INAUGURAL – DISSERTATION

zur Erlangung der Doktorwürde der
Naturwissenschaftlich-Mathematischen Gesamtfakultät
der Ruprecht - Karls - Universität Heidelberg

vorgelegt von

Dipl.-Ing. Michael Wibmer

aus Untergaimberg

Tag der mündlichen Prüfung: 28.05.2010

Thema

Geometric Difference Galois Theory

Gutachter:	Prof. Dr. Bernd Heinrich Matzat
	Priv.-Doz. Dr. Michael Dettweiler

Abstract

This work presents a difference geometric approach to the strongly normal Galois theory of difference equations. In this approach, a system of ordinary difference equations is encoded in a difference extension, and the Galois groups are group schemes of finite type over the constants. The Galois groups need neither be linear nor reduced. The main result is a characterization of the extensions that admit a reasonable Galois theory by a normality property. This approach has been inspired by the recent work of J. Kovacic on the differential Galois theory of strongly normal extensions.

Zusammenfassung

Die vorliegende Arbeit entwickelt eine Galoistheorie für Differenzengleichungen basierend auf differenzenalgebraischer Geometrie. Hierbei wird ein System von gewöhnlichen Differenzengleichungen durch eine Differenzenerweiterung beschrieben, und die Galoisgruppen sind Gruppenschemata vom endlichen Typ über den Konstanten. Die Galoisgruppen müssen weder linear noch reduziert sein. Das Hauptresultat ist eine Charakterisierung jener Differenzenerweiterungen, die eine gutartige Galoistheorie zulassen, durch eine Normalitätseigenschaft. Inspiration für diesen Zugang war die Arbeit von J. Kovacic über die Galoistheorie von stark normalen Differentialerweiterungen.

Introduction

The present work develops a Galois theory for difference equations, or more specifically for difference extensions. As in the classical Galois theory of algebraic equations, one does not have a good Galois theory for arbitrary algebraic equations or arbitrary field extensions. The theory rather only applies to a very special class of field extensions, namely the ones that are Galois.

The main topic of this work is to find a reasonable difference analog of this Galois property. That is, we want to define and study difference Galois extension. In search of an adequate definition of "difference Galois", it seems a good idea to reflect on the classical case. For a finite field extension $L|K$, the following four statements are equivalent to "$L|K$ is Galois".

(1) $L|K$ is separable, and for any field extension $M|K$ and K-morphisms $\sigma_s, \sigma_t : L \to M$ we have $\sigma_t(L) \subset \sigma_s(L)$.

(2) For any K-algebra M and K-morphisms $\sigma_s, \sigma_t : L \to M$ we have $\sigma_t(L) \subset \sigma_s(L)M^X$. Here, M^X denotes the set of idempotent elements of M [1] and $\sigma_s(L)M^X$ denotes the smallest subring of M containing $\sigma_s(L)$ and M^X.

(3) For $M = L \otimes_K L$, $\sigma_s : L \to M,\ a \mapsto a \otimes 1$ and $\sigma_t : L \to M,\ a \mapsto 1 \otimes a$ we have $\sigma_t(L) \subset \sigma_s(L)M^X$.

(4) L splits over itself, i.e. $\operatorname{Spec}(L \otimes_K L)$ is a (finite) set of L-rational points.

This leads to the following difference analogues for a difference extension $L|K$:

(1) For any difference extension $M|K$ and K-ϕ-morphisms $\sigma_s, \sigma_t : L \to M$ we have $\sigma_t(L) \subset \sigma_s(L)M^\phi$. Here, M^ϕ denotes the constants of M with respect to the endomorphism ϕ that defines the difference structure on M.

(2) For any K-ϕ-algebra M and K-ϕ-morphisms $\sigma_s, \sigma_t : L \to M$ we have $\sigma_t(L) \subset \sigma_s(L)M^\phi$.

(3a) For $M = L \otimes_K L$ and $\sigma_s : L \to M,\ a \mapsto a \otimes 1$ and $\sigma_t : L \to M,\ a \mapsto 1 \otimes a$ we have $\sigma_t(L) \subset \sigma_s(L)M^\phi$.

(3b) There exists a difference overring M of $L \otimes_K L$ with $M = K(L \otimes_K L)$ such that for $\sigma_s : L \to M,\ a \mapsto a \otimes 1$ and $\sigma_t : L \to M,\ a \mapsto 1 \otimes a$ we have $\sigma_t(L) \subset \sigma_s(L)M^\phi$.

(4) ϕ-$\operatorname{Spec}(L \otimes_K L)$ is split over L. I.e. there exists a scheme $\mathcal{G}$ (of finite type) over the constants $C = L^\phi = K^\phi$ such that ϕ-$\operatorname{Spec}(L \otimes_K L) \simeq L \times_C \mathcal{G}$.

[1] With a little fantasy one can interpret the idempotent elements of M as the constants under the operator X corresponding to the variable in an algebraic equation. The analogy in point (4) can also be made more apparent using the somewhat mysterious field with one element: We have $\operatorname{Spec}(L \otimes_K L) = L \times_{\mathbb{F}_1} G$ where G denotes the Galois group of $L|K$.

It is not at all clear whether the above difference analogs are also equivalent. We will explore the relations between them.

From the equational point of view, very roughly speaking, our Galois theory applies to systems of algebraic difference equations whose solutions can be parametrized by constants (via a superposition law). For example, if Y is a fundamental solution matrix of a first order system of difference equations given by an invertible matrix, then the fundamental linear superposition principle tells us that any further solution is given as a linear combination of the columns of Y with constant coefficients. Therefore, Picard-Vessiot extensions are examples of our ϕ-Galois extensions. The Galois theory of linear difference equations (also known as Picard-Vessiot theory) is well studied and to a certain extent well understood. In [43], M. van der Put and M. Singer showed that the linear theory runs much smoother if one abandons the world of fields and allows zero divisors into the solution rings. Instead of ϕ-fields one uses finite direct products of fields where the factors are permuted in a cyclic way by ϕ. Let's agree to call such difference rings ϕ-pseudo fields. [2]

Maybe the difference Galois theory that we will present here is best described as the geometric completion of Picard-Vessiot theory. (Hence the "Geometric" in the title.) Conversely, Picard-Vessiot theory can be interpreted as the "affine case" of our difference Galois theory. As it is often more comfortable to work directly with rings than with affine schemes, the geometric point of view is usually lost in Picard-Vessiot theory.

One of the main difficulties in developing a difference (or differential) Galois theory is to make precise sense of the vague idea that the Galois group is an algebraic group. After all, it seems that it was precisely this problem that lead E. Kolchin to the introduction of his axiomatic algebraic groups. We will not follow his path. The modern language of schemes and functors provides a very clear way to formulate the problem and its solution. We simply have to define an appropriate automorphism functor and show that it is representable by an algebraic group. So let $L|K$ be an extension of ϕ-pseudo fields with no new constants and set $C = K^\phi = L^\phi$. We define $\operatorname{Gal}(L|K)$ to be the functor from the category of schemes of finite type over C to the category of groups that assigns to a scheme Y the automorphisms of $L \times_C Y$ over $K \times_C Y$. One has to exercise some care here and specify what kind of object $L \times_C Y$ should be. The answer is: a difference scheme. And this answer leads directly to the more basic question: What kind of geometry should form the basis of our *geometric* difference Galois theory?

The classical language of difference algebraic geometry as developed in [10] does not seem adequate. For example, it can not handle nilpotent elements in the structure sheaf, which are essential for the construction and understanding of non-reduced Galois groups. On the other hand, the theory of difference schemes is still in its infancy.

In principle, it seems possible to develop a difference Galois theory by using usual schemes with an endomorphism and rational maps that commute with the endomor-

[2] The keen reader might have noticed that until this point we have been talking somewhat imprecisely about difference extensions. What we actually meant was "extension of ϕ-pseudo fields".

phism (cf. [41], [5] or [23]). However, this has the drawback that one needs to choose models (of the involved field extensions). And then also the Galois group is at first only available birationally. However one can then use a theorem of A. Weil about birational group laws ("Group chunks") to produce the Galois group as algebraic group out of the hat.

It is very easy to construct the Galois group up to birational isomorphisms, because the ring of rational functions on the Galois group will be isomorphic to the constants of the total quotient ring of $L \otimes_K L$. It was clear to E. Kolchin that the Galois groups of strongly normal differential extensions are honest algebraic groups (see e.g. [23]), but it seems that due to the lack of a simple direct construction of this algebraic group structure he preferred to axiomatize the notion of algebraic group. The usage of Weil's theorem does not seem very fortunate from a didactical point of view and one could argue that it does not canonically define the Galois group variety (as a set). Now the ingenious observation of J. Kovacic [26] was that one needs to take the constants of $L \otimes_K L$ in a *geometric* way to directly obtain the Galois group as group scheme. So it is a very simple matter to define the Galois group scheme $\mathcal{G}$ as a locally ringed space, namely $\mathcal{G} = (\phi\text{-Spec}(L \otimes_K L))^\phi$. But now the really hard part is to prove that $\mathcal{G}$ is in fact a scheme.

A very convenient fact about difference schemes is that on the one hand the category of schemes is a full subcategory and on the other hand we can also think of varieties up to birational isomorphisms together with a dominant rational map as being embedded into difference schemes because the ϕ-spectrum of the function field precisely encapsulates these data.

As indicated above, one might argue that difference schemes could be avoided in the development of our difference Galois theory. But I believe that difference algebra deserves a geometry of its own and the fact that the language of difference/differential schemes is so amazingly well suited for addressing the problems of difference/differential Galois theory should be seen as an indication in favor of difference/differential schemes. Finally, as difference algebraic geometry is more than just adding an endomorphism to usual algebraic geometry, I think this is also the most interesting way to go.

In his fascinating article [18], E. Hrushovski develops the notions of difference algebraic geometry in scheme theoretic language to a quite advanced degree, but unfortunately his definitions and results only apply well for so called well-mixed difference rings. A Picard-Vessiot ring is typically not well-mixed and as our Galois theory should generalize the Picard-Vessiot theory, we need to modify Hrushovski's approach. I hope that these "modifications" will also be useful in other difference algebraic problems.

It is of course a very basic question, for which extensions $L|K$ of ϕ-pseudo fields the functor $\mathrm{Gal}(L|K)$ is representable. If it is representable by a group scheme $\mathcal{G}$ over $C = K^\phi = L^\phi$, then by a straightforward general nonsense construction one obtains a K-linear action of $\mathcal{G}$ on $Z = \phi\text{-Spec}(L)$.

The main result of the present work is a characterization of those extensions $L|K$ of ϕ-pseudo fields that admit a reasonable Galois theory with algebraic groups as Galois groups. (See Theorem 3.9.3 for more details.)

Theorem. *Let $L|K$ be an extension of ϕ-pseudo fields satisfying some mild technical conditions. Then the following three statements are equivalent.*

1. *The functor* $\operatorname{Gal}(L|K)$ *is representable by a group scheme $\mathcal{G}$ and $Z = \phi\text{-}\operatorname{Spec}(L)$ is a $\mathcal{G}$-torsor.*

2. *$\phi\text{-}\operatorname{Spec}(L \otimes_K L)$ is split, i.e. there exists a scheme $\mathcal{G}$ of finite type over the constants $C = L^\phi = K^\phi$ such that $\phi\text{-}\operatorname{Spec}(L \otimes_K L) \simeq L \times_C \mathcal{G}$.*

3. *$L|K$ is ϕ-Galois, i.e. $L|K$ satisfies conditions (1) and (3b) above.*

With the above theorem in hand, it is then a short way to the Galois correspondence. I would like to stress the point that the Galois groups here are group schemes of finite type over the constants with no further a priori restrictions. In particular, they need not be affine or reduced.

One can find two approaches to a Galois theory of difference extensions with not necessarily affine Galois groups in the periodical literature. One is by R. Infante ([20], [19]) and the other one by A. Bialynicki-Birula ([5]) and H. F. Kreimer ([28]). Bialynicki-Birula considers fields with differential and difference operators and Kreimer considers even more general operators, but if one focuses on the difference case their theories agree and so we will only refer to Bialynicki-Birula in what follows.

From a technical point of view, I have made an effort to avoid unnecessarily restrictive assumptions. In comparison with the works of Infante and Bialynicki-Birula this concerns the following issues.

Infante and Bialynicki-Birula, only consider field extensions. But as demonstrated in [43], it is in general advantageous to work with ϕ-pseudo fields. In fact, in [43] the base K is always assumed to be a field and only the extension L is allowed to be a ϕ-pseudo field. But if M is an intermediate ϕ-pseudo field of $L|K$, then M need not be a field and it is a little awkward not to be able to say that $L|M$ is Picard-Vessiot. It adds only little difficulty to also allow the base K to be a ϕ-pseudo field. The approach to Picard-Vessiot theory in [2] is also based on pseudo fields rather than fields. However, the idea of replacing ϕ-fields with ϕ-pseudo fields is also part of a bigger philosophy that governs our approach to difference algebraic geometry.

Both Infante and Bialynicki-Birula only consider inversive ϕ-fields, i.e. ϕ is assumed to be an automorphism. We will not make this assumption. (However, ϕ is automatically injective on a ϕ-pseudo field.) This keeps the theory open for applications to Mahler-equations and Frobenius modules when non-perfect fields are involved.

In addition, Infante and Bialynicki-Birula need to make the assumption that K is relatively algebraically closed in L. Therefore, they only obtain connected Galois groups. They also assume that L is separable over K (Infante works only in characteristic zero) and therefore they only obtain reduced Galois groups.

We will not make these assumptions, thus the restrictions on the group side will also disappear. Finally, Bialynicki-Birula only worked with algebraically closed constants. We do not make this assumption, but it requires some extra work to avoid it.

Nevertheless, I believe that the main advantage of the approach presented here compared to the earlier works of Infante and Bialynicki-Birula lies in the direct construction of the Galois group as group scheme, the usage of representable functors and the language of difference schemes. The groups used by Infante were Kolchin's axiomatic algebraic groups, and Bialynicki-Birula used Weil's theorem to produce the Galois group as algebraic group.

Recently, two approaches to difference Galois theory that apply in much more general situations have emerged. One was developed by G. Casale based on ideas of B. Malgrange in a more analytic setting and one by H. Umemura and his followers in a more algebraic context. As these theories apply to more general types of equations the group-like objects are much more sophisticated. The reason why a Galois theory with algebraic groups as Galois groups is still interesting is that in a less general setting one can obtain stronger results. If one encounters an equation that admits an algebraic group as Galois group one should better make use of this fact.

Finally, I would like to point out that the main inspiration for the present paper was the beautiful recent work of J. Kovacic on the differential Galois theory of strongly normal extensions ([26], [27]).

As it seems somewhat tiresome, I do not always give a reference to a differential analog of a specific result in all cases possible. In general, it can be said that most difference theoretic results in this work do have differential analogs. Almost all of them can be found in [26] or [27]. There are also some constructions (e.g. the usage of representable functors in Section 3.2 or the issue of non-reduced Galois groups coupled with a slight modification of the strongly normal property) for which the differential analog is currently not available but it seems very natural to believe that it is true.

We conclude this introduction with a short overview of the different chapters. This work is divided into three chapters:

1 Some commutative ϕ-algebra
2 ϕ-algebraic geometry
3 ϕ-Galois theory

The first two chapters are of a preparatory nature. The main results are presented in Chapter 3. Thus, to understand the motivations behind the preparatory results, it might be a good idea for the reader to start with Chapter 3 (maybe even with Section 3.2) and to refer back to the earlier results and definitions whenever needed. (There is an index at the end.)

Chapter 1 contains some elementary difference algebraic results that were not available or not available in an appropriate form in the literature. The main point is that we systematically use ϕ-pseudo fields instead of ϕ-fields. For example, ϕ-pseudo fields lead to what we will call ϕ-prime ideals (whereas ϕ-fields would lead to reflexive prime ideals). We also introduce the concepts of ϕ-separability and bounded periodicity.

Chapter 2 contains the rudiments of a difference algebraic geometry based on ϕ-pseudo fields instead of ϕ-fields. This approach still holds many open problems and we are far from a well-established theory. Nevertheless, the results of Chapter 2, which are aimed at the application to ϕ-Galois theory, are sufficient for our needs in Chapter 3.

Finally, Chapter 3 contains the theory of ϕ-Galois extensions. The first section in Chapter 3 is concerned with a kind of Galois theory for arbitrary extensions of ϕ-pseudo fields. Following [2], we give a difference version of the Sweedler correspondence ([38]). However we use a more geometric formulation, replacing coideals with subgroupoids.

Section 3.2 proposes a rather conceptual approach to the Galois theory, emphasizing the use of representable functors and torsors (principal homogeneous spaces) (cf. [36]). Section 3.3 introduces the normality conditions akin to Kolchin's "strong normality" and the definition of ϕ-Galois extensions. Section 3.4 proves a very basic lemma, which seems inevitable for the approach presented here. Unfortunately, it has a somewhat intricate proof. Section 3.5 gives two applications of this basic lemma which bring us closer to the big goal of proving that ϕ-Spec$(L \otimes_K L)$ is split for every ϕ-Galois extension $L|K$. This goal is then achieved in Section 3.6 under the assumption that the constants are algebraically closed. The restriction of algebraically closed constants is then removed in Sections 3.7 and 3.8 by employing descent techniques. In Section 3.9 we present the main theorem (the theorem above) in its final form. Finally, we conclude with the Galois correspondence and some examples.

It is my pleasure to thank all the people who accompanied me on the way to the completion of this thesis, in particular Prof. B. H. Matzat, the members of the Algorithmic Algebra research group in Heidelberg and the people who worked with me during my research visits in Barcelona and Paris. I am especially thankful to A. Maurischat for proofreading the manuscript.

Contents

Notation and Conventions:

The following conventions will be in force throughout the whole text. All rings and algebras are commutative with unit. A difference ring (or ϕ-ring for short) is a ring R together with an ring endomorphism $\phi : R \to R$. For $r \in R$ we define $r^0 = 1$ and $\phi^0(r) = r$. If S is a subset of R and $n \geq 0$ an integer then $\phi^{-n}(S) = \{r \in R;\ \phi^n(r) \in S\}$.

A morphism of ϕ-rings is a morphism of rings that commutes with ϕ. If $K \to R$ is a morphism of ϕ-rings we also say that R is a K-ϕ-algebra. If R is a K-ϕ-algebra and S a subset of R then $K\{S\}$ denotes the smallest K-ϕ-subalgebra of R that contains S. If R and R' are K-ϕ-algebras then we consider $R \otimes_K R'$ as ϕ-ring by setting $\phi(r \otimes r') = \phi(r) \otimes \phi(r')$.

A subset S of R is called ϕ-stable if $\phi(S) \subset S$. If S is a multiplicatively closed ϕ-stable subset of R then we consider $S^{-1}R$ as ϕ-ring by $\phi(\frac{r}{s}) = \frac{\phi(r)}{\phi(s)}$. If $r \in R$ we denote with $\langle \phi, r \rangle$ the smallest multiplicatively closed and ϕ-stable subset of R that contains r. Explicitly the elements of $\langle \phi, r \rangle$ are of the form

$$\phi^{\alpha_1}(r)^{\beta_1} \cdots \phi^{\alpha_n}(r)^{\beta_n}$$

with $\alpha_i, \beta_i \geq 0$. We denote with $R_{\langle \phi, r \rangle}$ the ϕ-ring $\langle \phi, r \rangle^{-1}R$.

If $\mathfrak{a}$ is an ideal of R that is stable under ϕ then $R/\mathfrak{a}$ is a ϕ-ring by $\phi(\overline{r}) = \overline{\phi(r)}$.

An ideal of a ring is called proper if it is not the whole ring. It is called trivial if it zero or the whole ring.

A ring is called total if every non zero divisor is invertible. If R is a ring then $\mathfrak{Q}(R)$ denotes the total quotient ring of R.

If R_1, R_2 are subrings of a ring R we write $R_1 \cdot R_2$ for the smallest subring of R containing R_1 and R_2. (Thus $R_1 \cdot R_2$ consists of all sums of products of elements of R_1 and R_2.) We write R_1R_2 for the smallest subring of R containing R_1 and R_2 with the property that every element of R_1R_2 which is invertible in R is also invertible in R_1R_2. Explicitly the elements of R_1R_2 are of the form ab^{-1} where $a, b \in R_1 \cdot R_2$ and $b \in R^\times$. (If R, R_1, R_2 are fields then R_1R_2 is the field compositum.)

The cardinality of a set S is denoted by $|S|$.

Chapter 1

Some commutative ϕ-algebra

This chapter is a collection of elementary difference algebraic results that are typically not (or not in a form appropriate for us) available in the literature. This chapter also contains some basic definitions (like ϕ-pseudo field, ϕ-prime ideal, ...) that will be of fundamental importance later on. Nevertheless it might be advantageous for the reader to start with Chapter 3 and to refer back to the earlier chapters whenever needed.

1.1 ϕ-simple rings

For the convenience of the reader we start with recalling some basic definitions from difference algebra. The standard references for difference algebra are [10] and [29].

A *difference ring* or *ϕ-ring* for short is a pair (R, ϕ) consisting of a ring R (commutative as always) and a ring endomorphism $\phi : R \to R$. We deliberately do not make the assumption that ϕ is injective which is often present in the literature. A difference ring is called *inversive* if ϕ is an automorphism. We often suppress the ϕ in the notation and simply use R to denote a difference ring. All the usual terminology of commutative algebra applies to difference structures by applying it to the underlying algebraic structure. E.g. a Noetherian difference ring is a difference ring (R, ϕ) whose underlying ring R is Noetherian. Properties relating to the difference structure will usually be prefixed with "ϕ-". E.g. a ϕ-Noetherian difference ring would be a difference ring such that every strictly increasing chain of difference ideals is finite. By the way a *difference ideal* or *ϕ-ideal* for short is an ideal $\mathfrak{a}$ of R such that $\phi(\mathfrak{a}) \subset \mathfrak{a}$.

If R is a ϕ-ring then

$$R^\phi = \{r \in R;\ \phi(r) = r\}$$

denotes the *ring of constants* of R. A difference ring is called *ϕ-simple* if it has no non-trivial ϕ-ideals. (The trivial ideals are (0) and R.) We have the following simple lemma (cf. [43, Lemma 1.7, p. 6]).

Lemma 1.1.1. *Let R be a ϕ-simple ϕ-ring. Then R is reduced, $\phi : R \to R$ is injective and R^ϕ is a field.*

Proof: For $r \in R$ with $r^n = 0$ we see that $\phi(r)^n = 0$. So the nilradical of R is a ϕ-ideal and thus must be zero. Similarly the kernel of ϕ is a ϕ-ideal and so also must be zero. If $c \in R^\phi \smallsetminus \{0\}$ then $(c) \subset R$ is a non-zero ϕ-ideal and thus must be equal to R. This means that c is a unit of R. Applying ϕ to $cc^{-1} = 1$ gives $c\phi(c^{-1}) = 1$. Consequently $c^{-1} \in R^\phi$, i.e. R^ϕ is a field. □

The following proposition reveals a fundamental difference between difference and differential algebra: A simple differential ring is an integral domain (See [44, Lemma 1.17, p. 13] for the case of Ritt algebras and [31, Proposition 3.2, p. 21] for the general case using iterative derivations.) but a simple difference ring may well have zero divisors. A statement similar to the proposition below can be found in [43, Corollary 1.16, p. 12].

Proposition 1.1.2. *Let R be a ϕ-simple ϕ-ring with only finitely many minimal prime ideals (e.g. R is Noetherian). Then there exist orthogonal idempotent elements $e_1, \dots, e_t$ of R such that*

(1) $R = e_1R \oplus \cdots \oplus e_tR$,

(2) $\phi(e_i) = e_{i+1}$ *for* $i = 1, \dots, t-1$ *and* $\phi(e_t) = e_1$ *(in particular e_iR is a ϕ^t-ring for $i = 1, \dots, t$),*

(3) *the ring e_iR is an integral domain and ϕ^t-simple for $i = 1, \dots, t$.*

Proof: Let $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ denote the minimal prime ideals of R. Since R is reduced (Lemma 1.1.1) we have

$$\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_t = 0.$$

From the injectivity of ϕ (Lemma 1.1.1) it follows that also

$$\phi^{-1}(\mathfrak{p}_1) \cap \cdots \cap \phi^{-1}(\mathfrak{p}_t) = 0.$$

Because of the uniqueness of such a decomposition we see that ϕ^{-1} induces a permutation of the minimal prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_t$. Let $d \in \mathbb{N}$ be minimal with the property that $\phi^{-(d+1)}(\mathfrak{p}_t) = \mathfrak{p}_t$. Then

$$\mathfrak{p}_t \cap \phi^{-1}(\mathfrak{p}_t) \cap \cdots \cap \phi^{-d}(\mathfrak{p}_t)$$

is a ϕ-ideal of R which must be zero by the ϕ-simplicity of R. This shows that the permutation induced by ϕ^{-1} is a cycle of length t. So after a suitable renumbering of the minimal prime ideals we can assume that $\phi^{-1}(\mathfrak{p}_{i+1}) = \mathfrak{p}_i$ for $i = 1, \dots, t$ where $\mathfrak{p}_{t+1} := \mathfrak{p}_1$.

Next we will show that $R/\mathfrak{p}_i$ is ϕ^t-simple for $i = 1, \dots, t$. For this it suffices to show that $\mathfrak{p}_i$ is a ϕ^t-maximal ideal. So let $I \subset R$ be a proper ϕ^t-ideal with $\mathfrak{p}_i \subset I$. Since

$$J := I \cap \phi^{-1}(I) \cap \cdots \cap \phi^{-(t-1)}(I) \subset R$$

is a ϕ-ideal it must be zero, in particular $J \subset \mathfrak{p}_i$. Since $\mathfrak{p}_i$ is prime this implies that there exist $j \in \{0, \ldots, t-1\}$ with $\phi^{-j}(I) \subset \mathfrak{p}_i$. But as $\mathfrak{p}_i \subset I$ we have $\phi^{-j}(\mathfrak{p}_i) \subset \phi^{-j}(I) \subset \mathfrak{p}_i$. Hence $\phi^{-j}(\mathfrak{p}_i) = \mathfrak{p}_i$ and thus $j = 0$, i.e. $I \subset \mathfrak{p}_i$.

It remains to prove that the canonical map

$$R \to R/\mathfrak{p}_1 \times \cdots \times R/\mathfrak{p}_t$$

is an isomorphism. The injectivity is obvious from $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_t = 0$. For the surjectivity it suffices to check the hypothesis of the Chinese remainder theorem. But for $i \neq j$ the ideal $\mathfrak{p}_i + \mathfrak{p}_j \subset R$ is a ϕ^t-ideal of R properly containing $\mathfrak{p}_i$. Thus it follows from the ϕ^t-maximality of $\mathfrak{p}_i$ that $\mathfrak{p}_i + \mathfrak{p}_j = R$. □

Remark 1.1.3. *There is a converse to Proposition 1.1.2. Namely, if R is a ϕ-ring and $e_1, \ldots, e_t$ are orthogonal idempotent elements of R such that* (1), (2) *and* (3) *are satisfied then R is ϕ-simple and has only finitely many minimal prime ideals.*

Since we shall not need this result we omit the easy proof. The following Lemma guarantees that one can always extend ϕ from a ϕ-simple ring to its total ring of quotients.

Lemma 1.1.4. *Let R be a ϕ-simple ϕ-ring. Then ϕ maps non zero divisors to non zero divisors and if $r \in R$ is a zero divisor then there exists $m \geq 0$ such that*

$$r\phi(r)\phi^2(r)\cdots\phi^m(r) = 0$$

and $\phi(r)\phi^2(r)\cdots\phi^m(r) \neq 0$.

Proof: Let $r \in R \smallsetminus \{0\}$. The set S of all elements of R which are of the form

$$r^{i_0}\phi(r)^{i_1}\phi^2(r)^{i_2}\cdots\phi^m(r)^{i_m}$$

for some $m \geq 0$ and $i_0, \ldots, i_m \geq 0$ is a multiplicatively closed ϕ-stable subset of R. Thus $S^{-1}R$ becomes naturally a ϕ-ring and the canonical map $\psi : R \to S^{-1}R$ is a morphism of ϕ-rings, and so the kernel of ψ is a ϕ-ideal. Since R is ϕ-simple there are two possibilities: either the kernel is equal to zero or it is equal to R.

First we treat the case that r is a non zero divisor: Suppose that $\phi(r)$ is a zero divisor of R, then there exists $r' \in R \smallsetminus \{0\}$ with $\phi(r)r' = 0$. By definition of the localization $S^{-1}R$ we see that r' lies in the kernel of ψ. Thus the kernel of ψ must be all of R, which means that $S^{-1}R$ is the zero ring and this is equivalent to $0 \in S$. In other words, there exists $m \geq 0$ and $i_0, \ldots, i_m \geq 0$ such that $r^{i_0}\phi(r)^{i_1}\phi^2(r)^{i_2}\cdots\phi^m(r)^{i_m} = 0$. Multiplying with appropriate elements we see that

$$\left(r\phi(r)\phi^2(r)\cdots\phi^m(r)\right)^i = 0$$

for some $i \geq 0$. Since R is reduced (Lemma 1.1.1) we see that $r\phi(r)\phi^2(r)\cdots\phi^m(r) = 0$. Now let $m \geq 0$ be minimal with this property. If

$$\phi(r)\phi^2(r)\cdots\phi^m(r) = \phi(r\phi(r)\cdots\phi^{m-1}(r))$$

would be zero then by the injectivity of ϕ also $r\phi(r)\cdots\phi^{m-1}(r)$ would be zero – contradicting the minimality of m. Thus $\phi(r)\phi^2(r)\cdots\phi^m(r) \neq 0$ and so – in contradiction to our assumption – r is a zero divisor.

Now we treat the case that r is a zero divisor. As above this implies that the kernel of ψ is non-zero and analogously we obtain the existence of an $m \geq 0$ such that $r\phi(r)\phi^2(r)\cdots\phi^m(r) = 0$. □

Lemma 1.1.5. *Let R be a ϕ-simple ϕ-ring. Then ϕ extends to $\mathfrak{Q}(R)$, the total ring of quotients of R and $\mathfrak{Q}(R)^\phi = R^\phi$.*

Proof: By Lemma 1.1.4 we can extend ϕ to $\mathfrak{Q}(R)$. Let $a \in \mathfrak{Q}(R)^\phi$ then $\mathfrak{a} = \{r \in R;\ ra \in R\}$ is a non-zero ϕ-ideal of R. Thus $1 \in \mathfrak{a}$, i.e. $a \in R^\phi$. □

The following basic lemma will be used several times later on. A related statement can be found in [2, Corollary 3.2, p. 753].

Lemma 1.1.6. *Let $K \subset R$ be an inclusion of ϕ-rings such that K is ϕ-simple. Then K and R^ϕ are linearly disjoint over K^ϕ.*

Proof by contradiction: Let $n \geq 1$ be minimal such that there exist $c_1, \ldots, c_n \in R^\phi$ which are K^ϕ-linearly independent but K-linearly dependent. Then

$$\mathfrak{a} = \{a_1 \in K;\ \exists\ a_2, \ldots, a_n \in K \text{ such that } a_1c_1 + \cdots + a_nc_n = 0\}$$

is a non-zero ϕ-ideal of K. Thus $1 \in \mathfrak{a}$ and we can find $a_2, \ldots, a_n \in K$ such that

$$c_1 + a_2c_2 + \cdots + a_nc_n = 0. \tag{1.1}$$

Applying ϕ to the above equation and subtracting yields

$$(a_2 - \phi(a_2))c_2 + \cdots + (a_n - \phi(a_n))c_n = 0.$$

By the minimality of n the a_i's must be constant. But then equation (1.1) contradicts the K^ϕ-linear independence of the c_i's. □

1.2 Total ϕ-rings

Following [43, Definition 1.22, p. 16] and [2, Corollary 2.5, p. 750] we make the following definition.

Definition 1.2.1. *A ring is called* total *if every non zero divisor is invertible.*

If R is a ring then $\mathfrak{Q}(R)$ will denote its total ring of fractions, i.e. $\mathfrak{Q}(R)$ is the localization of R at the multiplicatively closed subset of non zero divisors. Of course $\mathfrak{Q}(R)$ is a total ring.

Definition 1.2.2. *Let K be a total ring, R a ring containing K and S a subset of R. We denote with $K(S)$ the smallest subring of R which contains K and S and is closed under inverses, i.e. $r \in R^\times$ and $r \in K(S)$ implies $r^{-1} \in K(S)$.*

Explicitly the elements of $K(S)$ are of the form

$$\frac{P(a_1, \dots, a_n)}{Q(b_1, \dots, b_m)}$$

where $a_1, \dots, a_n, b_1, \dots, b_m$ are elements of S and P, Q polynomials with coefficients in K such that $Q(b_1, \dots, b_m)$ is invertible in R.

Definition 1.2.3. *Let $K \subset L$ be an inclusion of total rings. We say that L is finitely generated as total ring over K if there exists a finite subset S of L such that $L = K(S)$.*

Lemma 1.2.4. *Let $K \subset L$ be an inclusion of total rings such that K is Noetherian and L is finitely generated as total ring over K then $L \otimes_K L$ is Noetherian.*

Proof: Suppose that $a_1, \dots, a_n \in L$ generates L as total ring over K. Let A denote the K-subalgebra of $L \otimes_K L$ generated by $a_1 \otimes 1, \dots, a_n \otimes 1$ and $1 \otimes a_1, \dots, 1 \otimes a_n$. Let $S \subset A$ denote the set of all elements of the form $a \otimes b$ where $a, b \in K[a_1, \dots, a_n] \subset L$ are non zero divisors in L. Clearly S is a multiplicatively closed subset of A and every element of S is invertible in $L \otimes_K L$. Thus there is a canonical surjective mapping

$$S^{-1}A \to L \otimes_K L.$$

Since $S^{-1}A$ is Noetherian also $L \otimes_K L$ must be Noetherian. □

If $K \subset L$ is an inclusion of differential fields such that L is finitely generated as field extension of K then it is easy to see that there exists an affine differential model of $L|K$, i.e. there is a finitely generated K-subalgebra of L which is stable under the derivation and whose quotient field equals L (see [41, Lemma 1.5, p. 7]). The analogous statement for extensions of difference fields is not quite true. It seems the following lemma and its two corollaries (Corollary 1.2.6 and 1.3.3) is the best we can do.

Lemma 1.2.5. *Let $K \subset L$ be an inclusion of total ϕ-rings and $\eta \in L^n$ such that $L = K(\eta)$. Assume that*

$$\phi(\eta_i) = \frac{P_i}{Q}$$

for $i = 1, \dots, n$ with $P_i \in K[\eta]$ and $Q \in K[\eta] \cap L^\times$. Then for every $P \in K\{\eta, \frac{1}{Q}\}$ there exists $u \in K\{\eta, \frac{1}{Q}\}^\times$ with $uP \in K[\eta]$.

Proof: We first observe that

$$K\left\{\eta, \frac{1}{Q}\right\} = K\left[\eta, \frac{1}{Q}, \frac{1}{\phi(Q)}, \dots\right]$$

because the right hand side is a ϕ-ring.

Next we show by induction on $i \geq 0$ that $\phi^i(Q) \in K\left[\eta, \frac{1}{Q}, \dots, \frac{1}{\phi^{i-1}(Q)}\right]$. The case $i = 0$ being trivial we assume $\phi^{i-1}(Q) \in K\left[\eta, \frac{1}{Q}, \dots, \frac{1}{\phi^{i-2}(Q)}\right]$. Thus $\phi^{i-1}(Q)$ is a finite sum of elements of the form

$$a\frac{\eta_1^{\beta_1} \cdots \eta_n^{\beta_n}}{Q^{\alpha_0} \cdots \phi^{i-2}(Q)^{\alpha_{i-2}}}$$

where $a \in K$. Therefore $\phi^i(Q)$ is a sum of terms of the form

$$\phi(a)\frac{\phi(\eta_1)^{\beta_1} \cdots \phi(\eta_n)^{\beta_n}}{\phi(Q)^{\alpha_0} \cdots \phi^{i-1}(Q)^{\alpha_{i-2}}} = \phi(a)\frac{P_1^{\beta_1} \cdots P_n^{\beta_n}}{Q^{\beta_1} \cdots Q^{\beta_n}\phi(Q)^{\alpha_0} \cdots \phi^{i-1}(Q)^{\alpha_{i-2}}}$$

and so $\phi^i(Q) \in K\left[\eta, \frac{1}{Q}, \dots, \frac{1}{\phi^{i-1}(Q)}\right]$.

Next we show by induction on i that for every $i \geq 0$ there exists $u_i \in K[\eta] \cap K\{\eta, \frac{1}{Q}\}^\times$ such that $u_i\phi^i(Q) \in K[\eta]$. Again, the case $i = 0$ being trivial we assume that there exists $u_{i-1} \in K[\eta] \cap K\{\eta, \frac{1}{Q}\}^\times$ such that $u_{i-1}\phi^{i-1}(Q) \in K[\eta]$. Note that for $R \in K[\eta]$ one has $\phi(R) = \frac{P}{Q^m}$ for some $P \in K[\eta]$ and $m \geq 0$. Consequently $\phi(u_{i-1})\phi^i(Q) = \frac{P}{Q^m}$ and $\phi(u_{i-1}) = \frac{P'}{Q^{m'}}$ for some $P, P' \in K[\eta]$ and $m, m' \geq 0$. This gives

$$Q^m P'\phi^i(Q) = PQ^{m'} \in K[\eta].$$

Because $u_{i-1} \in K\{\eta, \frac{1}{Q}\}^\times$ also $\phi(u_{i-1}) = \frac{P'}{Q^{m'}} \in K\{\eta, \frac{1}{Q}\}^\times$. And this gives $P' \in K\{\eta, \frac{1}{Q}\}^\times$ which implies $Q^mP' \in K\{\eta, \frac{1}{Q}\}^\times$. Therefore we can take $u_i = Q^mP'$.

Because $u_i\phi^i(Q) \in K[\eta] \cap K\{\eta, \frac{1}{Q}\}^\times$ and $u_i \in K[\eta]$ the claim of the Lemma follows by considering a general element of $K\left\{\eta, \frac{1}{Q}\right\} = K\left[\eta, \frac{1}{Q}, \frac{1}{\phi(Q)}, \dots\right]$ and removing denominators by appropriate multiplications with $u_i\phi^i(Q)$. □

Corollary 1.2.6. *Under the assumptions of Lemma 1.2.5 every ideal I of $\subset K\{\eta, \frac{1}{Q}\}$ is generated by $I \cap K[\eta]$.*

Proof: By the lemma we can find for $P \in I$ a $u \in K\{\eta, \frac{1}{Q}\}^\times$ with $uP \in I \cap K[\eta]$. Therefore $P = \frac{1}{u}uP$ lies in the ideal generated by $I \cap K[\eta]$. □

1.3 ϕ-pfields

Definition 1.3.1. *A* ϕ-pseudo field *(or* ϕ-pfield *for short) is a Noetherian, total and ϕ-simple difference ring.*

For us ϕ-pfields will play the same role as fields in the ordinary Galois theory or differential fields in the differential Galois theory. They were essentially introduced by M. van der Put and M. F. Singer to avoid certain pathologies which arise when restricting the attention to fields. In [43] ϕ-pfields appear naturally as minimal solution "fields" of linear (ordinary) difference equations. Also the approach of K. Amano and A. Masuoka in [2] which generalizes [43] is not based on fields (but artinian simple module algebras, which become ϕ-pseudo fields if one specializes to the difference case). However in [43] and [2] ϕ is always assumed to be an automorphism – an assumption which we do not make.

One could argue that a ϕ-simple ϕ-ring is the difference analog of a field. After all a field is just a simple ring. Or in more categorical language: In the category of rings one can recognize a field, say K, by the property that every arrow with source K is monic. And clearly the same characterization is valid for ϕ-simple rings in the category of ϕ-rings.

If R is a ϕ-simple ring then by Lemma 1.1.4 we can (uniquely) extend ϕ to $\mathfrak{Q}(R)$, which is then also ϕ-simple and it often seems out of place to make a big distinction between R and $\mathfrak{Q}(R)$ as they both embody "the same point". In the differential case the situation is similar: If R is a δ-simple ring then $\delta\text{-Spec}(R) = \delta\text{-Spec}(\mathfrak{Q}(R))$ (see [24]). So it would make sense to consider total ϕ-simple rings as the difference analog of fields. Finally the Noetherianity property in Definition 1.3.1 is only present to avoid the apparently more complicated non-Noetherian situation. For our interests the Noetherianity assumption is never a real problem. Essentially because the ϕ-Galois theory takes places in ϕ-dimension zero (just as classical Galois theory takes places in dimension zero). However it would surely be interesting to have the rudiments of a difference-algebraic geometry based on ϕ-simple rings instead of fields which we will develop in the sequel also available in the non-Noetherian situation.

To put things in perspective and to motivate the definitions to come (and also to make some advertisement for ϕ-pfields) we now present two lists: The first one contains some closely related problems which one encounters in commutative ϕ-algebra when one restricts the attention to ϕ-fields. The second list contains some hints how ϕ-pfields can be used to (partly) resolve the corresponding problem.

(1) Universal difference fields do not exist: This unqualified statement needs some explanation, in fact one might (and model theorists do) argue it is not true. First of all we have to observe that "universality" is a relative property: Following the differential case (see e.g. [21, Section 1.5, p. 768]) one could say that an extension $U|K$ of difference fields is universal if for every finitely ϕ-generated ϕ-field K_1 of K inside U and every finitely ϕ-generated ϕ-field extension K_2 of K_1 there exists an embedding of K_2 over K_1 into U. One can demonstrate by a simple example (see [10, Example 4, p. 59]) that not every difference field does have such a universal extension and this is the reason why, in the classical difference algebraic geometry setup one is usually looking for solutions in a universal *family* of fields and not just in one big field (cf. [10, Chapter 2, Section 10, p. 74 and Chapter 4]). However certain difference fields, say the algebraically closed and inversive ones might well have a universal extension and in this sense universal difference fields do exist.

(2) Difference fields can be incompatible: If L_1 and L_2 are ϕ-field extension of K it might happen that there does not exist a ϕ-field which contains L_1 and L_2 (See

[10, Chapter 7, Section 1]).

(3) As fields lead to prime ideals or δ-fields lead to prime δ-ideals ϕ-fields lead to reflexive prime ϕ-ideals. Every non-zero ring has a prime ideal, indeed every maximal ideal is prime. Similarly, every non-zero δ-ring has a prime δ-ideal and every δ-maximal ideal is prime. The corresponding statements in the difference setting are not true: There are ϕ-rings that have no reflexive prime ϕ-ideals. For example a ϕ-pfield has a reflexive prime ideal only if it is a field.

(4) The perfect closure of a ϕ-ideal which is considered to be the analog of the radical of an ideal in usual algebra is not quite as well behaved. For example the perfect closure of a proper ϕ-ideal can be the whole ring, there are ϕ-rings that have no perfect ϕ-ideal (apart from the whole ring) and there is no really simple formula to compute the perfect closure. In this respect ϕ-algebra is not analogous to δ-algebra. Rather it is analogous to differential algebra in characteristic p when one is *not* using iterative derivations (See e.g. [22, Exercise 1, p. 92] and [24, Proposition 2.2 and the explanation above, p. 73]). This setting produces some pathologies which can be avoided by considering "the higher powers of δ", i.e. iterative derivations. Here the idea is similar, we also have to take into account "the higher powers of ϕ". For example every ϕ-pfield has a prime ideal that is reflexive with respect to ϕ^n for some $n \geq 1$.

(5) Let K be a difference field and $C = K^\phi$ the field of constants of K. For certain constructions one might need to slightly extend the constants of K. But contrary to the differential case, if C' is a finite algebraic extension of C then $K' = K \otimes_C C'$ need not be a field.

Here comes the second list that replaces ϕ-fields with ϕ-pfields.

(1)' As a matter of principle (or maybe better, as a matter of style) we are not interested in using these somewhat controversial universal constructions.

(2)' Let K be a ϕ-pfield and assume that L_1 and L_2 are ϕ-pfield extensions of K. If L_1 and L_2 are finitely generated as total rings over K then L_1 and L_2 are compatible in the sense that there exists a ϕ-pfield extension of K which contains L_1 and L_2.

(3)' The notion of ϕ-pfield leads to what we will call a ϕ-prime ideal (see Definition 1.4.3). Every non-zero Noetherian ϕ-ring has a ϕ-prime ideal and every ϕ-maximal ϕ-ideal is ϕ-prime.

(4)' Considering ϕ-pfields instead of ϕ-fields replaces the perfect closure by what we will call the ϕ-radical (Definition 1.4.6). If $\mathfrak{a}$ is a ϕ-ideal of a ϕ-ring R then the ϕ-radical of $\mathfrak{a}$ is simply given by $\{r \in R; \exists\ n \geq 0,\ m \geq 1 :\ \phi^n(a)^m \in \mathfrak{a}\}$. In particular if $\mathfrak{a}$ is a proper ideal also its ϕ-radical is a proper ideal and every ϕ-ring has a proper ϕ-radical ideal, namely the ϕ-radical of the zero ideal. See also Lemma 1.4.10.

(5)' If K is a ϕ-pfield and C' a finite algebraic extension of $C = K^\phi$ then $K' = K \otimes_C C'$ is a ϕ-pfield.

We continue with a simple characterization of ϕ-pfields.

Proposition 1.3.2. *Let K be a ϕ-ring. Then K is a ϕ-pfield if and only if there exist orthogonal idempotent elements $e_1, \dots, e_t$ of K such that*

(1) $K = e_1 K \oplus \cdots \oplus e_t K$,

(2) $\phi(e_i) = e_{i+1}$ *for* $i = 1, \dots, t-1$ *and* $\phi(e_t) = e_1$,

(3) $e_i K$ *is a field for* $i = 1, \dots, t$.

Proof: If K is a ϕ-pfield then it follows from Proposition 1.1.2 and the fact that K is total that (1), (2) and (3) must be satisfied. Conversely a ϕ-ring K satisfying (1), (2) and (3) is clearly Noetherian and total. Every ideal of K is of the form Ke for some idempotent element e of K and because of (2) it easily follows that Ke is a ϕ-ideal only if $e = 0$ or $e = 1$. □

Notation: In the following, if we write $K = e_1 K \oplus \cdots \oplus e_t K$ for some ϕ-pfield K we always assume (without explicitly mentioning it) that $e_1, \dots, e_t$ are orthogonal idempotent elements of K satisfying the conditions (1),(2) and (3) of Proposition 1.3.2.

With the definition of ϕ-pfields at hand we can now give a corollary to Lemma 1.2.5.

Corollary 1.3.3. *Let $K \subset L$ be an inclusion of ϕ-pfields and $\eta \in L^n$ such that $L = K(\eta)$. If*

$$\phi(\eta_i) = \frac{P_i}{Q}$$

for $i = 1, \dots, n$ with $P_i \in K[\eta]$ and $Q \in K[\eta] \cap L^\times$ then $K\{\eta, \frac{1}{Q}\}$ is Noetherian.

Proof: By Corollary 1.2.6 an ascending chain of ideals in $K\{\eta, \frac{1}{Q}\}$ corresponds to an ascending chain of ideals in $K[\eta]$ which is Noetherian. □

Lemma 1.3.4. *Let R be a ϕ-subring of a ϕ-pfield K. Then a non zero divisor of R is also a non zero divisor in K and so $\mathfrak{Q}(R)$ is naturally embedded in K. Moreover $\mathfrak{Q}(R)$ is a ϕ-pfield, i.e. a sub ϕ-pfield of K. In particular every total ϕ-subring of a ϕ-pfield is a ϕ-pfield.*

Proof: It follows from Lemma 1.1.4 that a non zero divisor of R is a non zero divisor in K. Thus there is a canonical map $\mathfrak{Q}(R) \to K$ which is clearly injective. Again from Lemma 1.1.4 it follows that ϕ maps a non zero divisor of R to a non zero divisor of R, consequently $\mathfrak{Q}(R) \subset K$ is a ϕ-subring.

By [8, Proposition 16, Chapter II, Paragraph 2.6, p. 74] every minimal prime ideal of $\mathfrak{Q}(R)$ is of the form $\mathfrak{q} \cap \mathfrak{Q}(R)$ for some minimal prime ideal $\mathfrak{q}$ of K. In particular

$\mathfrak{Q}(R)$ has only finitely many minimal prime ideals. But a reduced total ring with only finitely many minimal prime ideals must be a finite direct product of fields. If $\mathfrak{q}$ is a minimal prime ideal of K then

$$\mathfrak{q} \cap \phi^{-1}(\mathfrak{q}) \cap \cdots \cap \phi^{-(d-1)}(\mathfrak{q}) = 0$$

for some $d \geq 1$. So if $\mathfrak{q}' = \mathfrak{Q}(R) \cap \mathfrak{q}$ then

$$\mathfrak{q}' \cap \cdots \cap \phi^{-(d-1)}(\mathfrak{q}') = 0.$$

This shows that $\mathfrak{Q}(R)$ is a ϕ-pfield (cf. Proposition 1.3.2). □

Lemma 1.3.5. *Let $K = e_1K \oplus \cdots \oplus e_tK$ be a ϕ-pfield. Then for $i = 1, \ldots, t$ the map*

$$K^{\phi} \to (e_iK)^{\phi^t}, \ c \mapsto e_ic$$

is an isomorphism of fields.

Proof: The inverse is given by

$$(e_iK)^{\phi^t} \to K^{\phi}, \ c \mapsto c + \phi(c) + \cdots + \phi^{t-1}(c).$$

□

1.4 ϕ-ideals

This section provides some basic properties of ϕ-prime and ϕ-radical ideals. We first recall some definitions.

Definition 1.4.1. *Let R be a ϕ-ring and $\mathfrak{a}$ a ϕ-ideal of R. Then $\mathfrak{a}$ is called*

- reflexive *if $\phi^{-1}(\mathfrak{a}) = \mathfrak{a}$,*
- ϕ-maximal *if $\mathfrak{a}$ is a maximal element in the set of all ϕ-ideals not equal to R,*
- ϕ-radical *if $\mathfrak{a}$ is reflexive and radical.*

Proposition 1.4.2. *Let R be a ϕ-ring and $\mathfrak{p}$ a ϕ-ideal of R. Then the following are equivalent:*

(1) *ϕ can be extended to $\mathfrak{Q}(R/\mathfrak{p})$ and $\mathfrak{Q}(R/\mathfrak{p})$ is a ϕ-pfield.*

(2) *There exists a ϕ-pfield K and a morphism $\psi : R \to K$ of difference rings such that $\mathfrak{p} = \ker(\psi)$.*

(3) *There exists a prime ideal $\mathfrak{q}$ of R and $d \geq 1$ such that $\phi^{-d}(\mathfrak{q}) = \mathfrak{q}$ and*

$$\mathfrak{p} = \mathfrak{q} \cap \phi^{-1}(\mathfrak{q}) \cap \cdots \cap \phi^{-(d-1)}(\mathfrak{q}).$$

If R is additionally assumed to be Noetherian this is also equivalent to:

(4) *There exits a multiplicatively closed and ϕ-stable subset S of R such that $\mathfrak{p}$ is maximal among ϕ-ideals not meeting S.*

Proof: The implication (1) ⇒ (2) is trivial.
(2) ⇒ (3) : Let $\mathfrak{q}'$ be a minimal prime ideal of $K = e_1K \oplus \cdots \oplus e_tK$. Then $\phi^{-t}(\mathfrak{q}') = \mathfrak{q}'$ and $0 = \mathfrak{q}' \cap \phi^{-1}(\mathfrak{q}') \cap \cdots \cap \phi^{-(t-1)}(\mathfrak{q}')$. Now $\mathfrak{q} = \psi^{-1}(\mathfrak{q}')$ has the desired property.
(3) ⇒ (1) : Let $S = \{r \in R;\ r \notin \phi^{-i}(\mathfrak{q}) \text{ for } i = 0, \ldots, d-1\}$. Then S is a multiplicatively closed, ϕ-stable subset of R. Thus the same is true for $\overline{S} \subset R/\mathfrak{p}$. Since $\overline{S}$ also agrees with the set of non zero divisors of $R/\mathfrak{p}$ we conclude that ϕ naturally extends to $\mathfrak{Q}(R/\mathfrak{p})$. We know that

$$\mathfrak{Q}(R/\mathfrak{p}) = \mathfrak{Q}(R/\phi^{-(d-1)}(\mathfrak{q})) \oplus \cdots \oplus \mathfrak{Q}(R/\phi^{-1}(\mathfrak{q})) \oplus \mathfrak{Q}(R/\mathfrak{q})$$

is a finite direct product of fields. Because ϕ maps $\mathfrak{Q}(R/\phi^{-i}(\mathfrak{q}))$ into $\mathfrak{Q}(R/\phi^{-(i-1)}(\mathfrak{q}))$ it follows that $\mathfrak{Q}(R/\mathfrak{p})$ is a ϕ-pfield (cf. Proposition 1.3.2).
(3) ⇒ (4) : Let S be defined as in (3) ⇒ (1). The ϕ-ideals of R which do not meet S and lie above $\mathfrak{p}$ correspond to ϕ-ideals of $\overline{S}^{-1}(R/\mathfrak{p})$. As we have already seen that $\overline{S}^{-1}(R/\mathfrak{p}) = \mathfrak{Q}(R/\mathfrak{p})$ is ϕ-simple and $\mathfrak{p} : S = \mathfrak{p}$ we infer the validity of (4).
(4) ⇒ (2): It follows from (4) that $\overline{S}^{-1}(R/\mathfrak{p})$ is ϕ-simple. Let K denote the total quotient ring of $\overline{S}^{-1}(R/\mathfrak{p})$. Because of the Noetherianity assumption it follows that K is a ϕ-pfield. The kernel of the canonical map $\psi : R \to K$ is a ϕ-ideal containing $\mathfrak{p}$ and not meeting S, thus it must be equal to $\mathfrak{p}$. □

Taking $\phi = \text{id}$ in the above proposition gives a well known characterization of prime ideals. This motivates the following definition.

Definition 1.4.3. *Let R be a ϕ-ring. A difference ideal $\mathfrak{p}$ of R is called* ϕ-prime *if there exists a prime ideal $\mathfrak{q}$ of R and $d \geq 1$ such that $\phi^{-d}(\mathfrak{q}) = \mathfrak{q}$ and*

$$\mathfrak{p} = \mathfrak{q} \cap \phi^{-1}(\mathfrak{q}) \cap \cdots \cap \phi^{-(d-1)}(\mathfrak{q}).$$

The set of all ϕ-prime ideals of R is denoted with $\operatorname{Spec}^{\phi}(R)$. *And with* ϕ-$\operatorname{Spec}(R)$ *we denote the set of all prime ideals $\mathfrak{q}$ of R such that there exists an integer $d \geq 1$ with $\phi^{-d}(\mathfrak{q}) = \mathfrak{q}$.*

Taking $S = \{1\}$ in Proposition 1.4.2 we see that at least in a Noetherian ϕ-ring every ϕ-maximal ideal is ϕ-prime. A simple application of Zorn's Lemma shows that there always exists a ϕ-maximal ideal.

In [29, Definition 2.3.20, p. 128] A. Levin uses the term σ-prime (his σ is our ϕ) for a slightly different but related concept. He postulates that a ϕ-ideal $\mathfrak{p}$ of a ϕ-ring R is σ-prime if for any two ϕ-ideals $\mathfrak{a}$ and $\mathfrak{b}$ of R with $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$ one has $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$. As the concept of σ-prime ideals does not play a relevant role in the subsequent developments in [29] (or in difference algebra in general) there seems no harm in enforcing our terminology. Our ϕ-prime ideals are σ-prime:

Lemma 1.4.4. *Let R be a ϕ-ring and $\mathfrak{p}$ a ϕ-prime ideal of R. If $\mathfrak{a}$ and $\mathfrak{b}$ are ϕ-ideals of R such that $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$ then $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$.*

Proof: If

$$\mathfrak{a}\mathfrak{b} \subset \mathfrak{p} = \mathfrak{q} \cap \cdots \cap \phi^{-(d-1)}(\mathfrak{q}) \subset \mathfrak{q}$$

then, as $\mathfrak{q}$ is prime, either $\mathfrak{a} \subset \mathfrak{q}$ or $\mathfrak{b} \subset \mathfrak{q}$. We assume without loss of generality that $\mathfrak{a} \subset \mathfrak{q}$. Then $\mathfrak{a} \subset \phi^{-1}(\mathfrak{a}) \subset \phi^{-1}(\mathfrak{q})$ and so also $\mathfrak{a} \subset \phi^{-1}(\mathfrak{a}) \subset \phi^{-2}(\mathfrak{q})$. Continuing in this way we obtain $\mathfrak{a} \subset \mathfrak{q} \cap \cdots \cap \phi^{-(d-1)}(\mathfrak{q}) = \mathfrak{p}$ as desired. □

Definition 1.4.5. *If R is a ϕ-ring and $\mathfrak{p} = \mathfrak{q} \cap \cdots \cap \phi^{-(d-1)}(\mathfrak{q})$ is a ϕ-prime ideal of R then we define*

$$R_{\mathfrak{p}} = S(\mathfrak{p})^{-1}R,$$

where $S(\mathfrak{p})$ is the multiplicatively closed ϕ-stable subset of R consisting of all elements $s \in R$ such that $s \notin \mathfrak{q}, \ldots, \phi^{-(d-1)}(\mathfrak{q})$. We note that $R_{\mathfrak{p}}$ is a ϕ-local ring in the sense that it has a unique ϕ-maximal ideal, namely $R_{\mathfrak{p}}\mathfrak{p}$. And

$$k(\mathfrak{p}) = R_{\mathfrak{p}}/R_{\mathfrak{p}}\mathfrak{p} = \mathfrak{Q}(R/\mathfrak{p})$$

is a ϕ-pfield (cf. Proposition 1.4.2). We call it the residue ϕ-pfield at $\mathfrak{p}$.

Definition 1.4.6. *Let $\mathfrak{a} \subset R$ be a ϕ-ideal. The smallest reflexive ϕ-ideal of R containing $\mathfrak{a}$ is called the* reflexive closure of $\mathfrak{a}$. *The smallest ϕ-radical ideal of R containing $\mathfrak{a}$ is called the ϕ*-radical of $\mathfrak{a}$, *it is denoted by ϕ-$\sqrt{\mathfrak{a}}$.*

The reflexive closure and the ϕ-radical are well defined because the intersection of reflexive (ϕ-radical) ϕ-ideals is reflexive (ϕ-radical) and the whole ring is reflexive (ϕ-radical).

Proposition 1.4.7. *Let $\mathfrak{a} \subset R$ be a ϕ-ideal. Then*

- *the reflexive closure of $\mathfrak{a}$ is equal to $\{r \in R;\ \exists\ n \geq 0$ such that $\phi^n(r) \in \mathfrak{a}\}$ and*
- *ϕ-$\sqrt{\mathfrak{a}} = \{r \in R;\ \exists\ n \geq 0, m \geq 1$ such that $\phi^n(r)^m \in \mathfrak{a}\}$.*

In particular the ϕ-radical of $\mathfrak{a}$ equals the radical of the reflexive closure of $\mathfrak{a}$ and this is also equal to the reflexive closure of the radical of $\mathfrak{a}$.

Proof: The easy proof is left to the reader.

Proposition 1.4.8. *Let R be Noetherian ϕ-ring and $\mathfrak{a} \subset R$ a ϕ-ideal. Then*

$$\phi\text{-}\sqrt{\mathfrak{a}} = \bigcap_{\substack{\mathfrak{a} \subset \mathfrak{p} \\ \phi\text{-}prime}} \mathfrak{p}$$

Proof: Because R is Noetherian and $\phi\text{-}\sqrt{\mathfrak{a}}$ a radical ideal we have a unique decomposition

$$\phi\text{-}\sqrt{\mathfrak{a}} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

of $\phi\text{-}\sqrt{\mathfrak{a}}$ in its minimal prime ideals. Because $\phi\text{-}\sqrt{\mathfrak{a}}$ is reflexive we see that the application of ϕ^{-1} induces a permutation of $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$. Each cycle in the cycle decomposition of this permutation corresponds to a ϕ-prime ideal. □

Of course the above proof also shows that every ϕ-radical ideal of R can uniquely be written as an irredudant intersection of ϕ-prime ideals. This is a variation on the classical result that every perfect ϕ-ideal is the intersection of reflexive prime ideals (see [10, p. 88]).

Corollary 1.4.9. *Let R be a Noetherian ϕ-ring. Then R is ϕ-simple if and only if R has no non-zero ϕ-prime ideals.*

Proof: If $\mathfrak{a}$ is a proper ϕ-ideal of R then by Proposition 1.4.8 the ϕ-radical of $\mathfrak{a}$ is the intersection of ϕ-prime ideals. Thus by assumption $\mathfrak{a}$ must be zero. □

Lemma 1.4.10. *Let $\psi : R \to S$ be a morphism of ϕ-rings and $\mathfrak{a}$ a ϕ-ideal of S then*

$$\psi^{-1}(\phi\text{-}\sqrt{\mathfrak{a}}) = \phi\text{-}\sqrt{\psi^{-1}(\mathfrak{a})}.$$

In particular if $\mathfrak{a} \subset S$ is ϕ-radical then $\psi^{-1}(\mathfrak{a}) \subset R$ is ϕ-radical.

Proof: This is immediate from the explicit formula given in Proposition 1.4.7. □

The above lemma is false if the ϕ-radical is replaced by the perfect closure as one can easily verify with the example $k[x^2] \subset k[x],\ \phi(x) = -x,\ \mathfrak{a} = (x^2 - 1)$.

Let R be a ϕ-ring. We can define a topology on $\operatorname{Spec}^\phi(R)$ by postulating that a subset of $\operatorname{Spec}^\phi(R)$ is closed if and only if it is of the form

$$\mathbb{V}(\mathfrak{a}) = \{\mathfrak{p} \in \operatorname{Spec}^\phi(R);\ \mathfrak{a} \subset \mathfrak{p}\}$$

for some ϕ-ideal (or subset) $\mathfrak{a}$ of R: One immediately sees that

$$\cap \mathbb{V}(\mathfrak{a}_i) = \mathbb{V}(\Sigma \mathfrak{a}_i)$$

and it follows from Lemma 1.4.4 that

$$\mathbb{V}(\mathfrak{a}) \cup \mathbb{V}(\mathfrak{b}) = \mathbb{V}(\mathfrak{a} \cap \mathfrak{b}).$$

Thus we have indeed a well defined topology on $\operatorname{Spec}^\phi(R)$. If $\psi : R \to S$ is a morphism of ϕ-rings then

$$\psi^* : \operatorname{Spec}^\phi(S) \to \operatorname{Spec}^\phi(R),\ \mathfrak{p} \mapsto \psi^{-1}(\mathfrak{p})$$

is continuous because $\psi^{*-1}(\mathbb{V}(\mathfrak{a})) = \mathbb{V}(\psi(\mathfrak{a}))$.

Lemma 1.4.11. *Let $\psi : S \to R$ be a morphism of ϕ-rings such that*

$$\{\phi\text{-radical ideals of } R\} \longrightarrow \{\phi\text{-radical ideals of } S\}, \ \mathfrak{a} \mapsto \psi^{-1}(\mathfrak{a})$$

is injective. Then

$$\psi^* : \operatorname{Spec}^\phi(R) \to \operatorname{Spec}^\phi(S)$$

is a homeomorphism onto its image.

Proof: Because ϕ-prime ideals are ϕ-radical ψ^* is injective. To see that it is a homeomorphism onto the image it suffices to show that

$$\psi^*(\mathbb{V}(\mathfrak{a})) = \operatorname{im}(\psi^*) \cap \mathbb{V}(\psi^{-1}(\mathfrak{a}))$$

for every ϕ-radical ideal $\mathfrak{a}$ of R. The inclusion "$\subset$" is obvious. If $\mathfrak{p}$ is a ϕ-prime ideal of R with $\psi^{-1}(\mathfrak{p}) \supset \psi^{-1}(\mathfrak{a})$ then $\psi^{-1}(\mathfrak{p} \cap \mathfrak{a}) = \psi^{-1}(\mathfrak{p}) \cap \psi^{-1}(\mathfrak{a}) = \psi^{-1}(\mathfrak{a})$. The injectivity then gives $\mathfrak{p} \cap \mathfrak{a} = \mathfrak{a}$ which means $\mathfrak{a} \subset \mathfrak{p}$, i.e. $\psi^{-1}(\mathfrak{p}) \in \psi^*(\mathbb{V}(\mathfrak{a}))$. □

Lemma 1.4.12. *Let $\psi : S \to R$ be a morphism of ϕ-rings such that*

$$\{\phi\text{-radical ideals of } R\} \longrightarrow \{\phi\text{-radical ideals of } S\}, \ \mathfrak{a} \mapsto \psi^{-1}(\mathfrak{a})$$

is bijective and assume that R is Noetherian. Then

$$\psi^* : \operatorname{Spec}^\phi(R) \to \operatorname{Spec}^\phi(S)$$

is a homeomorphism.

Proof: By Lemma 1.4.11 it suffices to show that ψ^* is surjective. So let $\mathfrak{p}'$ be a ϕ-prime ideal of S. By assumption there exists a ϕ-radical ideal $\mathfrak{a}$ of R with $\psi^{-1}(\mathfrak{a}) = \mathfrak{p}'$. Because R is assumed to be Noetherian it follows from Proposition 1.4.8 that

$$\mathfrak{a} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$$

is the intersection of finitely many ϕ-prime ideals. We have

$$\mathfrak{p}' = \psi^{-1}(\mathfrak{a}) = \psi^{-1}(\mathfrak{p}_1) \cap \cdots \cap \psi^{-1}(\mathfrak{p}_n).$$

Because $\mathfrak{p}'$ is ϕ-prime we conclude that $\mathfrak{p}' = \psi^{-1}(\mathfrak{p}_i)$ for some i. □

Lemma 1.4.13. *Let $\psi : S \to R$ be a morphism of ϕ-rings such that*

$$\{\phi\text{-radical ideals of } R\} \longrightarrow \{\phi\text{-radical ideals of } S\}, \ \mathfrak{a} \mapsto \psi^{-1}(\mathfrak{a})$$

is bijective. Then the inverse is given by $\mathfrak{b} \mapsto \phi\text{-}\sqrt{R\psi(\mathfrak{b})}$ and for ϕ-radical ideals $\mathfrak{a}, \mathfrak{a}'$ of R we have $\mathfrak{a} \subset \mathfrak{a}'$ if and only if $\psi^{-1}(\mathfrak{a}) \subset \psi^{-1}(\mathfrak{a}')$.

Proof: We only have to show that $\psi^{-1}(\phi\text{-}\sqrt{R\psi(\mathfrak{b})})) = \mathfrak{b}$ for every ϕ-radical ideal $\mathfrak{b}$ of S. By assumption there exists a ϕ-radical ideal $\mathfrak{a}$ of R such that $\psi^{-1}(\mathfrak{a}) = \mathfrak{b}$. Then $\psi(\mathfrak{b}) \subset \mathfrak{a}$ and so also $\phi\text{-}\sqrt{R\psi(\mathfrak{b})} \subset \mathfrak{a}$. Therefore $\psi^{-1}(\phi\text{-}\sqrt{R\psi(\mathfrak{b})}) \subset \psi^{-1}(\mathfrak{a}) = \mathfrak{b}$ and so $\psi^{-1}(\phi\text{-}\sqrt{R\psi(\mathfrak{b})}) = \mathfrak{b}$.

If $\psi^{-1}(\mathfrak{a}) \subset \psi^{-1}(\mathfrak{a}')$ then $\mathfrak{a} = \phi\text{-}\sqrt{R\psi(\psi^{-1}(\mathfrak{a}))} \subset \phi\text{-}\sqrt{R\psi(\psi^{-1}(\mathfrak{a}'))} = \mathfrak{a}'$. □

Lemma 1.4.14. *Let R be a ϕ-ring such that $C = R^\phi$ is a field and D a C-algebra (considered as a constant ϕ-ring). Then $(R \otimes_C D)^{\phi^n} = R^{\phi^n} \otimes_C D$ for every $n \geq 1$.*

Proof: Let $(d_i)_{i \in I}$ be a C-basis of D and $a = \sum r_i \otimes d_i \in R \otimes_C D$. If $a \in (R \otimes_C D)^{\phi^n}$ then

$$\sum \phi^n(r_i) \otimes d_i = \sum r_i \otimes d_i.$$

This implies $\phi^n(r_i) = r_i$ which gives $a \in R^{\phi^n} \otimes_C D$. □

Proposition 1.4.15. *Let L be a ϕ-pfield, $C = L^\phi$ and D a C-algebra (considered as a constant ϕ-ring). Set $R = L \otimes_C D$. Then the map*

$$\{\phi\text{-}ideals\ of\ R\} \longrightarrow \{ideals\ of\ D\}$$

which sends a ϕ-ideal $\mathfrak{a}$ of R to $\mathfrak{a}^\phi = \mathfrak{a} \cap D$ is bijective with inverse $\mathfrak{b} \mapsto R\mathfrak{b} = L \otimes \mathfrak{b} \subset R$. Under this bijection ϕ-radical ideals of R correspond to radical ideals of D. If R is Noetherian (e.g. if D is finitely generated as C-algebra) then ϕ-prime ideals of R correspond to prime ideals of D.

Furthermore every ϕ-ideal of R is reflexive.

Proof: Let $\mathfrak{a} \subset R$ be a ϕ-ideal. We will show that $R\mathfrak{a}^\phi = \mathfrak{a}$. Let $(d_i)_{i \in I}$ be a C-basis of $\mathfrak{a}^\phi = \mathfrak{a} \cap D$ and extend it to a C-basis $(d_i)_{i \in I \uplus I'}$ of D. Then every $a \in \mathfrak{a}$ is uniquely of the form

$$a = \sum_{i \in I \cup I'} a_i \otimes d_i \in L \otimes_C D.$$

Now suppose $R\mathfrak{a}^\phi \subsetneqq \mathfrak{a}$ and let $a \in \mathfrak{a} \smallsetminus R\mathfrak{a}^\phi$ be such that the cardinality of

$$J = J_a = \{i \in I \cup I';\ a_i \neq 0\}$$

is minimal. Then $J \subset I'$. Choose $j' \in J$ and set

$$I = \left\{ b_{j'} \in L;\ \text{For } j \in J \smallsetminus \{j'\} \text{ there exists } b_j \in L \text{ such that } \sum_{j \in J} b_j \otimes d_j \in \mathfrak{a}. \right\}.$$

One immediately verifies that I is a ϕ-ideal of L. Since $a_{j'} \in I$ it is not the zero ideal and so $1 \in I$. Therefore we can assume that $a_{j'} = 1$.

As $\mathfrak{a}$ is a ϕ-ideal

$$a - \phi(a) = \sum_{\substack{j \in J \\ j \neq j'}} (a_j - \phi(a_j)) \otimes d_j \in \mathfrak{a}.$$

By choice of a we must have $a - \phi(a) \in R\mathfrak{a}^\phi$. But since $J \subset I'$ we must have $a_j - \phi(a_j) = 0$, i.e. $a_j \in C$ for all $j \in J$. But then we arrive at the contradiction

$$a = \sum_{j \in J} a_j \otimes d_j \in \mathfrak{a}^\phi.$$

Therefore $R\mathfrak{a}^\phi = \mathfrak{a}$.

Next we will show that $(R\mathfrak{b})^\phi = \mathfrak{b}$ for every ideal $\mathfrak{b}$ of D. Let $(d_i)_{i\in I}$ be a C-basis of $\mathfrak{b}$. Then every element a of $R\mathfrak{b} = L \otimes \mathfrak{b}$ is uniquely of the form

$$a = \sum_{i\in I} a_i \otimes d_i \in L \otimes_C D.$$

If $a \in (R\mathfrak{b})^\phi$ then

$$0 = a - \phi(a) = \sum_{i\in I} (a_i - \phi(a_i)) \otimes d_i$$

and so $a_i \in L^\phi$ which gives $a \in \mathfrak{b}(= 1 \otimes \mathfrak{b})$. Thus $(R\mathfrak{b})^\phi = \mathfrak{b}$ and we have established the one-to-one correspondence.

Next we will show that for every ideal $\mathfrak{b}$ of D the ϕ-ideal $L \otimes \mathfrak{b}$ of R is reflexive. Let $(d_i)_{i\in I}$ be a C-basis of $\mathfrak{b}$ and extend it to a C-basis $(d_i)_{i\in I\uplus I'}$ of D. Then every $a \in R$ is uniquely of the form

$$a = \sum_{i\in I\cup I'} a_i \otimes d_i \in L \otimes_C D.$$

If

$$\phi(a) = \sum_{i\in I\cup I'} \phi(a_i) \otimes d_i$$

lies in $L \otimes \mathfrak{b}$ then we must have $\phi(a_i) = 0$ for $i \in I'$. But because ϕ is injective this implies $a \in L \otimes \mathfrak{b}$ and so $R\mathfrak{b}$ is reflexive.

Next we want to see that ϕ-radical ideals correspond to radical ideals. If $\mathfrak{a} \subset R$ is ϕ-radical then clearly $\mathfrak{a}^\phi \subset D$ is radical. Conversely suppose that $\mathfrak{b}$ is a radical ideal of D. Since we already know that $R\mathfrak{b}$ is reflexive we only have to to show that $R\mathfrak{b}$ is radical. And because the map $\mathfrak{a} \mapsto \mathfrak{a}^\phi$ is injective it suffices to show that $(\sqrt{R\mathfrak{b}})^\phi = \mathfrak{b}$. But if $a \in (\sqrt{R\mathfrak{b}})^\phi$ then there exists $n \geq 1$ such that $a^n \in (R\mathfrak{b})^\phi = \mathfrak{b}$. And so $(\sqrt{R\mathfrak{b}})^\phi = \mathfrak{b}$.

The correspondence between ϕ-prime and prime ideals in case R is Noetherian follows from Lemma 1.4.12 applied to the morphism $D \to R$ of difference rings. □

Corollary 1.4.16. *Let L be a ϕ-pfield. Then L is a separable L^ϕ-algebra.*

Proof: Let D be a field extension of L^ϕ considered as trivial ϕ-ring. Let $\mathfrak{a}$ denote the nilradical of $L \otimes_C D$. Since $\mathfrak{a}$ is a difference ideal it follows from the proposition that $\mathfrak{a} = (L \otimes_C D)(\mathfrak{a} \cap D) = 0$. □

1.5 ϕ-separable ϕ-algebras

In the difference Galois theory that will be developed in Chapter 3 we will not impose the condition that the base ϕ-pfield is inversive. This necessitates the study of ϕ-separability.

Definition 1.5.1. *Let K be a ϕ-pfield and R a K-ϕ-algebra. We say that R is ϕ-*separable (over K) *if*

$$\phi : R \otimes_K L \to R \otimes_K L$$

is injective for every extension $L|K$ of ϕ-pfields.

Let K be a field of characteristic p and consider K as a difference field in virtue of the Frobenius, i.e. $\phi(a) = a^p$ for $a \in K$. Then any K-algebra R has naturally the structure of a K-ϕ-algebra. It will follow from Proposition 1.5.2 below that R is a separable K-algebra if and only if R is ϕ-separable over K. In other words, ϕ-separable with ϕ the Frobenius is the same as separable. As we will see below, many of the basic statements about separable extensions have ϕ-analogues. The following proposition is a straightforward generalization of [7, Theorem 2, Chapter 5, Paragraph 15, Section 4, A.V.122].

Proposition 1.5.2. *Let $K = e_1K \oplus \cdots \oplus e_tK$ be a ϕ-pfield and R a K-ϕ-algebra. Then the following statements are equivalent:*

(1) *R is ϕ-separable over K.*

(2) *There exists an inversive ϕ-overring K' of K such that*

$$\phi : R \otimes_K K' \to R \otimes_K K'$$

is injective.

(3) *The map*

$$\phi : R \otimes_K K^* \to R \otimes_K K^*$$

is injective where K^* denotes the inversive closure of K (see [10, Chapter 2, Section 5, p.66]).

(4) *If $(a_j)_{j \in J}$ are e_iK-linearly independent elements of e_iR then the family $(\phi(a_j))_{j \in J}$ is $e_{i+1}K$-linearly independent.*

(5) *The map*

$$\phi : R \otimes_K L \to R \otimes_K L$$

is injective for any K-ϕ-algebra L with $\phi : L \to L$ injective.

Proof: It is easy to see that the inversive closure of a ϕ-pfield is a ϕ-pfield (cf. [10, Theorem 2, Chaper 2, Section 5, p.66]). Thus (1) implies (2). Any inversive ϕ-overring of K contains the inversive closure of K ([10, Theorem 2, Chaper 2, Section 5, p.66]) and so (2) implies (3).

We now prove the implication (3) $\Rightarrow$ (4). So fix $i \in \{1, \dots, t\}$ and let $(a_j)_{j \in J}$ be a family of e_iK-linearly independent elements of e_iR. Suppose

$$\sum_j \lambda_j \phi(a_j) = 0$$

with $\lambda_j \in e_{i+1}K$. As K^* is inversive there exists $\mu_j \in K^*$ with $\phi(\mu_j) = \lambda_j$. We have

$$\phi\left(\sum a_j \otimes \mu_j\right) = \sum \phi(a_j) \otimes \lambda_j = \sum \phi(a_j)\lambda_j \otimes 1 = 0 \in R \otimes_K K^*.$$

So, by assumption, $\sum a_j \otimes \mu_j = 0$. Multiplication with e_i gives $\sum_j a_j \otimes e_i\mu_j = 0$. Since the a_j's are e_iK-linearly independent we must have $e_i\mu_j = 0$ for all j. Applying ϕ yields $e_{i+1}\lambda_j = 0$. But $\lambda_j \in e_{i+1}K$ and so $\lambda_j = 0$ for all j.

Next we show that (4) implies (5). Let L be a K-ϕ-algebra with $\phi : L \to L$ injective. For $i = 1, \dots, t$ let $(a_{ij})_{j \in J_i}$ be an e_iK-basis of e_iR. Then every element b of

$$R \otimes_K L = (e_1R \otimes_{e_1K} e_1L) \oplus \cdots \oplus (e_tR \otimes_{e_tK} e_tL)$$

is uniquely of the form

$$b = \sum_{i=1}^{t} \sum_{j \in J_i} a_{ij} \otimes b_{ij}$$

where $b_{ij} \in e_iL$. If

$$\phi(b) = \sum_{i=1}^{t} \sum_{j \in J_i} \phi(a_{ij}) \otimes \phi(b_{ij}) = 0$$

then by assumption $\phi(b_{ij}) = 0$ for all i and j. As $\phi : L \to L$ is injective this implies $b_{ij} = 0$ and consequently $b = 0$ as desired.

Finally the implication (5) ⇒ (1) is trivial. □

Corollary 1.5.3. *If K is an inversive ϕ-pfield then every K-ϕ-algebra R with $\phi : R \to R$ injective is ϕ-separable over K.*

Proof: We will use characterization (4) of the above proposition. Let R be a K-ϕ-algebra and fix $i \in \{1, \dots, t\}$. Furthermore let $(a_j)_{j \in J}$ be an e_iK-linearly independent family in e_iR and $\sum \lambda_j \phi(a_j) = 0$ with $\lambda_j \in e_{i+1}K$. An application of the map ϕ^{-1} yields $\sum \phi^{-1}(\lambda_j)a_j = 0$ with $\phi^{-1}(\lambda_j) \in e_iK$. By e_iK-linear independence of the a_j's we obtain $\phi^{-1}(\lambda_j) = 0$ and so $\lambda_j = \phi(0) = 0$ for all j. □

Corollary 1.5.4. *Let $L|K$ be an extension of ϕ-pfields, R a K-ϕ-algebra and $\mathfrak{a}$ a reflexive ϕ-ideal of R. If L is ϕ-separable over K then $\mathfrak{a} \otimes L$ is a reflexive ϕ-ideal of $R \otimes_K L$.*

Proof: As $(R \otimes_K L)/(\mathfrak{a} \otimes L) = (R/\mathfrak{a}) \otimes_K L$ the corollary follows from point (5) of the proposition. □

Remark 1.5.5. *In [18, Definition 3.23, p. 24] E. Hrushovski defines an extension $L|K$ of difference fields to be* transformally separable *if L is linearly disjoint from K^* over K (inside L^*). Here K^* (respectively L^*) denotes the inversive closure of K (respectively L). Using Proposition 1.5.2 it is easy to see that ϕ-separability and transformal separability are the same (for difference fields).*

Proof: If L and K^* are linearly disjoint over K then $L \otimes_K K^*$ is naturally a ϕ-subring of L^*. Because ϕ is injective on L^* it must be injective on $L \otimes_K K^*$. Thus L is ϕ-separable over K by Proposition 1.5.2, (3).

Conversely assume that $L|K$ is ϕ-separable and let $a_1, \ldots, a_n \in L \subset L^*$ be K-linearly independent. We have to show that the a_i's are also K^*-linearly independent. So let $\lambda_1, \ldots, \lambda_n \in K^*$ with $\lambda_1 a_1 + \cdots + \lambda_n a_n = 0$. There exists an $m \geq 0$ such that $\phi^m(a_i) \in K$ for $i = 1, \ldots, n$. Thus

$$\phi^m(\lambda_1)\phi^m(a_1) + \cdots + \phi^m(\lambda_n)\phi^m(a_n) = 0$$

is a K-linear relation between $\phi^m(a_1), \ldots, \phi^m(a_n)$. But by Proposition 1.5.2, (4) this implies $\phi^m(\lambda_i) = 0$ for $i = 1, \ldots, n$. Therefore the λ_i's must all be zero. □

Lemma 1.5.6. *Let K be a ϕ-pfield and R a ϕ-separable K-ϕ-algebra. Then every K-ϕ-subalgebra of R is also ϕ-separable over K.*

Proof: Let S be a K-ϕ-subalgebra of R and L a ϕ-pfield extension of K. By assumption ϕ is injective on $R \otimes_K L$. Therefore ϕ is also injective on $S \otimes_K L \hookrightarrow R \otimes_K L$. □

If L is a field and G a group of automorphisms of L then L is a separable extension of the fixed field of G (see e.g. [7, Proposition 7, Chapter 5, Paragraph 15, Section 3, A.V.121]). The following Proposition generalizes this well known fact. It also shows that ϕ-separability is a condition that appears very naturally if one is interested in developing a Galois theory for difference extensions. The reason why ϕ-separability has not appeared in the literature on difference Galois theory so far is that people have only considered inversive difference rings/fields (cf. Corollary 1.5.3).

Proposition 1.5.7. *Let L be a ϕ-pfield and G a group of ϕ-automorphisms of L. Set*

$$K = L^G = \{a \in L;\ g(a) = a \text{ for all } g \in G\}.$$

Then K is a ϕ-pfield and L is ϕ-separable over K.

Proof: One immediately checks that K is a ϕ-subring of L. If $a \in K$ is a non zero divisor then a is invertible in L by Lemma 1.3.4 and as $g(a^{-1}) = g(a)^{-1} = a^{-1}$ we see that $a^{-1} \in K$. Therefore K is total and it follows from Lemma 1.3.4 that K is a ϕ-pfield.

To prove that L is ϕ-separable over K we shall need the following two intermediate results: Let V_0 be a K-ϕ-module and extend the action of G to $V = L \otimes_K V_0$ by $g(a \otimes v) = g(a) \otimes v$. Then

(1) the set of elements of V that are fixed by G is $V_0 = 1 \otimes V_0$ and

(2) every L-ϕ-submodule W of V that is stable under the action of G is generated by $W_0 = W \cap V_0$.

To prove (1) write $K = e_1K \oplus \cdots \oplus e_tK$ and for $i = 1, \ldots, t$ fix an e_iK-basis $\{b_{ij}\}_{j\in J_i}$ of e_iV_0. Then every element v of V is uniquely of the form

$$v = \sum_{i=1}^{t} \sum_{j\in J_i} a_{ij} \otimes b_{ij} \in (e_1L \otimes_{e_1K} e_1V_0) \oplus \cdots \oplus (e_tL \otimes_{e_tK} e_tV_0) = L \otimes_K V_0$$

with $a_{ij} \in e_iL$. Let $g \in G$. Because $e_i \in K$ is fixed by g we know that $g(a_{ij}) \in e_iL$. Thus if $g(v) = v$ then $g(a_{ij}) = a_{ij}$. This implies $a_{ij} \in K$ and consequently $v \in 1 \otimes V_0$.

Now let W be an L-ϕ-submodule of V that is stable under G and set $W_0 = W \cap V_0$. Then $W/(L \otimes_K W_0)$ is an L-ϕ-submodule of $V/(L \otimes_K W_0) = L \otimes_K (V_0/W_0)$ that is stable under the action of G. Thus to prove (2) it suffices to prove that an L-ϕ-submodule W of V which is stable under G and satisfies $W \cap V_0 = 0$ is zero.

Let $\{v_j\}_{j\in J}$ be a generating set of V_0 as K-module. For $v \in V$ let the length of v (with respect to $\{v_j\}_{j\in J}$) be defined as the smallest integer n such that there exists a subset I of J of cardinality n and $a_i \in L$ with

$$v = \sum_{i\in I} a_i \otimes v_i \in L \otimes_K V_0.$$

Suppose for a contradiction that W is non-zero. Then we can choose a non-zero $w \in W$ of minimal length. Then if

$$w = \sum_{i\in I} a_i \otimes v_i \in L \otimes_K V_0$$

is a representation of w of minimal length we can choose $i_0 \in I$ and consider

$$\mathfrak{b} = \left\{ b_{i_0} \in L;\ \exists\, b_i \in L,\ i \in I \smallsetminus \{i_0\} \text{ such that } \sum_{i\in I} b_i \otimes v_i \in W \right\}.$$

As $\mathfrak{b}$ is a non-zero ϕ-ideal of L it must contain 1. So we can assume without loss of generality that $a_{i_0} = 1$. Therefore, for every $g \in G$ the difference $w - g(w) \in W$ has a strictly smaller length than w and so must be zero. This implies that w is fixed by G and so it follows from (1) that $w \in V_0$. This contradicts the assumption $W \cap V_0 = 0$.

Now we are prepared to prove that L is ϕ-separable over K. Let M be a ϕ-pfield containing K. We have to show that

$$\phi : L \otimes_K M \to L \otimes_K M$$

is injective. As above we extend the action of G to $L \otimes_K M$ by $g(a \otimes m) = g(a) \otimes m$. The kernel W of $\phi : L \otimes_K M \to L \otimes_K M$ is then stable under ϕ and the action of G. Thus it follows from (2) that W is generated by $W \cap M$ but as ϕ is injective on M we know that $W \cap M$ must be zero. Therefore W is zero. □

For later reference we record a simple algebraic lemma.

Lemma 1.5.8. *Let R be a ring and A, B R-algebras. Assume that B is flat over R and let a be a non zero divisor of A. Then $a \otimes 1$ is a non zero divisor in $A \otimes_R B$.*

Proof: Since multiplication with a defines an injective map $A \to A$ of R-modules it follows from flatness that multiplication with $a \otimes 1$ is injective on $A \otimes_R B$. □

Unfortunately the Galois theory of linear difference equations (also known as Picard-Vessiot theory) is presented in the standard literature (e.g. [43]) only for inversive base fields (or pseudo-fields). However, with a little care, it is possible to develop the theory in straightforward analogy without this assumption. I.e. one can take an arbitrary ϕ-pfield as the base (cf. Definition 3.3.5).

In classical Galois theory one only considers separable polynomials in order to get the right (i.e. maximal) number of solutions. Similarly in the difference Picard-Vessiot theory one only considers systems of linear difference equations given by an *invertible* matrix in order to be able to obtain a solution space of the maximal dimension. In the classical theory the splitting field of a separable polynomial is separable. As demonstrated in the following proposition the ϕ-analog is also true: The "splitting field" of a system of linear difference equations given by an invertible matrix is ϕ-separable.

Proposition 1.5.9. *Let K be a ϕ-pfield and R a Picard-Vessiot ring over K. Then R is ϕ-separable over K. Similarly if $L|K$ is a Picard-Vessiot extension (of ϕ-pfields) then L is ϕ-separable over K.*

Proof: Let R^* denote the inversive closure of R and set $C = K^\phi = L^\phi$. We know that there is a natural isomorphism $\psi : R \otimes_K R \simeq R \otimes_C D$ where $D = (R \otimes_K R)^\phi$ is the (constant) coordinate ring of the Galois group of $L|K$. (This is essentially the torsor theorem.) We can trivially extend ψ to an isomorphism

$$R^* \otimes_K R \simeq R^* \otimes_C D$$

of ϕ-rings. Because ϕ is injective on $R^* \otimes_C D$ (in fact ϕ is an automorphism on $R^* \otimes_C D$) it follows that ϕ is injective on $R^* \otimes_K R$. Thus R is ϕ-separable over K by Proposition 1.5.2, (2). The fact that $L = \mathfrak{Q}(R)$ is also ϕ-separable over K follows immediately from the following lemma. □

Lemma 1.5.10. *Let K be a ϕ-pfield and R a ϕ-separable K-ϕ-algebra. Let S be a multiplicatively closed, ϕ-stable subset of R consisting of non zero divisors. Then $S^{-1}R$ is also ϕ-separable over K.*

Proof: We first observe that if R is a ϕ-ring with $\phi : R \to R$ injective and S a multiplicatively closed ϕ-stable subset of R consisting of non zero divisors then $\phi : S^{-1}R \to S^{-1}R$ is also injective.

Now let K and R be as stated in the lemma and L a ϕ-pfield extension of K. By assumption ϕ is injective on $R \otimes_K L$. Because $S \otimes 1 \subset R \otimes_K L$ consists of non zero divisors (Lemma 1.5.8) it follows that ϕ is injective on $(S \otimes 1)^{-1}(R \otimes_K L) = S^{-1}R \otimes_K L$. □

We shall need the following algebraic version of Chevalley's Theorem.

Proposition 1.5.11. *Let R be a Noetherian reduced ring and S an overring of R such that S is finitely generated as R-algebra. If s is a non zero divisor of S then there exists a non zero divisor r of R such that for every prime ideal $\mathfrak{q}$ of R with $r \notin \mathfrak{q}$ there exists a prime ideal $\mathfrak{q}'$ of S with $s \notin \mathfrak{q}'$ and $\mathfrak{q}' \cap R = \mathfrak{q}$.*

Proof: The geometric version of Chevalley's Theorem (see e.g. [17, Exercise 3.19, p.94]) states that if $f : Y \to X$ is a morphism of finite type between Noetherian schemes then for any constructible subset D of Y the image of D under f is a constructible subset of X. Let $X = \operatorname{Spec}(R)$, $Y = \operatorname{Spec}(S)$ and f the morphism induced by the inclusion $R \subset S$. Because $s \in S$ is a non zero divisor, s lies outside every minimal prime ideal of S and therefore $D(s) = \{\mathfrak{q}' \in Y;\ s \notin \mathfrak{q}'\}$ is a dense subset of Y. So $f(Y) = f(\overline{D(s)}) \subset \overline{f(D(s))}$. But as $R \subset S$ the morphism f is dominant and so $f(D(s))$ is dense in X. So $f(D(s))$ is a dense and constructible subset of X and must therefore contain a dense open subset of X. This dense open subset can be chosen of the form $D(r)$ for some non zero divisor r of R. □

The relevance of the following proposition will be revealed in the proof of Lemma 3.4.1.

Proposition 1.5.12. *Let $L|K$ be a ϕ-separable extension of ϕ-pfields such that L is finitely generated as total ring over K. Furthermore let R be a Noetherian reduced K-ϕ-algebra and $P \in R \otimes_K L$ a non zero divisor. Then there exists a non zero divisor $r \in R$ such that for every ϕ-prime ideal $\mathfrak{p}$ of R with $r \notin \mathfrak{p}$ there exists a ϕ-prime ideal $\mathfrak{p}'$ of $R \otimes_K L$ with $P \notin \mathfrak{p}'$ and $\mathfrak{p} \subset \mathfrak{p}'$.*

Proof: Let $\eta \in L^n$ such that $L = K(\eta)$. Enlarging η if necessary we may assume that P lies in $R \otimes_K K[\eta]$. Applying Proposition 1.5.11 to the inclusion $R \subset R \otimes_K K[\eta]$ gives us a non zero divisor $r \in R$ such that for every prime ideal $\mathfrak{q}$ of R with $r \notin \mathfrak{q}$ there exists a prime ideal $\mathfrak{q}'$ of $R \otimes_K K[\eta]$ with $P \notin \mathfrak{q}'$ and $\mathfrak{q}' \cap R = \mathfrak{q}$.

Now let $\mathfrak{p} \subset R$ be ϕ-prime with $r \notin \mathfrak{p}$. Then $\mathfrak{p}$ is of the form

$$\mathfrak{p} = \mathfrak{q} \cap \cdots \cap \phi^{-(d-1)}(\mathfrak{q})$$

where $\mathfrak{q}$ is a prime ideal of R with $\phi^{-d}(\mathfrak{q}) = \mathfrak{q}$. Without loss of generality we may assume $r \notin \mathfrak{q}$. As explained above there exists a prime ideal $\mathfrak{q}'$ of $R \otimes_K K[\eta]$ with $P \notin \mathfrak{q}'$ and $\mathfrak{q}' \cap R = \mathfrak{q}$. In particular $\mathfrak{p} \otimes K[\eta] \subset \mathfrak{q}'$. Since $P \notin \mathfrak{q}'$ we have $P^k \notin \mathfrak{q}'$ for $k \geq 1$ and so $P^k \notin \mathfrak{p} \otimes K[\eta] \subset \mathfrak{q}'$. This implies $P^k \notin \mathfrak{p} \otimes L$ because $(\mathfrak{p} \otimes L) \cap (R \otimes_K K[\eta]) = \mathfrak{p} \otimes K[\eta]$ ([8, Proposition 7, Chapter 1, Paragraph 2, Section 6, p. 18]). In other words $P \notin \sqrt{\mathfrak{p} \otimes L}$.

From Corollary 1.5.4 we know that $\mathfrak{p} \otimes L$ is a reflexive ϕ-ideal and so by Proposition 1.4.7 we see that $\sqrt{\mathfrak{p} \otimes L}$ is a ϕ-radical ϕ-ideal of $R \otimes_K L$. Since $R \otimes_K L$ is Noetherian we know from Proposition 1.4.8 that $\sqrt{\mathfrak{p} \otimes L}$ is the intersection of ϕ-prime ideals and since $P \notin \sqrt{\mathfrak{p} \otimes L}$ at least one of these does not contain P. □

1.6 ϕ-pfields with bounded periodicity

In this section we introduce the concept of "bounded periodicity" and provide some elementary results about ϕ-pfields with bounded periodicity. "Bounded periodicity" is a technical condition that will be helpful in developing the ϕ-Galois theory later on. In particular a ϕ-Galois extension $L|K$ will be assumed to be of bounded periodicity.

Definition 1.6.1. *Let L be a ϕ-pfield. An element a of L is called* periodic *if there exists an integer $d \geq 1$ such that $\phi^d(a) = a$. The set of all periodic elements of L is denoted by L^{ϕ^∞}.*

Clearly L^{ϕ^∞} is an L^ϕ-ϕ-algebra and $\phi : L^{\phi^\infty} \to L^{\phi^\infty}$ is an isomorphism. We also note that all the idempotent elements of L belong to L^{ϕ^∞}.

Definition 1.6.2. *Let L be a ϕ-pfield. We say that L* has bounded periodicity *if there exists an integer $N \geq 1$ such that for every $a \in L^{\phi^\infty}$ we have $\phi^N(a) = a$.*

Lemma 1.6.3. *Let L be a ϕ-field. Then L^{ϕ^∞} is the relative algebraic closure of L^ϕ in L and is a cyclic Galois extension of L^ϕ with Galois group generated by ϕ.*

Proof: By [29, Theorem 2.1.12, p. 114] we know that L^{ϕ^∞} agrees with the relative algebraic closure of L^ϕ in L. By Artin's Theorem L^{ϕ^d} is a Galois extension of L^ϕ with Galois group generated by ϕ for every $d \geq 1$. □

Proposition 1.6.4. *Let $L = e_1L \oplus \cdots \oplus e_tL$ be a ϕ-pfield and set $C = L^\phi$. Then the following statements are equivalent:*

(1) *L has bounded periodicity.*

(2) *L^{ϕ^∞} is a finite dimensional C-vector space.*

(3) *The relative algebraic closure of e_iC in e_iL is a finite extension of e_iC for $i = 1, \dots, t$.*

Proof: Let $D_i \subset e_iL$ denote all periodic elements of (e_iL, ϕ^t). Then one immediately sees that

$$L^{\phi^\infty} = D_1 \oplus \cdots \oplus D_t.$$

The claim now follows from Lemma 1.6.3 and Lemma 1.3.5. □

Lemma 1.6.5. *Let L be a ϕ-pfield. If L^ϕ is algebraically closed or L is finitely generated as total ring over L^ϕ then L has bounded periodicity.*

Proof: The case when L^ϕ is algebraically closed is clear from Proposition 1.6.4. If $L = e_1L \oplus \cdots \oplus e_tL$ is finitely generated as total ring over L^ϕ then e_iL is a finitely generated field extension of e_iL^ϕ for every $i = 1, \dots, t$. Thus the relative algebraic closure of e_iL^ϕ in e_iL must be finite (see [7, Corollary 1, Chapter 5, Paragraph 14, Section 7, A.V.117]) and it follows again from Proposition 1.6.4 that L has bounded periodicity. □

The typical example of a ϕ-pfield which does not have bounded periodicity is $\overline{\mathbb{F}_p}$, the algebraic closure of the finite field with p elements where ϕ is taken as the Frobenius.

Lemma 1.6.6. *Let L be a ϕ-pfield with bounded periodicity, $C = L^\phi$ and D a C-algebra. Then there exists $N \geq 1$ such that $\phi^{-N}(\mathfrak{q}) = \mathfrak{q}$ for every $\mathfrak{q} \in \phi\text{-}\mathrm{Spec}(L \otimes_C D)$.*

Proof: By Proposition 1.4.15 every ϕ-prime ideal of $R = L \otimes_C D$ is of the from $L \otimes \mathfrak{p}$ where $\mathfrak{p}$ is a prime ideal of D. Therefore it suffices to find an $N \geq 1$ such that for every prime ideal $\mathfrak{p}$ of D the ideal $L \otimes \mathfrak{p}$ of R has at most N minimal prime ideals. If $L = e_1 L_1 \oplus \cdots \oplus e_t L$ then

$$L \otimes \mathfrak{p} = (e_1 L \otimes \mathfrak{p}) \oplus \cdots \oplus (e_t L \otimes \mathfrak{p}) \subset (e_1 L \otimes D) \oplus \cdots \oplus (e_t L \otimes D) = L \otimes D.$$

So by Lemma 1.3.5 we can assume without loss of generality that L is a ϕ-field. Then by Lemma 1.6.4 the relative algebraic closure E of $C = L^\phi$ in L is a finite extension of C. Let $N = [E : C]$. We have an inclusion

$$E \otimes_C (D/\mathfrak{p}) \hookrightarrow E \otimes_C \mathfrak{Q}(D/\mathfrak{p}).$$

As $E \otimes_C \mathfrak{Q}(D/\mathfrak{p})$ is a $\mathfrak{Q}(D/\mathfrak{p})$-vector space of dimension N there are at most N prime ideals in $E \otimes_C \mathfrak{Q}(D/\mathfrak{p})$. By [8, Proposition 16, Chapter II, Paragraph 2.6, p. 74] every minimal prime ideal of $E \otimes_C (D/\mathfrak{p})$ comes from a minimal prime ideal of $E \otimes_C \mathfrak{Q}(D/\mathfrak{p})$. Therefore $E \otimes_C (D/\mathfrak{p})$ has at most N minimal primes.

Because E is relatively algebraically closed in L it follows from [42, Proposition 2 (c), p.27] that there is a bijection between the minimal prime ideals of $E \otimes_C (D/\mathfrak{p})$ and the minimal prime ideals of

$$L \otimes_E (E \otimes_C (D/\mathfrak{p})) = L \otimes_C (D/\mathfrak{p}) = (L \otimes_C D)/L \otimes_C \mathfrak{p}.$$

Thus $L \otimes_C \mathfrak{p}$ has at most N minimal prime ideals. □

Lemma 1.6.7. *Let R be a ϕ-ring and $r \in R$. Assume that there exists $N \geq 1$ such that $\phi^{-N}(\mathfrak{q}) = \mathfrak{q}$ for every $\mathfrak{q} \in \phi\text{-}\mathrm{Spec}(R)$ and set $\widetilde{r} = r\phi(r) \cdots \phi^{N-1}(r)$. Then for $\mathfrak{q} \in \phi\text{-}\mathrm{Spec}(R)$ we have $\mathfrak{q} \cap \langle \phi, \widetilde{r} \rangle = \emptyset$ if and only if $\widetilde{r} \notin \mathfrak{q}$. In particular $D(\widetilde{r}) \subset \phi\text{-}\mathrm{Spec}(R)$ is Φ-stable.*

Proof: Assume for a contradiction that $\widetilde{r} \notin \mathfrak{q}$ and $\phi^{\alpha_1}(\widetilde{r})^{\beta_1} \cdots \phi^{\alpha_n}(\widetilde{r})^{\beta_n} \in \mathfrak{q}$. Inserting the expression for $\widetilde{r}$ into this formula and using that $\mathfrak{q}$ is prime we conclude that there exists $m \geq 0$ such that $\phi^m(r) \in \mathfrak{q}$. As $\phi^{-N}(\mathfrak{q}) = \mathfrak{q}$ we can assume that $m \leq N-1$, but this implies $\widetilde{r} \in \mathfrak{q}$. □

Lemma 1.6.8. *Let L be a ϕ-pfield with bounded periodicity, $C = L^\phi$ and C' an algebraic extension of C (considered as constant ϕ-ring). Then*

$$L' = L \otimes_C C'$$

is a ϕ-pfield with $L'^\phi = C'$.

Proof: We already know from Proposition 1.4.15 that L' is ϕ-simple. Thus to show that L' is a ϕ-pfield it suffices to see that L' is a finite direct product of fields. For this we can assume that L is a field (Lemma 1.3.5 and Proposition 1.6.4).

Let $D = L^{\phi^\infty}$. It follows from the assumption and Lemma 1.6.3 that D is a *finite* Galois extension of C and that D is relatively algebraically closed in L. We have

$$L' = L \otimes_D (D \otimes_C C').$$

We know that $D \otimes_C C'$ is a finite product of algebraic field extensions of D, say $D \otimes_C C' = D_1 \oplus \cdots \oplus D_n$. (To see this write $D = C[x]/(f)$ where f is an irreducible, separable polynomial in $C[x]$. Then

$$D \otimes_C C' = C'[x]/(f) \simeq C'[x]/(f_1) \oplus \cdots \oplus C'[x]/(f_n)$$

where $f_1, \ldots, f_n$ denote the irreducible factors of f in $C'[x]$.) Therefore

$$L' = (L \otimes_D D_1) \oplus \cdots \oplus (L \otimes_D D_n).$$

Because D is relatively algebraically closed in L one knows that the nilradical of $L \otimes_C D_i$ is a prime ideal ([7, Corollary, Chapter V, Paragraph 17, Section 2 A.V.140]), but as L' is reduced (it is even ϕ-simple) we know that also $L \otimes_D D_i$ is reduced. Thus $L \otimes_D D_i$ is an integral domain. Because D_i is algebraic over D every element of $L \otimes_D D_i$ is algebraic over L, from this it follows that $L \otimes_D D_i$ is a field. (If a is an element of $L \otimes_D D_i$ then the kernel of $L[x] \to L \otimes_D D_i$, $x \mapsto a$ is a non-zero prime ideal of $L[x]$ which hence must be maximal.) The fact that $L'^\phi = C'$ follows from Lemma 1.4.14. □

We note that if $L = e_1 L \oplus \cdots \oplus e_t L$ and $L' = L \otimes_C C' = e'_1 L' \oplus \cdots \oplus e'_{t'} L'$ then it might well happen that t' is strictly larger then t. In particular if L is a ϕ-field then $L \otimes_C C'$ need not be a ϕ-field. So we have another instant where ϕ-pfields prove to be better behaved then ϕ-fields. In fact if L is a ϕ-field which contains a non-constant periodic element then $L \otimes_C \overline{C}$ will not be a field. (Here $\overline{C}$ denotes the algebraic closure of $C = L^\phi$.)

We also remark that the above lemma is not true without the finite periodicity assumption. For example if $L = \overline{\mathbb{F}_p}$ is the algebraic closure of the field with p elements considered as difference ring by virtue of the Frobenius endomorphism $\phi : a \mapsto a^p$. Then $C = L^\phi = \mathbb{F}_p$ and $L \otimes_C \overline{\mathbb{F}_p} = \overline{\mathbb{F}_p} \otimes_{\mathbb{F}_p} \overline{\mathbb{F}_p}$ is not a ϕ-pfield because it is not Noetherian. Indeed $\overline{\mathbb{F}_p} \otimes_{\mathbb{F}_p} \overline{\mathbb{F}_p}$ can not be Noetherian because this ring has infinitely many minimal prime ideals. (All prime ideals of $\overline{\mathbb{F}_p} \otimes_{\mathbb{F}_p} \overline{\mathbb{F}_p}$ are maximal and hence minimal and they are in one-to-one correspondence with the automorphisms of $\overline{\mathbb{F}_p}$ over $\mathbb{F}_p$.)

In fact it is not difficult to see that a ϕ-pfield L has bounded periodicity if and only if $L \otimes_C C'$ is a ϕ-pfield for every algebraic extension of C' of C.

Lemma 1.6.9. *Let $L|K$ be an extension of ϕ-pfields such that $K^\phi = L^\phi$ and L has bounded periodicity. Let C' be an algebraic extension of $C = K^\phi = L^\phi$ and set $L' = L \otimes_C C'$ and $K' = K \otimes_C C'$. Then $L'|K'$ is an extension of ϕ-pfields such that $K'^\phi = L'^\phi = C'$ and L' has bounded periodicity.*

Proof: It follows from Lemma 1.6.8 that L' and K' are ϕ-pfields. By Lemma 1.4.14 we know that $L'^{\phi^n} = L^{\phi^n} \otimes_C C'$. In particular L' has bounded periodicity and $L'^{\phi} = C' = K'^{\phi}$. □

1.7 The algebraic structure of $L \otimes_K L$

We recall that a ring R is called *primary* if its zero ideal is primary, i.e. if every zero divisor of R is nilpotent. This implies that the nilradical of R is prime (but the converse is not true).

Lemma 1.7.1. *Let $L|K$ be an extension of ϕ-pfields such that L is finitely generated as total ring over K. Then $L \otimes_K L$ is a finite direct product of primary rings.*

Proof: We first note that if L and L' are field extensions of a field K such that K is separably algebraically closed in L' then $L \otimes_K L'$ is a primary ring ([42, Proposition 2 (a), p. 27]).

If L and L' are finitely generated field extensions of K then $L \otimes_K L'$ is Noetherian (cf. Lemma 1.2.4), and so in particular the are only finitely many minimal prime ideals in $L \otimes_K L$. Thus it follows from [42, Proposition 5, p. 28] that $L \otimes_K L'$ is a finite direct product of primary rings.

Now the general case easily reduces to this one: If $K = e_1K \oplus \cdots \oplus e_tK$ then

$$L \otimes_K L = (e_1L \otimes_{e_1K} e_1L) \oplus \cdots \oplus (e_tL \oplus_{e_tK} e_tL).$$

Thus we can assume without loss of generality that K is field. (If L is finitely generated over K then also e_iL is finitely generated over e_iK.) Then if $L = e_1L \oplus \cdots \oplus e_tL$ we have

$$L \otimes_K L = \bigoplus_{1 \leq i,j \leq t} e_iL \otimes_K e_jL.$$

All the summands are orthogonal to each other and as L is finitely generated as total ring over K we see that e_iL is finitely generated as a field over K. Thus the general claim follows from the case of fields explained above. □

Proposition 1.7.2. *Let $L|K$ be an extension of ϕ-pfields such that L is finitely generated as total ring over K and ϕ is injective on $L \otimes_K L$. Then $L \otimes_K L$ is a finite direct product of difference rings of the form*

$$R = R_1 \oplus \cdots \oplus R_n$$

where the R_i's are primary rings and $\phi^{-1}(R_i) = R_{i-1}$ (in a cyclic notation).

Proof: By Lemma 1.7.1 there exist primary rings $R_1, \ldots, R_n$ such that

$$L \otimes_K L = R_1 \oplus \cdots \oplus R_n.$$

For $i = 1, \ldots, n$ let

$$\mathfrak{a}_i = R_1 + \cdots + R_{i-1} + R_{i+1} + \cdots + R_n.$$

Then $\mathfrak{a}_i$ is a primary ideal of $L \otimes_K L$ and

$$0 = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$$

is the unique primary decomposition of the zero ideal in $L \otimes_K L$. (It is unique because there are no embedded components.) By assumption $\phi : L \otimes_K L \to L \otimes_K L$ is injective and therefore

$$0 = \phi^{-1}(0) = \phi^{-1}(\mathfrak{a}_1) \cap \cdots \cap \phi^{-1}(\mathfrak{a}_n)$$

is another (but actually the same) primary decomposition. This shows that ϕ^{-1} permutes the $\mathfrak{a}_i$'s. The cycle decomposition of this permutation yields the desired decomposition of $L \otimes_K L$. □

Proposition 1.7.3. *Let $L|K$ be an extension of ϕ-pfields such that L is finitely generated as total ring over K and ϕ is injective on $L \otimes_K L$ (e.g. $L|K$ is ϕ-separable). Then the set of non zero divisors of $R = L \otimes_K L$ is ϕ-stable and therefore ϕ extends naturally to the total ring of quotients $\mathfrak{Q}(R)$ of R. Moreover if $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ denote the minimal ϕ-prime ideals of R then*

$$\mathfrak{Q}(R) \simeq R_{\mathfrak{p}_1} \oplus \cdots \oplus R_{\mathfrak{p}_m}.$$

Proof: By Lemma 1.7.1 we know that $R = R_1 \oplus \cdots \oplus R_n$ is a finite direct product of primary rings R_i. For $i = 1, \ldots, n$ let $\mathfrak{r}_i$ denote the nilradical of R_i and set

$$\mathfrak{b}_i = R_1 + \cdots + R_{i-1} + \mathfrak{r}_i + R_{i+1} + \cdots + R_n.$$

Then $\mathfrak{b}_1, \ldots, \mathfrak{b}_n$ is the set of minimal prime ideals of R and this also agrees with the set of associated prime ideals of R. An element of R is a non zero divisor if and only if it lies outside every $\mathfrak{b}_i$. As in Proposition 1.7.2 on sees that ϕ^{-1} induces a permutation of the $\mathfrak{b}_i$'s. Thus the set of non zero divisors of R is stable under ϕ.

Because $\phi : R \to R$ is injective the nilradical of R is a reflexive ideal, i.e. the nilradical of R is a ϕ-radical ideal and thus it is the intersection of the minimal ϕ-prime ideals (Proposition 1.4.8). In particular, if $s \in R$ is a non zero divisor then $s \in S(\mathfrak{p}_i)$ (see Definition 1.4.5) for $i = 1, \ldots, n$.

We have a canonical morphism of difference rings

$$\psi : R \to R_{\mathfrak{p}_1} \oplus \cdots \oplus R_{\mathfrak{p}_m},\ r \mapsto \frac{r}{1} + \cdots + \frac{r}{1}.$$

As seen above it maps non zero divisors to invertible elements. Thus it extends to

$$\psi : \mathfrak{Q}(R) \to R_{\mathfrak{p}_1} \oplus \cdots \oplus R_{\mathfrak{p}_m}.$$

If $r \in R$ such that $\psi(r) = 0$ then there exists for $i = 1, \ldots, m$ an $s_i \in S(\mathfrak{p}_i)$ such that $s_i r = 0$. In particular $\operatorname{Ann}(r) \nsubseteq \mathfrak{b}_j$ for $j = 1, \ldots, n$. But this means $1 \in \operatorname{Ann}(r)$, i.e. $r = 0$. Thus ψ is injective.

To see that ψ is surjective it suffices to see that it maps surjectively onto the first factor say. So let $\frac{r}{s} \in R_{\mathfrak{p}_1}$ with $r \in R$ and $s \in S(\mathfrak{p}_1)$. After renumbering we may assume that $\mathfrak{b}_1, \ldots, \mathfrak{b}_l$ are the minimal prime ideals of $\mathfrak{p}_1$.

Let $r = r_1 + \cdots + r_n$ and $s = s_1 + \cdots + s_n$ be the representations according to the decomposition $R = R_1 \oplus \cdots \oplus R_n$. Set $r' = r_1 + \cdots + r_l$ and $s' = s_1 + \cdots + s_l + 1 + \cdots + 1 \in R_1 \oplus \cdots \oplus R_l \oplus R_{l+1} \oplus \cdots \oplus R_n$. If e denotes the element of $R = R_1 \oplus \cdots \oplus R_n$ having ones at the first l places an zeros afterwards then $e \in S(\mathfrak{p}_1)$ and $e(r - r') = 0$, $e(s - s') = 0$ and so $\psi(\frac{r'}{s'}) = \frac{r}{s}$. □

Chapter 2

ϕ-algebraic geometry

In this chapter we develop some basic notions of difference algebraic geometry to the extend that we shall need in the next chapter for our main goal: difference Galois theory. Classical difference algebraic geometry (and classical algebraic geometry) is governed by the paradigm that points are tuples with entries in some field. The basic setup is as follows (see e.g. [10]): One starts with a fixed difference field K and one wants to study difference equations over K, i.e. one is interested in the solutions of a given set of difference polynomials with coefficients in K. These solutions are to be found in difference overfields of K. One usually fixes a family of difference overfields of K which is large enough to yield a kind of difference Nullstellensatz.

As in usual algebraic geometry this point of view is adequate for many things but has some limitations. For example the classical setup does not allow nilpotent elements in the structure sheaf. This is a very important feature also for our difference Galois theory because in positive characteristic one can have non-reduced Galois groups (corresponding to inseparable extensions). Thus it is not only the fact that it is about time that difference (as well as differential) algebraic geometry embraced Grothendieck's ideas but also concrete mathematical needs that lead us to the use of difference schemes. Unfortunately the theory of difference schemes is still in its infancy.

In a fascinating article [18] E. Hrushovski develops the notions of difference algebraic geometry in scheme theoretic language to a quite advanced degree but regrettably his definitions and theorems apply well only for well-mixed rings. A ϕ-ring R is called well-mixed if for $a, b \in R$ with $ab = 0$ one has $\phi(a)b = 0$. In other words a difference ring is well-mixed if and only if annihilators are difference ideals. As a set Hrushovski defines the difference spectrum of a difference ring to be the set of reflexive prime ideals.

A characteristic feature of difference Galois theory as compared to differential Galois theory is that Picard-Vessiot rings and Picard-Vessiot extensions can have zero divisors. Since of course the difference Galois theory which we want to develop here should contain the Picard-Vessiot theory we also have to work with ϕ-pfields instead of ϕ-fields. But with Hrushovski's definition the difference spectrum of a ϕ-pfield is the empty set unless it is a ϕ-field. As already indicated in Section 1.3 the solution is to also take into account the higher powers of ϕ. In other words we do not only consider the difference spectrum with respect to ϕ but simultaneously the difference spectrum with respect to ϕ^n for all $n \geq 1$.

We stress the point that the present chapter is not a sound introduction to difference algebraic geometry. In fact we do not even give the definition of a difference scheme. Rather it is a collection of definitions and results aimed to provide the necessary tools for the development of a *geometric* difference Galois theory. In particular we do not hesitate to introduce a Noetherianity assumption whenever useful. For the situation usually of interest in difference algebraic geometry this assumption will not be satisfied.

2.1 Basic definitions

This section contains the very basic definitions and ends with some results on the existence of fibred products.

In usual algebraic geometry there are different ways to introduce the spectrum of a ring. But maybe the most conceptual one is to say that Spec$(-)$ is the adjoint of the global section functor, which is a functor from the category of locally ringed spaces to the category of rings. If we want the difference analog to be true it is then clear that the difference spectrum will be determined by specifying an ambient category. If one takes as the objects of this ambient category locally ringed spaces together with an endomorphism of locally ringed spaces that is the identity on points one obtains Hrushovski's notion of difference spectrum. Here we need to allow the endomorphism to move the points but only in a very restricted way.

Definition 2.1.1. *By a* ϕ-space *we mean a locally ringed space* $(X, \mathcal{O}_X)$ *together with a morphism* $(\Phi, \phi) : (X, \mathcal{O}_X) \to (X, \mathcal{O}_X)$ *of locally ringed spaces such that* Φ *is pointwise of finite order. That is, for every* $x \in X$ *there exists a* $d_x \geq 1$ *such that* $\Phi^{d_x}(x) = x$.

Often the ϕ-space will simply be denoted with X or (X, Φ) or (X, Φ_X), the other data being implicitly understood. For $x \in X$ the maximal ideal of $\mathcal{O}_{X,x}$ is denoted with $\mathfrak{m}_x$ and if $s \in \mathcal{O}_X(U)$ for some open subset U of X containing x then the image of s in $\mathcal{O}_{X,x}$ is denoted with s_x.

Lemma 2.1.2. *If* (X, Φ) *is a* ϕ*-space then* $\Phi : X \to X$ *is bijective and for a subset* U *of* X *the following are equivalent:*

(1) $\Phi(U) \subset U$

(2) $\Phi(U) = U$

(3) $U = \Phi^{-1}(U)$

We omit the trivial proof.

Definition 2.1.3. *A subset* U *of* X *satisfying the equivalent conditions of Lemma 2.1.2 is called* Φ*-stable.*

If $U \subset X$ is an open, Φ-stable subset then $\mathcal{O}_X(U)$ has naturally the structure of a difference ring given by $\phi(U) : \mathcal{O}_X(U) \to \mathcal{O}_X(\Phi^{-1}(U)) = \mathcal{O}_X(U)$ and if $V \subset U$ is an inclusion of open, Φ-stable subsets then the corresponding restriction map is a morphism of difference rings. We will often just write ϕ, (or ϕ_U if we want to be more precise) for $\phi(U)$.

Remark 2.1.4. *Let X be a ϕ-space, $x \in X$ and $d \geq 1$ the smallest integer such that $\Phi^d(x) = x$. Then $\mathcal{O}_{X,x}$ has naturally the structure of a difference ring. Somewhat suggestively this endomorphism $\mathcal{O}_{X,x} \to \mathcal{O}_{X,x}$ is denoted with ϕ_x^d. We have $(\phi_x^d)^{-1}(\mathfrak{m}_x) = \mathfrak{m}_x$ and the natural map $(\mathcal{O}_X(X), \phi_X^d) \to (\mathcal{O}_{X,x}, \phi_x^d)$ is a morphism of difference rings.*

Proof: The morphism $(\Phi, \phi) : (X, \mathcal{O}_X) \to (X, \mathcal{O}_X)$ of locally ringed spaces induces local morphisms of local rings

$$\phi_x^d : \mathcal{O}_{X,x} = \mathcal{O}_{X,\Phi(\Phi^{d-1}(x))} \to \mathcal{O}_{X,\Phi^{d-1}(x)} \to \cdots \to \mathcal{O}_{X,\Phi(x)} \to \mathcal{O}_{X,x}.$$

□

Definition 2.1.5. *A morphism between ϕ-spaces (X, Φ) and (X', Φ') is a morphism $f : X \to X'$ of locally ringed spaces such that*

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, "\Phi"'] & X' \arrow[d, "\Phi'"] \\
X \arrow[r, "f"] & X'
\end{tikzcd}$$

commutes.

If U is an open Φ-stable subset of a ϕ-space X then U has naturally the structure of a ϕ-space by restricting $\mathcal{O}_X$ and Φ to U and the inclusion map is a morphism of ϕ-spaces.

Definition 2.1.6. *A ϕ-space $(X, (\Phi, \phi))$ is called* constant (or trivial) *if Φ and ϕ are the identity mappings.*

The category of constant ϕ-spaces is thus simply the category of locally ringed spaces and the category of schemes is a full subcategory of the category of ϕ-spaces.

Let R be a ϕ-ring. As a set we define

$$\phi\text{-Spec}(R) = \{\mathfrak{q} \subset R \text{ prime ideal ; there exists } d \geq 1 \text{ such that } \phi^{-d}(\mathfrak{q}) = \mathfrak{q}\}.$$

As topology we use the subspace topology induced from the usual (Zariski) topology on Spec(R). So a subset of ϕ-Spec(R) is closed if and only if it is of the form

$$\mathbb{V}(\mathfrak{a}) = \{\mathfrak{q} \in \phi\text{-Spec}(R);\ \mathfrak{q} \supset \mathfrak{a}\}$$

for some subset (or ideal) $\mathfrak{a}$ of R. It is also clear that the open sets of the form

$$D(r) = \{\mathfrak{q} \in \phi\text{-Spec}(R);\ r \notin \mathfrak{q}\}$$

with $r \in R$ are a basis of the topology of ϕ-Spec(R). The structure sheaf $\mathcal{O}_{\phi\text{-Spec}(R)}$ of ϕ-Spec(R) is defined to be the restriction of the usual structure sheaf $\mathcal{O}_{\text{Spec}(R)}$ on Spec(R). So if U is open subset of ϕ-Spec(R) then an element s of $\mathcal{O}_{\phi\text{-Spec}(R)}(U)$ can explicitly be described as a function

$$s : U \to \coprod_{\mathfrak{q}\in U} R_{\mathfrak{q}}$$

with the properties that $s(\mathfrak{q}) \in R_{\mathfrak{q}}$ for all $\mathfrak{q} \in U$ and for each $\mathfrak{q} \in U$ there exists an open neighborhood V of $\mathfrak{q}$ in U and elements $a, b \in R$ such that $b \notin \mathfrak{q}'$ and $s(\mathfrak{q}') = \frac{a}{b} \in R_{\mathfrak{q}'}$ for all $\mathfrak{q}' \in V$.

For $\mathfrak{q} \in \phi$-Spec(R) the stalk $\mathcal{O}_{\phi\text{-Spec}(R),\mathfrak{q}}$ is naturally identified with $R_{\mathfrak{q}}$.

We define

$$\Phi : \phi\text{-Spec}(R) \to \phi\text{-Spec}(R)$$

by $\Phi(\mathfrak{q}) = \phi^{-1}(\mathfrak{q})$ and if U is an open subset of ϕ-Spec(R) then we define

$$\phi(U) : \mathcal{O}_{\phi\text{-Spec}(R)}(U) \to \mathcal{O}_{\phi\text{-Spec}(R)}(\Phi^{-1}(U))$$

by

$$\phi(U)(s)(\mathfrak{q}) = \phi_{\mathfrak{q}}(s(\Phi(\mathfrak{q}))) \in R_{\mathfrak{q}}$$

for $\mathfrak{q} \in \Phi^{-1}(U)$ and $s \in \mathcal{O}_{\phi\text{-Spec}(R)}(U)$. Here $\phi_{\mathfrak{q}} : R_{\Phi(\mathfrak{q})} \to R_{\mathfrak{q}}$ is given by $\phi_{\mathfrak{q}}(\frac{a}{b}) = \frac{\phi(a)}{\phi(b)}$. One immediately verifies that

$$(\Phi, \phi) : \big(\phi\text{-Spec}(R), \mathcal{O}_{\phi\text{-Spec}(R)}\big) \longrightarrow \big(\phi\text{-Spec}(R), \mathcal{O}_{\phi\text{-Spec}(R)}\big)$$

is a morphism of locally ringed spaces and so ϕ-Spec(R) is a ϕ-space.

It is also straight forward to check that ϕ-Spec$(-)$ is indeed a functor from the category of ϕ-rings to the category of ϕ-spaces: If $\psi : R \to S$ is a morphism of difference rings then

$$\phi\text{-Spec}(\psi) : \phi\text{-Spec}(S) \longrightarrow \phi\text{-Spec}(R)$$

is defined by sending $\mathfrak{q} \in \phi$-Spec(S) to $\psi^{-1}(\mathfrak{q}) \in \phi$-Spec$(R)$. A section of ϕ-Spec(R) which is locally given by a fraction $\frac{a}{b}$ is mapped to a section over ϕ-Spec(S) which is then locally given by $\frac{\psi(a)}{\psi(b)}$.

If R is a ϕ-ring then we denote with $\widehat{R}$ the difference ring of global sections of ϕ-Spec(R). There is a canonical map of difference rings

$$\iota : R \to \widehat{R},\ r \mapsto \widehat{r}$$

given by $\iota(r)(\mathfrak{q}) = \frac{r}{1} \in R_{\mathfrak{q}}$ for $\mathfrak{q} \in \phi$-Spec(R).

We note that if R is a ϕ-ring and $n \geq 1$ then ϕ-Spec(R) and ϕ^n-Spec(R) are equal as sets and even as locally ringed spaces but not (in general) as difference spaces.

Example 2.1.7. Let $K = e_1K \oplus \cdots \oplus e_tK$ be a ϕ-pfield. Then ϕ-Spec(K) is a discrete topological space consisting of t points which form a single orbit under Φ. The local ring at the prime ideal $(1 - e_i)K$ is e_iK. In particular $\iota : K \to \widehat{K}$ is an isomorphism.

Example 2.1.8. Let R be a Noetherian ϕ-simple ring. By Lemma 1.1.5 we can (uniquely) extend ϕ to $\mathfrak{Q}(R)$ and then $\mathfrak{Q}(R)$ is a ϕ-pfield. It follows easily from Proposition 1.1.2 that the morphism

$$\phi\text{-Spec}(\mathfrak{Q}(R)) \to \phi\text{-Spec}(R)$$

induced from $R \to \mathfrak{Q}(R)$ is an isomorphism of ϕ-spaces.

Lemma 2.1.9. *Let R be a Noetherian ϕ-ring. Then there is a one-to-one correspondence between the closed Φ-stable subsets of ϕ-*Spec(R) *and the ϕ-radical ideals of R. More precisely every closed Φ-stable subset of ϕ-*Spec(R) *is of the form $\mathbb{V}(\mathfrak{a})$ for a uniquely determined ϕ-radical ideal $\mathfrak{a}$ of R.*

Proof: Let $V \subset \phi$-Spec(R) be closed and Φ-stable. Then $V = \mathbb{V}(\mathfrak{b})$ for some ideal $\mathfrak{b}$ of R. Set

$$\mathfrak{a} = \bigcap_{\mathfrak{q} \in \mathbb{V}(\mathfrak{a})} \mathfrak{q}.$$

Then $\mathbb{V}(\mathfrak{b}) = \mathbb{V}(\mathfrak{a})$ and because V is Φ-stable it follows that $\mathfrak{a}$ is ϕ-radical. If $\mathfrak{a}$ and $\mathfrak{a}'$ are ϕ-radical ideals of R then it follows from Proposition 1.4.8 that $\mathfrak{a} = \mathfrak{a}'$. □

For later use we record the following simple lemma.

Lemma 2.1.10. *Let $(X, \mathcal{O}_X)$ be a locally ringed space and $s \in \mathcal{O}_X(X)$. Then*

$$X_s = \{x \in X;\ s_x \notin \mathfrak{m}_x\}$$

is an open subset of X and $s|_{X_s}$ is invertible in $\mathcal{O}_X(X_s)$.

Proof: Let $x \in X_s$. Then $s_x \notin \mathfrak{m}_x$ and so s_x is invertible in $\mathcal{O}_{X,x}$. This means that there exists an open neighborhood U of x such that $s|_U$ is invertible in $\mathcal{O}_X(U)$. Thus $s_{x'} \notin \mathfrak{m}_{x'}$ for all $x' \in U$ and X_s is open.

As seen above, for every $x \in X_s$ there exists an open neighborhood U of x in X_s and an element $t \in \mathcal{O}_X(U)$ which is inverse to $s|_U$. By the uniqueness of the inverse the t's glue together to a section of U which is then of course the inverse of $s|_{X_s}$. □

Theorem 2.1.11. *The functor ϕ-*Spec$(-)$ *is the adjoint of the global section functor Γ : $\underline{\phi\text{-spaces}} \to \underline{\phi\text{-rings}}$. In particular if X is a ϕ-space and R a ϕ-ring then there is a natural bijection*

$$\mathrm{Hom}(X, \phi\text{-Spec}(R)) \simeq \mathrm{Hom}(R, \Gamma(X)).$$

Proof: Let X be a ϕ-space and $\psi : R \to \mathcal{O}_X(X)$ a morphism of difference rings. We will construct a morphism $(\psi^a, \psi^\sharp) : (X, \mathcal{O}_X) \to \big(\phi\text{-Spec}(R), \mathcal{O}_{\phi\text{-Spec}(R)}\big)$ of ϕ-spaces.

Let $x \in X$ and $d \geq 1$ minimal with $\Phi^d(x) = x$. Because

$$\rho_x : (\mathcal{O}_X(X), \phi_X^d) \to (\mathcal{O}_{X,x}, \phi_x^d)$$

is a morphism of difference rings and $(\phi_x^d)^{-1}(\mathfrak{m}_x) = \mathfrak{m}_x$ (see Remark 2.1.4) we see that $\mathfrak{q} = \psi^{-1}(\rho_x^{-1}(\mathfrak{m}_x))$ is a prime ideal of R with $\phi^{-d}(\mathfrak{q}) = \mathfrak{q}$. We can thus define ψ^a by $\psi^a(x) = \psi^{-1}(\rho_x^{-1}(\mathfrak{m}_x))$. Next we check that ψ^a is continuous.

For $r \in R$ and $x \in X$ we have $\psi^a(x) \in D(r)$ if and only if $\psi(r)_x \notin \mathfrak{m}_x$. Therefore

$$(\psi^a)^{-1}(D(r)) = X_{\psi(r)}.$$

Because the $D(r)$'s are a basis of the topology and $X_{\psi(r)}$ is open by Lemma 2.1.10 we conclude that ψ^a is continuous.

To construct $\psi^\sharp : \mathcal{O}_{\phi\text{-Spec}(R)} \to \psi^a_*\mathcal{O}_X$ let $U \subset \phi\text{-Spec}(R)$ be open and $s \in \mathcal{O}_{\phi\text{-Spec}(R)}(U)$. Let $r, a, b \in R$ such that $D(r) \subset U$ and s is given on $D(r)$ by the fraction $\frac{a}{b}$. So in particular $D(r) \subset D(b)$.

By Lemma 2.1.10, $\psi(b)|_{X_{\psi(b)}}$ is invertible in $\mathcal{O}_X(X_{\psi(b)})$. Because

$$X_{\psi(r)} = (\psi^a)^{-1}(D(r)) \subset (\psi^a)^{-1}(D(b)) = X_{\psi(b)}$$

we see that $\psi(b)|_{X_{\psi(r)}}$ is invertible in $\mathcal{O}_{X_{\psi(r)}}$ and so we can define an element $\widetilde{s}_{r,a,b} \in \mathcal{O}_X(X_{\psi(r)})$ by $\widetilde{s}_{r,a,b} = \frac{\psi(a)|_{X_{\psi(r)}}}{\psi(b)|_{X_{\psi(r)}}}$.

Suppose that similarly s is given on $D(r') \subset U$ by a fraction $\frac{a'}{b'}$. We want to show that

$$\widetilde{s}_{r,a,b}|_{X_{\psi(r)} \cap X_{\psi(r')}} = \widetilde{s}_{r',a',b'}|_{X_{\psi(r)} \cap X_{\psi(r')}}.$$

So let $x \in X_{\psi(r)} \cap X_{\psi(r')}$. Then $\mathfrak{q} = \psi^a(x) \in D(r) \cap D(r')$ and therefore $\frac{a}{b} = s(\mathfrak{q}) = \frac{a'}{b'} \in R_\mathfrak{q}$. This means that there exists $b'' \in R \smallsetminus \mathfrak{q}$ such that $b''(ab' - ba') = 0 \in R$. And so $\psi(b'')(\psi(a)\psi(b') - \psi(b)\psi(a')) = 0 \in \mathcal{O}_X(X)$. Because $\psi^a(x) = \mathfrak{q} \in D(b'')$ we see that $x \in (\psi^a)^{-1}(D(b'')) = X_{\psi(b'')}$ and therefore $\psi(b'')_x$ is invertible in $\mathcal{O}_{X,x}$. Thus $\psi(a)_x\psi(b')_x - \psi(b)_x\psi(a')_x \in \mathcal{O}_{X,x}$ and we see that the images of $\widetilde{s}_{r,a,b}$ and $\widetilde{s}_{r',a',b'}$ in $\mathcal{O}_{X,x}$ agree. Because the $x \in X_{\psi(r)} \cap X_{\psi(r')}$ was arbitrary we conclude that indeed $\widetilde{s}_{r,a,b}$ and $\widetilde{s}_{r',a',b'}$ agree on $X_{\psi(r)} \cap X_{\psi(r')}$.

As the $D(r)$'s cover U the open sets of the form $(\psi^a)^{-1}(D(r)) = X_{\psi(r)}$ cover $(\psi^a)^{-1}(U)$ and we can define $\psi^\sharp(U)(s) \in \mathcal{O}_X((\psi^a)^{-1}(U))$ by gluing together the $\widetilde{s}_{r,a,b}$. One immediately sees that $\psi^\sharp$ is a morphism of sheaves of rings. For $x \in X$ and $\mathfrak{q} = \psi^a(x) \in \phi\text{-Spec}(R)$ the induced morphism on the stalks is given by

$$\psi_x^\sharp : R_\mathfrak{q} \to \mathcal{O}_{X,x},\ \frac{a}{b} \mapsto \frac{\psi(a)_x}{\psi(b)_x}.$$

Because $a \in \mathfrak{q}$ if and only if $\psi(a)_x \in \mathfrak{m}_x$ it is a local morphism. So $(\psi^a, \psi^\sharp) : (X, \mathcal{O}_X) \to \big(\phi\text{-Spec}(R), \mathcal{O}_{\phi\text{-Spec}(R)}\big)$ is a morphism of locally ringed spaces. To conclude that ψ^a is a morphism of ϕ-spaces it remains to check that

$$\begin{tikzcd}
X \arrow[r, "\Phi_X"] \arrow[d, "\psi^a"'] & X \arrow[d, "\psi^a"] \\
\phi\text{-Spec}(R) \arrow[r, "\Phi"] & \phi\text{-Spec}(R)
\end{tikzcd}$$

commutes. We have a commutative diagram

$$\begin{tikzcd}
R \arrow[r, "\psi"] \arrow[d, "\phi"'] & \mathcal{O}_X(X) \arrow[r, "\rho_{\Phi(x)}"] \arrow[d, "\phi_X"] & \mathcal{O}_{X,\Phi(x)} \arrow[d, "\phi_x"] \\
R \arrow[r, "\psi"] & \mathcal{O}_X(X) \arrow[r, "\rho_x"] & \mathcal{O}_{X,x}
\end{tikzcd}$$

Because Φ_X is a morphism of locally ringed spaces we know that $(\phi_x)^{-1}(\mathfrak{m}_x) = \mathfrak{m}_{\Phi(x)}$ and so

$$\psi^a(\Phi_X(x)) = \psi^{-1}(\rho^{-1}_{\Phi(x)}(\mathfrak{m}_{\Phi(x)})) = \phi^{-1}(\psi^{-1}(\rho_x^{-1}(\mathfrak{m}_x))) = \Phi(\psi^a(x)).$$

It follows from the fact that ψ is a morphism of difference rings that also the corresponding maps of sheaves commute. So $(\psi^a, \psi^\sharp) : (X, \mathcal{O}_X) \to \big(\phi\text{-Spec}(R), \mathcal{O}_{\phi\text{-Spec}(R)}\big)$ is indeed a morphism of ϕ-spaces.

If

$$(f, f^\sharp) : (X, \mathcal{O}_X) \longrightarrow \big(\phi\text{-Spec}(R), \mathcal{O}_{\phi\text{-Spec}(R)}\big)$$

is a morphism of ϕ-spaces we can define $\psi = \psi_f : R \to \mathcal{O}_X(X)$ by

$$\psi : R \xrightarrow{\iota} \widehat{R} \xrightarrow{f^\sharp(X)} \mathcal{O}_X(X).$$

We have natural mappings

$$\text{Hom}(X, \phi\text{-Spec}(R)) \longleftrightarrow \text{Hom}(R, \Gamma(X))$$

given by $f \mapsto \psi_f$ and $(\psi^a, \psi^\sharp) \leftarrow\!\shortmid \psi$. We claim that they are inverse to each other.

We will first prove that $(f, f^\sharp) = (\psi^a, \psi^\sharp)$. There is a commutative diagram

$$\begin{tikzcd}
R \arrow[r] \arrow[rr, bend left, "\psi"] \arrow[dr, "\nu"'] & \widehat{R} \arrow[r] \arrow[d] & \mathcal{O}_X(X) \arrow[d, "\rho_x"] \\
 & R_{f(x)} \arrow[r, "f_x^\sharp"] & \mathcal{O}_{X,x}
\end{tikzcd}$$

where $\nu : R \to R_{f(x)}$ denotes the usual localization homomorphism. Because $f_x^\sharp$ is a local morphism we have $f(x) = \nu^{-1}((f_x^\sharp)^{-1}(\mathfrak{m}_x)) = \psi^{-1}(\rho_x^{-1}(\mathfrak{m}_x)) = \psi^a(x)$. To prove that also $f^\sharp$ and $\psi^\sharp$ agree, it suffices to see that they agree on the stalks, which also follows form the above diagram.

If $\psi : R \to \mathcal{O}_X(X)$ is a morphism of difference rings then clearly ψ agrees with

$$R \xrightarrow{\iota} \widehat{R} \xrightarrow{\psi^\sharp(\phi\text{-Spec}(R))} \mathcal{O}_X(X).$$

We have thus established a bijection

$$\mathrm{Hom}(X, \phi\text{-Spec}(R)) \simeq \mathrm{Hom}(R, \Gamma(X)).$$

Finally it is quite obvious that for morphisms $X' \to X$ and $R' \to R$ the diagram

$$\begin{tikzcd}
\mathrm{Hom}(X, \phi\text{-Spec}(R)) \arrow[r, "\simeq"] \arrow[d] & \mathrm{Hom}(R, \mathcal{O}_X(X)) \arrow[d] \\
\mathrm{Hom}(X', \phi\text{-Spec}(R')) \arrow[r, "\simeq"] & \mathrm{Hom}(R', \mathcal{O}_{X'}(X'))
\end{tikzcd}$$

is commutative. □

Corollary 2.1.12. *Let $T \to R$ and $T \to S$ be morphisms of difference rings and $X = \phi$-Spec(R), $Y = \phi$-Spec(S), $Z = \phi$-Spec(T). Then the fibred product $X \times_Z Y$ exists in the category of ϕ-spaces and is given by ϕ-Spec$(R \otimes_T S)$.*

Proof: Because $R \otimes_T S$ is the fibred coproduct in the category of difference rings it follows from Theorem 2.1.11 that ϕ-Spec$(R \otimes_T S)$ is the fibred product in the category of ϕ-spaces. □

Definition 2.1.13. *Let R be a ϕ-ring. By a* ϕ-space *over R we mean a ϕ-space X together with a homomorphism $X \to \phi$-Spec(R) of ϕ-spaces.*

Proposition 2.1.14. *Let $T \to R$ be a morphism of ϕ-rings and Y a ϕ-space over T that can be covered with open Φ-stable subsets of the form ϕ-Spec(S) for some T-ϕ-algebra S. Set $X = \phi$-Spec(R) and $Z = \phi$-Spec(T). Then the fibred product $X \times_Z Y$ exists in the category of ϕ-spaces.*

Proof: The proof is straight forward but too tedious to be written down in full detail. So we only give a sketch. The strategy is similar to the classical case (see [17, Theorem 3.3, Chapter II, p. 87]).

If $U_i = \phi$-Spec(S_i) is an open covering of Y then by Corollary 2.1.12 the products $X \times_Z U_i$ exist in the category of ϕ-spaces and we have to glue the products $X \times_Z U_i$ to obtain the product $X \times_Z Y$. This is done by virtue of the following gluing lemmas:

Gluing ϕ-spaces: Let $\{X_i\}$ be a family of ϕ-spaces and for each $i \neq j$ let U_{ij} be an open Φ-stable subset of X_i and $f_{ij} : U_{ij} \to U_{ji}$ an isomorphism of ϕ-spaces such that (1) $f_{ji} = f_{ij}^{-1}$ for all i, j and (2) $f_{ij}(U_{ij} \cap U_{ik}) = U_{ji} \cap U_{jk}$ and $f_{ik} = f_{jk} \circ f_{ij}$ on $U_{ij} \cap U_{ik}$ for all i, j, k. Then there exists a ϕ-space X together with morphisms $g_i : X_i \to X$ for each i such that (1) g_i is an isomorphism onto an open Φ-stable subset of X, (2) the $g_i(X_i)$ cover X, (3) $g_i(U_{ij}) = g_i(X_i) \cap g_j(X_j)$ and (4) $g_i = g_j \circ f_{ij}$ on U_{ij}.

Gluing morphisms of ϕ-spaces: Let X and Y be ϕ-spaces and $\{U_i\}$ an open Φ-stable covering of X together with morphisms $f_i : U_i \to Y$ of ϕ-spaces such that the restrictions of f_i and f_j to $U_i \cap U_j$ are the same. Then there exists a unique morphism $f : X \to Y$ such that the restriction of f to U_i equals f_i.

Returning to the proof we put $U_{ij} = U_i \cap U_j$. Because $p_{U_i}^{-1}(U_{ij}) \subset X \times_Z U_i$ and $p_{U_j}^{-1}(U_{ij}) \subset X \times_Z U_j$ are both the product $X \times_Z U_{ij}$ we obtain isomorphisms $f_i : p_{U_i}^{-1}(U_{ij}) \to p_{U_j}^{-1}(U_{ij})$ which are easily seen to satisfy the conditions of the gluing lemma for ϕ-spaces. We thus obtain a ϕ-space which we denote (somewhat previsionary) with $X \times_Z Y$. To define the projections we use the gluing lemma for morphisms. Finally the universal property of $X \times_Z Y$ follows from the universal property of the $X \times_Z U_i$'s by using the gluing lemma for morphisms.

□

For later use we record the following lemma about products. It gives a sufficient condition for the canonical map from $X \times_Z Y$ to the set theoretic fibre product of X with Y over Z to be surjective.

Lemma 2.1.15. *Let T be a ϕ-ring and R, S T-ϕ-algebras such that R and S are finitely generated as T-algebras. Set $X = \phi\text{-Spec}(R), Y = \phi\text{-Spec}(S), Z = \phi\text{-Spec}(T)$ and let $f : X \to Z$, $g : Y \to Z$ denote the morphisms induced from the R-ϕ-algebra structures. Let $x \in X$ and $y \in Y$ with $f(x) = g(y)$. Then there exists $w \in X \times_Z Y$ such that $p_X(w) = x$ and $p_Y(w) = y$.*

Proof: Let $z = f(x) = g(y) \in Z$ and $d \geq 1$ such that Let $\Phi^d(x) = x$, $\Phi^d(y) = y$ and $\Phi^d(z) = z$. We have inclusions $k(z) \hookrightarrow k(x)$ and $k(z) \hookrightarrow k(y)$ of ϕ^d-fields. Because S and T are finitely generated as R-algebras it follows that $k(x)$ and $k(y)$ are finitely generated as fields over $k(z)$. Therefore the ϕ^d-ring $k(x) \otimes_{k(z)} k(y)$ is Noetherian (Lemma 1.2.4). Therefore (cf. the remark after Definition 1.4.3) we can find a ϕ^d-prime ideal $\mathfrak{p}$ of $k(x) \otimes_{k(z)} k(y)$ and so $\Omega = \mathfrak{Q}((k(x) \otimes_{k(z)} k(y))/\mathfrak{p})$ is a ϕ^d-pfield containing $k(x)$ and $k(y)$. The situation is summarized in the following commutative diagram of ϕ^d-rings.

$$\begin{tikzcd}
R \arrow[r] & k(x) \arrow[dr] & \\
T \arrow[u] \arrow[r] \arrow[d] & k(z) \arrow[u] \arrow[d] & \Omega \\
S \arrow[r] & k(y) \arrow[ur] &
\end{tikzcd}$$

We thus obtain a morphism $h : \phi^d\text{-Spec}(\Omega) \to \phi^d\text{-Spec}(R \otimes_T S)$ and by construction every point in the image h projects onto the prime ideal corresponding to x under ϕ^d-Spec$(R \otimes_T S) \to \phi^d$-Spec$(R)$ and to the prime ideal corresponding to y under ϕ^d-Spec$(R \otimes_T S) \to \phi^d$-Spec$(S)$. As $X \times_Z Y$ and ϕ^d-Spec$(R \otimes_T S)$ have the same underlying topological space and also the projection maps as maps of topological spaces are the same for ϕ and ϕ^d it is clear that every w in the image of h satisfies $p_X(w) = x$ and $p_Y(w) = y$. □

Lemma 2.1.16. *If R is a Noetherian ϕ-ring then every open subset of ϕ-*Spec(R) *is quasi-compact.*

Proof: Let U, U_i be open subsets of $X = \phi$-Spec(R) such that the U_i's cover U. We can find ideals $\mathfrak{a}, \mathfrak{a}_i \subset R$ such that $U = X \smallsetminus \mathbb{V}(\mathfrak{a})$, $U_i = X \smallsetminus \mathbb{V}(\mathfrak{a}_i)$. Then $U = \bigcup U_i$ translates into $\mathbb{V}(\mathfrak{a}) = \bigcap \mathbb{V}(\mathfrak{a}_i) = \mathbb{V}(\sum \mathfrak{a}_i)$. Because R is Noetherian the ideal $\sum \mathfrak{a}_i$ is already generated by finitely many summands. □

2.2 Global sections and the RAAD condition

If one tries to develop a theory of difference (or differential) schemes from scratch one finds that there is a certain problem with the global sections that can be traced back to the fact that annihilators need not be difference (or differential ideals). See [25] and [18].

First of all we observe that – contrary to the situation in usual algebraic geometry – if R is a difference ring then the canonical map $\iota : R \to \widehat{R}$ from R into the global sections of ϕ-Spec(R) is in general not an isomorphism. So far this is not a problem: As we want to do geometry and not algebra we do not need to be able to recover the ring from the space. It suffices if we can recover the space from the global sections. I.e. we would like the induced map ϕ-Spec$(\widehat{R}) \to \phi$-Spec(R) to be an isomorphism. In fact if ι always was an isomorphism there would be no need for an intrinsic difference algebraic geometry as this would make difference schemes the same as schemes with endomorphism (at least in the affine case).

Now the simplest way to guarantee that ϕ-Spec$(\widehat{R}) \to \phi$-Spec(R) is an isomorphism is to assume that annihilators are difference ideals (see [18, Proposition 3.8, p. 19]). However ϕ-pfields usually do not have this property. Rather in ϕ-pfields annihilators are ϕ^n-ideals for some $n \geq 1$. Following [25, Definition 6.3] we make the following definition.

Definition 2.2.1. *A difference ring R is called* RAAD *(radical annihilators are difference ideals) if for every $r \in R$ there exists an $n \geq 1$ such that*

$$\phi^n(\sqrt{\text{Ann}(r)}) \subset \sqrt{\text{Ann}(r)}.$$

As demonstrated by the following lemma (especially point (1)) the RAAD condition is sufficiently general for the applications we have in mind.

Lemma 2.2.2. *Let R be a ϕ-ring. Then R is* RAAD *in all of the following cases:*

(1) *R is Noetherian and $\phi : R \to R$ is injective.*

(2) *R is reduced, has only finitely many minimal prime ideals and $\phi : R \to R$ is injective.*

(3) *R is an integral domain.*

(4) *R is constant.*

Proof: (1): In this prove we will use a somewhat exceptional notation: $\mathfrak{p}$ denotes a prime ideal and $\mathfrak{q}$ a primary ideal. The first case results from the following two facts:

(i) The mapping $\mathfrak{p} \mapsto \phi^{-1}(\mathfrak{p})$ induces a permutation of the (finitely many) associated primes of R.

(ii) For every $r \in R$ the ideal $\sqrt{\operatorname{Ann}(r)}$ is the intersection of associated primes.

To prove (i) let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ denote the associated prime ideals of R. If

$$(0) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

is a reduced primary decomposition then $\{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}\} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. Because ϕ is injective we see that also

$$(0) = \phi^{-1}(\mathfrak{q}_1) \cap \cdots \cap \phi^{-1}(\mathfrak{q}_n)$$

is a reduced primary decomposition. Therefore

$$\left\{\sqrt{\phi^{-1}(\mathfrak{q}_1)}, \ldots, \sqrt{\phi^{-1}(\mathfrak{q}_n)}\right\} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}.$$

Because $\sqrt{\phi^{-1}(\mathfrak{q}_i)} = \phi^{-1}(\sqrt{\mathfrak{q}_i})$ the result follows.

To prove (ii) fix $r \in R$. Let $\mathfrak{p}'_1, \ldots \mathfrak{p}'_m$ denote the minimal prime ideals of $\operatorname{Ann}(r)$. Then

$$\sqrt{\operatorname{Ann}(r)} = \mathfrak{p}'_1 \cap \cdots \cap \mathfrak{p}'_m$$

and the $\mathfrak{p}'_i$'s are associated primes of $R/\operatorname{Ann}(r)$. This means that there exists $b_i \in R$ such that

$$\mathfrak{p}'_i = \{a \in R;\ \overline{ab_i} = 0 \in R/\operatorname{Ann}(r)\}$$

and so $\mathfrak{p}'_i = \operatorname{Ann}(b_i r)$ is an associated prime of R.

Point (2) can be proved in a manner analogous to (1). Finally (3) and (4) are obvious. □

Lemma 2.2.3. *Let L be a ϕ-pfield, $C = L^\phi$ and D a finitely generated C-algebra (considered as constant ϕ-ring). Then $L \otimes_C D$ is Noetherian and* RAAD*.*

Proof: Because $L \otimes_C D$ is finitely generated as L-algebra $L \otimes_C D$ is Noetherian. By Proposition 1.4.15 every ϕ-ideal of R is reflexive. Because the zero ideal is a ϕ-ideal this means that ϕ is injective on $L \otimes_C D$. Thus it follows from Lemma 2.2.2 that $L \otimes_C D$ is RAAD. □

The following two lemmas are modifications of Lemmas 3.6 and 3.7 in [18].

Lemma 2.2.4. *Let R be a Noetherian,* RAAD *difference ring and set $X = \phi\text{-}\mathrm{Spec}(R)$. Let $U \subset X$ be open, $F \in \mathcal{O}_X(U)$, $\mathfrak{q}, \mathfrak{q}' \in U$ and $F(\mathfrak{q}) = 0 \in R_\mathfrak{q}$. Then there exists $b \in R \smallsetminus \mathfrak{q}$ such that $(bF)(\mathfrak{q}') = 0 \in R_{\mathfrak{q}'}$.*

Proof: On an open neighborhood U' of $\mathfrak{q}'$ the function F is given by a fraction $\frac{r}{s}$. If $\mathrm{Ann}(r) \nsubseteq \mathfrak{q}'$ we have $F(\mathfrak{q}') = 0 \in R_{\mathfrak{q}'}$ and we can take $b = 1$ to satisfy the claim of the lemma. If $\mathrm{Ann}(r) \nsubseteq \mathfrak{q}$ there exists $b \in R \smallsetminus \mathfrak{q}$ such that $br = 0$ and so $(bF)(\mathfrak{q}') = 0$.

Altogether we see that we can assume without loss of generality that $\mathrm{Ann}(r) \subset \mathfrak{q} \cap \mathfrak{q}'$. Because R is RAAD there exists an $n \geq 1$ such that $\sqrt{\mathrm{Ann}(r)}$ is a ϕ^n-ideal. By Proposition 1.4.8 we have

$$\phi^n\text{-}\sqrt{\sqrt{\mathrm{Ann}(r)}} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$$

with $\mathfrak{q}_1, \ldots, \mathfrak{q}_m \in \phi\text{-}\mathrm{Spec}(R)$.

Suppose $\mathfrak{q}_i \subset \mathfrak{q} \cap \mathfrak{q}'$ for some $i \in \{1, \ldots, m\}$. Then $\mathfrak{q}_i$ lies in U. Because $\mathfrak{q}_i \subset \mathfrak{q}$ and $F(\mathfrak{q}) = 0$ we also have $F(\mathfrak{q}_i) = 0$. On the other hand, because $\mathfrak{q}_i \subset \mathfrak{q}'$ and $F(\mathfrak{q}') = \frac{r}{s}$ we have $F(\mathfrak{q}_i) = \frac{r}{s}$. Thus we must have $\frac{r}{1} = 0 \in R_{\mathfrak{q}_i}$ but this contradicts $\mathrm{Ann}(r) \subset \mathfrak{q}_i$.

Consequently, for $i = 1, \ldots, m$ there exists either $a_i \in \mathfrak{q}_i$, $a_i \notin \mathfrak{q}'$ or $b_i \in \mathfrak{q}_i$, $b_i \notin \mathfrak{q}$. Set $a = \prod a_i \notin \mathfrak{q}'$ and $b = \prod b_i \notin \mathfrak{q}$. Then

$$ab \in \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m = \phi^n\text{-}\sqrt{\sqrt{\mathrm{Ann}(r)}}.$$

This means that there exist $k \geq 0$ and $l \geq 1$ such that $\phi^{kn}(ab)^l r = 0$. Let $\phi^{-d}(\mathfrak{q}) = \mathfrak{q}$ and $\phi^{-d'}(\mathfrak{q}') = \mathfrak{q}'$. We can assume without loss of generality that d and d' divide k. Then $\phi^{kn}(a)^l \notin \mathfrak{q}'$ and $\phi^{kn}(b)^l \notin \mathfrak{q}$. Also

$$(\phi^{kn}(b)^l F)(\mathfrak{q}') = \frac{\phi^{kn}(b)^l r}{s} = 0 \in R_{\mathfrak{q}'}$$

as desired. □

Lemma 2.2.5. *Let R be a Noetherian,* RAAD *difference ring and $X = \phi\text{-}\mathrm{Spec}(R)$. Let $U \subset X$ be open, $F \in \mathcal{O}_X(U)$ and $\mathfrak{q} \in U$. Then there exist $a, b \in R$, $b \notin \mathfrak{q}$ such that $bF = a$ on U.*

Proof: Suppose $F(\mathfrak{q}) = \frac{a}{b} \in R_\mathfrak{q}$. If we set $F' = bF - a \in \mathcal{O}_X(U)$ then $F'(\mathfrak{q}) = 0$. If there are $a', b' \in R$, $b' \notin \mathfrak{q}$ with $b'F' = a'$ on U then $b'bF = a' + b'a$ on U and $bb' \notin \mathfrak{q}$. Therefore we can assume without loss of generality that $F(\mathfrak{q}) = 0$.

Then by Lemma 2.2.4 there exists for every $\mathfrak{q}' \in U$ a $b_{\mathfrak{q}'} \in R \smallsetminus \mathfrak{q}$ such that $(b_{\mathfrak{q}'}F)(\mathfrak{q}') = 0 \in R_{\mathfrak{q}'}$. Now fix $\mathfrak{q}' \in U$ and assume F is given by the fraction $\frac{r}{s}$ in an open neighborhood U' of U in $\mathfrak{q}'$. Because $(b_{\mathfrak{q}'}F)(\mathfrak{q}') = \frac{b_{\mathfrak{q}'}r}{s} = 0 \in R_{\mathfrak{q}'}$ there must exist $s' \in R \smallsetminus \mathfrak{q}'$ such that $s'b_{\mathfrak{q}'}r = 0 \in R$. If we set $U_{\mathfrak{q}'} = U' \cap D(s')$ then $U_{\mathfrak{q}'}$ is an open neighborhood of $\mathfrak{q}'$ in U and on $U_{\mathfrak{q}'}$ we have $b_{\mathfrak{q}'}F = 0$. We observe that the $U_{\mathfrak{q}'}$'s form an open covering of U. Because R is Noetherian a finite number, say $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_n$ will do (Lemma 2.1.16). Set

$$b = \prod_{i=1}^{n} b_{\mathfrak{q}'_i} \notin \mathfrak{q}.$$

Then $bF = 0$ on U. □

Let R be a ϕ-ring. The natural map $\iota : R \to \widehat{R},\ r \mapsto \widehat{r}$ induces a morphism

$$\alpha : \phi\text{-Spec}(\widehat{R}) \to \phi\text{-Spec}(R)$$

of ϕ-spaces. There also is a natural morphism

$$\beta : \phi\text{-Spec}(R) \to \phi\text{-Spec}(\widehat{R})$$

into the other direction which we will now define: For $\mathfrak{q} \in \phi\text{-Spec}(R)$ set

$$\beta(\mathfrak{q}) = \widehat{\mathfrak{q}} = \{F \in \widehat{R};\ F(\mathfrak{q}) \in \mathfrak{m}_{\mathfrak{q}} \subset R_{\mathfrak{q}}\}.$$

Since $\widehat{\mathfrak{q}}$ is the inverse image of $\mathfrak{m}_{\mathfrak{q}}$ under $\widehat{R} \to R_{\mathfrak{q}}$ we see that $\widehat{\mathfrak{q}} \in \phi\text{-Spec}(\widehat{R})$. If $F \in \widehat{R}$ and $r, s \in R$, $s \notin \mathfrak{q}$ such that $F(\mathfrak{q}) = \frac{r}{s} \in R_{\mathfrak{q}}$ then $F \in \widehat{\mathfrak{q}}$ if and only if $r \in \mathfrak{q}$. Thus for an ideal $\mathfrak{a}$ of $\widehat{R}$ we have

$$\beta^{-1}(\mathbb{V}(\mathfrak{a})) = \{\mathfrak{q} \in \phi\text{-Spec}(R);\ F \in \widehat{\mathfrak{q}}\ \forall\ F \in \mathfrak{a}\} = \mathbb{V}(\mathfrak{b})$$

for some ideal $\mathfrak{b}$ of R. Therefore β is continuous. For $\mathfrak{q} \in \phi\text{-Spec}(R)$ with $\phi^{-d}(\mathfrak{q}) = \mathfrak{q}$ the evaluation map $\widehat{R} \to R_{\mathfrak{q}}$ gives rise to a morphism $\widehat{R}_{\widehat{\mathfrak{q}}} \to R_{\mathfrak{q}}$ of ϕ^d-rings. These morphisms naturally induce a map $\beta^\sharp : \mathcal{O}_{\phi\text{-Spec}(\widehat{R})} \to \beta_*\mathcal{O}_{\phi\text{-Spec}(R)}$ and we see that β is indeed a morphism of ϕ-spaces. One also immediately sees that $\alpha \circ \beta$ is the identity on ϕ-Spec(R).

Theorem 2.2.6. *Let R be a Noetherian* RAAD *ϕ-ring. Then*

$$\phi\text{-Spec}(\widehat{R}) \simeq \phi\text{-Spec}(R).$$

Proof: By the above considerations it suffices to show that $\beta \circ \alpha$ is the identity mapping on ϕ-Spec(R). So let $\mathfrak{q} \in \phi\text{-Spec}(\widehat{R})$. We have to show that

$$\{F \in \widehat{R};\ F(\alpha(\mathfrak{q})) \in \mathfrak{m}_{\alpha(\mathfrak{q})}\} = \mathfrak{q}.$$

$\subseteq$: Let $F \in \widehat{R}$ such that $F(\alpha(\mathfrak{q})) \in \mathfrak{m}_{\alpha(\mathfrak{q})}$. By Lemma 2.2.5 there exist $a, b \in R$, $b \notin \alpha(\mathfrak{q})$ such that $\widehat{b}F = \widehat{a}$. Then $\frac{a}{1} = \frac{b}{1}F(\alpha(\mathfrak{q})) \in \mathfrak{m}_{\alpha(\mathfrak{q})}$ so that $a \in \alpha(\mathfrak{q})$ and consequently $\widehat{a} \in \mathfrak{q}$. Because $\widehat{b} \notin \mathfrak{q}$, $\widehat{b}F = \widehat{a} \in \mathfrak{q}$ and $\mathfrak{q}$ is prime we conclude that $F \in \mathfrak{q}$.
$\supseteq$: Let $F \in \mathfrak{q}$. Again by Lemma 2.2.5 there exist $a, b \in R$, $b \notin \alpha(\mathfrak{q})$ such that $\widehat{b}F = \widehat{a}$. Then $\widehat{a} \in \mathfrak{q}$, i.e. $a \in \alpha(\mathfrak{q})$. Therefore $\frac{b}{1}F(\alpha(\mathfrak{q})) = \frac{a}{1} \in \mathfrak{m}_{\alpha(\mathfrak{q})}$ and so $F(\alpha(\mathfrak{q})) \in \mathfrak{m}_{\alpha(\mathfrak{q})}$ as required.

This shows that α and β are inverses of each other on the level of sets. It remains to prove that for $\mathfrak{q} \in \phi\text{-Spec}(R)$ the map $\widehat{R}_{\widehat{\mathfrak{q}}} \to R_{\mathfrak{q}}$ is an isomorphism. Surjectivity is obvious. So let $F \in \widehat{R}$ and assume that $F(\mathfrak{q}) = 0 \in R_{\mathfrak{q}}$. By Lemma 2.2.5 there exist $a, b \in R$, $b \notin \mathfrak{q}$ such that $\widehat{b}F = \widehat{a}$. Consequently $\frac{a}{1} = 0 \in R_{\mathfrak{q}}$ and there exists $s \in R \smallsetminus \mathfrak{q}$ such that $sa = 0$. Therefore $\widehat{bs}F = 0$ and because $\widehat{bs} \notin \widehat{\mathfrak{q}}$ it follows that $\frac{F}{1} = 0 \in \widehat{R}_{\widehat{\mathfrak{q}}}$.

Lemma 2.2.7. *Let R be a Noetherian,* RAAD *ϕ-ring. Then the canonical map $\iota : R \to \widehat{R}$ is injective.*

Proof: Suppose there exists $r \in R \smallsetminus \{0\}$ with $\widehat{r} = 0$. By assumption $\sqrt{\mathrm{Ann}(r)}$ is a proper ϕ^n-ideal for some n. Thus the ϕ^n-radical of $\sqrt{\mathrm{Ann}(r)}$ is a proper ϕ^n-radical ideal containing $\mathrm{Ann}(r)$. It follows from Proposition 1.4.8 that there exists $\mathfrak{q} \in \phi\text{-Spec}(R)$ with $\mathrm{Ann}(r) \subset \mathfrak{q}$. Therefore $\frac{r}{1} \neq 0 \in R_{\mathfrak{q}}$, in contradiction to $\widehat{r} = 0$. □

Definition 2.2.8. *Let X be a Φ-space and $y = \{x, \Phi(x), \ldots, \Phi^{d-1}(x)\}$ an orbit under Φ, i.e. $\Phi^d(x) = x$. Then we define*

$$\mathcal{O}_{X,y} = \varinjlim \mathcal{O}_X(U)$$

where the direct limit is taken over all open subsets U of X which contain y.

We note that $\mathcal{O}_{X,y}$ carries a natural structure of difference ring because if U is an open subset of X containing y then also $\Phi^{-1}(U)$ is an open subset containing y.

We recall that the expression $R_{\mathfrak{p}}$ was explained in Definition 1.4.5.

Lemma 2.2.9. *Let R be a Noetherian* RAAD *ϕ-ring, $X = \phi\text{-Spec}(R)$ and $x \in X$ with $\Phi^d(x) = x$. Set $y = \{x, \Phi(x), \ldots, \Phi^{d-1}(x)\}$ and $\mathfrak{p} = \mathfrak{q} \cap \cdots \cap \phi^{-(d-1)}(\mathfrak{q})$ where $\mathfrak{q}$ is the prime ideal corresponding to x. Then*

$$R_{\mathfrak{p}} \simeq \mathcal{O}_{X,y}.$$

Proof: If $\frac{r}{s} \in R_{\mathfrak{p}}$ then $U = D(s)$ is an open subset of X containing y and by interpreting $\frac{r}{s}$ as function on U be obtain an element of $\mathcal{O}_{X,y}$ which is easily seen to be independent of the choice of r and s. Thus we have a well defined morphism of difference rings

$$\psi : R_{\mathfrak{p}} \to \mathcal{O}_{X,y}.$$

We first show that ψ is injective. Let $r \in R$ such that $\psi(\frac{r}{1}) = 0$. Then the image of r in $\mathcal{O}_{X,x} = R_{\mathfrak{q}}$ must be zero. Hence there exists for $i = 0, \ldots, d-1$ an $s_i \in R \smallsetminus \phi^{-i}(\mathfrak{q})$ such that $s_i r = 0$. By the classical prime avoidance Lemma ([12, Lemma 3.3, p. 90]) there exists $s \in S(\mathfrak{p})$ such that $sr = 0$.

Now we will show that ψ is surjective. So let U be an open subset of X containing y and $F \in \mathcal{O}_X(U)$. By Lemma 2.2.5 there exist for $i = 0, \dots, d-1$ elements $s_i \in R \smallsetminus \phi^{-i}(\mathfrak{q})$ and $r_i \in R$ such that $s_i F = r_i$ on U. Again by prime avoidance we can find $a_0, \dots, a_{d-1} \in R$ such that $s = \sum a_i s_i \in S(\mathfrak{p})$. Set $r = \sum a_i r_i \in R$. Then over U we have

$$sF = \sum a_i s_i F = \sum a_i r_i = r.$$

This shows that $\psi(\frac{r}{s})$ equals the image of F in $\mathcal{O}_{X,y}$. □

2.3 Closed ϕ-subspaces

This section deals with closed ϕ-subspaces. The main results assert that certain ϕ-subspaces are induced by ϕ-ideals.

Definition 2.3.1. *Let $f : Z \to X$ be a morphism of ϕ-spaces. We say that f is a closed immersion if f induces an homeomorphism of Z onto a closed subset of X and if $f^\sharp : \mathcal{O}_X \to f_*\mathcal{O}_Z$ is surjective. (This is equivalent to $f^\sharp_z : \mathcal{O}_{X,f(z)} \to \mathcal{O}_{Z,z}$ is surjective for every $z \in Z$.) By a* closed ϕ-subspace *of X we mean an equivalence class of closed immersions where two closed immersions $f : Z \to X$ and $f' : Z' \to X$ are said to be equivalent if there exists an isomorphism $i : Z \to Z'$ such that $f'i = f$.*

As usual we will be rather careless about distinguishing closed immersions and closed subschemes.

Let R be a ϕ-ring and $\mathfrak{a}$ a ϕ-ideal of R. Then the canonical map $R \to R/\mathfrak{a}$ induces a morphism

$$\phi\text{-Spec}(R/\mathfrak{a}) \hookrightarrow \phi\text{-Spec}(R)$$

which is easily seen to be a closed immersion. It is called the *closed ϕ-subspace of ϕ-*Spec(R) *induced by* $\mathfrak{a}$.

Lemma 2.3.2. *Let R be a ϕ-ring, $\mathfrak{a}$ a ϕ-ideal of R and*

$$Z = \phi\text{-Spec}(R/\mathfrak{a}) \hookrightarrow \phi\text{-Spec}(R) = X$$

*the closed ϕ-subspace induced by $\mathfrak{a}$. Let U be an open Φ-stable subset of X such that $U = \phi$-*Spec(S) *for some Noetherian,* RAAD *ϕ-ring S. Then the closed ϕ-subspace*

$$U \cap Z \hookrightarrow U = \phi\text{-Spec}(S)$$

is induced from a ϕ-ideal $\mathfrak{b}$ of S.

Proof: We note that the ϕ-space structure on $U \cap Z$ is given by restricting the ϕ-space structure of Z to the open Φ-stable subset $U \cap Z$ of Z. By Theorem 2.1.11 the open inclusion

$$j : \phi\text{-Spec}(S) = U \hookrightarrow X = \phi\text{-Spec}(R)$$

is induced by a morphism $\psi : R \to \widehat{S}$ of ϕ-rings. Similarly the closed immersion

$$U \cap Z \hookrightarrow U = \phi\text{-Spec}(S)$$

is induced from

$$\alpha : S \to \widehat{S} = \mathcal{O}_X(U) \to \mathcal{O}_Z(U \cap Z).$$

Now let $\mathfrak{b} \subset S$ denote the inverse image under $S \to \widehat{S}$ of the ϕ-ideal of $\widehat{S}$ generated by $\psi(\mathfrak{a})$. Then $\mathfrak{b} \subset \ker(\alpha)$ and we obtain a commutative diagram of ϕ-rings

$$\begin{tikzcd}
S/\mathfrak{b} \arrow[rr] & & \mathcal{O}_Z(U \cap Z) \\
& S \arrow[ul] \arrow[ur, "\alpha"'] &
\end{tikzcd}$$

giving rise to

$$\begin{tikzcd}
\phi\text{-Spec}(S/\mathfrak{b}) \arrow[dr, hook] & & U \cap Z \arrow[ll, "f"'] \arrow[dl, hook] \\
& \phi\text{-Spec}(S) = U &
\end{tikzcd}$$

We will show that f is an isomorphism. To see that f is a homeomorphism we need to know that $\mathbb{V}(\mathfrak{b})$ gets identified with $U \cap Z$. I.e. we need to prove that for $\mathfrak{q}' \in \phi\text{-Spec}(S)$ and $\mathfrak{q} = j(\mathfrak{q}') \in \phi\text{-Spec}(R)$ we have

$$\mathfrak{q}' \supset \mathfrak{b} \Leftrightarrow \mathfrak{q} \supset \mathfrak{a}.$$

$\Rightarrow$: If $a \in \mathfrak{a}$ then $\psi(a) \in \widehat{S}$ and because S is Noetherian and RAAD we can use Lemma 2.2.5 to find $s_1, s_2 \in S$, $s_2 \notin \mathfrak{q}'$ such that $\widehat{s_2}\psi(a) = \widehat{s_1} \in \widehat{S}$. Then by definition of $\mathfrak{b}$ we have $s_1 \in \mathfrak{b} \subset \mathfrak{q}'$. Because $\mathfrak{q} = j(\mathfrak{q}')$ is the inverse image of the maximal ideal $\mathfrak{m}_{\mathfrak{q}'} \subset S_{\mathfrak{q}'}$ under $R \xrightarrow{\psi} \widehat{S} \to S_{\mathfrak{q}'}$ this implies $a \in \mathfrak{q}$. Therefore $\mathfrak{a} \subset \mathfrak{q}$.
$\Leftarrow$: If $b \in \mathfrak{b}$ then $\widehat{b} \in \widehat{S}\psi(\mathfrak{a})$. Since by assumption the image of $\psi(\mathfrak{a})$ under $\widehat{S} \to S_{\mathfrak{q}'}$ lies in $\mathfrak{m}_{\mathfrak{q}'}$ we conclude that $\frac{b}{1} \in \mathfrak{m}_{\mathfrak{q}'}$, i.e. $b \in \mathfrak{q}'$.

Now to prove that f is an isomorphism it suffices to see that the induced maps on stalks are isomorphisms. So let $\mathfrak{q}' \in \mathbb{V}(\mathfrak{b}) \subset \phi\text{-Spec}(S)$, $\mathfrak{q} = j(\mathfrak{q}') \supset \mathfrak{a}$ and

$$f^{\sharp}_{\mathfrak{q}} : (S/\mathfrak{b})_{\overline{\mathfrak{q}'}} = S_{\mathfrak{q}'}/\mathfrak{b}_{\mathfrak{q}'} \longrightarrow R_{\mathfrak{q}}/\mathfrak{a}_{\mathfrak{q}} = (R/\mathfrak{a})_{\overline{\mathfrak{q}}}.$$

By Theorem 2.2.6 we have a commutative diagram of isomorphisms

$$\begin{tikzcd}
R_{\mathfrak{q}} \arrow[rr] \arrow[dr] & & S_{\mathfrak{q}'} \arrow[dl] \\
& \widehat{S}_{\widehat{\mathfrak{q}'}} &
\end{tikzcd}$$

Obviously $f^\sharp_{\mathfrak{q}}$ is surjective and it only remains to prove injectivity. So let $s_1, s_2 \in S$, $s_2 \notin \mathfrak{q}'$ such that $f^\sharp_{\mathfrak{q}}(\overline{\frac{s_1}{s_2}}) = 0$. This implies that there exists $r_1, r_2 \in R$, $r_1 \in \mathfrak{a}$, $r_2 \notin \mathfrak{q}$ such that $\frac{s_1}{s_2}$ corresponds to $\frac{r_1}{r_2}$ under the isomorphism $S_{\mathfrak{q}'} \simeq R_{\mathfrak{q}}$. Then $\frac{\widehat{s_1}}{\widehat{s_2}} = \frac{\psi(r_1)}{\psi(r_2)} \in \widehat{S}_{\widehat{\mathfrak{q}'}}$. Hence there exists $F \in \widehat{S} \smallsetminus \widehat{\mathfrak{q}'}$ such that

$$F(\widehat{s_1}\psi(r_2) - \widehat{s_2}\psi(r_1)) = 0 \in \widehat{S} \tag{2.1}$$

By Lemma 2.2.5 there exist $s_1', s_2' \in S$, $s_2' \notin \mathfrak{q}'$ such that $\widehat{s_2'}F = \widehat{s_1'}$. This implies $s_1' \notin \mathfrak{q}'$. Similarly for $\psi(r_2) \in \widehat{S} \smallsetminus \widehat{\mathfrak{q}'}$ there is $s_1'', s_2'' \in S$, $s_2'' \notin \mathfrak{q}'$ such that $\widehat{s_2''}\psi(r_2) = \widehat{s_1''}$ and so $s_1'' \notin \mathfrak{q}'$. Multiplying equation (2.1) with $\widehat{s_2'}\widehat{s_2''}$ yields

$$\widehat{s_1'}(\widehat{s_1}\widehat{s_1''} - \widehat{s_2''}\widehat{s_2}\psi(r_2)) = 0 \in \widehat{S}$$

which shows that $s_1's_1''s_1 \in \mathfrak{b}$ because $r_2 \in \mathfrak{a}$. Therefore $\overline{\frac{s_1}{s_2}} = 0 \in S_{\mathfrak{q}'}/\mathfrak{b}_{\mathfrak{q}'}$. □

Our next goal is to show that certain closed ϕ-subspaces $Z \hookrightarrow \phi\text{-Spec}(R)$ are induced by ϕ-ideals of R. For this we will need the following two Lemmas.

Lemma 2.3.3. *Let Z be a ϕ-space such that Z can be covered with finitely many open Φ-stable subsets $U_i = \phi\text{-Spec}(R_i)$ where R_i is Noetherian and* RAAD. *Then*

$$\{F \in \mathcal{O}_Z(Z);\ F_z \in \mathfrak{m}_z\ \forall\ z \in Z\} = \phi\text{-}\sqrt{\mathcal{O}_Z(Z)}.$$

(Here $\phi\text{-}\sqrt{\mathcal{O}_Z(Z)}$ denotes the ϕ-radical of the zero ideal of $\mathcal{O}_Z(Z)$.)

Proof: We first assume that $Z = \phi\text{-Spec}(R)$ with R Noetherian and RAAD. Let $F \in \widehat{R}$ such that $F(\mathfrak{q}) \in \mathfrak{m}_{\mathfrak{q}} \subset R_{\mathfrak{q}}$ for all $\mathfrak{q} \in \phi\text{-Spec}(R)$ and fix $\mathfrak{q}' \in \phi\text{-Spec}(R)$. Then by Lemma 2.2.5 there exist $a, b \in R$, $b \notin \mathfrak{q}'$ such that $\widehat{b}F = \widehat{a}$. Then it follows from the assumption on F that $a \in \mathfrak{q}$ for every $\mathfrak{q} \in \phi\text{-Spec}(R)$. Thus by Proposition 1.4.8

$$a \in \bigcap_{\mathfrak{q} \in \phi\text{-Spec}(R)} \mathfrak{q} = \phi\text{-}\sqrt{R}.$$

And so by Proposition 1.4.7 there exist $n \geq 0$, $m \geq 1$ such that $\phi^n(a)^m = 0$. If $d \geq 1$ is such that $\phi^{-d}(\mathfrak{q}) = \mathfrak{q}$ then we may assume $d|n$. It follows that $\widehat{\phi^n(b)^m}\phi^n(F)^m = 0$ and therefore the restriction of $\phi^n(F)^m$ to $D(\phi^n(b))$ equals zero. As $d|n$ we have $\mathfrak{q}' \in D(\phi^n(b))$.

Summarily we have shown that for every $\mathfrak{q} \in \phi\text{-Spec}(R)$ there exists an open neighborhood $U = U_{\mathfrak{q}}$ of $\mathfrak{q}$ in $\phi\text{-Spec}(R)$ and integers $n = n_{\mathfrak{q}} \geq 0$, $m = m_{\mathfrak{q}} \geq 1$ such that the restriction of $\phi^n(F)^m$ to U is zero. As $\phi\text{-Spec}(R)$ is quasi-compact (Lemma 2.1.16) a finite number of such U's, say $U_{\mathfrak{q}_1}, \ldots, U_{\mathfrak{q}_k}$ suffices to cover $\phi\text{-Spec}(R)$. Set $n = \max n_{\mathfrak{q}_i}$ and $m = \max m_{\mathfrak{q}_i}$. Then $\phi^n(F)^m = 0$ as desired.

Now we treat the general case. First we observe the validity of the inclusion "$\supset$": If $F \in \mathcal{O}_Z(Z)$ with $\phi^n(F)^m = 0$ and $z \in Z$ then $\Phi^d(z) = z$ for some $d \geq 1$ and we have a morphism $(\mathcal{O}_Z(Z), \phi_Z^d) \to (\mathcal{O}_{Z,z}, \phi_z^d)$ of difference rings (see Remark 2.1.4). Furthermore $(\phi_z^d)^{-1}(\mathfrak{m}_z) = \mathfrak{m}_z$. After applying ϕ to $\phi^n(F)^m = 0$ an appropriate number of times we can assume that $n = kd$ for some $k \geq 1$. Then $(\phi_z^d)^k(F_z)^m = (\phi^n(F)^m)_z = 0 \in \mathfrak{m}_z$ yields $F_z \in \mathfrak{m}_z$.

Now we prove the inclusion "$\subset$": From the affine case considered above it follows that for each i there exist integers n_i, m_i such that $\phi^{n_i}(F|_{U_i})^{m_i} = 0$. Take $n = \max n_i$ and $m = \max m_i$ then $\phi^n(F)^m = 0$, i.e. $F \in \phi\text{-}\sqrt{\mathcal{O}_Z(Z)}$ □

Lemma 2.3.4. *Let Z be a ϕ-space that can be covered with finitely many open Φ-stable subsets $U_i = \phi\text{-Spec}(R_i)$ where the R_i's are Noetherian* RAAD *difference rings. Let $F, G \in \mathcal{O}_Z(Z)$ such that $F_z = 0 \in \mathcal{O}_{Z,z}$ for all $z \in Z_G = \{z \in Z;\ G_z \notin \mathfrak{m}_z \subset \mathcal{O}_{Z,z}\}$. Then for every $d \geq 1$ there exists $k \geq 1$ and $n_1, \ldots, n_k \geq 0$, $m_1, \ldots, m_k \geq 1$ such that d divides each n_i and*

$$\phi^{n_1}(G)^{m_1} \cdots \phi^{n_k}(G)^{m_k} F = 0.$$

Proof: We first assume that $Z = \phi\text{-Spec}(R)$ for some Noetherian RAAD ϕ-ring R. Fix $\mathfrak{q} \in \phi\text{-Spec}(R)$. By Lemma 2.2.5 there exist $r, s \in R$, $s \notin \mathfrak{q}$ such that $\widehat{s}F = \widehat{r}$ and similarly $r', s' \in R$, $s' \notin \mathfrak{q}$ such that $\widehat{s'}G = \widehat{r'}$. By the RAAD assumption $\sqrt{\text{Ann}(r)}$ is a ϕ^n-ideal for some $n \geq 1$ and by Proposition 1.4.8

$$\phi^n\text{-}\sqrt{\sqrt{\text{Ann}(r)}} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$$

for some $\mathfrak{q}_1, \ldots, \mathfrak{q}_m \in \phi\text{-Spec}(R)$.

Now suppose $r' \notin \phi^n\text{-}\sqrt{\sqrt{\text{Ann}(r)}}$. Say $r' \notin \mathfrak{q}_1$. Then $G(\mathfrak{q}_1) \notin \mathfrak{m}_{\mathfrak{q}_1} \subset R_{\mathfrak{q}_1}$, i.e. $\mathfrak{q}_1 \in Z_G$. Hence by assumption $F(\mathfrak{q}_1) = 0 \in R_{\mathfrak{q}_1}$, which implies $\frac{r}{1} = 0 \in R_{\mathfrak{q}_1}$. But this contradicts $\text{Ann}(r) \subset \mathfrak{q}_1$.

Therefore $r' \in \phi^n\text{-}\sqrt{\sqrt{\text{Ann}(r)}}$. This means that there exists $l \geq 0$, $j \geq 1$ such that $\phi^{ln}(r')^j r = 0$. We may assume that dd' divides l where $d' \geq 1$ is such that $\phi^{-d'}(\mathfrak{q}) = \mathfrak{q}$. We have

$$\phi^{ln}\big(\widehat{s'}\big)^j \widehat{s} \phi^{ln}(G)^j F = \phi^{ln}\big(\widehat{r'}\big)^j \widehat{r} = 0.$$

Thus the restriction of $\phi^{ln}(G)^j F$ to the open neighborhood $D(s\phi^{ln}(s'))$ of $\mathfrak{q}$ is zero.

Summarily we have found for every point $\mathfrak{q} \in \phi\text{-Spec}(R)$ an open neighborhood $U = U_{\mathfrak{q}}$ and integers $n = n_{\mathfrak{q}} \geq 0$, $m = m_{\mathfrak{q}} \geq 1$ such that $d|n$ and the restriction of $\phi^n(G)^m F$ to U is zero. Because $\phi\text{-Spec}(R)$ is quasi-compact a finite number of such U's, say $U_{\mathfrak{q}_1}, \ldots, U_{\mathfrak{q}_k}$ will be enough to cover $\phi\text{-Spec}(R)$. Then clearly $\phi^{n_{\mathfrak{q}_1}}(G)^{m_{\mathfrak{q}_1}} \cdots \phi^{n_{\mathfrak{q}_k}}(G)^{m_{\mathfrak{q}_k}} F = 0$ as desired.

The general case easily reduced to the affine case treated above. □

Proposition 2.3.5. *Let R be a ϕ-ring and $X = \phi\text{-Spec}(R)$. Let*

$$f : Z \hookrightarrow X$$

be a closed ϕ-subspace such that Z can be covered by a finite family of open Φ-stable subsets $U_i = \phi\text{-Spec}(R_i)$ where the R_i's are Noetherian RAAD *difference rings. Then f is induced by a ϕ-ideal $\mathfrak{a}$ of R. In fact we can take $\mathfrak{a}$ to be the kernel of $\psi : R \to \mathcal{O}_X(X) \to \mathcal{O}_Z(Z)$.*

Proof: Let $\mathfrak{a} = \ker(\psi)$. We will first show that $f(Z) = \mathbb{V}(\mathfrak{a})$. We know from Theorem 2.1.11 that f is induced from ψ. More precisely if $z \in Z$ then $f(z)$ is the inverse image of $\mathfrak{m}_z$ under $R \xrightarrow{\psi} \mathcal{O}_Z(Z) \to \mathcal{O}_{Z,z}$. Therefore clearly $f(Z) \subset \mathbb{V}(\mathfrak{a})$. On the other hand, using Lemmas 2.3.3 and 1.4.10

$$f(Z) = \overline{f(Z)} = \mathbb{V}\left(\bigcap_{\mathfrak{q} \in f(Z)} \mathfrak{q}\right) = \mathbb{V}\Big(\{r \in R;\ \psi(r)_z \in \mathfrak{m}_z \subset \mathcal{O}_{Z,z}\ \forall z \in Z\}\Big) =$$
$$= \mathbb{V}\Big(\Big\{r \in R;\ \psi(r) \in \phi\text{-}\sqrt{\mathcal{O}_Z(Z)}\Big\}\Big) = \mathbb{V}\left(\psi^{-1}\left(\phi\text{-}\sqrt{\mathcal{O}_Z(Z)}\right)\right) =$$
$$= \mathbb{V}\left(\phi\text{-}\sqrt{\ker(\psi)}\right) = \mathbb{V}(\mathfrak{a}).$$

The commutative diagram

$$\begin{tikzcd}
\mathcal{O}_Z(Z) & \\
& R \arrow[ul, "\psi"'] \arrow[dl] \\
R/\mathfrak{a} \arrow[uu] &
\end{tikzcd}$$

yields

$$\begin{tikzcd}
Z \arrow[dr, "f"] \arrow[dd, "g"'] & \\
& \phi\text{-Spec}(R) \\
\phi\text{-Spec}(R/\mathfrak{a}) \arrow[ur, "h"'] &
\end{tikzcd}$$

We need to show that g is an isomorphism. Because f and h are homeomorphisms onto the same closed subset $f(Z) = \mathbb{V}(\mathfrak{a}) = h(Z)$ we already know that g is a homeomorphism.

Let $\mathfrak{q} \in \mathbb{V}(\mathfrak{a})$, $\overline{\mathfrak{q}} \in \phi$-Spec$(R/\mathfrak{a})$ with $h(\overline{\mathfrak{q}}) = \mathfrak{q}$ and $z \in Z$ with $f(z) = \mathfrak{q}$. We have a commutative diagram

$$\begin{tikzcd}
\mathcal{O}_{Z,z} & \\
& R_{\mathfrak{q}} \arrow[ul, "f_z^\sharp"'] \arrow[dl] \\
(R/\mathfrak{a})_{\overline{\mathfrak{q}}} \arrow[uu, "g_z^\sharp"] &
\end{tikzcd}$$

It suffices to show that $g_z^\sharp$ is an isomorphism. By definition $f_z^\sharp$ is surjective, thus also $g_z^\sharp$ is surjective.

Now let $r \in R$ such that $g_z^\sharp(\frac{\overline{r}}{1}) = 0$. This means that there exists an open neighborhood U of $z \in Z$ such that the restriction of $\psi(r)$ to U is zero. Then $f(U)$ is open in $f(Z) = \mathbb{V}(\mathfrak{a})$ and we can find $s \in R$ such that $\mathfrak{q} \in D(s) \cap \mathbb{V}(\mathfrak{a}) \subset f(U)$, in particular $s \notin \mathfrak{q}$. As $Z_{\psi(s)} = f^{-1}(D(s)) = f^{-1}(D(s) \cap f(Z)) \subset U$ we know that $\psi(r)_z = 0$ for all $z \in Z_{\psi(s)}$. Let $d \geq 1$ be such that $\phi^{-d}(\mathfrak{q}) = \mathfrak{q}$. By Lemma 2.3.4 there exists $k \geq 1$ and $n_1, \dots, n_k \geq 0$, $m_1, \dots, m_k \geq 1$ such that $d | n_i$ and

$$\phi^{n_1}(\psi(s))^{m_1} \cdots \phi^{n_k}(\psi(s))^{m_k}\psi(r) = 0.$$

Therefore $\phi^{n_1}(s)^{m_1} \cdots \phi^{n_k}(s)^{m_k} r \in \ker \psi = \mathfrak{a}$. Because $d|n_i$ we have

$$\phi^{n_1}(s)^{m_1} \cdots \phi^{n_k}(s)^{m_k} \notin \mathfrak{q}$$

which proves $\frac{\overline{r}}{1} = 0 \in (R/\mathfrak{a})_{\overline{q}}$ as desired. □

2.4 The functor of constants

The goal of this section is to define the functor of constants. It is a functor from the category of ϕ-spaces to the category of locally ringed spaces.

Let X be a ϕ-space. As a set we define X^ϕ to be the quotient of X by the action of Φ. That is, X^ϕ is the set of orbits of Φ on X. Thus, formally an element y of X^ϕ is of the form $y = \{x, \Phi(x), \dots, \Phi^{d-1}(x)\}$ with $x \in X$ and $d \geq 1$ such that $\Phi^d(x) = x$. We denote with π or π_X the quotient map

$$\pi : X \to X^\phi, \ x \mapsto y.$$

As topology on X^ϕ we use the quotient topology. So π is continuous and a subset U of X^ϕ is open if and only if $\pi^{-1}(U)$ is open.

Lemma 2.4.1. *There is a one-to-one correspondence*

$$\{\textit{open } \Phi\textit{-stable subsets of } X\} \longleftrightarrow \{\textit{open subsets of } X^\phi\}$$

given by $V \mapsto \pi(V)$ and $\pi^{-1}(U) \leftarrow\!\shortmid U$.

Proof: Because V is Φ-stable $\pi^{-1}(\pi(V)) = V$. Therefore $\pi(V)$ is open in X^ϕ. Because π is surjective $\pi(\pi^{-1}(U)) = U$. □

For a simpler notation we will now write Y instead of X^ϕ. We note that $\pi_*\mathcal{O}_X$ is a sheaf of difference rings on $Y = X^\phi$ (cf. the remark after 2.1.3). Therefore we can define

$$\mathcal{O}_Y = (\pi_*\mathcal{O}_X)^\phi,$$

or more explicitly $\mathcal{O}_Y(U) = \mathcal{O}_X(\pi^{-1}(U))^\phi$ for $U \subset Y$ open. If $U' \subset U$ the restriction map $\mathcal{O}_X(\pi^{-1}(U))^\phi \to \mathcal{O}_X(\pi^{-1}(U'))^\phi$ is induced from the restriction map $\mathcal{O}_X(\pi^{-1}(U)) \to \mathcal{O}_X(\pi^{-1}(U'))$.

Lemma 2.4.2. *$(Y, \mathcal{O}_Y)$ is a locally ringed space.*

Proof: Clearly $\mathcal{O}_Y$ is a presheaf of rings. It is a sheaf because "being constant" is a local property: If $\{U_i\}$ is an open covering of an open set U and $s_i \in \mathcal{O}_Y(U_i) \subset \mathcal{O}_X(\pi^{-1}(U_i))$ such that they agree on the intersections then there exists an $s \in \mathcal{O}_X(\pi^{-1}(U))$ such that the restriction of s to U_i equals s_i. But also the restriction of $\phi(s)$ to U_i equals $\phi(s_i) = s_i$ and so $s = \phi(s)$ is constant.

It remains to see that for $y \in Y$ the ring $\mathcal{O}_{Y,y}$ is a local ring. Let $x \in X$ with $\pi(x) = y$ and $d \geq 1$ minimal with $\Phi^d(x) = x$. An element of $\mathcal{O}_{Y,y}$ is an equivalence class (U, f) where U is an open neighborhood of y in Y and $f \in \mathcal{O}_X(\pi^{-1}(U))^\phi$. The elements $x, \Phi(x), \ldots, \Phi^{d-1}(x)$ all map to y under π and so are in $\pi^{-1}(U)$. We claim that

$$\mathfrak{m}_y = \left\{(U, f) \in \mathcal{O}_{Y,y};\ f_{\Phi^i(x)} \in \mathfrak{m}_{\Phi^i(x)} \subset \mathcal{O}_{X,\Phi^i(x)} \text{ for } i = 0, \ldots, d-1\right\}$$

is the unique maximal ideal of $\mathcal{O}_{Y,y}$. Choose $(U, f) \in \mathcal{O}_{Y,y} \smallsetminus \mathfrak{m}_y$ and let

$$V = \{x' \in \pi^{-1}(U);\ f_{x'} \notin \mathfrak{m}_{x'} \subset \mathcal{O}_{X,x'}\} \subset X.$$

For $x' \in V$ the map $\mathcal{O}_{X,\Phi(x')} \to \mathcal{O}_{X,x'}$ is a morphism of local rings and maps $f_{\Phi(x')}$ to $\phi(f)_{x'} = f_{x'} \notin \mathfrak{m}_{x'}$. Therefore $f_{\Phi(x')} \notin \mathfrak{m}_{\Phi(x')}$ and so $\Phi(x') \in V$. Consequently V is Φ-stable. By Lemma 2.1.10 the set V is also open and $f|_V$ is invertible in $\mathcal{O}_X(V)$. Because $f|_V$ is constant and the inverse of a constant is also constant we see that $f|_V \in \mathcal{O}_X(V)^\phi = \mathcal{O}_X(\pi^{-1}(\pi(V))^\phi$ is invertible in $\mathcal{O}_X(V)^\phi$. By construction V is an open Φ-stable neighborhood of x and so $\pi(V)$ is an open neighborhood of y. We have $(U, f) = (\pi(V), f|_V)$ and so (U, f) is invertible in $\mathcal{O}_{Y,y}$. □

If we let $\pi^\sharp : \mathcal{O}_Y \to \pi_*\mathcal{O}_X$ denote the inclusion map then one easily verifies that the quotient map $\pi : X \to X^\phi$ is actually a morphism in the category of ϕ-spaces. In fact the reader fond of categorical statements can verify without difficulty that $\pi : X \to X^\phi$ is the coequalizer of $(\Phi, \phi) : X \to X$ and $\mathrm{id} : X \to X$. In other words X^ϕ is the quotient of X by the action of Φ.

Next we want to see that $X \mapsto X^\phi$ is indeed a functor. So let $f : X \to X'$ be a morphism of ϕ-spaces. We will construct a morphism $f^\phi : X^\phi \to X'^\phi$ of locally ringed spaces. As above we will write Y and Y' instead of X^ϕ and X'^ϕ. Because f maps orbits to orbits we can define f^ϕ on sets to be the unique mapping making

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, "\pi"'] & X' \arrow[d, "\pi'"] \\
Y \arrow[r, "f^\phi"] & Y'
\end{tikzcd}$$

commutative. If $U' \subset Y'$ is open then $\pi^{-1}((f^\phi)^{-1}(U')) = f^{-1}(\pi'^{-1}(U'))$ is open in X. Therefore f^ϕ is continuous.

The difference morphism

$$f^\sharp(\pi'^{-1}(U')) : \mathcal{O}_{X'}(\pi'^{-1}(U')) \longrightarrow \mathcal{O}_X(f^{-1}(\pi'^{-1}(U'))) = \mathcal{O}_X(\pi^{-1}((f^\phi)^{-1}(U')))$$

induces a morphism $(f^\phi)^\sharp(U') : \mathcal{O}_{Y'}(U') \to \mathcal{O}_Y((f^\phi)^{-1}(U'))$ by restricting to constants.

It remains to see that $(f^\phi)^\sharp_y : \mathcal{O}_{Y',f^\phi(y)} \to \mathcal{O}_{Y,y}$ is a local morphism for every $y \in Y$. Let $x \in X$ with $\pi(x) = y$. Because all the morphism aside from maybe $(f^\phi)^\sharp_y$ in the commutative diagram

$$\begin{tikzcd}
\mathcal{O}_{X,x} & \mathcal{O}_{X',f(x)} \arrow[l, "f^\sharp_x"'] \\
\mathcal{O}_{Y,y} \arrow[u, "\pi^\sharp_x"] & \mathcal{O}_{Y',f^\phi(y)} \arrow[l, "(f^\phi)^\sharp_y"] \arrow[u, "\pi'^\sharp_{\pi'(f(x))}"']
\end{tikzcd}$$

are local also $(f^\phi)^\sharp_y$ is local.

Obviously $f^\phi : X^\phi \to X'^\phi$ is the unique morphism making

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, "\pi"'] & X' \arrow[d, "\pi'"] \\
X^\phi \arrow[r, "f^\phi"] & X'^\phi
\end{tikzcd}$$

a commutative diagram in the category of ϕ-spaces.

We observe that if X is already constant then of course $X^\phi = X$.

Lemma 2.4.3. *If U is an open Φ-stable subset of a ϕ-space X (considered as a ϕ-space with the structure induced from X) then $U^\phi \subset X^\phi$ is an open inclusion of locally ringed spaces.*

Proof: Because U is Φ-stable $U^\phi = \pi(U)$ is open in X. The rest is obvious from the definitions. □

Theorem 2.4.4. *Let R be a ϕ-ring. Then $(\phi\text{-Spec}(R))^\phi$ and $\text{Spec}^\phi(R)$ are isomorphic as topological spaces.*

Proof: The isomorphism

$$f : (\phi\text{-Spec}(R))^\phi \longrightarrow \text{Spec}^\phi(R)$$

is given by sending an orbit $\{\mathfrak{q}, \phi^{-1}(\mathfrak{q}), \ldots, \phi^{-(d-1)}(\mathfrak{q})\}$ to $\mathfrak{p} = \mathfrak{q} \cap \cdots \cap \phi^{-(d-1)}(\mathfrak{q})$. The map f is clearly bijective because the inverse is given by sending a ϕ-prime ideal to the set of its minimal prime ideals. We have a commutative diagram

$$\begin{tikzcd}
 & \phi\text{-Spec}(R) \arrow[dl, "\pi"'] \arrow[dr, "g"] & \\
(\phi\text{-Spec}(R))^\phi \arrow[rr, "f"] & & \text{Spec}^\phi(R)
\end{tikzcd}$$

where g maps $\mathfrak{q}$ to $\mathfrak{q} \cap \cdots \cap \phi^{-(d-1)}(\mathfrak{q})$. To see that f is a homeomorphism it suffices to see that a subset V of $\text{Spec}^\phi(R)$ is closed if and only if $g^{-1}(V)$ is closed in ϕ-Spec(R).

But if V is closed in $\mathrm{Spec}^{\phi}(R)$ then $V = \mathbb{V}(\mathfrak{a})$ for some ϕ-ideal $\mathfrak{a}$. And for $\mathfrak{q} \in \phi\text{-}\mathrm{Spec}(R)$ we see as in the proof of Lemma 1.4.4 that $g(\mathfrak{q}) \in V$ if and only if $\mathfrak{a} \subset \mathfrak{q}$. Therefore $g^{-1}(V) = \mathbb{V}(\mathfrak{a})$ is closed in ϕ-Spec(R).

Conversely if $g^{-1}(V)$ is closed in ϕ-Spec(R) then $g^{-1}(V) = \mathbb{V}(\mathfrak{a})$ for some ideal $\mathfrak{a}$ of R. Because $g^{-1}(V)$ is Φ-stable we can assume that $\mathfrak{a}$ is a ϕ-ideal. Then $V = g(\mathbb{V}(\mathfrak{a})) = \mathbb{V}(\mathfrak{a})$ is closed in $\mathrm{Spec}^{\phi}(R)$. □

Proposition 2.4.5. *Let R be a Noetherian,* RAAD *ϕ-ring such that the map*

$$\{\phi\text{-}\textit{radical ideals of } R\} \longrightarrow \{\textit{radical ideals of } R^{\phi}\},\ \mathfrak{a} \mapsto \mathfrak{a}^{\phi} = \mathfrak{a} \cap R^{\phi}$$

is bijective. Then $(\phi\text{-}\mathrm{Spec}(R))^{\phi}$ *is isomorphic to* $\mathrm{Spec}(R^{\phi})$.

Proof: We write X for ϕ-Spec(R) and Y for $X^{\phi} = (\phi\text{-}\mathrm{Spec}(R))^{\phi}$. We will identify Y with $\mathrm{Spec}^{\phi}(R)$ by virtue of Theorem 2.4.4. In particular π gets identified with g and if $\mathfrak{a} \subset R$ is a ϕ-ideal then $\pi^{-1}(\mathbb{V}(\mathfrak{a})) = \mathbb{V}(\mathfrak{a})$. (Caution! This only holds for *ϕ-ideals* and not for arbitrary ideals).

The inclusion map $R^{\phi} \to R$ is a morphism of difference rings giving rise to a morphism of ϕ-spaces

$$X \longrightarrow \phi\text{-}\mathrm{Spec}(R^{\phi}) = \mathrm{Spec}(R^{\phi}).$$

Applying the constant functor yields a morphism

$$f : Y \to \mathrm{Spec}(R^{\phi})$$

of locally ringed spaces. On points f is simply given by mapping a ϕ-prime ideal $\mathfrak{p}$ of R to $\mathfrak{p}^{\phi} = \mathfrak{p} \cap R^{\phi}$. Thus it follows from Lemma 1.4.12 that f is a homeomorphism.

That $f^{\sharp}$ is also an isomorphism can be checked on the stalks. So let $y \in Y$ be the point corresponding to a ϕ-prime ideal $\mathfrak{p}$ of R. We have to show that

$$f^{\sharp}_y : R^{\phi}_{\mathfrak{p}^{\phi}} \to \mathcal{O}_{Y,y}$$

is an isomorphism. Explicitly the mapping $f^{\sharp}_y$ can be described as follows: If $\frac{r}{s} \in R^{\phi}_{\mathfrak{p}^{\phi}}$ set $U = Y \smallsetminus \mathbb{V}(s)$. Then because $(s) \subset R$ is a ϕ-ideal $\pi^{-1}(U) = X \smallsetminus \mathbb{V}(s) = D(s) \subset X$. Define $F \in \mathcal{O}_Y(U) = \mathcal{O}_X(\pi^{-1}(U))^{\phi}$ by $F(\mathfrak{q}') = \frac{r}{s} \in R_{\mathfrak{q}'}$ for $\mathfrak{q}' \in \pi^{-1}(U) = D(s)$. Then

$$f^{\sharp}_y\left(\frac{r}{s}\right) = (U, F) \in \mathcal{O}_{Y,y}.$$

First we will prove that $f^{\sharp}_y$ is injective. Let $r \in R^{\phi}$ with $f^{\sharp}_y(\frac{r}{1}) = 0$. This means that there exists an open neighborhood U of y in Y such that r vanishes on $\pi^{-1}(U)$, i.e Ann$(r) \nsubseteq \mathfrak{q}'$ for all $\mathfrak{q}' \in \pi^{-1}(U)$. If

$$\mathfrak{p} = \mathfrak{q} \cap \cdots \cap \phi^{-(d-1)}(\mathfrak{q})$$

then $\mathfrak{q} \in \pi^{-1}(U)$ and Ann$(r) \nsubseteq \mathfrak{q}$. Therefore Ann$(r) \nsubseteq \mathfrak{p}$. Since r is constant Ann(r) is a ϕ-ideal. We have $\phi\text{-}\sqrt{\mathrm{Ann}(r)} \nsubseteq \mathfrak{p}$ and thus by Lemma 1.4.13 also $(\phi\text{-}\sqrt{\mathrm{Ann}(r)})^{\phi} \nsubseteq \mathfrak{p}^{\phi}$.

This means that we can find an $s \in (\phi\text{-}\sqrt{\mathrm{Ann}(r)})^{\phi} \smallsetminus \mathfrak{p}^{\phi}$. Thus there exist n, m such that $\phi^n(s)^m \in \mathrm{Ann}(r)$. Because s is constant we actually have $s^m r = 0$ and so $\frac{r}{1} = 0 \in R^{\phi}_{\mathfrak{p}^{\phi}}$.

It remains to prove that $f_y^{\sharp}$ is surjective. So take $(U, F) \in \mathcal{O}_{Y,y}$. This means that U is an open neighborhood of y in Y and $F \in \mathcal{O}_X(\pi^{-1}(U))^{\phi}$. Set

$$\mathfrak{a} = \{b \in R;\ \exists\ a \in R:\ bF = a \text{ on } \pi^{-1}(U)\}.$$

Because F is constant $\mathfrak{a}$ is a difference ideal of R. If

$$\mathfrak{p} = \mathfrak{q} \cap \cdots \cap \phi^{-(d-1)}(\mathfrak{q})$$

then $\mathfrak{q} \in \pi^{-1}(U)$ and by Lemma 2.2.5 we have $\mathfrak{a} \not\subseteq \mathfrak{q}$. Thus $\mathfrak{a} \not\subseteq \mathfrak{p}$, and so also ϕ-$\sqrt{\mathfrak{a}} \not\subseteq \mathfrak{p}$. Then by Lemma 1.4.13 we have $(\phi\text{-}\sqrt{\mathfrak{a}})^{\phi} \not\subseteq \mathfrak{p}^{\phi}$, which means that there exists $s \in R^{\phi} \smallsetminus \mathfrak{p}^{\phi}$, $r \in R$ and n, m such that $\phi^n(s)^m F = r$ on $\pi^{-1}(U)$. Using that s is constant and replacing s^m with s we conclude that there exists $s \in R^{\phi} \smallsetminus \mathfrak{p}^{\phi}$ and $r \in R$ such that $sF = r$ on $\pi^{-1}(U)$. Because s and F are constant also r must be constant on $\pi^{-1}(U)$, i.e. $r - \phi(r)$ vanishes on $\pi^{-1}(U)$. This means that $\pi^{-1}(U) \subset X \smallsetminus \mathbb{V}(\mathrm{Ann}(r - \phi(r))$. So if $\mathfrak{b}$ is the ϕ-radical ideal of R with $\pi^{-1}(U) = X \smallsetminus \mathbb{V}(\mathfrak{b})$ (see Lemma 2.1.9) then $\mathbb{V}(\mathrm{Ann}(r - \phi(r))) \subset \mathbb{V}(\mathfrak{b})$. Using Proposition 1.4.8 we obtain

$$\mathfrak{b} = \bigcap_{\mathfrak{q}' \in \mathbb{V}(\mathfrak{b})} \mathfrak{q}' \subset \bigcap_{\mathfrak{q}' \in \mathbb{V}(\mathrm{Ann}(r - \phi(r)))} \mathfrak{q}' \subset \phi^n\text{-}\sqrt{\sqrt{\mathrm{Ann}(r - \phi(r))}}. \tag{2.2}$$

The last inclusion holds because by the RAAD condition $\sqrt{\mathrm{Ann}(r - \phi(r))}$ is a ϕ^n-ideal (for some n) and therefore its ϕ^n-radical is the intersection of prime ideals in ϕ^n-Spec$(R) = \phi$-Spec(R).

As $\mathfrak{q} \in \pi^{-1}(U) = X - \mathbb{V}(\mathfrak{b})$ we have $\mathfrak{b} \not\subseteq \mathfrak{q}$ and thus $\mathfrak{b} \not\subseteq \mathfrak{p}$. Using again Lemma 1.4.13 we obtain $\mathfrak{b}^{\phi} \not\subseteq \mathfrak{p}^{\phi}$. So we can find an $s' \in R^{\phi} \smallsetminus \mathfrak{p}^{\phi}$ such that $s' \in \mathfrak{b}$. By formula (2.2) there exist k, m such that $\phi^{nk}(s')^m \in \mathrm{Ann}(r - \phi(r))$. Because s' is constant we have $s'^m(r - \phi(r)) = 0$. Thus $\phi(s'^m r) = s'^m r \in R^{\phi}$. Set $r'' = s'^m r \in R^{\phi}$ and $s'' = s'^m s \in R^{\phi} \smallsetminus \mathfrak{p}^{\phi}$. We recall that on the open Φ-stable subset $\pi^{-1}(U) \cap D(s)$ the function F is given by the fraction $\frac{r}{s}$. Obviously $\frac{r''}{s''}$ and $\frac{r}{s}$ agree on $D(s'')$ and so

$$f_y^{\sharp}\left(\frac{r''}{s''}\right) = (U, F).$$

□

2.5 Split ϕ-spaces

Definition 2.5.1. *Let L be a ϕ-pfield, $C = L^{\phi}$ and X a ϕ-space over L. We say that X is* split *(over L) if there exists a scheme Y of finite type over C such that X is isomorphic to $L \times_C Y$ as ϕ-space over L.*

Philosophically the following theorem is like a Galois descent result.

Theorem 2.5.2. *Let L be a ϕ-pfield, $C = L^\phi$ and Y a scheme of finite type over C. Then*

$$(L \times_C Y)^\phi \simeq Y.$$

Proof: Applying the constant functor to the projection $L \times_C Y \to Y$ gives a morphism

$$f : (L \times_C Y)^\phi \to Y^\phi = Y$$

of locally ringed spaces. We will show that it is an isomorphism.

We first assume that Y is affine, i.e. $Y = \mathrm{Spec}(D)$ for some finitely generated C-algebra D. Then $L \times_C Y = \phi\text{-}\mathrm{Spec}(L \otimes_C D)$ by Corollary 2.1.12.

We know from Lemma 2.2.3 that $R = L \otimes_C D$ is Noetherian and RAAD. It follows from Proposition 1.4.15 that R satisfies all assumptions of Proposition 2.4.5. Bearing in mind that $(L \otimes_C D)^\phi = D$ by Lemma 1.4.14 we realize that indeed the claim follows from Proposition 2.4.5.

Now we treat the general case. It is enough to show that f is locally an isomorphism. So let $y \in Y$ and $U = \mathrm{Spec}(D)$ an open affine neighborhood of y. If $p_Y : L \times_C Y \to Y$ denotes the projection then $p_Y^{-1}(U) = L \times_C U$ and we have a commutative diagram

$$\begin{tikzcd}
L \times_C Y \arrow[r, "p_Y"] & Y \\
L \times_C U \arrow[r, "p_U"] \arrow[u, hook] & U \arrow[u, hook]
\end{tikzcd}$$

From Lemma 2.4.3 wee see that $(L \times_C U)^\phi$ is an open subspace of $(L \times_C Y)^\phi$ and so an application of the constant functor yields

$$\begin{tikzcd}
(L \times_C Y)^\phi \arrow[r, "f"] & Y \\
(L \times_C U)^\phi \arrow[r, "p_U^\phi"] \arrow[u, hook] & U \arrow[u, hook]
\end{tikzcd}$$

From the affine case - treated above - we know that p_U^ϕ is an isomorphism. So we can conclude that also f is an isomorphism. □

It follows from Theorem 2.5.2 that if X is split then X^ϕ is a scheme of finite type over C and $X \simeq L \times_C X^\phi$ where the isomorphism is induced from the structure map $X \to \phi\text{-}\mathrm{Spec}(L)$ and the projection $\pi : X \to X^\phi$.

Corollary 2.5.3. *Let L be a ϕ-pfield with $C = L^\phi$ and X, X' split ϕ-spaces over L. Then*

$$\mathrm{Hom}_L(X, X') \simeq \mathrm{Hom}_C(X^\phi, X'^\phi).$$

Proof: The constant functor yields a mapping

$$\alpha : \mathrm{Hom}_L(X, X') \to \mathrm{Hom}_C(X^\phi, X'^\phi).$$

As $X = L \times_C X^\phi$ and the quotient map $\pi : X \to X^\phi$ agrees with the projection we have for any morphism $f : X \to X'$ over L a commutative diagram

$$\begin{tikzcd}
L \times_C X^\phi \arrow[r, "f"] \arrow[d] & L \times_C X'^\phi \arrow[d] \\
X^\phi \arrow[r, "f^\phi"] & X'^\phi
\end{tikzcd}$$

This shows that "base extension to L" gives the inverse of α. □

Lemma 2.5.4. *Let L be a ϕ-pfield, $C = L^\phi$ and X a split ϕ-space over L. Then every open Φ-stable subset of X is split.*

Proof: Let $X = L \times_C Y$ where Y is a scheme of finite type over C. Because $\pi : L \times_C Y \to (L \times_C Y)^\phi = Y$ agrees with the projection onto the second factor we see that every open Φ-stable subset of X is of the form $\pi^{-1}(U) = L \times_C U$ for some open subscheme U of Y. □

The following proposition asserts that "being split" is a local property.

Proposition 2.5.5. *Let L be a ϕ-pfield, $C = L^\phi$, X a ϕ-space over L and $\{U_i\}$ a finite covering of X with open Φ-stable subsets. Then X is split if and only if every U_i is split.*

Proof: By Lemma 2.5.4 we only have to prove that X is split. As $\{U_i\}$ is an open Φ-stable covering of X we see by Lemma 2.4.3 that $\{U_i^\phi\}$ is an open covering of X^ϕ. Because U_i is split if follows from Theorem 2.5.2 that U_i^ϕ is a scheme of finite type over C. Therefore X^ϕ is a scheme of finite type over C. The structure map $X \to \phi\text{-Spec}(L)$ and the projection $\pi : X \to X^\phi$ induce a morphism $f : X \to L \times_C X^\phi$. By assumption f is an isomorphism when restricted to U_i, consequently f is an isomorphism. □

Lemma 2.5.6. *Let L be a ϕ-pfield and R an L-ϕ-algebra such that $X = \phi\text{-Spec}(R)$ is split over L. If $\mathfrak{a}$ is a ϕ-ideal of R and*

$$\phi\text{-Spec}(R/\mathfrak{a}) = Z \hookrightarrow X$$

is the closed ϕ-subspace of X induced by $\mathfrak{a}$ then Z is split and $Z^\phi \to X^\phi$ is a closed subscheme of X^ϕ.

Proof: Let $z \in Z \subset X$ and $U = \mathrm{Spec}(D)$ an open affine neighborhood of $\pi_X(z) \in X^\phi$. Then $\phi\text{-Spec}(L \otimes_C D) = L \times_C U = \pi_X^{-1}(U) \subset X$ is an open Φ-stable neighborhood of z in X. By Lemma 2.2.3 the ϕ-ring $L \otimes_C D$ is Noetherian and RAAD. Thus it follows from Lemma 2.3.2 that the closed ϕ-subspace $Z \cap (L \times_C U) \hookrightarrow L \times_C U$ is induced from a ϕ-ideal $\mathfrak{b}$ of $L \otimes_C D$. By Proposition 1.4.15 every ϕ-ideal of $L \otimes_C D$ is of the form $L \otimes_C \mathfrak{d}$ for some ideal $\mathfrak{d}$ of D. Hence if $\mathfrak{b} = L \otimes_C \mathfrak{d}$ then

$$Z \cap (L \times_C U) \simeq \phi\text{-Spec}(L \otimes_C D / L \otimes_C \mathfrak{d}) = \phi\text{-Spec}(L \otimes_C (D/\mathfrak{d})) = L \times_C \operatorname{Spec}(D/\mathfrak{d})$$

which shows that $Z \cap (L \times_C U)$ is an open Φ-stable split neighborhood of z in Z. Because X^ϕ is covered by a finite number of such U's it follows from Proposition 2.5.5 that Z is split. Furthermore an application of the constant functor to the commutative diagram

$$\begin{tikzcd}
Z \cap (L \times_C U) \arrow[r, hook] \arrow[d, "\simeq"'] & L \times_C U \arrow[d, "\simeq"] \\
L \times_C \operatorname{Spec}(D/\mathfrak{d}) \arrow[r] & L \times_C \operatorname{Spec}(D)
\end{tikzcd}$$

yields

$$\begin{tikzcd}
Z^\phi \arrow[r] & X^\phi \\
(Z \cap (L \times_C U))^\phi \arrow[r] \arrow[u, hook] \arrow[d, "\simeq"'] & U \arrow[u, hook] \arrow[d, "\simeq"] \\
\operatorname{Spec}(D/\mathfrak{d}) \arrow[r] & \operatorname{Spec}(D)
\end{tikzcd}$$

Thus $Z^\phi \to X^\phi$ is a closed immersion. □

Proposition 2.5.7. *Let L be a ϕ-pfield, $C = L^\phi$ and R an L-ϕ-algebra such that $X = \phi$-Spec(R) is split (over L). Then there is a one-to-one correspondence between the ϕ-ideals $\mathfrak{a}$ of R such that the natural map $R/\mathfrak{a} \to \widehat{R/\mathfrak{a}}$ is injective and the closed subschemes of X^ϕ. In more detail: If $\mathfrak{a}$ is a ϕ-ideal of R and*

$$\phi\text{-Spec}(R/\mathfrak{a}) = Z \hookrightarrow X$$

is the closed ϕ-subspace of X induced by $\mathfrak{a}$ then $Z^\phi \hookrightarrow X^\phi$ is a closed subscheme of X^ϕ.

Conversely if $Y \hookrightarrow X^\phi$ is a closed subscheme then $L \times_C Y \hookrightarrow L \times_C X^\phi = X$ is a closed ϕ-subspace which is induced from a ϕ-ideal of R. In fact it is induced by $\mathfrak{a} = \ker(R \to \mathcal{O}_{L \times_C Y}(L \times_C Y))$ and $R/\mathfrak{a} \to \widehat{R/\mathfrak{a}}$ is injective.

Proof: For given $\mathfrak{a}$ the map ϕ-Spec$(R/\mathfrak{a})^\phi \hookrightarrow X^\phi$ defines a closed subscheme by Lemma 2.5.6.

For a given subscheme Y of X^ϕ one immediately sees that $L \times_C Y \hookrightarrow L \times_C X^\phi$ is a closed immersion by considering an open affine subset of X^ϕ. Because X^ϕ is of finite type over C also Y is of finite type over C. If $\{U_i = \operatorname{Spec}(D_i)\}$ is a finite open affine covering of Y then $L \times_C U_i = \phi$-Spec$(L \otimes_C D_i)$ is a finite open Φ-stable covering of $L \times_C Y$. As the rings $L \otimes_C D_i$ are Noetherian and RAAD (Lemma 2.2.3) it follows from Proposition 2.3.5 that $L \times_C Y \hookrightarrow L \times_C X^\phi = X$ is induced by $\mathfrak{a} = \ker(R \to \mathcal{O}_{L\times_C Y}(L \times_C Y))$. Because

$$\begin{tikzcd} & R \arrow[dl] \arrow[dr] & \\ \widehat{R/\mathfrak{a}} \arrow[rr, "\simeq"] & & \mathcal{O}_{L\times_C Y}(L \times_C Y) \end{tikzcd}$$

is commutative it is clear that $R/\mathfrak{a} \to \widehat{R/\mathfrak{a}}$ is injective.

Now we will show that these two constructions are inverse to each other. We start with a ϕ-ideal $\mathfrak{a}$ of R such that $R/\mathfrak{a} \to \widehat{R/\mathfrak{a}}$ is injective. From Lemma 2.5.6 we know that $Z = \phi\text{-Spec}(R/\mathfrak{a}) = L \times_C Z^\phi$ is split. We need to show that $\mathfrak{a}$ is the kernel of $R \to \mathcal{O}_{L\times_C Z^\phi}(L \times_C Z^\phi)$. But this follows from the assumption that $R/\mathfrak{a} \to \widehat{R/\mathfrak{a}}$ is injective and the commutative diagram

$$\begin{tikzcd} & R \arrow[dl] \arrow[dr] & \\ \widehat{R/\mathfrak{a}} \arrow[rr, "\simeq"] & & \mathcal{O}_{L\times_C Z^\phi}(L \times_C Z^\phi) \end{tikzcd}$$

If we start with a closed subscheme Y of X^ϕ and $\mathfrak{a} \subset R$ is such that $L \times_C Y \hookrightarrow X$ is induced by $\mathfrak{a}$ then of course Y and $\phi\text{-Spec}(R/\mathfrak{a})^\phi$ define the same subscheme of X^ϕ. □

Chapter 3

ϕ-Galois theory

This chapter contains the main results of the present work. We address the question "When does an extension of ϕ-pfields admit a reasonable Galois theory with algebraic groups as Galois groups?". Our answer is a certain ϕ-normality property analogous to normality in the classical Galois theory (and strong normality in the differential Galois theory). And under this assumption we will develop our difference Galois theory. In particular we will establish the Galois correspondence between intermediate ϕ-pfields and closed subgroup schemes of the Galois group.

3.1 The general theory and the ϕ-Galois groupoid

Before dealing with ϕ-normality we first collect in this section some results on a very general kind of Galois correspondence. The impatient reader might well skip this section upon first reading as it is not strictly necessary for the understanding of the later sections.

The correspondence we have in mind is essentially a difference version of the Sweedler correspondence ([38]). The setting is very general: If $L|K$ is an extension of ϕ-pfields then there is a one-to-one correspondence between the intermediate ϕ-pfields of $L|K$ and certain ϕ-ideals of $L \otimes_K L$. We note that one may well take $\phi = \mathrm{id}$ and so as a special case one obtains some kind of Galois correspondence for an arbitrary field extension. In fact the same thing even works for skew fields.

One might get the impression that this Sweedler correspondence is too general to be really useful but in fact we shall use it in the later sections to establish our Galois correspondence. (This tactic has also been used in [39], [2] and [26]). Moreover it gives a further explanation why $L \otimes_K L$ is such an important thing. The key observation of M. Sweedler was that the crucial group-like structure of $L \otimes_K L$ can be encapsulated by saying that $L \otimes_K L$ is a coring and that precisely the coideals of $L \otimes_K L$ appear in the correspondence. In his article [38] M. Sweedler never mentions groupoids but corings relate to groupoids in much the same way as coalgebras relate to (algebraic) groups. As it seems more intuitive and closer to the classical Galois correspondence we choose to present the theory in the language of groupoids rather than in the language of corings. (Also groupoids are very fashionable in difference and differential Galois theory these days.) We therefore start by recalling some basic notions from the theory of groupoids.

A *groupoid* is a small category in which every morphism is invertible. A basic example (however quite irrelevant to us) is the groupoid of homotopy classes of paths in a topological space. A *subgroupoid* of a groupoid is a subcategory with the same set of objects that is also a groupoid. The set of objects of a groupoid G is usually called the base of G and denoted with S. The morphism of G are usually called arrows. A morphism of groupoids is simply a functor.

In the following let $\mathcal{C}$ be a category. We assume that $\mathcal{C}$ has a terminal object $\{*\}$ and that all the required fibred products exist. If X and T are objects of $\mathcal{C}$ we write $X(T) = \operatorname{Hom}_{\mathcal{C}}(T, X)$ for the T-valued points of X. A *groupoid in* $\mathcal{C}$ (cf. [16, p. 212-08]) consists of two objects G and S of $\mathcal{C}$ together with, for every object T of $\mathcal{C}$, the structure of a groupoid with arrows $G(T)$ and basis $S(T)$ which is functorial in T.

Since the appropriate fibre products exist by Yoneda's Lemma to specify a groupoid in $\mathcal{C}$ is equivalent to specifying morphism

$$\begin{aligned} s : G \to S &\quad \text{the source} \\ t : G \to S &\quad \text{the target} \\ \circ : G \underset{{}_tS^s}{\times} G \to G &\quad \text{the multiplication} \\ \epsilon : S \to G &\quad \text{the identity} \\ \text{“}-1\text{”} : G \to G &\quad \text{the inverse} \end{aligned}$$

satisfying some obvious commutative diagrams. [1]

Example 3.1.1 (The trivial groupoid)**.** If Z is an object of $\mathcal{C}$ then the trivial groupoid on Z is the groupoid of arrows in Z. To be precise $G = Z \times Z$ has a groupoid structure with base $S = Z$ given by

$$s : Z \times Z \to Z \quad \text{the projection onto the first factor,}$$

$$t : Z \times Z \to Z \quad \text{the projection onto the second factor,}$$

$$\circ : (Z \times Z) \underset{{}_tZ^s}{\times} (Z \times Z) \xrightarrow{s \times t} Z \times Z \quad \text{the natural map}$$

$$\epsilon : Z \xrightarrow{\mathrm{id} \cdot \mathrm{id}} Z \times Z \quad \text{the diagonal}$$

$$\text{“}-1\text{”} : Z \times Z \xrightarrow{t \cdot s} Z \times Z \quad \text{the twist.}$$

We note that in the category of sets the subgroupoids of $Z \times Z$ are simply the equivalence relations on Z.

[1] According to A. Grothendieck [16, p. 212-06.] “La traduction de cet axiome par la commutativité de certains diagrammes dans $\mathcal{C}$ est facile, mais fastidieuse, et en fait, parfaitement inutile dans tous le cas à ma connaissance.”

Example 3.1.2 (Action Groupoid)**.** Let $\mathcal{G}$ be a group object in $\mathcal{C}$ with multiplication $m : \mathcal{G} \times \mathcal{G} \to \mathcal{G}$, identity $1 : \{*\} \to \mathcal{G}$ and inverse $(^{-1}) : \mathcal{G} \to \mathcal{G}$ acting (from the right) on an object Z via

$$\rho : Z \times \mathcal{G} \to Z$$

then $G = Z \times \mathcal{G}$ has a natural groupoid structure with base $S = Z$ given by

$$s : Z \times \mathcal{G} \to Z \quad \text{the projection onto the first factor,}$$

$$t : Z \times \mathcal{G} \xrightarrow{\rho} Z \quad \text{the group action,}$$

$$\circ : (Z \times \mathcal{G}) \underset{{}^{t}Z^{s}}{\times} (Z \times \mathcal{G}) \xrightarrow{(sp_1)\cdot m(p_{\mathcal{G}}p_1 \times p_{\mathcal{G}}p_2))} Z \times \mathcal{G} \quad \text{or more intuitively}$$

$$((z,g),(z',g')) \mapsto (z, gg') \text{ if } zg = z'$$

$$\epsilon : Z = Z \times \{*\} \xrightarrow{\mathrm{id}\times 1} Z \times \mathcal{G}$$

$$\text{“}-1\text{”} : Z \times G \xrightarrow{t\cdot(^{-1})p_{\mathcal{G}}} Z \times G \quad \text{or more intuitively}$$

$$(z,g) \mapsto (zg, g^{-1}).$$

One calls G the *action groupoid* associated to ρ. By Yoneda's Lemma it suffices to give the prove in the case where $\mathcal{C}$ is the category of sets, and there it is a straight forward verification.

Example 3.1.3. The morphism

$$f : Z \times \mathcal{G} \xrightarrow{p_Z \cdot \rho} Z \times Z, \quad (z,g) \mapsto (z, zg)$$

is a morphism of groupoids. In case it is an isomorphism one calls Z a $\mathcal{G}$-torsor.

Let $\pi : Z \to S$ be a morphism in $\mathcal{C}$. An *action* (from the right) of a groupoid object G on Z is given by a morphism

$$\rho : Z \underset{{}^{\pi}S^{s}}{\times} G \to Z$$

such that $\pi\rho = tp_G$ and the following diagrams are commutative:

$$\begin{tikzcd}
Z = Z \underset{S}{\times} S \arrow[rr, "\mathrm{id}\times\epsilon"] \arrow[dr, "\mathrm{id}"'] & & Z \underset{{}^{\pi}S^{s}}{\times} G \arrow[dl, "\rho"] & \text{“identity”} \\
& Z & &
\end{tikzcd}$$

$$\begin{tikzcd}
Z \underset{{}^{\pi}S^{s}}{\times} G \underset{{}^{t}S^{s}}{\times} G \arrow[r, "\mathrm{id}\times\circ"] \arrow[d, "\rho\times\mathrm{id}"'] & Z \underset{{}^{\pi}S^{s}}{\times} G \arrow[d, "\rho"] & \text{“associativity”} \\
Z \underset{{}^{\pi}S^{s}}{\times} G \arrow[r, "\rho"] & Z &
\end{tikzcd}$$

The idea is that G operates *between* the fibres of π.

Example 3.1.4. The groupoid $G = Z \times Z$ naturally acts on Z by

$$\rho : Z \underset{\pi Z^s}{\times} G \xrightarrow{tp_G} Z$$

or more intuitively $(z,(z,z')) \mapsto z'$. Here $\pi : Z \to Z$ is taken to be the identity. The idea is simply that the arrow (z,z') maps its source to the target.

Example 3.1.5. The action groupoid $G = Z \times \mathcal{G}$ naturally operates on Z by

$$Z \underset{\pi Z^s}{\times} (Z \times \mathcal{G}) \longrightarrow Z, \ (z,(z,g)) \mapsto zg$$

Again $\pi : Z \to Z$ is taken to be the identity. If Z is a $\mathcal{G}$-torsor then the actions in Examples 3.1.4 and 3.1.5 agree.

From now on we fix a ϕ-pfield K. To study arbitrary ϕ-pfield extensions of K from the Galois theoretic point of view we will work with schemes with endomorphism rather than with difference schemes.

By a *scheme with endomorphism* (X, Φ) we of course mean a scheme X together with a morphism $\Phi : X \to X$ of schemes. A morphism in this category is a morphism $f : X \to X'$ of schemes such that $f\Phi = \Phi' f$. Obviously Spec$(-)$ induces a fully faithful functor from the category of ϕ-rings to the category of schemes with endomorphism. It is also clear that fibred products exist in the category of schemes with endomorphism.

From now on till the end of this section we will work in the category $\mathcal{C}$ of schemes with endomorphism over K. (I.e the objects are schemes with endomorphism together with a morphism to Spec(K) in the category of schemes with endomorphism.) Then Spec(K) is the terminal object in $\mathcal{C}$.

By a *closed immersion (in $\mathcal{C}$)* one means a morphism in $\mathcal{C}$ such that the induced morphism of schemes is a closed immersion. As usual a *closed subscheme with endomorphism* is an equivalence class of closed immersions. If R is a K-ϕ-algebra then clearly the closed subschemes with endomorphism of Spec(R) are in one-to-one correspondence with the ϕ-ideals of R.

Suppose that G is a groupoid in $\mathcal{C}$. By a *closed subgroupoid with endomorphism* H of G we mean a closed subscheme with endomorphism H of G such that $H(T)$ is a subgroupoid of $G(T)$ for every object T of $\mathcal{C}$.

Let G be a groupoid in $\mathcal{C}$ with basis S. Assume that G and S are affine, i.e. $G = \text{Spec}(R)$ and $S = \text{Spec}(L)$ where R and L are K-ϕ-algebras. Then by dualizing one can express the axioms that turn G into a groupoid purely algebraically in terms of R and L (cf. [11, Section 1.14, p. 116]).

If one dualizes the concept of (affine) algebraic groups then one arrives at Hopf-algebras and only keeping the "co"-structure leads to coalgebras. The similar process in our setting leads to the notion of ϕ-coring.

Definition 3.1.6. *Let L be ϕ-ring. A coalgebra in the monoidal category of L-ϕ-bimodules is called a* ϕ-coring *(over L).*

Explicitly a ϕ-coring R over L is an L-ϕ-bimodule together with L-ϕ-bimodule morphism $\triangle : R \to R \otimes_L R$ and $\epsilon : R \to L$ such that the diagrams

$$\begin{tikzcd}
R \arrow[r, "\triangle"] \arrow[d, "\triangle"'] & R \otimes_L R \arrow[d, "\mathrm{id} \otimes \triangle"] \\
R \otimes_L R \arrow[r, "\triangle \otimes \mathrm{id}"] & R \otimes_L R \otimes_L R
\end{tikzcd}$$

“coassociativity”

and

$$\begin{tikzcd}
R \arrow[r, "\triangle"] \arrow[d, "\triangle"'] \arrow[dr, "\mathrm{id}"] & R \otimes_L R \arrow[d, "\mathrm{id} \cdot \epsilon"] \\
R \otimes_L R \arrow[r, "\epsilon \cdot \mathrm{id}"] & R
\end{tikzcd}$$

“coidentity”

are satisfied. We stress the point that the definition of $R \otimes_L R$ uses the right L-module structure on the left factor and the left L-module structure on the right factor. Whereas the L-bimodule structure on $R \otimes_L R$ uses the left L-module structure on the left factor and the right L-module structure on the right factor.

A *coring* is simply a ϕ-coring with $\phi = \mathrm{id}$. Corings were introduced by M. Sweedler in [38] but by now they have already acquired a quite rich theory of their own (See [9]).

One also has the obvious notion of *ϕ-coideal* of a ϕ-coring: This is an L-ϕ-subbimodule $\mathfrak{a}$ of R such that $\epsilon(\mathfrak{a}) = 0$ and $\triangle(\mathfrak{a}) \subset \mathfrak{a} \otimes R + R \otimes \mathfrak{a}$. Then $R/\mathfrak{a}$ is naturally a ϕ-coring over L.

Example 3.1.7. Let L be a ϕ-pfield extension of K. By Example 3.1.1 $\mathrm{Spec}(L \otimes_K L)$ is naturally a groupoid in $\mathcal{C}$. Thus $L \otimes_K L$ is naturally a ϕ-coring over L. The structure maps are given by

$$\triangle : L \otimes_K L \to (L \otimes_K L) \otimes_L (L \otimes_K L),\ a \otimes b \mapsto (a \otimes 1) \otimes_L (1 \otimes b)$$

and

$$\epsilon : L \otimes_K L \to L,\ a \otimes b \mapsto ab.$$

If G is a groupoid (in the category of sets) acting on $\pi : Z \to S$ then one says that a function f on Z is invariant under the action of G if $f(z) = f(zg)$ for all $z \in Z$ and $g \in G$ with $\pi(z) = s(g)$. With a little care one can generalize this notion to $\mathcal{C}$:

Let G be a groupoid in $\mathcal{C}$ acting on $\pi : Z \to S$, $f \in \mathcal{O}_Z(Z)$, T a scheme with endomorphism over K and $g \in G(T)$. For a morphism $T' \to T$ in $\mathcal{C}$ we denote with $g_{T'} \in G(T')$ the composite $T' \to T \xrightarrow{g} G$. For $z \in Z(T')$ with $\pi(z) = s(g_{T'})$ we have two elements z and $zg_{T'}$ of $Z(T') = \mathrm{Hom}_{\mathcal{C}}(T', Z)$.

We say that f *is invariant under* g if the two images of f in $\mathcal{O}_{T'}(T')$ under the dual maps of z and $zg_{T'}$ coincide for every $z \in Z(T')$ with $\pi(z) = s(g_{T'})$ and every morphism $T' \to T$ in $\mathcal{C}$. If N is a subset of $\mathcal{O}_Z(Z)$ we define

$$G_N(T) = \{g \in G(T);\ \text{ every } f \text{ in } N \text{ is invariant under } g\}.$$

One easily checks that $G_N(T)$ is a subgroupoid of $G(T)$ and so G_N is a groupoid subfunctor of G. We define the *ring of invariants* under G by

$$\mathcal{O}_Z(Z)^G = \{f \in \mathcal{O}_Z(Z);\ f \text{ is invariant under } g \text{ for every } g \in G(T) \text{ and } T \in \mathcal{C}\}.$$

Definition 3.1.8. *Let $L|K$ be an arbitrary extension of ϕ-pfields. We set $Z = \operatorname{Spec}(L)$. By examples 3.1.1 and 3.1.4*

$$\widetilde{G}(L|K) = Z \times Z = \operatorname{Spec}(L \otimes_K L)$$

is naturally a groupoid in $\mathcal{C}$ that acts on Z. We call it the Galois groupoid with endomorphism of $L|K$.

We note that if Z is a set then the subgroupoids of $Z \times Z$ are in one-to-one correspondence with the equivalence relations on Z. Thus, even though $\operatorname{Spec}(L)$ might topologically just be a point, we can think of the subgroupoids of $\widetilde{G}$ (in $\mathcal{C}$) as equivalence relations on $\operatorname{Spec}(L)$ which are compatible with the difference structure and defined over K.

Lemma 3.1.9. *Let $L|K$ be an extension of ϕ-pfields, $\widetilde{G} = \widetilde{G}(L|K)$ the Galois groupoid with endomorphism acting on $Z = \operatorname{Spec}(L)$, $f \in L$, T a scheme with endomorphism over K and $g \in \widetilde{G}(T)$. Then f is invariant under g if and only if the images of $f \otimes 1$ and $1 \otimes f$ under $\Gamma(g) : L \otimes_K L \to \mathcal{O}_T(T)$ agree.*

Proof: Assume f is invariant under G. Take $T' = T$ and $T' \to T$ to be the identity. Let $z \in Z(T)$ be defined as $z : T \xrightarrow{g} \widetilde{G} \xrightarrow{s} Z$. Then $\pi(z) = z = s(g)$ and by definition $zg \in Z(T)$ equals $T \xrightarrow{g} \widetilde{G} \xrightarrow{t} Z$. To say that the images of f and under the duals of z and zg agree means that $f \otimes 1$ and $1 \otimes f$ have the same image under the dual of g.

To prove the converse let $T' \to T$ be a morphism in $\mathcal{C}$ and $z \in Z(T')$ such that $\pi(z) = z = s(g_{T'})$. Then $zg_{T'} : T' \to T \xrightarrow{g} \widetilde{G} \xrightarrow{t} Z$ and $z = s(g_{T'}) : T' \to T \xrightarrow{g} \widetilde{G} \xrightarrow{s} Z$. Therefore the images of f under the duals of z and $zg_{T'}$ must coincide if $\Gamma(g)(f \otimes 1) = \Gamma(g)(1 \otimes f)$. □

Lemma 3.1.10. *Let $L|K$ be an extension of ϕ-pfields, $\widetilde{G} = \widetilde{G}(L|K)$ the Galois goupoid with endomorphism and $K \subset N \subset L$ an intermediate ϕ-pfield. Then $\widetilde{G}_N$ is a closed subgroupoid with endomorphism of $\widetilde{G}$ naturally identified with $\widetilde{G}(L|N)$.*

Proof: Let $\mathfrak{a}$ denote the ϕ-ideal of $L \otimes_K L$ generated by $a \otimes 1 - 1 \otimes a$ for $a \in N$. We easily see that $\mathfrak{a}$ is the kernel of the canonical map $L \otimes_K L \to L \otimes_N L$ because there is a well defined map $L \otimes_N L \to (L \otimes_K L)/\mathfrak{a}$. Let $\widetilde{H}$ denote the subscheme with endomorphism defined by $\mathfrak{a}$. By Lemma 3.1.9 we know that $g \in \widetilde{G}(T)$ lies in $\widetilde{G}_N(T)$ if and only if $g : T \to \widetilde{G}$ factors through $\widetilde{H} \hookrightarrow \widetilde{G}$. This means that $\widetilde{G}_N$ is identified with $\widetilde{H} = \operatorname{Spec}((L \otimes_K L)/\mathfrak{a}) = \operatorname{Spec}(L \otimes_N L) = \widetilde{G}(L|N)$. □

Lemma 3.1.11. *Let $L|K$ be an extension of ϕ-pfields, $\widetilde{G} = \widetilde{G}(L|K)$ the Galois goupoid with endomorphism and $\widetilde{H}$ a closed subgroupoid with endomorphism of $\widetilde{G}$. Then $\widetilde{H}$ is defined by a ϕ-coideal $\mathfrak{a}$ of $L \otimes_K L$ and $a \in L$ is invariant under $\widetilde{H}$ with respect to the induced action of $\widetilde{H}$ on $Z = \operatorname{Spec}(L)$ if and only if $a \otimes 1 - 1 \otimes a \in \mathfrak{a}$. Moreover $L^{\widetilde{H}}$ is an intermediate ϕ-pfield of $L|K$.*

Proof: As $\widetilde{H}$ is a closed subscheme with endomorphism of $\widetilde{G} = \mathrm{Spec}(L \otimes_K L)$ it is defined by a ϕ-ideal $\mathfrak{a}$ of $L \otimes_K L$. Because $\widetilde{H}$ is a subgroupoid $\mathfrak{a}$ must be a ϕ-coideal. (In fact $\mathfrak{a}$ has further structural properties. For example since $\widetilde{H}$ is stable under inverses it follows that $\mathfrak{a}$ is stable under the twist. We shall not need this further properties.)

Assume that $a \in L$ is invariant under $\widetilde{H}$. In the definition of invariance take $T = T' = \widetilde{H}$, $T' \to T$ as the identity, $g = \mathrm{id} \in \widetilde{H}(T')$ and $z \in Z(T')$ as the source map of $\widetilde{H}$. Then $\pi(z) = z = s(g_{T'})$ and $zg_{T'} : \widetilde{H} \to Z$ agrees with the target map. Therefore the images of a under the dual maps of the source and target maps from $\widetilde{H}$ to Z must agree. This means that $a \otimes 1 - 1 \otimes a$ lies in $\mathfrak{a}$.

For the converse assume that $a \otimes 1 - 1 \otimes a$ lies in $\mathfrak{a}$. Let $g \in \widetilde{H}(T)$, $T' \to T$ a morphism $\mathcal{C}$ and $z \in Z(T')$ with $\pi(z) = s(g_{T'})$. As $z = \pi(z) = s(g_{T'})$ we see that z is given as

$$T' \to T \xrightarrow{g} \widetilde{H} \xrightarrow{s} Z$$

and $zg_{T'}$ is given as

$$T' \to T \xrightarrow{g} \widetilde{H} \xrightarrow{t} Z.$$

Because $a \otimes 1 - 1 \otimes a \in \mathfrak{a}$ already the images of a under the duals of source and target coincide.

It is obvious that the invariants $L^{\widetilde{H}}$ contain K and are stable under ϕ. Also if $a \in L$ is a non zero divisor that is invariant under $\widetilde{H}$ then also a^{-1} is invariant under $\widetilde{H}$. It therefore follows from Lemma 1.3.4 that $L^{\widetilde{H}}$ is a ϕ-pfield. □

Lemma 3.1.12. *Let $L|K$ be an extension of ϕ-pfields and $\widetilde{G} = \widetilde{G}(L|K)$ the Galois groupoid with endomorphism of L over K. Then $L^{\widetilde{G}} = K$.*

Proof: Clearly $K \subset L^{\widetilde{G}}$. Assume that $a \in L$ is invariant under $\widetilde{G}$. Taking $T = \widetilde{G}$ and $g = \mathrm{id} \in \widetilde{G}(T)$ in Lemma 3.1.9 we see that $a \otimes 1 = 1 \otimes a \in L \otimes_K L$. Because K is a direct product of fields this implies $a \in K$. □

The following lemma is the key to the general correspondence. It corresponds to [38, Fundamental Lemma 2.2, p. 397]. For us the proof is complicated by the fact that we have to work with ϕ-pfields and not just fields. In [2, Proposition 3.10, p. 755] K. Amano and A. Masuoka proved the corresponding statement for artinian simple module algebras using a beautiful categorical argument. Unfortunately if one specializes their setup to the difference case one finds that their results only apply to inversive ϕ-pfields so we can not directly cite their result. However, the proof presented here follows very closely the lines of [2], see also [3].

Lemma 3.1.13. *Let L be a ϕ-pfield and R a ϕ-coring over L that is generated as L-bimodule by a constant group-like element g, i.e. $g \in R$ satisfies $R = LgL$, $\phi(g) = g$, $\triangle(g) = g \otimes g$ and $\epsilon(g) = 1$. Set $M = \{a \in L;\ ag = ga\}$. Then M is a ϕ-pfield and the canonical map*

$$\alpha : L \otimes_M L \to R,\ a \otimes b \mapsto agb$$

is an isomorphism of ϕ-corings.

Proof: One immediately sees that M is a total ϕ-subring of L. Therefore M is a ϕ-pfield by Lemma 1.3.4. We also note that R is naturally a M-ϕ-module, i.e. the left and right M-module structures agree. The only difficulty is to show that α is injective.

As a first step we will show that we can assume without loss of generality that M is a field. Let $M = e_1M \oplus \cdots \oplus e_tM$. Clearly it suffices to show that $e_i(L \otimes_M L) \to e_iR$ is injective. We see that $e_iM \subset e_iL$ is an inclusion of ϕ^t-pfields and e_iM is a field. Also e_iR is a ϕ^t-coring over e_iL and $e_ig \in e_iR$ satisfies the same properties as stated in the lemma but with respect to ϕ^t. Because $e_i(L \otimes_M L) \to e_iR$ gets identified with the canonical map $e_iL \otimes_{e_iM} e_iL$ we can indeed assume that M is a field.

Now consider R only as coring over L. For the moment we do not take into account the difference structure on L or R. We will work in the category $\mathfrak{A}$ of R-comodules. A R-comodule V is a right L-module with a right L-linear structure map $\rho : V \to V \otimes_L R$ such that $(\mathrm{id} \otimes \triangle) \circ \rho = (\rho \otimes \mathrm{id}) \circ \rho$ and $(\mathrm{id} \otimes \epsilon) \circ \rho = \mathrm{id}$.

We consider L as R-comodule via the structure map

$$L \to L \otimes_L R,\ a \mapsto 1 \otimes_L ga.$$

A right L-linear map $f : L \to L$ is of course given by multiplication with $a = f(1) \in L$ and one sees that f is a morphism in $\mathfrak{A}$ if and only if $ag = ga$, which by definition is only possible if $a \in M$. Thus $\mathrm{End}_{\mathfrak{A}}(L)$ can be identified with M.

We claim that L is simple as R-comodule. Every R-subcomodule is of the form eL for some idempotent element e of L and one sees that for an arbitrary idempotent e the right L module eL is a R-subcomodule if and only if there exist $r \in R$ such that

$$ge = er.$$

Therefore $\phi^i(e)L$ is a R-subcomodule for every $i \geq 1$. We may choose a simple R-subcomodule eL of L. If $\phi(e)L$ had a non-trivial R-subcomodule $e'L$ then $\phi^{t-1}(e')L \subset \phi^t(e)L = eL$ would be a non-trivial R-subcomodule of L. Therefore also $\phi(e)L$ is simple and it follows that L is semisimple, i.e. the finite direct sum of simple R-comodules. But because the endomorphism ring of L equals M which is a field we can conclude that L is simple as R-comodule.

An element a of L defines an element $\widetilde{a}$ of $\mathrm{Hom}_{\mathfrak{A}}(L, R)$ by sending $b \in L$ to $agb \in R$.

Let $a_1, \ldots, a_n \in L$ be M-linearly independent elements. We claim that the sum $\mathrm{Im}(\widetilde{a_1}) + \cdots + \mathrm{Im}(\widetilde{a_n})$ in M is direct. We proceed by induction on n, the case $n = 1$ being trivial. So we assume that $\mathrm{Im}(\widetilde{a_1}) + \cdots + \mathrm{Im}(\widetilde{a_{n-1}})$ is a direct sum. Because $\mathrm{Im}(\widetilde{a_n}) \simeq L$ is simple the intersection of $\mathrm{Im}(\widetilde{a_n})$ with $\mathrm{Im}(\widetilde{a_1}) + \cdots + \mathrm{Im}(\widetilde{a_{n-1}})$ is zero or $\mathrm{Im}(\widetilde{a_n})$. If it is zero we are done. So we assume for a contradiction that $\mathrm{Im}(\widetilde{a_n}) \subset \mathrm{Im}(\widetilde{a_1}) + \cdots + \mathrm{Im}(\widetilde{a_{n-1}})$. For $i = 1, \ldots, n-1$ let $b_i \in M$ denote the element corresponding to the $\mathfrak{A}$-morphism

$$L \simeq \mathrm{Im}(\widetilde{a_n}) \hookrightarrow \mathrm{Im}(\widetilde{a_1}) \oplus \cdots \oplus \mathrm{Im}(\widetilde{a_{n-1}}) \to \mathrm{Im}(\widetilde{a_i}) \simeq L.$$

Here the second map is simply the projection. We note that $\mathrm{Hom}_{\mathfrak{A}}(L, R)$ is naturally a right module over $\mathrm{End}_{\mathfrak{A}}(L) = M$. In $\mathrm{Hom}_{\mathfrak{A}}(L, R)$ we have by construction $\widetilde{a_n} =$

$\widetilde{a_1}b_1 + \cdots + \widetilde{a_{n-1}}b_{n-1}$. Evaluating this identity at $1 \in L$ yields $a_n g = a_1 g b_1 + \cdots + a_{n-1} g b_{n-1} \in R$. Then applying $\epsilon : R \to L$ shows that $a_n = a_1 b_1 + \cdots + a_{n-1} b_{n-1} \in L$. This contradicts the M-linear independence of the a_i's.

We recall that we have to show that $\alpha : L \otimes_M L \to R$ is injective. If $a_1 \otimes b_1 + \cdots + a_n \otimes b_n$ lies in the kernel of α then we can assume that the a_i's are M-linearly independent. But then the fact that $\mathrm{Im}(\widetilde{a_1}) + \cdots + \mathrm{Im}(\widetilde{a_n})$ is direct in R implies that the b_i's must all be zero. □

Corollary 3.1.14. *Let $L|K$ be an extension of ϕ-pfields and $\mathfrak{a} \subset L \otimes_K L$ a ϕ-coideal. Then as an ideal $\mathfrak{a}$ is generated by the elements of the form $a \otimes 1 - 1 \otimes a$ with $a \in L$ and $a \otimes 1 - 1 \otimes a \in \mathfrak{a}$.*

Proof: Consider the ϕ-coring $R = (L \otimes_K L)/\mathfrak{a}$ over L. Then R satisfies the assumptions of Lemma 3.1.13 with $g = \overline{1 \otimes 1}$. Set $M = \{a \in L;\ a \otimes 1 - 1 \otimes a \in \mathfrak{a}\}$ and let $\mathfrak{a}' \subset L \otimes_K L$ denote the ideal generated by the elements of the form $a \otimes 1 - 1 \otimes a$ with $a \in M$. Then $(L \otimes_K L)/\mathfrak{a}' \simeq L \otimes_M L$. On the other hand we have a commutative diagram

$$\begin{tikzcd}
 & L \otimes_K L \arrow[dl] \arrow[dr] & \\
L \otimes_M L \arrow[rr] & & (L \otimes_K L)/\mathfrak{a}
\end{tikzcd}$$

where the horizontal arrow is an isomorphism by Lemma 3.1.13. Consequently $\mathfrak{a} = \mathfrak{a}'$. □

We note that it follows from the above corollary that every ϕ-coideal of $L \otimes_K L$ is also stable under the twist $L \otimes_K L \to L \otimes_K L,\ a \otimes b \mapsto b \otimes a$.

Corollary 3.1.15. *Let $L|K$ be an extension of ϕ-pfields and $\widetilde{G} = \widetilde{G}(L|K)$ the Galois groupoid with endomorphism of L over K. If $\widetilde{H}$ is a closed subgroupoid with endomorphism not equal to $\widetilde{G}$ then $L^{\widetilde{H}}$ is strictly larger than K.*

Proof: This is obvious from Lemma 3.1.11 and Corollary 3.1.14. □

Theorem 3.1.16 (The general Galois correspondence)**.** *Let $L|K$ be an extension of ϕ-pfields and $\widetilde{G} = \widetilde{G}(L|K)$ the Galois groupoid with endomorphism of $L|K$. Then there is an inclusion reversing one-to-one correspondence between the set of intermediate ϕ-pfields of $L|K$ and the set of closed subgroupoids with endomorphism of $\widetilde{G}$ given by $N \mapsto \widetilde{G}(L|N)$ and $\widetilde{H} \mapsto L^{\widetilde{H}}$.*

Proof: We know from Lemma 3.1.10 that $\widetilde{G}(L|N)$ is a closed subgroupoid with endomorphism of $\widetilde{G}$ and from Lemma 3.1.11 that $L^{\widetilde{H}}$ is an intermediate ϕ-pfield. We have $L^{\widetilde{G}(L|N)} = N$ by Lemma 3.1.12.

If $\widetilde{H}$ is a closed subgroupoid with endomorphism of $\widetilde{G}$ then obviously $\widetilde{H}$ is also a closed subgroupoid with endomorphism of $\widetilde{G}(L|L^{\widetilde{H}})$. By Lemma 3.1.12 we have $L^{\widetilde{G}(L|L^{\widetilde{H}})} = L^{\widetilde{H}}$. Thus it follows from Corollary 3.1.15 that $\widetilde{H} = \widetilde{G}(L|L^{\widetilde{H}})$. □

We conclude this section with an alternative formulation of Theorem 3.1.16.

Theorem 3.1.17 (Sweedler Correspondence). *Let $L|K$ be an extension of ϕ-pfields. Then there is a one-to-one correspondence between the intermediate ϕ-pfields of $L|K$ and the ϕ-coideals of $L \otimes_K L$ given as follows:*

If N is an intermediate ϕ-pfield of $L|K$ then the ideal $\mathfrak{a}$ of $L \otimes_K L$ generated by the elements of the form $a \otimes 1 - 1 \otimes a$ with $a \in N$ is a ϕ-coideal of $L \otimes_K L$. Conversely if $\mathfrak{a}$ is a ϕ-coideal of $L \otimes_K L$ then $N = \{a \in L;\ a \otimes 1 - 1 \otimes a \in \mathfrak{a}\}$ is an intermediate ϕ-pfield of $L|K$.

Proof: This is clear from Corollary 3.1.14 and the fact that $a \otimes 1 = 1 \otimes a \in L \otimes_N L$ implies $a \in N$ because N is direct product of fields. □

We remark that our version of the Sweedler correspondence is more extensive then the one given in [2, Proposition 3.10 (ii), p. 755]. If $L|K$ is an extension of inversive ϕ-pfields then the correspondence in [2] is between inversive intermediate ϕ-pfields and reflexive ϕ-coideals whereas our correspondence is between *all* intermediate ϕ-pfields and *all* ϕ-coideals. An extension of inversive ϕ-pfields may well have intermediate ϕ-pfields that are not inversive.

3.2 The Galois group

This section explains what the Galois group is meant to be. The existence of the Galois group (as group scheme) will be established in a later section.

One of the crucial problems in developing a Galois theory for difference or differential extensions $L|K$ is to make clear sense of the somewhat vague statement that "The Galois group is an algebraic group". After all it seems that it was precisely this issue which led E. Kolchin to the introduction of his axiomatic algebraic groups. In the contemporary literature one will sometimes find a statement like "There exists an algebraic group $\mathcal{G}$ over the constants C such that $\mathrm{Aut}(L|K) \simeq \mathcal{G}(C)$". Although logically correct this statement is deficient as it fails to uniquely determine the algebraic group $\mathcal{G}$ (even if $\mathcal{G}$ is reduced and the constants are algebraically closed. This is simply because there might well be an automorphism of abstract groups $\mathcal{G}(C) \simeq \mathcal{G}(C)$ which is not induced from an automorphism of algebraic groups. Take for example $\mathbb{G}_a(\mathbb{C})$ with the complex conjugation.)

Now the language of functors provides a very convenient and clear way to formulate the solution of such a "moduli problem". We simply have to define an appropriate automorphism functor of $L|K$ and then show that it is representable by an algebraic group.

Definition 3.2.1. *Let $L|K$ be an extension of ϕ-pfields such that $K^\phi = L^\phi$. We define the* Galois group (functor) $\mathrm{Gal}(L|K)$ *of L over K as the (contravariant) functor from the category of schemes of finite type over $C = K^\phi = L^\phi$ to the category of groups given by*

$$\mathrm{Gal}(L|K)(Y) = \mathrm{Aut}(L \times_C Y | K \times_C Y).$$

In more detail: If Y is a scheme of finite type over C then an element σ of $\mathrm{Gal}(L|K)(Y)$ is an invertible morphism $\sigma : L \times_C Y \to L \times_C Y$ in the category of ϕ-spaces such that

$$\begin{tikzcd}
L \times_C Y \arrow[rr, "\sigma"] \arrow[dr] & & L \times_C Y \arrow[dl] \\
& K \times_C Y &
\end{tikzcd}$$

commutes. We recall that $L \times_C Y$ is short hand for $\phi\text{-}\mathrm{Spec}(L) \times_{\phi\text{-}\mathrm{Spec}(C)} Y$ and this product exists in the category of ϕ-spaces (Proposition 2.1.14). On morphisms $\mathrm{Gal}(L|K)$ is given by "base extension".

We note that $\mathrm{Gal}(L|K)(C) = \mathrm{Aut}(\phi\text{-}\mathrm{Spec}(L)|\phi\text{-}\mathrm{Spec}(K))$ can be identified with the difference automorphisms of L over K.

A central topic of this work is to find natural conditions on $L|K$ which imply that $\mathrm{Gal}(L|K)$ is representable. So the question is, does there exists a scheme $\mathcal{G}$ of finite type over C and a functorial isomorphism

$$\mathrm{Gal}(L|K) \simeq \mathrm{Hom}_C(-, \mathcal{G}).$$

By the Yoneda Lemma such a $\mathcal{G}$ is uniquely determined (up to unique isomorphisms) and is naturally equipped with the structure of a group scheme over C.

The following proposition reflects the equivalence of the two definitions of a fine moduli space given in [34, Chapter 1, Paragraph 2, p. 22].

Proposition 3.2.2. *Let $L|K$ be an extension of ϕ-pfields such that $L^\phi = K^\phi (= C)$. Then the following are equivalent:*

(1) *The functor* $\mathrm{Gal}(L|K)$ *is representable.*

(2) *There exists a group scheme $\mathcal{G}$ of finite type over C together with a group action*

$$\rho : Z \times_C \mathcal{G} \to Z$$

of $\mathcal{G}$ on $Z = \phi$-$\mathrm{Spec}(L)$ *over K with the following property: For every scheme Y of finite type over C and every isomorphism $\sigma : Z \times_C Y \to Z \times_C Y$ over $K \times_C Y$ there exists a unique morphism $f : Y \to \mathcal{G}$ of schemes over C such that σ is the pullback of $Z \times_C \mathcal{G} \xrightarrow{\rho \cdot p_{\mathcal{G}}} Z \times_C \mathcal{G}$ along f.*

Proof: We first show that (1) implies (2). Let $\mathcal{G}$ be scheme of finite type over C which represents $\mathrm{Gal}(L|K)$, i.e. there exists an isomorphism

$$\mathrm{Aut}(L \times_C Y | K \times_C Y) \simeq \mathrm{Hom}_C(Y, \mathcal{G}) \qquad (3.1)$$

functorial in Y. Taking $Y = \mathcal{G}$ and the identity on $\mathcal{G}$ on the right hand side we obtain on the left hand side the so called "universal family" $\rho' \in \mathrm{Aut}(L \times_C \mathcal{G} | K \times_C \mathcal{G})$. Composing $\rho' : L \times_C \mathcal{G} \to L \times_C \mathcal{G}$ with the projection $p_Z : Z \times_C \mathcal{G} \to Z$ we obtain a morphism $\rho : Z \times_C \mathcal{G} \to Z$ over K.

We have to show that ρ defines a group action. We note that by the Yoneda Lemma $\mathcal{G}$ already comes equipped with the structure of a group scheme over C. The unitality respectively associativity of the action follows by applying the functoriality of (3.1) to the unit $\mathrm{Spec}(C) \to \mathcal{G}$ respectively the composition $\mathcal{G} \times_C \mathcal{G} \to \mathcal{G}$ and chasing $\mathrm{id} \in \mathrm{Hom}_C(\mathcal{G}, \mathcal{G})$ through the resulting diagrams

$$\begin{tikzcd}
\mathrm{Aut}(Z \times_C \mathcal{G} | K \times_C \mathcal{G}) \arrow[r, leftrightarrow, "\simeq"] \arrow[d] & \mathrm{Hom}_C(\mathcal{G}, \mathcal{G}) \arrow[d] \\
\mathrm{Aut}(Z|K) \arrow[r, leftrightarrow, "\simeq"] & \mathrm{Hom}_C(\mathrm{Spec}(C), \mathcal{G})
\end{tikzcd}$$

and

$$\begin{tikzcd}
\mathrm{Aut}(Z \times_C \mathcal{G} | K \times_C \mathcal{G}) \arrow[r, leftrightarrow, "\simeq"] \arrow[d] & \mathrm{Hom}_C(\mathcal{G}, \mathcal{G}) \arrow[d] \\
\mathrm{Aut}(Z \times_C \mathcal{G} \times_C \mathcal{G} | K \times_C \mathcal{G} \times_C \mathcal{G}) \arrow[r, leftrightarrow, "\simeq"] & \mathrm{Hom}_C(\mathcal{G} \times_C \mathcal{G}, \mathcal{G})
\end{tikzcd}$$

To see the last property in (2) let $f \in \mathrm{Hom}_C(Y, \mathcal{G})$ denote the element corresponding to $\sigma \in \mathrm{Aut}(Z \times_C Y | K \times_C Y)$ under (3.1). Applying functoriality to $f : Y \to \mathcal{G}$ we obtain

$$\begin{tikzcd}
\mathrm{Aut}(Z \times_C \mathcal{G} | K \times_C \mathcal{G}) \arrow[r, leftrightarrow, "\simeq"] \arrow[d] & \mathrm{Hom}_C(\mathcal{G}, \mathcal{G}) \arrow[d] \\
\mathrm{Aut}(Z \times_C Y | K \times_C Y) \arrow[r, leftrightarrow, "\simeq"] & \mathrm{Hom}_C(Y, \mathcal{G})
\end{tikzcd}$$

Again chasing $\mathrm{id} \in \mathrm{Hom}_C(\mathcal{G}, \mathcal{G})$ gives the desired result.

Now we will show that (2) implies (1). If $\mathcal{G}$ is a group scheme of finite type over C and $\rho : Z \times_C \mathcal{G} \to Z$ a group action over K then $\rho' : Z \times_C \mathcal{G} \xrightarrow{\rho \cdot p_{\mathcal{G}}} Z \times_C \mathcal{G}$ is an isomorphism over $K \times_C \mathcal{G}$ and there is a natural transformation of functors $\mathrm{Hom}_C(-, \mathcal{G}) \to \mathrm{Gal}(L|K)$. The requirement in (2) exactly means that this natural transformation is an isomorphism. □

Let $L|K$ be an extension of ϕ-pfields with $K^\phi = L^\phi$. If one is interested in developing a Galois theory for $L|K$ is seems very natural to require that $\mathrm{Gal}(L|K)$ is representable as this provides a Galois group with a good algebraic structure. However it is quite clear that this requirement alone will not suffice to guarantee the existence of a reasonable Galois theory. For example, in principle the Galois group could still be trivial. The additional requirement we need to make is that $Z = \phi$-$\mathrm{Spec}(L)$ is a torsor (=principal homogeneous space) for the natural action of the Galois group. Let's be more precise: Suppose that $\mathrm{Gal}(L|K)$ is representable by a group scheme $\mathcal{G}$ of finite type over C. Then, as explained in Proposition 3.2.2, there is a natural group action $\rho : Z \times_C \mathcal{G} \to Z$ over K and we require that

$$Z \times_C \mathcal{G} \xrightarrow{p_Z \cdot \rho} Z \times_K Z, \ (z, g) \mapsto (z, zg)$$

is an isomorphism. It is well known that some kind of torsor theorem sits at the heart of Galois theory, or at least at the heart of most Galois theories. It has even become quite standard to take the validity of an appropriate torsor theorem as the definition of "Galois". See for example [36], [41] or[3]. Here we do not follow this nomenclature and reserve the word "Galois" for a normality property of an extension which, under certain technical assumptions, is equivalent to the torsor theorem. (See Theorem 3.9.3.)

Definition 3.2.3. *Let $L|K$ be an extension of ϕ-pfields and $Z = \phi\text{-Spec}(L)$. By Example 3.1.1*

$$G = G(L|K) = \phi\text{-Spec}(L \otimes_K L) = Z \times_K Z$$

is naturally a groupoid (in the category of ϕ-spaces over K). We call it the ϕ-Galois groupoid of $L|K$. *If we want to consider $\phi\text{-Spec}(L \otimes_K L)$ without the groupoid structure we will usually write X instead of G. If we have occasion to consider X as ϕ-space over L it will always be via the first factor.*

The importance of $L \otimes_K L$ and its geometric interpretation as groupoid in Galois theory has been recognized by many authors, e.g. [38], [36], [26]. For example the passage from the usual Galois group to $L \otimes_K L$ is precisely how Grothendieck's faithfully flat descent generalizes Galois descent. Also Section 3.1 was meant to illustrate the key role played by $L \otimes_K L$.

One of the main goals of the present work is to answer the question "When does the ϕ-Galois groupoid come from an algebraic group?". As illustrated by the following theorem this question is closely related to the representability of $\text{Gal}(L|K)$.

Theorem 3.2.4. *Let $L|K$ be an extension of ϕ-pfields such that $K^\phi = L^\phi$. Then the following are equivalent:*

1. *The functor* $\text{Gal}(L|K)$ *is representable by a group scheme $\mathcal{G}$ and $Z = \phi\text{-Spec}(L)$ is a $\mathcal{G}$-torsor.*
2. *The ϕ-space $\phi\text{-Spec}(L \otimes_K L)$ is split over L.*

In this situation the ϕ-Galois groupoid of $L|K$ is naturally isomorphic to the action groupoid of the natural action of $\mathcal{G}$ on Z.

Proof: The implication (1)⇒(2) is trivial: If the torsor theorem holds then $\phi\text{-Spec}(L \otimes_K L) = Z \times_K Z \simeq Z \times_C \mathcal{G} = L \times_C \mathcal{G}$.

We have to prove (2)⇒(1): Set $G = \phi\text{-Spec}(L \otimes_K L) = Z \times_K Z$ and consider G as ϕ-space over L via the first factor. By assumption there exists a scheme $\mathcal{G}$ of finite type over C and an L-isomorphism $G \simeq L \times_C \mathcal{G}$. By Theorem 2.5.2 we can assume that $\mathcal{G} = G^\phi$.

Next we want to specify the group structure of $\mathcal{G}$. The basic idea is that the group structure of $\mathcal{G}$ is inherited from the groupoid structure of $G = G(L|K)$ via the functor of constants. This works because the functor of constants is compatible with products in the following sense: If R and R' are L-ϕ-algebras such that $X = \phi\text{-Spec}(R)$ and $X' = \phi\text{-Spec}(R')$ are split over L then

$$X \times_L X' = (L \times_C X^\phi) \times_L (L \times_C X'^\phi) = L \times_C X^\phi \times_C X'^\phi.$$

In particular $X \times_L X'$ is split and $(X \times_L X')^\phi = X^\phi \times_C X'^\phi$.

Some digression: If $\mathcal{G}$ is a group operating (from the right) on Z (say in the category of sets) then it is usually not possible to recover the group from the action groupoid $Z \times \mathcal{G}$. For example if Z is a $\mathcal{G}$ and a $\mathcal{G}'$ torsor then $Z \times \mathcal{G}$ and $Z \times \mathcal{G}'$ are isomorphic as groupoids because they are both isomorphic to the trivial groupoid $Z \times Z$.

However, if we are by some chance given the projection $Z \times \mathcal{G} \to \mathcal{G}$ where $\mathcal{G}$ is only given as set then we can apply this projection to

$$\begin{aligned} Z \times \mathcal{G} \times \mathcal{G} = (Z \times \mathcal{G}) \underset{{}^tZ^s}{\times} (Z \times \mathcal{G}) &\to Z \times \mathcal{G} \\ (z, g, g') \longmapsto ((z, g), (zg, g')) &\longmapsto (z, gg') \end{aligned}$$

to recover the group structure on $\mathcal{G}$.

In our situation we are lucky enough to have this projection

$$Z \times_C \mathcal{G} = Z \times_K Z = G \to \mathcal{G}$$

available as it is simply given by $\pi_G : G \to G^\phi = \mathcal{G}$ the projection onto constants. So we can actually *define* the group structure in this way.

Thus the multiplication $\mathcal{G} \times_C \mathcal{G} \to \mathcal{G}$ is obtained by applying the constant functor to

$$Z \times_C \mathcal{G} \times_C \mathcal{G} = (Z \times_C \mathcal{G}) \underset{{}^tZ^s}{\times} (Z \times_C \mathcal{G}) = G \underset{{}^tZ^s}{\times} G \longrightarrow G = Z \times_C \mathcal{G}.$$

The group identity $\text{Spec}(C) \to \mathcal{G}$ is obtained by applying the constant functor to the groupoid identity $Z \to G$. The group inverse is obtained by applying the constant functor to the groupoid inverse, associativity of the groupoid multiplication yields the associativity of the group multiplication and similarly for the other obligatory diagrams.

By definition the C-scheme structure map $\mathcal{G} \to \text{Spec}(C)$ is obtained by applying the constant functor to the source map $s : G \to Z$. (We always considered $L \otimes_K L$ as L-algebra via the first factor.) But $s^\phi = t^\phi : \mathcal{G} \to \text{Spec}(C)$ because $C = L^\phi = K^\phi \subset K$. This explains why $\mathcal{G}$ becomes a group and not just a groupoid. After all, a groupoid object whose base is the terminal object is just a group object.

In a similar fashion we obtain the group action (from the right) of $\mathcal{G}$ on $Z = \phi\text{-Spec}(L)$. The action

$$Z \times_C \mathcal{G} \to Z$$

is defined by composing the fundamental isomorphism $Z \times_C \mathcal{G} = Z \times_K Z$ with the projection onto the second factor. In other words the action is the target map (which makes perfect sense). The associativity and unit diagram of this action are obtained from the associativity and unit diagram of the natural groupoid action of $G = Z \times_K Z$

on Z (cf. Example 3.1.4). It is now trivial that Z is a $\mathcal{G}$-torsor (a $\mathcal{G}_K = K \times_C \mathcal{G}$-torsor to be precise) and that the ϕ-Galois groupoid G is the associated action groupoid.

It remains to see that $\mathcal{G} = G^{\phi}$ actually represents $\mathrm{Gal}(L|K)$. We first need to consider the functor $\mathrm{End}(L|K)$ of endomorphisms of $L|K$ defined by $\mathrm{End}(L|K)(Y) = \mathrm{End}(L \times_C Y | K \times_C Y)$ for a scheme Y of finite type over C.

We claim that $\mathrm{End}(L|K)$ and $\mathrm{Hom}_C(-, \mathcal{G})$ are isomorphic as functors from the category of schemes of finite type over C to the category of monoids. Using Corollary 2.5.3 we obtain the following chain of identifications for a scheme Y of finite type over C:

$$\begin{aligned}\mathrm{End}(L|K)(Y) &= \mathrm{Hom}_{K\times_C Y}(L \times_C Y, L \times_C Y) = \mathrm{Hom}_K(L \times_C Y, Z) = \\ &= \mathrm{Hom}_L(L \times_C Y, Z \times_K Z) = \mathrm{Hom}_L(L \times_C Y, L \times_C \mathcal{G}) = \\ &= \mathrm{Hom}_C(Y, \mathcal{G}) = \mathcal{G}(Y)\end{aligned}$$

If $f \in \mathrm{Hom}_C(Y, \mathcal{G})$ then the corresponding element

$$\widetilde{f} \in \mathrm{End}(L|K)(Y) = \mathrm{Hom}_{K\times_C Y}(Z \times_C Y, Z \times_C Y)$$

is given by

$$\widetilde{f} : Z \times_C Y \xrightarrow{(t\circ f_Z)\cdot p_Y} Z \times_C Y,\ (z, y) \mapsto (zf(y), y).$$

From this formula it follows easily that the construction is functorial in Y and that $\widetilde{fg} = \widetilde{f}\widetilde{g}$. Thus $\mathrm{End}(L|K)$ and $\mathrm{Hom}_C(-, \mathcal{G})$ are isomorphic. As the latter is a group functor $\mathrm{End}(L|K)(Y)$ must be a group for every Y, i.e. $\mathrm{End}(L|K) = \mathrm{Aut}(L|K) = \mathrm{Gal}(L|K)$. Therefore $\mathrm{Gal}(L|K)$ is represented by $\mathcal{G}$ and the group structure on $\mathcal{G}$ obtained via the functor of constants and the group structure on $\mathcal{G}$ obtained from the Yoneda Lemma agree. It is also clear that the action of $\mathcal{G}$ on Z defined above and the action of $\mathcal{G}$ on Z as constructed in the proof of Proposition 3.2.2 are the same. Therefore all definitions are consistent and the theorem is proved. □

3.3 ϕ-Galois extensions

In this section we introduce the ϕ-normality conditions and define ϕ-Galois extensions.

We start with a small reflection on the relation between $L \otimes_K L$ and automorphisms or rather isomorphisms of $L|K$.

Definition 3.3.1. *Let $L|K$ be an extension of ϕ-pfields and M a K-ϕ-algebra. By an* isomorphism of $L|K$ in M *we mean a pair $\sigma = (\sigma_s, \sigma_t)$ of K-ϕ-morphisms from L to M. In this situation one usually considers M as L-ϕ-algebra via σ_s, so that σ_s is interpreted as the identity and one writes simply σ for σ_t.*

The actual isomorphism we have in mind by this definition is the map that send $\sigma_s(a)$ to $\sigma_t(a)$ for $a \in L$. If M is a K-ϕ-algebra then clearly the set of isomorphisms of $L|K$ in M is in bijection with the K-ϕ-algebra morphisms from $L \otimes_K L$ to M.

Thus the isomorphisms of $L|K$ in M can be interpreted as the M-valued points of $G = \phi\text{-Spec}(L \otimes_K L)$.

If we enlarge the K-ϕ-algebra M in Definition 3.3.1 to a K-ϕ-algebra M' we obtain a "new" isomorphism σ' of L over K in M' which obviously contains no new information about the extension $L|K$. Alternatively we could also replace M by $\sigma_s(L) \cdot \sigma_t(L) \subset M$ without loosing valuable information. So we introduce a suitable equivalence relation between isomorphisms which will make σ and σ' equivalent. This is loosely analogous to how one can pass from the representing functor of an (affine) scheme to the actual topological space or its closed subschemes.

Definition 3.3.2. *Let $\sigma = (\sigma_s, \sigma_t)$ and $\sigma' = (\sigma'_s, \sigma'_t)$ be isomorphisms of $L|K$ in M respectively M'. We say that σ'* is a specialization of σ *(for short $\sigma \to \sigma'$) if the "mapping"*

$$\psi : \sigma_s(L) \cdot \sigma_t(L) \to \sigma'_s(L) \cdot \sigma'_t(L)$$

defined by $\psi(\sigma_s(a)\sigma_t(b)) = \sigma'_s(a)\sigma'_t(b)$ is well defined. If $\sigma \to \sigma'$ and $\sigma' \to \sigma$ we say that σ and σ' are equivalent. (In traditional language: σ' is a generic specialization of σ.)

Proposition 3.3.3. *There is a one-to-one correspondence between equivalence classes of isomorphisms of $L|K$ and ϕ-ideals of $L \otimes_K L$.*

More specifically if $\sigma = (\sigma_s, \sigma_t)$ is an isomorphism of $L|K$ in M then the kernel of $L \otimes_K L \to M$, $a \otimes b \mapsto \sigma_s(a)\sigma_t(b)$ is a ϕ-ideal of $L \otimes_K L$. Conversely if $\mathfrak{a}$ is a ϕ-ideal of $L \otimes_K L$ set $M = L \otimes_K L/\mathfrak{a}$ and define σ by $\sigma_s(a) = \overline{a \otimes 1} \in M$ and $\sigma_t(a) = \overline{1 \otimes a} \in M$.

Under this correspondence "$\to$" corresponds to inclusion of ideals and ϕ-prime ideals correspond to isomorphisms in ϕ-pfields.

Proof: Let σ be an isomorphism of $L|K$ in M. Obviously the kernel $\mathfrak{a}$ of the map $\overline{\sigma} : L \otimes_K L \to M$, $a \otimes b \mapsto \sigma_s(a)\sigma_t(b)$ does not depend on the choice of σ in an equivalence class. If $M' = L \otimes_K L/\mathfrak{a}$ and σ' is defined by $\sigma'_s(a) = \overline{a \otimes 1} \in M'$ and $\sigma'_t(a) = \overline{1 \otimes a} \in M'$ then the vertical map in the commutative diagram

$$\begin{tikzcd}
 & L \otimes_K L/\mathfrak{a} \arrow[dd] \\
L \otimes_K L \arrow[ur] \arrow[dr] & \\
 & M
\end{tikzcd}$$

induces an isomorphism from $\sigma'_s(L) \cdot \sigma'_t(L)$ onto $\sigma_s(L) \cdot \sigma_t(L)$ and we conclude that σ and σ' are equivalent.

Conversely if $\mathfrak{a}$ is a ϕ-ideal and σ is defined as in the statement of the lemma then it is trivial that $\mathfrak{a}$ is the kernel of $L \otimes_K L \to M = L \otimes_K L/\mathfrak{a}$.

If σ, σ' are isomorphisms of $L|K$ in M respectively M' then σ' is a specialization of σ if and only if the dotted arrow in

$$\begin{tikzcd}
 & \sigma_s(L)\cdot\sigma_t(L) \arrow[dd, dotted] \\
L\otimes_K L \arrow[ur, "\overline{\sigma}"] \arrow[dr, "\overline{\sigma'}"'] & \\
 & \sigma'_s(L)\cdot\sigma'_t(L)
\end{tikzcd}$$

exists, which is the case if and only if the kernel of $\overline{\sigma}$ lies in the kernel of $\overline{\sigma'}$.

Finally by Proposition 1.4.2 the kernel of a morphism into a ϕ-pfield is a ϕ-prime ideal and if $\mathfrak{p}$ is a ϕ-prime ideal of $L\otimes_K L$ then $\mathfrak{Q}(L\otimes_K L/\mathfrak{p})$ is a ϕ-pfield. □

Now we introduce the crucial ϕ-normality conditions.

Definition 3.3.4. *Let $L|K$ be an extension of ϕ-pfields.*

(1) *Let $\sigma=(\sigma_s,\sigma_t)$ be an isomorphism of $L|K$ in M. We say that $L|K$ is* ϕ-normal with respect to σ *if*

$$\sigma_t(L)\subset\sigma_s(L)M^{\phi}.$$

(2) *If $\mathcal{C}$ is some class of K-ϕ-algebras we say that $L|K$* is ϕ-normal with respect to $\mathcal{C}$ *if $L|K$ is ϕ-normal with respect to every isomorphism of $L|K$ in M for every M in $\mathcal{C}$.*

(3) *We call $L|K$* generically ϕ-normal *if there exists a ϕ-over ring M of $L\otimes_K L$ such that $K(L\otimes_K L)=M$ and $L|K$ is ϕ-normal with respect to σ defined by $\sigma_s(a)=a\otimes 1$ and $\sigma_t(a)=1\otimes a$.*

We recall (see the "conventions" after the table of contents) that LM^{ϕ} denotes the smallest subring of M that contains L and M^{ϕ} *and is closed under inverses.* In (3) above M might, but need not be the total quotient ring of $L\otimes_K L$. It is in general not clear if ϕ can be extended to $\mathfrak{Q}(L\otimes_K L)$ (but see Proposition 1.7.3). Of course this is always possible if L and K are inversive.

To give an example of ϕ-normality we need to recall the definition of a Picard-Vessiot extension. In the standard literature (such as [43]) this definition is usually only made for inversive base fields (or ϕ-pseudo fields) and often the constants are assumed to be algebraically closed. With a little care these assumptions can be avoided.

Definition 3.3.5. *Let K be a ϕ-pfield and $A\in\mathrm{GL}_n(K)$. A ϕ-pfield extension $L|K$ is called* Picard-Vessiot (for the equation $\phi(y)=Ay$) *if*

(1) *there exists $Y\in\mathrm{GL}_n(L)$ such that $\phi(Y)=AY$,*

(2) *$L=K(Y_{ij};\ 1\leq i,j\leq n)$ and*

(3) *$K^{\phi}=L^{\phi}$.*

It has become customary to define Picard-Vessiot extensions via a detour through Picard-Vessiot rings but for our purposes the above definition seems more suitable. The equivalence of these definitions follows as in [43, Proposition 1.23, p. 17].

Example 3.3.6. If $L|K$ is a Picard-Vessiot extension then $L|K$ is ϕ-normal with respect to K-ϕ-algebras.

Proof: Let M be a K-ϕ-algebra and $\sigma_s, \sigma_t : L \to M$ two K-ϕ-morphisms. If Y is a fundamental solution matrix in L for $A \in \mathrm{GL}_n(K)$, i.e. $Y \in \mathrm{GL}_n(L)$ and $\phi(Y) = AY$. Then $\sigma_s(Y)$ and $\sigma_t(Y)$ are fundamental solution matrices in M. Set $D = \sigma_s(Y)^{-1}\sigma_t(Y) \in \mathrm{GL}_n(M)$. We have

$$\phi(D) = (A\sigma_s(Y))^{-1}A\sigma_t(Y) = \sigma_s(Y)^{-1}\sigma_t(Y) = D$$

and therefore $D \in \mathrm{GL}_n(M^\phi)$. By definition $\sigma_t(Y) = \sigma_s(Y)D$ and because L is generated by the entries of Y it follows that $\sigma_t(L) \subset \sigma_s(L)M^\phi$. □

It seems quite natural to conjecture that the converse of Example 3.3.6 is also true, namely:

Conjecture: Let $L|K$ be an extension of ϕ-pfields such that $L^\phi = K^\phi$ is algebraically closed and L is finitely generated as total ring over K. Then $L|K$ is Picard-Vessiot if and only if $L|K$ is ϕ-normal with respect to K-ϕ-algebras.

Lemma 3.3.7. *Let $L|K$ be an extension of ϕ-pfield. Then $L|K$ is ϕ-normal with respect to the class of ϕ-pfield extension of K if and only if $k(\mathfrak{p}) = Lk(\mathfrak{p})^\phi$ for every ϕ-prime ideal $\mathfrak{p}$ of $L \otimes_K L$. (We recall that $k(\mathfrak{p}) = \mathfrak{Q}((L \otimes_K L)/\mathfrak{p})$ denotes the residue ϕ-pfield at $\mathfrak{p}$.)*

Proof: If $\sigma_s, \sigma_t : L \to M$ are K-ϕ-morphisms into some ϕ-pfield M then the kernel $\mathfrak{p}$ of $L \otimes_K L \to M,\ a \otimes b \mapsto \sigma_s(a)\sigma_t(b)$ is a ϕ-prime ideal and the inclusion $Lk(\mathfrak{p})^\phi = k(\mathfrak{p}) \hookrightarrow M$ shows that $L|K$ is ϕ-normal with respect to $\sigma = (\sigma_s, \sigma_t)$. □

The following proposition gives a recipe to construct extensions that are ϕ-normal with respect to ϕ-pfields. It seems well possible to generalize this construction to non-constant A's (cf. Section 3.12).

Proposition 3.3.8. *Let C be a (constant) field, $\mathcal{H}$ a connected (not necessarily linear) algebraic group over C and $A \in \mathcal{H}(C)$. Let $L = C(\mathcal{H})$ denote the function field of $\mathcal{H}$. Consider L as difference field via left translation with A, i.e.*

$$\phi : L \to L,\ f \mapsto (z \mapsto f(Az)).$$

Then $L|C$ is ϕ-normal with respect to ϕ-pfield extensions of C.

Proof: If M is a ϕ-pfield extension of C then we have an induced group morphism $\phi : \mathcal{H}(M) \to \mathcal{H}(M)$ on $\mathcal{H}(M) = \mathrm{Hom}_C(\mathrm{Spec}(M), \mathcal{H})$: If $h : \mathrm{Spec}(M) \to \mathcal{H}$ then $\phi(h) : \mathrm{Spec}(M) \xrightarrow{\phi^*} \mathrm{Spec}(M) \xrightarrow{h} \mathcal{H}$.

We first show that if $\phi(h) = h$ then h factors through $\mathrm{Spec}(M^\phi)$, in other words: $\mathcal{H}(M)^\phi = \mathcal{H}(M^\phi)$. The elements of $\mathrm{Spec}(M)$ are of the form $\mathfrak{q}, \phi^{-1}(\mathfrak{q}), \ldots, \phi^{-(d-1)}(\mathfrak{q})$ for some prime ideal $\mathfrak{q}$ of M with $\phi^{-d}(\mathfrak{q}) = \mathfrak{q}$. If

$$\begin{tikzcd}
\mathrm{Spec}(M) \arrow[rr, "\phi^*"] \arrow[dr, "h"'] & & \mathrm{Spec}(M) \arrow[dl, "h"] \\
& \mathcal{H} &
\end{tikzcd}$$

is commutative then $h(\mathfrak{q}) = h(\phi^{-1}(\mathfrak{q}))$ and it follows that the image of h is just a single point. Let $U = \mathrm{Spec}(D)$ be an open affine neighborhood of this point in $\mathcal{H}$. Then h factors through $U \subset \mathcal{H}$ and we have an induced commutative diagram

$$\begin{tikzcd}
& D \arrow[dl] \arrow[dr] & \\
M \arrow[rr, "\phi"] & & M
\end{tikzcd}$$

of the dual maps. This shows that $D \to M$ factors through M^ϕ and therefore h factors through $\mathrm{Spec}(M^\phi)$.

Let (as before) M be a ϕ-pfield extension of C and $\sigma_s, \sigma_t : L \to M$ a pair of C-ϕ-morphisms. Let $gen : \mathrm{Spec}(L) \to \mathcal{H}$ denote the generic point and let $h_s, h_t \in \mathcal{H}(M)$ be defined by

$$h_s : \mathrm{Spec}(M) \xrightarrow{\sigma_s^*} \mathrm{Spec}(L) \xrightarrow{gen} \mathcal{H}$$

$$h_t : \mathrm{Spec}(M) \xrightarrow{\sigma_t^*} \mathrm{Spec}(L) \xrightarrow{gen} \mathcal{H}.$$

By construction $\phi(gen) = Agen$ and also $\phi(h_s) = Ah_s$, $\phi(h_t) = Ah_t$. Let $c = h_s^{-1}h_t \in \mathcal{H}(M)$. Computing

$$\phi(c) = \phi(h_s)^{-1}\phi(h_t) = (Ah_s)^{-1}Ah_t = h_s^{-1}h_t = c$$

as in Example 3.3.6 we see that $c \in \mathcal{H}(M)^\phi = \mathcal{H}(M^\phi)$.

Let $a \in L$. We have to show that $\sigma_t(a) \in \sigma_s(L)M^\phi \subset M$. By definition $h_t = h_s c \in \mathcal{H}(M)$. Let $U = \mathrm{Spec}(D)$ be an affine open subset of $\mathcal{H}$ such that $a \in L = C(\mathcal{H})$ defines a regular function on U. Let $U_s = \mathrm{Spec}(D_s)$ and $U_c = \mathrm{Spec}(D_c)$ be affine open subsets of $\mathcal{H}$ containing the image (which is just one point) of h_s and c respectively. The composition

$$\mathrm{Spec}(M) \xrightarrow{h_s \cdot c} U_s \times_C U_c \xrightarrow{m} \mathcal{H} \tag{3.2}$$

is simply $h_t = h_s c$. Here m denotes the map induced by the group multiplication. Because the image of h_t is only the generic point, the open set $m^{-1}(U) \subset U_s \times_C U_c$ contains the image of $h_s \cdot c$.

In general, if $\mathrm{Spec}(R)$ is an affine scheme and V an open subset containing the points $p_1, \dots, p_n$ then there exists $f \in R$ such that $p_1, \dots, p_n \in D(f) \subset V$. (This is just the prime avoidance Lemma ([12, Lemma 3.3, p. 90])). Consequently there exists $f \in D_s \otimes_C D_c$ such that the (finite) image of $h_s \cdot c$ lies in

$$D(f) = \mathrm{Spec}((D_s \otimes_C D_c)_f) \subset \mathrm{Spec}(D_s \otimes_C D_c) = U_s \times_C U_c$$

and $D(f) \subset m^{-1}(U)$. This implies that we can restrict the maps in (3.2) to

$$\mathrm{Spec}(M) \to \mathrm{Spec}((D_s \otimes_C D_c)_f) \to \mathrm{Spec}(D) = U. \tag{3.3}$$

Because $h_t = h_s c$ we know that $\sigma_t(a)$ equals the image of a under the map dual to the map above. The map $D_s \to M$ dual to $\mathrm{Spec}(M) \to \mathrm{Spec}(D_s) = U_s \subset \mathcal{H}$ has image in $\sigma_s(L)$. As seen at the beginning of the proof, the map $D_c \to M$ dual to $\mathrm{Spec}(M) \to \mathrm{Spec}(D_c) = U_c \subset \mathcal{H}$ has image in M^ϕ. Therefore, looking at the duals in (3.3) yields $\sigma_t(a) \in \sigma_s(L)M^\phi$ as desired. □

Lemma 3.3.9. *Let $L|K$ be a generically ϕ-normal extension of ϕ-pfields. Then L is ϕ-separable over K.*

Proof: By assumption there exists a ϕ-overring M of $L \otimes_K L$ such that $M = K(L \otimes_K L)$ and $L|K$ is ϕ-normal with respect to σ defined by $\sigma_s(a) = a \otimes 1$ and $\sigma_t(a) = 1 \otimes a$. Let $S = \{s \in L \otimes_K L;\ s \in M^\times\}$. Then S is a multiplicatively closed ϕ-stable subset of $L \otimes_K L$ consisting of non zero divisors and M can be identified with $S^{-1}(L \otimes_K L)$. We consider M as L-ϕ-algebra via the first factor. By assumption $\sigma(L) = \sigma_t(L) \subset LM^\phi$ and so $M = LM^\phi$.

It follows from Lemma 1.1.6 that L and M^ϕ are linearly disjoint over $C = L^\phi$ inside M. Therefore M is identified with $T^{-1}(L \otimes_C M^\phi)$ where T is a multiplicatively closed ϕ-stable subset of $L \otimes_C M^\phi$ consisting of non zero divisors. We have thus an L-ϕ-isomorphism $\psi : S^{-1}(L \otimes_K L) \to T^{-1}(L \otimes_C M^\phi)$. Let L^* denote the inversive closure of L. We can trivially extend ψ to an L^*-ϕ-isomorphism

$$\psi : S^{-1}(L^* \otimes_K L) \to T^{-1}(L^* \otimes_C M^\phi).$$

As $L^* \otimes_K L = L^* \otimes_L (L \otimes_K L)$ (respectively $L^* \otimes_C M^\phi = L^* \otimes_L (L \otimes_C M^\phi)$) and L^* is flat as L-module it follows from Lemma 1.5.8 that the elements of S (respectively T) are non zero divisors in $L^* \otimes_K L$ (respectively $L^* \otimes_C M^\phi$). Because ϕ is an automorphism on $L^* \otimes_C M^\phi$ we see that ϕ is injective on $T^{-1}(L^* \otimes_C M^\phi)$. Therefore ϕ must also be injective on $L^* \otimes_K L$ and it follows from Proposition 1.5.2 (2) that L is ϕ-separable over K. □

Definition 3.3.10. *We say that an extension $L|K$ of ϕ-pfields is* ϕ-Galois *if the following assertions are satisfied.*

(1) *L is finitely generated as total ring over K.*

(2) *L has bounded periodicity.*

(3) *$L^\phi = K^\phi$.*

(4) *$L|K$ is generically ϕ-normal.*

(5) *$L|K$ is ϕ-normal with respect to all ϕ-pfield extensions of K.*

Some remarks on the conditions: Condition (1) is quite basic and ensures that we will find ourselves in a Noetherian situation for most of the time. Since we want to study difference algebraic elements it seems reasonable.

Condition (2) is more of a technical nature and is always satisfied if L^ϕ is algebraically closed and in a lot of other situations (see Lemma 1.6.5). Maybe it is not strictly necessary but anyway it simplifies the technicalities in the proofs which are already complicated enough, especially the proof of Lemma 3.4.1.

Condition (3) can be interpreted as a smallness condition (cf. [43, Proposition 1.23, p. 17]) and its importance should not be underestimated. Still it might be possible to relax it a little bit (cf. [41]) in certain situations.

Condition (4) is the really crucial one and justifies the usage of the word "Galois" as ϕ-normality closely resembles the classical normality used in the definition of classical algebraic Galois extensions. By Lemma 3.3.9 condition (4) implies that every ϕ-Galois extension is ϕ-separable which is a condition of "technical importance".

I believe that condition (4) implies condition (5) but as of this writing this is still conjectural (cf. Section 3.12). However one can show (Proposition 3.3.13) that in characteristic zero ϕ-separability and condition (5) imply condition (4). One can not hope that (5) implies (4) in general because (5) does not take into account nilpotent elements. Thus (4) is the "correct normality condition". As said it would be nice if condition (5) could be removed. By Lemma 3.3.7 condition (5) is equivalent to $k(\mathfrak{p}) = Lk(\mathfrak{p})^\phi$ for every ϕ-prime ideal $\mathfrak{p}$ of $L \otimes_K L$.

Of course conditions (4) and (5) are very similar to the notion of "strong normality" which was originally introduced by E. Kolchin for differential extensions and subsequently adapted to difference (or more general) extensions in [5], [28] and [20]. So maybe it would be more suitable to also use "strongly normal" instead of "ϕ-Galois". But this would not be consistent with the "putting a ϕ before the classical definition"-philosophy and might cause some confusion with the other literature.

Our main objective now is to prove that ϕ-Spec$(L \otimes_K L)$ is split for every ϕ-Galois extension $L|K$. This approach is motivated by Theorem 3.2.4 and will occupy us till the end of Section 3.8.

Example 3.3.11. If $L|K$ is a Picard-Vessiot extension such that L has bounded periodicity (e.g. L^ϕ is algebraically closed) then $L|K$ is ϕ-Galois.

Proof: Conditions (1), (2) and (3) are satisfied by definition. Conditions (4) and (5) are explained in Example 3.3.6. □

Example 3.3.12. Let $L = \mathbb{C}(x)$ where x is a transcendental over $\mathbb{C}$ and let $\phi : L \to L$ be defined by $\phi(f(x)) = f(x^2)$. Set $K = \mathbb{C}(x^2) \subset L$ and consider the extension $L|K$

of ϕ-fields. One easily sees that conditions (1), (2) and (3) of Definition 3.3.10 are satisfied. If R is a K-ϕ-algebra and $\sigma: L \to R$ a K-ϕ-morphism then σ is determined by the image of x. Because $\phi(\sigma(x)) = x^2$ it follows that if ϕ is injective on R then there is at most one K-ϕ-morphism from L into R. Thus $L|K$ is ϕ-normal with respect to ϕ-pfield extensions of K and also condition (5) of Definition 3.3.10 is satisfied. This also shows that there is no non-trivial K-ϕ-automorphism of $L|K$. The crux with this example is that L is not ϕ-separable over K. Indeed $x \otimes 1 - 1 \otimes x \in L \otimes_K L$ lies in the kernel of ϕ.

The above example illustrates that conditions (1), (2), (3) and (5) alone are not sufficient to guarantee the existence of a reasonable Galois theory. However if $L|K$ is ϕ-separable and $L \otimes_K L$ is reduced then condition (5) already implies condition (4):

Proposition 3.3.13. *Let $L|K$ be a ϕ-separable extension of ϕ-pfields such that $L \otimes_K L$ is reduced and L is finitely generated as total ring over K. Assume that $L|K$ is ϕ-normal with respect to ϕ-pfield extensions of K. Then $L|K$ is generically ϕ-normal.*

Proof: From Lemma 1.7.1 we know that $L \otimes_K L$ is a finite direct sum of primary rings. Because $L \otimes_K L$ is reduced it follows that $L \otimes_K L$ is a finite direct sum of integral domains. Therefore $\mathfrak{Q}(L \otimes_K L)$ is a finite direct sum of fields and by Proposition 1.7.3 we can extend ϕ to $\mathfrak{Q}(L \otimes_K L)$. Consequently $\mathfrak{Q}(L \otimes_K L)$ is a finite direct sum of ϕ-pfields, say

$$\mathfrak{Q}(L \otimes_K L) = L_1 \oplus \cdots \oplus L_n.$$

Let $M = \mathfrak{Q}(L \otimes_K L)$ and $\sigma_s, \sigma_t : L \to M$ defined by $\sigma_s(a) = a \otimes 1$ and $\sigma_t(a) = 1 \otimes a$. We have to show that $L|K$ is ϕ-normal with respect to $\sigma = (\sigma_s, \sigma_t)$. The projections $p_i : M \to L_i$ are morphisms of difference rings and by assumption $L|K$ is ϕ-normal with respect to $(p_i\sigma_s, p_i\sigma_t)$. Because the idempotent elements of M corresponding to the unit of L_i are constants of M this implies that $L|K$ is ϕ-normal with respect to σ. □

Corollary 3.3.14. *If K is inversive and of characteristic zero then one can omit condition (4) from Definition 3.3.10.*

Proof: The tensor product of two reduced algebras over a field of characteristic zero (or more generally over a perfect field) is reduced ([7, Theorem 3 (d), Chapter V, Paragraph 15, Section 5, A.V. 125]). If $K = e_1K \oplus \cdots \oplus e_tK$ then

$$L \otimes_K L = (e_1L \otimes_{e_1K} e_1L) \oplus \cdots \oplus (e_tL \otimes_{e_tK} e_tL)$$

and so $L \otimes_K L$ is reduced. By Corollary 1.5.3 we know that $L|K$ is ϕ-separable. Thus by Proposition 3.3.13, condition (5) of Definition 3.3.10 implies condition (4). □

Lemma 3.3.15. *Let $L|K$ be ϕ-Galois and $\tau : L \to L$ a K-ϕ-morphism. Then τ is an automorphism.*

Proof: We only have to show that τ is surjective. Define $\sigma_s, \sigma_t : L \to L$ by $\sigma_s = \tau$ and $\sigma_t = \mathrm{id}$. By assumptions (3) and (5) of Definition 3.3.10 we have

$$L=\sigma_t(L)\subset\sigma_s(L)L^\phi=\tau(L)K^\phi=\tau(L).$$

□

Lemma 3.3.16. *Let $L|K$ be a ϕ-Galois extension of ϕ-pfields. Then $L\otimes_K L$ is Noetherian and* RAAD *and $\phi: L\otimes_K L\to L\otimes_K L$ is injective. Moreover $X=\phi\text{-Spec}(L\otimes_K L)$ is quasi-compact.*

Proof: Because L is finitely generated as total ring over K it follows from Lemma 1.2.4 that $L\otimes_K L$ is Noetherian. We know from Lemma 3.3.9 that $L|K$ is ϕ-separable. Therefore $\phi: L\otimes_K L\to L\otimes_K L$ is injective. It thus follows from Lemma 2.2.2 that $L\otimes_K L$ is RAAD. Because $L\otimes_K L$ is Noetherian it follows from Lemma 2.1.16 that ϕ-Spec$(L\otimes_K L)$ is quasi-compact. □

3.4 The basic lemma

In the differential setting every strongly normal extension embeds into the differential algebraic closure of the base field (see [26, Section 13]). Although there is a notion of difference algebraically closed field it seems that no satisfactory notion of difference algebraic closure exists for difference *fields*. Nevertheless the following basic lemma is a difference analog of the above statement. It is also the first important step towards proving nice properties of ϕ-Galois extensions.

Lemma 3.4.1 (Basic lemma)**.** *Let $L|K$ be a ϕ-Galois extension of ϕ-pfields. Then for every $\eta\in L^n$ with $L=K(\eta)$ there exists $Q\in K[\eta]\cap L^\times$ such that $K\{\eta,\frac{1}{Q}\}\subset L$ is Noetherian and ϕ-simple.*

Before presenting the proof we give some little motivation why such a lemma could be useful. In classical algebraic geometry one has the dimension theorem which states that if K is a field and R an integral domain which is finitely generated as K-algebra then the transcendence degree of the quotient field of R equals the Krull dimension of R. In particular if R is a subring of an algebraic extension of K then R can not have a non zero prime ideal (and so must be a field). Now this kind of dimension theorem fails in the difference (and differential) setting, but still it seems natural to expect that a finitely generated ϕ-subring of a difference algebraic extension should not have much of a geometric significance, i.e. no non-trivial ϕ-prime ideals or no non-trivial difference ideals at all. Now Lemma 3.4.1 can be interpreted as an approximation to this expected nice behavior.

The key idea of the proof is a certain dimension argument but it is a somewhat lengthy way to get there. In the proof we will need a few simple observations about the transcendence degree. For clarity of the exposition we have collected them in the following subsection.

3.4.1 Transcendence degree

Let K be a field and R a K-algebra. The transcendence degree of R over K is defined as

$$\operatorname{trdeg}(R|K) = \sup\{\operatorname{trdeg}(k(\mathfrak{p})|K);\ \mathfrak{p} \in \operatorname{Spec}(R)\}.$$

Here $k(\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}} = \mathfrak{Q}(R/\mathfrak{p})$ denotes the residue field of $\mathfrak{p}$. (Since we are only interested in the case when the transcendence degree is finite we simply set $\operatorname{trdeg}(R|K) = \infty$ if the supremum is not finite.)

If $K = e_1K \oplus \cdots \oplus e_tK$ is a finite direct product of fields and R a K-algebra then the transcendence degree of R over K is defined as

$$\operatorname{trdeg}(R|K) = \sup\{\operatorname{trdeg}(e_iR|e_iK);\ i = 1, \ldots, t\}.$$

Lemma 3.4.2. *Let $K = e_1K \oplus \cdots \oplus e_tK$ be a finite direct product of fields and R a finitely generated K-algebra. Then*

$$\operatorname{trdeg}(R|K) = \dim(R)$$

where $\dim(R)$ *denotes the Krull dimension of R.*

Proof: First we assume that K is a field. If S is an integral domain and finitely generated as K-algebra then $\operatorname{trdeg}(\mathfrak{Q}(S)|K) = \dim(S)$ ([12, Theorem A, Section 13.1, p. 286]). Therefore $\operatorname{trdeg}(k(\mathfrak{p})|K) = \dim(R/\mathfrak{p})$ for every prime ideal of R. Consequently

$$\operatorname{trdeg}(R|K) = \sup\{\dim(R/\mathfrak{p});\ \mathfrak{p} \in \operatorname{Spec}(R)\} = \dim(R).$$

Now we treat the general case. Because $R = e_1R \oplus \cdots \oplus e_tR$ every (minimal) prime ideal of R contains all but one of the idempotents $e_1, \ldots, e_t$. Therefore

$$\dim(R) = \sup\{\dim(e_iR);\ i = 1, \ldots, t\}$$

Since e_iR is finitely generated as e_iK-algebra the first case yields

$$\dim(e_iR) = \operatorname{trdeg}(e_iR|e_iK)$$

and we are done. □

Lemma 3.4.3. *Let $R \subset S$ be an inclusion of K-algebras where $K = e_1K \oplus \cdots \oplus e_tK$ is a finite direct product of fields. Then* $\operatorname{trdeg}(R|K) \leq \operatorname{trdeg}(S|K)$.

Proof: As $e_iK \subset e_iR \subset e_iS$ we immediately reduce to the case that K is a field. If $\mathfrak{p} \subset \mathfrak{p}'$ is an inclusion of prime ideals of R then we have a natural map $R/\mathfrak{p} \to R/\mathfrak{p}'$. Thus if the images of some elements of R in $R/\mathfrak{p}'$ are algebraically independent over K their images in $R/\mathfrak{p}$ must also be algebraically independent over K. That is $\operatorname{trdeg}(k(\mathfrak{p})|K) \geq \operatorname{trdeg}(k(\mathfrak{p}')|K)$. Therefore it suffices to take the supremum over all minimal prime ideals in the definition of the transcendence degree.

If $\mathfrak{p}$ is a minimal prime ideal of R then by [8, Proposition 16, Chapter II, Paragraph 2.6, p. 74] there exists a (minimal) prime ideal $\widetilde{\mathfrak{p}}$ of S with $\widetilde{\mathfrak{p}} \cap R = \mathfrak{p}$. This gives rise to an inclusion $k(\mathfrak{p}) \subset k(\widetilde{\mathfrak{p}'})$ of residue fields and thus $\operatorname{trdeg}(k(\mathfrak{p})|K) \leq \operatorname{trdeg}(k(\widetilde{\mathfrak{p}})|K)$. Hence $\operatorname{trdeg}(R|K) \leq \operatorname{trdeg}(S|K)$. □

Lemma 3.4.4. *Let $K = e_1K \oplus \cdots \oplus e_tK$ be a finite direct product of fields and R a K-algebra. Let $a_1, \ldots, a_n \in R$ and $S \subset R$ a subset such that every element of S is integral over K. Then*

$$\operatorname{trdeg}(K(a_1, \ldots, a_n, S)|K) = \operatorname{trdeg}(K[a_1, \ldots, a_n]|K).$$

Proof: As

$$e_i(K(a_1, \ldots, a_n, S)) = (e_iK)(e_ia_1, \ldots, e_ia_n, e_iS) \subset e_iR$$

we can reduce to the case that K is a field.

Let $\mathfrak{p} \subset K(a_1, \ldots, a_n, S)$ be a prime ideal and set $\mathfrak{p}' = \mathfrak{p} \cap K[a_1, \ldots, a_n]$. We obtain an inclusion of residue fields $k(\mathfrak{p}') \subset k(\mathfrak{p})$. We see that $k(\mathfrak{p}')$ is generated by the images of $a_1, \ldots, a_n$ as a field over K and $k(\mathfrak{p})$ is generated by the images of the a_j's and the elements of S as a field over K. But the image of an element of S is algebraic over K by assumption. Therefore $\operatorname{trdeg}(k(\mathfrak{p}')|K) = \operatorname{trdeg}(k(\mathfrak{p})|K)$ and consequently

$$\operatorname{trdeg}(K(a_1, \ldots, a_n, S)|K) \leq \operatorname{trdeg}(K[a_1, \ldots, a_n]|K).$$

The reverse inequality follows from Lemma 3.4.3. □

3.4.2 Proof of the basic lemma

Because $L|K$ is generically ϕ-normal there is a ϕ-over ring M of $L \otimes_K L$ such that $K(L \otimes_K L) = M$ and $\sigma(L) \subset LM^\phi$ where $\sigma : L \to M$ is given by $\sigma(a) = 1 \otimes a$.

Claim 1: As the first step we will show that we can assume without loss of generality that also $L \subset M^\phi \sigma(L)$.

Let $S = \{s \in L \otimes_K L;\ s \in M^\times\}$. Then S is a multiplicatively closed and ϕ-stable subset of $L \otimes_K L$ and M can be identified with $S^{-1}(L \otimes_K L)$. The twist map $T : L \otimes_K L \to L \otimes_K L$ with $T(a \otimes b) = b \otimes a$ is a K-ϕ-automorphism and so $T(S)$ is a multiplicatively closed ϕ-stable subset of $L \otimes_K L$. Therefore the same holds for

$$S' = \{st;\ s \in S,\ t \in T(S)\}.$$

Because S consists of non zero divisors also S' consists of non zero divisors and consequently we obtain an inclusion of $L \otimes_K L$ in $M' = S'^{-1}(L \otimes_K L)$. Because S' is stable under the twist, T extends to an automorphism of M'. As $M \subset M'$ we have $M^\phi \subset M'^\phi$. We know $\sigma(L) \subset LM^\phi$ where LM^ϕ is formed inside M, this is clearly contained in LM'^ϕ which is formed inside M'. Therefore $\sigma(L) \subset LM'^\phi$. Applying the twist to this formula gives $L \subset M'^\phi \sigma(L)$. This finishes the first step and from now on we will assume $L \subset M^\phi \sigma(L)$.

Because $L = K(\eta)$ we may write for $i = 1, \ldots, n$

$$\phi(\eta_i) = \frac{P_i}{Q'}$$

where $P_i \in K[\eta]$ and $Q' \in K[\eta] \cap L^\times$. Set $\eta_{n+1} = \frac{1}{Q'} \in L$ and $\widehat{\eta} = (\eta_1, \dots, \eta_{n+1})$. We note that by Corollary 1.3.3, the ring $K\{\widehat{\eta}\}$ is Noetherian.

Because $\sigma(L) \subset LM^\phi$ we may write

$$\sigma(\eta_i) = \frac{A_i}{B_i}$$

for $i = 1, \dots, n+1$ with $A_i \in L \cdot M^\phi$ and $B_i \in (L \cdot M^\phi) \cap M^\times$. Since $L = K(\eta)$ we may assume $A_i, B_i \in K[\eta] \cdot M^\phi$. Then, after multiplying with appropriate factors we may indeed assume

$$\sigma(\eta_i) = \frac{A_i}{B}$$

for $A_i \in K[\eta] \cdot M^\phi$ and $B \in (K[\eta] \cdot M^\phi) \cap M^\times$.

Similarly, because $L \subset M^\phi \sigma(L)$ we may write

$$\eta_i = \frac{A'_i}{B'}$$

for $i = 1, \dots, n+1$ with $A'_i \in M^\phi \cdot \sigma(L)$ and $B' \in (M^\phi \cdot \sigma(L)) \cap M^\times$. We have

$$A_i = \sum_j a_{ij} c_{ij} \qquad\qquad B = \sum_j b_j c_j$$

$$A'_i = \sum_j c'_{ij} a'_{ij} \qquad\qquad B' = \sum_j c'_j b'_j$$

with $c_{ij}, c_j, c'_{ij}, c'_j \in M^\phi$, $a_{ij}, b_j \in K[\eta]$ and $a'_{ij}, b'_j \in \sigma(L)$.

We set $C = L^\phi = K^\phi$ and $D = C[c_{ij}, c_j, c'_{ij}, c'_j] \subset M^\phi$. By Lemma 1.6.6 there exists $N \geq 1$ such that $\phi^{-N}(\mathfrak{q}) = \mathfrak{q}$ for all $\mathfrak{q} \in \phi$-Spec$(D \cdot \sigma(L))$ because $D \cdot \sigma(L) = D \otimes_C \sigma(L)$ by Lemma 1.1.6 and L has bounded periodicity by assumption. As

$$B \in K[\eta] \cdot D \subset (D \cdot \sigma(L))_{B'}$$

there is $B'' \in D \cdot \sigma(L)$ and $m \geq 0$ such that $B = \frac{B''}{B'^m}$. Because $B, B' \in M^\times$ also $B'' \in M^\times$. Set

$$\widetilde{B} = B'B''\phi(B'B'') \cdots \phi^{N-1}(B'B'') \in (D \cdot \sigma(L)) \cap M^\times.$$

Multiplying the equations $\eta_i = \frac{A'_i}{B'}$ with appropriate factors yields for $i = 1, \dots, n+1$

$$\eta_i = \frac{\widetilde{A}_i}{\widetilde{B}}$$

with $\widetilde{A}_i \in D \cdot \sigma(L)$. We have $K[\widehat{\eta}] \subset (D \cdot \sigma(L))_{\widetilde{B}}$ and therefore $K\{\widehat{\eta}\} \subset (D \cdot \sigma(L))_{\langle \phi, \widetilde{B} \rangle}$ and $K\{\widehat{\eta}\} \cdot \sigma(L) \subset (D \cdot \sigma(L))_{\langle \phi, \widetilde{B} \rangle}$.

As $M = K(L \otimes_K L)$ and $L = K(\eta)$ we can find $E_{ij}, E'_{ij}, E_j, E'_j \in K[\eta] \cdot \sigma(L)$ and $F \in (K[\eta] \cdot \sigma(L)) \cap M^\times$ such that

$$\begin{aligned} c_{ij} &= \frac{E_{ij}}{F} & \qquad c_j &= \frac{E_j}{F} \\ c'_{ij} &= \frac{E'_{ij}}{F} & \qquad c'_j &= \frac{E'_j}{F}. \end{aligned}$$

It follows

$$D \cdot \sigma(L) \subset (K[\eta] \cdot \sigma(L))_F \subset (K\{\widehat{\eta}\} \cdot \sigma(L))_F.$$

Summarily we have the following inclusions of rings:

$$\begin{tikzcd} & D \cdot \sigma(L) \arrow[dl, hook] \arrow[dr, hook] & \\ (D \cdot \sigma(L))_{\langle \phi, \widetilde{B} \rangle} & & (K\{\widehat{\eta}\} \cdot \sigma(L))_F \\ & K\{\widehat{\eta}\} \cdot \sigma(L) \arrow[ul, hook] \arrow[ur, hook] & \\ & K\{\widehat{\eta}\} \arrow[u, hook] & \end{tikzcd}$$

As $\widetilde{B} \in D \cdot \sigma(L) \subset (K\{\widehat{\eta}\} \cdot \sigma(L))_F$ there is $G \in K\{\widehat{\eta}\} \cdot \sigma(L)$ and $k \geq 1$ such that $\widetilde{B} = \frac{G}{F^k}$.

Claim 2: For all $\mathfrak{q} \in \phi$-Spec$(K\{\widehat{\eta}\} \cdot \sigma(L))$ with $GF \notin \mathfrak{q}$. The ideal generated by $\mathfrak{q}$ in $(D \cdot \sigma(L))_{\langle \phi, \widetilde{B} \rangle}$ is proper.

Let $\mathfrak{q} \subset K\{\widehat{\eta}\} \cdot \sigma(L)$ be prime with $\phi^{-d}(\mathfrak{q}) = \mathfrak{q}$ and $GF \notin \mathfrak{q}$. Because $F \notin \mathfrak{q}$ the ideal $\mathfrak{q}_1$ generated by $\mathfrak{q}$ in $(K\{\widehat{\eta}\} \cdot \sigma(L))_{\langle \phi^d, F \rangle}$ is a prime ideal with $\phi^{-d}(\mathfrak{q}_1) = \mathfrak{q}_1$. As $D \cdot \sigma(L) \subset K\{\widehat{\eta}\} \cdot \sigma(L)_{\langle \phi^d, F \rangle}$ is an inclusion of ϕ^d-rings the ideal $\mathfrak{q}_2 = (D \cdot \sigma(L)) \cap \mathfrak{q}_1$ is a prime ideal of $D \cdot \sigma(L)$ with $\phi^{-d}(\mathfrak{q}) = \mathfrak{q}$.

Suppose $\widetilde{B} \in \mathfrak{q}_2$. But then $\widetilde{B} = \frac{G}{F^k} \in \mathfrak{q}_1$ which implies the contradictory $G \in \mathfrak{q}$. Thus $\widetilde{B} \notin \mathfrak{q}_2$ and by construction of $\widetilde{B}$ and Lemma 1.6.7 we obtain $\langle \phi, \widetilde{B} \rangle \cap \mathfrak{q} = \emptyset$. Hence the ideal $\mathfrak{q}_3$ generated by $\mathfrak{q}_2$ in $(D \cdot \sigma(L)_{\langle \phi, \widetilde{B} \rangle}$ is proper.

Now to prove Claim 2 it suffices to show that $\mathfrak{q} \subset \mathfrak{q}_3$. So let $a \in \mathfrak{q} \subset K\{\widehat{\eta}\} \cdot \sigma(L) \subset (D \cdot \sigma(L))_{\langle \phi, \widetilde{B} \rangle}$ and write $a = \frac{b}{\widetilde{B}^\alpha}$ with $b \in D \cdot \sigma(L)$ and $\alpha \in \mathbb{N}[\phi]$. Since $a \in \mathfrak{q}_1 \subset (K\{\widehat{\eta}\} \cdot \sigma(L))_{\langle \phi^d, F \rangle}$ and $\widetilde{B}^\alpha \in D \cdot \sigma(L) \subset (K\{\widehat{\eta}\} \cdot \sigma(L))_{\langle \phi^d, F \rangle}$ also $\widetilde{B}^\alpha a = b \in \mathfrak{q}_1$. Therefore $b \in \mathfrak{q}_2$ and so $b = \widetilde{B}^\alpha a \in \mathfrak{q}_3 \subset (D \cdot \sigma(L))_{\langle \phi, \widetilde{B} \rangle}$. But then $a = \frac{b}{\widetilde{B}^\alpha} \in \mathfrak{q}_3$ as desired. So Claim 2 is proved.

Because $GF \in M^\times$ we see that GF is a non zero divisor in $K\{\widehat{\eta}\} \cdot \sigma(L)$. As $L|K$ is ϕ-separable we can apply Proposition 1.5.12 to the inclusion

$$K\{\widehat{\eta}\} \subset K\{\widehat{\eta}\} \cdot \sigma(L) = K\{\widehat{\eta}\} \otimes_K L$$

to obtain a non zero divisor $r \in K\{\widehat{\eta}\}$ such that for every ϕ-prime ideal $\mathfrak{p}$ of $K\{\widehat{\eta}\}$ with $r \notin \mathfrak{p}$ there exists a ϕ-prime ideal $\mathfrak{p}'$ of $K\{\widehat{\eta}\} \cdot \sigma(L)$ with $GF \notin \mathfrak{p}'$ and $\mathfrak{p} \subset \mathfrak{p}'$.

By Lemma 1.2.5 there exists $u \in K\{\widehat{\eta}\}^\times$ such that $ur \in K[\eta]$. Because r is a non zero divisor of $K\{\widehat{\eta}\}$ we know from Lemma 1.1.4 that r is also a non zero divisor in L, i.e. $r \in L^\times$. Thus $Q = Q'ur \in K[\eta] \cap L^\times$.

Claim 3: We claim that $K\{\eta, \frac{1}{Q}\}$ is Noetherian and ϕ-simple.

We have for $i = 1, \dots, n$

$$\phi(\eta_i) = \frac{P_i}{Q'} = \frac{P_i ur}{Q}.$$

Thus it follows from Corollary 1.3.3 that $K\{\eta, \frac{1}{Q}\}$ is Noetherian.

It remains to prove that $K\{\eta, \frac{1}{Q}\}$ is ϕ-simple. Because $K\{\eta, \frac{1}{Q}\}$ is Noetherian we know from Corollary 1.4.9 that $K\{\eta, \frac{1}{Q}\}$ is ϕ-simple if and only if $K\{\eta, \frac{1}{Q}\}$ has no non-zero ϕ-prime ideals.

Assume $\mathfrak{p} \subset K\{\eta, \frac{1}{Q}\}$ is a non-zero ϕ-prime ideal. As

$$\frac{1}{Q'} = \frac{ur}{Q} \in K\left\{\eta, \frac{1}{Q}\right\}$$

we have $K\{\widehat{\eta}\} \subset K\{\eta, \frac{1}{Q}\}$. Because $\mathfrak{p}$ is generated by $\mathfrak{p} \cap K[\eta]$ (Corollary 1.2.6) we see that $\mathfrak{p} \cap K\{\widehat{\eta}\}$ is a non-zero ϕ-prime ideal of $K\{\widehat{\eta}\}$. As $Q'ur = Q \notin \mathfrak{p}$ we must have $r \notin \mathfrak{p}$.

Therefore to show that $K\{\eta, \frac{1}{Q}\}$ is ϕ-simple it suffices to show that every non-zero ϕ-prime ideal of $K\{\widehat{\eta}\}$ contains r. So suppose that $\mathfrak{p}$ is a ϕ-prime ideal of $K\{\widehat{\eta}\}$ with $r \notin \mathfrak{p}$. We have to show that $\mathfrak{p}$ is zero.

By construction of r there exists a ϕ-prime ideal $\mathfrak{p}'$ of $K\{\widehat{\eta}\} \cdot \sigma(L)$ with $\mathfrak{p} \subset \mathfrak{p}'$ and $GF \notin \mathfrak{p}'$. Let $\mathfrak{q}' \subset K\{\widehat{\eta}\} \cdot \sigma(L)$ be a prime ideal with $\phi^{-d'}(\mathfrak{q}') = \mathfrak{q}'$ and

$$\mathfrak{p}' = \mathfrak{q}' \cap \cdots \cap \phi^{-(d'-1)}(\mathfrak{q}').$$

Without loss of generality we may assume $GF \notin \mathfrak{q}'$.

Then by Claim 2 the ideal generated by $\mathfrak{q}'$ in $(D \cdot \sigma(L))_{\langle \phi, \widetilde{B} \rangle}$ is proper. As $\mathfrak{p} \subset \mathfrak{p}' \subset \mathfrak{q}'$ the ideal $\mathfrak{p}_1$ generated by $\mathfrak{p}$ in $(D \cdot \sigma(L))_{\langle \phi, \widetilde{B} \rangle}$ is a proper ϕ-ideal. Let

$$\mathfrak{p}_2 = \phi\text{-}\sqrt{\mathfrak{p}_1} \subset (D \cdot \sigma(L))_{\langle \phi, \widetilde{B} \rangle}.$$

Then $\mathfrak{p}_3 = \mathfrak{p}_2 \cap (D \cdot \sigma(L))$ is a proper ϕ-radical ideal of $D \cdot \sigma(L)$. Because $\widetilde{B} \notin \mathfrak{p}_3$ we have $\phi\text{-}(\widetilde{B}) \nsubseteq \mathfrak{p}_3$. By Proposition 1.4.15 this yields $\left(\phi\text{-}(\widetilde{B})\right)^\phi \nsubseteq \mathfrak{p}_3^\phi$. Thus there exists $d \in D$ with $d \in \left(\phi\text{-}(\widetilde{B})\right)^\phi \smallsetminus \mathfrak{p}_3^\phi$.

We note that D is a finitely generated C-algebra and $\mathfrak{p}_3^\phi$ a radical ideal of D. Thus by Hilbert's Nullstellensatz $\mathfrak{p}_3^\phi$ is the intersection of maximal ideals. And so, as $d \notin \mathfrak{p}_3^\phi$, there exists a maximal ideal $\mathfrak{m}$ of D containing $\mathfrak{p}_3^\phi$ with $d \notin \mathfrak{m}$.

Next we show that $\widetilde{B} \notin \mathfrak{m} \cdot \sigma(L) \subset D \cdot \sigma(L)$. So assume $\widetilde{B} \in \mathfrak{m} \cdot \sigma(L)$. Then $\phi\text{-}(\widetilde{B}) \subset \mathfrak{m} \cdot \sigma(L)$ and therefore $d \in (\phi\text{-}(\widetilde{B}))^\phi \subset (\mathfrak{m} \cdot \sigma(L))^\phi = \mathfrak{m}$; a contradiction.

By Proposition 1.4.15 we know that $\mathfrak{m} \cdot \sigma(L)$ is a ϕ-prime ideal of $D \cdot \sigma(L)$ and so there is a prime ideal $\widetilde{\mathfrak{q}}$ in $D \cdot \sigma(L)$ with $\phi^{-\widetilde{d}}(\widetilde{\mathfrak{q}}) = \widetilde{\mathfrak{q}}$ and

$$\mathfrak{m} \cdot \sigma(L) = \widetilde{\mathfrak{q}} \cap \cdots \cap \phi^{-(\widetilde{d}-1)}(\widetilde{\mathfrak{q}}).$$

Without loss of generality we may assume $\widetilde{B} \notin \widetilde{\mathfrak{q}}$. By construction of $\widetilde{B}$ and Lemma 1.6.7 we have $\langle \phi, \widetilde{B} \rangle \cap \widetilde{\mathfrak{q}} = \emptyset$. Therefore the ideal generated by $\mathfrak{m}$ in $(D \cdot \sigma(L))_{\langle \phi, \widetilde{B} \rangle}$ is a proper ϕ-ideal. We set

$$S = (D \cdot \sigma(L))_{\langle \phi, \widetilde{B} \rangle} / (D \cdot \sigma(L))_{\langle \phi, \widetilde{B} \rangle} \mathfrak{m}$$

and denote with ψ the canonical map

$$\psi : (D \cdot \sigma(L))_{\langle \phi, \widetilde{B} \rangle} \longrightarrow S.$$

Let k denote the image of D in S under ψ. By Hilbert's Nullstellensatz $k \simeq D/\mathfrak{m}$ is a finite algebraic field extension of C. In particular every element of k is integral over K. Next we want to prove

Claim 4: $\operatorname{trdeg}(K(\psi(\eta), k)|K) \geq \operatorname{trdeg}(K[\sigma(\eta)]|K)$.

In the next formula we will need that B is a unit in $(D \cdot \sigma(L))_{\langle \phi, \widetilde{B} \rangle}$. But clearly

$$\frac{1}{B} = \frac{B'^m}{B''} = \frac{B'^{m+1}\phi(B'B'') \cdots \phi^{N-1}(B'B'')}{\widetilde{B}} \in (D \cdot \sigma(L))_{\langle \phi, \widetilde{B} \rangle}.$$

We recall the inclusion of rings

$$K[\eta] \subset K\{\widehat{\eta}\} \cdot \sigma(L) \subset (D \cdot \sigma(L))_{\langle \phi, \widetilde{B} \rangle}.$$

We have for $i = 1, \ldots, n$

$$\psi(\sigma(\eta_i)) = \psi\left(\frac{A_i}{B}\right) = \frac{\psi(A_i)}{\psi(B)} = \frac{\sum_j \psi(a_{ij})\psi(c_{ij})}{\sum_j \psi(b_j)\psi(c_j)}.$$

This formula says that

$$\psi(\sigma(\eta_i)) \in K(\psi(\eta), k) \subset S$$

for $i = 1, \ldots, n$ and so $K[\psi(\sigma(\eta))] \subset K(\psi(\eta), k)$. By Lemma 3.4.3

$$\operatorname{trdeg}(K[\psi(\sigma(\eta))]|K) \leq \operatorname{trdeg}(K(\psi(\eta), k)|K).$$

As the restriction of ψ to $\sigma(L)$ is of course injective we have $\mathrm{trdeg}(K[\psi(\sigma(\eta))]|K) = \mathrm{trdeg}(K[\sigma(\eta)]|K)$ and we witness the validity of Claim 4.

By Lemma 3.4.4 we have $\mathrm{trdeg}(K[\psi(\eta)]|K) = \mathrm{trdeg}(K(\psi(\eta), k)|K)$. Putting these equations together we obtain

$$\begin{aligned}\dim\left(K[\eta]/\ker(\psi|_{K[\eta]})\right) &= \dim(\psi(K[\eta])) = \dim(K[\psi(\eta)]) = \mathrm{trdeg}(K[\psi(\eta)]|K)\\ &= \mathrm{trdeg}(K(\psi(\eta), k)|K) \geq \mathrm{trdeg}(K[\sigma(\eta)]|K)\\ &= \mathrm{trdeg}(K[\eta]|K) = \dim(K[\eta]).\end{aligned}$$

This means that $\ker(\psi|_{K[\eta]})$ is contained in a minimal prime ideal of $K[\eta]$. By construction

$$\mathfrak{p} \subset \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset (D \cdot \sigma(L))_{\langle\phi, \widetilde{B}\rangle}\mathfrak{m} = \ker(\psi).$$

I.e. $\widetilde{\mathfrak{p}} = \mathfrak{p} \cap K[\eta] \subset \ker(\psi|_{K[\eta]})$. Therefore $\widetilde{\mathfrak{p}}$ is contained in a minimal prime ideal of $K[\eta]$. But the minimal prime ideals of $K[\eta]$ are of the form $K[\eta] \cap \widetilde{\mathfrak{q}}$ where $\widetilde{\mathfrak{q}}$ is a minimal prime ideal of L ([8, Proposition 16, Chapter II, Paragraph 2.6, p. 74]). Because $\mathfrak{p}$ is generated by $\widetilde{\mathfrak{p}}$ (Corollary 1.2.6) we see that $\mathfrak{p} \subset \widetilde{\mathfrak{q}}$. If $d \geq 1$ is such that $\phi^{-d}(\widetilde{\mathfrak{q}}) = \widetilde{\mathfrak{q}}$ then, as $\mathfrak{p}$ is a ϕ-ideal, $\mathfrak{p} \subset \phi^{-1}(\widetilde{\mathfrak{q}})$, $\mathfrak{p} \subset \phi^{-2}(\widetilde{\mathfrak{q}}), \ldots$ and therefore

$$\mathfrak{p} \subset \widetilde{\mathfrak{q}} \cap \cdots \cap \phi^{-(d-1)}(\widetilde{\mathfrak{q}}) = 0.$$

Consequently $\mathfrak{p} = 0$ as desired and Claim 3 is proved. □

Corollary 3.4.5. *Let $L|K$ be a ϕ-Galois extension of ϕ-pfields. Then there exists $\eta \in L^n$ such that $L = K(\eta)$ and $K\{\eta\} \subset L$ is Noetherian and ϕ-simple.*

The proof is clear from the basic lemma. □

We note that in the Picard-Vessiot case one gets the important corollary above for free as the Picard-Vessiot ring is required to be ϕ-simple.

3.5 Generic splitting

This section essentially consists of two applications of the basic lemma.

We recall that for the time being our main goal is to prove that $\phi\text{-Spec}(L \otimes_K L)$ is split for every ϕ-Galois extension $L|K$. The following proposition states that this is generically true.

Proposition 3.5.1. *Let $L|K$ be a ϕ-Galois extension of ϕ-pfields. Then there exists a non-empty open Φ-stable subset U of $\phi\text{-Spec}(L \otimes_K L)$ which is split over L.*

Proof: By Corollary 3.4.5, there exists $\eta \in L^n$ with $L = K(\eta)$ such that $K\{\eta\} \subset L$ is ϕ-simple and Noetherian. As $L|K$ is generically ϕ-normal there exists a difference ring extension M of $L \otimes_K L$ such that $M = K(L \otimes_K L)$ and $\sigma(L) \subset LM^{\phi}$ where $\sigma : L \to M$ is given by $\sigma(a) = 1 \otimes a$. Thus we may write for $i = 1, \ldots, n$

$$\sigma(\eta_i) = \frac{A_i}{B} \tag{3.4}$$

with

$$A_i = \sum_j a_{ij} c_{ij}, \quad B = \sum_j b_j c_j \in M^{\times},\ a_{ij}, b_j \in L,\ c_{ij}, c_j \in M^{\phi}.$$

Set $D = C[c_{ij}, c_j]$. Then by Lemma 1.6.6 there exists $N \geq 1$ such that for all $\mathfrak{q} \in \phi\text{-Spec}(L \cdot D) = \phi\text{-Spec}(L \otimes_C D)$ we have $\phi^{-N}(\mathfrak{q}) = \mathfrak{q}$. Set

$$B' = B\phi(B) \cdots \phi^{N-1}(B) \in (L \cdot D) \cap M^{\times}.$$

Extending the fraction with $\phi(B) \cdots \phi^{N-1}(B)$ transforms equation (3.4) into

$$\sigma(\eta_i) = \frac{A_i'}{B'} \text{ with } A_i' \in L \cdot D.$$

This means that

$$L \cdot K[\sigma(\eta)] \subset (L \cdot D)_{B'}$$

and consequently

$$L \otimes_K K\{\eta\} = L \cdot K\{\sigma(\eta)\} \subset (L \cdot D)_{\langle \phi, B' \rangle}.$$

We may also write

$$c_{ij} = \frac{E_{ij}}{F}, \qquad c_j = \frac{E_j}{F} \tag{3.5}$$

with $E_{ij}, E_j, F \in L \otimes_K K\{\eta\}$, $F \in M^{\times}$ so that

$$L \cdot D \subset (L \otimes_K K\{\eta\})_F.$$

In fact applying ϕ^i to the equations in (3.5) gives

$$L \cdot D \subset (L \otimes_K K\{\eta\})_{\phi^i(F)}$$

for every $i \geq 0$. We set

$$X = \phi\text{-Spec}(L \otimes_K K\{\eta\}) \text{ and } Y = \phi\text{-Spec}(L \otimes_C D).$$

From Lemma 1.6.7 we know that $V = D(B')$ is an open Φ-stable subset of Y and $\langle \phi, B' \rangle \cap \mathfrak{q}$ is empty for every $\mathfrak{q} \in V$. We have a natural morphism

$$g^* : L \otimes_K K\{\eta\} \longrightarrow \mathcal{O}_Y(V)$$

of difference rings derived from the inclusion

$$L \otimes_K K\{\eta\} \subset (L \cdot D)_{\langle \phi, B' \rangle}.$$

If $a \in L \otimes_K K\{\eta\}$ then a is of the form $a = \frac{b}{B'^\alpha}$ (with $\alpha \in \mathbb{N}[\phi]$ and $b \in L \otimes_C D$) and $g^*(a)$ is simply given by

$$g^*(a)(\mathfrak{q}) = \frac{b}{B'^\alpha} \in (L \otimes_C D)_\mathfrak{q}$$

for $\mathfrak{q} \in V$. By Theorem 2.1.11 the map g^* induces a morphism

$$g : V \to X$$

of ϕ-spaces. Let

$$U = \bigcup_{i \geq 0} D(\phi^i(F)) = \{\mathfrak{q} \in X;\ \exists\, i \geq 0 :\ \phi^i(F) \notin \mathfrak{q}\}.$$

Then U is an open Φ-stable subset of X and from the inclusions

$$L \otimes_C D = L \cdot D \subset (L \otimes_K K\{\eta\})_{\phi^i(F)}$$

we obtain a morphism

$$f^* : L \otimes_C D \to \mathcal{O}_X(U)$$

of ϕ-rings. If $a \in L \otimes_C D$ then a is of the form $a = \frac{b}{\phi^i(F)^m}$ with $b \in L \otimes_K K\{\eta\}$ and on $D(\phi^i(F)) \subset U$ the function $f^*(a)$ is given by the fraction $\frac{b}{\phi^i(F)^m}$. Again by Theorem 2.1.11 we obtain a morphism

$$f : U \to Y$$

of ϕ-spaces.

We claim that $U \cap f^{-1}(V)$ is non-empty. Because

$$B' \in L \otimes_C D \subset (L \otimes_K K\{\eta\})_F$$

we can find $B'' \in L \otimes_K K\{\eta\}$ and $m \geq 1$ such that $B' = \frac{B''}{F^m}$. Because B' is unit in M also $B''F$ is a unit in M. Therefore the multiplicatively closed ϕ-stable subset $\langle \phi, B''F \rangle$ of $L \otimes_K K\{\eta\}$ has empty intersection with the zero ideal. From the obvious application of Zorn's Lemma it follows that there exists a maximal element $\mathfrak{p}$ in the set of all ϕ-ideals of $L \otimes_K K\{\eta\}$ which do not meet $\langle \phi, B''F \rangle$. Since $K\{\eta\}$ is Noetherian we know (cf. Lemma 1.2.4) that also $L \otimes_K K\{\eta\}$ is Noetherian and so we can use Proposition 1.4.2 to conclude that $\mathfrak{p}$ is a ϕ-prime ideal. This implies that there exists a $\mathfrak{q} \in \phi\text{-Spec}(L \otimes_K K\{\eta\})$ such that $B''F \notin \mathfrak{q}$, in particular $F \notin \mathfrak{q}$ so that $\mathfrak{q} \in U$. Now $f(\mathfrak{q})$ is the inverse image of the maximal ideal of $(L \otimes_K K\{\eta\})_\mathfrak{q}$ under

$$L \otimes_C D \hookrightarrow (L \otimes_K K\{\eta\})_F \to (L \otimes_K K\{\eta\})_\mathfrak{q}.$$

So if $B' = \frac{B''}{F^m}$ would lie in $f(\mathfrak{q})$ then B'' would lie in $\mathfrak{q}$ - which is not the case. Therefore $B' \notin f(\mathfrak{q})$, i.e. $\mathfrak{q} \in f^{-1}(D(B')) = f^{-1}(V)$. Thus $\mathfrak{q} \in U \cap f^{-1}(V) \neq \emptyset$.

Next we will show that

$$\begin{tikzcd} U \cap f^{-1}(V) \arrow[r, "f"] & V \arrow[r, "g"] & X \end{tikzcd}$$

is simply the inclusion mapping. By Theorem 2.1.11 it suffices to see that the induced mapping

$$\psi : L \otimes_K K\{\eta\} \to \mathcal{O}_X(X) \to \mathcal{O}_Y(V) \to \mathcal{O}_X(U \cap f^{-1}(V))$$

is given by $\psi(a)(\mathfrak{q}) = \frac{a}{1} \in (L \otimes_K K\{\eta\})_{\mathfrak{q}}$ for $a \in L \otimes_K K\{\eta\}$ and $\mathfrak{q} \in U \cap f^{-1}(V)$. By Theorem 2.1.11 the image of $a \in L \otimes_K K\{\eta\}$ in $\mathcal{O}_Y(V)$ equals $g^*(a)$ and $g^*(a)$ is the function that assigns to every $\mathfrak{q}' \in V$ the image of a under

$$L \otimes_K K\{\eta\} \subset (L \otimes_C D)_{\langle \phi, B' \rangle} \to (L \otimes_C D)_{\mathfrak{q}'}.$$

If $\mathfrak{q} \in U \cap f^{-1}(V)$ then $\phi^i(F) \notin \mathfrak{q}$ for some $i \geq 0$ and $f^*(r)(\mathfrak{q}) = \nu(r)$ where $r \in L \otimes_C D$ and

$$\nu : L \otimes_C D \subset (L \otimes_K K\{\eta\})_{\phi^i(F)} \to (L \otimes_K K\{\eta\})_{\mathfrak{q}} = \mathcal{O}_{X,\mathfrak{q}}.$$

By definition $f(\mathfrak{q}) = \nu^{-1}(\mathfrak{m}_{\mathfrak{q}})$. Because $f(\mathfrak{q}) \in V = D(B')$ we see that ν extends to

$$\nu' : (L \otimes_C D)_{\langle \phi, B' \rangle} \to (L \otimes_K K\{\eta\})_{\mathfrak{q}}$$

and by definition $\psi(a)(\mathfrak{q})$ is the image of a under

$$L \otimes_K K\{\eta\} \hookrightarrow (L \otimes_C D)_{\langle \phi, B' \rangle} \xrightarrow{\nu'} (L \otimes_K K\{\eta\})_{\mathfrak{q}}$$

which is of course just $\frac{a}{1} \in (L \otimes_K K\{\eta\})_{\mathfrak{q}}$ as claimed.

Similarly, one sees that

$$\begin{tikzcd} V \cap g^{-1}(U) \arrow[r, "g"] & U \arrow[r, "f"] & Y \end{tikzcd}$$

is the inclusion map. For the sake of completeness we give the details: Again it suffices to see that

$$\psi : L \otimes_C D \to \mathcal{O}_Y(Y) \to \mathcal{O}_X(U) \to \mathcal{O}_Y(V \cap g^{-1}(U))$$

is given by $\psi(a)(\mathfrak{q}) = \frac{a}{1} \in (L \otimes_C D)_{\mathfrak{q}}$ for $a \in L \otimes_C D$ and $\mathfrak{q} \in V \cap g^{-1}(U)$.

So let $\mathfrak{q} \in V \cap g^{-1}(U)$ and

$$\nu : L \otimes_K K\{\eta\} \subset (L \cdot D)_{\langle \phi, B' \rangle} \to (L \cdot D)_{\mathfrak{q}} = \mathcal{O}_{Y,\mathfrak{q}}.$$

Because $g(\mathfrak{q}) = \nu^{-1}(\mathfrak{m}_{\mathfrak{q}}) \in U$ there is an $i \geq 0$ such that $\phi^i(F) \notin g(\mathfrak{q})$ and so ν extends to

$$\nu' : (L \otimes_K K\{\eta\})_{\phi^i(F)} \to (L \cdot D)_{\mathfrak{q}}.$$

Now $\psi(a)(\mathfrak{q})$ is the image of $a \in L \cdot D \subset (L \otimes_K K\{\eta\})_{\phi^i(F)}$ under ν' which equals $\frac{a}{1} \in (L \cdot D)_{\mathfrak{q}}$.

Altogether we see that $V \cap g^{-1}(U)$ and $U \cap f^{-1}(V)$ are isomorphic as ϕ-spaces over L. Because $Y = L \times_C \operatorname{Spec}(D)$ is split it follows from Lemma 2.5.4 that also the open Φ-stable subset $V \cap g^{-1}(U) \subset Y$ is split. Consequently $U \cap f^{-1}(V)$ is a non-empty split open Φ-stable subset of X. Finally by Example 2.1.8 we have ϕ-Spec$(K\{\eta\}) \simeq$ ϕ-Spec(L) and so $X \simeq \phi$-Spec$(L \otimes_K L)$. □

Proposition 3.5.2. *Let $L|K$ be a ϕ-Galois extension of ϕ-pfields. Let $\mathfrak{a}$ be a ϕ-ideal of $R = L \otimes_K L$, $r \in R$ and $\mathfrak{p}$ a maximal element of the set*

$$\{\mathfrak{p} \subset R \ \phi\text{-}prime; \ \mathfrak{a} \subset \mathfrak{p}, \ r \notin \mathfrak{p}\}.$$

Let $k(\mathfrak{p}) = \mathfrak{Q}(R/\mathfrak{p})$. Then $k(\mathfrak{p})^\phi$ is an algebraic extension of $C = L^\phi = K^\phi$.

Proof: By Corollary 3.4.5 there exists $\eta \in L^n$ such that $K\{\eta\}$ is ϕ-simple and $K(\eta) = L$. Set $M = k(\mathfrak{p})$ and $\sigma : L \to M$, $a \mapsto \frac{1 \otimes a}{1}$. Because $L|K$ is ϕ-normal with respect to σ we may write for $i = 1, \ldots, n$

$$\sigma(\eta_i) = \frac{A_i}{B} \tag{3.6}$$

where $A_i, B \in L \cdot M^\phi$, $B \in M^\times$ and

$$A_i = \sum_j a_{ij} c_{ij} \qquad\qquad B = \sum_j b_j c_j$$

with $a_{ij}, b_j \in L$ and $c_{ij}, c_j \in M^\phi$.

Suppose for a contradiction that $M^\phi|C$ is not algebraic. So we can find $d \in M^\phi$ transcendental over C. Set $D = C[c_{ij}, c_j, d]$.

Now by Lemma 1.6.6 there exists $N \geq 1$ such that for all $\mathfrak{q} \in \phi\text{-Spec}(L \cdot D) = \phi\text{-Spec}(L \otimes_C D)$ we have $\phi^{-N}(\mathfrak{q}) = \mathfrak{q}$. Set

$$B' = B\phi(B) \cdots \phi^{N-1}(B) \in (L \cdot D) \cap M^\times.$$

Extending the fraction with $\phi(B) \cdots \phi^{N-1}(B)$ transforms equation (3.6) into

$$\sigma(\eta_i) = \frac{A_i'}{B'} \text{ with } A_i' \in L \cdot D.$$

This means that

$$L \cdot K[\sigma(\eta)] \subset (L \cdot D)_{B'}$$

and consequently

$$L \cdot K\{\sigma(\eta)\} \subset (L \cdot D)_{\langle \phi, B' \rangle}.$$

Let $\overline{r}$ denote the image of r under the canonical map $L \otimes_K L \to M$. Because $K(\eta) = L$ there exists $u \in (L \cdot \sigma(L))^\times$ such that

$$u\overline{r} \in L \cdot K[\sigma(\eta)] \subset (L \cdot D)_{B'}.$$

Thus there exists $m \geq 0$ such that $B'^m u\overline{r} \in L \cdot D$. Set $b = B'^{m+1} u\overline{r} \in L \cdot D$. By Proposition 1.4.15 the ideal $\phi\text{-}\sqrt{b} \subset L \cdot D$ is generated by $\phi\text{-}\sqrt{b} \cap D$. Since $r \notin \mathfrak{p}$, the element b is not equal to zero and so we can find a non-zero element $c \in (\phi\text{-}\sqrt{b})^\phi \subset D$.

Since D is a reduced, finitely generated C-algebra, the intersection of all maximal ideals of D is the zero ideal. Consequently there exists a maximal ideal $\mathfrak{m}$ of D with $c \notin \mathfrak{m}$.

By Proposition 1.4.15, the ideal $(L \cdot D)\mathfrak{m}$ generated by $\mathfrak{m}$ in $L \cdot D$ is ϕ-prime. We claim that $b \notin (L \cdot D)\mathfrak{m}$. Suppose the contrary. Then $\phi\text{-}\sqrt{b} \subset (L \cdot D)\mathfrak{m}$ and so

$$c \in (\phi\text{-}\sqrt{b})^{\phi} \subset ((L \cdot D)\mathfrak{m})^{\phi} = \mathfrak{m}$$

which contradicts $c \notin \mathfrak{m}$. So $b \notin (L \cdot D)\mathfrak{m}$.

Because $B'(B'^m u\overline{r}) = b \notin (L \cdot D)\mathfrak{m}$ we have $B' \notin (L \cdot D)\mathfrak{m}$ and thus by construction of B' and Lemma 1.6.7 we have $\langle \phi, B' \rangle \cap (L \cdot D)\mathfrak{m} = \emptyset$. Therefore the ideal $(L \cdot D)_{\langle \phi, B' \rangle}\mathfrak{m}$ generated by $\mathfrak{m}$ in $(L \cdot D)_{\langle \phi, B' \rangle}$ is ϕ-prime and

$$M' = \mathfrak{Q}\left((L \cdot D)_{\langle \phi, B' \rangle}/(L \cdot D)_{\langle \phi, B' \rangle}\mathfrak{m}\right)$$

is a ϕ-pfield. Let

$$\psi : L \cdot K\{\sigma(\eta)\} \subset (L \cdot D)_{\langle \phi, B' \rangle} \longrightarrow M'$$

denote the canonical map. Because $K\{\sigma(\eta)\}$ is ϕ-simple the restriction of ψ to $K\{\sigma(\eta)\}$ is injective. It follows from Lemma 1.3.4 that ψ extends uniquely to $\psi : L \cdot \sigma(L) \to M'$. Now let $\mathfrak{p}'$ denote the kernel of the map

$$L \otimes_K L \to M', \; a \otimes b \mapsto \psi(a\sigma(b)).$$

We claim that $\mathfrak{p}'$ is a ϕ-prime ideal of $L \otimes_K L$ with $r \notin \mathfrak{p}'$ which properly contains $\mathfrak{p}$. (This claim contradicts the maximality of $\mathfrak{p}$ and thus will finish the proof.)

From Proposition 1.4.2 we know that $\mathfrak{p}'$ is a ϕ-prime ideal and it is obvious that $\mathfrak{p}'$ contains $\mathfrak{p}$. Suppose $r \in \mathfrak{p}'$, i.e. $\overline{r} \in \ker(\psi)$. Then also $u\overline{r} \in L \cdot K\{\sigma(\eta)\} \subset (L \cdot D)_{\langle \phi, B' \rangle}$ lies in the kernel of ψ. In particular $u\overline{r}$ and thus also $b = B'^{m+1}u\overline{r}$ lie in the kernel of $(L \cdot D)_{\langle \phi, B' \rangle} \to M'$. This yields the contradiction $b \in (L \cdot D)\mathfrak{m} : \langle \phi, B' \rangle = (L \cdot D)\mathfrak{m}$.

It remains to see that the inclusion $\mathfrak{p} \subset \mathfrak{p}'$ is proper. If $\mathfrak{m}$ was the zero ideal of D then D would be a field. But, as D is finitely generated as C-algebra and contains the transcendental element d, this is not possible. So we can find a non-zero element $e \in \mathfrak{m} \subset D \subset M = L\sigma(L)$. Thus e is of the form $e = \frac{E}{F}$ with $E, F \in L \cdot K\{\sigma(\eta)\} \subset (L \cdot D)_{\langle \phi, B' \rangle}$. Since e lies in the kernel of $(L \cdot D)_{\langle \phi, B' \rangle} \to M'$ also $E = eF \in (L \cdot D)_{\langle \phi, B' \rangle}$ lies in the kernel of $(L \cdot D)_{\langle \phi, B' \rangle} \to M'$ and so E lies in the kernel of ψ. So if $E = \sum a_i\sigma(b_i)$ with $a_i, b_i \in L$ then $\sum a_i \otimes b_i$ lies in $\mathfrak{p}'$ but not in $\mathfrak{p}$ because e is non-zero. Therefore $\mathfrak{p} \subsetneqq \mathfrak{p}'$. □

3.6 The main theorem with algebraically closed constants

For the convenience of the reader who only cares for algebraically closed constants we present in this section a proof of the main theorem, namely that ϕ-Spec$(L \otimes_K L)$ is split for every ϕ-Galois extension $L|K$, under the assumption that the constants are algebraically closed. This assumption greatly simplifies the argument. The reader ignorant towards arbitrary constants can then safely skip sections 3.7 and 3.8.

Throughout this section we assume that $L|K$ is a ϕ-Galois extension with algebraically closed field of constants $C = K^\phi = L^\phi$.

Lemma 3.6.1. *Let $L|K$ be ϕ-Galois with algebraically closed constants. Let $\mathfrak{a}$ be a ϕ-ideal of $R = L \otimes_K L$, $r \in R$ and $\mathfrak{p}$ a maximal element of the set*

$$\{\mathfrak{p} \subset R \ \phi\text{-}prime;\ \mathfrak{a} \subset \mathfrak{p},\ r \notin \mathfrak{p}\}.$$

Then the maps

$$\sigma_s : L \to R/\mathfrak{p},\ a \mapsto \overline{a \otimes 1}$$

and

$$\sigma_t : L \to R/\mathfrak{p},\ a \mapsto \overline{1 \otimes a}$$

are isomorphisms and $\sigma = \sigma_s^{-1}\sigma_t$ is a K-ϕ-automorphism of L. Moreover, as an ideal $\mathfrak{p}$ is generated by the elements of the form $\sigma(a) \otimes 1 - 1 \otimes a$ with $a \in L$.

Proof: By Proposition 3.5.2 we have $k(\mathfrak{p})^\phi = C = L^\phi \subset L$. Because $L|K$ is ϕ-normal with respect to ϕ-pfield extensions of K we have $k(\mathfrak{p}) = Lk(\mathfrak{p})^\phi = L$. This shows that $L \to R/\mathfrak{p},\ a \mapsto \overline{a \otimes 1}$ is surjective and thus an isomorphism.

We recall that the twist

$$T : L \otimes_K L \to L \otimes_K L,\ a \otimes b \mapsto b \otimes a$$

is a K-ϕ-automorphism. We have a commutative diagram

$$\begin{tikzcd}
 & L \otimes_K L/T^{-1}(\mathfrak{p}) \arrow[dd, "\overline{T}"] \\
L \arrow[ur, "\tau_s"] \arrow[dr, "\sigma_t"'] & \\
 & L \otimes_K L/\mathfrak{p}
\end{tikzcd}$$

where τ_s is derived from the inclusion into the first factor and $\overline{T}$ is induced from the twist. The ϕ-prime ideal $T^{-1}(\mathfrak{p})$ is maximal in the set

$$\{\mathfrak{p}' \subset R \ \phi\text{-prime};\ T^{-1}(\mathfrak{a}) \subset \mathfrak{p}',\ T^{-1}(r) \notin \mathfrak{p}'\}$$

and so, by the above consideration τ_s is an isomorphism. Since also $\overline{T}$ is an isomorphism we conclude that σ_t is an isomorphism.

As $\overline{a \otimes b} = \sigma_s(a)\sigma_t(b) \in R/\mathfrak{p}$ we see that $\overline{\sigma(a) \otimes 1 - 1 \otimes a} = \sigma_s(\sigma(a)) - \sigma_t(a) = 0$. Conversely, if $s = \sum a_i \otimes b_i$ lies in $\mathfrak{p}$ then $\sum \sigma_s(a_i)\sigma_t(b_i) = 0$ and so $\sum a_i\sigma(b_i) = 0$. Therefore

$$\begin{aligned} s &= \sum a_i \otimes b_i = -\sum a_i \otimes 1(\sigma(b_i) \otimes 1 - 1 \otimes b_i) + \sum a_i\sigma(b_i) \otimes 1 \\ &= -\sum a_i \otimes 1(\sigma(b_i) \otimes 1 - 1 \otimes b_i). \end{aligned}$$

□

Theorem 3.6.2 (Homogeneity)**.** *Let $L|K$ be ϕ-Galois with algebraically closed constants. Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be two ϕ-maximal ideals of $L \otimes_K L$. Then there exists an L-ϕ-automorphism $\psi : L \otimes_K L \to L \otimes_K L$ with $\psi^{-1}(\mathfrak{p}_1) = \mathfrak{p}_2$. (Here we consider $L \otimes_K L$ as L-algebra via the first factor.) Indeed ψ can be chosen of the form $\psi(a \otimes b) = a \otimes \sigma(b)$ for some K-ϕ-automorphism σ of L.*

Proof: By Lemma 3.6.1 (with $\mathfrak{a} = 0$ and $r = 1$) there exists for $i = 1, 2$ a K-ϕ-automorphism σ_i of L such that $\mathfrak{p}_i$ is generated by the elements of the form $\sigma_i(a) \otimes 1 - 1 \otimes a$. If we define

$$\psi : L \otimes_K L \to L \otimes_K L, \quad a \otimes b \mapsto a \otimes \sigma_1^{-1}(\sigma_2(b))$$

then

$$\psi(\sigma_2(a) \otimes 1 - 1 \otimes a) = \sigma_1(\sigma_1^{-1}(\sigma_2(a))) \otimes 1 - 1 \otimes \sigma_1^{-1}(\sigma_2(a)) \in \mathfrak{p}_1$$

and we see that $\psi^{-1}(\mathfrak{p}_1) = \mathfrak{p}_2$. □

Corollary 3.6.3. *Let $L|K$ be ϕ-Galois with algebraically closed constants, $x \in X = \phi\text{-}\mathrm{Spec}(L \otimes_K L)$ and U a non-empty, open, Φ-stable subset of X. Then there exists an automorphism $f : X \to X$ of ϕ-spaces over L such that $x \in f(U)$. Indeed f can be chosen to be induced from $L \otimes_K L \to L \otimes_K L$, $a \otimes b \mapsto a \otimes \sigma(b)$ where σ is a K-ϕ-automorphism of L.*

Proof: The open Φ-stable set U is of the form $U = X \smallsetminus \mathbb{V}(\mathfrak{a})$ for some ϕ-ideal $\mathfrak{a}$. Since U is non-empty there exists $r \in \mathfrak{a}$ and a ϕ-prime ideal of $R = L \otimes_K L$ which does not contain r. Let $\mathfrak{p}_1$ be a maximal element of the set

$$\{\mathfrak{p} \subset R \ \phi\text{-prime}; \ r \notin \mathfrak{p}\}.$$

By Lemma 3.6.1 the ϕ-ring $R/\mathfrak{p}_1$ is isomorphic to L and so $\mathfrak{p}_1$ is ϕ-maximal. There is a minimal prime ideal of $\mathfrak{p}_1$ that does not contain r and thus lies in U. Since U is Φ-stable all the minimal prime ideals of $\mathfrak{p}_1$ belong to U.

Let $\mathfrak{q} \in \phi\text{-}\mathrm{Spec}(R)$ denote the prime ideal corresponding to x and $\mathfrak{p} = \mathfrak{q} \cap \cdots \cap \phi^{-(d-1)}(\mathfrak{q})$ the ϕ-prime ideal belonging to $\mathfrak{q}$. Let $\mathfrak{p}_2$ be a ϕ-maximal ϕ-ideal lying above $\mathfrak{p}$.

By Theorem 3.6.2 there exists an L-ϕ-automorphism ψ of R (of the prescribed form) with $\psi^{-1}(\mathfrak{p}_1) = \mathfrak{p}_2$. Let $\mathfrak{q}_2$ denote a minimal prime ideal of $\mathfrak{p}_2$. Then there exists a minimal prime ideal $\mathfrak{q}_1$ of $\mathfrak{p}_1$ with $\psi^{-1}(\mathfrak{q}_1) = \mathfrak{q}_2$. If f denotes the automorphism of X induced by ψ then $\mathfrak{q}_2 = f(\mathfrak{q}_1) \in f(U)$. As $\mathfrak{q} \cap \cdots \cap \phi^{-(d-1)}(\mathfrak{q}) = \mathfrak{p} \subset \mathfrak{p}_2 \subset \mathfrak{q}_2$ we have $\phi^{-i}(\mathfrak{q}) \subset \mathfrak{q}_2$ for some $i \geq 0$ and so $\phi^{-i}(\mathfrak{q}) \in f(U)$ because $\mathfrak{q}_2 \in f(U)$ and $f(U)$ is open. Since $f(U)$ is also Φ-stable we see that $\mathfrak{q} \in f(U)$. □

Theorem 3.6.4 (Main Theorem with algebraically closed constants)**.** *Let $L|K$ be ϕ-Galois with algebraically closed constants $C = K^\phi = L^\phi$. Then $X = \phi\text{-}\mathrm{Spec}(L \otimes_K L)$ is split. I. e. there exists a scheme $\mathcal{G}$ of finite type over C such that $X \simeq L \times_C \mathcal{G}$ as ϕ-spaces over L.*

Proof: By Proposition 2.5.5 it suffices to see that we can cover X with a finite number of open, Φ-stable, split subsets. By Proposition 3.5.1 we know that there exists a non-empty, open, Φ-stable, split subset of X. Using Corollary 3.6.3, we can transport it to every point of X, so that we have a covering of X with split, open, Φ-stable subsets. By Lemma 3.3.16, we know that X is quasi-compact and so a finite number will suffice. □

3.7 When the constants are not algebraically closed

Let $L|K$ be a ϕ-Galois extension of ϕ-pfields. In the previous section we established the main result, namely that ϕ-Spec$(L \otimes_K L)$ is split, under the assumption that $C = K^\phi = L^\phi$ is an algebraically closed field. More precisely the closedness of C was required for the homogeneity theorem (Theorem 3.6.2). The purpose of this and the following section is to remove the assumption that the constants are algebraically closed. The main result of this section is that ϕ-Spec$(L \otimes_K L)$ splits after a finite extension of the constants. The required descent will then be performed in the next section.

As a starting point we have the following proposition.

Proposition 3.7.1. *Let $L|K$ be a ϕ-Galois extension of ϕ-pfields with field of constants $C = K^\phi = L^\phi$ and C' an algebraic extension of C. Set $K' = L \otimes_C C'$ and $L' = L \otimes_C C'$. Then $L'|K'$ is a ϕ-Galois extension of ϕ-pfields with field of constants $L'^\phi = K'^\phi = C'$.*

Proof: We already know from Lemma 1.6.9 that $L'|K'$ is an extension of ϕ-pfields with $L'^\phi = K'^\phi = C'$ and that L' has bounded periodicity. Because L is finitely generated as total ring over K obviously also L' is finitely generated as total ring over K'.

Next we will show that $L'|K'$ is generically ϕ-normal. By assumption there exists a ϕ-ring M containing $L \otimes_K L$ such that $M = K(L \otimes_K L)$ and $\sigma_t(L) \subset \sigma_s(L)M^\phi$, where $\sigma_s, \sigma_t : L \to M$ are defined by $\sigma_s(a) = a \otimes 1$ and $\sigma_t(a) = 1 \otimes a$. Set $M' = M \otimes_C C'$. The inclusion $L \otimes_K L \hookrightarrow M$ gives rise to an inclusion $L' \otimes_{K'} L' = (L \otimes_K L) \otimes_C C' \hookrightarrow M'$. Clearly $M' = K'(L' \otimes_{K'} L')$ and also $\sigma'_t(L') \subset \sigma'_s(L')M'^\phi$.

It remains to see that $L'|K'$ is ϕ-normal with respect to all ϕ-pfield extensions of K'. So let M' be a ϕ-pfield extension of K' and $\sigma' = (\sigma'_s, \sigma'_t)$ an isomorphism of $L'|K'$ inside M'. By composing with the inclusion $L \hookrightarrow L'$ we obtain an isomorphism $\sigma = (\sigma_s, \sigma_t)$ of $L|K$ inside M'. By assumption $\sigma_t(L) \subset \sigma_s(L)M'^\phi$ and it follows that also $\sigma'_t(L') \subset \sigma'_s(L')M'^\phi$. □

Lemma 3.7.2. *Let $L|K$ be ϕ-Galois with $C = K^\phi = L^\phi$ and $\mathfrak{p} \subset L \otimes_K L$ a ϕ-maximal ideal. Then $k(\mathfrak{p})^\phi$ is a finite algebraic extension of C and*

$$k(\mathfrak{p}) = (L \otimes_K L)/\mathfrak{p} = L \otimes_C k(\mathfrak{p})^\phi.$$

Proof: It follows from Lemma 1.1.5 that $k(\mathfrak{p})^\phi = ((L \otimes_K L)/\mathfrak{p})^\phi$. Because $L|K$ is ϕ-normal with respect to ϕ-pfields we have $k(\mathfrak{p}) = Lk(\mathfrak{p})^\phi$. From Lemma 1.1.6 we know that $L \cdot k(\mathfrak{p})^\phi = L \otimes_C k(\mathfrak{p})^\phi$ and because $k(\mathfrak{p})^\phi$ is an algebraic extension of C (Proposition

3.5.2) it follows from Lemma 1.6.8 that $L \otimes_C k(\mathfrak{p})^\phi$ is a ϕ-pfield. In particular $L \otimes_C k(\mathfrak{p})^\phi$ is a total ring and so

$$k(\mathfrak{p}) = Lk(\mathfrak{p})^\phi = L \cdot k(\mathfrak{p})^\phi \subset (L \otimes_K L)/\mathfrak{p}.$$

Therefore $k(\mathfrak{p}) = (L \otimes_K L)/\mathfrak{p} = L \otimes_C k(\mathfrak{p})^\phi$.

It remains to prove that $k(\mathfrak{p})^\phi$ is finite over C. Let $\eta \in L^n$ with $L = K(\eta)$ and $\sigma = \sigma_t : L \to k(\mathfrak{p}) = \mathfrak{Q}((L \otimes_K L)/\mathfrak{p}))$, $a \mapsto \frac{\overline{1 \otimes a}}{1}$. As $k(\mathfrak{p}) = L \otimes_C k(\mathfrak{p})^\phi$ there already exists a finite extension D of C inside $k(\mathfrak{p})^\phi$ such that $\sigma(\eta_i) \in L \otimes_C D$ for $i = 1, \ldots, n$. Consequently $K\{\sigma(\eta)\} \subset L \otimes_C D$. By Lemma 1.6.8 we know that $L \otimes_C D$ is a ϕ-pfield and so it follows from Lemma 1.3.4 that $\sigma(L) \subset L \otimes_C D$. Therefore $k(\mathfrak{p}) = L \otimes_C D$. This shows that $k(\mathfrak{p})^\phi = D$ which is a finite extension of C. □

Lemma 3.7.3. *Let $L|K$ be ϕ-Galois with $C = K^\phi = L^\phi$ and C' an algebraic extension of C. Let $\mathcal{G}(C')$ denote the set of tuples $(\mathfrak{p}, \varphi)$ where $\mathfrak{p}$ is a ϕ-maximal ideal of $L \otimes_K L$ and $\varphi : k(\mathfrak{p})^\phi \to C'$ an embedding of $k(\mathfrak{p})^\phi$ into C' over C. Then there is a natural bijection between $\mathcal{G}(C')$ and $\operatorname{Aut}(L \otimes_C C'|K \otimes_C C')$.*

Proof: We set $L' = L \otimes_C C'$ and $K' = K \otimes_C C'$. By Proposition 3.7.1 the extension $L'|K'$ is ϕ-Galois. Let $(\mathfrak{p}, \varphi) \in \mathcal{G}(C')$. By Lemma 3.7.2 we have $k(\mathfrak{p}) = L \otimes_C k(\mathfrak{p})^\phi$. Let $\sigma_t : L \to k(\mathfrak{p}) = \mathfrak{Q}((L \otimes_K L)/\mathfrak{p})$, $a \mapsto \frac{\overline{1 \otimes a}}{1}$ and define a K-ϕ-morphism $\sigma : L \to L \otimes_C C'$ by

$$\sigma : L \xrightarrow{\sigma_t} k(\mathfrak{p}) = L \otimes_C k(\mathfrak{p})^\phi \xrightarrow{\operatorname{id} \otimes \varphi} L \otimes_C C'.$$

Then the trivial extension $\sigma' : L \otimes_C C' \to L \otimes_C C'$ of σ to $L \otimes_C C'$ is a K'-ϕ-morphism and so $\sigma' \in \operatorname{Aut}(L'|K')$ by Lemma 3.3.15.

Conversely if we start with $\sigma' \in \operatorname{Aut}(L'|K')$ then we can define $\mathfrak{p}$ as the kernel of $L \otimes_K L \to L'$, $a \otimes b \mapsto a\sigma'(b)$. Then $\mathfrak{p}$ is a ϕ-prime ideal of $L \otimes_K L$ (Proposition 1.4.2) and we have an embedding $L \otimes_K L/\mathfrak{p} \hookrightarrow L'$ which extends (by Lemma 1.3.4) to an embedding $k(\mathfrak{p}) = \mathfrak{Q}(L \otimes_K L/\mathfrak{p}) \hookrightarrow L'$. Passing to constants we obtain an embedding $\varphi : k(\mathfrak{p})^\phi \hookrightarrow L'^\phi = C'$ (over C). We need to verify that $\mathfrak{p} \subset L \otimes_K L$ is ϕ-maximal. Let $\mathfrak{p}' \subset L' \otimes_{K'} L' = (L \otimes_K L) \otimes_C C'$ denote the kernel of $L' \otimes_{K'} L' \to L'$, $a' \otimes b' \mapsto a'\sigma'(b')$. Then $\mathfrak{p} = (L \otimes_K L) \cap \mathfrak{p}'$ and because $(L' \otimes_{K'} L')/\mathfrak{p}' \simeq L'$ is a ϕ-pfield we see that the minimal prime ideals of $\mathfrak{p}'$ are maximal ideals of $L' \otimes_{K'} L'$. Let $\mathfrak{q}'$ be a minimal prime ideal above $\mathfrak{p}'$. Because $L' \otimes_{K'} L'$ is an integral ring extension of $L \otimes_K L$ and $\mathfrak{q}'$ is a maximal ideal of $L' \otimes_{K'} L'$ it follows ([4, Corollary 5.8, p. 61]) that $\mathfrak{q} = \mathfrak{q}' \cap (L \otimes_K L)$ is a maximal ideal of $L \otimes_K L$. As $\mathfrak{q}$ is a minimal prime ideal of $\mathfrak{p}$ this implies that $\mathfrak{p}$ is ϕ-maximal in $L \otimes_K L$.

It is not difficult to see that the two constructions described above are inverse to each other: If $(\mathfrak{p}, \varphi)$ is an element of $\mathcal{G}(C')$ then the kernel of $L \otimes_K L \to L'$, $a \otimes b \mapsto a\sigma(b)$ is of course $\mathfrak{p}$ and the embedding φ is recovered on the constants.

Conversely if $\sigma' \in \operatorname{Aut}(L'|K')$ and $(\mathfrak{p}, \varphi)$ are obtained from σ' then it follows from the commutativity of

$$\begin{tikzcd}
L\otimes_C k(\mathfrak{p})^\phi \arrow[r, hook] \arrow[d, equal] & L\otimes_C C' \arrow[d, equal] \\
(L\otimes_K L)/\mathfrak{p} \arrow[r, hook] & L'
\end{tikzcd}$$

that

$$L \xrightarrow{\sigma_t} k(\mathfrak{p}) = L\otimes_C k(\mathfrak{p})^\phi \xrightarrow{\mathrm{id}\otimes\varphi} L\otimes_C C = L'$$

and $L\to L',\ a\mapsto \sigma'(a)$ agree. □

We shall need the following technical lemma.

Lemma 3.7.4. *Let $C'|C$ be a (constant) algebraic field extension and R a C-ϕ-algebra. Assume that $R' = R\otimes_C C'$ is Noetherian. Let $X = \phi\text{-}\mathrm{Spec}(R)$ and $X' = X\times_C C' = \phi\text{-}\mathrm{Spec}(R')$. Then the projection $p : X'\to X$ is surjective.*

Proof: Let $\mathfrak{q}\in\phi\text{-}\mathrm{Spec}(R)$ because R' is integral over R there exists $\mathfrak{q}'\in\mathrm{Spec}(R')$ with $\mathfrak{q}'\cap R = \mathfrak{q}$ ([4, Theorem 5.10, p. 62]). In particular $\mathfrak{q}\otimes C'\subset\mathfrak{q}'$. If $\mathfrak{q}_1'$ is a minimal prime ideal of $\mathfrak{q}\otimes C'$ contained in $\mathfrak{q}'$ then also $\mathfrak{q} = R\cap\mathfrak{q}_1'$. It therefore suffices to show that $\mathfrak{q}_1'\in\phi\text{-}\mathrm{Spec}(R')$. If $d\geq 1$ with $\phi^{-d}(\mathfrak{q}) = \mathfrak{q}$ then $\phi^{-d}(\mathfrak{q}\otimes C') = \mathfrak{q}\otimes C'$ by Corollary 1.5.4 and the fact that $C'|C$ is ϕ^d-separable (Corollary 1.5.3). Therefore $\phi^d\text{-}\sqrt{\mathfrak{q}\otimes C'} = \sqrt{\mathfrak{q}\otimes C'}$ by Proposition 1.4.7. As R' is Noetherian $\sqrt{\mathfrak{q}\otimes C'}$ is the intersection of the finitely many minimal prime ideals of $\mathfrak{q}\otimes C'$ and we see that ϕ^{-d} induces a permutation of the minimal prime ideals of $\mathfrak{q}\otimes C'$. Therefore there exists $n\geq 1$ such that $\phi^{-n}(\mathfrak{q}_1') = \mathfrak{q}_1'$, i.e. $\mathfrak{q}_1'\in\phi\text{-}\mathrm{Spec}(R')$. □

Proposition 3.7.5. *Let $L|K$ be a ϕ-Galois extension of ϕ-pfields and $X = \phi\text{-}\mathrm{Spec}(L\otimes_K L)$. Then there exists a finite algebraic extension C' of $C = K^\phi = L^\phi$ such that $X' = X\times_C C'$ is split over $L' = L\otimes_C C'$. In other words $L'|K'$ is a ϕ-Galois extension such that $\phi\text{-}\mathrm{Spec}(L'\otimes_{K'} L')$ is split.*

Proof: Let $\overline{C}$ denote an algebraic closure of C and set $\overline{L} = L\otimes_C\overline{C}$, $\overline{K} = K\otimes_C\overline{C}$. It follows from Proposition 3.7.1 that $\overline{L}|\overline{K}$ is ϕ-Galois with $\overline{L}^\phi = \overline{K}^\phi = \overline{C}$. Set $\overline{X} = \phi\text{-}\mathrm{Spec}(\overline{L}\otimes_{\overline{K}}\overline{L}) = X\times_C\overline{C}$ and let $p:\overline{X}\to X$ denote the projection. By Proposition 3.5.1 there exists a non-empty open Φ-stable subset U of X which is split over L. Let $\overline{U} = p^{-1}(U)\subset\overline{X}$. Then using Lemma 3.7.4 we see that also $\overline{U}$ is open non-empty and Φ-stable.

Let $\overline{x}$ be an arbitrary point of $\overline{X}$. By Corollary 3.6.3 there exists a $\overline{K}$-ϕ-automorphism $\overline{\tau}$ of $\overline{L}$ such that the $\overline{L}$-automorphism $\overline{\tau}^*:\overline{X}\to\overline{X}$ induced from

$$\overline{L}\otimes_{\overline{K}}\overline{L}\to\overline{L}\otimes_{\overline{K}}\overline{L},\ a\otimes b\mapsto a\otimes\overline{\tau}(b)$$

satisfies $x\in\overline{\tau}^*(\overline{U})$. As $\overline{X}$ is quasi-compact (Lemma 3.3.16) we can find finitely many $\overline{K}$-ϕ-automorphism $\overline{\tau_1},\ldots,\overline{\tau_n}$ of $\overline{L}$ such that the $\overline{\tau_i}^*(\overline{U})$'s cover $\overline{X}$.

As explained in Lemma 3.7.3 each $\overline{\tau_i}$ corresponds to a pair $(\mathfrak{p}_i,\varphi_i)$ where $\mathfrak{p}_i$ is a ϕ-maximal ideal of $L\otimes_K L$ and $\varphi_i : k(\mathfrak{p}_i)^\phi\to\overline{C}$ an embedding over C. In particular

$\overline{\tau_i}\colon L\otimes_C\overline{C}\to L\otimes_C\overline{C}$ restricts to an automorphism $L\otimes_C\varphi_i(k(\mathfrak{p}_i)^\phi)\to L\otimes_C\varphi_i(k(\mathfrak{p}_i)^\phi)$. We know from Lemma 3.7.2 that $k(\mathfrak{p}_i)^\phi$ is a finite extension of C. Thus there exists a finite extension C' of C inside $\overline{C}$ that contains $\varphi_i(k(\mathfrak{p}_i)^\phi)$ for $i=1,\ldots,n$. Set $K'=K\otimes_C C'$ and $L'=L\otimes_C C'$. The $\overline{\tau_i}$'s restrict to K'-ϕ-automorphisms $\tau_i'\colon L'\to L'$.

We have to show that

$$X'=\phi\text{-Spec}(L'\otimes_{K'}L')=X\times_C C'$$

is split over L'. Let $p'\colon X'=X\times_C C'\to X$ denote the projection. Then $U'=p'^{-1}(U)$ is a non-empty open Φ-stable subset of X'. Because

$$U'=p'^{-1}(U)=U\times_C C'=(L\times_C U^\phi)\times_C C'=L'\times_{C'}(U^\phi\times_C C')$$

it follows that U' is split over L'. Let $\tau_i'^*\colon X'\to X'$ denote the L'-automorphism induced from $L'\otimes_{K'}L'\to L'\otimes_{K'}L'$, $a'\otimes b'\mapsto a'\otimes\tau_i'(b')$. Then the $\tau_i'^*(U')$ are open Φ-stable subsets of X' that are split over L'. To show that X' is split it suffices to show by Proposition 2.5.5 that the $\tau_i'^*(U')$'s cover X'. So let $x'\in X'$. By construction the $\overline{\tau_i}^*(\overline{U})$'s cover $\overline{X}$ and

$$\begin{tikzcd}
\overline{X} \arrow[r, "\overline{\tau_i}^*"] \arrow[d] & \overline{X} \arrow[d] \\
X' \arrow[r, "\tau_i'^*"] & X'
\end{tikzcd}$$

commutes. Because the projection $\overline{p}\colon\overline{X}=X'\times_{C'}\overline{C}\to X'$ is surjective (Lemma 3.7.4) there is $\overline{x}\in\overline{X}$ with $\overline{p}(\overline{x})=x'$ and $\overline{x}\in\overline{\tau_i}^*(\overline{U})$ for some $i\in\{1,\ldots,n\}$. Say $\overline{x}=\overline{\tau_i}^*(\overline{y})$ for $\overline{y}\in\overline{U}$. We have

$$x'=\overline{p}(\overline{x})=\overline{p}(\overline{\tau_i}^*(\overline{y}))=\tau_i'^*(\overline{p}(\overline{y})).$$

Because $\overline{p}(\overline{y})\in U'$ we have $x'\in\tau_i'^*(U')$. □

3.8 Descent

Let $L|K$ be a ϕ-Galois extension of ϕ-pfields and set $C=K^\phi=L^\phi$. In the above section we proved that there exists a finite algebraic field extension C' of C such that $X'=\phi\text{-Spec}(L'\otimes_{K'}L')$ is split over L', where $L'|K'$ denotes the ϕ-Galois extension obtained from $L|K$ by extending the constants from C to C', i.e. $K'=K\otimes_C C'$ and $L'=L\otimes_C C'$. The purpose of this section is to prove that we can indeed assume that $C'=C$, in other words: $X=\phi\text{-Spec}(L\otimes_K L)$ is split over L without any additional assumption on the constants. The quite obvious method of proof is descent. The application of descent theory is complicated by two things:

- We know that $\mathcal{G}'=X'^\phi$ is a scheme and there is a natural way to define a descent datum on $\mathcal{G}'$ relative to $C'|C$ but it is not a priori clear that the descent datum on $\mathcal{G}'$ is effective. The standard condition to ensure effectivity of the descent datum would be quasi-projectivity of $\mathcal{G}'$. But it seems to be unknown (cf. [40, Remark 2.2, p. 50]) if every group scheme of finite type over a field is quasi-projective.

- As we want to avoid the assumption that the constants C are perfect we have to use Grothendieck's faithfully flat descent rather than classical Galois descent.

While the second problem is more of a notational character the first one is solved in Proposition 3.8.1 by recurrence to a deep theorem about algebraic groups which states that every reduced group scheme of finite type over a field is quasi-projective.

We start by recalling the formalism of descent data. The descent problem is most naturally formulated in fibred categories but to keep things down to earth we refrain from introducing too much machinery and only state the results we need in simple language. Also we are not interested in developing decent theory for ϕ-spaces in general. Rather we strive to prove the above mentioned result with the least possible effort. The standard references for descent theory are [16] (which is "explained" in [13]) and [1, Chapters VI and VIII].

Let $C'|C$ be a finite field extension and Y' a scheme over C'. We set $C'' = C' \otimes_C C'$ and $C''' = C' \otimes_C C' \otimes_C C'$. Corresponding to the two natural maps (source and target) from C' to C'' there are two natural ways to obtain a C''-scheme from Y', namely $Y' \times_C C'$ and $C' \times_C Y'$ which are considered as schemes over C'' in a diagonal manner. Similarly there are three natural ways to obtain a C'''-scheme from Y' namely $Y' \times_C C' \times_C C'$, $C' \times_C Y' \times_C C'$ and $C' \times_C C' \times_C Y'$, again these are considered as C'''-schemes in a diagonal fashion.

A *descent datum* on Y' (relative to $C'|C$ or $\mathrm{Spec}(C') \to \mathrm{Spec}(C)$) is an isomorphism

$$\varphi : Y' \times_C C' \simeq C' \times_C Y'$$

of schemes over C'' such that the following diagram of C'''-schemes, expressing the cocycle condition is commutative.

$$\begin{tikzcd}
Y' \times_C C' \times_C C' \arrow[rr, "p_{12}^*\varphi"] \arrow[dr, "p_{13}^*\varphi"'] & & C' \times_C Y' \times_C C' \arrow[dl, "p_{23}^*\varphi"] \\
 & C' \times_C C' \times_C Y' &
\end{tikzcd}$$

Here $p_{ij} : \mathrm{Spec}(C''') \to \mathrm{Spec}(C'')$ denotes the projection onto the i-th and j-th factor for $1 \leq i < j \leq 3$ and $p_{ij}^*\varphi$ the pullback of φ along p_{ij}, e.g. $p_{12}^*\varphi = \varphi \times \mathrm{id}$.

If Y_1' and Y_2' are schemes over C' equipped with descend data φ_1, φ_2 then a morphism $f' : Y_1' \to Y_2'$ of schemes over C' is said to be *compatible with the descend data* if

$$\begin{tikzcd}
Y_1' \times_C C' \arrow[r, "f' \times \mathrm{id}"] \arrow[d, "\varphi_1"'] & Y_2' \times_C C' \arrow[d, "\varphi_2"] \\
C' \times_C Y_1' \arrow[r, "\mathrm{id} \times f'"] & C' \times_C Y_2'
\end{tikzcd}$$

commutes.

If Y is a scheme over C then $Y' = Y \times_C C'$ is a scheme over C' naturally equipped with a descent datum

$$\varphi : Y' \times_C C' \simeq Y \times_C C' \times_C C' \simeq C' \times_C Y'.$$

Finally a descent datum on a C'-scheme Y' is called *effective* if there exists a C-scheme Y and an isomorphism $Y \times_C C' \simeq Y'$ which is compatible with descent data. We shall need the following basic descent result for group schemes. I could not locate it in the literature elsewhere.

Proposition 3.8.1. *Let $C'|C$ be a finite algebraic extension of fields and Y' a scheme of finite type over C'. Suppose that Y' can be endowed with the structure of a group scheme over C'. Then any descent datum on Y' relative to* $\mathrm{Spec}(C') \to \mathrm{Spec}(C)$ *is effective.*

Proof: Let $q_1, q_2 : Y'' \rightrightarrows Y'$ denote the couple of equivalence induced by the descend datum [1, Chapter VIII, Section 7, p. 219]. By [1, Corollaire 7.6, Chapter VIII, p. 222] it suffices to prove that $R(y') = q_2(q_1^{-1}(y'))$ is contained in an open affine subset of Y' for every $y' \in Y'$. Let $\widetilde{C}$ denote the perfect closure of C'. We have natural morphisms

$$\left(Y' \times_{C'} \widetilde{C}\right)_{\mathrm{red}} \xrightarrow{f} Y' \times_{C'} \widetilde{C} \xrightarrow{g} Y'.$$

and both f and g are homeomorphisms of the underlying topological spaces. The reduced scheme $\mathcal{G} = (Y' \times_{C'} \widetilde{C})_{\mathrm{red}}$ is naturally endowed with a structure of group scheme of finite type over $\widetilde{C}$. (This is in general not true for Y'_{red}.) Let $\overline{C}$ denote the algebraic closure of $\widetilde{C}$. Because $\widetilde{C}$ is perfect $\mathcal{G} \times_{\widetilde{C}} \overline{C}$ is reduced and hence a reduced group scheme of finite type over an algebraically closed field. The standard translation argument shows that $\mathcal{G} \times_{\widetilde{C}} \overline{C}$ is smooth over $\overline{C}$ and by [1, Corollaire 4.13, Chapter II, p. 43] this implies that $\mathcal{G}$ is smooth over $\widetilde{C}$.

Now it is known that every smooth group scheme of finite type over a field is quasi-projective (see e.g. [6, Theorem 1, Section 6.4, p. 153]) and in a quasi-projective scheme every finite set of points has an open affine neighborhood (see e.g. [30, Proposition 3.36, Chapter 3, p. 109]). Thus the finite set $f^{-1}(g^{-1}(R(y'))$ is contained in an open affine U of $\mathcal{G} = (Y' \times_{C'} \widetilde{C})_{\mathrm{red}}$. It follows from [14, Corollaire 6.1.7, p. 142] that $f(U)$ is an open affine of $Y' \times_{C'} \widetilde{C}$. As $f(U) = g^{-1}(g(f(U))) = g(f(U)) \times_{C'} \widetilde{C}$ is affine it follows from fpqc descent ([15, Proposition 2.7.1, p. 29]) that $g(f(U))$ is affine. Therefore $g(f(U))$ is an open affine subset of Y' containing $R(y')$. □

Let as above $C'|C$ denote a finite algebraic extension of fields. If X is a ϕ-space over C which can be covered by open Φ-stable subsets of the form ϕ-Spec(R) where R is a C-ϕ-algebra then the products $X \times_C C', X \times_C C' \times_C C'$ and $X \times_C C' \times_C C' \times_C C'$ all exist (Proposition 2.1.14) and the notion of descent datum on $X' = X \times_C C'$ (relative to $C''|C$) can be defined in a manner completely analogous to the case of schemes treated above, i.e. a descent datum on X' is an isomorphism

$$\varphi : X' \times_C C' \simeq C' \times_C X'$$

of ϕ-spaces over C'' satisfying the cocycle condition. Similarly $X' = X \times_C C'$ is equipped with a natural descent datum. The main descent result for ϕ-spaces that we will need is the following proposition.

Proposition 3.8.2. *Let $C'|C$ be a (constant) finite algebraic field extension and X_1 and X_2 ϕ-spaces over C which can be covered by open Φ-stable subsets of the form ϕ-$\operatorname{Spec}(R)$ where R is a Noetherian C-ϕ-algebra with $\phi: R \to R$ injective. Then the natural map*

$$\operatorname{Hom}_C(X_1, X_2) \to \operatorname{Hom}_{C'|C}(X_1', X_2')$$

is bijective. Here $\operatorname{Hom}_{C'|C}(X_1', X_2')$ denotes the C'-morphisms from $X_1' = X_1 \times_C C'$ to $X_2' = X_2 \times_C C'$ which are compatible with the descent data.

The proof of Proposition 3.8.2 will be achieved through a series of four preparatory lemmas. The actual proof can then be found below Lemma 3.8.6. The first lemma does not take into account any difference structure. It is surely well known, but because of lack of a suitable reference we include the proof.

Lemma 3.8.3. *Let C be a field and C' a C-algebra that is finite dimensional as C-vector space. Set $R' = R \otimes_C C'$, $X = \operatorname{Spec}(R), X' = X \times_C C' = \operatorname{Spec}(R')$ and let $p: X' \to X$ denote the projection. Let $\mathfrak{q} \subset R$ be the prime ideal corresponding to a point $x \in X$. Then $p^{-1}(x)$ is a finite, non-empty set and agrees with the minimal prime ideals of $\mathfrak{q} \otimes C' \subset R'$. Furthermore if $S = R \smallsetminus \mathfrak{q}$ and $S' = \{s' \in R';\ s' \notin \mathfrak{q}' \text{ for all } \mathfrak{q}' \in p^{-1}(x)\}$ then the natural map*

$$S^{-1}R' \to S'^{-1}R'$$

is an isomorphism.

Proof: Let $k(x) = \mathfrak{Q}(R/\mathfrak{q})$ denote the residue field at x. We have

$$p^{-1}(x) \simeq X_x' = X' \times_X \operatorname{Spec}(k(x)) = \operatorname{Spec}(k(x) \otimes_C C')$$

Because C' is finite dimensional as C-vector space $k(x) \otimes_C C'$ is finite dimensional as $k(x)$-vector space, in particular $k(x) \otimes_C C'$ is Artinian. It follows that $\operatorname{Spec}(k(x) \otimes_C C')$ is finite and discrete ([4, Chapter 8]). We have a commutative diagram

$$\begin{tikzcd}
R \otimes_C C' \arrow[rr, "\psi"] \arrow[dr] & & k(x) \otimes_C C' \\
& (R \otimes_C C')/(\mathfrak{q} \otimes C') = (R/\mathfrak{q}) \otimes_C C' \arrow[ur, "\alpha"'] &
\end{tikzcd}$$

and the prime ideals in $p^{-1}(x)$ are precisely those of the form $\psi^{-1}(\widetilde{\mathfrak{q}})$ for some prime ideal $\widetilde{\mathfrak{q}}$ of $k(x) \otimes_C C'$. As α is injective every minimal prime ideal of $(R/\mathfrak{q}) \otimes_C C'$ is of the form $\alpha^{-1}(\widetilde{\mathfrak{q}})$ for some prime ideal $\widetilde{\mathfrak{q}}$ of $k(x) \otimes_C C'$ ([8, Proposition 16, Chapter II, Paragraph 2.6, p. 74]). Because $\operatorname{Spec}(k(x) \otimes_C C')$ is discrete and ψ induces a homeomorphism from $\operatorname{Spec}(k(x) \otimes_C C')$ onto $p^{-1}(x)$ it follows that $p^{-1}(x)$ agrees with the set of minimal prime ideals above $\mathfrak{q} \otimes_C C'$.

Finally to prove that the natural map $S^{-1}R' \to S'^{-1}R'$ is an isomorphism it suffices to show that S' is the saturation of $S = S \otimes 1$ (see [8, Exercise 1 for Paragraph 2 of Chapter II, p. 123] or [37, Exercises 5.7 and 5.12, p. 84ff.]). In other words, we have to show that

$$S' = R' \smallsetminus \bigcup_{\mathfrak{q}' \cap S = \emptyset} \mathfrak{q}'.$$

Let $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_n$ denote the minimal prime ideals of $\mathfrak{q} \otimes C'$. By definition $S' = R' \smallsetminus \cup \mathfrak{q}'_i$ and so we have to show that

$$\bigcup_{i=1}^{n} \mathfrak{q}'_i = \bigcup_{\mathfrak{q}' \cap S = \emptyset} \mathfrak{q}'.$$

The inclusion "$\subset$" is trivial. But if $\mathfrak{q}' \in \operatorname{Spec}(R')$ with $\mathfrak{q}' \cap S = \emptyset$ then $\mathfrak{q}' \cap R \subset \mathfrak{q}$. Because R' is integral over R it follows from the "going-up" Theorem (see e.g. [4, Theorem 5.11, p. 62]) that there exists $\mathfrak{q}'_0 \in \operatorname{Spec}(R')$ such that $\mathfrak{q}' \subset \mathfrak{q}'_0$ and $\mathfrak{q}'_0 \cap R = \mathfrak{q}$. As shown above we must have $\mathfrak{q}'_0 = \mathfrak{q}'_i$ for some $i \in \{1, \ldots, n\}$. Therefore $\mathfrak{q}' \subset \mathfrak{q}'_i$ as desired. □

Lemma 3.8.4. *Let C be a field and C' a constant C-algebra such that C' is finite dimensional as C-vector space. Let R be a C-ϕ-algebra and set $R' = R \otimes_C C'$, $X = \phi\text{-}\operatorname{Spec}(R)$, $X' = X \times_C C' = \phi\text{-}\operatorname{Spec}(R')$ and let $p : X' \to X$ denote the projection. Let $\mathfrak{q} \in \phi\text{-}\operatorname{Spec}(R)$ denote the prime ideal corresponding to a point $x \in X$. Then $p^{-1}(x)$ is a finite non-empty set and agrees with the minimal prime ideals above $\mathfrak{q} \otimes C' \subset R'$. Moreover p is closed and for $U \subset X$ open the natural map*

$$\alpha : \mathcal{O}_X(U) \otimes_C C' \to \mathcal{O}_{X'}(p^{-1}(U))$$

is injective.

Proof: By Lemma 3.8.3 it suffices to see that the minimal prime ideals of $\mathfrak{q} \otimes C'$ belong to ϕ-Spec(R'). If $d \geq 1$ is such that $\phi^{-d}(\mathfrak{q}) = \mathfrak{q}$ then $\phi^{-d}(\mathfrak{q} \otimes C') = \mathfrak{q} \otimes C'$. This follows for example from Corollary 1.5.4 using that $C'|C$ is ϕ^d-separable (where of course ϕ is the identity on C and C'). Therefore by Proposition 1.4.7

$$\phi^d\text{-}\sqrt{\mathfrak{q} \otimes C'} = \sqrt{\mathfrak{q} \otimes C'}.$$

Because $\sqrt{\mathfrak{q} \otimes C'}$ is the (finite) intersection of the minimal prime ideals above $\mathfrak{q} \otimes C'$ it follows as in the proof of Proposition 1.4.8 that the minimal prime ideals of $\mathfrak{q} \otimes C'$ belong to ϕ-Spec(R').

Next we will show that p is a closed map. So let $\mathfrak{a}' \subset R'$ be an ideal and set $\mathfrak{a} = \mathfrak{a}' \cap R$. We will show that $p(\mathbb{V}(\mathfrak{a}')) = \mathbb{V}(\mathfrak{a})$. The inclusion "$\subset$" is trivial. So let $\mathfrak{q} \in \mathbb{V}(\mathfrak{a})$. Because $R/\mathfrak{a} \hookrightarrow R'/\mathfrak{a}'$ is an integral ring extension every prime ideal $\widetilde{\mathfrak{q}}$ of $R/\mathfrak{a}$ is of the form $\widetilde{\mathfrak{q}} = \widetilde{\mathfrak{q}}' \cap (R/\mathfrak{a})$ for some prime ideal $\widetilde{\mathfrak{q}}'$ of $R'/\mathfrak{a}'$. This implies that there exists a prime ideal $\mathfrak{q}'$ of R' with $\mathfrak{q}' \supset \mathfrak{a}'$ such that $\mathfrak{q}' \cap R = \mathfrak{q}$. It follows from Lemma 3.8.3 and the considerations above that $\mathfrak{q}'$ belongs to ϕ-Spec(R'), i.e. $\mathfrak{q} \in p(\mathbb{V}(\mathfrak{a}'))$.

Now we will show that α is injective. Let $\{c'_i\}$ be a C-basis of C' and assume that $\alpha(\sum F_i \otimes c'_i) = 0$. We have to show that $F_i = 0$ for all i. Thus it suffices to show that $F_i(\mathfrak{q}) = 0$ for a fixed $\mathfrak{q} \in U$. We may write $F_i(\mathfrak{q}) = \frac{r_i}{s_i} \in R_{\mathfrak{q}}$. After multiplying with appropriate factors we can assume $F_i(\mathfrak{q}) = \frac{r_i}{s} \in R_{\mathfrak{q}}$ with $r_i \in R$ and $s \in R \smallsetminus \mathfrak{q}$. Let $r' = \sum r_i \otimes c_i'$. By assumption $\frac{r'}{1} = 0 \in R'_{\mathfrak{q}'}$ for all $\mathfrak{q}' \in p^{-1}(U) \subset \phi\text{-Spec}(R')$. In particular for every $\mathfrak{q}' \in p^{-1}(\mathfrak{q})$ there exists an $s'_{\mathfrak{q}'} \in R' \smallsetminus \mathfrak{q}'$ such that $s'_{\mathfrak{q}'}r' = 0$. By the prime avoidance lemma ([12, Lemma 3.3, p. 90]) there exists an $s' \in R'$ with $s'r' = 0$ and $s' \notin \mathfrak{q}'$ for all $\mathfrak{q}' \in p^{-1}(\mathfrak{q})$. Now it follows from Lemma 3.8.3 that there exists $\widetilde{s} \in R \smallsetminus \mathfrak{q}$ such that $0 = (\widetilde{s} \otimes 1)r' = \sum \widetilde{s}r_i \otimes c_i'$. This yields $\widetilde{s}r_i = 0$ and so $F_i(\mathfrak{q}) = \frac{r_i}{s} = 0 \in R_{\mathfrak{q}}$ as desired. □

We shall need a certain quotient construction which is detailed in the proof of the following lemma.

Lemma 3.8.5. *Let $q_1, q_2 : X'' \rightrightarrows X'$ be two morphisms of ϕ-spaces. Then the coequalizer of q_1, q_2 exists in the category of ϕ-spaces. I.e. there exists a ϕ-space X together with a morphism $p : X' \to X$ such that $pq_1 = pq_2$ and for any other pair $(\widetilde{X}, \widetilde{p})$ enjoying the same property there exists a unique morphism $f : X \to \widetilde{X}$ making*

$$\begin{tikzcd}
X' \arrow[r, "p"] \arrow[dr, "\widetilde{p}"'] & X \arrow[d, dotted, "f"] \\
 & \widetilde{X}
\end{tikzcd}$$

commutative.

Proof: Let $\sim$ denote the equivalence relation on X' generated by

$$x_1' \sim x_2' \text{ if and only if there exists } x'' \in X'' \text{ such that } q_1(x'') = x_1' \text{ and } q_2(x'') = x_2'.$$

Let $X = X'/\sim$ denote the quotient set. We have a natural projection $p : X' \to X$ (of sets) which by construction satisfies $pq_1 = pq_2$. We endow X with the quotient topology. Because $q_i\Phi'' = \Phi' q_i$ for $i = 1, 2$ we see that $x_1' \sim x_2'$ implies $\Phi'(x_1') \sim \Phi'(x_2')$ and we obtain a well-defined continuous map $\Phi : X \to X$ such that

$$\begin{tikzcd}
X' \arrow[r, "\Phi'"] \arrow[d, "p"'] & X' \arrow[d, "p"] \\
X \arrow[r, "\Phi"] & X
\end{tikzcd}$$

commutes. Next we want to define the structure sheaf $\mathcal{O}_X$ of X. If U is an open subset of X then we have two parallel arrows

$$q_1^\sharp, q_2^\sharp : \mathcal{O}_{X'}(p^{-1}(U)) \longrightarrow \mathcal{O}_{X''}(q_1^{-1}(p^{-1}(U))) = \mathcal{O}_{X''}(q_2^{-1}(p^{-1}(U)))$$

and we can define $\mathcal{O}_X(U)$ to be the equalizer of this pair, i.e.

$$\mathcal{O}_X(U) = \left\{ F \in \mathcal{O}_{X'}(p^{-1}(U));\ q_1^\sharp(F) = q_2^\sharp(F) \right\}.$$

It is immediate that $\mathcal{O}_X$ is a sheaf of rings on X. We have to show that $(X, \mathcal{O}_X)$ is a locally ringed space. More precisely we will show that for $x \in X$

$$\mathfrak{m}_x = \{(U, F) \in \mathcal{O}_{X,x};\ F(x') \in \mathfrak{m}_{x'} \subset \mathcal{O}_{X',x'} \text{ for all } x' \in p^{-1}(x)\}$$

is the unique maximal ideal of $\mathcal{O}_{X,x}$. Suppose $(U, F) \notin \mathfrak{m}_x$. (We recall that here U denotes an open neighborhood of $x \in X$ and $F \in \mathcal{O}_X(U)$.) We have to show that (U, F) is invertible in $\mathcal{O}_{X,x}$.

We have an open subset $U' = \{x' \in p^{-1}(U);\ F(x') \notin \mathfrak{m}_x\}$ of $p^{-1}(U) \subset X'$ (Lemma 2.1.10). Let $x'_1, x'_2 \in p^{-1}(U)$ such that $F(x'_1) \notin \mathfrak{m}_{x'_1}$ and assume that there exists an $x'' \in X''$ such that $q_1(x'') = x'_1$ and $q_2(x'') = x'_2$. We have two local morphisms $\mathcal{O}_{X',x'_1} \to \mathcal{O}_{X'',x''}$ and $\mathcal{O}_{X',x'_2} \to \mathcal{O}_{X'',x''}$ which map $F(x'_1)$ respectively $F(x'_2)$ to the same element of $\mathcal{O}_{X'',x''}$. As $F(x'_1) \notin \mathfrak{m}_{x'_1}$ it follows that also $F(x'_2) \notin \mathfrak{m}_{x'_2}$. This shows that U' is stable under the equivalence relation $\sim$. Therefore $V = p(U') \subset U$ is an open neighborhood of x in X. As the restriction of F to U' is invertible in $\mathcal{O}_{X'}(U')$ and also in $\mathcal{O}_X(U)$ we find that $(V, F|_{U'}^{-1})$ is the inverse of (U, F) as desired.

To complete the construction of X it remains to define $\phi : \mathcal{O}_X \to \Phi_* \mathcal{O}_X$. But if $U \subset X$ is open we already have a map

$$\phi' : \mathcal{O}_{X'}(p^{-1}(U)) \to \mathcal{O}_{X'}(\Phi'^{-1}(p^{-1}(U)))$$

and it is easy to see that it restricts to

$$\phi : \mathcal{O}_X(U) \to \mathcal{O}_X(\Phi^{-1}(U)) \subset \mathcal{O}_{X'}(p^{-1}(\Phi^{-1}(U))) = \mathcal{O}_{X'}(\Phi'^{-1}(p^{-1}(U))).$$

Because ϕ' induces local maps on stalks also ϕ induces local maps on stalks. Summarily we see that X has the structure of a ϕ-space and of course there is a natural map of ϕ-spaces $p : X' \to X$ such that $pq_1 = pq_2$.

Finally we have to check the universal property. So let $\widetilde{X}$ be a ϕ-space and $\widetilde{p} : X \to \widetilde{X}$ a morphism of ϕ-spaces such that $\widetilde{p}q_1 = \widetilde{p}q_2$. Then $x'_1 \sim_{\widetilde{p}} x'_2$ if and only if $\widetilde{p}(x'_1) = \widetilde{p}(x'_2)$ defines an equivalence relation on X' which is coarser than $\sim$. Therefore there exists a unique map of sets $f : X \to \widetilde{X}$ such that $fp = \widetilde{p}$. As X caries the quotient topology f is continuous. Because $f\Phi p = fp\Phi' = \widetilde{p}\Phi' = \widetilde{\Phi}\widetilde{p} = \widetilde{\Phi} fp$ it follows from the surjectivity of p that $f\Phi = \widetilde{\Phi} f$. Existence and uniqueness of a morphism $f^\sharp : \mathcal{O}_{\widetilde{X}} \to f_* \mathcal{O}_X$ such that $fp = \widetilde{p}$ in the category of ringed spaces follows immediately from the universal property of equalizers in the category of rings. The commutative diagram

$$\begin{tikzcd}
\mathcal{O}_{X',x'} & \mathcal{O}_{X,p(x')} \arrow[l] \\
 & \mathcal{O}_{\widetilde{X},\widetilde{p}(x')} \arrow[u] \arrow[ul]
\end{tikzcd}$$

shows that f is indeed a morphism of locally ringed spaces. Finally a diagram chase through

$$\begin{tikzcd}
\mathcal{O}_{\widetilde{X}}(\widetilde{U}) \arrow[r] \arrow[rr, bend left] \arrow[d, "\widetilde{\phi}"'] & \mathcal{O}_{X'}(\widetilde{p}^{-1}(\widetilde{U})) \arrow[d, "\phi'"] & \mathcal{O}_X(f^{-1}(\widetilde{U})) \arrow[l, hook'] \arrow[d, "\phi"] \\
\mathcal{O}_{\widetilde{X}}(\widetilde{\Phi}^{-1}(\widetilde{U})) \arrow[r] \arrow[rr, bend right] & \mathcal{O}_{X'}(\Phi'^{-1}(\widetilde{p}^{-1}(\widetilde{U})) & \mathcal{O}_X(\Phi^{-1}(f^{-1}(\widetilde{U}))) \arrow[l, hook']
\end{tikzcd}$$

reveals that f is in fact a morphism of ϕ-spaces. □

Lemma 3.8.6. *Let $C'|C$ be a finite algebraic field extension and X a ϕ-space over C which can be covered by open Φ-stable subsets of the form ϕ-*Spec(R) *where R is a Noetherian C-ϕ-algebra with $\phi : R \to R$ injective. Then X can be recovered from $X' = X \times_C C'$ and the natural descent datum on X'.*

Proof: Let $\varphi : X' \times_C C' \simeq C' \times_C X'$ denote the natural descend datum. Set $X'' = X' \times_C C'$ and let $q_1 : X'' \to X'$ denote the projection. We define $q_2 : X'' \to X'$ as the composition of φ and the projection onto X'. As explained in Lemma 3.8.5 the coequalizer

$$X'' \rightrightarrows X' \overset{\widetilde{p}}{\to} \widetilde{X}$$

of $q_1, q_2 : X'' \rightrightarrows X'$ exists in the category of ϕ-spaces. We see that $\widetilde{X}$ is naturally a ϕ-space over C. Let $p : X' = X \times_C C' \to X$ denote the projection. By definition $pq_1 = pq_2$ and from the universal property of $\widetilde{X}$ we obtain a morphism $f : \widetilde{X} \to X$ of ϕ-spaces. We will show that f is an isomorphism. (This is what is meant by the statement of Lemma 3.8.6.) The situation is summarized in the following diagram. The triangle at the top is not commutative.

$$\begin{tikzcd}
X' \times_C C' \arrow[rr, "\varphi"] \arrow[dr, "q_1"'] & & C' \times_C X' \arrow[dl] \\
& X' \arrow[d, "p"'] \arrow[dr, "\widetilde{p}"] & \\
& X & \widetilde{X} \arrow[l, "f"']
\end{tikzcd}$$

If $U = \phi$-Spec(R) is an open Φ-stable subset of X (where R is a Noetherian C-ϕ-algebra with $\phi : R \to R$ injective) then $U' = U \times_C C'$ is an open subset of X'. The isomorphism $\varphi : X' \times_C C' \simeq C' \times_C X'$ restricts to an isomorphism $U' \times_C C' \simeq C \times_C U'$ and this restriction agrees with the natural descent datum on U'. As $U'' = U' \times_C C' = q_1^{-1}(U') = q_2^{-1}(U')$ it is clear that U' is stable under the equivalence relation defined in the proof of Lemma 3.8.5. Therefore the coequalizer $\widetilde{U}$ of $q_1, q_2 : U'' \to U'$ is naturally an open ϕ-subspace of $\widetilde{X}$. Furthermore f restricts to the natural map $\widetilde{U} \to U$. Summarily we see that we can assume without loss of generality that $X = U$, i.e. from now on we assume that $X = \phi$-Spec(R) where R is a Noetherian C-ϕ-algebra with $\phi : R \to R$ injective.

We first show that $f : \widetilde{X} \to X$ is bijective. Because p is surjective (Lemma 3.8.4) it is clear that f is surjective. To prove that f is injective we have to show that $p(x'_1) = p(x'_2)$ implies $x'_1 \sim x'_2$. As the upper triangle in

$$\begin{tikzcd}
 & X' \times_X X' \arrow[dl, "\simeq"'] \arrow[dr, "\simeq"] & \\
X' \times_C C' \arrow[rr, "\varphi"] \arrow[dr] & & C' \times_C X' \arrow[dl] \\
 & X' \arrow[d, "p"] & \\
 & X &
\end{tikzcd}$$

is commutative it suffices to prove that the natural map from $X' \times_X X'$ to the set theoretic fibred product of X' with X' over X is surjective. But this is guaranteed by Lemma 2.1.15 because $R' = R \otimes_C C'$ is finitely generated as R-algebra. Therefore f is bijective. Because p is closed (Lemma 3.8.4) it follows that f is a homeomorphism.

To complete the proof we have to show that for every $\widetilde{x} \in \widetilde{X}$ the induced map

$$f^\sharp_{\widetilde{x}} : \mathcal{O}_{X,f(\widetilde{x})} \to \mathcal{O}_{\widetilde{X},\widetilde{x}}$$

is bijective. Let $\mathfrak{q} \in \phi$-Spec$(R) = X$ denote the ideal corresponding to $f(\widetilde{x}) \in X$. As we have already seen above, for $x'_1, x'_2 \in X'$ one has $x'_1 \sim x'_2$ if and only $p(x'_1) = p(x'_2)$. Together with Lemma 3.8.4 this implies that the equivalence class $\widetilde{x}$ consists of all the minimal prime ideals, say $\{\mathfrak{q}'_1, \dots, \mathfrak{q}'_n\}$ of $\mathfrak{q} \otimes C' \subset R'$.

If $\frac{r}{1} \in R_{\mathfrak{q}} = \mathcal{O}_{X,f(\widetilde{x})}$ maps to zero under $f^\sharp_{\widetilde{x}}$ then we must have $\frac{r\otimes 1}{1} = 0 \in R'_{\mathfrak{q}'_i}$ for $i = 1, \dots, n$. By prime avoidance there exists an $s' \in R'$ with $s' \notin \mathfrak{q}'_i$ for $i = 1, \dots, n$ and $s'(r \otimes 1) = 0 \in R'$. By Lemma 3.8.3 there exists $s \in R \smallsetminus \mathfrak{q}$ such that $sr = 0$ and we can conclude that $f^\sharp_{\widetilde{x}}$ is injective.

The rest of the proof is devoted to showing that $f^\sharp_{\widetilde{x}}$ is surjective. So let $(\widetilde{U}, F)$ be an element of $\mathcal{O}_{\widetilde{X},\widetilde{x}}$. This means that $\widetilde{U}$ is an open neighborhood of $\widetilde{x}$ in $\widetilde{X}$ and $F \in \mathcal{O}_{X'}(\widetilde{p}^{-1}(\widetilde{U}))$ is such that $q_1^\sharp(F) = q_2^\sharp(F)$.

The C''-isomorphism $\varphi : X' \times_C C' \simeq C' \times_C X'$ is induced from the C''-isomorphism $\psi : C' \otimes_C R' \simeq R' \otimes_C C'$. Let

$$I' = \{s' \in R';\ \exists\ r' \in R' \text{ such that } s'F = r' \text{ on } \widetilde{p}^{-1}(\widetilde{U})\}.$$

Then I' is an ideal of R' and we will show that I' is stable under the descent datum, i.e. we will prove the following

Claim: The mapping ψ restricts to an isomorphism $\psi : C' \otimes_C I' \simeq I' \otimes_C C'$.

For reasons of symmetry it suffices to show that $\psi(C' \otimes_C I') \subset I' \otimes_C C'$. Let $s' \in I'$. We have to show that $\psi(1 \otimes s') \subset I' \otimes_C C'$. There exists $r' \in R'$ such that $s'F = r'$ on

$\widetilde{p}^{-1}(\widetilde{U})$. Let $p_2 : C' \times_C X' \to X'$ denote the projection. Then $(1 \otimes s')p_2^{\sharp}(F) = 1 \otimes r'$ on $p_2^{-1}(\widetilde{p}^{-1}(\widetilde{U}))$ and an application of $\varphi^{\sharp}$ gives $\psi(1 \otimes s')q_1^{\sharp}(F) = \psi(1 \otimes r')$ on $q_1^{-1}(\widetilde{p}^{-1}(\widetilde{U}))$.

It therefore suffices to show that for every $s'' \in R' \otimes_C C'$ such that there exists $r'' \in R' \otimes_C C'$ with $s'' q_1^{\sharp}(F) = r''$ on $q_1^{-1}(\widetilde{p}^{-1}(\widetilde{U}))$ we have $s'' \in I' \otimes_C C'$. Let $\{c_i'\}$ be a C-basis of C'. We may write $s'' = \sum s_i' \otimes c_i'$ and $r'' = \sum r_i' \otimes c_i'$. By Lemma 3.8.4 the map

$$\alpha : \mathcal{O}_{X'}(\widetilde{p}^{-1}(\widetilde{U})) \otimes_C C' \longrightarrow \mathcal{O}_{X' \times_C C'}(q_1^{-1}(\widetilde{p}^{-1}(\widetilde{U})))$$

is injective and by assumption $\alpha(\sum s_i' F \otimes c_i') = \alpha(\sum r_i' \otimes c_i')$. Hence $\sum s_i' F \otimes c_i' = \sum r_i' \otimes c_i'$ and consequently $s_i' F = r_i'$ on $\widetilde{p}^{-1}(\widetilde{U})$. Therefore $s_i' \in I'$ and $s'' \in I' \otimes_C C'$ as desired.

Now it follows from the above claim and faithfully flat descent for modules (see e.g. [1, Chapter VIII, Lemme 1.6, p. 199]) that there exists an ideal I of R such that $I' = I \otimes_C C'$. Because R is Noetherian and $\phi : R \to R$ injective the same is true for $R' = R \otimes_C C'$. (Every constant extension of fields is ϕ-separable by Lemma 1.5.3 and so it follows from Proposition 1.5.2 (5) that $\phi : R' \to R'$ is injective.) In particular R' is RAAD by Lemma 2.2.2. Thus it follows from Lemma 2.2.5 that $I' \nsubseteq \mathfrak{q}_i'$ for every $i = 1, \ldots, n$. Therefore $I \nsubseteq \mathfrak{q}$ and we can find $s \in R \smallsetminus \mathfrak{q}$ and $r' \in R'$ such that $sF = r'$ on $\widetilde{p}^{-1}(\widetilde{U})$.

Set $R'' = R \otimes_C C' \otimes_C C'$, $X'' = X' \times_C C' = \phi\text{-Spec}(R'')$ and let $i_1, i_2 : R' \to R''$ denote the two canonical maps. We know that $i_1(r') = i_2(r')$ on $q_1^{-1}(\widetilde{p}^{-1}(\widetilde{U}))$. By Lemma 3.8.4 every $\mathfrak{q}'' \in \operatorname{Spec}(R'')$ with $\mathfrak{q}'' \cap R = \mathfrak{q}$ belongs to $\phi\text{-Spec}(R'')$. Therefore it follows that $\frac{i_1(r') - i_2(r')}{1} = 0 \in R''_{\mathfrak{q}''}$ for every $\mathfrak{q}'' \in \operatorname{Spec}(R)$ with $\mathfrak{q}'' \cap R = \mathfrak{q}$. Again by prime avoidance there exists an $s'' \in R''$ with $s'' \notin \mathfrak{q}''$ for all $\mathfrak{q}'' \in \operatorname{Spec}(R)$ with $\mathfrak{q}'' \cap R = \mathfrak{q}$ and $s''(i_1(r') - i_2(r')) = 0 \in R''$. By Lemma 3.8.3 there exists $s_1 \in R \smallsetminus \mathfrak{q}$ such that $s_1(i_1(r') - i_2(r')) = 0$. So $i_1(s_1 r') = i_2(s_1 r')$ and consequently $s_1 r' \in R$ ([1, Corollaire 1.5, Chapter VIII, p. 198]), say $s_1 r' = r_1 \in R$. Then $s s_1 F = s_1 r' = r_1$ on $\widetilde{p}^{-1}(\widetilde{U})$, i.e. $f_{\widetilde{x}}^{\sharp}(\frac{r_1}{s s_1}) = (\widetilde{U}, F)$ showing that $f_{\widetilde{x}}^{\sharp}$ is surjective. □

Remark 3.8.7. *An alternative formulation of Lemma 3.8.6 is the following: The projection $X \times_C C' \to X$ is the coequalizer of the two canonical maps*

$$X \times_C C' \times_C C' \rightrightarrows X \times_C C'.$$

Proof of Proposition 3.8.2: Let $f' : X_1' \to X_2'$ be a morphism of ϕ-spaces over C' which is compatible with the natural descent data. We have to show that there exists a unique $f : X_1 \to X_2$ making

$$\begin{tikzcd}
X_1' \arrow[r, "f'"] \arrow[d] & X_2' \arrow[d] \\
X_1 \arrow[r, dotted, "f"] & X_2
\end{tikzcd}$$

commutative. Set $X_1'' = X_1 \times_C C' \times_C C'$ and $X_2'' = X_2 \times_C C' \times_C C'$. To say that f' is compatible with descend data means that the two maps from X_1'' to X_2'' induced by f'

agree.

$$\begin{tikzcd}
X_1'' \arrow[r] \arrow[d, shift left] \arrow[d, shift right] & X_2'' \arrow[d, shift left] \arrow[d, shift right] \\
X_1' \arrow[r, "f'"] \arrow[d] & X_2' \arrow[d, "p"] \\
X_1 \arrow[r, dotted, "f"] & X_2
\end{tikzcd}$$

As illuminated in the above diagram this implies that pf' coequalizes $X_1'' \rightrightarrows X_1'$. Therefore the desired f exists by Lemma 3.8.6 (and Remark 3.8.7.) $\square$

From Proposition 3.8.2 we obtain the following corollary.

Corollary 3.8.8. *Let $C'|C$ be a finite field extension and X_1, X_2 ϕ-spaces over C that can be covered by open Φ-stable subsets of the form ϕ-*Spec*(R) where R is a Noetherian C-ϕ-algebra with $\phi : R \to R$ injective. Set $X_1' = X_1 \times_C C'$, $X_2' = X_2 \times_C C'$ and assume that there exists an isomorphism $f' : X_1' \to X_2'$ of ϕ-spaces over C' which is compatible with the natural descent data. Then X_1 and X_2 are isomorphic as ϕ-spaces over C.*

Proof: One immediately checks that also $g' = f'^{-1}$ is compatible with the descent data. By Proposition 3.8.2 there exist $f : X_1 \to X_2$ and $g : X_2 \to X_1$ such that $f' = f \times \mathrm{id}$ and $g' = g \times \mathrm{id}$. As $(gf) \times \mathrm{id} = g'f'$ is the identity on X_1' it follows again from Proposition 3.8.2 that also $gf = \mathrm{id}$, similarly for fg. $\square$

Now we are prepared to prove the main result of this work without restrictions on the constants.

Theorem 3.8.9 (Main Theorem)**.** *Let $L|K$ be a ϕ-Galois extension of ϕ-pfields. Then ϕ-*Spec*$(L \otimes_K L)$ is split over L.*

Proof: Let $X = \phi\text{-Spec}(L \otimes_K L)$ and $C = K^\phi = L^\phi$. We already know from Proposition 3.7.5 that there exists a finite algebraic field extension C' of C and a scheme $\mathcal{G}'$ of finite type over C' such that

$$X' = L' \times_{C'} \mathcal{G}',$$

where $X' = X \times_C C'$ and $L' = L \otimes_C C'$. We note that X' comes equipped with a natural descent datum $\varphi : X' \times_C C' \to C' \times_C X'$. Because

$$X' \times_C C' = (L' \times_{C'} \mathcal{G}') \times_C C' = L' \times_{C'} (\mathcal{G}' \times_C C')$$

it follows from Theorem 2.5.2 that $(X' \times_C C')^\phi = \mathcal{G}' \times_C C'$. Similarly $(C' \times_C X')^\phi = C' \times_C \mathcal{G}'$. Therefore we obtain a descent datum

$$\varphi^\phi : \mathcal{G}' \times_C C' \to C' \times_C \mathcal{G}'$$

on $\mathcal{G}'$. By virtue of the constant functor one easily checks that the cocycle condition is preserved. As explained in the proof of Theorem 3.2.4 the scheme $\mathcal{G}'$ can naturally be equipped with the structure of a group scheme over C'. Therefore we can apply Proposition 3.8.1 to find a scheme $\mathcal{G}$ over C and an isomorphism $\mathcal{G} \times_C C' \simeq \mathcal{G}'$ compatible with descent data. By [15, Proposition 2.7.1, p. 29] we know that $\mathcal{G}$ is of finite type over C. We have

$$X \times_C C' = X' = L' \times_{C'} \mathcal{G}' = (L \times_C C') \times_{C'} (\mathcal{G} \times_C C') = (L \times_C \mathcal{G}) \times_C C'$$

and these identifications are compatible with the descent data. To apply Corollary 3.8.8 we need to know that X and $L \times_C \mathcal{G}$ can be covered with open Φ-stable subset of the form ϕ-Spec(R) where R is a Noetherian C-ϕ-algebra with $\phi : R \to R$ injective. This is clear for X because $L \otimes_K L$ is Noetherian and $\phi : L \otimes_K L \to L \otimes_K L$ is injective by Lemma 3.3.16. We can cover $\mathcal{G}$ with open affines Spec(D_i) where D_i is a finitely generated C-algebra. Then ϕ-Spec$(L \otimes_C D_i)$ is an open Φ-stable covering of $L \times_C \mathcal{G}$. Clearly $L \otimes_C D_i$ is Noetherian and it follows from Proposition 1.4.15 that ϕ is injective on $L \otimes_C D_i$.

Summarily we see that we can apply Corollary 3.8.8 to conclude that $X \simeq L \times_C \mathcal{G}$. □

3.9 Elaboration of the main theorem

In the previous section we established the main result, namely that ϕ-Spec$(L \otimes_K L)$ is split for every ϕ-Galois extension $L|K$. In this section we show that the converse is also true (under some mild technical assumptions).

Proposition 3.9.1. *Let $L|K$ be an extension of ϕ-pfields such that L is finitely generated as total ring over K and ϕ is injective on $L \otimes_K L$ (e.g. $L|K$ is ϕ-separable). If $X = \phi$-*Spec$(L \otimes_K L)$ *is split then $L|K$ is generically ϕ-normal and ϕ-normal with respect to the class of all ϕ-pfield extensions of K.*

Proof: To prove that $L|K$ is ϕ-normal with respect to the class of ϕ-pfield extensions of K it suffices by Lemma 3.3.7 to show that $k(\mathfrak{p}) = Lk(\mathfrak{p})^\phi$ for every ϕ-prime ideal $\mathfrak{p}$ of $L \otimes_K L$. By Theorem 2.4.4 the ϕ-prime ideal $\mathfrak{p}$ corresponds to a unique point $y \in X^\phi$. By assumption X^ϕ is a scheme (of finite type over $C = K^\phi = L^\phi$) and we can find an open affine neighborhood $U = \mathrm{Spec}(D)$ of y. Here D is a constant finitely generated C-algebra. Then $V = \pi_X^{-1}(U) \simeq L \times_C U = \phi$-Spec$(L \otimes_C D)$ is an open Φ-stable subset of X containing all the minimal prime ideals of $\mathfrak{p}$. Let $\mathfrak{p}'$ denote the ϕ-prime ideal of $L \otimes_C D$ which corresponds to $\mathfrak{p}$ under the L-isomorphism $V \simeq \phi$-Spec$(L \otimes_C D)$. As $R = L \otimes_K L$ and $L \otimes_C D$ are both Noetherian and RAAD (Lemma 2.2.2 and Lemma 2.2.3) we obtain from Lemma 2.2.9 an L-ϕ-isomorphism

$$R_\mathfrak{p} \simeq (L \otimes_C D)_{\mathfrak{p}'}$$

of ϕ-local rings. Passing to the residue ϕ-pfields yields $k(\mathfrak{p}) = Lk(\mathfrak{p})^\phi$.

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ denote the minimal ϕ-prime ideals of $R = L \otimes_K L$. By Proposition 1.7.3 the endomorphism ϕ extends to $\mathfrak{Q}(R)$ and

$$\mathfrak{Q}(R) = R_{\mathfrak{p}_1} \oplus \cdots \oplus R_{\mathfrak{p}_m}.$$

Now let $\sigma = (\sigma_s, \sigma_t)$ be given by $\sigma_s : L \to \mathfrak{Q}(R),\ a \mapsto a \otimes 1$ and $\sigma_t : L \to \mathfrak{Q}(R),\ a \mapsto 1 \otimes a$. We will show that $L|K$ is ϕ-normal with respect to σ. For this it suffices to see that $R_{\mathfrak{p}_i} \subset L\mathfrak{Q}(R)^\phi \subset \mathfrak{Q}(R)$ for $i = 1, \dots, m$. For simplicity we restrict to the case $i = 1$. As seen above every element s of $R_{\mathfrak{p}_1}$ is of the form

$$s = \frac{\sum a_i c_i}{\sum b_j d_j}$$

with a_i, b_j in the image of $L \to R_{\mathfrak{p}_1},\ a \mapsto \frac{a \otimes 1}{1}$ and $c_i, d_j \in (R_{\mathfrak{p}_1})^\phi$. We denote for $i = 1, \dots, m$ with e_i the idempotent element of $\mathfrak{Q}(R)$ corresponding to the identity element of $R_{\mathfrak{p}_i}$. Clearly $e_1, \dots, e_m \in \mathfrak{Q}(R)^\phi$. As $\sum b_j d_j$ is invertible in $R_{\mathfrak{p}_1}$ we see that

$$\sum b_j d_j + e_2 + \cdots + e_m \in L \cdot \mathfrak{Q}(R)^\phi$$

is invertible in $\mathfrak{Q}(R)$. Indeed

$$\frac{1}{\sum b_j d_j} + e_2 + \cdots + e_m = \frac{1}{\sum b_j d_j + e_2 + \cdots + e_m} \in L\mathfrak{Q}(R)^\phi.$$

Multiplying this equation with $e_1 \in \mathfrak{Q}(R)^\phi$ yields $\frac{1}{\sum b_j d_j} \in L\mathfrak{Q}(R)^\phi$. Therefore

$$s = \frac{\sum a_i c_i}{\sum b_j d_j} \in L\mathfrak{Q}(R)^\phi.$$

□

Remark 3.9.2. *It follows from the above proof that if $L|K$ is ϕ-Galois then $L|K$ is ϕ-normal with respect to $\sigma_s, \sigma_t : L \to (L \otimes_K L)_\mathfrak{p}$ defined by $\sigma_s(a) = \frac{a \otimes 1}{1}$ and $\sigma_t(a) = \frac{1 \otimes a}{1}$ for every ϕ-prime ideal $\mathfrak{p}$ of $L \otimes_K L$.*

This is the fully adorned version of the main theorem:

Theorem 3.9.3. *Let $L|K$ be an extension of ϕ-pfields such that*

(i) *L is finitely generated as total ring over K,*

(ii) *$L|K$ is ϕ-separable,*

(iii) *L has bounded periodicity and*

(iv) *$L^\phi = K^\phi$.*

Then the following three statements are equivalent.

(1) *$L|K$ is ϕ-Galois, i.e. generically ϕ-normal and ϕ-normal with respect to ϕ-pfield extensions of K.*

(2) *ϕ-*Spec*$(L \otimes_K L)$ is split.*

(3) *The functor* Gal$(L|K)$ *is representable by a group scheme* $\mathcal{G}$ *and* $Z = \phi\text{-Spec}(L)$ *is a* $\mathcal{G}$*-torsor.*

Proof: By Theorem 3.8.9 we know that (1) implies (2). It follows from Proposition 3.9.1 that (2) implies (1). The equivalence of (2) and (3) was already proved in Theorem 3.2.4. □

3.10 The Galois correspondence

Rather unsurprisingly in this section we will establish the Galois correspondence.

Definition 3.10.1. *Let* $L|K$ *be a* ϕ*-Galois extension of* ϕ*-pfields. By Theorem 3.9.3 we know that*

$$\mathcal{G} = \mathcal{G}(L|K) = \phi\text{-Spec}(L \otimes_K L)^\phi$$

is a group scheme of finite type over $C = K^\phi = L^\phi$*. We call it the* ϕ-Galois group scheme of $L|K$*.*

By Theorem 3.9.3 we also know that $\mathcal{G}$ acts naturally (from the right) on $Z = \phi\text{-Spec}(L)$ and that Z is a $\mathcal{G}$-torsor, i.e. $Z \times_C \mathcal{G} \simeq Z \times_K Z$. Moreover $\mathcal{G}$ represents the Galois group functor Gal$(L|K)$.

Proposition 3.10.2. *Let* $L|K$ *be a* ϕ*-Galois extension and* $K \subset M \subset L$ *an intermediate* ϕ*-pfield. Then* Gal$(L|M)$ *is a closed subgroup functor of* Gal$(L|K)$*.*

In more detail: If $\mathfrak{a} \subset L \otimes_K L$ *denotes the* ϕ*-ideal generated by the elements of the form* $a \otimes 1 - 1 \otimes a$ *with* $a \in M$ *then applying the constant functor to the closed* ϕ*-subspace* $\phi\text{-Spec}(L \otimes_K L/\mathfrak{a}) \hookrightarrow \phi\text{-Spec}(L \otimes_K L)$ *yields a closed subscheme* $\mathcal{H} \hookrightarrow \mathcal{G}$ *that represents* Gal$(L|M)$*.*

Proof: Obviously Gal$(L|M)$ is a subgroup functor of Gal$(L|K)$. Let $\mathfrak{a} \subset L \otimes_K L$ denote the ϕ-ideal generated by $a \otimes 1 - 1 \otimes a$ with $a \in M$ and

$$W = \phi\text{-Spec}(L \otimes_K L/\mathfrak{a}) \hookrightarrow \phi\text{-Spec}(L \otimes_K L) = Z \times_K Z$$

the closed ϕ-subspace induced by $\mathfrak{a}$. As in the proof of Theorem 3.2.4 we have for every Y of finite type over C a functorial identification

$$\text{Gal}(L|K)(Y) = \text{Hom}_Z(Z \times_C Y, Z \times_K Z).$$

If $\sigma \in \text{Gal}(L|K)(Y)$, then $\sigma \in \text{Gal}(L|M)(Y)$ if and only if $\Gamma(\sigma)(\Gamma(p_Z)(a)) = \Gamma(p_Z)(a)$ for all $a \in M$ where $p_Z : Z \times_C Y \to Z$ denotes the projection onto the first factor. Thus, under the above identification Gal$(L|M)(Y)$ corresponds to those $\sigma \in \text{Hom}_Z(Z \times_C Y, Z \times_K Z)$ such that

$$\Gamma(\sigma)(\Gamma(p_2)(a)) = \Gamma(p_Z)(a) \ \forall a \in M \tag{3.7}$$

where $p_2 : Z \times_K Z \to Z$ denotes the projection onto the second factor. According to Theorem 2.1.11 every $\sigma \in \text{Hom}_Z(Z \times_C Y, Z \times_K Z)$ is induced from a morphism

$\sigma^* : L \otimes_K L \to \mathcal{O}_{Z\times_C Y}(Z \times_C Y)$. Now condition (3.7) precisely means that $\mathfrak{a}$ lies in the kernel of σ^*, which in turn is equivalent to saying that σ factors through W, i.e.

$$\begin{tikzcd}
Z \times_C Y \arrow[rr, "\sigma"] \arrow[dr, dotted] & & Z \times_K Z \\
& W \arrow[ur, hook] &
\end{tikzcd}$$

By Lemma 2.5.6, the closed ϕ-subspace W of $Z \times_K Z$ is split and $\mathcal{H} = W^\phi$ is a closed subscheme of $(Z \times_K Z)^\phi = \mathcal{G}$. Thus it follows from Corollary 2.5.3 that $\mathrm{Gal}(L|M)$ corresponds to $\mathrm{Hom}_C(Y, \mathcal{H})$ under the identification $\mathrm{Gal}(L|K)(Y) = \mathrm{Hom}_C(Y, \mathcal{G})$. □

Let $L|K$ be ϕ-Galois and let H be a subgroup functor of $\mathrm{Gal}(L|K)$. We say that $a \in L$ is *invariant under* H if

$$\Gamma(\sigma)(\Gamma(p_Z)(a)) = \Gamma(p_Z)(a)$$

for all Y and all $\sigma \in H(Y)$. Here $p_Z : Z \times_C Y \to Z$ denotes the projection onto the first factor. We set

$$L^H = \{a \in L;\ a \text{ is invariant under } H\}.$$

Let $\mathcal{H} \hookrightarrow \mathcal{G} = \mathcal{G}(L|K)$ be a closed subgroup scheme. Then we have an induced action

$$\rho_{\mathcal{H}} : Z \times_C \mathcal{H} \to Z \times_C \mathcal{G} \to Z$$

of $\mathcal{H}$ on $Z = \phi\text{-Spec}(L)$ and the closed ϕ-subspace

$$Z \times_C \mathcal{H} \hookrightarrow Z \times_C \mathcal{G} = \phi\text{-Spec}(L \otimes_K L)$$

is induced from a morphism $\psi : L \otimes_K L \to \mathcal{O}_{Z\times_C \mathcal{H}}(Z \times_C \mathcal{H})$. If H denotes the closed subfunctor of $\mathrm{Gal}(L|K)$ represented by $\mathcal{H} \hookrightarrow \mathcal{G}$, then – chasing through the identifications made in the proof of Theorem 3.2.4 – we see that for $a \in L$ the following are equivalent (cf. Lemma 3.1.11):

(1) a is invariant under H

(2) $\Gamma(\rho_{\mathcal{H}})(a) = \Gamma(p_Z)(a)$

(3) $a \otimes 1 - 1 \otimes a \in \ker \psi$.

Lemma 3.10.3. *Let $L|K$ be a ϕ-Galois extension and H a subgroup functor of* $\mathrm{Gal}(L|K)$*. Then L^H is a sub ϕ-pfield of L containing K, i.e. L^H is an intermediate ϕ-pfield of $L|K$.*

Proof: It is obvious that L^H is a ϕ-ring containing K. Let a be a non zero divisor of L^H. Then it follows from Lemma 1.3.4 that a is a non zero divisor in L, i.e a is invertible in L. Because $a \in L^H$ also $a^{-1} \in L^H$. Hence L^H is a total ring. By Lemma 1.3.4, this implies that L^H is a ϕ-pfield. □

We shall need the following technical lemma.

Lemma 3.10.4. *Let L be a ϕ-pfield and Y a scheme of finite type over $C = L^{\phi}$. Set $Z = \phi$-Spec(L) and let R denote the difference ring of global sections of $Z \times_C Y$. Then $\phi : R \to R$ is injective and R is ϕ-separable over L.*

Proof: We first show that ϕ is injective on R. The problem is local and so we can assume that $R = \widehat{L \otimes_C D}$ where D is a finitely generated C-algebra. It follows from Lemma 2.2.3 that $L \otimes_C D$ is Noetherian and RAAD. Thus $\iota : L \otimes_C D \to \widehat{L \otimes_C D}$ is injective by Lemma 2.2.7. Now let $F \in \widehat{L \otimes_C D}$ with $\phi(F) = 0$. Fix $\mathfrak{q} \in \phi$-Spec$(L \otimes_C D)$. By Lemma 2.2.5 there exist $a, b \in L \otimes_C D$, $b \notin \mathfrak{q}$ such that $\widehat{b}F = \widehat{a}$. As $\phi(F) = 0$ it follows that $\phi(\widehat{a}) = 0$, but as ϕ is injective on $L \otimes_C D$ it follows that $a = 0$. Therefore $\frac{b}{1}F(\mathfrak{q}) = 0 \in (L \otimes_C D)_{\mathfrak{q}}$. Because $b \notin \mathfrak{q}$ this implies $F(\mathfrak{q}) = 0$. Because $\mathfrak{q}$ was arbitrary we can conclude that $F = 0$.

Next we want to show that R is ϕ-separable. Let M be a ϕ-pfield extension of L and D a finitely generated C-algebra. First we will show that ϕ is injective on $\widehat{L \otimes_C D} \otimes_L M$.

Let $L = e_1 L \oplus \cdots \oplus e_t L$ and $\{m_{ij}\}_{j \in J_i}$ an $e_i L$-basis of $e_i M$ for $i = 1, \dots, t$. Then every element x of $\widehat{L \otimes_C D} \otimes_L M$ is uniquely of the form

$$x = \sum_{i=1}^{t} \sum_{j \in J_i} F_{ij} \otimes m_{ij}$$

with $F_{ij} \in e_i \widehat{L \otimes_C D}$. Assume that $\phi(x) = 0$ and fix $\mathfrak{q} \in \phi$-Spec$(L \otimes_C D)$. By Lemma 2.2.5 there exist $b \in L \otimes_C D \smallsetminus \mathfrak{q}$ and $a_{ij} \in L \otimes_C D$ such that $\widehat{b}F_{ij} = \widehat{a_{ij}}$ for all i, j. In particular $\widehat{a_{ij}} \in e_i \widehat{L \otimes_C D}$. We have

$$0 = \phi(\widehat{b} \otimes 1 \cdot x) = \phi\left(\sum_{i=1}^{t} \sum_{j \in J_i} \widehat{a_{ij}} \otimes m_{ij}\right). \tag{3.8}$$

As $\iota : L \otimes_C D \to \widehat{L \otimes_C D}$ is injective also $(L \otimes_C D) \otimes_L M \to \widehat{L \otimes_C D} \otimes_L M$ is injective. Now ϕ is injective on $(L \otimes_C D) \otimes_L M = M \otimes_C D$ by Proposition 1.4.15. Therefore it follows from equation 3.8 that $\sum_i \sum_j \widehat{a_{ij}} \otimes m_{ij} = 0$. Because $\widehat{a_{ij}} \in e_i \widehat{L \otimes_C D}$ we know that $\widehat{a_{ij}} = 0$ and so $a_{ij} = 0$ for all i, j. Hence $\frac{b}{1}F_{ij}(\mathfrak{q}) = 0 \in (L \otimes_C D)_{\mathfrak{q}}$ and so $F_{ij}(\mathfrak{q}) = 0$. Because $\mathfrak{q}$ was arbitrary we can conclude that $F_{ij} = 0$ and so $x = 0$. Thus we have shown that ϕ is injective on $\widehat{L \otimes_C D} \otimes_L M$.

We have to prove that ϕ is injective on $R \otimes_L M$. As above an element x of $R \otimes_L M$ is uniquely of the form

$$x = \sum_{i=1}^{t} \sum_{j \in J_i} F_{ij} \otimes m_{ij}$$

with $F_{ij} \in e_i R$. Assume $\phi(x) = 0$. We can cover $Z \times_C Y$ with open Φ-stable subsets of the form $U = \phi$-Spec$(L \otimes_C D)$ where D is a finitely generated C-algebra. The restriction map $R \to \widehat{L \otimes_C D}$ is a morphism of ϕ-rings and so is $R \otimes_L M \to \widehat{L \otimes_C D} \otimes_L M$. Because ϕ is injective on $\widehat{L \otimes_C D} \otimes_L M$ we can conclude that the image of x in $\widehat{L \otimes_C D} \otimes_L M$ is zero. As the restriction of F_{ij} to ϕ-Spec$(L\otimes_C D)$ lies in $e_i\widehat{L\otimes_C D}$ this implies that the restriction of F_{ij} to ϕ-Spec$(L\otimes_C D)$ is zero. Hence $F_{ij}=0$ for all i,j and so $x=0$. □

Now we are prepared to prove the first half of the Galois correspondence.

Lemma 3.10.5. *Let $L|K$ be a ϕ-Galois extension of ϕ-pfields and H a closed subgroup functor of* Gal$(L|K)$*. Then $L|L^H$ is a ϕ-Galois extension of ϕ-pfields and*

$$\operatorname{Gal}(L|L^H)=H.$$

Proof: Let $\mathcal{H}\hookrightarrow\mathcal{G}=\mathcal{G}(L|K)$ denote the closed subgroup scheme that represents H. As explained in Proposition 2.5.7 the closed ϕ-subspace

$$Z\times_C\mathcal{H}\hookrightarrow Z\times_C\mathcal{G}=\phi\text{-Spec}(L\otimes_K L)$$

is induced by $\mathfrak{a}=\ker(L\otimes_K L\to\mathcal{O}_{Z\times_C\mathcal{H}}(Z\times_C\mathcal{H}))$. We know from Lemma 3.10.4 that ϕ is injective on $\mathcal{O}_{Z\times_C\mathcal{H}}(Z\times_C\mathcal{H})$. Therefore $\mathfrak{a}$ is a reflexive ϕ-ideal. Moreover $\mathcal{O}_{Z\times_C\mathcal{H}}(Z\times_C\mathcal{H})$ is ϕ-separable over L (Lemma 3.10.4). As $L\otimes_K L/\mathfrak{a}\hookrightarrow\mathcal{O}_{Z\times_C\mathcal{H}}(Z\times_C\mathcal{H})$ this implies that $L\otimes_K L/\mathfrak{a}$ is also ϕ-separable over L by Lemma 1.5.6.

Next we will show that $\mathfrak{a}$ is a ϕ-coideal of $L\otimes_K L$. We consider $Z\times_C\mathcal{G}$ with its natural groupoid structure (as action groupoid, cf. Example 3.1.2). Because $\mathcal{H}$ is a closed subgroup scheme of $\mathcal{G}$ acting on $Z=\phi$-Spec(L) via the induced action it is clear that $Z\times_C\mathcal{H}$ is a closed ϕ-subgroupoid of $Z\times_C\mathcal{G}$. We know from Theorem 3.2.4 that $Z\times_C\mathcal{G}$ and $Z\times_K Z$ are isomorphic as groupoids. So we have a commutative diagram of groupoids

$$\begin{tikzcd}
Z\times_C\mathcal{G} \arrow[r, "\simeq"] & Z\times_K Z=\phi\text{-Spec}(L\otimes_K L) \\
Z\times_C\mathcal{H} \arrow[u, hook] \arrow[r, "\simeq"] & \phi\text{-Spec}(L\otimes_K L/\mathfrak{a}) \arrow[u, hook]
\end{tikzcd}$$

In particular ϕ-Spec$(L\otimes_K L/\mathfrak{a})$ is a closed ϕ-subroupoid of ϕ-Spec$(L\otimes_K L)$ and this implies that there is a well defined map

$$L\otimes_K L/\mathfrak{a}\longrightarrow(L\otimes_K L/\mathfrak{a})\widehat{\otimes_L}(L\otimes_K L/\mathfrak{a}),\ \overline{a\otimes b}\mapsto\overline{a\otimes 1}\widehat{\otimes_L}\overline{1\otimes b}.$$

We already noted above that ϕ is injective on $L\otimes_K L/\mathfrak{a}$ and $L\otimes_K L/\mathfrak{a}$ is ϕ-separable as L-algebra. By Proposition 1.5.2 (5) this implies that ϕ is injective on $(L\otimes_K L/\mathfrak{a})\otimes_L(L\otimes_K L/\mathfrak{a})$. Because this ring is Noetherian it follows from Lemma 2.2.2 that it is RAAD and so by Lemma 2.2.7 the canonical map

$$\iota:(L\otimes_K L/\mathfrak{a})\otimes_L(L\otimes_K L/\mathfrak{a})\to(L\otimes_K L/\mathfrak{a})\widehat{\otimes_L}(L\otimes_K L/\mathfrak{a})$$

is injective. This shows that in fact

$$L\otimes_K L/\mathfrak{a}\longrightarrow(L\otimes_K L/\mathfrak{a})\otimes_L(L\otimes_K L/\mathfrak{a}),\ \overline{a\otimes b}\mapsto\overline{a\otimes 1}\otimes_L\overline{1\otimes b}$$

is well defined. To prove that $\mathfrak{a}$ is a coideal it remains to see that $\mathfrak{a}$ lies in the kernel of $L \otimes_K L \to L,\ a \otimes b \mapsto ab$. But this is clear because the groupoid identity $Z \to$ ϕ-Spec$(L \otimes_K L/\mathfrak{a})$ is induced from $L \otimes_K L/\mathfrak{a} \to L,\ \overline{a \otimes b} \to ab$.

We have
$$L^H = \{a \in L;\ a \otimes 1 - 1 \otimes a \in \mathfrak{a}\}$$
and we already know that L^H is a ϕ-pfield (Lemma 3.10.3). Because $\mathfrak{a}$ is a ϕ-coideal it follows from Corollary 3.1.14 that as an ideal $\mathfrak{a}$ is generated by the elements of the form $a \otimes 1 - 1 \otimes a$ with $a \in L^H$. Thus it follows from Proposition 3.10.2 that $\operatorname{Gal}(L|L^H)$ is represented by ϕ-Spec$(L \otimes_K L/\mathfrak{a})^\phi = (Z \times_C \mathcal{H})^\phi = \mathcal{H}$, i.e. $\operatorname{Gal}(L|L^H) = H$.

We still have to show that $L|L^H$ is ϕ-Galois. Conditions (1), (2) and (3) of Definition 3.3.10 are trivially satisfied. Because $L \otimes_{L^H} L \simeq L \otimes_K L/\mathfrak{a}$ we know that ϕ is injective on $L \otimes_{L^H} L$, also ϕ-Spec$(L \otimes_{L^H} L) = \phi$-Spec$(L \otimes_K L/\mathfrak{a}) = Z \times_C \mathcal{H}$ is split. Thus it follows from Proposition 3.9.1 that also conditions (4) and (5) are satisfied. □

Here comes the second part of the Galois correspondence.

Lemma 3.10.6. *Let $L|K$ be ϕ-Galois and M an intermediate ϕ-pfield such that $\iota : L \otimes_M L \to \widehat{L \otimes_M L}$ is injective. Then*
$$L^{\operatorname{Gal}(L|M)} = M.$$

Proof: Trivially $L^{\operatorname{Gal}(L|M)} \supset M$. Let $\mathfrak{a} \subset R = L \otimes_K L$ denote the ϕ-ideal generated by $a \otimes 1 - 1 \otimes a$ with $a \in M$. Then $L \otimes_M L \simeq L \otimes_K L/\mathfrak{a}$ and by assumption the canonical map $\iota : R/\mathfrak{a} \to \widehat{R/\mathfrak{a}}$ is injective. Consider the closed ϕ-subspace
$$W = \phi\text{-Spec}(R/\mathfrak{a}) \hookrightarrow \phi\text{-Spec}(R) = Z \times_K Z$$
induced by $\mathfrak{a}$. We see from Proposition 3.10.2 that $W = Z \times_C \mathcal{H}$ is split and that $\operatorname{Gal}(L|M)$ is represented by $\mathcal{H}$. Because

$$\begin{tikzcd}
W \arrow[dr, hook] \arrow[dd, "\simeq"'] & \\
& Z \times_K Z = Z \times_C \mathcal{G} \\
Z \times_C \mathcal{H} \arrow[ur, hook] &
\end{tikzcd}$$

commutes we infer that
$$\ker(R \to \mathcal{O}_{Z \times_C \mathcal{H}}(Z \times_C \mathcal{H})) = \ker(R \to \widehat{R/\mathfrak{a}}).$$

Because $R/\mathfrak{a} \to \widehat{R/\mathfrak{a}}$ is injective it follows that $\mathfrak{a}$ agrees with the kernel of $R \to \mathcal{O}_{Z \times_C \mathcal{H}}(Z \times_C \mathcal{H})$. Summarily we arrive at
$$\begin{aligned} L^{\operatorname{Gal}(L|M)} &= \{a \in L;\ a \otimes 1 - 1 \otimes a \in \ker(L \otimes_K L \to \mathcal{O}_{Z \times_C \mathcal{H}}(Z \times_C \mathcal{H}))\} = \\ &= \{a \in L;\ a \otimes 1 - 1 \otimes a \in \mathfrak{a}\} = M. \end{aligned}$$

The last identity was already observed in Theorem 3.1.17. □

Now it is a simple matter to combine the above results to obtain the Galois correspondence.

Theorem 3.10.7 (Galois correspondence)**.** *Let $L|K$ be a ϕ-Galois extension of ϕ-pfields. Then there is a one-to-one correspondence between the intermediate ϕ-pfields M of $L|K$ such that $L|M$ is ϕ-Galois and the closed subgroup functors of* $\mathrm{Gal}(L|K)$*.*

In detail: If $K \subset M \subset L$ is an intermediate ϕ-pfield such that $L|M$ is ϕ-Galois then $\mathrm{Gal}(L|M)$ *is a closed subgroup functor of* $\mathrm{Gal}(L|K)$*. If H is a closed subgroup functor of* $\mathrm{Gal}(L|K)$ *then L^H is an intermediate ϕ-pfield of $L|K$ such that $L|L^H$ is ϕ-Galois. These two constructions are inverse to each other.*

Proof: By Proposition 3.10.2, Lemma 3.10.5 and Lemma 3.10.6 it suffices to see that $\iota : L \otimes_M K \to \widehat{L \otimes_M} L$ is injective if $L|M$ is ϕ-Galois. But this follows from Lemma 2.2.7 because $L \otimes_M L$ is RAAD by Lemma 3.3.16. □

It is not clear if *all* intermediate ϕ-pfields appear in the Galois correspondence. By Theorem 3.10.7 only those intermediate ϕ-pfields M such that $L|M$ is ϕ-Galois appear in the correspondence. It is an open question if $L|M$ is ϕ-Galois for every intermediate ϕ-pfield M of $L|K$ (see Section 3.12). However there is the following lemma.

Lemma 3.10.8. *Let $L|K$ be a ϕ-Galois extension and M an intermediate ϕ-pfield of $L|K$. Then the following are equivalent:*

(1) *$L|M$ is ϕ-Galois.*

(2) *$L|M$ is ϕ-separable.*

(3) *The endomorphism ϕ is injective on $L \otimes_M L$.*

(4) *The canonical map $\iota : L \otimes_M L \to \widehat{L \otimes_M} L$ is injective.*

Proof: The implication (1) ⇒ (2) follows from Lemma 3.3.9. Then (2) ⇒ (3) is trivial and (3) ⇒ (4) follows from Lemma 2.2.7 because $L \otimes_M L$ is RAAD by Lemma 2.2.2. Finally if (4) is satisfied then $M = L^{\mathrm{Gal}(L|M)}$ by Lemma 3.10.6 and $L|M$ is ϕ-Galois by Lemma 3.10.5. □

Remark 3.10.9. *Let $L|K$ be ϕ-Galois. If $L|K$ is Picard-Vessiot then for every intermediate ϕ-pfield M of $L|K$ the extension $L|M$ is ϕ-Galois. Therefore in the Picard-Vessiot case the Galois correspondence is between all closed subgroup functors and all intermediate ϕ-pfields.*

Proof: It is immediate from the definition of Picard-Vessiot extensions (Definition 3.3.5) that $L|M$ is Picard-Vessiot and so $L|M$ is ϕ-Galois by Example 3.3.11. □

Remark 3.10.10. *Let $L|K$ be ϕ-Galois and assume that L and K are inversive. Then for an intermediate ϕ-pfield M the extension $L|M$ is ϕ-Galois if and only if M is inversive. In particular the Galois correspondence is between all closed subgroup functors and all* inversive *intermediate ϕ-pfields. It is however not clear if every intermediate ϕ-pfield is inversive.*

Proof: By Theorem 3.10.7 it suffices to show that L^H is inversive for every closed subgroup functor of $\operatorname{Gal}(L|K)$. But this is immediate because then the ϕ-rings appearing in the definition of invariance are inversive. □

Corollary 3.10.11. *If K is an inversive ϕ-pfield and $L|K$ a Picard-Vessiot extension then also L is inversive. Moreover if L has bounded periodicity (e.g. $K^\phi = L^\phi$ is algebraically closed), then every intermediate ϕ-pfield of $L|K$ is inversive.*

Proof: It is immediate from the definition (3.3.5) that L is inversive. The claim follows from Remarks 3.10.9 and 3.10.10. □

3.11 Examples

In this last section we present some very simple concrete examples of ϕ-Galois extensions.

It was already observed in Example 3.3.11 that a Picard-Vessiot extension with algebraically closed constants (or more generally with bounded periodicity) is ϕ-Galois. As one expects, in the Picard-Vessiot case the Galois group we have constructed here agrees with the usual Galois group, as for example defined in [43]. This is easily seen as follows: Let $L|K$ be a Picard-Vessiot extension with algebraically closed constants C and $R \subset L$ the Picard-Vessiot ring. The torsor theorem yields the basic isomorphism of difference rings $R \otimes_K R \simeq R \otimes_C C[\mathcal{G}]$ where $C[\mathcal{G}] = (R \otimes_K R)^\phi$ is the coordinate ring of the Galois group (in the sense of [43]). Let $Z = \phi\text{-Spec}(L)$. Because R is ϕ-simple $\phi\text{-Spec}(R) = \phi\text{-Spec}(L) = Z$ (see Example 2.1.8). Thus applying $\phi\text{-Spec}(-)$ to the torsor isomorphism we obtain $Z \times_K Z \simeq Z \times_C \mathcal{G}$ and we see that $\mathcal{G} = \phi\text{-Spec}(L \otimes_K L)^\phi$.

Many examples of Picard-Vessiot extension can be found in [43]. However the Picard-Vessiot extensions $L|K$ considered in [43] are inversive and usually it is also assumed that L is separable over K so that the Galois group scheme is reduced. The theory of Frobenius modules (see [32] or [33]) yields examples where these two assumptions are in general not satisfied.

We first give an example of a non-inversive Picard-Vessiot extension. It is an example of a Mahler-difference equation (see [35]). The idea to consider Mahler-difference equations was given to me by Daniel Bertrand and Pierre Nguyen.

Example 3.11.1. Let $K = \mathbb{C}(z)$, $d \geq 2$ an integer and $\phi : \mathbb{C}(z) \to \mathbb{C}(z)$ determined by $\phi(z) = z^d$. Then K is a non-inversive ϕ-field. We work inside the field of meromorphic functions at the origin, which we denote by $\mathcal{M}$. We consider $\mathcal{M}$ as difference field via $\phi(f(z)) = f(z^d)$. By considering the power series expansion of an element in $\mathcal{M}$ one easily sees that $\mathcal{M}^\phi = \mathbb{C}$. Let $f \in \mathcal{M}$ be defined by $f = z + z^d + z^{d^2} + \cdots$. Then f satisfies the Mahler difference equation

$$\phi(f) = f - z.$$

This is a linear but inhomogeneous difference equation. To get something homogeneous we consider the linear system

$$\phi \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 1 & -z \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \tag{3.9}$$

Then $\begin{pmatrix} f \\ 1 \end{pmatrix}$ is a solution of (3.9). If we set $L = K(f) \subset \mathcal{M}$ then L is a difference field and

$$Y = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_n(L)$$

is a fundamental solution matrix for equation (3.9). Thus L is a Picard-Vessiot extension of K (cf. Definition 3.3.5).

Of course one can also give a purely algebraic construction of a Picard-Vessiot extension for $\phi(y) = y - z$ (or the system 3.9 to be more precise): We consider $\mathbb{C}(z)[T]$ as difference ring by $\phi(z) = z^d$ and $\phi(T) = T - z$. (Here T is transcendental over $\mathbb{C}(z)$.) We will show that $\mathbb{C}(z)[T]$ is ϕ-simple. Suppose there exists a proper ϕ-ideal I of $\mathbb{C}(z)[T]$. Then I is of the form $I = (g)$ for a unique monic polynomial g of positive degree in T. We have $\phi(g) \in I$ and because $\phi(g)$ also is monic and of the same degree it follows that $\phi(g) = g$. If we write $g = T^n + g_{n-1}T^{n-1} + \cdots + g_0 \in \mathbb{C}(z)[T]$ then $\phi(g) = (T - z)^n + g_{n-1}(z^d)(T - z)^{n-1} + \cdots + g_0(z^d)$. Comparing the coefficient at T^{n-1} of g and $\phi(g)$ yields $g_{n-1}(z) = g_{n-1}(z^d) - nz$. If we write $g_{n-1}(z) = \frac{a(z)}{b(z)}$ with $a(z), b(z) \in \mathbb{C}[z]$ coprime. Then

$$a(z)b(z^d) = a(z^d)b(z) - nzb(z)b(z^d)$$

and so $b(z^d)$ divides $a(z^d)b(z)$. Because $a(z^d)$ and $b(z^d)$ are coprime it follows that $b(z^d)$ divides $b(z)$. For degree reasons this is only possible if b is constant and so $g_{n-1}(z) \in \mathbb{C}[z]$. But then the equation $g_{n-1}(z) = g_{n-1}(z^d) - nz$ yields a contradiction (by again looking at the degree).

Therefore $\mathbb{C}(z)[T]$ is ϕ-simple and it follows that $\mathbb{C}(z)[T]$ is a Picard-Vessiot ring and $L = \mathbb{C}(z, T)$ a Picard-Vessiot extension of K. From the uniqueness of Picard-Vessiot extensions (with algebraically closed field of constants) it follows that f is transcendental over $\mathbb{C}(x)$. A very similar proof of the transcendence of f can be found in [35, Theorem 1.1.2, p. 3]. Finally it is not difficult to determine the Galois group of $L|K$, it is $\mathbb{G}_a$ acting on $L|K$ by $T \mapsto T + \lambda$ for $\lambda \in \mathbb{G}_a(\mathbb{C})$.

An example of a Picard-Vessiot extension with the non-reduced Group μ_p, the p-th roots of unity in characteristic p can be found in [43, Example 1.14, p. 11]. The following example is not Picard-Vessiot.

Example 3.11.2. Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$ and denote with L the field of meromorphic Λ-periodic functions on $\mathbb{C}$. Choose $a \in \mathbb{C}$ such that $a \notin \mathbb{Q}\Lambda$. We consider L as difference field by $\phi(f(z)) = f(z+a)$.

We will show that L is a ϕ-Galois extension of $K = \mathbb{C}$ (considered as constant field) with Galois group the elliptic curve associated with Λ. We first verify that $L^\phi = \mathbb{C}$. Because $a \notin \mathbb{Q}\Lambda$ the set $\mathbb{Z}a + \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ has an accumulation point. An $f \in L^\phi$ is constant on $\mathbb{Z}a + \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ and thus must be constant. Let $\wp = \wp_\Lambda$ denote the Weierstrass function. It is well known that $L = \mathbb{C}(\wp, \wp')$ and

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3$$

where g_2, g_3 are complex numbers depending on Λ. We have already seen that conditions (1) and (3) of Definition 3.3.10 are satisfied. Condition (2) is also satisfied by Lemma 1.6.5 because $\mathbb{C} = L^\phi$ is algebraically closed.

Let $E \subset \mathbb{P}^2_\mathbb{C}$ denote the elliptic curve defined by the equation

$$Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3.$$

For simplicity we abbreviate $x = \wp$ and $y = \wp'$. Let $u = \wp(a)$ and $v = \wp'(a)$, then $A = [u : v : 1] \in E(\mathbb{C})$. Because $L = \mathbb{C}(x, y)$ is the function field of E and $\phi : L \to L$ is induced by translation with A it follows from Proposition 3.3.8 that L satisfies condition (5). By Corollary 3.3.14 condition (4) is also satisfied. Thus $L|\mathbb{C}$ is ϕ-Galois.

Every $\tau \in E(\mathbb{C})$ induces an $\mathbb{C}$-ϕ-automorphism of L by translation. Using the ideas of the proof of Proposition 3.3.8 it is easy to see that every $\mathbb{C}$-ϕ-automorphism $\tau : L \to L$ is of this form: To use the notation of Proposition 3.3.8 we set $M = L$, $\sigma_s = \mathrm{id}, \sigma_t = \tau : L \to M$. Then, as computed in the proof of Proposition 3.3.8 we have $h_t = h_s c \in E(L)$ with $c \in E(L)^\phi = E(L^\phi) = E(\mathbb{C})$. This identity says that the maps

$$\mathrm{Spec}(L) \xrightarrow{\tau^*} \mathrm{Spec}(L) \xrightarrow{gen} E$$

and

$$\mathrm{Spec}(L) \xrightarrow{gen\cdot c} E \times_\mathbb{C} E \to E$$

agree. Therefore τ is induced from translation with $c \in E(\mathbb{C})$.

3.12 Some open problems/Work for the future

The main goal of this work was to find a setup as general as possible, where a Galois theory for difference equations (with group schemes of finite type as Galois groups) is still well-behaved. Now that this setup has been settled it is an obvious challenge to further develop the theory in this setting. For example, a rather obvious next step would be the second fundamental theorem. Further tasks can be found by looking at the differential theory which is in general better developed.

In the differential setting one can use equations involving the logarithmic derivative to produce strongly normal extensions. Following the lines indicated in the proof of

Proposition 3.3.8 one could try to develop the difference analog: Let K be a difference field with field of constants C, $\mathcal{H}$ a (not necessarily linear) algebraic group over C and $A \in \mathcal{H}(K)$. Imitating the constructions of Picard-Vessiot theory it should be possible to associate to the equation $\phi(Y) = AY$ a "splitting ϕ-pfield" which will then be a ϕ-Galois extension of K.

It would be nice if one could remove condition (5) from the definition of ϕ-Galois (Definition 3.3.10). In the differential setting this is possible. In fact, if all the ϕ-pseudo fields involved would be fields then one could carry over the proof to the difference case. This seems to be one of the rare situations where dealing with ϕ-pseudo fields instead of ϕ-fields really makes things more complicated.

The question, if for an intermediate ϕ-pfield M of a ϕ-Galois extension $L|K$ the extension $L|M$ is also ϕ-Galois is to some extend answered in Lemma 3.10.8. It would be good to know whether or not it can really happen that $L|M$ is not ϕ-Galois. It does not happen if $L|K$ is Picard-Vessiot.

Inside the strongly normal extensions the Picard-Vessiot extensions are characterized by the property that their Galois groups are affine (see [27] and [5]). It would be nice to have a characterization of Picard-Vessiot extensions only in terms of automorphisms or isomorphisms as proposed in the conjecture after Example 3.3.6. It might be better to first approach this conjecture in the differential setting.

Index

Bibliography

[1] *Revêtements étales et groupe fondamental.* Springer-Verlag, Berlin, 1971. Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1), Dirigé par Alexandre Grothendieck. Augmenté de deux exposés de M. Raynaud, Lecture Notes in Mathematics, Vol. 224.

[2] Katsutoshi Amano and Akira Masuoka. Picard-Vessiot extensions of Artinian simple module algebras. *J. Algebra*, 285(2):743–767, 2005.

[3] Katsutoshi Amano, Akira Masuoka, and Mitsuhiro Takeuchi. Hopf algebraic approach to Picard-Vessiot theory. In *Handbook of algebra. Vol. 6*, volume 6 of *Handb. Algebr.*, pages 127–171. Elsevier/North-Holland, Amsterdam, 2009.

[4] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[5] A. Białynicki-Birula. On Galois theory of fields with operators. *Amer. J. Math.*, 84:89–109, 1962.

[6] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)].* Springer-Verlag, Berlin, 1990.

[7] N. Bourbaki. *Algebra. II. Chapters 4–7.* Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1990. Translated from the French by P. M. Cohn and J. Howie.

[8] Nicolas Bourbaki. *Elements of mathematics. Commutative algebra.* Hermann, Paris, 1972. Translated from the French.

[9] Tomasz Brzezinski and Robert Wisbauer. *Corings and comodules*, volume 309 of *London Mathematical Society Lecture Note Series.* Cambridge University Press, Cambridge, 2003.

[10] Richard M. Cohn. *Difference algebra.* Interscience Publishers John Wiley & Sons, New York-London-Sydeny, 1965.

[11] P. Deligne. Catégories tannakiennes. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, pages 111–195. Birkhäuser Boston, Boston, MA, 1990.

[12] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry.* Number 150 in GTM. Springer, 2004.

[13] Barbara Fantechi, Lothar Göttsche, Luc Illusie, Steven L. Kleiman, Nitin Nitsure, and Angelo Vistoli. *Fundamental algebraic geometry*, volume 123 of *Mathematical Surveys and Monographs.* American Mathematical Society, Providence, RI, 2005. Grothendieck's FGA explained.

[14] A. Grothendieck. Éléments de géométrie algébrique. I. Le langage des schémas. *Inst. Hautes Études Sci. Publ. Math.*, (4):228, 1960.

[15] A. Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II. *Inst. Hautes Études Sci. Publ. Math.*, (24):231, 1965.

[16] Alexander Grothendieck. *Fondements de la géométrie algébrique (FGA). [Extraits du Séminaire Bourbaki, 1957–1962.].* Secrétariat mathématique, Paris, 1962.

[17] Robin Hartshorne. *Algebraic Geometry.* Number 52 in GTM. Springer, 1977.

[18] Ehud Hrushovski. The elementary theory of the Frobenius automorphisms, 2004. arXiv:math/0406514v1, updated version available from http://www.ma.huji.ac.il/∼ ehud/.

[19] Ronald P. Infante. Strong normality and normality for difference fields. *Aequationes Math.*, 20(2-3):159–165, 1980.

[20] Ronald P. Infante. On the Galois theory of difference fields. *Aequationes Math.*, 22(2-3):194–207, 1981.

[21] E. R. Kolchin. Galois theory of differential fields. *Amer. J. Math.*, 75:753–824, 1953.

[22] E. R. Kolchin. *Differential algebra and algebraic groups.* Academic Press, New York, 1973. Pure and Applied Mathematics, Vol. 54.

[23] Ellis Kolchin and Serge Lang. Algebraic groups and the Galois theory of differential fields. *Amer. J. Math.*, 80:103–110, 1958.

[24] Jerald J. Kovacic. Differential schemes. In *Differential algebra and related topics (Newark, NJ, 2000)*, pages 71–94. World Sci. Publ., River Edge, NJ, 2002.

[25] Jerald J. Kovacic. Global sections of diffspec. *J. Pure Appl. Algebra*, 171(2-3):265–288, 2002.

[26] Jerald J. Kovacic. The differential Galois theory of strongly normal extensions. *Trans. Amer. Math. Soc.*, 355(11):4475–4522, 2003.

[27] Jerald J. Kovacic. Geometric characterization of strongly normal extensions. *Trans. Amer. Math. Soc.*, 358(9):4135–4157 (electronic), 2006.

[28] H. F. Kreimer. An extension of differential Galois theory. *Trans. Amer. Math. Soc.*, 118:247–256, 1965.

[29] Alexander Levin. *Difference algebra*, volume 8 of *Algebra and Applications*. Springer, New York, 2008.

[30] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[31] B. Heinrich Matzat. Differential Galois theory in positive characteristic. IWR-Preprint, 2001.

[32] B. Heinrich Matzat. Frobenius modules and Galois representations. *Ann. Inst. Fourier*, 59(7):2805–2818, 2009.

[33] B. Heinrich Matzat. From Frobenius structures to differential equations. In *DART II Proceedings*. World Scientific, 2009.

[34] P. E. Newstead. *Introduction to moduli problems and orbit spaces*, volume 51 of *Tata Institute of Fundamental Research Lectures on Mathematics and Physics*. Tata Institute of Fundamental Research, Bombay, 1978.

[35] Kumiko Nishioka. *Mahler functions and transcendence*, volume 1631 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1996.

[36] J.-F. Pommaret. *Differential Galois theory*, volume 15 of *Mathematics and its Applications*. Gordon & Breach Science Publishers, New York, 1983.

[37] R. Y. Sharp. *Steps in commutative algebra*, volume 51 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, second edition, 2000.

[38] Moss Sweedler. The predual theorem to the Jacobson-Bourbaki theorem. *Trans. Amer. Math. Soc.*, 213:391–406, 1975.

[39] Mitsuhiro Takeuchi. A Hopf algebraic approach to the Picard-Vessiot theory. *J. Algebra*, 122(2):481–509, 1989.

[40] Hiroshi Umemura. Cohomological dimension of group schemes. *Nagoya Math. J.*, 52:47–52, 1973.

[41] Hiroshi Umemura. Galois theory of algebraic and differential equations. *Nagoya Math. J.*, 144:1–58, 1996.

[42] P. Vámos. On the minimal prime ideal of a tensor product of two fields. *Math. Proc. Cambridge Philos. Soc.*, 84(1):25–35, 1978.

[43] Marius van der Put and Michael F. Singer. *Galois theory of difference equations*, volume 1666 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1997.

[44] Marius van der Put and Michael F. Singer. *Galois theory of linear differential equations*, volume 328 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2003.