\mathfrak{P} 0$ and $b >_\mathfrak{P} 0$, then $ab <_\mathfrak{P} 0$ and thus $ab(ax^2 + by^2) <_\mathfrak{P} -a^2b^2x^2y^2 \leq_\mathfrak{P} 0$ by (2.5). □

PROPOSITION 2.8.7. *If F is PSCC, then F is S-SAP.*

PROOF. Let $\mathfrak{p} \in S$. If $\mathrm{char}(\mathfrak{p}) \neq \infty$, then $S_{\mathfrak{p}}(F)$ satisfies SAP by Lemma 2.8.3. Therefore, assume that $\mathrm{char}(\mathfrak{p}) = \infty$, and let $a, b \in F^{\times}$.

We want to use the polynomials constructed in Section 2.3. Recall Lemma 2.4.1, which gives a translation from our current setting to Setting 2.3.1. Let

$$G_{a,b}(X, Y, Z) = H_2(Z)(1 - A_i(X)C(X)f_{a,b}(X, Y)) - H_2(1),$$

where $A_i, C, H_u, f_{a,b}$ are as in Lemma 2.3.5 (where π_i is chosen according to Lemma 2.4.1), Lemma 2.3.9, Lemma 2.3.11, and Lemma 2.8.6. By (A1), (C1), and Lemma 2.8.6(1), $A_i(X)C(X)f_{a,b}(X, Y)$ has a zero in $F_{\mathfrak{P}}$ for each $\mathfrak{P} \in \mathcal{S}_S(F)$. Since F is PSCC, (H3) and Lemma 2.3.4 imply that there exist $x, y, z \in F$ such that $G_{a,b}(x, y, z) = 0$. Thus, if $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$, then

$$1 - A_i(x)C(x)f_{a,b}(x, y) = \frac{H_2(1)}{H_2(z)} \leq_{\mathfrak{P}} \frac{5}{4},$$

by (H1) and (H2), so

$$A_i(x)C(x)f_{a,b}(x, y) \geq_{\mathfrak{P}} -\frac{1}{4}.$$

Since $A_i(x)C(x) >_{\mathfrak{P}} 1$ by (A5) and (C2), this implies that

$$f_{a,b}(x, y) \geq_{\mathfrak{P}} -\frac{1}{4} >_{\mathfrak{P}} -1.$$

Therefore, by Lemma 2.8.6(2),

$$H(a) \cap H(b) \cap \mathcal{S}_{\mathfrak{p}}(F) = H(c) \cap \mathcal{S}_{\mathfrak{p}}(F),$$

where

$$c = ab(ax^2 + by^2) \in F.$$

Hence, $\mathcal{S}_{\mathfrak{p}}(F)$ satisfies SAP, as claimed. □

2.9. Totally S-adic Field Extensions

We define totally S-adic field extensions and describe them in terms of holomorphy domains.

DEFINITION 2.9.1. Let $\mathfrak{p} \in S$. If M/F is an extension, let

$$\mathrm{res}_{\mathfrak{p}} \colon \mathcal{S}_{\mathfrak{p}}(M) \to \mathcal{S}_{\mathfrak{p}}(F)$$

given by

$$\mathfrak{Q} \mapsto \mathfrak{Q}|_F$$

be the **restriction map** (cf. Definition 2.1.4).

LEMMA 2.9.2. *If $\mathfrak{p} \in S$ and M/F is an extension, then the restriction map $\mathrm{res}_{\mathfrak{p}} \colon \mathcal{S}_{\mathfrak{p}}(M) \to \mathcal{S}_{\mathfrak{p}}(F)$ is continuous in the Zariski-topology (Definition 2.8.1).*

PROOF. Let $a \in F$. The inverse image under $\mathrm{res}_{\mathfrak{p}}$ of the basic open set $\{\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F) \colon a \in \mathcal{O}_{\mathfrak{P}}\}$ is the basic open set $\{\mathfrak{Q} \in \mathcal{S}_{\mathfrak{p}}(M) \colon a \in \mathcal{O}_{\mathfrak{Q}}\}$. Hence, $\mathrm{res}_{\mathfrak{p}}$ is continuous. □

DEFINITION 2.9.3. Let $\mathfrak{p} \in S$. We call an extension M/F **totally $\mathfrak{p}$-adic** if the restriction map $\mathrm{res}_{\mathfrak{p}} \colon \mathcal{S}_{\mathfrak{p}}(M) \to \mathcal{S}_{\mathfrak{p}}(F)$ is surjective. We call M/F **totally S-adic** if M/F is totally $\mathfrak{p}$-adic for each $\mathfrak{p} \in S$.

REMARK 2.9.4. Note that if $K = \mathbb{Q}$ and $|S| = 1$, then our notion of totally S-adic extensions coincides with the classical notions of totally real extensions (as in [Pre81], [Ers82]) resp. totally p-adic extensions (as in [Gro87], [Jar91]). The following lemmas unify results from these works.

REMARK 2.9.5. In [HJP09b] there is a section titled 'Totally S_1-adic Extensions', and there is a definition of a 'maximal totally S_1-adic extension'. However, note that the 'maximal totally S_1-adic extension' of K is *not* a maximal totally S-adic extension in our sense (where $S = S_1$).

LEMMA 2.9.6. *Let $\mathfrak{p} \in S$. If M/F is an extension and $\mathcal{S}_{\mathfrak{p}}(F)$ satisfies* SAP*, then the following statements are equivalent:*

(1) *M/F is totally $\mathfrak{p}$-adic.*
(2) *$R_{\mathfrak{p}}(M) \cap F = R_{\mathfrak{p}}(F)$.*
(3) *$R_{\mathfrak{p}}(M) \cap F \subseteq R_{\mathfrak{p}}(F)$.*

PROOF. PROOF OF (1) ⇒ (2). Assume that M/F is totally $\mathfrak{p}$-adic. Then

$$R_{\mathfrak{p}}(F) = \bigcap_{\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)} \mathcal{O}_{\mathfrak{P}} = \bigcap_{\mathfrak{Q} \in \mathcal{S}_{\mathfrak{p}}(M)} (\mathcal{O}_{\mathfrak{Q}} \cap F) = R_{\mathfrak{p}}(M) \cap F.$$

PROOF OF (2) ⇒ (3). This is trivial.

PROOF OF (3) ⇒ (1). Assume that the restriction map $\mathrm{res}_{\mathfrak{p}} \colon \mathcal{S}_{\mathfrak{p}}(M) \to \mathcal{S}_{\mathfrak{p}}(F)$ is not surjective. By Lemma 2.8.2, $\mathcal{S}_{\mathfrak{p}}(M)$ and $\mathcal{S}_{\mathfrak{p}}(F)$ are profinite spaces. Hence, since $\mathrm{res}_{\mathfrak{p}}$ is continuous (Lemma 2.9.2), $\mathrm{res}_{\mathfrak{p}}(\mathcal{S}_{\mathfrak{p}}(M))$ is closed in $\mathcal{S}_{\mathfrak{p}}(F)$. Therefore, $\mathcal{S}_{\mathfrak{p}}(F) \setminus \mathrm{res}_{\mathfrak{p}}(\mathcal{S}_{\mathfrak{p}}(M))$ is nonempty and open. If follows that the complement of a basic open-closed set contained in $\mathcal{S}_{\mathfrak{p}}(F) \setminus \mathrm{res}_{\mathfrak{p}}(\mathcal{S}_{\mathfrak{p}}(M))$ is an open-closed proper subset X of $\mathcal{S}_{\mathfrak{p}}(F)$ containing $\mathrm{res}_{\mathfrak{p}}(\mathcal{S}_{\mathfrak{p}}(M))$.

By Lemma 2.8.2, the subbasis $H(a) \cap \mathcal{S}_{\mathfrak{p}}(F)$, $a \in F$, of $\mathcal{S}_{\mathfrak{p}}(F)$ is closed under complements. Hence, since $\mathcal{S}_{\mathfrak{p}}(F)$ satisfies SAP, $X = H(x) \cap \mathcal{S}_{\mathfrak{p}}(F)$ for some $x \in F$ by Lemma 1.3.5. Therefore,

$$\mathrm{res}_{\mathfrak{p}}(\mathcal{S}_{\mathfrak{p}}(M)) \subseteq H(x) \cap \mathcal{S}_{\mathfrak{p}}(F) \subsetneqq \mathcal{S}_{\mathfrak{p}}(F).$$

Then $x \in R_{\mathfrak{p}}(M) \cap F$ but $x \notin R_{\mathfrak{p}}(F)$, so $R_{\mathfrak{p}}(M) \cap F \not\subseteq R_{\mathfrak{p}}(F)$. □

COROLLARY 2.9.7. *Assume that F is* PSCC. *If $F \prec M$ is an elementary extension, then M/F is regular and totally S-adic.*

PROOF. Every elementary extension is regular, see for example [FJ08, 7.3.3]. By Proposition 2.7.3, since F is PSCC and $M \equiv F$, M is PSCC. Thus, by Proposition 2.4.2, since $F \prec M$, $R_{\mathfrak{p}}(M) \cap F = R_{\mathfrak{p}}(F)$ for each $\mathfrak{p} \in S$. By Proposition 2.8.7, since F is PSCC, F is S-SAP. Therefore, by Lemma 2.9.6, M/F is totally S-adic. □

LEMMA 2.9.8. *The field F is* PSCC *if and only if for every domain $R = F[x_1, \ldots, x_n]$ which is finitely generated over F and whose quotient field M is regular and totally S-adic over F, there exists an F-homomorphism $R \to F$.*

PROOF. First assume that F is PSCC. If M/F is regular, then R is the coordinate ring of an absolutely irreducible affine variety V defined over F. Let $\mathfrak{p} \in S$ and $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$. By Proposition 2.2.11, since F is PSCC, $\mathfrak{P}$ is quasi-local. If M/F is totally S-adic, there exists $\mathfrak{Q} \in \mathcal{S}_{\mathfrak{p}}(M)$ lying over $\mathfrak{P}$. Then $M_{\mathfrak{Q}} \supseteq F_{\mathfrak{P}}(V)$, hence $\mathcal{S}_{\mathfrak{p}}(F_{\mathfrak{P}}(V)) \neq \emptyset$. Thus, since $F_{\mathfrak{P}} \in \mathrm{CC}(F, \mathfrak{P})$, V has a simple $F_{\mathfrak{P}}$-rational point by Lemma 2.7.1. So since F is PSCC, V has an F-rational point, and therefore there exists an F-homomorphism $R \to F$.

Conversely, let V be an absolutely irreducible affine variety over F, and assume that it has an F'-rational point for every $F' \in \mathrm{CC}(F, S)$. Then $R = F[V]$ is a domain which is finitely generated over F and whose quotient field $M = F(V)$ is regular over F. Let $\mathfrak{p} \in S$, $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$, and $F' \in \mathrm{CC}(F, \mathfrak{P})$. Then $\mathcal{S}_{\mathfrak{p}}(F'(V)) \neq \emptyset$ by Lemma 2.7.1, so if $\mathfrak{Q} \in \mathcal{S}_{\mathfrak{p}}(F'(V))$, then $\mathfrak{Q}|_M \in \mathcal{S}_{\mathfrak{p}}(M)$ and $\mathfrak{Q}|_F = \mathfrak{P}$, hence M/F is totally S-adic. Consequently, by assumption there exists an F-homomorphism $R \to F$, i.e. V has an F-rational point, as claimed. □

LEMMA 2.9.9. *Let M/F be an algebraic extension. Then the following holds:*

1. $\mathrm{CC}(M, S) \subseteq \mathrm{CC}(F, S)$.
2. *If M/F is totally S-adic Galois and F is S-quasi-local, then* $\mathrm{CC}(M, S) = \mathrm{CC}(F, S)$.
3. *If N/F is totally S-adic Galois, $F \subseteq M \subseteq N$ is a subextension, and F is S-quasi-local, then* $\mathrm{CC}(F, S) = \mathrm{CC}(M, S) = \mathrm{CC}(N, S)$.

PROOF. PROOF OF (1). Let $\mathfrak{Q} \in \mathcal{S}_{\mathfrak{p}}(M)$ and let $M' \in \mathrm{CC}(M, \mathfrak{Q})$. Since $\mathrm{tp}(\mathfrak{Q}) = \mathrm{tp}(\mathfrak{Q}|_F) = \mathrm{tp}(\mathfrak{p})$, and M'/F is algebraic, $M' \in \mathrm{CC}(F, \mathfrak{Q}|_F) \subseteq \mathrm{CC}(F, S)$, as claimed.

PROOF OF (2). Let $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$, and let $F' \in \mathrm{CC}(F, \mathfrak{P})$. Since $\mathfrak{P}$ is quasi-local, $F' \cong_F F_{\mathfrak{P}}$. Since M/F is totally S-adic, there exists

$\mathfrak{Q} \in \mathcal{S}_{\mathfrak{p}}(M)$ with $\mathfrak{Q}|_F = \mathfrak{P}$. Then $F_{\mathfrak{P}} \subseteq M_{\mathfrak{Q}}$, so $F_{\mathfrak{P}} = M_{\mathfrak{Q}}$ since $F_{\mathfrak{P}} \in \mathrm{CC}(F, \mathfrak{P})$. Thus, $F_{\mathfrak{P}} \in \mathrm{CC}(M, S)$. Hence, since M/F is Galois, $F' \in \mathrm{CC}(M, S)$, as claimed.

PROOF OF (3). Since $\mathrm{CC}(N, S) \subseteq \mathrm{CC}(M, S) \subseteq \mathrm{CC}(F, S)$ by (1), and $\mathrm{CC}(N, S) = \mathrm{CC}(F, S)$ by (2), $\mathrm{CC}(F, S) = \mathrm{CC}(M, S) = \mathrm{CC}(N, S)$. □

2.10. The Classical Closures of a PSCL Field

We prove that local primes of an algebraic PSCL field lie over primes in S.

LEMMA 2.10.1. *Let $\mathfrak{p}$ be a local prime of K which is not contained in S. If F is* PSCL*, then $\mathcal{S}_{\mathfrak{p}}(F) = \emptyset$.*

PROOF. Let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ and $S' = S \cup \{\mathfrak{p}_{n+1}\}$, where $\mathfrak{p}_{n+1} = \mathfrak{p}$. By Lemma 2.4.1, we can apply Setting 2.3.1 to S'. Let $a \in F$ be arbitrary.

PART A: CASE $\mathrm{char}(\mathfrak{p}) \neq \infty$. Let

$$G_{i,a}(X, Y) = A_i(Y)(1 + \pi_i^{-4} A_i(X) B_i(X) D_{i,a}(X)) - A_i(1)$$

be as in Lemma 2.3.8 applied to S' and $i = n + 1$. Let $\mathfrak{P} \in \mathcal{S}_S(F) = \mathcal{S}_{S'}(F) \setminus \mathcal{S}_{\mathfrak{p}}(F)$. We claim that

$$A_i(X) B_i(X) D_{i,a}(X)$$

has a zero in $F_{\mathfrak{P}}$. Indeed, if $\mathrm{char}(\mathfrak{P}) \neq 2$, this follows from (A1). If $\mathrm{char}(\mathfrak{P}) = 2$, this follows from (B1).

Assume without loss of generality that $A_i(1) \neq 0$. By Lemma 2.3.4 and (A4), $G_{i,a}$ is absolutely irreducible and has a simple zero in $F_{\mathfrak{P}}$ for all $\mathfrak{P} \in \mathcal{S}_S(F)$. Since F is PSCL, $G_{i,a}$ has a zero in F. Hence, by Lemma 2.3.8(1), $v_{\mathfrak{P}}(a) \geq 0$ for all $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$. So since $a \in F$ was arbitrary, $\mathcal{S}_{\mathfrak{p}}(F) = \emptyset$, as claimed.

PART B: CASE $\mathrm{char}(\mathfrak{p}) = \infty$. Let $u \in F^\times$ and let

$$G_{i,a,u}(X, Y) = H_u(Y)(1 + A_i(X) C(X) E_a(X)) - H_u(1)$$

be as in Lemma 2.3.12 applied to S' and $i = n+1$. Let $\mathfrak{P} \in \mathcal{S}_S(F)$. We claim that $A_i(X) C(X) E_a(X)$ has a zero in $F_{\mathfrak{P}}$. Indeed, if $\mathrm{char}(\mathfrak{P}) \neq 2$, this follows from (A1). If $\mathrm{char}(\mathfrak{P}) = 2$, it follows from (C1).

Assume without loss of generality that $H_u(1) \neq 0$. By Lemma 2.3.4, (H3), and the assumption that F is PSCL, it follows that $G_{i,a,u}$ has a zero in F. Hence, Lemma 2.3.12(1) implies that $a \geq_{\mathfrak{P}} -\frac{1}{u^2}$ for all $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$. Consequently, since u was arbitrary, $a \geq_{\mathfrak{P}} 0$. Hence, since a was arbitrary, $\mathcal{S}_{\mathfrak{p}}(F) = \emptyset$, as claimed. □

PROPOSITION 2.10.2. *Let $\mathfrak{P}$ be a local prime of F. If F/K is algebraic and F is* PSCL*, then $\mathfrak{P}|_K \in S$.*

PROOF. Since F/K is algebraic, there exists a finite extension K_1/K contained in F such that $\mathrm{tp}(\mathfrak{P}) = \mathrm{tp}(\mathfrak{P}|_{K_1})$. Let $S_1 = \mathcal{S}_S(K_1)$. Then $\mathcal{S}_S(F) = \mathcal{S}_{S_1}(F)$, and F is PS_1CL. Since K_1/K is finite, S_1 is finite. Therefore, assume without loss of generality that $K = K_1$.

Let $\mathfrak{p} = \mathfrak{P}|_K$. Since $\mathfrak{P}$ is local, also $\mathfrak{p}$ is local. Since $\mathrm{tp}(\mathfrak{P}) = \mathrm{tp}(\mathfrak{p})$, $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$. In particular, $\mathcal{S}_{\mathfrak{p}}(F) \neq \emptyset$. Therefore, $\mathfrak{p} \in S$ by Lemma 2.10.1, as claimed. □

REMARK 2.10.3. With the generalization of our results indicated in Remark 2.7.6, one could prove Proposition 2.10.2 for arbitrary PSCL fields F and for arbitrary classical primes $\mathfrak{P}$ of F.

REMARK 2.10.4. In the case that F is PAC, Proposition 2.10.2 follows from the theorem of Frey-Prestel, see [FJ08, 11.5.1] and [FJ08, 11.5.5]. The case of PRC and PpC fields is proven in [GJ91]. The general case appears in [Pop03, Theorem 2.9].

2.11. A PSCC Embedding Lemma

In this section we prove an embedding theorem for PSCC fields. It generalizes the 'PAC Embedding Lemma' of [JK75] (cf. [FJ08, 20.2.2]), and the proofs are very similar. A slightly more general statement, in fact a generalization to 'PCC' fields, appears in [Pop86]. The work [Dar01] contains a further generalization to certain rings with an 'RC-local' quotient field. The special case of PRC fields is proven in [Ers84], and a partial case for PpC fields in [Kün89b].

LEMMA 2.11.1. *If $\mathfrak{P}$ is a classical prime of F with $F \in \mathrm{CC}(F, \mathfrak{P})$, and E is a field with $\mathrm{Gal}(E) \cong \mathrm{Gal}(F)$, then there exists a classical prime $\mathfrak{Q}$ of E with $\mathrm{tp}(\mathfrak{Q}) = \mathrm{tp}(\mathfrak{P})$ and $E \in \mathrm{CC}(E, \mathfrak{Q})$.*

PROOF. If $\mathrm{char}(\mathfrak{P}) = \infty$, this follows from Proposition 1.4.3. If $\mathrm{char}(\mathfrak{P}) \neq \infty$, it follows from Proposition 1.6.6. □

LEMMA 2.11.2. *Let $K \subseteq E \subseteq F$, $\mathfrak{p} \in S$, $\mathfrak{Q} \in \mathcal{S}_{\mathfrak{p}}(F)$ and $\mathfrak{P} = \mathfrak{Q}|_E \in \mathcal{S}_{\mathfrak{p}}(E)$. If $F' \in \mathrm{CC}(F, \mathfrak{Q})$, then $E' := F' \cap \tilde{E} \in \mathrm{CC}(E, \mathfrak{P})$ and* res: $\mathrm{Gal}(F') \to \mathrm{Gal}(E')$ *is an isomorphism. In particular, if $F' \in \mathrm{CC}(F, \mathfrak{p})$, then $E' := F' \cap \tilde{E} \in \mathrm{CC}(E, \mathfrak{p})$.*

PROOF. The field E' is algebraically closed in the real closed resp. p-adically closed field F', so it is real closed resp. p-adically closed itself, see Lemma 1.4.2 and Lemma 1.6.1. Let $\mathfrak{Q}'$ be the unique prime of F' over $\mathfrak{Q}$. Then $\mathfrak{P}' = \mathfrak{Q}'|_{E'}$ is the unique classical prime of E' with $\mathrm{char}(\mathfrak{P}') = \mathrm{char}(\mathfrak{Q}')$. Moreover, $\mathrm{tp}(\mathfrak{P}') = \mathrm{tp}(\mathfrak{P}'|_E) = \mathrm{tp}(\mathfrak{p})$, so $E' \in \mathrm{CC}(E, \mathfrak{P}'|_E)$. Since $\mathfrak{P}'|_E = \mathfrak{Q}'|_E = \mathfrak{P}$, it follows that $E' \in \mathrm{CC}(E, \mathfrak{P})$.

Since $E' \equiv F'$ by model completeness (Proposition 1.4.5 and Proposition 1.6.3), and $\mathrm{Gal}(F')$ is finitely generated (Proposition 1.4.3 and

Lemma 1.6.5), $\mathrm{Gal}(E') \cong \mathrm{Gal}(F')$ by Lemma 1.3.4. Thus the epimorphism res: $\mathrm{Gal}(F') \to \mathrm{Gal}(E')$ is an isomorphism by Lemma 1.3.2(3). □

LEMMA 2.11.3. *Let $\mathfrak{p} \in S$, let L/K be an extension, and assume that E, F are linearly disjoint extensions of L. If $L \in \mathrm{CC}(L, \mathfrak{p})$, $E \in \mathrm{CC}(E, \mathfrak{p})$, and $F \in \mathrm{CC}(F, \mathfrak{p})$, then $\mathcal{S}_\mathfrak{p}(EF) \neq \emptyset$.*

PROOF. By Lemma 2.11.2, E/L and F/L are regular. Hence, EF/L is regular, since E and F are linearly disjoint over L. Suppose that $\mathcal{S}_\mathfrak{p}(EF) = \emptyset$. By Lemma 2.4.5, there exist finitely generated subextensions E_0/L of E/L and F_0/L of F/L such that $\mathcal{S}_\mathfrak{p}(E_0F_0) = \emptyset$.

The fields E_0, F_0, E_0F_0 are function fields of varieties V, W, $V \times W$ over L. By Lemma 2.7.1, since $\mathcal{S}_\mathfrak{p}(E_0) \neq \emptyset$ and $\mathcal{S}_\mathfrak{p}(F_0) \neq \emptyset$, V and W have simple L-rational points. This implies that also $V \times W$ has a simple L-rational point, so $\mathcal{S}_\mathfrak{p}(E_0F_0) \neq \emptyset$, again by Lemma 2.7.1, a contradiction. □

REMARK 2.11.4. The real case of this lemma occurs in [Pre81] and [Ers83b], where it is attributed to [vdD78]. The p-adic case is proven in [Gro87] and [Kün89b].

PROPOSITION 2.11.5. *Let $L \supseteq K$ and let E/L, F/L be regular extensions, where E is countable and F is $\aleph_1$-saturated and* PSCC. *Then for every homomorphism*

$$\gamma\colon \mathrm{Gal}(F) \to \mathrm{Gal}(E)$$

with $\mathrm{res}_{\tilde{E}/\tilde{L}} \circ \gamma = \mathrm{res}_{\tilde{F}/\tilde{L}}|_{\mathrm{Gal}(F)}$, there exists an L-embedding

$$\tilde{E} \to \tilde{F}$$

such that $\gamma(\tau) = \tau|_{\tilde{E}}$ for all $\tau \in \mathrm{Gal}(F)$.

PROOF.

PART A: THE FIELD CROSSING ARGUMENT. Assume without loss of generality that E and F are linearly disjoint over L and contained in a common field. Then $\tilde{E}$ and $\tilde{F}$ are linearly disjoint over $\tilde{L}$. So since $\mathrm{res}_{\tilde{E}/\tilde{L}} \circ \gamma = \mathrm{res}_{\tilde{F}/\tilde{L}}|_{\mathrm{Gal}(F)}$, the homomorphism γ defines an embedding

$$\varphi\colon \mathrm{Gal}(F) \to \mathrm{Gal}(\tilde{E}\tilde{F}/EF)$$

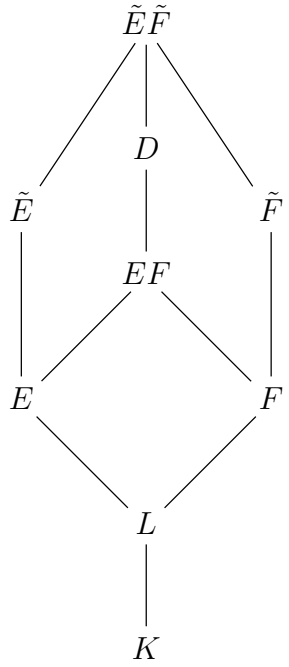
with

$$\mathrm{res}_{\tilde{E}\tilde{F}/\tilde{F}} \circ \varphi = \mathrm{id}_{\mathrm{Gal}(F)} \quad \text{and} \quad \mathrm{res}_{\tilde{E}\tilde{F}/\tilde{E}} \circ \varphi = \gamma,$$

see for example [FJ08, 2.5.5]. Let D be the fixed field of $\varphi(\mathrm{Gal}(F))$ in $\tilde{E}\tilde{F}$. Then

$$\mathrm{res}_{\tilde{E}\tilde{F}/\tilde{F}}\colon \mathrm{Gal}(\tilde{E}\tilde{F}/D) \to \mathrm{Gal}(F)$$

is an isomorphism, hence D/F is regular. The situation is as follows.



PART B: CLAIM. D/F is totally S-adic.

Let $\mathfrak{p} \in S$, $\mathfrak{P} \in \mathcal{S}_\mathfrak{p}(F)$, $F' \in \mathrm{CC}(F, \mathfrak{P})$, and $\mathfrak{P}' \in \mathcal{S}_\mathfrak{p}(F')$. Then $L' = \tilde{L} \cap F' \in \mathrm{CC}(L, \mathfrak{p})$, and $\mathrm{res}_{\tilde{F}/\tilde{L}}$ is injective on $\mathrm{Gal}(F')$ by Lemma 2.11.2. Since $\mathrm{res}_{\tilde{E}/\tilde{L}} \circ \gamma = \mathrm{res}_{\tilde{F}/\tilde{L}}|_{\mathrm{Gal}(F)}$, also γ is injective on $\mathrm{Gal}(F')$, and L' is the algebraic closure of L in the fixed field E' of $\gamma(\mathrm{Gal}(F'))$ in $\tilde{E}$. By Lemma 2.11.1, there exists a classical prime $\mathfrak{Q}'$ of E' with $\mathrm{tp}(\mathfrak{Q}') = \mathrm{tp}(\mathfrak{P})$ and $E' \in \mathrm{CC}(E', \mathfrak{Q}')$. Since L' is algebraically closed in both F' and E', $\mathfrak{Q}'|_{L'} = \mathfrak{P}'|_{L'}$ by Lemma 2.11.2, so $E' \in \mathrm{CC}(E, \mathfrak{p})$.

By Lemma 2.11.2, $\mathrm{res}_{\tilde{E}/\tilde{L}}\colon \mathrm{Gal}(E') \to \mathrm{Gal}(L')$ is an isomorphism, so $E'\tilde{L} = \tilde{E}$. Hence, $E'\tilde{F} = \tilde{E}\tilde{F}$ and thus $\mathrm{res}_{\tilde{E}\tilde{F}/\tilde{F}}$ is injective on $\mathrm{Gal}(\tilde{E}\tilde{F}/E'F')$. Together with $\mathrm{res}_{\tilde{E}\tilde{F}/\tilde{F}} \circ \varphi = \mathrm{id}_{\mathrm{Gal}(F)}$ this implies that $\mathrm{Gal}(\tilde{E}\tilde{F}/E'F') \subseteq \varphi(\mathrm{Gal}(F'))$. In particular, $E'F' \supseteq D$. By Lemma 2.11.3, there exists $\mathfrak{Q} \in \mathcal{S}_\mathfrak{p}(E'F')$. Since $F' \subseteq E'F'$ and $F' \in \mathrm{CC}(F, \mathfrak{P})$, $\mathfrak{Q}|_F = \mathfrak{P}$. Thus $\mathfrak{Q}|_D \in \mathcal{S}_\mathfrak{p}(D)$ extends $\mathfrak{P}$, and this proves the CLAIM.

PART C: CONCLUSION OF THE PROOF. Since $\tilde{E}\tilde{F} = D\tilde{F}$ and $\tilde{E}\tilde{F}/D$ is algebraic, $\tilde{E} \subseteq \tilde{E}\tilde{F} = D[\tilde{F}] = \tilde{F}[D]$. Hence, since $\tilde{E}$ is countable, there exists a countable subset $D_0 \subseteq D$ such that $\tilde{E} \subseteq \tilde{F}[D_0]$. Since F is PSCC and D/F is totally S-adic by the CLAIM, Lemma 2.9.8 implies that for every finite subset D_1 of D_0, there is an F-homomorphism $F[D_1] \to F$. Therefore, since F is $\aleph_1$-saturated, there exists an F-homomorphism $F[D_0] \to F$. Since D/F is regular, the latter homomorphism extends to an $\tilde{F}$-homomorphism $\delta\colon \tilde{F}[D_0] \to \tilde{F}$.

For $\tau \in \mathrm{Gal}(F)$ and $x \in \tilde{F} \cup D_0$, $\delta(\varphi(\tau)x) = \tau(\delta(x))$. Indeed, if $x \in \tilde{F}$, then $\delta(\varphi(\tau)x) = \delta(\tau x) = \tau x = \tau(\delta x)$, since $\mathrm{res}_{\tilde{E}\tilde{F}/\tilde{F}} \circ \varphi = \mathrm{id}_{\mathrm{Gal}(F)}$ and $\delta|_{\tilde{F}} = \mathrm{id}_{\tilde{F}}$. And if $x \in D_0$, then $\delta(\varphi(\tau)x) = \delta(x) = \tau(\delta(x))$ since $\varphi(\mathrm{Gal}(F)) = \mathrm{Gal}(\tilde{E}\tilde{F}/D)$ and $\delta(D_0) \subseteq F$. Therefore the restriction of δ to $\tilde{E}$ satisfies all of the requirements. $\square$

CHAPTER 3

Absolute Galois Group Piles

Starting from a Hilbertian field K and a finite set S of primes of K, [HJP09b] proves that for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, the absolute Galois group of $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$ is a free product of a free part and S-local subgroups. The proof depends on properties of the structures that consist of the groups and all the S-local subgroups. These structures are called 'group piles'. In Chapter 4 and Chapter 5 we use this notion to investigate the model theory of the fields $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$ and $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$.

For this chapter, we fix a finite set S not containing 0. All notions of this chapter depend on S. Furthermore, let $e \leq \omega$ be an ordinal number.

3.1. Group Piles

We introduce the subgroup functor and the category of group piles.

DEFINITION 3.1.1. Let $G = \varprojlim_N G/N$ be a profinite group, where N runs over all open normal subgroups of G. Then the set

$$\mathrm{Subgr}(G)$$

of all closed subgroups of G is equipped with a profinite topology, induced by $\mathrm{Subgr}(G) = \varprojlim_N \mathrm{Subgr}(G/N)$. A basis of open-closed sets for this topology is given by sets of the form

$$\{\Gamma \in \mathrm{Subgr}(G) \colon \Gamma N = HN\},$$

where N is an open normal subgroup of G and H is a closed subgroup of G. The group G acts continuously on $\mathrm{Subgr}(G)$ by conjugation.

A homomorphism $\alpha\colon G \to H$ of profinite groups induces a map

$$\mathrm{Subgr}(\alpha)\colon \mathrm{Subgr}(G) \to \mathrm{Subgr}(H)$$

given by $\Gamma \mapsto \alpha(\Gamma)$.

LEMMA 3.1.2. *The map* Subgr *is a covariant functor from the category of profinite groups (with homomorphisms) to the category of profinite spaces (with continuous maps).*

PROOF. We only have to show that if $\alpha\colon G \to H$ is a homomorphism of profinite groups, then the induced map $\mathrm{Subgr}(G) \to \mathrm{Subgr}(H)$ is continuous. Since $\mathrm{Subgr}(H) = \varprojlim_N \mathrm{Subgr}(H/N)$, it suffices to prove that

$\mathrm{Subgr}(G) \to \mathrm{Subgr}(H/N)$ is continuous, where N is an open normal subgroup of H. Since

$$\begin{array}{ccc} G & \longrightarrow & H \\ \downarrow & & \downarrow \\ G/\alpha^{-1}(N) & \longrightarrow & H/N \end{array}$$

commutes, also

$$\begin{array}{ccc} \mathrm{Subgr}(G) & \longrightarrow & \mathrm{Subgr}(H) \\ \downarrow & & \downarrow \\ \mathrm{Subgr}(G/\alpha^{-1}(N)) & \longrightarrow & \mathrm{Subgr}(H/N) \end{array}$$

commutes. Since $\mathrm{Subgr}(G/\alpha^{-1}(N))$ is discrete, and the vertical arrows are continuous, the claim follows. □

LEMMA 3.1.3. *If H is a closed subgroup of a profinite group G, then* $\mathrm{Subgr}(H)$ *is a closed subspace of* $\mathrm{Subgr}(G)$.[1]

PROOF. By Lemma 3.1.2, the inclusion $\mathrm{Subgr}(H) \to \mathrm{Subgr}(G)$ is continuous. Since both spaces are compact Hausdorff, the inclusion is closed, and thus a topological embedding. □

DEFINITION 3.1.4. A **group pile** is a structure

$$\mathbf{G} = (G, \mathcal{G}_0, \mathcal{G}_\mathfrak{p})_{\mathfrak{p} \in S}$$

consisting of

(1) a profinite group G,
(2) a nonempty G-invariant closed subset $\mathcal{G}_0 \subseteq \mathrm{Subgr}(G)$ such that the elements of $\mathcal{G}_0$ are pairwise conjugate in G, and
(3) a G-invariant closed subset $\mathcal{G}_\mathfrak{p} \subseteq \mathrm{Subgr}(G)$ for each $\mathfrak{p} \in S$.

We let

$$\mathcal{G} = \bigcup_{\mathfrak{p} \in S} \mathcal{G}_\mathfrak{p}.$$

REMARK 3.1.5. Condition (2) says that $\mathcal{G}_0$ consists of a single G-orbit in $\mathrm{Subgr}(G)$, i.e. there exists $G_0 \in \mathcal{G}_0$ such that $\mathcal{G}_0 = (G_0)^G := \{(G_0)^g \colon g \in G\}$. Hence, our notion of group piles coincides with the group piles of [HJP09b], except for a small difference in notation concerning $\mathcal{G}_0$. The notion of group piles is also related to the 'Δ^*-groups' in [Ers95], [Ers96a], and [Ers99].

DEFINITION 3.1.6. The **order** resp. **rank** of $\mathbf{G}$ is the order resp. (profinite) rank of G. A **finite** group pile is a group pile of finite order. We call $\mathbf{G}$ **self-generated** if there exists $G_0 \in \mathcal{G}_0$ such that $G = \langle G_0, \mathcal{G} \rangle$,

[1] That is, $\mathrm{Subgr}(H)$ is a closed subset of $\mathrm{Subgr}(G)$ and the inclusion $\mathrm{Subgr}(H) \to \mathrm{Subgr}(G)$ is a topological embedding.

i.e. G is generated by G_0 and the groups in $\mathcal{G}_\mathfrak{p}$, $\mathfrak{p} \in S$. It is called **bare** if $\mathcal{G} = \{1\}$, and **deficient** if $\mathcal{G}_0 = \{1\}$. The **deficient reduct** of $\mathbf{G}$ is

$$\mathbf{G}^{\mathrm{def}} = (G, \{1\}, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S}.$$

Instead of $(G, \{1\}, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S}$, we also write $(G, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S}$. We call $\mathbf{G}$ **separated** if the sets $\mathcal{G}_\mathfrak{p}$, $\mathfrak{p} \in \{0\} \cup S$, are disjoint, and **reduced** if there are no non-trivial inclusions among the elements of $\mathcal{G}$.

Remark 3.1.7. Note that if $\mathbf{G}$ is self-generated, then $G = \langle G_0, \mathcal{G}\rangle$ for *any* $G_0 \in \mathcal{G}_0$.

Definition 3.1.8. A **homomorphism** of group piles

$$f\colon (G, \mathcal{G}_0, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S} \to (H, \mathcal{H}_0, \mathcal{H}_\mathfrak{p})_{\mathfrak{p}\in S}$$

is a homomorphism of profinite groups $f\colon G \to H$ such that $f(\mathcal{G}_\mathfrak{p}) \subseteq \mathcal{H}_\mathfrak{p}$ for each $\mathfrak{p} \in \{0\} \cup S$. It is an **epimorphism** if $f\colon G \to H$ is surjective and $f(\mathcal{G}_\mathfrak{p}) = \mathcal{H}_\mathfrak{p}$ for each $\mathfrak{p} \in \{0\} \cup S$. It is an **isomorphism** if in addition $f\colon G \to H$ is an isomorphism. The homomorphism f is called **rigid** if $f|_\Gamma$ is injective for each $\Gamma \in \mathcal{G}$.

If N is a closed normal subgroup of G, let

$$\mathcal{G}_{\mathfrak{p},N} = \{\Gamma N/N\colon \Gamma \in \mathcal{G}_\mathfrak{p}\} \subseteq \mathrm{Subgr}(G/N).$$

Then the **quotient**

$$\mathbf{G}/N = (G/N, \mathcal{G}_{0,N}, \mathcal{G}_{\mathfrak{p},N})_{\mathfrak{p}\in S}$$

is again a group pile. The quotient map $G \to G/N$ extends to an epimorphism of group piles $\mathbf{G} \to \mathbf{G}/N$, and every epimorphism of group piles is of this form.

Remark 3.1.9. We identify the category of bare deficient group piles (with homomorphisms) with the category of profinite groups (with homomorphisms) via the forgetful functor $(G, \mathcal{G}_0, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S} \mapsto G$.

Definition 3.1.10. Let I be a directed set. An **inverse system** of group piles (over I) is a family $\mathbf{G}_i = (G_i, \mathcal{G}_{i,0}, \mathcal{G}_{i,\mathfrak{p}})_{\mathfrak{p}\in S}$, $i \in I$, of group piles with epimorphisms $\pi_{ji}\colon \mathbf{G}_j \to \mathbf{G}_i$ $(i \le j)$ that satisfy $\pi_{ii} = \mathrm{id}_{\mathbf{G}_i}$ and $\pi_{ji} \circ \pi_{kj} = \pi_{ki}$ $(i \le j \le k)$.

The **inverse limit**

$$\mathbf{G} = (G, \mathcal{G}_0, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S} = \varprojlim_{i\in I} \mathbf{G}_i$$

is defined as follows: Let

$$G := \varprojlim_{i\in I} G_i$$

be the inverse limit of profinite groups. Then

$$\mathrm{Subgr}(G) = \varprojlim_{i\in I} \mathrm{Subgr}(G_i),$$

so

$$\mathcal{G}_\mathfrak{p} := \varprojlim_{i\in I} \mathcal{G}_{i,\mathfrak{p}} \subseteq \mathrm{Subgr}(G)$$

is a closed subset of $\mathrm{Subgr}(G)$ for each $\mathfrak{p} \in \{0\} \cup S$. Since all $\mathcal{G}_{i,\mathfrak{p}}$ are G_i-invariant, $\mathcal{G}_\mathfrak{p}$ is G-invariant. Since each $\mathcal{G}_{i,0}$ consists of a single G_i-orbit, $\mathcal{G}_0$ consists of a single G-orbit. Therefore, $\mathbf{G}$ is indeed a group pile.

The failure of a deficient group pile $\mathbf{G}$ to be self-generated can be measured by a certain quotient $\bar{\mathbf{G}}$ of $\mathbf{G}$. We introduce some notions related to that quotient.

LEMMA 3.1.11. *Let $\mathbf{G} = (G, \mathcal{G}_0, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S}$ be a group pile and $H \leq G$ a closed subgroup with $\Gamma \leq H$ for all $\Gamma \in \mathcal{G}$. Then $\mathcal{G}_\mathfrak{p}$ is closed in $\mathrm{Subgr}(H)$ for each $\mathfrak{p} \in S$.*

PROOF. Since $\mathcal{G}_\mathfrak{p}$ is closed in $\mathrm{Subgr}(G)$ and is contained in the subspace $\mathrm{Subgr}(H)$ (Lemma 3.1.3), it is also closed in that subspace. □

DEFINITION 3.1.12. For a group pile $\mathbf{G} = (G, \mathcal{G}_0, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S}$ let

$$G' := \langle \mathcal{G} \rangle$$

be the closed subgroup generated by the subgroups in $\mathcal{G}_\mathfrak{p}$, $\mathfrak{p} \in S$. Then, by Lemma 3.1.11,

$$\mathbf{G}' := (G', \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S}$$

is a (self-generated and deficient) group pile. Since $\mathcal{G}$ is G-invariant, G' is normal in G. Hence, the quotient

$$\bar{\mathbf{G}} := \mathbf{G}/G'$$

is a (bare) group pile.

LEMMA 3.1.13. *If $\varphi\colon \mathbf{G} \to \mathbf{H}$ is an epimorphism of group piles, then $\varphi(G') = H'$.*

PROOF. By definition of an epimorphism of group piles, $\varphi(\mathcal{G}) = \mathcal{H}$. Hence, since φ is continuous and closed, $\varphi(\langle \mathcal{G} \rangle) = \langle \mathcal{H} \rangle$, as claimed. □

DEFINITION 3.1.14. Let $\varphi\colon \mathbf{G} \to \mathbf{H}$ be an epimorphism of group piles. By Lemma 3.1.13, its restriction

$$\varphi'\colon \mathbf{G}' \to \mathbf{H}'$$

is an epimorphism of self-generated deficient group piles. Moreover, the induced map

$$\bar{\varphi}\colon \bar{\mathbf{G}} \to \bar{\mathbf{H}}$$

is an epimorphism of bare group piles.

LEMMA 3.1.15. *The map* $\mathbf{G} \mapsto \mathbf{G}'$ *(resp.* $\mathbf{G} \mapsto \bar{\mathbf{G}}$*) is a covariant functor from the category of group piles with epimorphisms to the category of self-generated deficient group piles with epimorphisms (resp. the category of bare group piles with epimorphisms).*

PROOF. This follows from Lemma 3.1.13. □

LEMMA 3.1.16. *Let* $\mathbf{G} = (G, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S}$ *be a deficient group pile and* $\mathbf{A} = A$ *a bare deficient group pile. Then the map* $\varphi \mapsto \bar{\varphi}$ *gives a bijection between the epimorphisms from* $\mathbf{G}$ *to* $\mathbf{A}$ *and the epimorphisms from* $\bar{G}$ *to* A*.*

PROOF. If $\varphi\colon \mathbf{G} \to \mathbf{A}$ is an epimorphism of deficient group piles, then $\bar{\varphi}\colon \bar{\mathbf{G}} \to \bar{\mathbf{A}} = \mathbf{A}$ is an epimorphism of bare deficient group piles. Conversely, given an epimorphism $\bar{\varphi}\colon \bar{G} \to A$, the composition $\bar{\varphi} \circ \pi$, where $\pi\colon \mathbf{G} \to \bar{\mathbf{G}}$ is the quotient map, is an epimorphism from $\mathbf{G}$ to $\mathbf{A}$. These two operations are inverse to each other. □

DEFINITION 3.1.17. Let $\mathbf{G}$ be a group pile. We say that $\mathbf{G}$ is **e-generated** if $e < \omega$ and $\operatorname{rank}(\bar{\mathbf{G}}) \leq e$, or if $e = \omega$. We say that $\mathbf{G}$ is **e-bounded** if $e < \omega$, $\mathbf{G}$ is self-generated, and $\operatorname{rank}(G_0) \leq e$ for all $G_0 \in \mathcal{G}_0$, or if $e = \omega$.

REMARK 3.1.18. Note that a deficient group pile is self-generated if and only if it is 0-generated. Every e-bounded group pile is e-generated.

LEMMA 3.1.19. *Let* $\varphi\colon \mathbf{G} \to \mathbf{H}$ *be an epimorphism of group piles. If* $\mathbf{G}$ *is* e*-generated, then* $\mathbf{H}$ *is* e*-generated. If* $\mathbf{G}$ *is* e*-bounded, then* $\mathbf{H}$ *is* e*-bounded.*

PROOF. If $e = \omega$, there is nothing to prove, so assume that $e < \omega$. The induced map $\bar{\varphi}\colon \bar{\mathbf{G}} \to \bar{\mathbf{H}}$ is an epimorphism by Lemma 3.1.15, so $\operatorname{rank}(\bar{H}) \leq \operatorname{rank}(\bar{G}) \leq e$. If $\mathbf{G}$ is self-generated, then also $\mathbf{H}$ is self-generated. Since $\varphi(\mathcal{G}_0) = \mathcal{H}_0$, if $H_0 \in \mathcal{H}_0$, there exists $G_0 \in \mathcal{G}_0$ with $\varphi(G_0) = H_0$ and thus $\operatorname{rank}(H_0) \leq \operatorname{rank}(G_0) \leq e$. □

LEMMA 3.1.20. *A deficient group pile* $\mathbf{G}$ *is* e*-generated if and only if every finite quotient of* $\mathbf{G}$ *is* e*-generated.*

PROOF. If $e = \omega$, there is nothing to prove, so assume that $e < \omega$. If $\mathbf{G}$ is e-generated, then every finite quotient of $\mathbf{G}$ is e-generated by Lemma 3.1.19. Conversely, suppose that $\mathbf{G}$ is not e-generated. Then there is an epimorphism $\bar{G} \to A$ onto a finite group A with $\operatorname{rank}(A) > e$ (see for example [RZ00, 2.5.3]), so A is a finite quotient of $\mathbf{G}$ (Lemma 3.1.16) which is not e-generated. □

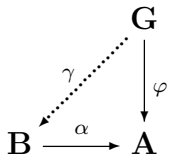
3.2. Embedding Problems for Group Piles

We introduce embedding problems and prove that a locally solvable finite embedding problem can be dominated by a rigid finite embedding problem.

DEFINITION 3.2.1. An **embedding problem** for $\mathbf{G}$ is a pair

$$EP = (\varphi\colon \mathbf{G} \to \mathbf{A},\ \alpha\colon \mathbf{B} \to \mathbf{A})$$

of epimorphisms of group piles. It is called **finite**, **self-generated**, e**-generated**, e**-bounded**, **deficient**, or **bare**, if $\mathbf{B}$ has this property. It is called **rigid** if α is rigid. A **solution** of the embedding problem (φ, α) is an epimorphism $\gamma\colon \mathbf{G} \to \mathbf{B}$ such that $\alpha \circ \gamma = \varphi$. We picture this as follows.



The embedding problem EP is **locally solvable** if, writing $\mathbf{G} = (G, \mathcal{G}_0, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S}$ and $\mathbf{B} = (B, \mathcal{B}_0, \mathcal{B}_\mathfrak{p})_{\mathfrak{p}\in S}$, the following holds for every $\mathfrak{p} \in \{0\} \cup S$:

(∗) For every $\Gamma \in \mathcal{G}_\mathfrak{p}$ there is a $\Delta \in \mathcal{B}_\mathfrak{p}$, and for every $\Delta \in \mathcal{B}_\mathfrak{p}$ there is a $\Gamma \in \mathcal{G}_\mathfrak{p}$, such that there exists an epimorphism $\gamma_\Gamma\colon \Gamma \to \Delta$ with $\alpha \circ \gamma_\Gamma = \varphi|_\Gamma$.

LEMMA 3.2.2. *If there exists $G_0 \in \mathcal{G}_0$ and $B_0 \in \mathcal{B}_0$ and an epimorphism $\gamma_0\colon G_0 \to B_0$ with $\alpha \circ \gamma_0 = \varphi|_{G_0}$, then (∗) holds for $\mathfrak{p} = 0$.*

PROOF. If $g \in G$ and $\Gamma = (G_0)^g \in \mathcal{G}_0$, choose $b \in B$ with $\alpha(b) = \varphi(g)$, and let $\Delta = (B_0)^b$. If $b \in B$ and $\Delta = (B_0)^b \in \mathcal{B}_0$, choose $g \in G$ with $\varphi(g) = \alpha(b)$, and let $\Gamma = (G_0)^g$. Define $\gamma_\Gamma\colon \Gamma \to \Delta$ by $\gamma_\Gamma(x) = \gamma_0(x^{g^{-1}})^b$. Then $\alpha(\gamma_\Gamma(x)) = \varphi(x^{g^{-1}})^{\varphi(g)} = \varphi(x)$ for all $x \in \Gamma$. □

LEMMA 3.2.3. *Every rigid deficient embedding problem is locally solvable.*

PROOF. Suppose EP is rigid and deficient. Since $\mathbf{B}$ is deficient, also $\mathbf{A}$ is deficient, so if $G_0 \in \mathcal{G}_0$, then $\varphi(G_0) = 1$. Thus, (∗) is satisfied for $\mathfrak{p} = 0$. Let $\mathfrak{p} \in S$. If $\Gamma \in \mathcal{G}_\mathfrak{p}$, choose $\Delta \in \mathcal{B}_\mathfrak{p}$ with $\alpha(\Delta) = \varphi(\Gamma)$. If $\Delta \in \mathcal{B}_\mathfrak{p}$, choose $\Gamma \in \mathcal{G}_\mathfrak{p}$ with $\varphi(\Gamma) = \alpha(\Delta)$. Since α is rigid, $\gamma_\Gamma = (\alpha|_\Delta)^{-1} \circ \varphi|_\Gamma$ maps Γ onto Δ and satisfies $\alpha \circ \gamma_\Gamma = \varphi|_\Gamma$. □

DEFINITION 3.2.4. Let $\varphi\colon \mathbf{G} \to \mathbf{A}$ and $\alpha\colon \mathbf{B} \to \mathbf{A}$ be homomorphisms of deficient group piles. Define the (symmetric) **deficient fibre product** as the deficient group pile

$$\mathbf{H} = (H, \mathcal{H}_\mathfrak{p})_{\mathfrak{p}\in S} = \mathbf{B} \times_\mathbf{A} \mathbf{G}$$

with projections $\beta\colon \mathbf{H} \to \mathbf{G}$, $\pi\colon \mathbf{H} \to \mathbf{B}$ as in the diagram

$$\begin{array}{ccc} \mathbf{B} \times_{\mathbf{A}} \mathbf{G} & \xrightarrow{\beta} & \mathbf{G} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \varphi} \\ \mathbf{B} & \xrightarrow{\alpha} & \mathbf{A} \end{array}$$

as follows:

$$H = B \times_A G$$

is the fibre product of profinite groups, $\beta\colon H \to G$ and $\pi\colon H \to B$ are the projections, and, for $\mathfrak{p} \in S$,

$$\mathcal{H}_{\mathfrak{p}} = \{\Gamma \in \mathrm{Subgr}(H)\colon \beta(\Gamma) \in \mathcal{G}_{\mathfrak{p}},\ \pi(\Gamma) \in \mathcal{B}_{\mathfrak{p}}\}\,.$$

Define the (asymmetric) **rigid product** as the deficient group pile

$$\mathbf{H}^{\mathrm{rig}} = (H, \mathcal{H}_{\mathfrak{p}}^{\mathrm{rig}})_{\mathfrak{p}\in S} = \mathbf{B} \times_{\mathbf{A}}^{\mathrm{rig}} \mathbf{G}$$

by

$$\mathcal{H}_{\mathfrak{p}}^{\mathrm{rig}} = \{\Gamma \in \mathcal{H}_{\mathfrak{p}}\colon \beta|_{\Gamma} \text{ is injective}\}\,.$$

LEMMA 3.2.5. *Let $EP = (\varphi\colon \mathbf{G} \to \mathbf{A},\ \alpha\colon \mathbf{B} \to \mathbf{A})$ be an embedding problem of deficient group piles.*

(1) *The deficient fibre product $\mathbf{B} \times_{\mathbf{A}} \mathbf{G}$ is a deficient group pile and the projections β and π are homomorphisms of group piles. If EP is locally solvable, then β and π are epimorphisms.*
(2) *If $\mathbf{B}$ and $\mathbf{G}$ are finite, then the rigid product $\mathbf{B} \times_{\mathbf{A}}^{\mathrm{rig}} \mathbf{G}$ is a deficient group pile. If EP is locally solvable, then π is an epimorphism and β is a rigid epimorphism.*

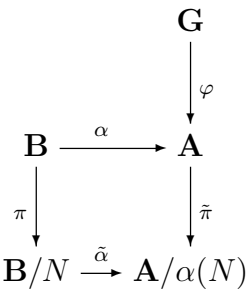
PROOF. Since $\mathcal{G}_{\mathfrak{p}}$ is G-invariant and $\mathcal{B}_{\mathfrak{p}}$ is B-invariant, $\mathcal{H}_{\mathfrak{p}}$ and $\mathcal{H}_{\mathfrak{p}}^{\mathrm{rig}}$ are H-invariant. The epimorphism $\beta\colon H \to G$ induces a continuous surjection $\mathrm{Subgr}(H) \to \mathrm{Subgr}(G)$ by Lemma 3.1.2. Hence, $\{\Gamma \le H\colon \beta(\Gamma) \in \mathcal{G}_{\mathfrak{p}}\}$, as the inverse image of the closed set $\mathcal{G}_{\mathfrak{p}}$, is closed. The same is true for π, and therefore $\mathcal{H}_{\mathfrak{p}}$ is closed. If B and G are finite, also H is finite, so in that case $\mathcal{H}_{\mathfrak{p}}^{\mathrm{rig}}$ is closed. By the definition of $\mathcal{H}_{\mathfrak{p}}$, β and π are homomorphisms of group piles.

Now suppose that EP is locally solvable. Given $G_1 \in \mathcal{G}_{\mathfrak{p}}$, there is $B_1 \in \mathcal{B}_{\mathfrak{p}}$ and an epimorphism $\gamma\colon G_1 \to B_1$ with $\alpha \circ \gamma = \varphi|_{G_1}$. It defines a homomorphism $\hat{\gamma}\colon G_1 \to H$ with $\beta \circ \hat{\gamma} = \mathrm{id}_{G_1}$ and $\pi \circ \hat{\gamma} = \gamma$. Let $H_1 = \hat{\gamma}(G_1)$. Then $\beta(H_1) = G_1 \in \mathcal{G}_{\mathfrak{p}}$ and $\pi(H_1) = \gamma(G_1) = B_1 \in \mathcal{B}_{\mathfrak{p}}$, so $H_1 \in \mathcal{H}_{\mathfrak{p}}$. Furthermore, since $\beta \circ \hat{\gamma} = \mathrm{id}_{G_1}$, $\beta|_{H_1}$ is injective. Consequently, $H_1 \in \mathcal{H}_{\mathfrak{p}}^{\mathrm{rig}}$. Similarly, given $B_1 \in \mathcal{B}_{\mathfrak{p}}$, there is $H_1 \in \mathcal{H}_{\mathfrak{p}}^{\mathrm{rig}}$ with $\pi(H_1) = B_1$. Therefore, β and π are epimorphisms of group piles. In the case of the rigid product, β is furthermore a rigid epimorphism by the definition of $\mathcal{H}_{\mathfrak{p}}^{\mathrm{rig}}$. □

REMARK 3.2.6. Note that the deficient fibre product is a fibre product in the category of deficient group piles (with homomorphisms). The

rigid product can be seen as a canonical version of [HJP09b, Lemma-Construction 4.2].

LEMMA 3.2.7. *Let* (φ: $\mathbf{G} \to \mathbf{A}$, α: $\mathbf{B} \to \mathbf{A}$) *be a locally solvable embedding problem. Then for every normal subgroup* $N \triangleleft B$*, the induced embedding problem* ($\mathbf{G} \to \mathbf{A}/\alpha(N), \mathbf{B}/N \to \mathbf{A}/\alpha(N)$) *is also locally solvable.*



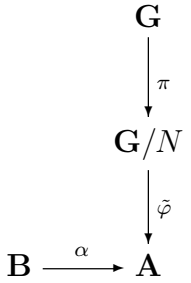
PROOF. Let $\tilde{\mathbf{B}} = (\tilde{B}, \tilde{\mathcal{B}}_0, \tilde{\mathcal{B}}_\mathfrak{p})_{\mathfrak{p}\in S} = \mathbf{B}/N$ and $\tilde{\mathbf{A}} = (\tilde{A}, \tilde{\mathcal{A}}_0, \tilde{\mathcal{A}}_\mathfrak{p})_{\mathfrak{p}\in S} = \mathbf{A}/\alpha(N)$, and let π: $\mathbf{B} \to \tilde{\mathbf{B}}$, $\tilde{\pi}$: $\mathbf{A} \to \tilde{\mathbf{A}}$ be the quotient maps and $\tilde{\alpha}$: $\tilde{\mathbf{B}} \to \tilde{\mathbf{A}}$ the induced epimorphism. Then $\tilde{\pi} \circ \alpha = \tilde{\alpha} \circ \pi$. We have to prove that the embedding problem $(\tilde{\pi} \circ \varphi, \tilde{\alpha})$ is locally solvable.

Let $\mathfrak{p} \in \{0\} \cup S$ and let $\Gamma \in \mathcal{G}_\mathfrak{p}$ be given. Then there is a $\Delta \in \mathcal{B}_\mathfrak{p}$ and an epimorphism γ_Γ: $\Gamma \to \Delta$ with $\alpha \circ \gamma_\Gamma = \varphi|_\Gamma$. Let $\Lambda = \pi(\Delta) \in \tilde{\mathcal{B}}_\mathfrak{p}$. Then $\pi \circ \gamma_\Gamma$: $\Gamma \to \Lambda$ is an epimorphism with $\tilde{\alpha} \circ (\pi \circ \gamma_\Gamma) = \tilde{\pi} \circ \alpha \circ \gamma_\Gamma = (\tilde{\pi} \circ \varphi)|_\Gamma$.

Conversely, let $\Lambda \in \tilde{\mathcal{B}}_\mathfrak{p}$ be given. Choose $\Delta \in \mathcal{B}_\mathfrak{p}$ with $\pi(\Delta) = \Lambda$. Then there is a $\Gamma \in \mathcal{G}_\mathfrak{p}$ and an epimorphism γ_Γ: $\Gamma \to \Delta$ with $\alpha \circ \gamma_\Gamma = \varphi|_\Gamma$. Hence, $\pi \circ \gamma_\Gamma$: $\Gamma \to \Lambda$ is an epimorphism with $\tilde{\alpha} \circ (\pi \circ \gamma_\Gamma) = \tilde{\pi} \circ \alpha \circ \gamma_\Gamma = (\tilde{\pi} \circ \varphi)|_\Gamma$. □

The following lemma is a special case of [HJP09b, Lemma 4.1].

LEMMA 3.2.8. *Let* (φ: $\mathbf{G} \to \mathbf{A}$, α: $\mathbf{B} \to \mathbf{A}$) *be a locally solvable finite embedding problem. Then there exists an open normal subgroup* $N \triangleleft G$ *with* $N \leq \mathrm{Ker}(\varphi)$*, such that the induced embedding problem* ($\mathbf{G}/N \to \mathbf{A}, \mathbf{B} \to \mathbf{A}$) *is locally solvable.*



PROOF. Since (φ, α) is locally solvable, we can find for each $\mathfrak{p} \in \{0\} \cup S$ an $I_\mathfrak{p}$, a family $\{(B_i, G_i) \in \mathcal{B}_\mathfrak{p} \times \mathcal{G}_\mathfrak{p} \colon i \in I_\mathfrak{p}\}$ with $\mathcal{B}_\mathfrak{p} = \{B_i \colon i \in I_\mathfrak{p}\}$ and $\mathcal{G}_\mathfrak{p} = \{G_i \colon i \in I_\mathfrak{p}\}$, and a family γ_i: $G_i \to B_i$ of epimorphisms with

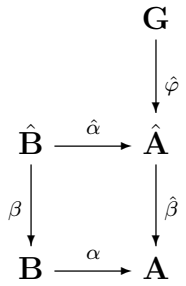
$\alpha\circ\gamma_i=\varphi|_{G_i}$ $(i\in I_{\mathfrak{p}})$. For every $i\in\bigcup_{\mathfrak{p}\in\{0\}\cup S} I_{\mathfrak{p}}$, choose an open normal subgroup $N_i\lhd G$ with $N_i\le\mathrm{Ker}(\varphi)$ and $N_i\cap G_i\le\mathrm{Ker}(\gamma_i)$. Extend γ_i to an epimorphism $\gamma_i\colon G_iN_i\to B_i$ by setting $\gamma_i(N_i)=1$, so now $\alpha\circ\gamma_i=\varphi|_{G_iN_i}$. The set $\mathcal{G}_i=\{\Delta\in\mathcal{G}_{\mathfrak{p}}\colon \Delta N_i=G_iN_i\}$ is an open-closed neighbourhood of G_i in $\mathcal{G}_{\mathfrak{p}}$. In particular, $\bigcup_{i\in I_{\mathfrak{p}}}\mathcal{G}_i=\mathcal{G}_{\mathfrak{p}}$. Since $\mathcal{G}_{\mathfrak{p}}$ is compact, there is a finite subset $J_{\mathfrak{p}}\subseteq I_{\mathfrak{p}}$ such that $\mathcal{G}_{\mathfrak{p}}=\bigcup_{i\in J_{\mathfrak{p}}}\mathcal{G}_i$.

Enlarge $J_{\mathfrak{p}}$, if necessary, to assume that $\mathcal{B}_{\mathfrak{p}}=\{B_i\colon i\in J_{\mathfrak{p}}\}$ for all $\mathfrak{p}\in\{0\}\cup S$. Let $J=\bigcup_{\mathfrak{p}\in\{0\}\cup S}J_{\mathfrak{p}}$. Then $N:=\bigcap_{i\in J}N_i$ is an open normal subgroup of G with $N\le\mathrm{Ker}(\varphi)$. Let $\mathbf{H}=\mathbf{G}/N$, and let $\pi\colon\mathbf{G}\to\mathbf{H}$ and $\tilde{\varphi}\colon\mathbf{H}\to\mathbf{A}$ be the induced epimorphisms. We claim that the embedding problem $(\tilde{\varphi},\alpha)$ is locally solvable.

Let $\mathfrak{p}\in\{0\}\cup S$ and let $H_1\in\mathcal{H}_{\mathfrak{p}}$. Then there is a $G_1\in\mathcal{G}_{\mathfrak{p}}$ with $\pi(G_1)=H_1$, and there is an $i\in J_{\mathfrak{p}}$ with $G_1\in\mathcal{G}_i$. Note that $\mathrm{Ker}(\pi)=N\le N_i\le\mathrm{Ker}(\gamma_i)$. Thus $G_1N_i=G_iN_i$ implies that $\gamma_i(G_1)=\gamma_i(G_i)=B_i$. Let $\gamma_1=\gamma_i|_{G_1}$. The epimorphism $\gamma_1\colon G_1\to B_i$ induces an epimorphism $\tilde{\gamma}_1\colon H_1\to B_i$ with $\alpha\circ\tilde{\gamma}_1=\tilde{\varphi}|_{H_1}$.

Let $B_1\in\mathcal{B}_{\mathfrak{p}}$. Choose $i\in J_{\mathfrak{p}}$ with $B_i=B_1$ and let $H_i=\pi(G_i)\in\mathcal{H}_{\mathfrak{p}}$. Then $\gamma_i\colon G_i\to B_1$ induces an epimorphism $\tilde{\gamma}_i\colon H_i\to B_1$ with $\alpha\circ\tilde{\gamma}_i=\tilde{\varphi}|_{H_i}$. □

Proposition 3.2.9. *Let $(\varphi\colon\mathbf{G}\to\mathbf{A},\ \alpha\colon\mathbf{B}\to\mathbf{A})$ be a locally solvable e-bounded finite embedding problem where $\mathbf{G}$ is e-bounded. Then it can be* **dominated** *by an e-bounded rigid finite embedding problem, i.e. there exist epimorphisms $\hat{\alpha}\colon\hat{\mathbf{B}}\to\hat{\mathbf{A}}$, $\hat{\varphi}\colon\mathbf{G}\to\hat{\mathbf{A}}$, $\hat{\beta}\colon\hat{\mathbf{A}}\to\mathbf{A}$, $\beta\colon\hat{\mathbf{B}}\to\mathbf{B}$ such that $\varphi=\hat{\beta}\circ\hat{\varphi}$ and $\hat{\beta}\circ\hat{\alpha}=\alpha\circ\beta$, and $(\hat{\varphi},\hat{\alpha})$ is an e-bounded rigid finite embedding problem.*



Proof. By Lemma 3.2.8, there are a finite group pile $\hat{\mathbf{A}}$ and epimorphisms $\hat{\varphi}\colon\mathbf{G}\to\hat{\mathbf{A}}$, $\hat{\beta}\colon\hat{\mathbf{A}}\to\mathbf{A}$ with $\varphi=\hat{\beta}\circ\hat{\varphi}$ such that $(\hat{\beta},\alpha)$ is a locally solvable embedding problem. Since $\mathbf{G}$ is e-bounded, also $\hat{\mathbf{A}}$ is e-bounded (Lemma 3.1.19).

Let $\tilde{\mathbf{B}}=\mathbf{B}^{\mathrm{def}}\times^{\mathrm{rig}}_{\mathbf{A}^{\mathrm{def}}}\hat{\mathbf{A}}^{\mathrm{def}}$ be the rigid product and let $\tilde{\alpha}\colon\tilde{\mathbf{B}}\to\hat{\mathbf{A}}^{\mathrm{def}}$ and $\tilde{\beta}\colon\tilde{\mathbf{B}}\to\mathbf{B}^{\mathrm{def}}$ be the projections. By Lemma 3.2.5(2), $\tilde{\alpha}$ is a rigid epimorphism and $\tilde{\beta}$ is an epimorphism. Choose $\hat{A}_0\in\hat{\mathcal{A}}_0$ and $B_0\in\mathcal{B}_0$ and an epimorphism $\gamma_0\colon\hat{A}_0\to B_0$ with $\alpha\circ\gamma_0=\hat{\beta}|_{\hat{A}_0}$. Then γ_0 defines

a homomorphism $\hat{\gamma}_0\colon \hat{A}_0 \to \tilde{B}$ with $\tilde{\alpha} \circ \hat{\gamma}_0 = \mathrm{id}_{\hat{A}_0}$ and $\tilde{\beta} \circ \hat{\gamma}_0 = \gamma_0$. Let $\tilde{B}_0 = \hat{\gamma}_0(\hat{A}_0)$ and note that $\tilde{\alpha}(\tilde{B}_0) = \hat{A}_0$ and $\tilde{\beta}(\tilde{B}_0) = B_0$.

Case $e = \omega$. If $e = \omega$, let $\hat{\mathbf{B}} = (\tilde{B}, (\tilde{B}_0)^{\tilde{B}}, \tilde{\mathcal{B}}_{\mathfrak{p}})_{\mathfrak{p}\in S}$, and let $\hat{\alpha}\colon \hat{\mathbf{B}} \to \hat{\mathbf{A}}$ and $\beta\colon \hat{\mathbf{B}} \to \mathbf{B}$ be the epimorphisms induced by $\tilde{\alpha}$ resp. $\tilde{\beta}$. Then $(\hat{\varphi}, \hat{\alpha})$ is a rigid finite embedding problem which dominates (φ, α), so we are done.

Case $e < \omega$. In this case, $\mathrm{rank}(\tilde{B}_0) \leq \mathrm{rank}(\hat{A}_0) \leq e$, and since $\hat{\mathbf{A}}$ and $\mathbf{B}$ are self-generated, $\hat{A} = \langle\, \hat{A}_0, \hat{A}' \,\rangle$ and $B = \langle B_0, B'\rangle$. Let $\hat{B} = \langle\, \tilde{B}_0, \tilde{B}' \,\rangle \leq \tilde{B}$ and $\hat{\mathcal{B}}_0 = (\tilde{B}_0)^{\hat{B}}$. Then $\hat{\mathbf{B}} = (\hat{B}, \hat{\mathcal{B}}_0, \tilde{\mathcal{B}}_{\mathfrak{p}})_{\mathfrak{p}\in S}$ is a self-generated group pile by Lemma 3.1.11, and $\tilde{\alpha}(\hat{B}) = \langle\, \hat{A}_0, \hat{A}' \,\rangle = \hat{A}$ and $\tilde{\beta}(\hat{B}) = \langle B_0, B'\rangle = B$ by Lemma 3.1.13. Since $\hat{\mathcal{A}}_0 = (\hat{A}_0)^{\hat{A}}$ and $\mathcal{B}_0 = (B_0)^B$, $\tilde{\alpha}(\hat{\mathcal{B}}_0) = \hat{\mathcal{A}}_0$ and $\tilde{\beta}(\hat{\mathcal{B}}_0) = \mathcal{B}_0$, so $\tilde{\alpha}|_{\hat{B}}$ and $\tilde{\beta}|_{\hat{B}}$ are epimorphisms of group piles. Therefore, with $\hat{\alpha} = \tilde{\alpha}|_{\hat{B}}$ and $\beta = \tilde{\beta}|_{\hat{B}}$, $(\hat{\varphi}, \hat{\alpha})$ is a rigid e-bounded finite embedding problem which dominates (φ, α). □

3.3. Free Product Group Piles

In this section we introduce and study the free product of a profinite group and a group pile.

Lemma 3.3.1. *Let $\pi\colon G \to H$ be an epimorphism of profinite groups. Let $e \in \mathbb{Z}_{\geq 0}$, let $N \lhd G$ be a closed normal subgroup with* $\mathrm{rank}(G/N) \leq e$, *and let $h_1, \ldots, h_e \in H$ such that $H = \langle h_1, \ldots, h_e, \pi(N)\rangle$. Then there exist $g_1, \ldots, g_e \in G$ such that $G = \langle g_1, \ldots, g_e, N\rangle$ and $\pi(g_i) = h_i$, $i = 1, \ldots, e$.*

Proof. Let $\bar{G} = G/N$, $\bar{H} = H/\pi(N)$, and let $\bar{\pi}\colon \bar{G} \to \bar{H}$ be the induced epimorphism. Then $\bar{H} = \langle \bar{h}_1, \ldots, \bar{h}_e\rangle$, so Gaschütz' lemma (Proposition 1.3.1) implies that there are $g_1, \ldots, g_e \in G$ such that $\bar{G} = \langle \bar{g}_1, \ldots, \bar{g}_e\rangle$ and $\bar{\pi}(\bar{g}_i) = \bar{h}_i$, $i = 1, \ldots, e$. So, $G = \langle g_1, \ldots, g_e, N\rangle$ and there are $n_1, \ldots, n_e \in N$ such that $\pi(g_i) = h_i\pi(n_i)$, $i = 1, \ldots, e$. Thus, setting $g_i' = g_i n_i^{-1}$, $G = \langle g_1', \ldots, g_e', N\rangle$ and $\pi(g_i') = h_i$, $i = 1, \ldots, e$. □

Lemma 3.3.2. *Let $\mathbf{A}$ be an e-bounded self-generated group pile and let $\mathbf{G}$ be an e-generated deficient group pile. For every epimorphism $\pi\colon \mathbf{G} \to \mathbf{A}^{\mathrm{def}}$ there exists an e-bounded self-generated group pile $\mathbf{B}$ with $\mathbf{B}^{\mathrm{def}} = \mathbf{G}$ such that $\pi\colon \mathbf{B} \to \mathbf{A}$ is an epimorphism.*

Proof. If $e = \omega$, let $A_0 \in \mathcal{A}_0$ and $\mathbf{B} = (G, (\pi^{-1}(A_0))^G, \mathcal{G}_{\mathfrak{p}})_{\mathfrak{p}\in S}$. Since $A = \langle A_0, A'\rangle$, $\mathbf{B}$ is self-generated by Lemma 3.1.13, and $\pi\colon \mathbf{B} \to \mathbf{A}$ is an epimorphism.

If $e < \omega$, let $A_0 \in \mathcal{A}_0$ and choose $a_1, \ldots, a_e \in A$ with $A_0 = \langle a_1, \ldots, a_e\rangle$. By Lemma 3.1.13, $A = \langle a_1, \ldots, a_e, A'\rangle$ and $A' = \pi(G')$, so Lemma 3.3.1 gives $g_1, \ldots, g_e \in G$ with $G = \langle g_1, \ldots, g_e, G'\rangle$ and

$\pi(g_i) = a_i$. Let $G_0 = \langle g_1, \dots, g_e \rangle$ and $\mathbf{B} = (G, (G_0)^G, \mathcal{G}_\mathfrak{p})_{\mathfrak{p} \in S}$. Then $\mathbf{B}$ is e-bounded and $\pi\colon \mathbf{B} \to \mathbf{A}$ is an epimorphism. □

Definition 3.3.3. Let $\mathbf{H} = (H, \mathcal{H}_\mathfrak{p})_{\mathfrak{p} \in S}$ be a deficient group pile and let F be a profinite group. Define the **free product group pile**

$$\mathbf{G} = (G, \mathcal{G}_0, \mathcal{G}_\mathfrak{p})_{\mathfrak{p} \in S} = F * \mathbf{H}$$

of F with $\mathbf{H}$ as follows: Let

$$G := F * H$$

be the free product of profinite groups,

$$\mathcal{G}_0 := \{F^g \colon g \in G\},$$

and, for $\mathfrak{p} \in S$,

$$\mathcal{G}_\mathfrak{p} := \{\Delta^g \colon \Delta \in \mathcal{H}_\mathfrak{p},\ g \in G\}.$$

Lemma 3.3.4. *Let $\mathbf{G} = F * \mathbf{H}$ be a free product group pile. Then the following holds:*

(1) $\mathbf{G}$ *is a group pile.*
(2) $G = \langle F, H \rangle$.
(3) *If* $\mathbf{H}$ *is self-generated, then* $\mathbf{G}$ *is self-generated.*
(4) *The map $\mathcal{H}_\mathfrak{p}/H \to \mathcal{G}_\mathfrak{p}/G$ induced by the embedding $\mathcal{H}_\mathfrak{p} \to \mathcal{G}_\mathfrak{p}$ is a homeomorphism for every $\mathfrak{p} \in S$.*

Proof.

Proof of (1). Since H is a closed subgroup of G, the embedding $\mathcal{H}_\mathfrak{p} \to \mathrm{Subgr}(G)$ is continuous for every $\mathfrak{p} \in S$ by Lemma 3.1.3. Thus also the map $\mathcal{H}_\mathfrak{p} \times G \to \mathrm{Subgr}(G)$ given by $(\Delta, g) \mapsto \Delta^g$ is continuous. Therefore, since $\mathcal{H}_\mathfrak{p} \times G$ is compact, its image $\mathcal{G}_\mathfrak{p}$ is closed in $\mathrm{Subgr}(G)$. By definition, $\mathcal{G}_\mathfrak{p}$ is also G-invariant. Similarly, also $\mathcal{G}_0$ is closed and G-invariant. Thus, $\mathbf{G}$ is indeed a group pile.

Proof of (2). Since $G = F * H$, we have $G = \langle F, H \rangle$, cf. Section 1.3.

Proof of (3). If $H = \langle \mathcal{H} \rangle$, then $G = \langle F, \mathcal{H} \rangle$ by (2), so $G = \langle F, \mathcal{G} \rangle$, since $\mathcal{H} \subseteq \mathcal{G}$. Therefore, since $F \in \mathcal{G}_0$, $\mathbf{G}$ is self-generated.

Proof of (4). By definition of $\mathcal{G}_\mathfrak{p}$, the map $\mathcal{H}_\mathfrak{p}/H \to \mathcal{G}_\mathfrak{p}/G$ is surjective. It is also injective, since if $1 \neq \Gamma_1, \Gamma_2 \in \mathcal{H}_\mathfrak{p}$ and $g \in G$ with $\Gamma_1^g = \Gamma_2$, then $H^g \cap H \neq 1$, so $g \in H$ by Lemma 1.3.3.

Since the embedding $\mathcal{H}_\mathfrak{p} \to \mathcal{G}_\mathfrak{p}$ is continuous (Lemma 3.1.3), and the projections $\mathcal{H}_\mathfrak{p} \to \mathcal{H}_\mathfrak{p}/H$ and $\mathcal{G}_\mathfrak{p} \to \mathcal{G}_\mathfrak{p}/H$ are continuous and closed (Lemma 1.3.6), the induced map $\mathcal{H}_\mathfrak{p}/H \to \mathcal{G}_\mathfrak{p}/H$ is continuous. Since also the quotient map $\mathcal{G}_\mathfrak{p}/H \to \mathcal{G}_\mathfrak{p}/G$ is continuous, the composition $\mathcal{H}_\mathfrak{p}/H \to \mathcal{G}_\mathfrak{p}/G$ is a homeomorphism. □

The following lemma justifies the name 'free product group pile'.

LEMMA 3.3.5. *Let $\mathbf{G} = F * \mathbf{H}$ be a free product group pile and let $\mathbf{A} = (A, (A_0)^A, \mathcal{A}_\mathfrak{p})_{\mathfrak{p}\in S}$ be a group pile. For every epimorphism $\alpha\colon F \to A_0$ and homomorphism $\beta\colon \mathbf{H} \to \mathbf{A}^{\mathrm{def}}$, there is a unique homomorphism $\gamma\colon \mathbf{G} \to \mathbf{A}$ with $\gamma|_F = \alpha$ and $\gamma|_{\mathbf{H}} = \beta$.*

PROOF. By the universal property of the free product there is a unique homomorphism $\gamma\colon G \to A$ with $\gamma|_F = \alpha$ and $\gamma|_H = \beta$. For $\mathfrak{p} \in S$, every $\Gamma \in \mathcal{G}_\mathfrak{p}$ is G-conjugate to some $\Delta \in \mathcal{H}_\mathfrak{p}$, so $\gamma(\Gamma) = \gamma(\Delta)^a = \beta(\Delta)^a \in \mathcal{A}_\mathfrak{p}$ for some $a \in A$. Moreover, $\gamma(F^g) = A_0^{\gamma(g)} \in (A_0)^A$, so γ extends to a homomorphism of group piles. □

LEMMA 3.3.6. *Let $\mathbf{G} = F * \mathbf{H}$ be a free product group pile where $\mathbf{H}$ is self-generated and deficient. Then the composition*

$$\epsilon\colon F \hookrightarrow G \to \bar{G}$$

is an isomorphism of profinite groups.

PROOF. The fact that $G = \langle F, H\rangle$ (Lemma 3.3.4(2)) and $G' \geq H' = H$ since $\mathbf{H}$ is self-generated imply that $G = \langle F, G'\rangle$. Hence, ϵ is surjective. By Lemma 3.3.5 there is an epimorphism $\delta\colon (F * \mathbf{H})^{\mathrm{def}} \to F$ with $\delta|_F = \mathrm{id}_F$ and $\delta|_H = 1$. Since every $\Gamma \in \mathcal{G}$ is conjugate to a subgroup of H, this implies that $\delta|_{G'} = 1$, so δ factors as $\delta = \delta_0 \circ \pi$ through the quotient map $\pi\colon G \to \bar{G}$. Then $\delta_0 \circ \epsilon = \mathrm{id}_F$, so ϵ is also injective. □

LEMMA 3.3.7. *Every finite e-generated bare deficient embedding problem $(\varphi\colon \hat{F}_e \to A,\ \alpha\colon B \to A)$ for the free group $\hat{F}_e$ has a solution.*

PROOF. Let $\hat{F}_e$ be free on $X \subseteq \hat{F}_e$. Since X converges to 1 and A is finite, there exists a finite subset $X_0 = \{x_1, \ldots, x_k\} \subseteq X$ with $k \leq e$ such that $\varphi(X \setminus X_0) = 1$. It follows that $\langle\varphi(X_0)\rangle = A$. Since $\mathrm{rank}(B) \leq e$, we can assume without loss of generality that $\mathrm{rank}(B) \leq k$. By Proposition 1.3.1, there exist generators $b_1, \ldots, b_k$ of B with $\alpha(b_i) = \varphi(x_i)$ for $i = 1, \ldots, k$. Then the map $\gamma_0\colon X \to B$ given by $\gamma_0(x) = 1$ if $x \in X \setminus X_0$, and $\gamma_0(x_i) = b_i$ for $i = 1, \ldots, k$, extends to an epimorphism $\gamma\colon \hat{F}_e \to B$ with $\alpha \circ \gamma = \varphi$, as claimed. □

LEMMA 3.3.8. *Let $\mathbf{G}$ be an e-bounded and self-generated group pile, and let $(\varphi\colon \mathbf{G}^{\mathrm{def}} \to \tilde{\mathbf{A}},\ \alpha\colon \tilde{\mathbf{B}} \to \tilde{\mathbf{A}})$ be a locally solvable e-generated deficient finite embedding problem. If $G_0 \cong \hat{F}_e$ for $G_0 \in \mathcal{G}_0$, then there exist $\mathbf{A}$ and $\mathbf{B}$ with $\mathbf{A}^{\mathrm{def}} = \tilde{\mathbf{A}}$ and $\mathbf{B}^{\mathrm{def}} = \tilde{\mathbf{B}}$ such that $(\varphi\colon \mathbf{G} \to \mathbf{A},\ \alpha\colon \mathbf{B} \to \mathbf{A})$ is a finite locally solvable e-bounded self-generated embedding problem.*

PROOF. Let $G_0 \in \mathcal{G}_0$ and $A_0 = \varphi(G_0)$. Then $G = \langle G_0, G'\rangle$ implies $\tilde{A} = \langle\, A_0, \tilde{A}'\,\rangle$ (Lemma 3.1.13), so $\mathbf{A} = (\tilde{A}, (A_0)^{\tilde{A}}, \tilde{\mathcal{A}}_\mathfrak{p})_{\mathfrak{p}\in S}$ is e-bounded self-generated. By Lemma 3.3.2, there exists an e-bounded self-generated group pile $\mathbf{B} = (\tilde{B}, (B_0)^{\tilde{B}}, \tilde{\mathcal{B}}_\mathfrak{p})_{\mathfrak{p}\in S}$ such that $\alpha\colon \mathbf{B} \to \mathbf{A}$ is

an epimorphism. Without loss of generality assume that $\alpha(B_0) = A_0$. We claim that $EP = (\varphi\colon \mathbf{G} \to \mathbf{A},\ \alpha\colon \mathbf{B} \to \mathbf{A})$ is locally solvable.

Since $G_0 \cong \hat{F}_e$ and $\mathbf{B}$ is e-bounded, there exists an epimorphism $\gamma_0\colon G_0 \to B_0$ with $\alpha \circ \gamma_0 = \varphi|_{G_0}$ by Lemma 3.3.7. By Lemma 3.2.2, this implies that EP is locally solvable. □

3.4. Semi-Constant Group Piles

In this section we introduce group piles of free products over semi-constant sheaves. First we recall the notion of free products of profinite groups in the sense of [Har87] and [Mel90].

A **sheaf** of profinite groups is a triple (X, τ, T) where $\tau\colon X \to T$ is a continuous surjection of profinite spaces such that all fibres of τ are profinite groups and the map

$$\{(x, y) \in X \times X\colon \tau(x) = \tau(y)\} \to X, \quad (x, y) \mapsto x^{-1}y \tag{3.1}$$

is continuous. A **morphism** $\lambda\colon (X, \tau, T) \to G$ from a sheaf (X, τ, T) into a profinite group G is a continuous map $\lambda\colon X \to G$ that is a homomorphism of groups on each fibre of τ. A **free product** of the sheaf (X, τ, T) is a morphism $\lambda\colon (X, \tau, T) \to G$ into a profinite group G with the following universal property: For every morphism β from (X, τ, T) into a profinite group H there exists a unique homomorphism $\gamma\colon G \to H$ such that $\gamma \circ \lambda = \beta$. For any sheaf (X, τ, T), a free product $(X, \tau, T) \to G$ exists and is unique up to isomorphism, see [Mel90, (1.14)]. Note that in the special case where $T = \{t_1, t_2\}$ is a discrete space consisting of two points, if $(X, \tau, T) \to G$ is a free product, then

$$G \cong \tau^{-1}(t_1) * \tau^{-1}(t_2)$$

is a free product in the sense of Section 1.3.

LEMMA 3.4.1. *If $\lambda\colon (X, \tau, T) \to G$ is a free product, then for every $t \in T$, λ maps the profinite group $\tau^{-1}(t)$ isomorphically onto the subgroup $G_t := \lambda(\tau^{-1}(t)) \leq G$. The groups G_t satisfy the following properties.*

1. *$G = \langle G_t\colon t \in T\rangle$.*
2. *If $g \in G$ and $t, s \in T$ with $(G_t)^g \cap G_s \neq 1$, then $t = s$ and $g \in G_t$.*

PROOF. For the fact that λ is injective on each fibre of τ see [Mel90, (1.15) Lemma (2)]. For (1) see [Mel90, (1.15) Lemma (1)]. For (2) see [Mel90, (4.9) Proposition (2)]. □

DEFINITION 3.4.2. Suppose that for every $\mathfrak{p} \in S$ we are given a non-trivial profinite group $\Gamma_\mathfrak{p}$ and a (nonempty) profinite space $T_\mathfrak{p}$. Define a triple

$$(X, \tau, T) = \left(\bigcup_{\mathfrak{p} \in S}^{\cdot} \Gamma_\mathfrak{p} \times T_\mathfrak{p}, \pi, \bigcup_{\mathfrak{p} \in S}^{\cdot} T_\mathfrak{p} \right),$$

where $\pi\colon \bigcup_{\mathfrak{p}\in S}\Gamma_{\mathfrak{p}}\times T_{\mathfrak{p}}\to\bigcup_{\mathfrak{p}\in S}T_{\mathfrak{p}}$ is piecewise defined to be the projection $\Gamma_{\mathfrak{p}}\times T_{\mathfrak{p}}\to T_{\mathfrak{p}}$. Then the map (3.1) is continuous, and hence (X,τ,T) is a sheaf, which is called the **semi-constant sheaf** of $(\Gamma_{\mathfrak{p}})_{\mathfrak{p}\in S}$ over $(T_{\mathfrak{p}})_{\mathfrak{p}\in S}$.

Definition 3.4.3. Let

$$\lambda\colon \left(\bigcup_{\mathfrak{p}\in S}\Gamma_{\mathfrak{p}}\times T_{\mathfrak{p}},\pi,\bigcup_{\mathfrak{p}\in S}T_{\mathfrak{p}}\right)\to H$$

be the free product of the semi-constant sheaf of $(\Gamma_{\mathfrak{p}})_{\mathfrak{p}\in S}$ over $(T_{\mathfrak{p}})_{\mathfrak{p}\in S}$, and let $H_{\mathfrak{p},t}:=\lambda(\Gamma_{\mathfrak{p}}\times\{t\})$. Define

$$\mathcal{H}_{\mathfrak{p},0}=\{H_{\mathfrak{p},t}\colon t\in T_{\mathfrak{p}}\}\subseteq\mathrm{Subgr}(H)$$

and

$$\mathcal{H}_{\mathfrak{p}}=\left\{\Gamma^h\colon \Gamma\in\mathcal{H}_{\mathfrak{p},0},\ h\in H\right\}\subseteq\mathrm{Subgr}(H).$$

Then $\mathbf{H}=(H,\mathcal{H}_{\mathfrak{p}})_{\mathfrak{p}\in S}$ is called the **semi-constant group pile** of $(\Gamma_{\mathfrak{p}})_{\mathfrak{p}\in S}$ over $(T_{\mathfrak{p}})_{\mathfrak{p}\in S}$.

Lemma 3.4.4. *Let* $\mathbf{H}$ *be the semi-constant group pile of* $(\Gamma_{\mathfrak{p}})_{\mathfrak{p}\in S}$ *over* $(T_{\mathfrak{p}})_{\mathfrak{p}\in S}$. *Then the following holds.*

(1) $\mathbf{H}$ *is a self-generated deficient group pile. Moreover,*

$$H=\langle\mathcal{H}_{\mathfrak{p},0}\rangle_{\mathfrak{p}\in S}.$$

(2) $\mathbf{H}$ *is separated and reduced (cf. Definition 3.1.6), and* $1\notin\mathcal{H}$.
(3) *Let* $\mathfrak{p}\in S$. *The map* $T_{\mathfrak{p}}\to\mathcal{H}$ *given by* $t\mapsto H_{\mathfrak{p},t}$ *is continuous. The map* $T_{\mathfrak{p}}\to\mathcal{H}_{\mathfrak{p}}/H$ *given by* $t\mapsto(H_{\mathfrak{p},t})^H$ *is a homeomorphism. In particular,* $T_{\mathfrak{p}}$ *and* $\mathcal{H}_{\mathfrak{p},0}$ *are homeomorphic.*

Proof.

Proof of (3). Let $\theta\colon T_{\mathfrak{p}}\to\mathcal{H}$ be the map $t\mapsto H_{\mathfrak{p},t}$.

To prove that θ is continuous, it suffices to show that the map $T_{\mathfrak{p}}\to\mathrm{Subgr}(H/N)$ given by $t\mapsto H_{\mathfrak{p},t}N/N$ is continuous for each open normal subgroup N of H. Let $\rho\colon H\to H/N$ be the quotient map. Then $\alpha=\rho\circ\lambda|_{\Gamma_{\mathfrak{p}}\times T_{\mathfrak{p}}}$ is continuous. If $x\in H/N$ and $t\in T_{\mathfrak{p}}$, then $x\in\rho(H_{\mathfrak{p},t})$ if and only if $t\in\pi(\alpha^{-1}(x))$. The projection $\pi|_{\Gamma_{\mathfrak{p}}\times T_{\mathfrak{p}}}$ is open, and H/N is finite. Hence, if $U\in\mathrm{Subgr}(H/N)$, then $\{t\in T_{\mathfrak{p}}\colon\rho(H_{\mathfrak{p},t})=U\}=\pi(\alpha^{-1}(U))$ is open, as claimed.

The map $T_{\mathfrak{p}}\to\mathcal{H}_{\mathfrak{p}}/H$ is the composition of θ and the quotient map $\eta\colon\mathcal{H}\to\mathcal{H}/H$. If $t_1,t_2\in T_{\mathfrak{p}}$ with $(\eta\circ\theta)(t_1)=(\eta\circ\theta)(t_2)$, then there exists $h\in H$ such that $(H_{\mathfrak{p},t_1})^h=H_{\mathfrak{p},t_2}$. Hence, $(H_{\mathfrak{p},t_1})^h\cap H_{\mathfrak{p},t_2}\cong\Gamma_{\mathfrak{p}}\neq 1$, so $t_1=t_2$ by Lemma 3.4.1(2). Therefore, $\eta\circ\theta$ is injective. By Lemma 1.3.6, η is continuous and $\mathcal{H}_{\mathfrak{p}}/H$ is a profinite space. Consequently, $\eta\circ\theta$ is a homeomorphism.

Proof of (1). First, $\mathbf{H}$ is a group pile. Indeed, $\mathcal{H}_{\mathfrak{p}}$ is the image of the compact set $T_{\mathfrak{p}}\times H$ under the map $(t,h)\mapsto(H_{\mathfrak{p},t})^h$, which is

continuous by (3). Therefore, $\mathcal{H}_\mathfrak{p}$ is closed for each $\mathfrak{p} \in S$. Finally, $H = \langle \mathcal{H}_{\mathfrak{p},0} \rangle_{\mathfrak{p}\in S}$ by Lemma 3.4.1(1), so in particular $\mathbf{H}$ is self-generated.

PROOF OF (2). Since $\Gamma_\mathfrak{p} \neq 1$ for each $\mathfrak{p} \in S$, $1 \notin \mathcal{H}$. If $\mathfrak{p}, \mathfrak{q} \in S$ and $\Gamma \in \mathcal{H}_\mathfrak{p}$, $\Gamma_1 \in \mathcal{H}_\mathfrak{q}$ with $\Gamma \subseteq \Gamma_1$, then there exist $h, h_1 \in H$ such that $\Gamma^h \in \mathcal{H}_{\mathfrak{p},0}$ and $\Gamma_1^{h_1} \in \mathcal{H}_{\mathfrak{q},0}$. Then $(\Gamma^h)^{h^{-1}h_1} \cap \Gamma_1^{h_1} = \Gamma^{h_1} \neq 1$, hence $\mathfrak{p} = \mathfrak{q}$, $\Gamma^h = \Gamma_1^{h_1}$, and $h^{-1}h_1 \in \Gamma^h$ by Lemma 3.4.1(2). This implies that $h_1 h^{-1} \in \Gamma \subseteq \Gamma_1$, so $\Gamma = \Gamma_1^{h_1 h^{-1}} = \Gamma_1$, and hence $\mathbf{H}$ is separated and reduced. □

DEFINITION 3.4.5. Let $\mathbf{H}$ be the semi-constant group pile of $(\Gamma_\mathfrak{p})_{\mathfrak{p}\in S}$ over $(T_\mathfrak{p})_{\mathfrak{p}\in S}$ (Definition 3.4.3), and let $\mathbf{G} = \hat{F}_e * \mathbf{H}$ be the free product group pile (Definition 3.3.3). We call $\mathbf{G}$ the ***e*-free semi-constant group pile** of $(\Gamma_\mathfrak{p})_{\mathfrak{p}\in S}$ over $(T_\mathfrak{p})_{\mathfrak{p}\in S}$.

LEMMA 3.4.6. *Let $\mathbf{G} = \hat{F}_e * \mathbf{H}$ be the e-free semi-constant group pile of $(\Gamma_\mathfrak{p})_{\mathfrak{p}\in S}$ over $(T_\mathfrak{p})_{\mathfrak{p}\in S}$. Then the following holds.*

(1) *$\mathbf{G}$ is an e-bounded and self-generated group pile.*
(2) *$\mathbf{G}$ is separated and reduced.*

PROOF.

PROOF OF (1). By Lemma 3.4.4(1) and Lemma 3.3.4(1), $\mathbf{G}$ is a group pile. By Lemma 3.4.4(1), $\mathbf{H}$ is self-generated, hence $\mathbf{G}$ is self-generated by Lemma 3.3.4(3). If $G_0 \in \mathcal{G}_0$, then $G_0 \cong \hat{F}_e$ implies that $\operatorname{rank}(G_0) = \operatorname{rank}(\hat{F}_e) = e$, and therefore $\mathbf{G}$ is e-bounded.

PROOF OF (2). By Lemma 3.4.4(2), $1 \notin \mathcal{H}$, and thus $1 \notin \mathcal{G}$. If $\mathfrak{p}, \mathfrak{q} \in S$, and $\Gamma \in \mathcal{G}_\mathfrak{p}$ and $\Gamma_1 \in \mathcal{G}_\mathfrak{q}$ with $\Gamma \subseteq \Gamma_1$, then there exist $g, g_1 \in G$ such that $\Gamma^g \in \mathcal{H}_\mathfrak{p}$ and $\Gamma_1^{g_1} \in \mathcal{H}_\mathfrak{q}$. In particular, $H^{g^{-1}} \cap H^{g_1^{-1}} \supseteq \Gamma \neq 1$, so Lemma 1.3.3 implies that $g^{-1}g_1 \in H$. Thus, $\Gamma^{g_1} \in \mathcal{H}_\mathfrak{p}$. Hence, $\Gamma^{g_1} \subseteq \Gamma_1^{g_1}$ implies that $\Gamma^{g_1} = \Gamma_1^{g_1}$, since $\mathbf{H}$ is reduced by Lemma 3.4.4(2). Therefore, $\Gamma = \Gamma_1$, hence $\mathbf{G}$ is reduced.

Moreover, $\Gamma^{g_1} \in \mathcal{H}_\mathfrak{p} \cap \mathcal{H}_\mathfrak{q}$. If follows that $\mathfrak{p} = \mathfrak{q}$ since $\mathbf{H}$ is separated by Lemma 3.4.4(2). Let $\Gamma \in \mathcal{G}_0$. If $e = 0$, then $\Gamma = 1$, hence $\Gamma \notin \mathcal{G}$. If $e > 0$ and $\Gamma \in \mathcal{G}$, then there exists $g \in G$ such that $\Gamma^g \in \mathcal{H}$, so $\Gamma^g \cap H = \Gamma^g \neq 1$, contradicting Lemma 3.4.1(2). Therefore, $\mathbf{G}$ is separated. □

Besides the Gaschütz lemma, we need the following variant of it:

PROPOSITION 3.4.7 (Efrat). *Let $\alpha\colon B \to A$ be an epimorphism of finite groups, $A_1, \dots, A_n$ subgroups of A, and $B_1, \dots, B_n$ subgroups of B. Suppose that $A = \langle A_1, \dots, A_n \rangle$, $B = \langle B_1, \dots, B_n \rangle$, and for all i, $\alpha(B_i)$ is conjugate to A_i. Then there exist $b_1, \dots, b_n \in B$ such that $B = \langle B_1^{b_1}, \dots, B_n^{b_n} \rangle$ and $\alpha(B_i^{b_i}) = A_i$ for all i.*

PROOF. See [Efr97]. □

The following result is essentially proven in [HJP09b, Proposition 5.3(h)]. One reason why we cannot just quote [HJP09b] is that we also need the case $e = \omega$.

PROPOSITION 3.4.8. *Let $\mathbf{G} = \hat{F}_e * \mathbf{H}$ be the e-free semi-constant group pile of $(\Gamma_\mathfrak{p})_{\mathfrak{p}\in S}$ over $(T_\mathfrak{p})_{\mathfrak{p}\in S}$, where each $T_\mathfrak{p}$ is perfect, and let $(\varphi\colon \mathbf{G} \to \mathbf{A},\ \alpha\colon \mathbf{B} \to \mathbf{A})$ be a finite rigid e-bounded self-generated embedding problem for $\mathbf{G}$. Then (φ, α) has a solution $\gamma\colon \mathbf{G} \to \mathbf{B}$.*

PROOF. By definition, $\mathbf{H} = (H, \mathcal{H}_\mathfrak{p})_{\mathfrak{p}\in S}$, where

$$\lambda\colon \left(\bigcup_{\mathfrak{p}\in S} \Gamma_\mathfrak{p} \times T_\mathfrak{p}, \pi, \bigcup_{\mathfrak{p}\in S} T_\mathfrak{p}\right) \to H$$

is a free product, $H_{\mathfrak{p},t} = \lambda(\Gamma_\mathfrak{p} \times \{t\})$, $\mathcal{H}_{\mathfrak{p},0} = \{H_{\mathfrak{p},t}\colon t \in T_\mathfrak{p}\}$, and $\mathcal{H}_\mathfrak{p} = \{\Delta^h\colon \Delta \in \mathcal{H}_{\mathfrak{p},0},\ h \in H\}$. Let $\mathcal{A}_{\mathfrak{p},0} = \varphi(\mathcal{H}_{\mathfrak{p},0})$.

Since $\mathcal{H}_{\mathfrak{p},0}$ meets all H-conjugacy classes of $\mathcal{H}_\mathfrak{p}$, and $\mathcal{H}_\mathfrak{p}$ meets all G-conjugacy classes of $\mathcal{G}_\mathfrak{p}$, $\mathcal{A}_{\mathfrak{p},0} = \varphi(\mathcal{H}_{\mathfrak{p},0})$ meets all A-conjugacy classes of $\mathcal{A}_\mathfrak{p}$. Thus, every subgroup in $\alpha(\mathcal{B}_\mathfrak{p})$ is conjugate to a subgroup in $\mathcal{A}_{\mathfrak{p},0}$. Since $\alpha(\mathcal{B}_\mathfrak{p}) = \mathcal{A}_\mathfrak{p}$, we can write $\mathcal{B}_\mathfrak{p} = \{B_{\mathfrak{p},i}\colon i \in I_\mathfrak{p}\}$ for some finite index set $I_\mathfrak{p}$, and $\mathcal{A}_{\mathfrak{p},0} = \{A_{\mathfrak{p},i}\colon i \in I_\mathfrak{p}\}$, such that $\alpha(B_{\mathfrak{p},i})$ is conjugate to $A_{\mathfrak{p},i}$ for every $\mathfrak{p} \in S$ and $i \in I_\mathfrak{p}$.

Let $B_0 \in \mathcal{B}_0$, $G_0 = \hat{F}_e \in \mathcal{G}_0$ and $A_0 = \varphi(G_0) \in \mathcal{A}_0$. Since $\mathbf{B}$ is self-generated, $B = \langle B_0, B_{\mathfrak{p},i}\rangle_{\mathfrak{p}\in S, i\in I_\mathfrak{p}}$. By Lemma 3.4.4(1) and Lemma 3.3.4(2), $G = \langle G_0, \mathcal{H}_{\mathfrak{p},0}\rangle_{\mathfrak{p}\in S}$. Therefore $A = \langle A_0, A_{\mathfrak{p},i}\rangle_{\mathfrak{p}\in S, i\in I_\mathfrak{p}}$, so by Proposition 3.4.7 there exist $b \in B$ and $b_{\mathfrak{p},i} \in B$ for every $\mathfrak{p} \in S$ and $i \in I_\mathfrak{p}$, such that with $\mathcal{B}_{\mathfrak{p},0} = \{(B_{\mathfrak{p},i})^{b_{\mathfrak{p},i}}\colon i \in I_\mathfrak{p}\}$, $B = \left\langle (B_0)^b, \mathcal{B}_{\mathfrak{p},0}\right\rangle_{\mathfrak{p}\in S}$, $\alpha((B_0)^b) = A_0$ and $\alpha((B_{\mathfrak{p},i})^{b_{\mathfrak{p},i}}) = A_{\mathfrak{p},i}$ for every $\mathfrak{p}$ and i. Without loss of generality assume that $B_0^b = B_0$. Omit some of the $(B_{\mathfrak{p},i})^{b_{\mathfrak{p},i}}$, if necessary, to assume from now on that they are distinct. Since $G_0 = \hat{F}_e$ and $\mathbf{B}$ is e-bounded, there exists an epimorphism $\gamma_0\colon G_0 \to B_0$ with $\alpha \circ \gamma_0 = \varphi|_{G_0}$ by Lemma 3.3.7.

Since $T_\mathfrak{p}$ is homeomorphic to $\mathcal{H}_{\mathfrak{p},0}$ by Lemma 3.4.4(3), $\mathcal{H}_{\mathfrak{p},0}$ is perfect. Hence, by Lemma 1.3.7, there exists a continuous surjective map $\lambda_\mathfrak{p}\colon \mathcal{H}_{\mathfrak{p},0} \to \mathcal{B}_{\mathfrak{p},0}$ such that $\alpha(\lambda_\mathfrak{p}(\Delta)) = \varphi(\Delta)$ for every $\Delta \in \mathcal{H}_{\mathfrak{p},0}$. For $i \in I_\mathfrak{p}$, let $T_{\mathfrak{p},i} = \{t \in T_\mathfrak{p}\colon \lambda_\mathfrak{p}(H_{\mathfrak{p},t}) = (B_{\mathfrak{p},i})^{b_{\mathfrak{p},i}}\}$. Then $T_\mathfrak{p} = \bigcup_{i\in I_\mathfrak{p}} T_{\mathfrak{p},i}$. Since $\lambda_\mathfrak{p}$ is surjective, each $T_{\mathfrak{p},i}$ is nonempty. Since $\lambda_\mathfrak{p}$ is continuous, and the map $t \mapsto H_{\mathfrak{p},t}$ is continuous by Lemma 3.4.4(3), $T_{\mathfrak{p},i}$ is open-closed. Note that if $t \in T_{\mathfrak{p},i}$, then $\varphi(H_{\mathfrak{p},t}) = A_{\mathfrak{p},i}$.

Since α is rigid, α is injective on each element of $\mathcal{B}_{\mathfrak{p},0}$. Hence, we can define a morphism β from the sheaf $(\bigcup_{\mathfrak{p}\in S} \Gamma_\mathfrak{p} \times T_\mathfrak{p}, \pi, \bigcup_{\mathfrak{p}\in S} T_\mathfrak{p})$ to B by

$$\beta|_{\Gamma_\mathfrak{p}\times T_{\mathfrak{p},i}} = (\alpha|_{(B_{\mathfrak{p},i})^{b_{\mathfrak{p},i}}})^{-1} \circ \varphi \circ \lambda.$$

The morphism β defines a homomorphism $\gamma_H\colon H \to B$ with $\gamma_H \circ \lambda = \beta$. Since for $t \in T_{\mathfrak{p},i}$, $\beta(\Gamma_\mathfrak{p} \times \{t\}) = (B_{\mathfrak{p},i})^{b_{\mathfrak{p},i}}$, the homomorphism

γ_H extends to a homomorphism of group piles $\gamma_H\colon \mathbf{H} \to \mathbf{B}^{\mathrm{def}}$. By Lemma 3.3.5, γ_H extends to a homomorphism $\gamma\colon \mathbf{G} \to \mathbf{B}$ with $\gamma|_{G_0} = \gamma_0$.

Since each $T_{\mathfrak{p},i}$ is nonempty, $\gamma(\mathcal{H}_{\mathfrak{p},0}) = \mathcal{B}_{\mathfrak{p},0}$, so $B = \langle B_0, \mathcal{B}_{\mathfrak{p},0}\rangle_{\mathfrak{p}\in S}$ implies that $\gamma\colon G \to B$ is surjective. Since $\mathcal{B}_{\mathfrak{p},0}$ meets every B-conjugacy class of $\mathcal{B}_{\mathfrak{p}}$, $\gamma(\mathcal{G}_{\mathfrak{p}}) = \mathcal{B}_{\mathfrak{p}}$ for every $\mathfrak{p} \in S$, so $\gamma\colon \mathbf{G} \to \mathbf{B}$ is an epimorphism of group piles. If $h = \lambda(x,t) \in H_{\mathfrak{p},t}$, $x \in \Gamma_{\mathfrak{p}}$, $t \in T_{\mathfrak{p},i}$, then

$$\alpha \circ \gamma_H(h) = \alpha \circ \gamma_H \circ \lambda(x,t) = \alpha \circ \beta(x,t) = \varphi \circ \lambda(x,t) = \varphi(h),$$

so $\alpha \circ \gamma|_H = \varphi|_H$ by the universal property of the free product. Also, $\alpha \circ \gamma|_{G_0} = \varphi|_{G_0}$, so $\alpha \circ \gamma = \varphi$ by the uniqueness in Lemma 3.3.5. □

3.5. S-adic Absolute Galois Group Piles

We now define the S-adic absolute Galois group pile of a field.

For the rest of this chapter, let S be a finite set of local primes of a field K of characteristic zero.

LEMMA 3.5.1. *Let G be a profinite group and Γ a finitely generated profinite group. Then*

$$\mathcal{G} = \{H \le G\colon H \text{ is a quotient of } \Gamma\} \subseteq \mathrm{Subgr}(G)$$

is closed.

PROOF. We prove that $\mathrm{Subgr}(G) \smallsetminus \mathcal{G}$ is open. Let $H \le G$ such that H is not a quotient of Γ. Since Γ is finitely generated, by Lemma 1.3.2(2) there exists an open normal subgroup $H_0 \lhd H$ such that H/H_0 is not a quotient of Γ. Let $N \lhd G$ be an open normal subgroup with $N \cap H \le H_0$. Since H/H_0 is not a quotient of Γ, also $H/(N\cap H)$ is not a quotient of Γ. If $H' \le G$ and $H'N = HN$, then $H'/(N\cap H') \cong H'N/N \cong H/(N\cap H)$, hence H' is not a quotient of Γ. Therefore, $\mathrm{Subgr}(G) \smallsetminus \mathcal{G}$ is open. □

DEFINITION 3.5.2. If $F \supseteq K$ is an extension, let

$$\mathcal{G}_{\mathfrak{p}} = \{\mathrm{Gal}(F')\colon F' \in \mathrm{CC}(F,\mathfrak{p})\},$$

cf. Definition 2.2.3, and let

$$\mathbf{Gal}_S(F) = (\mathrm{Gal}(F), \mathcal{G}_{\mathfrak{p}})_{\mathfrak{p}\in S}$$

be the **S-adic absolute Galois group pile** of F. For a Galois extension E/F, let

$$\mathbf{Gal}_S(E/F) = \mathbf{Gal}_S(F)/\mathrm{Gal}(E)$$

be the **S-adic Galois group pile** of E/F.

The following lemma is similar to [HJP09b, Lemma 10.3(c)-(d)], which, however, is concerned with fields instead of group piles, and is restricted to certain subfields of $K_{\mathrm{tot},S}$.

LEMMA 3.5.3. *The S-adic absolute Galois group pile $\mathbf{Gal}_S(F)$ is a separated reduced deficient group pile.*

PROOF. Let $\mathbf{G} = (G, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S} = \mathbf{Gal}_S(F)$.

PART A: $\mathbf{G}$ IS A GROUP PILE. Let $\mathbf{Gal}_S(K) = (H, \mathcal{H}_\mathfrak{p})_{\mathfrak{p}\in S}$ and $\mathfrak{p} \in S$. We have to show that $\mathcal{G}_\mathfrak{p}$ is closed. Let $\Gamma = \mathrm{Gal}(K_\mathfrak{p})$. Since $\mathfrak{p}$ is local, $\mathcal{H}_\mathfrak{p} = \Gamma^H$ is closed in $\mathrm{Subgr}(H)$. By Proposition 1.4.3 and Lemma 1.6.5, Γ is finitely generated. Let $G_0 \leq G$.

We claim that $G_0 \in \mathcal{G}_\mathfrak{p}$ if and only if G_0 is a quotient of Γ and $\mathrm{res}_{\tilde{F}/\tilde{K}}(G_0) \in \mathcal{H}_\mathfrak{p}$. Indeed, if $G_0 \in \mathcal{G}_\mathfrak{p}$, then $\mathrm{res}_{\tilde{F}/\tilde{K}}(G_0) \in \mathcal{H}_\mathfrak{p}$ and $G_0 \cong \mathrm{res}_{\tilde{F}/\tilde{K}}(G_0) \cong \Gamma$ by Lemma 2.11.2. Conversely, if $\mathrm{res}_{\tilde{F}/\tilde{K}}(G_0) \in \mathcal{H}_\mathfrak{p} = \Gamma^H$, then Γ is quotient of G_0. Hence, if also G_0 is a quotient of Γ, then $G_0 \cong \Gamma$ by Lemma 1.3.2(1). Therefore, by Lemma 2.11.1, the fixed field F' of G_0 is real closed resp. p-adically closed of the same type as $K_\mathfrak{p}$. In addition, $\mathrm{res}_{\tilde{F}/\tilde{K}}(G_0) \in \mathcal{H}_\mathfrak{p}$ implies that $F' \in \mathrm{CC}(F, \mathfrak{p})$, i.e. $G_0 \in \mathcal{G}_\mathfrak{p}$.

By Lemma 3.5.1, the set of $G_0 \leq G$ such that G_0 is a quotient of Γ is closed. Since $\mathcal{H}_\mathfrak{p} = \Gamma^H$ is closed, and $\mathrm{res}_{\tilde{F}/\tilde{K}}\colon \mathrm{Subgr}(G) \to \mathrm{Subgr}(H)$ is continuous by Lemma 3.1.2, the set of $G_0 \leq G$ with $\mathrm{res}_{\tilde{F}/\tilde{K}}(G_0) \in \mathcal{H}_\mathfrak{p}$ is closed. Therefore, $\mathcal{G}_\mathfrak{p}$ is closed.

PART B: $\mathbf{G}$ IS SEPARATED AND REDUCED. Let $\mathfrak{p}, \mathfrak{q} \in S$, $\Gamma \in \mathcal{G}_\mathfrak{p}$, $\Gamma_1 \in \mathcal{G}_\mathfrak{q}$, and assume that $\Gamma \subseteq \Gamma_1$.

If $\mathrm{char}(\mathfrak{p}) = \infty$ or $\mathrm{char}(\mathfrak{q}) = \infty$, then $\Gamma = \Gamma_1$, since the absolute Galois group of a real closed field is finite (Proposition 1.4.3), and the absolute Galois group of a p-adically closed field is non-trivial and torsion-free (Lemma 1.6.5). So since the ordering of a real closed field is unique, $\mathfrak{p} = \mathfrak{q}$.

If $\mathrm{char}(\mathfrak{p}) = p \neq \infty$ and $\mathrm{char}(\mathfrak{q}) = q \neq \infty$, let F' and F_1' be the fixed fields of Γ resp. Γ_1, and let $K' = \tilde{K} \cap F'$ and $K_1' = \tilde{K} \cap F_1'$. Then $K_1' \subseteq K'$, and $K' \in \mathrm{CC}(K, \mathfrak{p})$ and $K_1' \in \mathrm{CC}(K, \mathfrak{q})$ by Lemma 2.11.2. Thus, since $\mathfrak{p}$ and $\mathfrak{q}$ are local, K' is Henselian with respect to two rank one valuations, which must be equivalent by F. K. Schmidt's theorem, cf. [EP05, 4.4.1]. In particular, $p = q$. Thus the restriction of the unique p-valuation of F' to F_1' is the unique p-valuation of F', so $\mathfrak{p} = \mathfrak{q}$. Therefore, by the maximality of p-adically closed fields (of the same type), $F' = F_1'$, hence $\Gamma = \Gamma_1$. □

REMARK 3.5.4. The reader might want to check that in Lemma 3.5.3 we indeed proved what we promised in the proof of Proposition 2.2.11, and that we did not use Proposition 2.2.11 or any of its consequences in the proof of Lemma 3.5.3.

REMARK 3.5.5. If $(N_i)_{i\in I}$ is a directed family of closed normal subgroups of a group pile $\mathbf{G}$ with $\bigcap_{i\in I} N_i = 1$, then $\mathbf{G} \cong \varprojlim_{i\in I} \mathbf{G}/N_i$. In particular, $\mathbf{Gal}_S(F) = \varprojlim_E \mathbf{Gal}_S(E/F)$, where E ranges over all finite Galois extensions of F.

LEMMA 3.5.6. *Let $F \supseteq K$ be S-quasi-local, let M/F be an extension, and let*

$$\mathrm{res}_{\tilde{M}/\tilde{F}}\colon \mathbf{Gal}_S(M) \to \mathbf{Gal}_S(F)$$

be the restriction map. Then $\mathrm{res}_{\tilde{M}/\tilde{F}}$ is a homomorphism of group piles, and the following are equivalent.

1. *$\mathrm{res}_{\tilde{M}/\tilde{F}}$ is an epimorphism.*
2. *$\mathrm{res}_{\tilde{M}/\tilde{F}}$ is a rigid epimorphism.*
3. *M/F is regular and totally S-adic.*

PROOF. Let $\mathfrak{p} \in S$. If $M' \in \mathrm{CC}(M, \mathfrak{p})$, then $F' = M' \cap \tilde{F} \in \mathrm{CC}(F, \mathfrak{p})$ by Lemma 2.11.2. Thus, $\mathrm{res}_{\tilde{M}/\tilde{F}}\colon \mathrm{Gal}(M) \to \mathrm{Gal}(F)$ indeed induces a homomorphism of group piles $\mathrm{res}_{\tilde{M}/\tilde{F}}\colon \mathbf{Gal}_S(M) \to \mathbf{Gal}_S(F)$.

PROOF OF (1) $\Rightarrow$ (3). Suppose that $\mathrm{res}_{\tilde{M}/\tilde{F}}\colon \mathbf{Gal}_S(M) \to \mathbf{Gal}_S(F)$ is an epimorphism of group piles. Then $\mathrm{res}_{\tilde{M}/\tilde{F}}\colon \mathrm{Gal}(M) \to \mathrm{Gal}(F)$ is surjective, so M/F is regular. Let $\mathfrak{p} \in S$, $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$, and $F' \in \mathrm{CC}(F, \mathfrak{P})$. Then there exists $M' \in \mathrm{CC}(M, \mathfrak{p})$ with $M' \cap \tilde{F} = F'$. Let $\mathfrak{Q}'$ be the unique prime of M' lying over $\mathfrak{p}$ and let $\mathfrak{Q} = \mathfrak{Q}'|_M$. Then $\mathrm{tp}(\mathfrak{Q}) = \mathrm{tp}(\mathfrak{p})$, so $\mathfrak{Q} \in \mathcal{S}_{\mathfrak{p}}(M)$, and $\mathfrak{Q}|_F = \mathfrak{P}$. Therefore, M/F is totally S-adic.

PROOF OF (3) $\Rightarrow$ (2). Since M/F is regular, $\mathrm{res}_{\tilde{M}/\tilde{F}}\colon \mathrm{Gal}(M) \to \mathrm{Gal}(F)$ is surjective. Consider $\mathfrak{p} \in S$, $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(F)$, and $F' \in \mathrm{CC}(F, \mathfrak{P})$. Since M/F is totally S-adic, there exists $\mathfrak{Q} \in S_{\mathfrak{p}}(M)$ lying over $\mathfrak{P}$. If $M'' \in \mathrm{CC}(M, \mathfrak{Q})$, then $F'' = M'' \cap \tilde{F} \in \mathrm{CC}(F, \mathfrak{P})$ by Lemma 2.11.2. Since $\mathfrak{P}$ is quasi-local, F' and F'' are conjugate over F. Since $\mathrm{res}_{\tilde{M}/\tilde{F}}$ is surjective, there exists a conjugate $M' \in \mathrm{CC}(M, \mathfrak{Q})$ of M'' with $M' \cap \tilde{F} = F'$. Therefore, $\mathrm{res}_{\tilde{M}/\tilde{F}}\colon \mathbf{Gal}_S(M) \to \mathbf{Gal}_S(F)$ is an epimorphism of group piles. By Lemma 2.11.2, res: $\mathrm{Gal}(M') \to \mathrm{Gal}(F')$ is an isomorphism, so $\mathrm{res}_{\tilde{M}/\tilde{F}}$ is rigid.

PROOF OF (2) $\Rightarrow$ (1). This is trivial. □

3.6. e-Free C-Piles

We generalize the 'Cantor group piles' of [HJP09b] to e-free C-piles.

DEFINITION 3.6.1. An **e-free C-pile** is a deficient group pile $\mathbf{G}$ that satisfies the following conditions:

1. $\mathbf{G}$ is e-generated.
2. Every finite rigid e-generated deficient embedding problem for $\mathbf{G}$ is solvable.

LEMMA 3.6.2. *If $e < \omega$ and $\mathbf{G}$ is an e-free C-pile, then $\bar{G} \cong \hat{F}_e$.*

PROOF. If B is a finite group with $\mathrm{rank}(B) \leq e$, then $(\mathbf{G} \to 1, B \to 1)$ is a finite rigid e-generated deficient embedding problem for $\mathbf{G}$, so it

has a solution by (2). Therefore, by Lemma 3.1.16, every finite group B with $\mathrm{rank}(B) \leq e$ is a quotient of $\bar{G}$. Together with (1) this implies that $\bar{G} \cong \hat{F}_e$, cf. Lemma 1.3.2(1). □

PROPOSITION 3.6.3. *Let* $\mathbf{G}$ *be an* e*-free semi-constant group pile of non-trivial profinite groups* $(\Gamma_\mathfrak{p})_{\mathfrak{p}\in S}$ *over perfect profinite spaces* $(T_\mathfrak{p})_{\mathfrak{p}\in S}$*. Then the deficient reduct* $\mathbf{G}^{\mathrm{def}}$ *of* $\mathbf{G}$ *is an* e*-free* C*-pile.*

PROOF. By Lemma 3.4.6(1), $\mathbf{G}$ is e-bounded and self-generated. If $e < \omega$, then Lemma 3.4.4(1) and Lemma 3.3.6 imply that $\bar{G} \cong \hat{F}_e$, so $\mathbf{G}^{\mathrm{def}}$ satisfies (1). If $e = \omega$, then (1) is trivially satisfied.

Let $EP = (\varphi\colon \mathbf{G}^{\mathrm{def}} \to \tilde{\mathbf{A}}, \alpha\colon \tilde{\mathbf{B}} \to \tilde{\mathbf{A}})$ be a finite rigid e-generated deficient embedding problem for $\mathbf{G}^{\mathrm{def}}$. By Lemma 3.2.3, EP is locally solvable. By Lemma 3.3.8 there exist $\mathbf{A}$ and $\mathbf{B}$ with $\mathbf{A}^{\mathrm{def}} = \tilde{\mathbf{A}}$ and $\mathbf{B}^{\mathrm{def}} = \tilde{\mathbf{B}}$ such that $(\varphi\colon \mathbf{G} \to \mathbf{A},\ \alpha\colon \mathbf{B} \to \mathbf{A})$ is a locally solvable e-bounded rigid self-generated embedding problem. By Proposition 3.4.8, this embedding problem has a solution, which in turn induces a solution of EP. Therefore, $\mathbf{G}^{\mathrm{def}}$ satisfies (2). □

REMARK 3.6.4. If $\mathbf{G}$ is the e-free semi-constant group pile of $(\Gamma_\mathfrak{p})_{\mathfrak{p}\in S}$ over $(T_\mathfrak{p})_{\mathfrak{p}\in S}$, then $\mathcal{G}_\mathfrak{p}/G$ is homeomorphic to $T_\mathfrak{p}$ for every $\mathfrak{p} \in S$ by Lemma 3.4.4(3) and Lemma 3.3.4(4). Thus, if $T_\mathfrak{p}$ is perfect, then so is $\mathcal{G}_\mathfrak{p}/G$. Conversely, one can prove that if $\mathbf{G}$ is an e-free C-pile, then $\mathcal{G}_\mathfrak{p}/G$ is perfect for each $\mathfrak{p} \in S$.

LEMMA 3.6.5. *Every finite locally solvable* e*-generated deficient embedding problem for an* e*-free* C*-pile* $\mathbf{G}$ *is solvable.*

PROOF. Let $EP = (\varphi\colon \mathbf{G} \to \tilde{\mathbf{A}},\ \alpha\colon \tilde{\mathbf{B}} \to \tilde{\mathbf{A}})$ be a finite locally solvable e-generated deficient embedding problem for $\mathbf{G}$. We claim that there exist a locally solvable e-bounded embedding problem $EP_1 = (\varphi\colon \mathbf{G}^* \to \mathbf{A},\ \alpha\colon \mathbf{B} \to \mathbf{A})$ where $\mathbf{G}^*$ is e-bounded, $(\mathbf{G}^*)^{\mathrm{def}} = \mathbf{G}$, $\mathbf{A}^{\mathrm{def}} = \tilde{\mathbf{A}}$ and $\mathbf{B}^{\mathrm{def}} = \tilde{\mathbf{B}}$. Once this is shown, EP_1 can be dominated by a finite e-bounded rigid embedding problem EP_2 by Proposition 3.2.9. By property (2) of Definition 3.6.1, the deficient reduct of EP_2 has a solution. It induces a solution of EP.

PROOF OF THE CLAIM. If $e = \omega$, then $\mathbf{G}$ and $\mathbf{B}$ are e-bounded (Definition 3.1.17), so (φ, α) satisfies the claim. Therefore, assume that $e < \omega$. By Lemma 3.6.2, $\bar{G} \cong \hat{F}_e$. Let $G_0 \leq G$ be a subgroup of rank at most e that under the quotient map $G \to \bar{G}$ maps onto $\bar{G} \cong \hat{F}_e$. Since every finite group generated by e elements is a quotient of $\hat{F}_e$, it is also a quotient of G_0, and thus $G_0 \cong \hat{F}_e$ by Lemma 1.3.2(1). Moreover, $\mathbf{G}^* = (G, (G_0)^G, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S}$ is e-bounded. By Lemma 3.3.8, there exist $\mathbf{A}$ and $\mathbf{B}$ with $\mathbf{A}^{\mathrm{def}} = \tilde{\mathbf{A}}$ and $\mathbf{B}^{\mathrm{def}} = \tilde{\mathbf{B}}$ such that EP_1 is locally solvable and e-bounded. □

3.7. Axiomatization of C-Piles

We prove that the class of PSCC fields whose S-adic absolute Galois group pile is an e-free C-pile is elementary.

For the rest of this section we drop the usual simplifying assumption that all algebraic extensions of a field F are contained in a fixed algebraic closure $\tilde{F}$ of F. Note however that for example $\mathbf{Gal}_S(E/F)$ is still well defined up to isomorphism for any Galois extension E/F, since it does not depend on the choice of an embedding of E into $\tilde{F}$.

DEFINITION 3.7.1. A **regular representation** of a finite group pile $\mathbf{G}$ of order n (cf. Definition 3.1.6) is a regular permutation representation of the underlying group G, i.e. an embedding $G \hookrightarrow S_n$ such that G acts transitively on $\{1, \dots, n\}$.

REMARK 3.7.2. Note that if $\alpha\colon G \hookrightarrow S_n$ and $\beta\colon G \hookrightarrow S_n$ are regular representations of G, then α and β are conjugate in S_n, i.e. there exists $\tau \in S_n$ such that $\beta(g) = \tau^{-1}\alpha(g)\tau$ for each $g \in G$.

REMARK 3.7.3. Let F be a field and M/F a finite Galois extension with Galois group G. We represent the extension M/F and G in elementary terms.

First we choose an irreducible monic polynomial

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in F[X]$$

with coefficients in F such that a root of f generates M over F. Then let

$$F_{\mathbf{a}} := F[X]/(f(X))$$

and note that $F_{\mathbf{a}}$ is a field F-isomorphic to M. Every element of $F_{\mathbf{a}}$ can be uniquely represented as a polynomial in X of degree at most $n-1$ with coefficients in F. Addition and multiplication in $F_{\mathbf{a}}$ are carried out by adding and multiplying polynomials of degree at most $n-1$ and then reducing modulo f.

In particular, the n distinct roots $x_1, \dots, x_n$ of f can be represented by n polynomials $h_1, \dots, h_n \in F[X]$ of degree at most $n-1$ such that $x_1 = x := X + (f(X))$ and $x_i = h_i(x)$, $i = 1, \dots, n$. Fixing the roots of f in this way gives rise to an embedding $\sigma \mapsto \sigma'$ of $\mathrm{Gal}(F_{\mathbf{a}}/F)$ into the symmetric group S_n such that $\sigma(x_i) = x_j$ if and only if $\sigma'(i) = j$. Thus,

$$\sigma(h_i(x)) = h_{\sigma'(i)}(x).$$

It follows that by fixing the $(n+1)$-tuple of polynomials $(f, h_1, \dots, h_n)$ we represent both the Galois extension $F_{\mathbf{a}}$ of F and a regular representation of $\mathrm{Gal}(F_{\mathbf{a}}/F)$. We write this $(n+1)$-tuple of polynomials by the $(n+1)$-tuple $\mathbf{b} = (\mathbf{a}, \mathbf{a}_1, \dots, \mathbf{a}_n)$ of their tuples of coefficients.

LEMMA 3.7.4. *There exists a recursive map* $\mathbf{A} \mapsto \theta_{\mathrm{realize},\mathbf{A}}(\mathbf{x})$ *from finite group piles (with regular representations) to* $\mathcal{L}_{\mathrm{ring}}(K)$*-formulas*

with the following property: For each finite deficient group pile $\mathbf{A}$ *of order* n *with a regular representation* $A \hookrightarrow S_n$ *and each* PSCC *field* $F \supseteq K$,

$$F \models \theta_{\mathrm{realize},\mathbf{A}}(\mathbf{a})$$

if and only if $\mathbf{a}$ *represents a finite Galois extension* $M = F_{\mathbf{a}}$ *of* F *and a regular representation* $\mathrm{Gal}(M/F) \hookrightarrow S_n$ *that induces an isomorphism*

$$\eta_{\mathbf{a}} \colon \mathbf{Gal}_S(M/F) \to \mathbf{A}.^2$$

Proof. There are essentially two things to express elementarily: First, the image of the induced embedding $\mathrm{Gal}(M/F) \hookrightarrow S_n$ coincides with the image of the regular representation $A \hookrightarrow S_n$. Second, the induced isomorphism $\mathrm{Gal}(M/F) \to A$ extends to an isomorphism of group piles. To that end suppose that $\mathbf{x}$ is a tuple of variables representing the coefficients of polynomials $f, h_1, \dots, h_n$ as in Remark 3.7.3.

Concerning the first part, we assume that the reader knows how to express that f is an irreducible Galois polynomial and $h_1(x), \dots, h_n(x)$ are distinct roots of f, where x is the residue of X modulo f. Any $\sigma \in \mathrm{Gal}(M/F)$ is determined by its action on x. Indeed, if $\sigma(x) = h_j(x)$, then $\sigma(h_i(x)) = h_i(h_j(x))$. Thus the image of $\mathrm{Gal}(M/F) \hookrightarrow S_n$ consists of all $\tau \in S_n$ that satisfy for all i

$$h_{\tau(i)}(X) \equiv h_i(h_{\tau(1)}(X)) \bmod f(X).$$

So by going through all $\tau \in S_n$, one can formulate that this image is exactly the image of $A \hookrightarrow S_n$, also cf. [FJ08, proof of Proposition 20.4.4].

Now we turn to the second part. Write

$$\mathbf{G} = (G, \mathcal{G}_{\mathfrak{p}})_{\mathfrak{p} \in S} = \mathbf{Gal}_S(M/F)$$

and let $\mathfrak{p} \in S$. Note that a subgroup $\Gamma \leq \mathrm{Gal}(M/F)$ with fixed field M' belongs to $\mathcal{G}_{\mathfrak{p}}$ if and only if there exists $F' \in \mathrm{CC}(F, \mathfrak{p})$ such that $M' = F' \cap M$. Let $M_1, \dots, M_k$ be all intermediate fields of M/F and for each i choose a minimal polynomial f_i of a primitive element of M_i/F. Let I be the set of all $1 \leq i \leq k$ such that f_i has a zero in M'.

Then a field $L \supseteq F$ satisfies the sentence θ_I given by

$$\bigwedge_{i \in I} (\exists x)(f_i(x) = 0) \wedge \bigwedge_{i \notin I} \neg(\exists x)(f_i(x) = 0)$$

if and only if $L \cap M$ is conjugate to M' over F. Indeed, if L satisfies θ_I, then for every i, M_i can be F-embedded into M' if and only if M_i can be F-embedded into $L \cap M$. This implies that M' and $L \cap M$ are F-isomorphic. Conversely, assume that $M' \cong_F L \cap M$. Then each f_i has a zero in M' if and only if it has a zero in L, hence L satisfies θ_I.

By Corollary 2.7.7, $F \models \neg(\widehat{\neg\theta_I})_{\mathfrak{p},\forall}$, if and only if there exists $F' \in \mathrm{CC}(F, \mathfrak{p})$ such that $F' \cap M$ is F-conjugate to M'. Since a conjugate

[2]That is, the group pile $\mathbf{A}$ is *realized* over F.

of a classical closure is again a classical closure, this is the case if and only if $\Gamma \in \mathcal{G}_{\mathfrak{p}}$.

The image of Γ in S_n can be described as follows: Assume that $M' = M_i$ and let $g \in F[X]$ be such that $f_i(g(x)) = 0$. Then $\sigma \in \mathrm{Gal}(M/F)$ lies in $\Gamma = \mathrm{Gal}(M/M')$ if and only if $\sigma(g(x)) = g(x)$. Thus, up to conjugation, the image of Γ in S_n consists of all τ in the image of $\mathrm{Gal}(M/F)$ such that

$$g(h_{\tau(1)}(X)) \equiv g(X) \bmod f(X).$$

Combining the above ingredients, we get the formula $\theta_{\mathrm{realize},\mathbf{A}}(\mathbf{x})$ with the desired properties. This can be done in a way such that the map $\mathbf{A} \mapsto \theta_{\mathrm{realize},\mathbf{A}}(\mathbf{x})$ is recursive, since the map $\varphi \mapsto \hat{\varphi}_{\mathfrak{p},\forall}$ of Proposition 2.6.6 is recursive. Note that we do not need to 'compute' the polynomials $f_i \in F[X]$ and the set I. We rather write down formulas *defining* the f_i and I. □

LEMMA 3.7.5. *There exists a recursive map $\alpha \mapsto \theta_{\mathrm{res},\alpha}(\mathbf{y},\mathbf{x})$ from epimorphisms of finite deficient group piles (with regular representations) to $\mathcal{L}_{\mathrm{ring}}(K)$-formulas with the following property: For each epimorphism $\alpha\colon \mathbf{B} \to \mathbf{A}$ of finite deficient group piles with fixed regular representations and each* PSCC *field $F \supseteq K$,*

$$F \models \theta_{\mathrm{res},\alpha}(\mathbf{b},\mathbf{a})$$

if and only if $\mathbf{a}$ and $\mathbf{b}$ represent finite Galois extensions M/F, N/F, and isomorphisms $\eta_{\mathbf{a}}\colon \mathbf{Gal}_S(M/F) \to \mathbf{A}$, $\eta_{\mathbf{b}}\colon \mathbf{Gal}_S(N/F) \to \mathbf{B}$, such that there is an F-embedding $M \hookrightarrow N$ with

$$\alpha \circ \eta_{\mathbf{b}} = \eta_{\mathbf{a}} \circ \mathrm{res}_{N/M}|_{\mathrm{Gal}(N/F)}.$$[3]

PROOF. Let $\mathbf{b}$ be a list of the coefficients of polynomials $f, f_1, \ldots, f_m \in F[X]$ and $\mathbf{a}$ a list of the coefficients of polynomials $g, g_1, \ldots, g_n \in F[Y]$. Furthermore, identify A and B with their regular representations $A \subseteq S_n$, $B \subseteq S_m$. Also, identify $\mathbf{Gal}_S(M/F)$ with $\mathbf{A}$ via $\eta_{\mathbf{a}}$ and $\mathbf{Gal}_S(N/F)$ with $\mathbf{B}$ via $\eta_{\mathbf{b}}$.

Let $x \in N$ be the residue of X modulo f, and $y \in M$ the residue of Y modulo g. The F-embeddings $M \hookrightarrow N$ correspond to maps $y \mapsto q(x)$, where $q \in F[Z]$ is a polynomial of degree $< m$ such that $g(q(x)) = 0$.

Given $\sigma \in \mathrm{Gal}(N/F)$,

$$\sigma(q(x)) = q(\sigma(x)) = q(f_{\sigma(1)}(x))$$

and

$$\sigma(q(x)) = \mathrm{res}_{N/M}(\sigma)(y) = g_{\mathrm{res}_{N/M}(\sigma)(1)}(y).$$

Therefore, since $\mathrm{res}_{N/M} = \alpha$ if and only if $g_{(\mathrm{res}_{N/M}\sigma)(1)}(y) = g_{\alpha(\sigma)(1)}(y)$ for all $\sigma \in \mathrm{Gal}(N/F)$, it follows that $\mathrm{res}_{N/M} = \alpha$ if and only if $q(f_{\sigma(1)}(x)) = g_{\alpha(\sigma)(1)}(q(x))$ for all $\sigma \in B$, c.f. [FJ08, 23.4.1].

[3]The subscript $_{\mathrm{res}}$ stands for *restriction*.

Thus there exists an embedding $M \hookrightarrow N$ such that $\alpha \circ \eta_{\mathbf{b}} = \eta_{\mathbf{a}} \circ \mathrm{res}_{N/M}$ if and only if there exists $q(Z) \in F[Z]$ of degree $< m$ such that

$$g(q(X)) \equiv 0 \bmod f(X)$$

and

$$q(f_{\sigma(1)}(X)) \equiv g_{\alpha(\sigma)(1)}(q(X)) \bmod f(X)$$

for all $\sigma \in B$.

Using Lemma 3.7.4, one now sees how to construct $\theta_{\mathrm{res},\alpha}(\mathbf{y}, \mathbf{x})$. □

Definition 3.7.6. Let the $\mathcal{L}_{\mathrm{ring}}(K)$-theory $T_{\mathrm{C},S,e}$ consist of the following sentences.

(1) For each finite deficient group pile $\mathbf{A}$ (with regular representation) which is not e-generated the sentence

$$\neg(\exists \mathbf{x})\theta_{\mathrm{realize},\mathbf{A}}(\mathbf{x}).$$

(2) For each rigid epimorphism $\alpha\colon \mathbf{B} \to \mathbf{A}$ of finite e-generated deficient group piles (with regular representations) the sentence

$$(\forall \mathbf{x})[\theta_{\mathrm{realize},\mathbf{A}}(\mathbf{x}) \to ((\exists \mathbf{y})\theta_{\mathrm{realize},\mathbf{B}}(\mathbf{y}) \wedge \theta_{\mathrm{res},\alpha}(\mathbf{y}, \mathbf{x}))].$$

Lemma 3.7.7. *A* P*SCC field $F \supseteq K$ is a model of $T_{\mathrm{C},S,e}$ if and only if $\mathbf{Gal}_S(F)$ is an e-free C-pile.*

Proof. Let $\mathbf{G} = \mathbf{Gal}_S(F)$. By Lemma 3.7.4, F satisfies (1) of Definition 3.7.6 if and only if all finite quotients of $\mathbf{G}$ are e-generated. By Lemma 3.1.20 this is equivalent to (1) of Definition 3.6.1.

If F satisfies (2) of Definition 3.7.6, then $\mathbf{G}$ satisfies (2) of Definition 3.6.1 by Lemma 3.7.4 and Lemma 3.7.5. Conversely, if every finite rigid e-generated deficient embedding problem for $\mathbf{G}$ is solvable, then Remark 3.7.2 implies that F satisfies (2) of Definition 3.7.6. □

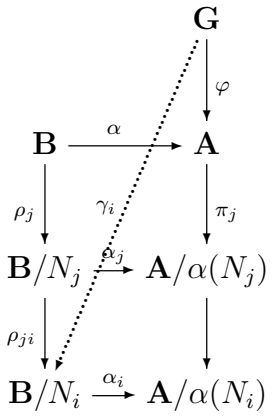
Remark 3.7.8. A more systematic approach to the elementary class of fields whose S-adic absolute Galois group pile is an e-free C-pile is possible by using the 'inverse systems' (also called 'CDM-presentations') of [CvdDM81], [CvdDM82], [Cha84], and [Cha98], or rather expansions of inverse systems to group piles, like in [Ers83a] (for so called 'involutory groups'), [Ers91] (for so called 'Γ-groups'), and [Ers95] (for 'Δ^*-groups'). The same is true for the proof of Proposition 3.8.1 below.

3.8. Solving Embedding Problems for C-Piles

By definition, a finite rigid e-generated deficient embedding problem for an e-free C-pile is solvable. We prove that under some conditions, also certain infinite embedding problems are solvable.

Proposition 3.8.1. *Let $F \supseteq K$ be an $\aleph_1$-saturated* P*SCC field, and assume that $\mathbf{G} = \mathbf{Gal}_S(F)$ is an e-free C-pile. Let $(\varphi\colon \mathbf{G} \to \mathbf{A},\ \alpha\colon \mathbf{B} \to \mathbf{A})$ be a rigid e-generated deficient embedding problem for $\mathbf{G}$, where $\mathbf{B}$ is of at most countable rank. Then (φ, α) has a solution.*

PROOF. Since $\operatorname{rank}(B) \leq \aleph_0$, there is a descending sequence of open normal subgroups $N_i \triangleleft B$, $i \in \mathbb{N}$, with $\bigcap_{i\in\mathbb{N}} N_i = 1$, cf. [FJ08, 17.1.7(a)]. For each $i \in \mathbb{N}$ let $\alpha_i\colon \mathbf{B}/N_i \to \mathbf{A}/\alpha(N_i)$ be the epimorphism induced by α, and for $i \leq j \in \mathbb{N}$ let $\pi_i\colon \mathbf{A} \to \mathbf{A}/\alpha(N_i)$, $\rho_i\colon \mathbf{B} \to \mathbf{B}/N_i$, $\rho_{ji}\colon \mathbf{B}/N_j \to \mathbf{B}/N_i$ be the quotient maps. Then $\alpha_i \circ \rho_i = \pi_i \circ \alpha$. By Lemma 3.2.3, the rigid deficient embedding problem (φ, α) is locally solvable, hence the induced embedding problem $(\pi_i \circ \varphi, \alpha_i)$ is locally solvable by Lemma 3.2.7. Since $\mathbf{B}$ is e-generated, $\mathbf{B}/N_i$ is e-generated by Lemma 3.1.19. Hence, $(\pi_i \circ \varphi, \alpha_i)$ is a finite locally solvable e-generated deficient embedding problem for $\mathbf{G}$. Since $\mathbf{G}$ is an e-free C-pile, this embedding problem has a solution $\gamma_i\colon \mathbf{G} \to \mathbf{B}/N_i$ by Lemma 3.6.5.



PART A: CONSTRUCTING A SET OF FORMULAS Σ. Once and for all choose regular representations of the groups B/N_i and the groups $A/\alpha(N_i)$. For every i, the epimorphism $\pi_i \circ \varphi$ corresponds to a finite Galois extension E_i/F with $E_i \subseteq \tilde{F}$. Choose $\mathbf{a}_i$ that represents a field $F_{\mathbf{a}_i}$ which is F-isomorphic to E_i and an isomorphism

$$\eta_i := \eta_{\mathbf{a}_i}\colon \mathbf{Gal}_S(F_{\mathbf{a}_i}/F) \to \mathbf{A}/\alpha(N_i),$$

such that for a certain identification $E_i = F_{\mathbf{a}_i}$ (which we fix from now on), $\eta_i \circ \operatorname{res}_{\tilde{F}/E_i} = \pi_i \circ \varphi$. This last condition implies that the inverse systems $(\mathbf{Gal}_S(E_i/F))_{i\in\mathbb{N}}$ and $(\mathbf{A}/\alpha(N_i))_{i\in\mathbb{N}}$ are isomorphic. In particular, writing $E_\infty = \bigcup_{i\in\mathbb{N}} E_i$, there is an isomorphism

$$\eta := \varprojlim_i \eta_i\colon \mathbf{Gal}_S(E_\infty/F) \to \mathbf{A}$$

with $\eta \circ \operatorname{res}_{\tilde{F}/E_\infty} = \varphi$.

Let $\Sigma(\mathbf{x}_1, \mathbf{x}_2, \dots)$ be the set of $\mathcal{L}_{\mathrm{ring}}(F)$-formulas that contains for each $k \in \mathbb{N}$ the formula

$$\bigwedge_{i\leq k} (\theta_{\mathrm{realize},\mathbf{B}/N_i}(\mathbf{x}_i) \wedge \theta_{\mathrm{res},\alpha_i}(\mathbf{x}_i, \mathbf{a}_i)) \wedge \bigwedge_{i\leq j\leq k} \theta_{\mathrm{res},\rho_{ji}}(\mathbf{x}_j, \mathbf{x}_i).$$

PART B: Σ IS FINITELY SATISFIABLE. We claim that every finite subset Σ_0 of Σ is satisfied in F. Let k be the maximal index that occurs in Σ_0. Let E be the fixed field of $\mathrm{Ker}(\gamma_k)$ in $\tilde{F}$. Choose $\mathbf{c}_k$ that represents a Galois extension $F_{\mathbf{c}_k}$ of F which is F-isomorphic to E and an isomorphism

$$\eta_{\mathbf{c}_k}\colon \mathbf{Gal}_S(F_{\mathbf{c}_k}/F) \to \mathbf{B}/N_k$$

such that for a certain identification $E = F_{\mathbf{c}_k}$ (which we fix from now on), $\eta_{\mathbf{c}_k} \circ \mathrm{res}_{\tilde{F}/E} = \gamma_k$. Then $F \models \theta_{\mathrm{realize},\mathbf{B}/N_k}(\mathbf{c}_k)$. Now combine $\mathrm{res}_{E/E_k} \circ \mathrm{res}_{\tilde{F}/E} = \mathrm{res}_{\tilde{F}/E_k}$ with $\alpha_k \circ \gamma_k = \pi_k \circ \varphi$ and $\eta_k \circ \mathrm{res}_{\tilde{F}/E_k} = \pi_k \circ \varphi$ to get that $\eta_k \circ \mathrm{res}_{E/E_k} \circ \mathrm{res}_{\tilde{F}/E} = \alpha_k \circ \eta_{\mathbf{c}_k} \circ \mathrm{res}_{\tilde{F}/E}$, and thus $\eta_k \circ \mathrm{res}_{E/E_k} = \alpha_k \circ \eta_{\mathbf{c}_k}$. Therefore, $F \models \theta_{\mathrm{res},\alpha_k}(\mathbf{c}_k, \mathbf{a}_k)$.

Since for $i \leq k$, $\mathbf{B}/N_i$ is a quotient of $\mathbf{B}/N_k$, there exist $\mathbf{c}_1, \ldots, \mathbf{c}_{k-1}$ such that for $i < k$, $F \models \theta_{\mathrm{realize},\mathbf{B}/N_i}(\mathbf{c}_i)$ and $F \models \theta_{\mathrm{res},\alpha_i}(\mathbf{c}_i, \mathbf{a}_i)$, and for $i \leq j \leq k$, $F \models \theta_{\mathrm{res},\rho_{ji}}(\mathbf{c}_j, \mathbf{c}_i)$. Therefore, $\mathbf{c}_1, \ldots, \mathbf{c}_k$ satisfy Σ_0.

PART C: USING $\aleph_1$-SATURATION. Since F is $\aleph_1$-saturated, Σ is satisfied in F. This means there are $\mathbf{b}_1, \mathbf{b}_2, \ldots$ such that for all pairs $i \leq j$,

$$F \models \theta_{\mathrm{realize},\mathbf{B}/N_i}(\mathbf{b}_i) \wedge \theta_{\mathrm{res},\alpha_i}(\mathbf{b}_i, \mathbf{a}_i) \wedge \theta_{\mathrm{res},\rho_{ji}}(\mathbf{b}_j, \mathbf{b}_i).$$

Since for every i, $F \models \theta_{\mathrm{realize},\mathbf{B}/N_i}(\mathbf{b}_i)$, every $\mathbf{b}_i$ represents a Galois extension F_i/F and an isomorphism

$$\zeta_i := \eta_{\mathbf{b}_i}\colon \mathbf{Gal}_S(F_i/F) \to \mathbf{B}/N_i.$$

Since for all i, $F \models \theta_{\mathrm{res},\rho_{i+1,i}}(\mathbf{b}_{i+1}, \mathbf{b}_i)$, we see that we can inductively choose embeddings $F_1 \hookrightarrow F_2 \hookrightarrow \ldots$ such that for all $i \leq j$, $\rho_{ji} \circ \zeta_j = \zeta_i \circ \mathrm{res}_{F_j/F_i}$. So the inverse systems $(\mathbf{Gal}_S(F_i/F))_{i\in\mathbb{N}}$ and $(\mathbf{B}/N_i)_{i\in\mathbb{N}}$ are isomorphic, and, with $F_\infty = \bigcup_{i\in\mathbb{N}} F_i$, there is an isomorphism

$$\zeta = \varprojlim_i \zeta_i\colon \mathbf{Gal}_S(F_\infty/F) \to \mathbf{B}.$$

Furthermore, since $F \models \theta_{\mathrm{res},\alpha_j}(\mathbf{b}_j, \mathbf{a}_j)$, we can choose embeddings $E_j \hookrightarrow F_j$ such that $\alpha_j \circ \zeta_j = \eta_j \circ \mathrm{res}_{F_j/E_j}$ for every j. If $i \leq j$, then the embedding $E_j \hookrightarrow F_j$ induces an embedding $E_i \hookrightarrow F_i$ (as we already fixed embeddings $E_i \hookrightarrow E_j$ and $F_i \hookrightarrow F_j$), and one may check that this one necessarily satisfies $\alpha_i \circ \zeta_i = \eta_i \circ \mathrm{res}_{F_i/E_i}$. Thus these embeddings combine to an embedding $E_\infty \hookrightarrow F_\infty$ with $\alpha \circ \zeta = \eta \circ \mathrm{res}_{F_\infty/E_\infty}$.

Now choose any embedding $F_\infty \hookrightarrow \tilde{F}$ that extends the embedding $E_\infty \hookrightarrow \tilde{F}$, and let $\gamma = \zeta \circ \mathrm{res}_{\tilde{F}/F_\infty}$. Then $\gamma\colon \mathbf{G} \to \mathbf{B}$ is an epimorphism and $\alpha \circ \gamma = \eta \circ \mathrm{res}_{F_\infty/E_\infty} \circ \mathrm{res}_{\tilde{F}/F_\infty} = \varphi$. Therefore, γ is a solution of the embedding problem (φ, α). $\square$

CHAPTER 4

Decidability of Almost All $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$

In this chapter, we define the fields $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$, give an axiomatization of the theory of almost all $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$, and prove that this theory is decidable.

For the rest of this work, let S be a finite set of local primes of a field K of characteristic zero, and let $0 \leq e \leq \omega$ be an ordinal number.

4.1. The Fields $K_{\mathrm{tot},S}$

We define and characterize the field $K_{\mathrm{tot},S}$ and give an axiomatization for the fields that are regular totally S-adic extensions of subfields of $K_{\mathrm{tot},S}$.

DEFINITION 4.1.1. The field of **totally S-adic elements** over K is defined as

$$K_{\mathrm{tot},S} = \bigcap_{\mathfrak{p} \in S} K_{\mathrm{tot},\mathfrak{p}},$$

where $K_{\mathrm{tot},\mathfrak{p}}$ is the maximal Galois extension of K in $K_{\mathfrak{p}}$.

REMARK 4.1.2. Note that although $K_{\mathfrak{p}} \subseteq \tilde{K}$ is determined only up to the action of $\mathrm{Gal}(K)$, the field $K_{\mathrm{tot},\mathfrak{p}} \subseteq \tilde{K}$ is independent of the chosen embedding.

LEMMA 4.1.3. *$K_{\mathrm{tot},S}$ is the largest totally S-adic Galois extension of K (cf. Definition 2.9.3).*

PROOF. First of all, $K_{\mathrm{tot},S}/K$ is totally S-adic. Indeed, if $\mathfrak{p} \in S$ and $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(K_{\mathfrak{p}})$, then $\mathfrak{P}|_{K_{\mathrm{tot},S}} \in \mathcal{S}_{\mathfrak{p}}(K_{\mathrm{tot},S})$.

Now suppose that L/K is a totally S-adic Galois extension. Let $\mathfrak{p} \in S$ and $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(L)$. Then Lemma 2.9.9(2) implies that $K_{\mathfrak{p}} \in \mathrm{CC}(K,\mathfrak{p}) = \mathrm{CC}(L,\mathfrak{p})$, so $L \subseteq K_{\mathfrak{p}}$. Since L/K is Galois, $L \subseteq K_{\mathrm{tot},S}$. $\square$

LEMMA 4.1.4. *$K_{\mathrm{tot},S}$ is the largest Galois extension of K in which each $\mathfrak{p} \in S$ totally splits (cf. Definition 2.1.6).*

PROOF. Let $\mathfrak{p} \in S$ and let L/K be a finite subextension of $K_{\mathrm{tot},S}/K$. Replace L by the Galois closure of L over K to assume without loss of generality that L/K is Galois. By Lemma 4.1.3, $K_{\mathrm{tot},S}/K$ is totally S-adic, so there exists $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(K_{\mathrm{tot},S})$. Let $\mathfrak{Q} = \mathfrak{P}|_L$. If $\mathrm{char}(\mathfrak{p}) = \infty$, then the primes of L lying over $\mathfrak{p}$ correspond to K-embeddings of L

into $K_{\mathfrak{p}}$. Since $L \subseteq L_{\mathfrak{Q}} = K_{\mathfrak{p}}$ is an embedding of this form, and L/K is Galois, there are $[L:K]$ many such embeddings. If $\mathrm{char}(\mathfrak{p}) \neq \infty$, then $v_{\mathfrak{Q}}/v_{\mathfrak{p}}$ is immediate and $v_{\mathfrak{p}}(K^{\times}) = \mathbb{Z}$, so the fundamental inequality (Lemma 1.5.2) implies that there are $[L:K]$ many conjugate extensions of $v_{\mathfrak{p}}$ to L. Therefore, $\mathfrak{p}$ totally splits in L/K, as claimed.

Conversely, let L/K be a Galois extension in which each $\mathfrak{p} \in S$ totally splits. We claim that L/K is totally S-adic. By Lemma 2.4.5, we can assume without loss of generality that L/K is finite. Let $\mathfrak{p} \in S$. If $\mathrm{char}(\mathfrak{p}) = \infty$, then $\mathcal{S}_{\mathfrak{p}}(L) \neq \emptyset$, since $\mathfrak{p}$ totally splits in L/K. If $\mathrm{char}(\mathfrak{p}) \neq \infty$, let $\mathfrak{P}$ be one of the $[L:K]$ many conjugate primes of L lying over $\mathfrak{p}$. By the fundamental inequality (Lemma 1.5.2), $v_{\mathfrak{P}}/v_{\mathfrak{p}}$ is immediate, so $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(L)$, as claimed. Therefore, L/K is totally S-adic, and thus $L \subseteq K_{\mathrm{tot},S}$ by Lemma 4.1.3. □

LEMMA 4.1.5. *Let $\mathfrak{p} \in S$ and $K \subseteq L \subseteq K_{\mathrm{tot},\mathfrak{p}}$. Then*

$$R_{\mathfrak{p}}(L) = L \cap \bigcap_{\tau \in \mathrm{Gal}(K)} R_{\mathfrak{p}}(K_{\mathfrak{p}})^{\tau}.$$

In particular, $R_{\mathfrak{p}}(L) = L \cap R_{\mathfrak{p}}(K_{\mathrm{tot},\mathfrak{p}})$.

PROOF. Since $\mathfrak{p}$ is local, every $K' \in \mathrm{CC}(K,\mathfrak{p})$ is K-conjugate to $K_{\mathfrak{p}}$. By Lemma 2.9.9(2), $\mathrm{CC}(L,\mathfrak{p}) = \mathrm{CC}(K,\mathfrak{p})$. Thus,

$$\begin{aligned} R_{\mathfrak{p}}(L) &= \bigcap_{\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(L)} \mathcal{O}_{\mathfrak{P}} \\ &= \bigcap_{L' \in \mathrm{CC}(L,\mathfrak{p})} (R_{\mathfrak{p}}(L') \cap L) \\ &= \bigcap_{K' \in \mathrm{CC}(K,\mathfrak{p})} (R_{\mathfrak{p}}(K') \cap L) \\ &= \bigcap_{\tau \in \mathrm{Gal}(K)} R_{\mathfrak{p}}(K_{\mathfrak{p}})^{\tau} \cap L. \end{aligned}$$

□

DEFINITION 4.1.6. If $R \subseteq S$ are rings, let

$$N_R(S) = \{f \in R[X] \colon f \text{ has no root in } S\}.$$

DEFINITION 4.1.7. Let the $\mathcal{L}_{\mathrm{ring}}(K)$-theory $T_{\mathrm{alg},S}$ consist of the following sentences:

(1) For each $f(X) \in N_K(K_{\mathrm{tot},S})$ the sentence
$$\neg(\exists x)(f(x) = 0).$$
(2) For each $\mathfrak{p} \in S$ and each $f(X) \in N_{\mathcal{O}_{\mathfrak{p}}}(R_{\mathfrak{p}}(K_{\mathrm{tot},S}))$ the sentence
$$\neg(\exists x)(\varphi_{\mathrm{holom},\mathfrak{p}}(x) \wedge f(x) = 0),$$
where $\varphi_{\mathrm{holom},\mathfrak{p}}$ is the formula of Proposition 2.4.2.

LEMMA 4.1.8. *A* P*S*CL *field $F \supseteq K$ is a model of $T_{\mathrm{alg},S}$ if and only if $F \cap \tilde{K} \subseteq K_{\mathrm{tot},S}$ and $F/F \cap \tilde{K}$ is totally S-adic.*

PROOF. Since F is PSCL, $\varphi_{\mathrm{holom},\mathfrak{p}}(F) = R_{\mathfrak{p}}(F)$ for each $\mathfrak{p} \in S$ by Proposition 2.4.2. Let $L = F \cap \tilde{K}$. Since L/K is algebraic, L is S-SAP by Lemma 2.8.5.

Suppose that F satisfies $T_{\mathrm{alg},S}$. By (1), $L \subseteq K_{\mathrm{tot},S}$. If $\mathfrak{p} \in S$, then $R_{\mathfrak{p}}(L) = R_{\mathfrak{p}}(K_{\mathrm{tot},S}) \cap L$ by Lemma 4.1.5, and (2) implies that $R_{\mathfrak{p}}(F) \cap \tilde{K} \subseteq R_{\mathfrak{p}}(K_{\mathrm{tot},S})$. Therefore, $R_{\mathfrak{p}}(F) \cap L \subseteq R_{\mathfrak{p}}(K_{\mathrm{tot},S}) \cap L = R_{\mathfrak{p}}(L)$, so F/L is totally S-adic by Lemma 2.9.6.

Conversely, suppose that $L \subseteq K_{\mathrm{tot},S}$ and F/L is totally S-adic. Since $L \subseteq K_{\mathrm{tot},S}$, F satisfies (1). By Lemma 2.9.6, $R_{\mathfrak{p}}(F) \cap L = R_{\mathfrak{p}}(L)$. So since $R_{\mathfrak{p}}(F) \cap L = R_{\mathfrak{p}}(F) \cap \tilde{K}$ and $R_{\mathfrak{p}}(L) = R_{\mathfrak{p}}(K_{\mathrm{tot},S}) \cap L$ by Lemma 4.1.5, F satisfies (2). □

4.2. Subfields of $K_{\mathrm{tot},S}$

We summarize some basic results on subfields of $K_{\mathrm{tot},S}$ and totally S-adic Galois extensions.

LEMMA 4.2.1. *Let $K \subseteq L \subseteq E \subseteq F$.*

(1) *If F/E and E/L are totally S-adic, then F/L is totally S-adic.*
(2) *If F/L is totally S-adic, then E/L is totally S-adic.*
(3) *If F/L is totally S-adic Galois, then F/E is totally S-adic.*

PROOF. Let $\mathfrak{p} \in S$.

PROOF OF (1). If $\mathcal{S}_{\mathfrak{p}}(F) \to \mathcal{S}_{\mathfrak{p}}(E)$ and $\mathcal{S}_{\mathfrak{p}}(E) \to \mathcal{S}_{\mathfrak{p}}(L)$ are surjective, then also the composition $\mathcal{S}_{\mathfrak{p}}(F) \to \mathcal{S}_{\mathfrak{p}}(L)$.

PROOF OF (2). Since the composition of $\mathcal{S}_{\mathfrak{p}}(F) \to \mathcal{S}_{\mathfrak{p}}(E)$ and $\mathcal{S}_{\mathfrak{p}}(E) \to \mathcal{S}_{\mathfrak{p}}(L)$ is surjective, $\mathcal{S}_{\mathfrak{p}}(E) \to \mathcal{S}_{\mathfrak{p}}(L)$ is surjective.

PROOF OF (3). Let $\mathfrak{P} \in \mathcal{S}_{\mathfrak{p}}(E)$. If $\mathrm{char}(\mathfrak{p}) = \infty$, then L is $\mathfrak{p}$-quasi-local, so Lemma 2.9.9(3) implies that $\mathrm{CC}(E, \mathfrak{p}) = \mathrm{CC}(F, \mathfrak{p})$. Hence, if $E' \in \mathrm{CC}(E, \mathfrak{P})$ and $\mathfrak{Q} \in \mathcal{S}_{\mathfrak{p}}(E')$, then $\mathfrak{Q}|_F \in \mathcal{S}_{\mathfrak{p}}(F)$ lies over $\mathfrak{P}$. If $\mathrm{char}(\mathfrak{p}) \neq \infty$, let $\mathfrak{Q}$ be any prime of F with $\mathfrak{Q}|_E = \mathfrak{P}$. Since F/L is totally S-adic, there exists $\mathfrak{Q}' \in \mathcal{S}_{\mathfrak{p}}(F)$ with $\mathfrak{Q}'|_L = \mathfrak{P}|_L$. Since F/L is Galois, $\mathfrak{Q}$ is conjugate to $\mathfrak{Q}'$ by Lemma 2.1.11. Hence, $\mathfrak{Q} \in \mathcal{S}_{\mathfrak{p}}(F)$, as claimed. □

The proof of the following lemma corrects an inaccuracy in [GJ02, Proof of Lemma 1.6 Part B].

LEMMA 4.2.2. *Let $K \subseteq E \subseteq F \subseteq K_{\mathrm{tot},S}$. If E is* P*S*CC*, then F is* P*S*CC*.*

PROOF. Let V be a smooth variety defined over F with $V(F') \neq \emptyset$ for all $F' \in \mathrm{CC}(F, S)$. Without loss of generality assume that V is affine.

Since F/E is algebraic, V is defined over a finite subextension F_0 of F/E. Let $W = \mathrm{res}_{F_0/E}(V)$ be the Weil restriction of V and let F_1 be the Galois closure of F_0/E. Then W is a variety defined over E and there are $\sigma_1, \dots, \sigma_n \in \mathrm{Gal}(E)$ with $\sigma_1 = \mathrm{id}_{\tilde{E}}$ such that W is isomorphic over F_1 to $\prod_{i=1}^n \sigma_i V$, and the projection onto the first factor $W \to \sigma_1 V = V$ is defined over F_0, cf. [FJ08, 10.6.2]. Since V is smooth, it follows that W is smooth, see [Lan58, Proposition VIII.6].

Since $E \subseteq F \subseteq K_{\mathrm{tot},S}$ and $E \subseteq F_1 \subseteq K_{\mathrm{tot},S}$, Lemma 4.1.3 and Lemma 2.9.9 imply that $\mathrm{CC}(E,S) = \mathrm{CC}(F,S) = \mathrm{CC}(F_1,S)$. In particular, if $E' \in \mathrm{CC}(E,S)$, then $F_1 \subseteq E'$.

Let $E' \in \mathrm{CC}(E,S)$. Then $\sigma_i^{-1}(E') \in \mathrm{CC}(E,S) = \mathrm{CC}(F,S)$, so $V(\sigma_i^{-1}(E')) \neq \emptyset$ by assumption. Thus $\sigma_i V(E') \neq \emptyset$ for all i, and therefore $W(E') \neq \emptyset$, as $F_1 \subseteq E'$. Since E is PSCC, $W(E) \neq \emptyset$, so in particular $W(F) \neq \emptyset$. Hence, since $F_0 \subseteq F$, it follows that $V(F) \neq \emptyset$, as claimed. □

Remark 4.2.3. Note that although every algebraic extension of a PRC field is PRC, cf. [Pre81], not every algebraic extension of a PpC field is PpC. For example, $\mathbb{Q}_p$ is PpC, but $\mathbb{Q}_p(\sqrt{p})$ is not. Hence, not every algebraic extension of a PSCC field is PSCC.

Lemma 4.2.4. *Let $K \subseteq F \subseteq M$. If M/F is totally S-adic Galois, then $\mathcal{S}_S(M)$ is the set of* all *primes of M lying over primes in $\mathcal{S}_S(F)$.*

Proof. By definition, $\mathcal{S}_S(M)$ is contained in the set of all primes of M lying over primes in $\mathcal{S}_S(F)$. Let $\mathfrak{P} \in \mathcal{S}_S(F)$ and let $\mathfrak{Q}$ be a prime of M lying over $\mathfrak{P}$. Since M/F is totally S-adic, there exists $\mathfrak{Q}' \in \mathcal{S}_S(M)$ with $\mathfrak{Q}'|_F = \mathfrak{P}$. Since M/F is Galois, $\mathfrak{Q}$ and $\mathfrak{Q}'$ are conjugate over F by Lemma 2.1.11, so $\mathfrak{Q} \in \mathcal{S}_S(M)$, as claimed. □

4.3. The Fields $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$

The proof of the decidability of the theory of almost all $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$ relies on two algebraic results, which we present in this section.

First of all recall that a field K is called **Hilbertian** if it satisfies the following property, cf. [FJ08, 13.2.2]. If $f(X,Y) \in K[X,Y]$ is irreducible, then there exists $a \in K$ such that $f(a,Y) \in K[Y]$ is irreducible.

Lemma 4.3.1. *Every number field and every function field is Hilbertian.*

Proof. See [FJ08, 13.4.2]. □

Definition 4.3.2. If

$$\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_e) \in \mathrm{Gal}(K)^e,$$

we denote by

$$\tilde{K}(\boldsymbol{\sigma})$$

the fixed field of the group $\langle \sigma_1, \ldots, \sigma_e \rangle \leq \mathrm{Gal}(K)$ in $\tilde{K}$, and by

$$\tilde{K}[\boldsymbol{\sigma}]$$

the maximal Galois extension of K in $\tilde{K}(\boldsymbol{\sigma})$. If L is a Galois extension of K, let $L(\boldsymbol{\sigma}) = L \cap \tilde{K}(\boldsymbol{\sigma})$ and $L[\boldsymbol{\sigma}] = L \cap \tilde{K}[\boldsymbol{\sigma}]$. In particular,

$$K_{\mathrm{tot},S}(\boldsymbol{\sigma}) = K_{\mathrm{tot},S} \cap \tilde{K}(\boldsymbol{\sigma})$$

and

$$K_{\mathrm{tot},S}[\boldsymbol{\sigma}] = K_{\mathrm{tot},S} \cap \tilde{K}[\boldsymbol{\sigma}].$$

Definition 4.3.3. We say that a statement holds for **almost all** $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ if the set of those $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ for which it holds has Haar measure 1.

Proposition 4.3.4 (Geyer-Jarden). *Let S be a finite set of local primes of a countable Hilbertian field K of characteristic zero, and let $e \in \mathbb{Z}_{\geq 0}$. Then for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, the field $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ is* PSCC.

Proof. By [GJ02, Theorem A], for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, $M = K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ is P$\mathcal{S}$CL, where $\mathcal{S}$ is the set of *all* primes of M lying over primes of S. By Lemma 4.1.3 and Lemma 4.2.1(2), M/K is a totally S-adic Galois extension, so $\mathcal{S} = \mathcal{S}_S(M)$ by Lemma 4.2.4. Hence, since M is S-quasi-local by Lemma 2.2.10, M is PSCC. □

Corollary 4.3.5. *Let S be a finite set of local primes of a countable Hilbertian field K of characteristic zero, and let $e \in \mathbb{Z}_{\geq 0}$. Then for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, the field $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$ is* PSCC.

Proof. Since $K \subseteq K_{\mathrm{tot},S}[\boldsymbol{\sigma}] \subseteq K_{\mathrm{tot},S}(\boldsymbol{\sigma}) \subseteq K_{\mathrm{tot},S}$, the corollary follows from the proposition by Lemma 4.2.2. □

Remark 4.3.6. The special case $S = \emptyset$ of the corollary was proven by Jarden, see [Jar69] and [Jar72]. The special case $S = \emptyset$ of the proposition was proven by Jarden in [Jar97]. The special case $e = 0$ and K a number field was proven by Moret-Bailly [MB89], Pop [Pop92], and Green-Pop-Roquette [GPR95]. Jarden-Razon proved the corollary in the case that K is a number field, see [JR98, Remark 8.3].

Proposition 4.3.7 (Haran-Jarden-Pop). *Let S be a finite set of local primes of a countable Hilbertian field K of characteristic zero, and let $e \in \mathbb{Z}_{\geq 0}$. Then for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, the S-adic absolute Galois group pile*

$$\mathbf{Gal}_S(K_{\mathrm{tot},S}(\boldsymbol{\sigma}))$$

is isomorphic to the deficient reduct of the e-free semi-constant group pile of $(\mathrm{Gal}(K_\mathfrak{p}))_{\mathfrak{p} \in S}$ over Cantor spaces $(C_\mathfrak{p})_{\mathfrak{p} \in S}$.

PROOF. This is proven in [HJP09b]. Indeed, by [HJP09b, Proposition 12.3], for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, the field $M = K_{\mathrm{tot},S}(\boldsymbol{\sigma})$ satisfies condition (1) of Section 10 of that work. In the proof of [HJP09b, Proposition 11.2] it is proven that in this case

$$\mathbf{Gal}(M,S) := (G, \mathrm{Gal}(\tilde{K}(\boldsymbol{\sigma}))^G, \mathcal{G}_{\mathfrak{p}})_{\mathfrak{p}\in S},$$

where $\mathbf{Gal}_S(M) = (G, \mathcal{G}_{\mathfrak{p}})_{\mathfrak{p}\in S}$, is a so called 'Cantor group pile over $(\mathrm{Gal}(K_{\mathfrak{p}}))_{\mathfrak{p}\in S}$'. By [HJP09b, Corollary 6.2] and [HJP09b, Proposition 6.3], every Cantor group pile over $(\mathrm{Gal}(K_{\mathfrak{p}}))_{\mathfrak{p}\in S}$ is isomorphic to the group pile $\mathbf{G}_T$ of [HJP09b, Proposition 5.3], which is exactly the e-free semi-constant group pile of $(\mathrm{Gal}(K_{\mathfrak{p}}))_{\mathfrak{p}\in S}$ over Cantor spaces $(C_{\mathfrak{p}})_{\mathfrak{p}\in S}$. Since the deficient reduct of $\mathbf{Gal}(M,S)$ is $\mathbf{Gal}_S(M)$, the claim follows. □

REMARK 4.3.8. The special case $S = \emptyset$ was proven by Jarden in [Jar74]. The special case $K = \mathbb{Q}$, $e = 0$ and $S = \{\infty\}$ was proven by Fried-Haran-Völklein, see [FHV93] and [FHV94]. The structure of the absolute Galois group in the special case where K is a number field and $e = 0$ was proven by Pop in [Pop96].

4.4. Axiomatization of the Theory of Almost All $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$

We axiomatize the theory of almost all $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$ and prove a classification result for the models of this theory: Two such models are elementarily equivalent if and only if their K-algebraic parts are isomorphic.

For the rest of this chapter, let S be a finite set of local primes of a countable Hilbertian field K of characteristic zero.

DEFINITION 4.4.1. Let the $\mathcal{L}_{\mathrm{ring}}(K)$-theory $T_{\mathrm{tot},S,e}$ consist of the following axioms:

(0) The axioms for fields and the positive diagram of K, cf. [FJ08, 7.3.1].
(1) The theory $T_{P\mathcal{S}\mathrm{CC}}$ (Definition 2.7.2).
(2) The theory $T_{\mathrm{C},S,e}$ (Definition 3.7.6).
(3) The theory $T_{\mathrm{alg},S}$ (Definition 4.1.7).

LEMMA 4.4.2. *A field $F \supseteq K$ is a model of $T_{\mathrm{tot},S,e}$ if and only if it satisfies the following conditions:*

(1) *F is* PSCC.
(2) *$\mathbf{Gal}_S(F)$ is an e-free C-pile.*
(3) *$F \cap \tilde{K} \subseteq K_{\mathrm{tot},S}$ and $F/F \cap \tilde{K}$ is totally S-adic.*

In that case, F satisfies also the following conditions:

(4) *F is* S-SAP.
(5) *F is S-quasi-local.*

PROOF. Suppose that $F \models T_{\mathrm{tot},S,e}$. Then F is PSCC by Proposition 2.7.3. Hence, Lemma 3.7.7 implies that $\mathbf{Gal}_S(F)$ is an e-free C-pile, Lemma 4.1.8 implies that $F \cap \tilde{K} \subseteq K_{\mathrm{tot},S}$ and $F/F \cap \tilde{K}$ is totally S-adic, Proposition 2.8.7 implies that F is S-SAP, and Proposition 2.2.11 implies that F is S-quasi-local.

Conversely, if F satisfies (1)-(3), then F satisfies Definition 4.4.1(1) by Proposition 2.7.3, Definition 4.4.1(2) by Lemma 3.7.7, and Definition 4.4.1(3) by Lemma 4.1.8. Since F is a field containing K, it also satisfies Definition 4.4.1(0). □

LEMMA 4.4.3. *Let $K \subseteq L \subseteq E, F$ be fields such that the following conditions are satisfied.*

(1) *E and F are models of $T_{\mathrm{tot},S,e}$.*
(2) *E/L and F/L are regular and totally S-adic.*
(3) *E is countable and F is $\aleph_1$-saturated.*
(4) *L is S-quasi-local.*

Then there exists an L-embedding $i\colon E \to F$ such that $F/i(E)$ is regular and totally S-adic.

PROOF. By (1) and Lemma 4.4.2(1), E and F are PSCC fields. Let $\mathbf{G} = \mathbf{Gal}_S(F)$, $\mathbf{B} = \mathbf{Gal}_S(E)$, and $\mathbf{A} = \mathbf{Gal}_S(L)$. By (1) and Lemma 4.4.2(2), $\mathbf{G}$ and $\mathbf{B}$ are e-free C-piles. By (2) and (4), it follows from Lemma 3.5.6 that the restriction maps $\mathrm{res}_{\tilde{F}/\tilde{L}}\colon \mathbf{G} \to \mathbf{A}$ and $\mathrm{res}_{\tilde{E}/\tilde{L}}\colon \mathbf{B} \to \mathbf{A}$ are rigid epimorphisms of group piles. So $(\mathrm{res}_{\tilde{F}/\tilde{L}}, \mathrm{res}_{\tilde{E}/\tilde{L}})$ is a rigid e-generated deficient embedding problem for $\mathbf{G}$.

By (3), E is countable, and thus $\mathbf{B}$ has countable rank, and F is $\aleph_1$-saturated. Hence, by Proposition 3.8.1 there exists an epimorphism $\gamma\colon \mathbf{G} \to \mathbf{B}$ such that $\mathrm{res}_{\tilde{E}/\tilde{L}} \circ \gamma = \mathrm{res}_{\tilde{F}/\tilde{L}}$. By Proposition 2.11.5, there is an L-embedding $i\colon E \to F$ such that $\gamma = \mathrm{res}_{\tilde{F}/\widetilde{i(E)}}$. By Lemma 4.4.2(5), E is S-quasi-local. Hence, since γ is an epimorphism of group piles, $F/i(E)$ is regular and totally S-adic by Lemma 3.5.6. □

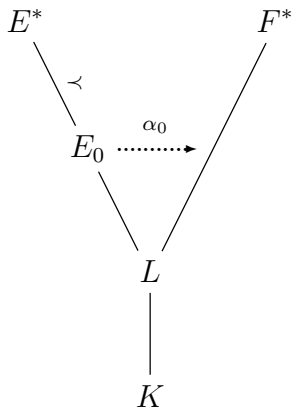
The proof of the following proposition follows the proof of [FJ08, 20.3.3].

PROPOSITION 4.4.4 (Elementary equivalence theorem). *Let $E, F \supseteq K$ be models of $T_{\mathrm{tot},S,e}$ with $E \cap \tilde{K} \cong_K F \cap \tilde{K}$. Then $E \equiv_K F$.*

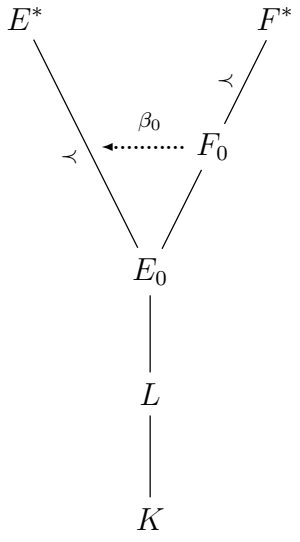
PROOF. Assume without loss of generality that $L := E \cap \tilde{K} = F \cap \tilde{K}$. By Lemma 4.4.2(3), E/L and F/L are regular and totally S-adic. Let E^* be an $\aleph_1$-saturated elementary extension of E and let F^* be an $\aleph_1$-saturated elementary extension of F, see for example [Mar02, 4.3.12].

By (1) and (4) of Lemma 4.4.2, the fields E, F, E^*, F^* are PSCC and S-SAP. By Corollary 2.9.7, E^*/E and F^*/F are regular and totally S-adic, so also E^*/L and F^*/L are regular and totally S-adic (Lemma 4.2.1(1)).

By Löwenheim-Skolem (Lemma 1.2.1), there exists a countable elementary subfield E_0 of E^* that contains L. Then also E_0/L is regular and totally S-adic (Lemma 4.2.1(2)), and E_0 is a model of $T_{\mathrm{tot},S,e}$. Since L/K is algebraic, L is S-quasi-local (Lemma 2.2.10). Therefore, by Lemma 4.4.3, there exists an L-embedding $\alpha_0\colon E_0 \to F^*$ with $F^*/\alpha_0(E_0)$ regular and totally S-adic.



Identify E_0 with $\alpha_0(E_0)$. Let F_0 be a countable elementary subfield of F^* that contains E_0. Then F_0/E_0 is regular and totally S-adic (Lemma 4.2.1(2)), and F_0 is a model of $T_{\mathrm{tot},S,e}$. Also E^*/E_0 is regular and totally S-adic by Corollary 2.9.7. By Lemma 4.4.2(5), E_0 is S-quasi-local. Hence, by Lemma 4.4.3, there is an E_0-embedding $\beta_0\colon F_0 \to E^*$ with $E^*/\beta_0(F_0)$ regular and totally S-adic.



Now iterate this process to construct a tower of countable fields

$$E_0 \subseteq F_0 \subseteq E_1 \subseteq F_1 \subseteq \dots$$

such that each E_i is an elementary subfield of E^* and each F_i is an elementary subfield of F^*. Then $M := \bigcup_{i\in\mathbb{N}} E_i = \bigcup_{i\in\mathbb{N}} F_i$ is an elementary subfield of both E^* and F^*, see for example [FJ08, 7.4.1(b)], so $E^* \equiv_M F^*$. In particular, $E^* \equiv_K F^*$, hence $E \equiv_K F$. □

Proposition 4.4.5. *Let $e < \omega$. Then for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$ is a model of $T_{\mathrm{tot},S,e}$.*

Proof. By Corollary 4.3.5, almost all $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$ are PSCC. By Proposition 4.3.7, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, $\mathbf{Gal}_S(K_{\mathrm{tot},S}(\boldsymbol{\sigma}))$ is isomorphic to the deficient reduct of the e-free semi-constant group pile of $(\mathrm{Gal}(K_\mathfrak{p}))_{\mathfrak{p}\in S}$ over Cantor spaces $(C_\mathfrak{p})_{\mathfrak{p}\in S}$. Since a Cantor space is perfect, this is an e-free C-pile by Proposition 3.6.3. Therefore, since $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$ is a field containing K, almost all $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$ are models of $T_{\mathrm{tot},S,e}$ by Lemma 4.4.2. □

Lemma 4.4.6. *Let $e < \omega$. If $F \supseteq K$ is a model of $T_{\mathrm{tot},S,e}$, then $L = F \cap \tilde{K} \subseteq K_{\mathrm{tot},S}$ and $\mathrm{rank}(\mathrm{Gal}(K_{\mathrm{tot},S}/L)) \leq e$.*

Proof. Let $\mathbf{G} = \mathbf{Gal}_S(F)$, and $\mathbf{A} = \mathbf{Gal}_S(L)$. By Lemma 4.4.2(3), $L \subseteq K_{\mathrm{tot},S}$ and F/L is totally S-adic. Since L/K is algebraic, L is S-quasi-local by Lemma 2.2.10, so the restriction $\mathbf{G} \to \mathbf{A}$ is an epimorphism of group piles by Lemma 3.5.6. By Lemma 4.4.2(2), $\mathbf{G}$ is an e-free C-pile. In particular, it is e-generated. Thus, by Lemma 3.1.19, also $\mathbf{A}$ is e-generated. Since $K_{\mathrm{tot},S}/K$ is totally S-adic Galois by Lemma 4.1.3, $\mathrm{CC}(L,S) = \mathrm{CC}(K_{\mathrm{tot},S},S)$ by Lemma 2.9.9(3). Thus, $\mathbf{A}' = \mathbf{Gal}_S(K_{\mathrm{tot},S})'$. But $\mathbf{Gal}_S(K_{\mathrm{tot},S})$ is self-generated (this follows from the definition of $K_{\mathrm{tot},S}$, or from Proposition 4.3.7), so $\mathbf{A}' = \mathbf{Gal}_S(K_{\mathrm{tot},S})$. Therefore, $\mathrm{Gal}(K_{\mathrm{tot},S}/L) = A/A' = \bar{A}$ is generated by e elements. □

Definition 4.4.7. If $e < \omega$, let

$$T_{\mathrm{almost},S,e}$$

denote the set of all $\mathcal{L}_{\mathrm{ring}}(K)$-sentences that are true in almost all fields $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$, $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$.

The proof of the following result follows the proof of [FJ08, 20.5.4].

Theorem 4.4.8. *If $e < \omega$, then the theory $T_{\mathrm{tot},S,e}$ is an axiomatization of $T_{\mathrm{almost},S,e}$, i.e. these two theories have the same models.*

Proof. First note that every model of $T_{\mathrm{almost},S,e}$ is a field containing K. By Definition 4.4.1(0), the same holds for every model of $T_{\mathrm{tot},S,e}$.

By Proposition 4.4.5, almost all $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$ satisfy $T_{\mathrm{tot},S,e}$, so every model of $T_{\mathrm{almost},S,e}$ is a model of $T_{\mathrm{tot},S,e}$.

Conversely, let E be a model of $T_{\mathrm{tot},S,e}$ and let $L = E \cap \tilde{K}$. If we can construct a model F of $T_{\mathrm{almost},S,e}$ with $F \cap \tilde{K} \cong_K L$, then $E \equiv_K F$ by Proposition 4.4.4, so E is a model of $T_{\mathrm{almost},S,e}$ and we are done.

Lemma 4.4.6 implies that $L \subseteq K_{\mathrm{tot},S}$ and there exist $\tau_1, \dots, \tau_e \in \mathrm{Gal}(K_{\mathrm{tot},S}/K)$ that generate $\mathrm{Gal}(K_{\mathrm{tot},S}/L)$. Let $\mathcal{N}$ be the set of finite Galois extensions of K inside $K_{\mathrm{tot},S}$. For each $N \in \mathcal{N}$, the set

$$\begin{aligned}\Sigma(N) &:= \{\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \colon \mathrm{res}_N(\sigma_i) = \mathrm{res}_N(\tau_i),\ i = 1, \dots, e\} \\ &\subseteq \{\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \colon K_{\mathrm{tot},S}(\boldsymbol{\sigma}) \cap N \cong_K L \cap N\}\end{aligned}$$

has positive Haar measure. If $N_1, \dots, N_r \in \mathcal{N}$, then $N_1 \cdots N_r \in \mathcal{N}$ and $\Sigma(N_1) \cap \cdots \cap \Sigma(N_r) = \Sigma(N_1 \cdots N_r)$. Hence, by [FJ08, 7.6.1], there exists an ultrafilter $\mathcal{D}$ on $\mathrm{Gal}(K)^e$ which contains each of the sets $\Sigma(N)$, $N \in \mathcal{N}$, and all sets of measure 1. Let

$$F = \prod_{\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e} K_{\mathrm{tot},S}(\boldsymbol{\sigma})/\mathcal{D}$$

be the ultraproduct, and let $M = F \cap \tilde{K}$. Since $\mathcal{D}$ contains all sets of measure 1, and almost all $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$ are models of $T_{\mathrm{almost},S,e}$, F is a model of $T_{\mathrm{almost},S,e}$ by Lemma 1.2.2. Furthermore, $M \subseteq K_{\mathrm{tot},S}$, and $M \cap N \cong L \cap N$ for each $N \in \mathcal{N}$, since $\mathcal{D}$ contains $\Sigma(N)$. Therefore, $M \cong_K L$, see for example [FJ08, 20.6.3], as claimed. □

Remark 4.4.9. Note that the theory $T_{\mathrm{almost},S,e}$ of almost all $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$, $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, is not complete if $e > 0$. Therefore, the decidability of this theory does not immediately follow from the existence of a recursive axiomatization.

4.5. Recursive Primes

In order to use the axiomatization of $T_{\mathrm{almost},S,e}$ in the proof of its decidability, we have to show that this axiomatization is recursive. For this purpose, we make some recursivity assumptions, and show that they are fulfilled for number fields.

Definition 4.5.1. A prime $\mathfrak{p}$ of a presented field $\rho\colon K \to \mathbb{N}$ is **recursive** if the set $\rho(\mathcal{O}_\mathfrak{p}) \subseteq \mathbb{N}$ is recursive.

Definition 4.5.2. Let $K/\mathbb{Q}$ be a number field of degree n. For the rest of this work, we fix a presentation $\rho\colon K \to \mathbb{N}$ as follows: Let $K = \mathbb{Q}(\alpha)$, where α is a root of a polynomial $f(X) \in \mathbb{Z}[X]$ of degree n. Then $K = \sum_{i=1}^n \mathbb{Q}\alpha^i$, and we present K as

$$\rho\colon K = \mathbb{Q}^n \hookrightarrow \mathbb{N}^{2n} \hookrightarrow \mathbb{N}$$

via iterated application of a recursive pairing function $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

LEMMA 4.5.3. *Every prime of a number field is recursive.*

PROOF. Let $\mathfrak{p}$ be a prime of a number field K of degree n, and let f and α be as in Definition 4.5.2.

PART A: CASE $\mathrm{char}(\mathfrak{p}) = \infty$. The orderings of K correspond to embedding $K \hookrightarrow \mathbb{R}$, so $\mathfrak{p}$ is determined by a specific root a of f in $\mathbb{R}$. Let $c, d \in \mathbb{Q}$ such that a is the only root of f in the interval $[c, d] \subseteq \mathbb{R}$. Let $\varphi(x_1, \ldots, x_n)$ be the $\mathcal{L}_{\leq}$-formula

$$(\exists x)(f(x) = 0 \wedge c \leq x \wedge x \leq d \wedge \sum_{i=1}^{n} x_i x^i \geq 0).$$

Then for $a_1, \ldots, a_n \in \mathbb{Q}$, $\sum_{i=1}^{n} a_i \alpha^i \in \mathcal{O}_{\mathfrak{p}}$ if and only if $(\mathbb{R}, \leq) \models \varphi(\mathbf{a})$. Note that since $a_1, \ldots, a_n \in \mathbb{Q}$, $\varphi(\mathbf{a})$ can be seen as an $\mathcal{L}_{\leq}$-sentence. Thus, since $(\mathbb{R}, \leq)$ is decidable by Proposition 1.4.5, the subset $\mathcal{O}_{\mathfrak{p}} \subseteq \mathbb{Q}^n$ is recursive, as claimed.

PART B: CASE $\mathrm{char}(\mathfrak{p}) = p \neq \infty$. Each of the n roots $\alpha_1, \ldots, \alpha_n$ of f in $\tilde{\mathbb{Q}}_p$ defines an embedding σ_i of K into $\tilde{\mathbb{Q}}_p$, and thereby induces a p-valuation on K. Two such embeddings σ_i, σ_j induce the same p-valuation on K if and only if α_i and α_j are conjugate over $\hat{\mathbb{Q}}_p$. This follows for example from [Lan94, II§1 Theorem 2].

Thus, if $f_1, \ldots, f_r \in \mathbb{Q}_p[X]$ are the irreducible factors of f over $\mathbb{Q}_p$, then these irreducible factors correspond to the p-valuations on K.[1] Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, for every i we can find a good approximation $\tilde{f}_i \in \mathbb{Q}[X]$ of f_i. This approximation can be chosen such that if the coefficients of some $\tilde{f}_j$ are close enough to the coefficients of $\tilde{f}_i$, then $i = j$. Assume without loss of generality that $\mathfrak{p}$ corresponds to $f_1(X) = \sum_{k=0}^{m} c_i X^i$. Using the approximation $\tilde{f}_1$ of f_1, the coefficients of f_1 can be defined in $\mathbb{Q}_p$. Therefore, the field $\mathbb{Q}_p[X]/(f_1(X)) \cong K_{\mathfrak{p}}$ can be interpreted in $\mathbb{Q}_p$. More precisely, the $\mathcal{L}_R(c)$-structure $\mathcal{M} = (K_{\mathfrak{p}}, +, -, \cdot, 0, 1, R_{\mathfrak{p}}(K_{\mathfrak{p}}), c)$, where c is the residue of X in $\mathbb{Q}_p[X]/(f_1(X))$, can be interpreted in $\mathbb{Q}_p$ without parameters. Hence, the complete $\mathcal{L}_R(c)$-theory of $\mathcal{M}$ is decidable since the complete $\mathcal{L}_R$-theory of $\mathbb{Q}_p$ is decidable (Proposition 1.6.3). Now let $\varphi(x_1, \ldots, x_n)$ be the $\mathcal{L}_R(c)$-formula

$$\sum_{i=1}^{n} x_i c^i \in R.$$

Then for $a_1, \ldots, a_n \in \mathbb{Q}$, $\sum_{i=1}^{n} a_i \alpha^i \in \mathcal{O}_{\mathfrak{p}}$ if and only if $\mathcal{M} \models \varphi(\mathbf{a})$. Therefore, $\mathcal{O}_{\mathfrak{p}}$ is recursive, as above. □

[1] Note that we do not have to prove that this factorization can be effectively computed. But it would be possible, of course.

REMARK 4.5.4. Note that the statement of Lemma 4.5.3 cannot even be generalized to local primes of finitely generated fields. For example, the presentable rational function field $\mathbb{Q}(X)$ has $2^{\aleph_0}$ many archimedean local primes, corresponding to the embeddings of $\mathbb{Q}(X)$ into $\mathbb{R}$, but only countably many of these primes can be recursive.

REMARK 4.5.5. Note that the non-archimedean case of Lemma 4.5.3 immediately follows from the well known fact that if $\mathfrak{p}$ is a non-archimedean prime of a global field K, then $\mathcal{O}_\mathfrak{p}$ is Diophantine in K, cf. [Shl07, 4.2.4, 4.3.4]. Indeed, every Diophantine set is recursively enumerable, and since for $x \in K^\times$, $\mathcal{O}_\mathfrak{p}$ satisfies $x \in \mathcal{O}_\mathfrak{p}$ or $x^{-1} \in \mathcal{O}_\mathfrak{p}$, this already implies that $\mathcal{O}_\mathfrak{p}$ is recursive. Similarly, if $\mathfrak{p}$ is an archimedean prime of a number field K, then $\mathcal{O}_\mathfrak{p}$ is Diophantine in K, see for example [Rum80, p. 212], and this implies that $\mathcal{O}_\mathfrak{p}$ is recursive.

For the rest of this chapter, let S be a finite set of recursive local primes of a presented countable Hilbertian field K of characteristic zero.

LEMMA 4.5.6. *Let $\mathfrak{p} \in S$. Then the following sets of polynomials are recursive:*

(1) $\{f \in K[X] \colon f$ *completely decomposes over* $K_{\mathrm{tot},S}\}$
(2) $\{f \in \mathcal{O}_\mathfrak{p}[X] \colon f$ *completely decomposes over* $R_\mathfrak{p}(K_{\mathrm{tot},S})\}$

PROOF.

PROOF OF (1). A polynomial $f \in K[X]$ completely decomposes over $K_{\mathrm{tot},S}$ if and only if it completely decomposes over $K_\mathfrak{p}$ for every $\mathfrak{p} \in S$. Let $\varphi_n(x_0, \dots, x_n)$ be the $\mathcal{L}_{\mathrm{ring}}$-formula

$$(\exists y_1, \dots, y_n) \bigwedge_{k=0}^{n} (x_k = s_k(\mathbf{y}) x_n),$$

where $s_0, \dots, s_n \in \mathbb{Z}[\mathbf{y}]$ are the elementary symmetric polynomials in $\mathbf{y}$ defined by

$$\sum_{k=0}^{n} s_k(\mathbf{y}) X^k = \prod_{i=1}^{n} (X - y_i).$$

A polynomial $f(X) = \sum_{k=0}^{n} a_k X^k \in K[X]$ of degree n completely decomposes over $K_\mathfrak{p}$ if and only if $K_\mathfrak{p} \models \varphi_n(\mathbf{a})$.

PART 1A: CASE $\mathrm{char}(\mathfrak{p}) = \infty$. Since the theory of real closed fields has quantifier elimination in the language of ordered fields (Proposition 1.4.5), there exists a quantifier free $\mathcal{L}_R$-formula $\psi_n(\mathbf{x})$ such that

$$(K_\mathfrak{p}, R_\mathfrak{p}(K_\mathfrak{p})) \models (\forall \mathbf{a})(\varphi_n(\mathbf{a}) \leftrightarrow \psi_n(\mathbf{a})).$$

Since the theory of real closed ordered fields is decidable by Proposition 1.4.5, this formula ψ_n can be effectively computed. If $a_0, \dots, a_n \in K$, then $(K_\mathfrak{p}, R_\mathfrak{p}(K_\mathfrak{p})) \models \psi_n(\mathbf{a})$ if and only if $(K, \mathcal{O}_\mathfrak{p}) \models \psi_n(\mathbf{a})$. Since

$(K, \mathcal{O}_\mathfrak{p})$ is recursive by assumption, there is an algorithm to decide if $(K, \mathcal{O}_\mathfrak{p}) \models \psi_n(\mathbf{a})$. Therefore, there is an algorithm to decide if a polynomial $f \in K[X]$ completely decomposes over $K_\mathfrak{p}$.

PART 1B: CASE $\mathrm{char}(\mathfrak{p}) = p \neq \infty$. The theory of p-adically closed fields of a fixed p-rank d has quantifier elimination in the extended language $\mathcal{L}_{P,d}$ (Proposition 1.6.3). Thus, arguing as in the case $\mathrm{char}(\mathfrak{p}) = \infty$, we can decide if a polynomial f completely decomposes over $K_\mathfrak{p}$ if we can decide, for a given $a \in K$, whether or not $K_\mathfrak{p} \models P_m(a)$, i.e. whether a is an m-th power in $K_\mathfrak{p}$. By Lemma 2.6.3, there exist quantifier free formulas $\varphi_m(x, y)$ and $\psi_m(x, y)$ such that a is an m-th power in $K_\mathfrak{p}$ if and only if $(K, \mathcal{O}_\mathfrak{p}) \models (\forall y)(\psi_m(a, y))$, if and only if $(K, \mathcal{O}_\mathfrak{p}) \not\models (\forall y)(\varphi_m(a, y))$. Therefore, the following is an algorithm to determine whether a is an m-th power in $K_\mathfrak{p}$:

List the elements of K as $b_1, b_2, b_3, \ldots$ and check for each i whether $(K, \mathcal{O}_\mathfrak{p}) \models \varphi_m(a, b_i)$ and $(K, \mathcal{O}_\mathfrak{p}) \models \psi_m(a, b_i)$. Then for some i either $(K, \mathcal{O}_\mathfrak{p}) \not\models \varphi_m(a, b_i)$ or $(K, \mathcal{O}_\mathfrak{p}) \not\models \psi_m(a, b_i)$. In the former case, a is an m-th power, in the second case a is not an m-th power in $K_\mathfrak{p}$.

PROOF OF (2). By Lemma 4.1.5, a polynomial $f \in K[X]$ completely decomposes over $R_\mathfrak{p}(K_{\mathrm{tot},S})$ if and only if it completely decomposes over $R_\mathfrak{p}(K_\mathfrak{p})$ and over $K_{\mathrm{tot},S}$. By (1), we can effectively decide if f completely decomposes over $K_{\mathrm{tot},S}$. If we replace $\varphi_n(x_0, \ldots, x_n)$ by the $\mathcal{L}_R$-formula

$$(\exists y_1, \ldots, y_n)(\bigwedge_{i=1}^{n} R(y_i) \wedge \bigwedge_{k=0}^{n} (x_k = s_k(\mathbf{y})x_n)),$$

then a polynomial $f(X) = \sum_{k=0}^{n} a_k X^k \in \mathcal{O}_\mathfrak{p}[X]$ of degree n completely decomposes over $R_\mathfrak{p}(K_\mathfrak{p})$ if and only if $(K_\mathfrak{p}, R_\mathfrak{p}(K_\mathfrak{p})) \models \varphi_n(\mathbf{a})$, and the proof of (1) carries over to this case. □

We remind the reader that $N_R(S)$ denotes the set of all polynomials $f \in R[X]$ without a root in S (Definition 4.1.6).

LEMMA 4.5.7. *If K has a splitting algorithm, then the sets $N_K(K_{\mathrm{tot},S})$ and $N_{\mathcal{O}_\mathfrak{p}}(R_\mathfrak{p}(K_{\mathrm{tot},S}))$, $\mathfrak{p} \in S$, are recursive.*

PROOF. Let $f \in K[X]$ be given. Use the splitting algorithm of K to recursively decompose f into irreducible factors $f_1, \ldots, f_r \in K[X]$. Since $K_{\mathrm{tot},S}/K$ is Galois, each of these irreducible polynomials f_i has a root in $K_{\mathrm{tot},S}$ if and only if it completely decomposes over $K_{\mathrm{tot},S}$. Thus, $f \in N_K(K_{\mathrm{tot},S})$ if and only if none of the factors f_i lies in the recursive set of polynomials of Lemma 4.5.6(1). Therefore, $N_K(K_{\mathrm{tot},S})$ is recursive. Similarly, using Lemma 4.5.6(2) and Lemma 4.1.5, one sees that $N_{\mathcal{O}_\mathfrak{p}}(R_\mathfrak{p}(K_{\mathrm{tot},S}))$ is recursive. □

LEMMA 4.5.8. *If K has a splitting algorithm, then the theory $T_{\mathrm{tot},S,e}$ (Definition 4.4.1) is recursive.*

PROOF. Since K is a presented field, the positive diagram of K is recursive.

The theory $T_{\mathrm{holom},\mathfrak{p}}$ (Definition 2.4.6) is recursive. Indeed, the axioms of (1), (3), (4), and (5) consist only of finitely many sentences, so there is nothing to prove, and the set of formulas $\varphi_{\mathrm{holom},\mathfrak{p}}(a)$, $a \in \mathcal{O}_{\mathfrak{p}}$, is recursive since $\mathcal{O}_{\mathfrak{p}}$ is recursive by assumption. So, since the map $\psi \mapsto \hat{\psi}_{\mathfrak{p},\forall}$ of Proposition 2.6.6 is recursive, the theory $T_{\mathrm{P}SCC}$ (Definition 2.7.2) is recursive.

The theory $T_{\mathrm{C},S,e}$ (Definition 3.7.6) is recursive since the maps $\mathbf{A} \mapsto \theta_{\mathrm{realize},\mathbf{A}}$ and $\alpha \mapsto \theta_{\mathrm{res},\alpha}$ are recursive (Lemma 3.7.4 and Lemma 3.7.5), and one can recursively determine if a given finite group pile is e-generated or deficient.

Since K has a splitting algorithm, Lemma 4.5.7 implies that the sets $N_K(K_{\mathrm{tot},S})$ and $N_{\mathcal{O}_{\mathfrak{p}}}(R_{\mathfrak{p}}(K_{\mathrm{tot},S}))$ are recursive. Thus, the theory $T_{\mathrm{alg},S}$ (Definition 4.1.7) is recursive. □

4.6. Decidability of the Theory of Almost All $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$

Now that we have a recursive axiomatization of the theory of almost all $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$, we can prove that the theory of almost all $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$ is decidable. The proof follows closely the proof of Jarden-Kiehne in [FJ08, Chapter 20.6] that the theory of almost all $\tilde{K}(\boldsymbol{\sigma})$ is decidable.

DEFINITION 4.6.1. The set of **test sentences** is the smallest set of $\mathcal{L}_{\mathrm{ring}}(K)$-sentences that contains all of the sentences of the form

$$(\exists X)(f(X) = 0),$$

where $f \in K[X]$ is a polynomial that completely decomposes over $K_{\mathrm{tot},S}$, and is closed under negations, conjunctions, and disjunctions.

LEMMA 4.6.2. *Let $E, F \supseteq K$ be models of $T_{\mathrm{tot},S,e}$. Then $E \equiv_K F$ if and only if E and F satisfy the same test sentences.*

PROOF. Trivially, if E and F are elementarily equivalent over K, then they satisfy the same test sentences. Conversely, assume that E and F satisfy the same test sentences, and let $E_0 = E \cap \tilde{K}$ and $F_0 = F \cap \tilde{K}$. By Lemma 4.4.2(3), $E_0 \subseteq K_{\mathrm{tot},S}$ and $F_0 \subseteq K_{\mathrm{tot},S}$. Let $f \in K[X]$ be an irreducible polynomial. If f does not completely decompose over $K_{\mathrm{tot},S}$, then it has no root in $K_{\mathrm{tot},S}$, so it has no root in E_0 and it has no root in F_0. If f completely decomposes over $K_{\mathrm{tot},S}$, then $(\exists X)(f(X) = 0)$ is a test sentence. Hence, f has a root in E_0 if and only if it has a root in F_0. Therefore, $E_0 \cong_K F_0$, see for example [FJ08, 20.6.3]. By Proposition 4.4.4, $E \equiv_K F$. □

LEMMA 4.6.3. *The set of test sentences is recursive.*

PROOF. Given a polynomial $f \in K[X]$, one can decide if $(\exists X)(f(X) = 0)$ is a test sentence or not by Lemma 4.5.6(1). Induction on the structure of formulas then shows that the set of test sentences is recursive. □

For the rest of this chapter, let S be a finite set of recursive local primes of a presented countable Hilbertian field K of characteristic zero with a splitting algorithm, and let $e < \omega$.

DEFINITION 4.6.4. For each $\mathcal{L}_{\mathrm{ring}}(K)$-sentence θ let

$$\Sigma_{S,e}(\theta) = \{\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \colon K_{\mathrm{tot},S}(\boldsymbol{\sigma}) \models \theta\}$$

be the **truth set** of θ.

NOTATION 4.6.5. We denote the normalized Haar measure on $\mathrm{Gal}(K)^e$ by μ, cf. Section 1.3.

LEMMA 4.6.6. *Let λ be a test sentence. Then $\Sigma_{S,e}(\lambda)$ is open-closed in $\mathrm{Gal}(K)^e$ and $\mu(\Sigma_{S,e}(\lambda))$ is a rational number. The map $\lambda \mapsto \mu(\Sigma_{S,e}(\lambda))$ from test sentences to $\mathbb{Q}$ is recursive.*

PROOF. Let $f_1, \ldots, f_n \in K[X]$ be the polynomials occurring in λ. Their splitting field L_λ is a finite Galois extension of K inside $K_{\mathrm{tot},S}$. Let L/K be a Galois extension with $L_\lambda \subseteq L \subseteq K_{\mathrm{tot},S}$. Then $K_{\mathrm{tot},S}(\boldsymbol{\sigma}) \cap L = L(\mathrm{res}_L(\boldsymbol{\sigma}))$ for each $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$. Let

$$\Sigma_{L,\lambda} = \{\boldsymbol{\tau} \in \mathrm{Gal}(L/K)^e \colon L(\boldsymbol{\tau}) \models \lambda\}\,.$$

We claim that

$$\Sigma_{S,e}(\lambda) = \{\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \colon \mathrm{res}_L(\boldsymbol{\sigma}) \in \Sigma_{L,\lambda}\}.$$

Indeed, if λ is of the form $(\exists X)(f(X) = 0)$, where $f \in K[X]$ completely decomposes over $K_{\mathrm{tot},S}$, then

$$\Sigma_{L,\lambda} = \{\boldsymbol{\tau} \in \mathrm{Gal}(L/K)^e \colon f \text{ has a zero in } L(\boldsymbol{\tau})\}.$$

Since L contains all roots of f, $K_{\mathrm{tot},S}(\boldsymbol{\sigma}) \models \lambda$ if and only if $K_{\mathrm{tot},S}(\boldsymbol{\sigma}) \cap L \models \lambda$, so the claim is true in that case. Induction on the structure of λ shows that the claim holds for all test sentences λ.

Thus, $\Sigma_{S,e}(\lambda)$ is open-closed, in particular measurable. Furthermore,

$$\mu(\Sigma_{S,e}(\lambda)) = \frac{|\Sigma_{L_\lambda,\lambda}|}{[L_\lambda : K]^e}$$

is a rational number, and this number is computable since K has a splitting algorithm, see for example [FJ08, 19.3.2]. □

THEOREM 4.6.7. *Let S be a finite set of recursive local primes of a presented countable Hilbertian field K of characteristic zero with a splitting algorithm, and let $e \in \mathbb{Z}_{\geq 0}$. Then the following holds:*

(1) *For every $\mathcal{L}_{\mathrm{ring}}(K)$-sentence θ, $\Sigma_{S,e}(\theta)$ is μ-measurable, and $\mu(\Sigma_{S,e}(\theta))$ is a rational number.*
(2) *The map $\theta \mapsto \mu(\Sigma_{S,e}(\theta))$ from $\mathcal{L}_{\mathrm{ring}}(K)$-sentences to $\mathbb{Q}$ is recursive.*

In particular, the theory $T_{\mathrm{almost},S,e}$ of almost all fields $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$, $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, is decidable.

PROOF. By Theorem 4.4.8, $T_{\mathrm{tot},S,e} \models T_{\mathrm{almost},S,e}$ and $T_{\mathrm{almost},S,e} \models T_{\mathrm{tot},S,e}$. By Lemma 4.6.2 and [FJ08, 7.8.2], for every $\mathcal{L}_{\mathrm{ring}}(K)$-sentence θ there exists a test sentence λ such that the sentence $\theta \leftrightarrow \lambda$ is in $T_{\mathrm{almost},S,e}$. In particular, $\Sigma_{S,e}(\theta)$ and $\Sigma_{S,e}(\lambda)$ differ only by a zero set. Lemma 4.6.6 implies that $\Sigma_{S,e}(\lambda)$ is μ-measurable and $\mu(\Sigma_{S,e}(\lambda)) \in \mathbb{Q}$, so also $\Sigma_{S,e}(\theta)$ is μ-measurable and $\mu(\Sigma_{S,e}(\theta)) = \mu(\Sigma_{S,e}(\lambda)) \in \mathbb{Q}$. This proves (1).

Since $T_{\mathrm{tot},S,e} \models T_{\mathrm{almost},S,e}$, we have $T_{\mathrm{tot},S,e} \models \theta \leftrightarrow \lambda$. The set of test sentences is recursive by Lemma 4.6.3. By Lemma 4.5.8, the theory $T_{\mathrm{tot},S,e}$ is recursive, so the set of consequences of $T_{\mathrm{tot},S,e}$ is recursively enumerable, cf. [Mar02, 2.1.1, 2.1.2]. Therefore, there is a recursive map $\theta \mapsto \lambda_\theta$ from $\mathcal{L}_{\mathrm{ring}}(K)$-sentences to test sentences such that for every θ, $\theta \leftrightarrow \lambda_\theta$ is in $T_{\mathrm{almost},S,e}$. In particular, $\mu(\Sigma_{S,e}(\theta)) = \mu(\Sigma_{S,e}(\lambda_\theta))$.

Since also the map $\lambda \mapsto \mu(\Sigma_{S,e}(\lambda))$ from test sentences to $\mathbb{Q}$ is recursive by Lemma 4.6.6, the composition

$$\theta \mapsto \lambda_\theta \mapsto \mu(\Sigma_{S,e}(\lambda_\theta)) = \mu(\Sigma_{S,e}(\theta))$$

is recursive. This proves (2).

Since $T_{\mathrm{almost},S,e}$ is the set of all θ with $\mu(\Sigma_{S,e}(\theta)) = 1$, it follows that $T_{\mathrm{almost},S,e}$ is decidable. □

REMARK 4.6.8. Note that the assumption that the primes in S are recursive is *necessary*. Indeed, we have shown that $R_{\mathfrak{p}}(K_{\mathrm{tot},S})$ is K-definable in $K_{\mathrm{tot},S}$ for each $\mathfrak{p} \in S$. An element $x \in K$ lies in $\mathcal{O}_{\mathfrak{p}}$ if and only if $x \in R_{\mathfrak{p}}(K_{\mathrm{tot},S})$, so the decidability of the complete $\mathcal{L}_{\mathrm{ring}}(K)$-theory of $K_{\mathrm{tot},S}$ implies that $\mathcal{O}_{\mathfrak{p}}$ is recursive.

On the other hand we do not know whether the assumption that K has a splitting algorithm is necessary.

The theorem does certainly not hold anymore if we allow S to be an arbitrary (possibly infinite) set of recursive local primes of K. In fact, although there exist trivial examples of Hilbertian fields K with an infinite set of local primes S such that $K_{\mathrm{tot},S}$ is decidable, we do not know any infinite set of primes S of $K = \mathbb{Q}$ for which the theorem holds. Moreover, [Jar95, Example 10.4] gives an example of an infinite set of primes S of $\mathbb{Q}$ *that has Dirichlet density zero*, but $\mathbb{Q}_{\mathrm{tot},S} = \mathbb{Q}$, hence $T_{\mathrm{almost},S,e} = \mathrm{Th}(\mathbb{Q})$ is undecidable.

COROLLARY 4.6.9. *Let S be a finite set of primes of a number field K, and let $e \in \mathbb{Z}_{\geq 0}$. Then the theory of almost all fields $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$, $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, is decidable.*

PROOF. Every number field is Hilbertian by Lemma 4.3.1, and countable. Moreover, every prime of a number field is local (Remark 2.1.19) and recursive by Lemma 4.5.3. By [FJ08, 19.1.3(b), 19.2.4], every number field has a splitting algorithm. Thus, the claim follows from Theorem 4.6.7. □

This finally proves Theorem I from the introduction.

REMARK 4.6.10. As mentioned in the introduction, Theorem I has as special cases decidability results from [JK75], [FHV94] and [Ers96b]. The following decidability results for algebraic fields are related, but do not follow from Theorem I: In [HL94], decidability is proven for theories of fields of the form $\mathbb{R}_{\mathrm{alg}}(\boldsymbol{\sigma})$, and in [Efr91] for fields of the form $\mathbb{Q}_p(\boldsymbol{\sigma})$.

In the light of Theorem 4.4.8, Theorem I gives decidability of the theory of a certain class of PSCC fields. For PRC and PpC fields, many such theories were proven decidable, see for example [Kün89b] and the references there. However, the undecidability results of [Har84] and [Efr92] for the theories of formally real PRC fields and formally p-adic PpC fields put a bound on such decidability results.

CHAPTER 5

Decidability of Almost All $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$

In this chapter we show how the proof of the decidability of almost all $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$ carries over to the fields $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$. However, we restrict ourselves to the case that K is a number field.

For the rest of this work, let S be a finite set of primes of a number field K, and let $0 < e < \omega$ be a positive integer.

Note that every number field is countable Hilbertian and has a splitting algorithm, and every prime of a number field is local and recursive, cf. the proof of Corollary 4.6.9.

5.1. Subgroups of Strongly Projective Groups

We will apply a result of Pop on prosolvable subgroups of 'strongly $\mathcal{G}$-projective' groups to our semi-constant group piles. To state this result, we need the following definitions from [Pop95].

Definition 5.1.1. Let G be a profinite group and $\mathcal{G} \subseteq \mathrm{Subgr}(G)$ a G-invariant closed set of subgroups. A **finite $\mathcal{G}$-embedding problem** for G is a triple $EP_{\mathcal{G}} = (\varphi, \alpha, \mathcal{B})$, where $\varphi\colon G \to A$ and $\alpha\colon B \to A$ are epimorphisms of profinite groups, B is finite, $\mathcal{B}$ is a set of subgroups of B, and for every $\Gamma \in \mathcal{G}$ there exists $\Delta \in \mathcal{B}$ and a homomorphism $\gamma_\Gamma\colon \Gamma \to \Delta$ with $\alpha \circ \gamma_\Gamma = \varphi|_\Gamma$. A **solution** of $EP_{\mathcal{G}}$ is a homomorphism $\gamma\colon G \to B$ with $\alpha \circ \gamma = \varphi$ such that for each $\Gamma \in \mathcal{G}$, there exists $\Delta \in \mathcal{B}$ and $b \in B$ with $\gamma(\Gamma) \subseteq \Delta^b$. Finally, G is **strongly $\mathcal{G}$-projective** if every finite $\mathcal{G}$-embedding problem for G has a solution.

Proposition 5.1.2 (Pop). *Let G be a profinite group, $\mathcal{G} \subseteq \mathrm{Subgr}(G)$ a G-invariant closed subset, and $\Gamma_0 \leq G$ a closed subgroup. If G is strongly $\mathcal{G}$-projective, then the following holds.*

(1) *If Γ_0 is finite, then there exists $\Gamma_1 \in \mathcal{G}$ such that $\Gamma_0 \subseteq \Gamma_1$.*
(2) *If Γ_0 is prosolvable, and there exist prime numbers $p \neq q$ such that $\mathrm{cd}_p(\Gamma_0), \mathrm{cd}_q(\Gamma_0) > 1$, and Γ_0 or all $\Gamma \in \mathcal{G}$ do not have p-torsion, then there exists $\Gamma_1 \in \mathcal{G}$ such that $\Gamma_0 \subseteq \Gamma_1$.*

Proof. See [Pop95, Theorem 2]. □

COROLLARY 5.1.3. *Let $\mathbf{G} = (G, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S}$ be the deficient reduct of the ω-free semi-constant group pile of $(\mathrm{Gal}(K_\mathfrak{p}))_{\mathfrak{p}\in S}$ over Cantor spaces $(C_\mathfrak{p})_{\mathfrak{p}\in S}$. If $\Gamma_0 \leq G$ is a subgroup with $\Gamma_0 \cong \mathrm{Gal}(F)$ for some classically closed field F, then there exists $\Gamma_1 \in \mathcal{G} = \bigcup_{\mathfrak{p}\in S} \mathcal{G}_\mathfrak{p}$ such that $\Gamma_0 \subseteq \Gamma_1$.*

PROOF. We claim that G is strongly $\mathcal{G}$-projective. Let $EP_\mathcal{G} = (\varphi\colon G \to A, \alpha\colon B \to A, \mathcal{B}_{EP})$ be a finite $\mathcal{G}$-embedding problem, and without loss of generality assume that $\mathcal{B}_{EP}$ is B-invariant and closed under taking subgroups. For each $\Gamma \in \mathcal{G}$ choose a homomorphism $\gamma_\Gamma\colon \Gamma \to B$ such that $\gamma_\Gamma(\Gamma) \in \mathcal{B}_{EP}$ and $\alpha \circ \gamma_\Gamma = \varphi|_\Gamma$. For each $\mathfrak{p} \in S$, let

$$\mathcal{B}_\mathfrak{p} = \left\{\gamma_\Gamma(\Gamma)^b\colon \Gamma \in \mathcal{G}_\mathfrak{p}, b \in B\right\} \subseteq \mathcal{B}_{EP}$$

and

$$\mathcal{A}_\mathfrak{p} = \alpha(\mathcal{B}_\mathfrak{p}) = \varphi(\mathcal{G}_\mathfrak{p}).$$

Then, with $\mathbf{A} = (A, \mathcal{A}_\mathfrak{p})_{\mathfrak{p}\in S}$ and $\mathbf{B} = (B, \mathcal{B}_\mathfrak{p})_{\mathfrak{p}\in S}$, $EP = (\varphi\colon \mathbf{G} \to \mathbf{A}, \alpha\colon \mathbf{B} \to \mathbf{A})$ is a finite deficient embedding problem of group piles. This embedding problem is locally solvable. Indeed, if $\Gamma \in \mathcal{G}_\mathfrak{p}$, then $\Delta = \gamma_\Gamma(\Gamma) \in \mathcal{B}_\mathfrak{p}$ and $\gamma_\Gamma\colon \Gamma \to \Delta$ satisfies $\alpha \circ \gamma_\Gamma = \varphi|_\Gamma$. And if $\Delta \in \mathcal{B}_\mathfrak{p}$, then there exist $\Gamma \in \mathcal{G}_\mathfrak{p}$ and $b \in B$ such that $\Delta = \gamma_\Gamma(\Gamma)^b$. Hence, if we choose $g \in G$ with $\varphi(g) = \alpha(b)$ and define $\tilde{\gamma}_{\Gamma^g}\colon \Gamma^g \to \Delta$ by $\tilde{\gamma}_{\Gamma^g}(x) = \gamma_\Gamma(x^{g^{-1}})^b$, then $\alpha \circ \tilde{\gamma}_{\Gamma^g} = \varphi|_{\Gamma^g}$. By Proposition 3.6.3, $\mathbf{G}$ is an ω-free C-pile, hence EP has a solution $\gamma\colon \mathbf{G} \to \mathbf{B}$ by Lemma 3.6.5. Since $\gamma(\mathcal{G}) = \mathcal{B} \subseteq \mathcal{B}_{EP}$, it follows that $\gamma\colon G \to B$ is a solution of $EP_\mathcal{G}$. Therefore, G is indeed strongly $\mathcal{G}$-projective.

If F is real closed, then $\Gamma_0 \cong \mathbb{Z}/2\mathbb{Z}$ is finite. If F is p-adically closed, then Lemma 1.6.5 implies that Γ_0 is prosolvable, torsion-free, and $\mathrm{cd}_l(\Gamma_0) = 2$ for all l. Hence, Proposition 5.1.2 implies that there exists $\Gamma_1 \in \mathcal{G}$ such that $\Gamma_0 \subseteq \Gamma_1$. □

5.2. The Fields $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$

In Proposition 4.3.4 we already presented the result of Geyer-Jarden that $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ is PSCC for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$. The description of the absolute Galois group pile of these fields can be derived from the following result.

PROPOSITION 5.2.1 (Haran-Jarden-Pop). *Let S be a finite set of primes of a number field K, let $e \in \mathbb{N}$, and let $\mathbf{G} = (G, \mathcal{G}_0, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S}$ be the ω-free semi-constant group pile of $(\mathrm{Gal}(K_\mathfrak{p}))_{\mathfrak{p}\in S}$ over Cantor spaces $(C_\mathfrak{p})_{\mathfrak{p}\in S}$. Then for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$,*

$$\mathrm{Gal}(K_{\mathrm{tot},S}[\boldsymbol{\sigma}]) \cong G.$$

PROOF. See [HJP09a, Theorem 3.11], □

REMARK 5.2.2. The special case $S = \emptyset$ was proven by Jarden in [Jar97].

For a different proof of the following topological lemma see [HJP09b, Lemma 2.1].

LEMMA 5.2.3. *If $\mathbf{G} = (G, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S}$ is a reduced deficient group pile, then for each $\mathfrak{p} \in S$, a basis for the topology on $\mathcal{G}_\mathfrak{p}$ is given by sets of the form*

$$\mathrm{Subgr}(U) \cap \mathcal{G}_\mathfrak{p},$$

where U is an open subgroup of G.[1]

PROOF. Since the intersection of two sets of the form $\mathrm{Subgr}(U) \cap \mathcal{G}_\mathfrak{p}$ is again of that form, and each of these sets is open-closed in $\mathcal{G}_\mathfrak{p}$ (cf. Definition 3.1.1), these sets form the basis for a zero-dimensional compact topology $\mathcal{T}$ on $\mathcal{G}_\mathfrak{p}$, which is coarser than the profinite topology on $\mathcal{G}_\mathfrak{p}$. Since a compact Hausdorff topology is minimal Hausdorff, it suffices to prove that $\mathcal{T}$ is Hausdorff.

Let $\Gamma, \Gamma' \in \mathcal{G}_\mathfrak{p}$ be distinct. Since $\mathbf{G}$ is reduced, Γ is not contained in Γ', and vice versa. So since Γ is the intersection of all open subgroups of G containing it, there exists an open subgroup $U \leq G$ such that $\Gamma \leq U$ but $\Gamma' \not\leq U$. That is, $\mathcal{T}$ is T_1. But any zero-dimensional T_1 space is Hausdorff, cf. [SS70, Figure 9], so this proves the claim. □

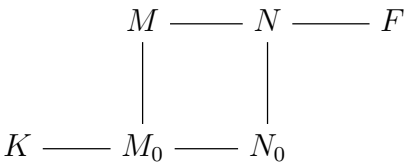
The following lemma is similar to [HJP09b, Lemma 10.3(e)].

LEMMA 5.2.4. *Let M/K be an infinite Galois extension contained in $K_{\mathrm{tot},S}$ and let $\mathbf{Gal}_S(M) = (G, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S}$. Then $\mathcal{G}_\mathfrak{p}/G$ is nonempty and perfect for each $\mathfrak{p} \in S$.*

PROOF. Let $\mathfrak{p} \in S$. By Lemma 4.1.3 and Lemma 4.2.1(2), M/K is totally S-adic, hence $\mathcal{S}_\mathfrak{p}(M) \neq \emptyset$. Consequently, $\mathcal{G}_\mathfrak{p} \neq \emptyset$, and hence $\mathcal{G}_\mathfrak{p}/G \neq \emptyset$.

Let $F \in \mathrm{CC}(M, \mathfrak{p})$, $\Gamma = \mathrm{Gal}(F)$, and suppose that the image of Γ in $\mathcal{G}_\mathfrak{p}/G$ is isolated. Then $\Gamma^G = \{\Gamma^g \colon g \in G\}$ is open in $\mathcal{G}_\mathfrak{p}$. By Lemma 3.5.3, $(G, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S}$ is reduced, so Lemma 5.2.3 gives an open subgroup $U \leq G$ such that $\Gamma \in \mathrm{Subgr}(U) \cap \mathcal{G}_\mathfrak{p} \subseteq \Gamma^G$. In other words, there exists a finite extension N/M contained in F such that every $F' \in \mathrm{CC}(M, \mathfrak{p})$ that contains N is conjugate to F over M.

Let N_0/K be a finite extension such that $MN_0 = N$, and let $M_0 = M \cap N_0$.



Then N/N_0 and M/M_0 are infinite Galois extensions. Let M_1 be a finite proper Galois extension of M_0 in M. Let $\mathfrak{Q} \in \mathcal{S}_\mathfrak{p}(N)$ be the

[1] In other words, the (**strict**) topology on $\mathcal{G}_\mathfrak{p}$ coincides with the topology induced by the **étale** topology of $\mathrm{Subgr}(G)$, cf. [HJP07], [HJP05], [HJP09a].

restriction of the unique prime of F above $\mathfrak{p}$, and let $\mathfrak{P} = \mathfrak{Q}|_M \in \mathcal{S}_\mathfrak{p}(M)$, $\mathfrak{P}_0 = \mathfrak{Q}|_{M_0} \in \mathcal{S}_\mathfrak{p}(M_0)$, $\mathfrak{P}_1 = \mathfrak{Q}|_{M_1} \in \mathcal{S}_\mathfrak{p}(M_1)$. Since $\mathfrak{p}$ totally splits in $K_{\mathrm{tot},S}/K$ by Lemma 4.1.4, there exists $\mathfrak{P}_1' \in \mathcal{S}_\mathfrak{p}(M_1)$ lying over $\mathfrak{P}_0$, and different from $\mathfrak{P}_1$. By Lemma 2.1.11, there exists $\tau \in \mathrm{Gal}(M_1/M_0)$ such that $\tau(\mathfrak{P}_1) = \mathfrak{P}_1'$. Since M/M_0 is Galois and M is linearly disjoint from N_0 over M_0, there exists $\sigma \in \mathrm{Gal}(N/N_0)$ with $\sigma|_{M_1} = \tau$.

Let $\mathfrak{Q}' = \sigma(\mathfrak{Q})$ and $\mathfrak{P}' = \mathfrak{Q}'|_M$. Then $\mathfrak{Q}' \in \mathcal{S}_\mathfrak{p}(N)$, $\mathfrak{P}' \in \mathcal{S}_\mathfrak{p}(M)$, and $\mathfrak{P}' \neq \mathfrak{P}$ since $\mathfrak{P}|_{M_1} = \mathfrak{P}_1$ and $\mathfrak{P}'|_{M_1} = \tau(\mathfrak{P}_1) = \mathfrak{P}_1'$. Choose $F' \in \mathrm{CC}(N, \mathfrak{Q}')$. Then $F' \in \mathrm{CC}(M, \mathfrak{P}') \subseteq \mathrm{CC}(M, \mathfrak{p})$ by Lemma 2.9.9(1). Moreover, $N \subseteq F'$ but F' is not conjugate to F over M, a contradiction. □

THEOREM 5.2.5. *Let S be a finite set of primes of a number field K, let $e \in \mathbb{N}$, and let $\mathbf{G} = (G, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S}$ be the deficient reduct of the ω-free semi-constant group pile of $(\mathrm{Gal}(K_\mathfrak{p}))_{\mathfrak{p}\in S}$ over Cantor spaces $(C_\mathfrak{p})_{\mathfrak{p}\in S}$. Then for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$,*

$$\mathbf{Gal}_S(K_{\mathrm{tot},S}[\boldsymbol{\sigma}]) \cong \mathbf{G}.$$

PROOF. By Proposition 5.2.1, $\mathrm{Gal}(K_{\mathrm{tot},S}[\boldsymbol{\sigma}]) \cong G$ for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$. By Proposition 4.3.4, almost all $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ are PSCC. Fix $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ such that $\mathrm{Gal}(K_{\mathrm{tot},S}[\boldsymbol{\sigma}]) \cong G$ and $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ is PSCC, and let $M = K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$. We identify $\mathrm{Gal}(M)$ with G and let $\mathbf{Gal}_S(M) = (G, \mathcal{G}_\mathfrak{p}')_{\mathfrak{p}\in S}$. Let $\mathcal{G} = \bigcup_{\mathfrak{p}\in S} \mathcal{G}_\mathfrak{p}$ and $\mathcal{G}' = \bigcup_{\mathfrak{p}\in S} \mathcal{G}_\mathfrak{p}'$. For $\mathfrak{p} \in S$ let $\Gamma_\mathfrak{p} = \mathrm{Gal}(K_\mathfrak{p})$. For each $\Gamma \in \{\Gamma_\mathfrak{p} \colon \mathfrak{p} \in S\}$ let $S_\Gamma = \{\mathfrak{q} \in S \colon \Gamma_\mathfrak{q} \cong \Gamma\}$, $\mathcal{G}_\Gamma = \bigcup_{\mathfrak{q}\in S_\Gamma} \mathcal{G}_\mathfrak{q}$, and $\mathcal{G}_\Gamma' = \bigcup_{\mathfrak{q}\in S_\Gamma} \mathcal{G}_\mathfrak{q}'$. Note that since every $\Gamma \in \mathcal{G}_\mathfrak{p}$ and every $\Gamma \in \mathcal{G}_\mathfrak{p}'$ is isomorphic to $\Gamma_\mathfrak{p}$, $\mathcal{G}_\Gamma = \{\Gamma_0 \in \mathcal{G} \colon \Gamma_0 \cong \Gamma\}$ and $\mathcal{G}_\Gamma' = \{\Gamma_0 \in \mathcal{G}' \colon \Gamma_0 \cong \Gamma\}$.

PART A. CLAIM: For each $\mathfrak{p} \in S$, $\mathcal{G}_{\Gamma_\mathfrak{p}} = \mathcal{G}'_{\Gamma_\mathfrak{p}}$.

If $\Gamma \in \mathcal{G}_{\Gamma_\mathfrak{p}}$, then $\Gamma \cong \mathrm{Gal}(K_\mathfrak{p})$ and thus the fixed field M' of Γ is classically closed with respect to some classical prime $\mathfrak{P}'$ by Lemma 2.11.1. Let $\mathfrak{P} = \mathfrak{P}'|_M$. Without loss of generality assume that $M_\mathfrak{P} \subseteq M'$. Since M is algebraic over $\mathbb{Q}$, $\mathfrak{P}$ is local. In particular, $\mathfrak{P}$ is quasi-local, i.e. $M_\mathfrak{P} \in \mathrm{CC}(M, \mathfrak{P})$. Since M is PSCL, Proposition 2.10.2 implies that $\mathfrak{q} := \mathfrak{P}|_K \in S$. Since $\mathfrak{q}$ totally splits in $K_{\mathrm{tot},S}/K$ by Lemma 4.1.4 and $M \subseteq K_{\mathrm{tot},S}$, Lemma 1.5.2 implies that $\mathrm{tp}(\mathfrak{P}) = \mathrm{tp}(\mathfrak{q})$, so $\mathfrak{P} \in \mathcal{S}_S(M)$. Hence, if we let $\Gamma_0 = \mathrm{Gal}(M_\mathfrak{P})$, then $\Gamma \subseteq \Gamma_0$ and $\Gamma_0 \in \mathcal{G}'$. By Proposition 5.1.3, there exists $\Gamma_1 \in \mathcal{G}$ such that $\Gamma_0 \subseteq \Gamma_1$. Thus, $\Gamma \subseteq \Gamma_0 \subseteq \Gamma_1$, and both Γ and Γ_1 are contained in $\mathcal{G}$. Since $\mathbf{G}$ is reduced by Lemma 3.4.6(2), $\Gamma = \Gamma_0 = \Gamma_1$, so $\Gamma \in \mathcal{G}'$. Consequently, $\Gamma \in \mathcal{G}'_{\Gamma_\mathfrak{p}}$.

Conversely, let $\Gamma \in \mathcal{G}'_{\Gamma_\mathfrak{p}}$, i.e. $\Gamma = \mathrm{Gal}(F')$, where $F' \in \mathrm{CC}(M, \mathfrak{q})$ for some $\mathfrak{q} \in S$ with $\Gamma_\mathfrak{q} \cong \Gamma_\mathfrak{p}$. Proposition 5.1.3 provides a $\Gamma_1 \in \mathcal{G}$ with

$\Gamma \subseteq \Gamma_1$. By the first part of the proof of the claim, $\Gamma_1 \in \mathcal{G}'$. Hence, $\Gamma = \Gamma_1$ since $\mathbf{Gal}_S(M)$ is reduced by Lemma 3.5.3. Thus, $\Gamma \in \mathcal{G}_{\Gamma_\mathfrak{p}}$.

PART B. THE CANTOR SPACES $\mathcal{G}_\mathfrak{p}/G$ AND $\mathcal{G}'_\mathfrak{p}/G$. By definition, $\mathbf{G} = (\hat{F}_\omega * \mathbf{H})^{\mathrm{def}}$, where $\mathbf{H} = (H, \mathcal{H}_\mathfrak{p})_{\mathfrak{p}\in S}$ is a semi-constant group pile of $(\Gamma_\mathfrak{p})_{\mathfrak{p}\in S}$ over $(C_\mathfrak{p})_{\mathfrak{p}\in S}$. Let $C := \bigsqcup_{\mathfrak{p}\in S} C_\mathfrak{p}$ and let

$$\lambda\colon \left(\bigsqcup_{\mathfrak{p}\in S} \Gamma_\mathfrak{p} \times C_\mathfrak{p}, \pi, C\right) \to H$$

be a free product of the sheaf $(\bigsqcup_{\mathfrak{p}\in S} \Gamma_\mathfrak{p} \times C_\mathfrak{p}, \pi, C)$.

By Lemma 3.4.4(3), the map $C_\mathfrak{p} \to \mathcal{H}_\mathfrak{p}/H$ given by $x \mapsto \lambda(\pi^{-1}(x))^H$ is a homeomorphism for each $\mathfrak{p} \in S$. By Lemma 3.3.4(4), the map $\mathcal{H}_\mathfrak{p}/H \to \mathcal{G}_\mathfrak{p}/G$ induced by the inclusion $\mathcal{H}_\mathfrak{p} \to \mathcal{G}_\mathfrak{p}$ is a homeomorphism, too. Hence, for each $\mathfrak{p} \in S$, the composition of these maps gives a homeomorphism $C_\mathfrak{p} \to \mathcal{G}_\mathfrak{p}/G$, and we identify $C_\mathfrak{p}$ and $\mathcal{G}_\mathfrak{p}/G$ via this homeomorphism.

By Lemma 3.4.6(2) and Lemma 3.5.3, $(G, \mathcal{G}_\mathfrak{p})_{\mathfrak{p}\in S}$ and $(G, \mathcal{G}'_\mathfrak{p})_{\mathfrak{p}\in S}$ are separated. Thus, if $\mathfrak{p} \in S$, then by PART A,

$$\bigsqcup_{\mathfrak{q}\in S_{\Gamma_\mathfrak{p}}} C_\mathfrak{q} = \bigsqcup_{\mathfrak{q}\in S_{\Gamma_\mathfrak{p}}} \mathcal{G}_\mathfrak{q}/G = \bigsqcup_{\mathfrak{q}\in S_{\Gamma_\mathfrak{p}}} \mathcal{G}'_\mathfrak{q}/G. \tag{5.1}$$

The extension M/K is infinite. This follows for example from Proposition 2.10.2, since M is PSCC and every prime of a number field, and hence of any finite extension of K, is local. Thus, by Lemma 5.2.4, $\mathcal{G}'_\mathfrak{p}/G$ is nonempty and perfect for each $\mathfrak{p} \in S$. Since C is a Cantor space, each of the perfect subspaces $\mathcal{G}'_\mathfrak{p}/G$ is a Cantor space. In particular, $\mathcal{G}_\mathfrak{p}/G$ and $\mathcal{G}'_\mathfrak{p}/G$ are homeomorphic.

PART C. CONSTRUCTION OF AN AUTOMORPHISM OF G. By PART B, there exists a homeomorphism τ of C onto itself with $\tau(\mathcal{G}_\mathfrak{p}/G) = \mathcal{G}'_\mathfrak{p}/G$ for each $\mathfrak{p} \in S$. By (5.1), τ maps $\bigsqcup_{\mathfrak{q}\in S_{\Gamma_\mathfrak{p}}} C_\mathfrak{q}$ onto itself. Hence, since $\Gamma_\mathfrak{q} \cong \Gamma_\mathfrak{p}$ for all $\mathfrak{q} \in S_{\Gamma_\mathfrak{p}}$, we can define a continuous bijection α from the sheaf $(\bigsqcup_{\mathfrak{p}\in S} \Gamma_\mathfrak{p} \times C_\mathfrak{p}, \pi, C)$ onto itself by $\alpha((g, x)) = (g, \tau(x))$. By the universal property of the free product, the morphism $\lambda \circ \alpha$ induces an automorphism β of G with $\lambda \circ \alpha = \beta \circ \lambda$ and $\beta|_{\hat{F}_\omega} = \mathrm{id}_{\hat{F}_\omega}$.

PART D. CONCLUSION OF THE PROOF. Since $\alpha((g, x)) = (g, \tau(x))$ for all $(g, x) \in \bigsqcup_{\mathfrak{p}\in S} \Gamma_\mathfrak{p} \times C_\mathfrak{p}$,

$$\alpha(\pi^{-1}(x)) = \pi^{-1}(\tau(x))$$

for each $x \in C$. Since each $\Gamma \in \mathcal{G}$ is G-conjugate to $\lambda(\pi^{-1}(\Gamma^G))$,

$$\mathcal{G}_\mathfrak{p} = \left\{\lambda(\pi^{-1}(x))^g \colon x \in \mathcal{G}_\mathfrak{p}/G,\ g \in G\right\}$$

and

$$\mathcal{G}'_\mathfrak{p} = \left\{\lambda(\pi^{-1}(x))^g \colon x \in \mathcal{G}'_\mathfrak{p}/G,\ g \in G\right\}.$$

It follows that

$$\begin{aligned}\beta(\mathcal{G}_{\mathfrak{p}}) &= \left\{\beta(\lambda(\pi^{-1}(x))^g) : x \in \mathcal{G}_{\mathfrak{p}}/G,\ g \in G\right\}\\ &= \left\{\lambda(\alpha(\pi^{-1}(x)))^{\beta(g)} : x \in \mathcal{G}_{\mathfrak{p}}/G,\ g \in G\right\}\\ &= \left\{\lambda(\pi^{-1}(\tau(x)))^g : x \in \mathcal{G}_{\mathfrak{p}}/G,\ g \in \beta(G)\right\}\\ &= \left\{\lambda(\pi^{-1}(x))^g : x \in \mathcal{G}'_{\mathfrak{p}}/G,\ g \in G\right\}\\ &= \mathcal{G}'_{\mathfrak{p}}\end{aligned}$$

for each $\mathfrak{p} \in S$. Therefore,

$$\mathbf{Gal}_S(M) = (G, \mathcal{G}'_{\mathfrak{p}})_{\mathfrak{p}\in S} = (G, \beta(\mathcal{G}_{\mathfrak{p}}))_{\mathfrak{p}\in S} = \beta(\mathbf{G}) \cong \mathbf{G},$$

as claimed. □

REMARK 5.2.6. I suspect that the same proof shows that one can deduce the number field case of the main result of [HJP09b] from the main result of [HJP09a].

5.3. Normally Generated Groups

The Galois group $H = \mathrm{Gal}(K_{\mathrm{tot},S}/K_{\mathrm{tot},S}[\boldsymbol{\sigma}])$ is isomorphic to $\hat{F}_\omega$ for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, so the parameter e is not visible in the isomorphism type of H. However, e appears when we consider H as a subgroup of $\mathrm{Gal}(K_{\mathrm{tot},S}/K)$ which is *normally generated by e elements.*

DEFINITION 5.3.1. Let G be a profinite group. A closed subgroup $H \leq G$ is **normally generated by** e **elements** in G if there exist $h_1, \ldots, h_e \in H$ such that $H = \langle h_i^g \colon i = 1, \ldots, e,\ g \in G\rangle$.

LEMMA 5.3.2. *Let G be a profinite group, and let $H \leq G$. Then H is normally generated in G by e elements if and only if for every open normal subgroup $N \lhd G$, HN/N is normally generated in G/N by e elements.*

PROOF. If $H = \langle h_i^g \colon i = 1, \ldots, e,\ g \in G\rangle$, then

$$HN/N = \langle (h_i N/N)^g \colon i = 1, \ldots, e,\ g \in G/N\rangle\,.$$

Conversely, suppose that HN/N is normally generated in G/N by e elements for every open normal subgroup $N \lhd G$. Note that $G = \varprojlim_N G/N$. For every N, let

$$\mathcal{N}_N = \{(h_1, \ldots, h_e) \in (G/N)^e \colon \langle h_i^g \colon 1 \leq i \leq e,\ g \in G/N\rangle = HN/N\}\,.$$

By the first paragraph of this proof, the $\mathcal{N}_N$ form an inverse system. By our assumption, each $\mathcal{N}_N$ is nonempty. Therefore, $\mathcal{N} := \varprojlim_N \mathcal{N}_N \subseteq G^e$ is nonempty. If $(h_1, \ldots, h_e) \in \mathcal{N}$, then $\langle h_i^g \colon i = 1, \ldots, e,\ g \in G\rangle = H$, so H is normally generated in G by e elements, as claimed. □

DEFINITION 5.3.3. We construct the $\mathcal{L}_{\mathrm{ring}}(K)$-theory $T_{\mathrm{normal},S,e}$ as follows:

Let N be a finite Galois extension of K in $K_{\mathrm{tot},S}$, let $N_1,\dots,N_{r(N)}$ be all subextensions of N/K, and let $f_1,\dots,f_{r(N)} \in K[X]$ be irreducible polynomials such that $N_i \cong_K K[X]/(f_i(X))$ for each i. Let J_i be the set of all j such that there exists no K-embedding of N_j into N_i, and let $\psi_{i,f_1,\dots,f_{r(N)}}$ be the $\mathcal{L}_{\mathrm{ring}}(K)$-sentence

$$(\exists x)(f_i(x)=0) \wedge \bigwedge_{j\in J_i} \neg(\exists x)(f_j(x)=0).$$

If $L \supseteq K$, then $L \models \psi_{i,f_1,\dots,f_{r(N)}}$ if and only if $L\cap N \cong_K N_i$. Let I_N be the set of all i such that $\mathrm{Gal}(N/N_i)$ is normally generated in $\mathrm{Gal}(N/K)$ by e elements, and let $\varphi_{N,f_1,\dots,f_{r(N)}}$ be the $\mathcal{L}_{\mathrm{ring}}(K)$-sentence

$$\bigvee_{i\in I_N} \psi_{i,f_1,\dots,f_{r(N)}}.$$

Then $L \models \varphi_{N,f_1,\dots,f_{r(N)}}$ if and only if $\mathrm{Gal}(N/L\cap N)$ is normally generated in $\mathrm{Gal}(N/K)$ by e elements.

Let $T_{\mathrm{normal},S,e}$ consist of all sentences $\varphi_{N,f_1,\dots,f_{r(N)}}$, where N runs over all finite Galois extensions of K in $K_{\mathrm{tot},S}$, and $f_1,\dots,f_{r(N)} \in K[X]$ are suitable irreducible polynomials.

LEMMA 5.3.4. *A field $F \supseteq K$ is a model of $T_{\mathrm{normal},S,e}$ if and only if $\mathrm{Gal}(K_{\mathrm{tot},S}/F\cap K_{\mathrm{tot},S})$ is normally generated in $\mathrm{Gal}(K_{\mathrm{tot},S}/K)$ by e elements.*

PROOF. Let $L = F\cap K_{\mathrm{tot},S}$. By construction, F satisfies $T_{\mathrm{normal},S,e}$ if and only if $\mathrm{Gal}(N/L\cap N)$ is normally generated in $\mathrm{Gal}(N/K)$ by e elements for each finite Galois extension N of K inside $K_{\mathrm{tot},S}$. In other words, $\mathrm{Gal}(K_{\mathrm{tot},S}/L)U/U$ is normally generated in $\mathrm{Gal}(K_{\mathrm{tot},S}/K)/U$ by e elements for each open normal subgroup U of $\mathrm{Gal}(K_{\mathrm{tot},S}/K)$. By Lemma 5.3.2, this is the case if and only if $\mathrm{Gal}(K_{\mathrm{tot},S}/L)$ is normally generated in $\mathrm{Gal}(K_{\mathrm{tot},S}/K)$ by e elements. □

5.4. Axiomatization of the Theory of Almost All $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$

In this section we axiomatize of the theory of almost all fields $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$.

DEFINITION 5.4.1. Let the $\mathcal{L}_{\mathrm{ring}}(K)$-theory $T'_{\mathrm{tot},S,e}$ consist of the following axioms:

(1) The theory $T_{\mathrm{tot},S,\omega}$ (Definition 4.4.1 for $e=\omega$).
(2) The theory $T_{\mathrm{normal},S,e}$ (Definition 5.3.3).

LEMMA 5.4.2. *A field $F \supseteq K$ is a model of $T'_{\mathrm{tot},S,e}$ if and only if it satisfies the following conditions:*

(1) *F is* PSCC.
(2) *$\mathbf{Gal}_S(F)$ is an ω-free C-pile.*
(3) *$F \cap \tilde{K} \subseteq K_{\mathrm{tot},S}$ and $F/F \cap \tilde{K}$ is totally S-adic.*
(4) *$\mathrm{Gal}(K_{\mathrm{tot},S}/F \cap \tilde{K})$ is normally generated in $\mathrm{Gal}(K_{\mathrm{tot},S}/K)$ by e elements.*

In that case, F satisfies also the following conditions:

(5) *F is S-*SAP.
(6) *F is S-quasi-local.*

PROOF. By Lemma 4.4.2, F satisfies $T_{\mathrm{tot},S,\omega}$ if and only if (1)-(3) hold. If (3) holds, then $F \cap \tilde{K} = F \cap K_{\mathrm{tot},S}$, hence by Lemma 5.3.4, F satisfies $T_{\mathrm{normal},S,e}$ if and only if (4) holds. Lemma 4.4.2 implies that if F satisfies $T_{\mathrm{tot},S,\omega}$, then (5) and (6) hold. □

LEMMA 5.4.3. *For almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ is a model of $T'_{\mathrm{tot},S,e}$.*

PROOF. By Proposition 4.3.4, almost all $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ are PSCC. By Theorem 5.2.5, $\mathbf{Gal}_S(K_{\mathrm{tot},S}[\boldsymbol{\sigma}])$ is isomorphic for almost all $\boldsymbol{\sigma}$ to the deficient reduct of the ω-free semi-constant group pile of $(\mathrm{Gal}(K_{\mathfrak{p}}))_{\mathfrak{p}\in S}$ over Cantor spaces $(C_{\mathfrak{p}})_{\mathfrak{p}\in S}$. Since each $C_{\mathfrak{p}}$ is perfect, this is an ω-free C-pile by Proposition 3.6.3. By Galois correspondence,

$$\mathrm{Gal}(K_{\mathrm{tot},S}/K_{\mathrm{tot},S}[\boldsymbol{\sigma}]) = \left\langle (\sigma_i|_{K_{\mathrm{tot},S}})^g \colon i = 1, \dots, e,\ g \in \mathrm{Gal}(K_{\mathrm{tot},S}/K) \right\rangle$$

is normally generated in $\mathrm{Gal}(K_{\mathrm{tot},S}/K)$ by e elements. Therefore, by Lemma 5.4.2, $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ is a model of $T'_{\mathrm{tot},S,e}$ for almost all $\boldsymbol{\sigma}$. □

DEFINITION 5.4.4. Let

$$T'_{\mathrm{almost},S,e}$$

denote the set of all $\mathcal{L}_{\mathrm{ring}}(K)$-sentences that are true in almost all fields $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$, $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$.

THEOREM 5.4.5. *The theory $T'_{\mathrm{tot},S,e}$ is an axiomatization of $T'_{\mathrm{almost},S,e}$, i.e. these two theories have the same models.*

PROOF. First note that every model of $T'_{\mathrm{almost},S,e}$ is a field containing K. By Definition 4.4.1(0), the same holds for every model of $T'_{\mathrm{tot},S,e}$.

By Lemma 5.4.3, almost all $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ satisfy $T'_{\mathrm{tot},S,e}$, so every model of $T'_{\mathrm{almost},S,e}$ is a model of $T'_{\mathrm{tot},S,e}$.

Conversely, let E be a model of $T'_{\mathrm{tot},S,e}$ and let $L = E \cap \tilde{K}$. Suppose we can construct a model F of $T'_{\mathrm{almost},S,e}$ with $F \cap \tilde{K} \cong_K L$. Since $F \models T'_{\mathrm{tot},S,e}$ by the first paragraph of this proof, $E, F \models T_{\mathrm{tot},S,\omega}$, cf. Definition 5.4.1(1). Thus, $E \equiv_K F$ by Proposition 4.4.4, hence E is a model of $T'_{\mathrm{almost},S,e}$ and we are done.

Conditions (3) and (4) of Lemma 5.4.2 imply that $L \subseteq K_{\mathrm{tot},S}$ and give $\tau_1, \dots, \tau_e \in \mathrm{Gal}(K_{\mathrm{tot},S}/K)$ that normally generate $\mathrm{Gal}(K_{\mathrm{tot},S}/L)$ in $\mathrm{Gal}(K_{\mathrm{tot},S}/K)$. In particular, L/K is Galois. Let $\mathcal{N}$ be the set of finite Galois extensions of K inside $K_{\mathrm{tot},S}$. For each $N \in \mathcal{N}$, the set

$$\begin{aligned}\Sigma(N) &:= \{\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \colon \mathrm{res}_N(\sigma_i) = \mathrm{res}_N(\tau_i),\ i = 1, \dots, e\}\\ &\subseteq \{\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \colon K_{\mathrm{tot},S}[\boldsymbol{\sigma}] \cap N = L \cap N\}\end{aligned}$$

has positive Haar measure. If $N_1, \dots, N_r \in \mathcal{N}$, then $N_1 \cdots N_r \in \mathcal{N}$ and $\Sigma(N_1) \cap \cdots \cap \Sigma(N_r) = \Sigma(N_1 \cdots N_r)$. Hence, by [FJ08, 7.6.1], there exists an ultrafilter $\mathcal{D}$ on $\mathrm{Gal}(K)^e$ which contains each of the sets $\Sigma(N)$, $N \in \mathcal{N}$, and all sets of measure 1. Let

$$F = \prod_{\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e} K_{\mathrm{tot},S}[\boldsymbol{\sigma}]/\mathcal{D}$$

be the ultraproduct, and let $M = F \cap \tilde{K}$. Since $\mathcal{D}$ contains all sets of measure 1, and almost all $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ are models of $T'_{\mathrm{almost},S,e}$, F is a model of $T'_{\mathrm{almost},S,e}$ by Lemma 1.2.2. Furthermore, $M \subseteq K_{\mathrm{tot},S}$, and $M \cap N = L \cap N$ for each $N \in \mathcal{N}$, since $\mathcal{D}$ contains $\Sigma(N)$. Therefore, $M = L$, as claimed. □

5.5. Decidability of the Theory of Almost All $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$

Using the axiomatization of the theory of almost all $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$, we prove that this theory is decidable. The proof follows the proof of Section 4.6 almost verbatim.

LEMMA 5.5.1. *The theory $T'_{\mathrm{tot},S,e}$ is recursive.*

PROOF. The theory $T_{\mathrm{tot},S,\omega}$ is recursive by Lemma 4.5.8. The set of polynomials $f \in K[X]$ that completely decompose over $K_{\mathrm{tot},S}$ is recursive by Lemma 4.5.6, hence one can recursively decide if the splitting field L of f is contained in $K_{\mathrm{tot},S}$. Since K has a splitting algorithm, one can also recursively decide if f is irreducible, and one can compute the Galois group $\mathrm{Gal}(L/K)$, [FJ08, 19.3.2]. Hence, the theory $T_{\mathrm{normal},S,e}$ is recursive. □

DEFINITION 5.5.2. For each $\mathcal{L}_{\mathrm{ring}}(K)$-sentence θ let

$$\Sigma'_{S,e}(\theta) = \{\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \colon K_{\mathrm{tot},S}[\boldsymbol{\sigma}] \models \theta\}$$

be the truth set of θ, and let μ be the normalized Haar measure on $\mathrm{Gal}(K)^e$ as in Notation 4.6.5.

LEMMA 5.5.3. *Let λ be a test sentence (cf. Definition 4.6.1). Then $\Sigma'_{S,e}(\lambda)$ is open-closed in $\mathrm{Gal}(K)^e$ and $\mu(\Sigma'_{S,e}(\lambda))$ is a rational number. The map $\lambda \mapsto \mu(\Sigma'_{S,e}(\lambda))$ from test sentences to $\mathbb{Q}$ is recursive.*

PROOF. Let $f_1, \dots, f_n \in K[X]$ be the polynomials occurring in λ. Their splitting field L_λ is a finite Galois extension of K inside $K_{\mathrm{tot},S}$.

Let L/K be a Galois extension with $L_\lambda \subseteq L \subseteq K_{\mathrm{tot},S}$. Then $K_{\mathrm{tot},S}[\boldsymbol{\sigma}] \cap L = L[\mathrm{res}_L(\boldsymbol{\sigma})]$ for each $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$. Let

$$\Sigma_{L,\lambda} = \{\boldsymbol{\tau} \in \mathrm{Gal}(L/K)^e \colon L[\boldsymbol{\tau}] \models \lambda\}.$$

We claim that

$$\Sigma'_{S,e}(\lambda) = \{\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \colon \mathrm{res}_L(\boldsymbol{\sigma}) \in \Sigma_{L,\lambda}\}.$$

Indeed, if λ is of the form $(\exists X)(f(X) = 0)$, where $f \in K[X]$ totally decomposes over $K_{\mathrm{tot},S}$, then

$$\Sigma_{L,\lambda} = \{\boldsymbol{\tau} \in \mathrm{Gal}(L/K)^e \colon f \text{ has a zero in } L[\boldsymbol{\tau}]\}.$$

Since L contains all roots of f, $K_{\mathrm{tot},S}[\boldsymbol{\sigma}] \models \lambda$ if and only if $K_{\mathrm{tot},S}[\boldsymbol{\sigma}] \cap L \models \lambda$, so the claim is true in that case. Induction on the structure of λ shows that the claim holds for all test sentences λ.

Hence, $\Sigma'_{S,e}$ is open-closed, in particular measurable. Furthermore,

$$\mu(\Sigma'_{S,e}(\lambda)) = \frac{|\Sigma_{L_\lambda,\lambda}|}{[L_\lambda : K]^e}$$

is a rational number, and this number is computable since K has a splitting algorithm, see for example [FJ08, 19.3.2]. □

THEOREM 5.5.4. *Let S be a finite set of primes of a number field K, and let $e \in \mathbb{N}$. Then the following holds:*

1. *For every $\mathcal{L}_{\mathrm{ring}}(K)$-sentence θ, $\Sigma'_{S,e}(\theta)$ is μ-measurable and $\mu(\Sigma'_{S,e}(\theta))$ is a rational number.*
2. *The map $\theta \mapsto \mu(\Sigma'_{S,e}(\theta))$ from $\mathcal{L}_{\mathrm{ring}}(K)$-sentences to $\mathbb{Q}$ is recursive.*

In particular, the theory $T'_{\mathrm{almost},S,e}$ of almost all fields $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$, $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, is decidable.

PROOF. By Theorem 5.4.5, $T'_{\mathrm{tot},S,e} \models T'_{\mathrm{almost},S,e}$ and $T'_{\mathrm{almost},S,e} \models T'_{\mathrm{tot},S,e}$. In particular, $T'_{\mathrm{almost},S,e} \models T_{\mathrm{tot},S,\omega}$. By Lemma 4.6.2 and [FJ08, 7.8.2], for every $\mathcal{L}_{\mathrm{ring}}(K)$-sentence θ there exists a test sentence λ such that the sentence $\theta \leftrightarrow \lambda$ is in $T'_{\mathrm{almost},S,e}$. In particular, $\Sigma'_{S,e}(\theta)$ and $\Sigma'_{S,e}(\lambda)$ differ only by a zero set. By Lemma 5.5.3, $\Sigma'_{S,e}(\lambda)$ is μ-measurable and $\mu(\Sigma'_{S,e}(\lambda)) \in \mathbb{Q}$, so also $\Sigma'_{S,e}(\theta)$ is μ-measurable and $\mu(\Sigma'_{S,e}(\theta)) = \mu(\Sigma'_{S,e}(\lambda)) \in \mathbb{Q}$. This proves (1).

Since $T'_{\mathrm{tot},S,e} \models T'_{\mathrm{almost},S,e}$, we have $T'_{\mathrm{tot},S,e} \models \theta \leftrightarrow \lambda$. The set of test sentences is recursive by Lemma 4.6.3. By Lemma 5.5.1, the theory $T'_{\mathrm{tot},S,e}$ is recursive, so the set of consequences of $T'_{\mathrm{tot},S,e}$ is recursively enumerable, cf. [Mar02, 2.1.1, 2.1.2]. Therefore, there is a recursive map $\theta \mapsto \lambda_\theta$ from $\mathcal{L}_{\mathrm{ring}}(K)$-sentences to test sentences such that for every θ, $\theta \leftrightarrow \lambda_\theta$ is in $T'_{\mathrm{almost},S,e}$. In particular, $\mu(\Sigma'_{S,e}(\theta)) = \mu(\Sigma'_{S,e}(\lambda_\theta))$.

Since also the map $\lambda \mapsto \mu(\Sigma'_{S,e}(\lambda))$ from test sentences to $\mathbb{Q}$ is recursive by Lemma 5.5.3, the composition

$$\theta \mapsto \lambda_\theta \mapsto \mu(\Sigma'_{S,e}(\lambda_\theta)) = \mu(\Sigma'_{S,e}(\theta))$$

is recursive. This proves (2).

Since $T'_{\mathrm{almost},S,e}$ is the set of all θ with $\mu(\Sigma'_{S,e}(\theta)) = 1$, it follows that $T'_{\mathrm{almost},S,e}$ is decidable. □

This, in combination with the case $e = 0$ of Corollary 4.6.9, finally proves Theorem II from the introduction.

Bibliography

[Bou98] Nicolas Bourbaki. *General Topology*. Springer, 1998.

[Cha84] Zoé Chatzidakis. *Model Theory of Profinite Groups*. Dissertation, Yale University, 1984.

[Cha98] Zoé Chatzidakis. Model theory of profinite groups having the Iwasawa property. *Illinois Journal of Mathematics*, 42(1):70–96, 1998.

[CvdDM81] Gregory Cherlin, Lou van den Dries, and Angus Macintyre. Decidability and undecidability theorems for PAC-fields. *Bulletin of the American Mathematical Society*, 4(1):101–104, 1981.

[CvdDM82] Gregory Cherlin, Lou van den Dries, and Angus Macintyre. The elementary theory of regularly closed fields. Manuscript, 1982.

[Dar00a] Luck Darnière. Decidability and local-global principles. In Denef, Lipshitz, Pheidas, and van Geel, editors, *Proceedings of the workshop: Hilbert's 10'th problem, Relations with Arithmetic and Algebraic Geometry*, Contemporary Mathematics 270, pages 145–167. American Mathematical Society, 2000.

[Dar00b] Luck Darnière. Nonsingular Hasse principle for rings. *Journal für die reine und angewandte Mathematik*, 529:75–100, 2000.

[Dar01] Luck Darnière. Pseudo-algebraically closed rings. *Manuscripta Mathematica*, 105(1):13–46, 2001.

[Efr91] Ido Efrat. The elementary theory of free pseudo p-adically closed fields of finite corank. *Journal of Symbolic Logic*, 56(2):484–496, 1991.

[Efr92] Ido Efrat. Undecidability of pseudo p-adically closed fields. *Achiv der Mathematik*, 58:444–452, 1992.

[Efr95] Ido Efrat. A Galois-theoretic characterization of p-adically closed fields. *Israel Journal of Mathematics*, 91:273–284, 1995.

[Efr97] Ido Efrat. Lifting of generating subgroups. *Proceedings of the American Mathematical Society*, 125(8):2217–2219, 1997.

[Efr06] Ido Efrat. *Valuations, Orderings, and Milnor K-Theory*. American Mathematical Society, 2006.

[End72] Otto Endler. *Valuation Theory*. Springer, 1972.

[EP05] Antonio J. Engler and Alexander Prestel. *Valued Fields*. Springer, 2005.

[Ers82] Yuri Ershov. Totally real field extensions. *Soviet Mathematics Doklady*, 25(2):477–480, 1982.

[Ers83a] Yuri Ershov. Involutory groups. *Algebra and Logic*, 22(3):185–196, 1983.

[Ers83b] Yuri Ershov. Regularly r-closed fields. *Algebra and Logic*, 22(4):277–291, 1983.

[Ers84] Yuri Ershov. Two theorems on regularly r-closed fields. *Journal für die reine und angewandte Mathematik*, 347:154–167, 1984.

[Ers91] Yuri Ershov. PC_p-fields with universal Galois group. *Siberian Advances in Mathematics*, 1(4):1–26, 1991.

[Ers92] Yuri Ershov. Relative regular closeness and π-valuations. *Algebra and Logic*, 31(6):342–360, 1992.

[Ers95] Yuri Ershov. Fields with continuous local elementary properties. II. *Algebra and Logic*, 34(3):140–146, 1995.

[Ers96a] Yuri Ershov. Free Δ^*-groups. *Algebra and Logic*, 35(2):86–95, 1996.

[Ers96b] Yuri Ershov. Nice local-global fields. I. *Algebra and Logic*, 35(4):229–235, 1996.

[Ers99] Yuri Ershov. Uniformly small Δ^*-groups. *Algebra and Logic*, 38(1):12–20, 1999.

[Ers01] Yuri Ershov. *Multi-Valued Fields*. Kluwer Academic, 2001.

[FHV93] Michael D. Fried, Dan Haran, and Helmut Völklein. The absolute Galois group of the totally real numbers. *Comptes Rendus de l'Académie des Sciences Paris*, 317:95–99, 1993.

[FHV94] Michael D. Fried, Dan Haran, and Helmut Völklein. Real Hilbertianity and the field of totally real numbers. In N. Childress and J. W. Jones, editors, *Arithmetic Geometry*, Contemporary Mathematics 174, pages 1–34. American Mathematical Society, 1994.

[FJ08] Michael D. Fried and Moshe Jarden. *Field Arithmetic*. Springer, third edition, 2008.

[GJ91] Wulf-Dieter Geyer and Moshe Jarden. The Henselian closures of a PpC field. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 61(1):63–71, 1991.

[GJ02] Wulf-Dieter Geyer and Moshe Jarden. PSC Galois extensions of Hilbertian fields. *Mathematische Nachrichten*, 236(1):119–160, 2002.

[GPR95] Barry Green, Florian Pop, and Peter Roquette. On Rumely's local-global principle. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 97(2):43–74, 1995.

[Gro87] Camilla Grob. *Die Entscheidbarkeit der Theorie der maximalen pseudo p-adisch abgeschlossenen Körper*. Dissertation, Konstanz, 1987.

[Har84] Dan Haran. The undecidability of pseudo real closed fields. *Manuscripta Mathematica*, 49:91–108, 1984.

[Har87] Dan Haran. On closed subgroups of free products of profinite groups. *Proceedings of the London Mathematical Society*, 55:266–298, 1987.

[HJP05] Dan Haran, Moshe Jarden, and Florian Pop. P-adically projective groups as absolute Galois groups. *International Mathematics Research Notices*, 32:1957–1995, 2005.

[HJP07] Dan Haran, Moshe Jarden, and Florian Pop. Projective group structures as absolute Galois structures with block approximation. *Memoirs of the American Mathematical Society*, 189(884), 2007. 56 pages.

[HJP09a] Dan Haran, Moshe Jarden, and Florian Pop. The absolute Galois group of subfields of the field of totally S-adic numbers. Manuscript, 2009.

[HJP09b] Dan Haran, Moshe Jarden, and Florian Pop. The absolute Galois group of the field of totally S-adic numbers. *Nagoya Mathematical Journal*, 194:91–147, 2009.

[HJP09c] Dan Haran, Moshe Jarden, and Florian Pop. The block approximation theorem. Manuscript, 2009.

[HL94] Dan Haran and Luc Lauwers. Galois stratification over e-fold ordered Frobenius fields. *Israel Journal of Mathematics*, 85:169–197, 1994.

[HP84] Bernhard Heinemann and Alexander Prestel. Fields regularly closed with respect to finitely many valuations and orderings. In C. R. Riehm and I. Hambleton, editors, *Quadratic and Hermitian Forms. 1983 Conference on Quadratic Forms and Hermitian K-Theory held at McMaster University, Hamilton, Ontario*, volume 4 of *Canadian Mathematical Society Conference Proceedings*, pages 297–336. American Mathematical Society, 1984.

[Jar69] Moshe Jarden. Rational points on algebraic varieties over large number fields. *Bulletin of the American Mathematical Society*, 75(3):603–606, 1969.

[Jar72] Moshe Jarden. Elementary statements over large algebraic fields. *Transactions of the American Mathematical Society*, 164:67–91, 1972.

[Jar74] Moshe Jarden. Algebraic extensions of finite corank of Hilbertian fields. *Israel Journal of Mathematics*, 18(3):279–307, 1974.

[Jar91] Moshe Jarden. Algebraic realization of p-adically projective groups. *Compositio Mathematica*, 79:21–62, 1991.

[Jar95] Moshe Jarden. Totally S-adic extensions of Hilbertian fields. Manuscript, 1995.

[Jar97] Moshe Jarden. Large normal extensions of Hilbertian fields. *Mathematische Zeitschrift*, 224:555–565, 1997.

[JK75] Moshe Jarden and Ursel Kiehne. The elementary theory of algebraic fields of finite corank. *Inventiones Mathematicae*, 30(3):275–294, 1975.

[JR79] Moshe Jarden and Jürgen Ritter. On the characterization of local fields by their absolute Galois groups. *Journal of Number Theory*, 11(1):1–13, 1979.

[JR98] Moshe Jarden and Aharon Razon. Rumely's local global principle for algebraic PSC fields over rings. *Transactions of the American Mathematical Society*, 350(1):55–85, 1998.

[JR01] Moshe Jarden and Aharon Razon. Skolem density problems over large Galois extensions of global fields (With an appendix by Wulf-Dieter Geyer). In Denef, Lipshitz, Pheidas, and van Geel, editors, *Proceedings of the workshop: Hilbert's 10'th problem, Relations with Arithmetic and Algebraic Geometry*, Contemporary Mathematics 270, pages 213–235. American Mathematical Society, 2001.

[Kec94] Alexander S. Kechris. *Classical Descriptive Set Theory*. Springer, 1994.

[Koe95] Jochen Koenigsmann. From p-rigid elements to valuations (with a Galois-characterization of p-adic fields). *Journal für die reine und angewandte Mathematik*, 465:165–182, 1995.

[Kün89a] Urs-Martin Künzi. Corps multiplement pseudo-p-adiquement clos. *Comptes Rendus de l'Académie des Sciences Paris, Série I*, 309:205–208, 1989.

[Kün89b] Urs-Martin Künzi. Decidable theories of pseudo-p-adic closed fields. *Algebra and Logic*, 28(6):421–438, 1989.

[Kün92] Urs-Martin Künzi. Multiply pseudo-p-adically closed fields. In L. A. Bokut, Yu L. Ershov, and A. I. Kostrikin, editors, *Proceedings of the International Conference on Algebra: Dedicated to the Memory of A. I. Malcev*, Contemporary Mathematics 131, pages 463–468. American Mathematical Society, 1992.

[Lan58] Serge Lang. *Introduction to Algebraic Geometry*. Interscience Publishers, 1958.

[Lan94] Serge Lang. *Algebraic Number Theory*. Springer, second edition, 1994.

[Lan02] Serge Lang. *Algebra*. Springer, third edition, 2002.

[Mar02] David Marker. *Model Theory: An Introduction*. Springer, 2002.

[MB89] Laurent Moret-Bailly. Groupes de Picard et problèmes de Skolem. II. *Annales scientifiques de l'École Normale Supérieure Série 4*, 22(2):181–194, 1989.

[Mel90] Oleg Vladimirovich Mel'nikov. Subgroups and homology of free products of profinite groups. *Math. USSR Izvestiya*, 34(1):97–119, 1990.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. Springer, second edition, 2008.

[Pop86] Florian Pop. *Galoissche Kennzeichnung p-adisch abgeschlossener Körper*. Dissertation, Heidelberg, 1986.

[Pop88] Florian Pop. Galoissche Kennzeichnung p-adisch abgeschlossener Körper. *Journal für die reine und angewandte Mathematik*, 392:145–175, 1988.

[Pop92] Florian Pop. Fields of totally Σ-adic numbers. Manuscript, 1992.

[Pop95] Florian Pop. On prosolvable subgroups of profinite free products and some applications. *Manuscripta Mathematica*, 86:125–135, 1995.

[Pop96] Florian Pop. Embedding problems over large fields. *Annals of Mathematics*, 144(1):1–34, 1996.

[Pop03] Florian Pop. Classically projective groups and pseudo classically closed fields. In F.-V. Kuhlmann, S. Kuhlmann, and M. Marshall, editors, *Valuation Theory and its Applications Vol. II. Fields Institute Communications*, pages 251–283. American Mathematical Society, 2003.

[PR84] Alexander Prestel and Peter Roquette. *Formally p-adic Fields*. Springer, 1984.

[Pre81] Alexander Prestel. Pseudo real closed fields. In R. B. Jensen and A. Prestel, editors, *Set Theory and Model Theory, Proceedings, Bonn 1979*, pages 127–156. Springer, 1981.

[Pre84] Alexander Prestel. *Lectures on Formally Real Fields*. Springer, 1984.

[Pre85] Alexander Prestel. On the axiomatization of PRC-fields. In C. A. Di Prisco, editor, *Methods in Mathematical Logic. Proceedings of the 6th Latin American Symposium on Mathematical Logic held in Caracas, Venezuela, August 1–6, 1983*, pages 351–359. Springer, 1985.

[Raz02] Aharon Razon. On the density property of PSC fields. *Mathematische Nachrichten*, 235(1):163–177, 2002.

[Rum80] Robert Scott Rumely. Undecidability and definability for the theory of global fields. *Transactions of the American Mathematical Society*, 262(1):195–217, 1980.

[RZ00] Luis Ribes and Pavel Zalesskii. *Profinite Groups*. Springer, 2000.

[Ser79] Jean-Pierre Serre. *Local Fields*. Springer, 1979.

[Shl07] Alexandra Shlapentokh. *Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields*. Cambridge University Press, 2007.

[SS70] Lynn Arthur Steen and J. Arthur Seebach, Jr. *Counterexamples in Topology*. Holt, Rinehart & Winston of Canada Ltd, 1970.

[vdD78] Lou van den Dries. *Model theory of fields*. Dissertation, University of Utrecht, 1978.