TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 355, Number 11, Pages 4475–4522
S 0002-9947(03)03306-3
Article electronically published on July 2, 2003

THE DIFFERENTIAL GALOIS THEORY OF STRONGLY NORMAL EXTENSIONS

JERALD J. KOVACIC

ABSTRACT. Differential Galois theory, the theory of strongly normal extensions, has unfortunately languished. This may be due to its reliance on Kolchin's elegant, but not widely adopted, axiomatization of the theory of algebraic groups. This paper attempts to revive the theory using a differential scheme in place of those axioms. We also avoid using a universal differential field, instead relying on a certain tensor product.

We identify automorphisms of a strongly normal extension with maximal differential ideals of this tensor product, thus identifying the Galois group with the closed points of an affine differential scheme. Moreover, the tensor product has a natural coring structure which translates into the Galois group operation: composition of automorphisms.

This affine differential scheme splits, i.e. is obtained by base extension from a (not differential, not necessarily affine) group scheme. As a consequence, the Galois group is canonically isomorphic to the closed, or rational, points of a group scheme defined over constants. We obtain the fundamental theorem of differential Galois theory, giving a bijective correspondence between subgroup schemes and intermediate differential fields.

On the way to this result we study certain aspects of differential algebraic geometry, e.g. closed immersions, products, local ringed space of constants, and split differential schemes.

INTRODUCTION

The theory of strongly normal extensions was first presented in Kolchin [11]. At the time of that article, algebraic geometry was dominated by the language of Weil [37]. So it was only natural that Kolchin used similar language. Thus we find notions such as universal differential field, specialization, generic points, etc. Today these notions have dropped out of favor in deference to the language of schemes.

The Galois groups obtained were not really algebraic groups. Kolchin [11, p. 757] states that they are groups with properties "which are like certain known results on algebraic matric groups ... and, more generally, group varieties in the sense of Weil". A later paper, Kolchin-Lang [15], remedied this, but at some cost. The proof used Weil's theory of "group chunks"; this makes the Galois groups birationally isomorphic to algebraic groups, but not canonically.

Kolchin always felt this to be a blemish on the theory. He wished that the Galois groups would actually *be* algebraic groups. So he axiomatized the notion of algebraic group. In this way the Galois group could be shown to satisfy the axioms and therefore *be* an algebraic group. In some sense this is analogous to the situation

Received by the editors June 1, 2002.
2000 *Mathematics Subject Classification.* Primary 12H05, 12F10; Secondary 14A15, 14L15.

of the usual Galois theory. At first the Galois group was merely isomorphic to a group of permutations. It was only after the axiomatization of the notion of group that the Galois groups became groups in their own right. Unfortunately the elegant axiomatization of Kolchin [12, Chapter V] has not been widely embraced. This has made the Galois theory languish; the learning curve is simply too steep.

There have been other presentations of the theory. Umemura [33] has developed it using scheme-theoretic language. However he too uses Weil's "group chunks", albeit a scheme-theoretic version. A generalization to infinite dimension is presented in Umemura [34]. Poizat [26, Section 5, pp. 1165–1169] develops the differential Galois theory using model-theoretic techniques. His groups turned out to be *definable* groups, and he asked whether all such were algebraic groups. The affirmative answer came in the form of the Weil-Hrushovski theorem (Poizat [27, Theorem 4.13, p. 84]). A generalization using certain types of differential algebraic groups and model theory has been developed by Pillay and Marker [24, 25, 21].

Tensor products have been introduced to great advantage into the Picard-Vessiot theory. Levelt [18] essentially gets the Galois group as spec of a certain tensor product. Takeuchi [32] also uses tensor products and Hopf algebras. We believe that these techniques can be used to elucidate the strongly normal theory as well. And that is the goal of this paper. We also believe that the treatment here clarifies the ideas of Levelt and Takeuchi.

Our treatment does not use universal differential fields, nor does it use group chunks. Instead we investigate the differential ring $\mathcal{P} = \mathcal{G} \otimes_{\mathcal{F}} \mathcal{G}$, where $\mathcal{G}$ is a strongly normal extension of $\mathcal{F}$. We show that the Galois group, the group of differential automorphisms of $\mathcal{G}$ over $\mathcal{F}$, is canonically identified with the set of closed points of $P = \operatorname{diffspec} \mathcal{P}$.

There is a natural differential coring structure on $\mathcal{P}$ which corresponds to the Galois group operations: composition and inverse of automorphisms. We obtain a bijective correspondence between differential coideals and intermediate differential fields. This is essentially the fundamental theorem of Sweedler corings. There is another bijective correspondence between closed subgroups of the Galois group and differential coideals. These two bijections together give the fundamental theorem of differential Galois theory.

We also show that there is a group scheme defined over constants such that the rational points are canonically identified with the automorphisms in the Galois group. We do this by showing that P splits: $P \approx G \times_C P^{\Delta}$, where $C = \operatorname{diffspec} \mathcal{C}$, $G = \operatorname{diffspec} \mathcal{G}$ and P^{Δ} is a group scheme that is canonically derived from P. If the notion of differential group scheme were defined, P would certainly be an example, however that theory does not seem to be available at this time.

Indeed, the current theory of differential schemes is lacking some results that we need, for example results concerning closed subschemes. So we present those results here. We do not do so with utmost generality, but rather make assumptions that are sufficient for our purposes (reduced Ritt algebras); this simplifies the arguments considerably. However most of the results can be proved for AAD (Kovacic [16, Definition 9.1]) rings or even RAAD (Kovacic [17, Definition 6.3]) and RAADZ ([17, Definition 7.2]) rings, using similar arguments.

We restrict our attention to characteristic 0; in positive characteristic it is probably better to use Hasse-Schmidt higher derivations. Okugawa [23] has done this, and developed the theory of strongly normal extensions using Kolchin's axiomatic

definition of algebraic group. We also assume that the field of constants is algebraically closed. This simplifies matters considerably, but is not strictly necessary. For example, instead of automorphisms we could consider isomorphisms whose image is an algebraic extension.

This paper is divided into four parts: Differential rings and ideals, Strongly normal extensions, Differential schemes, and Differential Galois group. In the following discussion we use the prefix Δ- in lieu of the word "differential".

In Part I, the first two sections define the notation and recall some elementary facts that will be used frequently in the sequel. Section 3 introduces notation for sets of (prime, radical) Δ-ideals and finds some bijections between them. This is important because an isomorphism between diffspec of two Δ-rings does not imply the rings are isomorphic; but it does imply that they have the "same" prime and even radical Δ-ideals. This material is used in Part III. Section 4 recalls some basic facts about rings of fractions and Δ-units which will be important later.

Section 5 investigates "almost constant" Δ-rings, Δ-rings $\mathcal{R}$ whose radical Δ-ideals come from ideals of $\mathcal{R}^{\Delta}$, the ring of constants of $\mathcal{R}$. The prototypical example is $\mathcal{R} = \mathcal{F} \otimes_{\mathcal{C}} \mathcal{D}$ where $\mathcal{F}$ is a Δ-field with field of constants $\mathcal{C}$ and $\mathcal{D}$ is a ring of constants. This is what we mean by saying that $\mathcal{R}$ splits. But there are other examples, e.g. Δ-simple rings (having no proper non-zero Δ-ideals).

Part II starts by introducing the Δ-ring $\mathcal{P} = \mathcal{G} \otimes_{\mathcal{F}} \mathcal{G}$, which will play a major role in this paper. Indeed, the prime Δ-ideals of $\mathcal{P}$ correspond to equivalence classes, under generic specialization, of Δ-isomorphisms. We also see that isolated isomorphisms correspond to minimal prime Δ-ideals. There are a finite number of such, and every prime Δ-ideal of $\mathcal{P}$ contains a unique one.

In Section 11 we define strongly normal extension. Section 13 then shows that a strong normal extension is constrained, i.e. contained in what model theorists call a differential closure. For a discussion of model theory and differential algebra, see, for example, Scanlon [28]. A Δ-ring is 1-constrained if and only if it is Δ-simple. We show that a strongly normal extension $\mathcal{G}$ contains a Δ-ring that is Δ-simple and whose quotient field is $\mathcal{G}$. This condition is used by van der Put [36, p. 171] as part of his definition of Picard-Vessiot extension.

In Section 14 we define the Galois group as the group of Δ-automorphisms of the strongly normal extension. Then Section 15 shows that $\mathcal{P}$ is a Δ-Jacobson ring, which implies that the Δ-automorphisms are very dense in the set of Δ-isomorphisms, i.e. every non-empty locally closed set of Δ-isomorphisms contains an automorphism.

Section 16 introduces a Δ-coring structure on $\mathcal{P}$, and Section 17 relates that structure to the group operations of the Galois group, i.e. composition and inversion of Δ-automorphisms.

The Kolchin topology is introduced in Section 18. This part concludes, in Sections 19 and 20, by proving the fundamental theorems of differential Galois theory.

Part III develops material about Δ-schemes, supplementing that of Kovacic [16]. However, we restrict our attention to Δ-schemes over a fixed Δ-field of characteristic 0 and often assume the schemes are reduced, this being sufficient for the applications we have in mind. The most important result is that a reduced closed subscheme of a reduced affine Δ-scheme is induced by a radical Δ-ideal. Our proof does not use a sheaf of ideals, partly because the theory of quasi-coherent sheaves has yet to be developed for Δ-schemes.

In Section 21 we examine the ring of global sections. In general, little can be said (but see Kovacic [17]); however, in the special case of reduced rings we have some information. Section 23 is quite technical, but provides the foundation needed for the proofs of Section 24, where we treat reduced closed subschemes, proving the result stated above.

In Sections 26 and 27 we introduce the local ringed space of constants X^Δ of a Δ-scheme X. The topological space is unchanged, but the rings are replaced by the subrings of constants of the original rings. It is particularly interesting when this local ringed space turns out to be a scheme, and we study this case in some detail. Later we shall see that this fortuitous case does indeed occur for $P = \operatorname{diffspec}(\mathcal{G} \otimes_{\mathcal{F}} \mathcal{G})$ when $\mathcal{G}$ is a strongly normal extension of $\mathcal{F}$.

Section 28 takes up another topic, split Δ-schemes. These are Δ-schemes that are isomorphic to the product of the scheme of constants with a field. This is like "base extension" in the category of Δ-schemes. Buium [3, p. 6] treats a similar notion, but he works in the category of schemes with derivations, not in the category of Δ-schemes.

We end this part with two examples. In the first, P^Δ is an affine scheme. The second is more interesting: P^Δ is a scheme, but is *not* affine. Thus a Δ-scheme P can be affine even if its scheme of constants P^Δ is not.

In Part IV we continue our study of the differential Galois theory of strongly normal extensions, showing that the differential Galois group is canonically identified with the set of closed or, what is the same, $\mathcal{C}$-rational points of a group scheme.

We start, in Section 30, by showing that P is a Jacobson space, i.e. the closed points are very dense. We also prove that P is homogeneous in the sense that any closed point can be "moved" into any other. Using this, we will find an affine open cover of P by simply finding one non-empty affine open set and then moving it around.

In Section 33 we find that affine open set. In Section 34 we show that the Galois group is canonically identified with the $\mathcal{C}$-rational points of a group scheme. In Section 36 we prove the fundamental theorem of differential Galois theory in its usual form. In the final section, Section 37, we make some observations about the set of differential isomorphisms. This requires a universal differential field, and it is the only place in this paper that does. We show that the set of equivalence classes of differential isomorphisms of $\mathcal{G}$ over $\mathcal{F}$ is canonically identified with a group scheme, the automorphisms then being identified with $\mathcal{C}$-rational points.

Part I. Differential rings and ideals

For the basic notions of differential algebra, see Kolchin [12], Kaplansky [7] or Magid [20]. Both Kaplansky and Magid restrict themselves to ordinary differential rings whereas we and Kolchin do not.

1. Notation

In this paper we use the prefix Δ in lieu of the word "differential", e.g. Δ-ring, Δ-ideal, etc. All Δ-rings are assumed to be Ritt algebras, i.e. algebras over $\mathbb{Q}$. Note that the 0 ring is a Ritt algebra. The set of (commuting) derivations is denoted by $\Delta = \{\delta_1, \ldots, \delta_m\}$. If $\mathcal{R}$ is any Δ-ring, then $\mathcal{R}^\Delta$ is its ring of constants.

The free commutative monoid generated by Δ is denoted by Θ; thus $\theta \in \Theta$ has a unique representation in the form

$$\theta = \delta_1^{e_1} \cdots \delta_m^{e_m}, \qquad e_1, \ldots, e_m \in \mathbb{N}.$$

Thinking of elements of Θ as differential operators, we denote by id the element having $e_1 = \cdots = e_m = 0$.

Throughout this paper, $\mathcal{F}$ is a Δ-field of characteristic 0 with field of constants $\mathcal{C} = \mathcal{F}^\Delta$. When dealing with strongly normal extensions (Parts II and IV) we shall assume that $\mathcal{C}$ is algebraically closed. We often require that a Δ-ring be reduced (have no non-zero nilpotents), but we explicitly state this assumption whenever we use it. We use $\mathcal{R}$ and $\mathcal{S}$ to denote Δ-rings, sometimes without comment.

2. Elementary facts

This section collects some elementary facts that will be used frequently in the sequel.

Proposition 2.1. *Let $\mathcal{R}$ be a Δ-ring containing $\mathcal{F}$. Then $\mathcal{F}$ and $\mathcal{R}^\Delta$ are linearly disjoint over $\mathcal{C}$.*

Proof. Kolchin [12, Corollary 1, p. 87] or Kaplansky [7, Theorem 3.7, p. 21]. □

Proposition 2.2. *Let $\mathcal{R}$ be a Δ-ring containing $\mathcal{F}$. Then $\mathcal{F}[\mathcal{R}^\Delta]^\Delta = \mathcal{R}^\Delta$.*

Proof. Let Λ be a basis of $\mathcal{R}^\Delta$ over $\mathcal{C}$ and therefore of $\mathcal{F}[\mathcal{R}^\Delta]$ over $\mathcal{F}$. If $c \in \mathcal{F}[\mathcal{R}^\Delta]^\Delta$ and

$$c = \sum_{\lambda \in \Lambda} f_\lambda \lambda,$$

then, for every $\delta \in \Delta$,

$$0 = \sum_{\lambda \in \Lambda} \delta f_\lambda \lambda,$$

which implies that $f_\lambda \in \mathcal{C}$. □

For any set $S \subset \mathcal{R}$, $[S]$ is the smallest Δ-ideal containing S and $\{S\}$ is the smallest radical Δ-ideal. Because $\mathcal{R}$ is a Ritt algebra, we have the following.

Proposition 2.3. *Let S be a subset of $\mathcal{R}$. Then $\{S\} = \sqrt{[S]}$.*

Proof. [12, Lemma 2, p. 62] or [7, Lemma 1.8, p. 12]. □

Proposition 2.4. *Let S and T be subsets of $\mathcal{R}$. Then $\{S\}\{T\} \subset \{ST\}$.*

Proof. [12, Lemma 1, p. 62] or [7, Lemma 1.6, p. 12]. □

Proposition 2.5. *Let $\mathfrak{a} \subset \mathcal{R}$ be a Δ-ideal and $\Sigma \subset \mathcal{R}$ a multiplicative set with $\mathfrak{a} \cap \Sigma = \emptyset$. If $\mathfrak{m}$ is a Δ-ideal containing $\mathfrak{a}$ that is maximal with respect to avoiding Σ, then $\mathfrak{m}$ is prime. In particular, a maximal Δ-ideal is prime.*

Proof. [12, Exercise 3, p. 63] or [7, Lemma, p. 13]. □

Definition 2.6. If $b \in \mathcal{R}$ we denote by b^∞ the multiplicative set

$$b^\infty = \{\, b^e \mid e \in \mathbb{N} \,\}.$$

Proposition 2.7. *Let $\mathfrak{a} \subset \mathcal{R}$ be a radical Δ-ideal. Then $\mathfrak{a}$ is the intersection of prime Δ-ideals.*

Proof. If $\mathfrak{a} = \mathcal{R}$ then $\mathfrak{a}$ is the empty intersection. If $\mathfrak{a} \neq \mathcal{R}$, then for every $b \notin \mathfrak{a}$ there is a prime Δ-ideal that contains $\mathfrak{a}$ and avoids b^∞. □

Proposition 2.8. *Every minimal prime ideal $\mathfrak{p} \subset \mathcal{R}$ is a Δ-ideal.*

Proof. Keigher [9, Proposition 1.5, p. 242]. If $\mathfrak{p}$ is a minimal prime, then

$$\mathfrak{p}_\# = \{\, a \in \mathfrak{p} \mid \delta a \in \mathfrak{p} \text{ for all } \delta \in \Delta \,\}$$

is a Δ-ideal which is maximal with respect to avoiding $\mathcal{R} \setminus \mathfrak{p}$. Therefore it is prime and, by minimality, equals $\mathfrak{p}$. □

In the following, $\mathcal{R}_\mathfrak{p}^\Delta = (\mathcal{R}_\mathfrak{p})^\Delta$ and $(\mathfrak{p}\mathcal{P}_\mathfrak{p})^\Delta = (\mathfrak{p}\mathcal{R}_\mathfrak{p}) \cap \mathcal{R}_\mathfrak{p}^\Delta$.

Proposition 2.9. *Let $\mathfrak{p} \subset \mathcal{R}$ be a prime Δ-ideal. Then $\mathcal{R}_\mathfrak{p}^\Delta$ is a local ring with maximal ideal $(\mathfrak{p}\mathcal{P}_\mathfrak{p})^\Delta$.*

Proof. If $a \in \mathcal{R}_\mathfrak{p}^\Delta$, $a \notin (\mathfrak{p}\mathcal{R}_\mathfrak{p})^\Delta$, then a is invertible in $\mathcal{R}_\mathfrak{p}$. But the inverse of a constant is a constant, so a is invertible in $\mathcal{R}_\mathfrak{p}^\Delta$. □

Beware: $\mathcal{R}_\mathfrak{p}^\Delta$ is not necessarily the same as $(\mathcal{R}^\Delta)_{\mathfrak{p}^\Delta}$.

3. Sets of Δ-ideals

The material in this and subsequent sections of this part will not be used until Part III. The reader may wish to skip ahead and return here after reading Part II.

Unlike the situation in algebraic geometry, $\operatorname{diffspec}\mathcal{R}$ may be isomorphic to $\operatorname{diffspec}\mathcal{S}$ without $\mathcal{R}$ and $\mathcal{S}$ being isomorphic. But they will have isomorphic sets of prime and even radical Δ-ideals.

Definition 3.1. Let $\mathcal{R}$ be a Δ-ring. Then:

(1) $\mathtt{I}(\mathcal{R})$ is the set of all Δ-ideals of $\mathcal{R}$,
(2) $\mathtt{R}(\mathcal{R})$ is the set of all radical Δ-ideals of $\mathcal{R}$,
(3) $\mathtt{P}(\mathcal{R})$ is the set of all prime Δ-ideals of $\mathcal{R}$.

Definition 3.2. Let $\phi\colon \mathcal{R} \to \mathcal{S}$ be a Δ-homomorphism. Then:

(1) ${}^i\phi\colon\ \mathtt{I}(\mathcal{S}) \longrightarrow \mathtt{I}(\mathcal{R})$,
(2) ${}^r\phi\colon\ \mathtt{R}(\mathcal{S}) \longrightarrow \mathtt{R}(\mathcal{R})$,
(3) ${}^p\phi\colon\ \mathtt{P}(\mathcal{S}) \longrightarrow \mathtt{P}(\mathcal{R})$

are defined by the formula $\mathfrak{a} \mapsto \phi^{-1}(\mathfrak{a})$.

$\mathtt{P}(\mathcal{R})$ is the same set as $\operatorname{diffspec}\mathcal{R}$ but without the topology and structure sheaf, and ${}^p\phi$ is the same as the adjoint ${}^a\phi$. Later, in Proposition 22.1, we shall see that ${}^a\phi$ is a homeomorphism of $\operatorname{diffspec}\mathcal{S}$ onto $\operatorname{diffspec}\mathcal{R}$ if and only if ${}^r\phi$ is bijective. The following two propositions are partial results in that direction.

Proposition 3.3. *Let $\phi\colon \mathcal{R} \to \mathcal{S}$ be a Δ-homomorphism. Then ${}^r\phi$ is surjective if and only if ${}^p\phi$ is surjective.*

Proof. Suppose that ${}^r\phi$ is surjective and let $\mathfrak{p} \in \mathtt{P}(\mathcal{R}) \subset \mathtt{R}(\mathcal{R})$. Choose $\mathfrak{b} \in \mathtt{R}(\mathcal{S})$ with ${}^r\phi(\mathfrak{b}) = \mathfrak{p}$. The multiplicative set $\Sigma = \phi(\mathcal{R} \setminus \mathfrak{p}) \subset \mathcal{S}$ is disjoint from $\mathfrak{b}$; so, by Proposition 2.5, there exists $\mathfrak{q} \in \mathtt{P}(\mathcal{S})$ containing $\mathfrak{b}$ and disjoint from Σ. Evidently ${}^p\phi(\mathfrak{q}) = \mathfrak{p}$.

For the converse, let $\mathfrak{a} \in \mathtt{R}(\mathcal{R})$. By Proposition 2.7

$$\mathfrak{a} = \bigcap_{i \in I} \mathfrak{p}_i, \quad \mathfrak{p}_i \in \mathtt{P}(\mathcal{R}).$$

Let $\mathfrak{q}_i \in \mathtt{P}(\mathcal{S})$ be such that ${}^p\phi(\mathfrak{q}_i) = \mathfrak{p}_i$ and

$$\mathfrak{b} = \bigcap_{i \in I} \mathfrak{q}_i \in \mathtt{R}(\mathcal{S}).$$

Evidently ${}^r\phi(\mathfrak{b}) = \mathfrak{a}$. □

Proposition 3.4. *Let $\phi\colon \mathcal{R} \to \mathcal{S}$ be a Δ-homomorphism. If ${}^i\phi$ is bijective, then so is ${}^r\phi$. If ${}^r\phi$ is bijective, then so is ${}^p\phi$.*

Proof. Suppose that ${}^i\phi$ is bijective. Clearly ${}^r\phi$ is injective. Let $\mathfrak{a} \in \mathtt{R}(\mathcal{R})$ and $\mathfrak{b} \in \mathtt{I}(\mathcal{S})$ with ${}^i\phi(\mathfrak{b}) = \mathfrak{a}$, and let $\mathfrak{c} = \sqrt{\mathfrak{b}}$. Evidently $\mathfrak{a} \subset {}^r\phi(\mathfrak{c})$. If $a \in {}^r\phi(\mathfrak{c})$, then $\phi(a)^e \in \mathfrak{b}$ for some $e \in \mathbb{N}$; hence $a^e \in \mathfrak{a}$, which gives $a \in \mathfrak{a}$ because $\mathfrak{a}$ is a radical Δ-ideal. Thus ${}^r\phi(\mathfrak{c}) = \mathfrak{a}$ (and hence $\mathfrak{c} = \mathfrak{b}$.) The second statement comes from the previous proposition. □

The next proposition will help us show that certain affine differential schemes are isomorphic.

Proposition 3.5. *Suppose that $\mathcal{R}$ and $\mathcal{S}$ are reduced and that $\phi\colon \mathcal{R} \to \mathcal{S}$ is a Δ-homomorphism with ${}^r\phi$ bijective. If $\mathfrak{q} \in \mathtt{P}(\mathcal{S})$ and $\mathfrak{p} = {}^p\phi(\mathfrak{q})$, then*

$$\phi_{\mathfrak{q}}\colon \mathcal{R}_{\mathfrak{p}} \to \mathcal{S}_{\mathfrak{q}}, \qquad a/b \longmapsto \phi(a)/\phi(b),$$

is injective.

Proof. First observe that ϕ is injective, because (0) is a radical Δ-ideal of $\mathcal{R}$ (since $\mathcal{R}$ is reduced) and ${}^r\phi$ is surjective.

Suppose that $\phi_{\mathfrak{q}}(a/b) = 0 \in \mathcal{S}_{\mathfrak{q}}$. Then there exists $s \in \mathcal{S}$, $s \notin \mathfrak{q}$, such that $s\,\phi(a) = 0 \in \mathcal{S}$. Let

$$\mathfrak{b} = \{\, s \in \mathcal{S} \mid s\,\phi(a) = 0 \,\} = \operatorname{Ann}(\phi(a)).$$

Because $\mathcal{S}$ is reduced, $\mathfrak{b}$ is a radical ideal. If $s \in \mathfrak{b}$ and $\delta \in \Delta$, then

$$\delta s\,\phi(a)^2 = \delta(s\,\phi(a))\,\phi(a) - s\,\delta(\phi(a))\,\phi(a) = 0,$$

so $\mathfrak{b}$ is a Δ-ideal. It is not contained in $\mathfrak{q}$, and therefore ${}^r\phi(\mathfrak{b})$ is not contained in $\mathfrak{p}$. Hence there exists $t \in {}^r\phi(\mathfrak{b})$ with $t \notin \mathfrak{p}$, $\phi(t)\phi(a) = 0$ and $ta = 0$. □

Let Σ be a multiplicative set of $\mathcal{R}$. Recall that a Δ-ideal $\mathfrak{a}$ is prime to Σ if $\mathfrak{a}\colon \Sigma = \mathfrak{a}$, i.e., $as \in \mathfrak{a}$ implies $a \in \mathfrak{a}$ whenever $s \in \Sigma$. We extend the notation of Definition 3.1 as follows.

Definition 3.6. Let Σ be a multiplicative set in $\mathcal{R}$. Then:

(1) $\mathtt{I}(\mathcal{R}, \Sigma)$ is the set of all Δ-ideals of $\mathcal{R}$ prime to Σ,
(2) $\mathtt{R}(\mathcal{R}, \Sigma)$ is the set of all radical Δ-ideals of $\mathcal{R}$ prime to Σ,
(3) $\mathtt{P}(\mathcal{R}, \Sigma)$ is the set of all prime Δ-ideals of $\mathcal{R}$ prime to Σ.

We do not introduce special notation for the restrictions of ${}^i\phi$ to $\mathtt{I}(\mathcal{R}, \Sigma)$, etc., but rather rely on the context to make the meaning clear.

4. Rings of fractions

Proposition 4.1. *Let $\Sigma \subset \mathcal{R}$ be a multiplicative set and $h\colon \mathcal{R} \to \mathcal{R}\Sigma^{-1}$ the canonical mapping. Then ${}^{i}h\colon \mathtt{I}(\mathcal{R}\Sigma^{-1}) \to \mathtt{I}(\mathcal{R},\Sigma)$ is bijective with inverse $\mathfrak{a} \mapsto \mathfrak{a}\,\mathcal{R}\Sigma^{-1}$. If $\mathfrak{b} \in \mathtt{I}(\mathcal{R})$, then ${}^{i}h(\mathfrak{b}\,\mathcal{R}\Sigma^{-1}) = \mathfrak{b}\colon\Sigma$.*

Proof. This is a differential version of a standard theorem, e.g. Zariski-Samuel [38, Theorem 15 p. 223], and has a similar proof. □

Proposition 4.2. *${}^{r}h\colon \mathtt{R}(\mathcal{R}\Sigma^{-1}) \to \mathtt{R}(\mathcal{R},\Sigma)$ is bijective and has inverse $\mathfrak{a} \mapsto \mathfrak{a}\,\mathcal{R}\Sigma^{-1}$.*

Proof. Proposition 3.4. □

The following is Kovacic [17, Definition 8.1].

Definition 4.3. $u \in \mathcal{R}$ is a Δ-*unit* if $1 \in \{u\}$.

In a Ritt algebra, as we are assuming, this is equivalent to $1 \in [u]$.

Proposition 4.4. *If $\Sigma \subset \mathcal{R}$ is a multiplicative set consisting of Δ-units, then $\mathtt{R}(\mathcal{R},\Sigma) = \mathtt{R}(\mathcal{R})$.*

Proof. Let $\mathfrak{a} \in \mathtt{R}(\mathcal{R})$ and suppose that $as \in \mathfrak{a}$ for some $s \in \Sigma$. By Proposition 2.4

$$a \cdot 1 \in \{a\}\{s\} \subset \mathfrak{a};$$

hence $\mathfrak{a} \in \mathtt{R}(\mathcal{R},\Sigma)$ and $\mathtt{R}(\mathcal{R}) \subset \mathtt{R}(\mathcal{R},\Sigma)$. The other inclusion is obvious. □

5. Almost constant Δ-rings

Definition 5.1. Let $j\colon \mathcal{R}^\Delta \to \mathcal{R}$ be the inclusion. We say that $\mathcal{R}$ is *almost constant* if ${}^{r}j\colon \mathtt{R}(\mathcal{R}) \to \mathtt{R}(\mathcal{R}^\Delta)$ is bijective.

If $\mathcal{R}$ is almost constant, then, by Proposition 3.4, ${}^{p}j\colon \mathtt{P}(\mathcal{R}) \to \mathtt{P}(\mathcal{R}^\Delta)$ is also bijective. This gives a bijection from $\operatorname{diffspec}\mathcal{R}$ onto $\operatorname{spec}\mathcal{R}^\Delta$, which, as we shall see in Proposition 22.1, is a homeomorphism. For $\mathfrak{a} \in \mathtt{I}(\mathcal{R})$ we often write $\mathfrak{a}^\Delta = {}^{i}j(\mathfrak{a}) = \mathfrak{a} \cap \mathcal{R}^\Delta$. For almost constant rings we can improve Proposition 2.9.

Proposition 5.2. *Suppose that $\mathcal{R}$ is almost constant. If $\mathfrak{p} \in \mathtt{P}(\mathcal{R})$, then $\mathcal{R}_\mathfrak{p}^\Delta = (\mathcal{R}_\mathfrak{p})^\Delta$ is isomorphic to $(\mathcal{R}^\Delta)_{\mathfrak{p}^\Delta}$.*

Proof. Define

$$j_\mathfrak{p}\colon (\mathcal{R}^\Delta)_{\mathfrak{p}^\Delta} \to \mathcal{R}_\mathfrak{p}^\Delta, \qquad a/b \longmapsto a/b.$$

We claim that $j_\mathfrak{p}$ is an isomorphism. If $j_\mathfrak{p}(a/1) = 0$, then there exists $c \in \mathcal{R}$, $c \notin \mathfrak{p}$, such that $c\,a = 0$. Let

$$\mathfrak{a} = \{\, c \in \mathcal{R} \mid c\,a = 0 \,\} = \operatorname{Ann}(a).$$

Because a is a constant, $\mathfrak{a}$ is a Δ-ideal. Hence $\sqrt{\mathfrak{a}}$ is a radical Δ-ideal which is not contained in $\mathfrak{p}$, so there exists $d \in \sqrt{\mathfrak{a}}^{\,\Delta}$ with $d \notin \mathfrak{p}^\Delta$. But then $d^e\,a = 0$ for some $e \in \mathbb{N}$, which means that $a/1 = 0 \in (\mathcal{R}^\Delta)_{\mathfrak{p}^\Delta}$.

Surjectivity is similar. If $x \in \mathcal{R}_\mathfrak{p}^\Delta$ we let $\mathfrak{a} = \{\, c \in \mathcal{R} \mid c\,x \in \mathcal{R} \,\}$. Again $\mathfrak{a}$ is a Δ-ideal and there exists $d \in \sqrt{\mathfrak{a}}^{\,\Delta}$, $d \notin \mathfrak{p}^\Delta$, and $d^e\,x = a \in \mathcal{R}$ for some $e \in \mathbb{N}$. Clearly $a \in \mathcal{R}^\Delta$ and $\phi(a/d^e) = x$. □

Proposition 5.3. *Let $c \in \mathcal{R}^\Delta$. If $\mathcal{R}$ is almost constant, then so is $\mathcal{R}_c$.*

Proof. First observe that $\mathcal{R}_c^\Delta = (\mathcal{R}_c)^\Delta = (\mathcal{R}^\Delta)_c$; then use Proposition 4.2. □

Proposition 5.4. *Let $\Sigma \subset \mathcal{R}$ be a multiplicative set consisting of Δ-units. Then $(\mathcal{R}\Sigma^{-1})^{\Delta} = \mathcal{R}^{\Delta}$. Moreover, $\mathcal{R}\Sigma^{-1}$ is almost constant if and only if $\mathcal{R}$ is.*

Proof. If $c \in (\mathcal{R}\Sigma^{-1})^{\Delta}$, then $sc \in \mathcal{R}$ for some $s \in \Sigma$. By Proposition 2.4,

$$c \in \{s\}\{c\} \subset \mathcal{R},$$

so $c \in \mathcal{R}^{\Delta}$. The last statement is because $\mathtt{R}(\mathcal{R}) = \mathtt{R}(\mathcal{R}, \Sigma^{-1})$ by Proposition 4.4. □

The following proposition will be used in Part IV. To simplify the proof we assume that $\mathcal{R}$ is an integral domain. This allows us to identify $\mathcal{R}$ with a subring of $\mathcal{R}_{bc}$.

Proposition 5.5. *Suppose that $\mathcal{R}$ is an almost constant integral domain, and let $b \in \mathcal{R}$, $b \neq 0$. Then there exists $c \in \mathcal{R}^{\Delta}$, $c \neq 0$, such that $\mathcal{R}_{bc}$ is almost constant. In addition, $b/1 \in \mathcal{R}_c$ is a Δ-unit and $\mathcal{R}_{bc}^{\Delta} = \mathcal{R}_c^{\Delta}$.*

Proof. Consider the radical Δ-ideal $\{b\}$ in $\mathcal{R}$. By hypothesis there exists $c \in \{b\} \cap \mathcal{R}^{\Delta}$, $c \neq 0$. Let $j\colon \mathcal{R}^{\Delta} \to \mathcal{R}$ be the inclusion. We claim that

$$^{r}j\colon \mathtt{R}(\mathcal{R}, (bc)^{\infty}) \to \mathtt{R}(\mathcal{R}^{\Delta}, c^{\infty})$$

is bijective.

Because $\mathcal{R}$ is almost constant, ^{r}j is injective. Let $\mathfrak{a} \in \mathtt{R}(\mathcal{R}^{\Delta}, c^{\infty})$ and set $\mathfrak{b} = \mathfrak{a}\mathcal{R}\colon c^{\infty}$. Evidently $\mathfrak{a} \subset \mathfrak{b}^{\Delta}$. Conversely, if $r \in \mathfrak{b}^{\Delta}$, then $c^{e}r \in (\mathfrak{a}\mathcal{R})^{\Delta} = \mathfrak{a}$ for some $e \in \mathbb{N}$. But $\mathfrak{a}$ is prime to c^{∞}, so $r \in \mathfrak{a}$, which proves that $\mathfrak{b}^{\Delta} = \mathfrak{a}$.

To complete the proof of our claim we must show that $\mathfrak{b} \in \mathtt{R}(\mathcal{R}, (bc)^{\infty})$, i.e. that $\mathfrak{b}$ is prime to b^{∞}. (It is easily seen to be a radical Δ-ideal, and it is prime to c^{∞} by definition.) If $b^{e}r \in \mathfrak{b}$ then, by Proposition 2.4,

$$cr \in \{b\}\{r\} \subset \mathfrak{b};$$

hence $r \in \mathfrak{b}$. This shows that ^{r}j is bijective, as claimed.

Next we prove that $\mathcal{R}_{bc}^{\Delta} = \mathcal{R}_c^{\Delta}$. Obviously $\mathcal{R}_c^{\Delta} \subset \mathcal{R}_{bc}^{\Delta}$. Let $x \in \mathcal{R}_{bc}^{\Delta}$ and set

$$\mathfrak{b} = \{\, r \in \mathcal{R} \mid rx \in \mathcal{R} \,\}.$$

Since x is constant, $\mathfrak{b}$ is a Δ-ideal. Note that $\sqrt{\mathfrak{b}}$ contains bc and therefore c by Proposition 2.4, since $c \in \{b\}$. Hence $x = a/c^{e}$ for some $e \in \mathbb{N}$. It follows that $a \in \mathcal{R}^{\Delta}$, which proves the second claim.

To complete the proof of the proposition we examine the following commutative diagram:

$$\begin{array}{ccc} \mathcal{R} & \hookrightarrow & \mathcal{R}_{bc} \\ \uparrow & & \uparrow \\ \mathcal{R}^{\Delta} & \hookrightarrow & \mathcal{R}_c^{\Delta} = \mathcal{R}_{bc}^{\Delta} \end{array}$$

This gives the following diagram:

$$\begin{array}{ccc} \mathtt{R}(\mathcal{R}, (bc)^{\infty}) & \longleftarrow & \mathtt{R}(\mathcal{R}_{bc}) \\ \downarrow & & \vdots \\ \mathtt{R}(\mathcal{R}^{\Delta}, c^{\infty}) & \longleftarrow & \mathtt{R}(\mathcal{R}_c^{\Delta}) = \mathtt{R}(\mathcal{R}_{bc}^{\Delta}) \end{array}$$

We have shown that the solid vertical arrow is bijective (our claim), and Proposition 4.2 shows that the horizontal arrows are bijective. Therefore the dotted arrow is bijective.

Finally, $b/1$ is a Δ-unit because $c/1$ is invertible in $\mathcal{R}_c$. □

The prototypical almost constant Δ-ring is $\mathcal{R} = \mathcal{F} \otimes_{\mathcal{C}} \mathcal{D} = \mathcal{F}[\mathcal{D}]$, where $\mathcal{D}$ is a ring of constants.

Proposition 5.6. *Let $\mathcal{D}$ be a ring of constants containing $\mathcal{C}$. Define*

$$\Phi\colon \mathtt{I}(\mathcal{D}) \to \mathtt{I}(\mathcal{F} \otimes_{\mathcal{C}} \mathcal{D}) \quad \text{by} \quad \Phi(\mathfrak{a}) = \mathcal{F} \otimes_{\mathcal{C}} \mathfrak{a}$$

and

$$\Psi\colon \mathtt{I}(\mathcal{F} \otimes_{\mathcal{C}} \mathcal{D}) \to \mathtt{I}(\mathcal{D}) \quad \text{by} \quad \Psi(\mathfrak{b}) = \{\, d \in \mathcal{D} \mid 1 \otimes d \in \mathfrak{b} \,\}.$$

Then Φ and Ψ are bijective and inverse to each other.

Proof. This is essentially Levelt [18, Proposition 1, p. 442], but, for the sake of completeness, we present a proof.

Evidently $\mathfrak{a} \subset \Psi(\Phi(\mathfrak{a})) = \Psi(\mathcal{F} \otimes_{\mathcal{C}} \mathfrak{a})$. Choose a basis Λ of $\mathfrak{a}$ over $\mathcal{C}$ and extend it to a basis M of $\mathcal{D}$ over $\mathcal{C}$. Then $1 \otimes_{\mathcal{C}} \mathrm{M}$ is a basis for $\mathcal{F} \otimes_{\mathcal{C}} \mathcal{D}$ over $\mathcal{F}$. Let $d \in \Psi(\Phi(\mathfrak{a}))$, so $1 \otimes d \in \mathcal{F} \otimes_{\mathcal{C}} \mathfrak{a}$. Therefore

$$1 \otimes d = \sum_{\lambda \in \Lambda} f_\lambda \otimes \lambda \qquad (f_\lambda \in \mathcal{F}).$$

But $d \in \mathcal{D}$, so

$$1 \otimes d = \sum_{\mu \in \mathrm{M}} 1 \otimes c_\mu \mu \qquad (c_\mu \in \mathcal{C}).$$

Comparing coefficients, we see that $c_\mu = 0$ for $\mu \notin \Lambda$, and $f_\lambda = c_\lambda$; thus $d \in \mathfrak{a}$.

It is also clear that $\Phi(\Psi(\mathfrak{b})) = \mathcal{F} \otimes_{\mathcal{C}} \Psi(\mathfrak{b}) \subset \mathfrak{b}$. Suppose they are unequal. As above, choose a vector space basis Λ of $\Psi(\mathfrak{b})$ over $\mathcal{C}$ and extend it to a basis M of $\mathcal{D}$ over $\mathcal{C}$. Among elements $a \in \mathfrak{b}$, $a \notin \mathcal{F} \otimes_{\mathcal{C}} \Psi(\mathfrak{b})$, choose one whose representation in the form

$$a = \sum_{\mu \in M} f_\mu \otimes \mu \qquad (f_\mu \in \mathcal{F})$$

has fewest non-zero terms. We may assume that some $f_\mu = 1$. For each $\delta \in \Delta$, $\delta a \in \mathfrak{b}$ has fewer non-zero terms, so $\delta f_\mu = 0$ for all $\mu \in \mathrm{M}$. But then $f_\mu \in \mathcal{C}$ and $a \in \mathcal{D}$, which is a contradiction. □

Proposition 5.7. *Let $\mathcal{D}$ be a ring of constants in some Δ-extension of $\mathcal{F}$. Let $\phi\colon \mathcal{D} \to \mathcal{F}[\mathcal{D}]$ be the inclusion. Then ${}^r\phi$ is bijective with inverse $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{F}[\mathcal{D}]$.*

Proof. By Proposition 2.1, $\mathcal{F} \otimes_{\mathcal{C}} \mathcal{D}$ is isomorphic to $\mathcal{F}[\mathcal{D}]$. By the previous proposition, ${}^i\phi$ is bijective with inverse $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{F}[\mathcal{D}]$. The result then follows from Proposition 3.4. □

Corollary 5.8. *Let $\mathcal{D}$ be a ring of constants in some Δ-extension of $\mathcal{F}$. Then $\mathcal{F}[\mathcal{D}]$ is almost constant.*

Part II. Strongly normal extensions

In this part we assume that $\mathcal{C} = \mathcal{F}^\Delta$ is *algebraically closed*. $\mathcal{G}$ is a Δ-extension field of $\mathcal{F}$ that is finitely Δ-generated over $\mathcal{F}$.

6. Δ-isomorphisms

Definition 6.1. By a Δ-*isomorphism* of $\mathcal{G}$ over $\mathcal{F}$ we mean a Δ-isomorphism σ of $\mathcal{G}$ into some extension $\mathcal{E}$ of $\mathcal{G}$ such that $\sigma \mid \mathcal{F} = \mathrm{id}$.

Here, as in Kolchin [10, p. 25], we allow $\mathcal{E}$ to be any Δ-field that contains $\mathcal{G}$ (allowing us to form the compositum $\mathcal{G}\sigma\mathcal{G}$). Alternatively we could use a fixed universal Δ-field for $\mathcal{E}$, as done in Kolchin [11] and [12]. The advantage in doing so is that we could then speak of the *set* of Δ-isomorphisms. However, as we shall see, we are only interested in equivalence classes of Δ-isomorphisms, and those do form a set.

Definition 6.2. $\mathcal{P} = \mathcal{G} \otimes_{\mathcal{F}} \mathcal{G}$.

Note that $\mathcal{P}$ is a reduced ring by Zariski-Samuel [38, Corollary, p. 196] but not, in general an integral domain. But it is, by Zariski-Samuel [38, Corollary 2, p. 198], whenever $\mathcal{G}$ is a regular extension of $\mathcal{F}$ (i.e. $\mathcal{F}$ is algebraically closed in $\mathcal{G}$). There are several articles that study various aspects of tensor products of fields; see, for example, Sharp [29] and Vámos [35].

Definition 6.3. Let σ be a Δ-isomorphism of $\mathcal{G}$ over $\mathcal{F}$. Denote by $\overline{\sigma} : \mathcal{P} = \mathcal{G} \otimes_{\mathcal{F}} \mathcal{G} \to \mathcal{G}[\sigma\mathcal{G}]$ the Δ-homomorphism defined by $\overline{\sigma}(a \otimes b) = a\sigma b$, and by $\mathfrak{p}_\sigma$ the kernel of $\overline{\sigma}$.

Proposition 6.4. *Let σ be a Δ-isomorphism of $\mathcal{G}$ over $\mathcal{F}$. Then $\mathfrak{p}_\sigma$ is a prime Δ-ideal of $\mathcal{P}$. Conversely, if $\mathfrak{p}$ is any prime Δ-ideal of $\mathcal{P}$, then there is a Δ-isomorphism σ of $\mathcal{G}$ over $\mathcal{F}$ such that $\mathfrak{p} = \mathfrak{p}_\sigma$.*

Proof. $\mathfrak{p}_\sigma$ is prime because $\mathcal{G}[\sigma\mathcal{G}]$ is an integral domain. For the converse, let $\pi : \mathcal{P} \to \mathcal{P}/\mathfrak{p}$ be the canonical mapping. π restricted to $\mathcal{G} \otimes 1$ is an isomorphism, and so we may identify $\mathcal{G}$ with a subring of $\mathcal{P}/\mathfrak{p}$. π restricted to $1 \otimes \mathcal{G}$ is also an isomorphism and defines a Δ-isomorphism of $\mathcal{G}$ over $\mathcal{F}$ into the field of quotients of $\mathcal{P}/\mathfrak{p}$. □

7. Specializations of Δ-isomorphisms

Kolchin ([11, p. 772] and [12, p. 385]) introduced the following notion of specialization of Δ-isomorphisms.

Definition 7.1. Let σ and τ be Δ-isomorphisms of $\mathcal{G}$ over $\mathcal{F}$. We say that τ is a *specialization* of σ, denoted $\sigma \to \tau$, if there is a Δ-homomorphism

$$\phi : \mathcal{G}[\sigma\mathcal{G}] \to \mathcal{G}[\tau\mathcal{G}]$$

over $\mathcal{G}$ with $\phi(\sigma g) = \tau g$ for every $g \in \mathcal{G}$. We call ϕ the *realization* of the specialization $\sigma \to \tau$. If in addition $\tau \to \sigma$, we say that τ is a *generic specialization* of σ and write $\sigma \leftrightarrow \tau$.

Proposition 7.2. *Let σ and τ be Δ-isomorphisms of $\mathcal{G}$ over $\mathcal{F}$. Then $\sigma \to \tau$ if and only if $\mathfrak{p}_\sigma \subset \mathfrak{p}_\tau$, and $\sigma \leftrightarrow \tau$ if and only if $\mathfrak{p}_\sigma = \mathfrak{p}_\tau$.*

Proof. "Chase" the diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{p}_\sigma & \longrightarrow & \mathcal{P} & \longrightarrow & \mathcal{G}[\sigma\mathcal{G}] & \longrightarrow & 0 \\ & & \downarrow & & \| & & \downarrow & & \\ 0 & \longrightarrow & \mathfrak{p}_\tau & \longrightarrow & \mathcal{P} & \longrightarrow & \mathcal{G}[\tau\mathcal{G}] & \longrightarrow & 0 \end{array}$$

□

Thus the set of equivalence classes under generic specialization is canonically identified with the set of prime Δ-ideals of $\mathcal{P}$, i.e. $\operatorname{diffspec}\mathcal{P}$. Specialization plays a central role in Kolchin's axiomatization of algebraic groups, just as it played a central role in Weil's work. In fact, in Weil [37, Chapter II] one can see where Kolchin got some of his ideas. In Chapter IV, Weil uses specializations to define the notion of algebraic variety.

8. Differential automorphisms

Proposition 8.1. *Suppose that σ is a Δ-automorphism of $\mathcal{G}$ over $\mathcal{F}$. Then $\mathfrak{p}_\sigma$ is generated as an ideal by $\sigma g \otimes 1 - 1 \otimes g$ $(g \in \mathcal{G})$. It is a maximal ideal and hence a maximal Δ-ideal.*

Proof. $\mathfrak{p}_\sigma$ is the kernel of $\overline{\sigma} : \mathcal{G} \otimes_{\mathcal{F}} \mathcal{G} \to \mathcal{G}$, where $\overline{\sigma}(a \otimes b) = a\sigma b$. Since the image is a field, $\mathfrak{p}_\sigma$ is a maximal ideal. Evidently $\overline{\sigma}(\sigma g \otimes 1 - 1 \otimes g) = 0$ for every $g \in \mathcal{G}$. If $x \in \mathfrak{p}_\sigma$, then

$$x = \sum_{i=1}^{n} \big(a_i \otimes b_i\big) = -\sum_{i=1}^{n} \big(a_i \otimes 1\big)\big(\sigma b_i \otimes 1 - 1 \otimes b_i\big) + \big(\sum_{i=1}^{n} a_i \sigma b_i\big) \otimes 1.$$

The last term is 0 since $\overline{\sigma} x = 0$. □

Corollary 8.2. $\mathfrak{p}_{\mathrm{id}}$ *is generated as an ideal by $g \otimes 1 - 1 \otimes g$ $(g \in \mathcal{G})$.*

9. Isolated isomorphisms

Definition 9.1. A Δ-isomorphism of $\mathcal{G}$ over $\mathcal{F}$ is *isolated* if it is not a non-generic specialization of any other.

By Proposition 7.2, σ is isolated if and only if $\mathfrak{p}_\sigma$ is a minimal prime Δ-ideal of $\mathcal{P}$. We shall see that there are only a finite number of isolated isomorphisms up to generic specialization, using the assumption that $\mathcal{G}$ is a finitely Δ-generated extension of $\mathcal{F}$.

Lemma 9.2. *Let $\mathcal{F}^\circ$ be the relative algebraic closure of $\mathcal{F}$ in $\mathcal{G}$. Then $\mathcal{F}^\circ \otimes_{\mathcal{F}} \mathcal{F}^\circ$ has a finite number of prime ideals. They are all maximal, minimal, and pairwise relatively prime.*

Proof. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{F}^\circ \otimes_{\mathcal{F}} \mathcal{F}^\circ$ and let σ be an isomorphism of $\mathcal{F}^\circ$ over $\mathcal{F}$ with $\mathfrak{p} = \mathfrak{p}_\sigma$ (by Proposition 6.4, where the set of derivations is empty). If $\mathcal{F}_a$ is an algebraic closure of $\mathcal{F}^\circ$, then there exists an isomorphism $\phi : \sigma\mathcal{F}^\circ \to \mathcal{F}_a$ over $\mathcal{F}$. Evidently $\phi \circ \sigma$ is a generic specialization of σ, i.e. we may suppose that σ takes $\mathcal{F}^\circ$ into $\mathcal{F}_a$. Since $\mathcal{F}^\circ$ is finitely generated over $\mathcal{F}$, by Kolchin [12, Corollary 2, p. 113], there are only a finite number of such Δ-isomorphisms. Hence $\mathcal{F}^\circ \otimes_{\mathcal{F}} \mathcal{F}^\circ$ has only a finite number of prime ideals.

The image of $\overline{\sigma} : \mathcal{F}^\circ \otimes_{\mathcal{F}} \mathcal{F}^\circ \to \mathcal{F}^\circ[\sigma\mathcal{F}^\circ]$ is a field, so $\mathfrak{p}_\sigma$ is maximal, i.e. every prime ideal is maximal. Hence there are no inclusions among them, they are all minimal and pairwise relatively prime. □

Corollary 9.3. *Every prime ideal of $\mathcal{F}^\circ \otimes_{\mathcal{F}} \mathcal{F}^\circ$ is a Δ-ideal.*

Proof. Proposition 2.8. Alternatively, note that any prime ideal is of the form $\mathfrak{p}_\sigma$, where σ is an isomorphism of $\mathcal{F}^\circ$ over $\mathcal{F}$. But all such isomorphisms are Δ-isomorphisms. □

By Bourbaki [2, Lemma 1, p. 73] every prime (Δ-) ideal of a Δ-ring $\mathcal{R}$ contains a minimal prime ideal, and by Proposition 2.8 that minimal prime ideal is a Δ-ideal. A priori a given prime Δ-ideal may contain several minimal prime Δ-ideals, but not so in $\mathcal{P}$. First we need a lemma, which is Vámos [35, Theorem 3, p. 28], but, for the sake of completeness, we prove it here.

Lemma 9.4. *The formula*

$$\mathfrak{p} \to \mathfrak{p} \cap (\mathcal{F}^\circ \otimes_{\mathcal{F}} \mathcal{F}^\circ)$$

defines a bijection between the set of minimal prime Δ-ideals of $\mathcal{P}$ and the set of prime ideals of $\mathcal{F}^\circ \otimes_{\mathcal{F}} \mathcal{F}^\circ$. The inverse is

$$\mathfrak{q} \to \mathfrak{q}\mathcal{P}.$$

Proof. Let $\mathcal{R} = \mathcal{F}^\circ \otimes_{\mathcal{F}} \mathcal{F}^\circ$, and let $\mathfrak{q}$ be a prime ideal of $\mathcal{R}$. Note that

$$\mathcal{P} \approx \mathcal{G} \otimes^\circ_{\mathcal{F}} \mathcal{R} \otimes^\circ_{\mathcal{F}} \mathcal{G},$$

so, by Zariski-Samuel [38, Theorem 35, p. 184],

$$\mathcal{P}/\mathfrak{q}\mathcal{P} \approx \mathcal{G} \otimes^\circ_{\mathcal{F}} (\mathcal{R}/\mathfrak{q}) \otimes^\circ_{\mathcal{F}} \mathcal{G}.$$

However, $\mathfrak{q}$ is also maximal, so $\mathcal{R}/\mathfrak{q}$ is a field. Since $\mathcal{F}^\circ$ is algebraically closed in $\mathcal{G}$, the tensor product is an integral domain (Zariski-Samuel [38, Corollary 2, p. 198]). Hence $\mathfrak{q}\mathcal{P}$ is prime.

But $\mathfrak{q}$ is also a Δ-ideal of $\mathcal{R}$, so $\mathfrak{q}\mathcal{P}$ is a Δ-ideal. Moreover, $\mathfrak{q} \subset \mathfrak{q}\mathcal{P} \cap \mathcal{R}$. The maximality of $\mathfrak{q}$ implies that $\mathfrak{q} = \mathfrak{q}\mathcal{P} \cap \mathcal{R}$. The minimality of $\mathfrak{q}$ implies that $\mathfrak{q}\mathcal{P}$ is a minimal prime ideal and therefore a minimal prime Δ-ideal. Finally, let $\mathfrak{p} \subset \mathcal{P}$ be a minimal prime Δ-ideal. Then $(\mathfrak{p} \cap \mathcal{R})\mathcal{P} \subset \mathfrak{p}$, and the minimality of $\mathfrak{p}$ gives equality. □

Proposition 9.5. *$\mathcal{P}$ has a finite number of minimal prime Δ-ideals. Every prime Δ-ideal of $\mathcal{P}$ contains a unique minimal Δ-ideal. If $\mathcal{G}$ is regular over $\mathcal{F}$, then there is a single minimal prime Δ-ideal in $\mathcal{P}$, and $\mathcal{P}$ is an integral domain.*

Proof. The uniqueness is because the prime ideals of $\mathcal{F}^\circ \otimes_{\mathcal{F}} \mathcal{F}^\circ$ are relatively prime. If $\mathcal{G}$ is regular over $\mathcal{F}$, then $\mathcal{F}^\circ \otimes_{\mathcal{F}} \mathcal{F}^\circ = \mathcal{F}$, which has a unique prime Δ-ideal. □

Looking ahead (Proposition 31.2), this proposition will show that $\operatorname{diffspec} \mathcal{P}$ is the disjoint union of a finite number of irreducible components. Vámos [35, Proposition 5, p. 28] proves that $\mathcal{R}$ is a direct product of a finite number of integral domains, and his proof easily generalizes to Δ-rings. However, we will not use that result here. Kolchin phrases the above proposition in terms of isomorphisms:

Corollary 9.6. *There is a finite set of isolated Δ-isomorphisms with the property that every Δ-isomorphism is a specialization of a unique one of these. If $\mathcal{G}$ is a regular extension of $\mathcal{F}$, then there is a single isolated Δ-isomorphism with this property.*

10. The minimal prime $\mathfrak{p}^\circ$

Proposition 10.1. *Let $\mathcal{H}$ be a Δ-field with $\mathcal{F} \subset \mathcal{H} \subset \mathcal{G}$. Then the kernel of the canonical Δ-homomorphism $\phi : \mathcal{P} = \mathcal{G} \otimes_{\mathcal{F}} \mathcal{G} \to \mathcal{G} \otimes_{\mathcal{H}} \mathcal{G}$ is generated, as an ideal, by $h \otimes 1 - 1 \otimes h$ ($h \in \mathcal{H}$). If $g \in \mathcal{G}$ is such that $\phi(g \otimes 1 - 1 \otimes g) = 0$, then $g \in \mathcal{H}$.*

Proof. Evidently $h \otimes 1 - 1 \otimes h \in \ker \phi$ for every $h \in \mathcal{H}$. Choose a basis Λ of $\mathcal{G}$ over $\mathcal{H}$. For $x \in \ker \phi$ we have, for some $a_{i\lambda}, b_{i\mu} \in \mathcal{H}$,

$$\begin{aligned} x &= \sum_{i=1}^{n} \big(\sum_{\lambda \in \Lambda} a_{i\lambda} \lambda \otimes \sum_{\mu \in \Lambda} b_{i\mu} \mu \big) \\ &= - \sum_{i=1}^{n} \sum_{\lambda, \mu \in \Lambda} (a_{i\lambda} \lambda \otimes \mu)(b_{i\mu} \otimes 1 - 1 \otimes b_{i\mu}) \\ &\qquad + \sum_{\lambda, \mu} \big(\sum_{i=1}^{n} a_{i\lambda} b_{i\mu} \big) \lambda \otimes \mu. \end{aligned}$$

The last term is 0 since $\phi(x) = 0$. For the last statement, observe that if $g \notin \mathcal{H}$, then 1 and g are linearly independent over $\mathcal{H}$, so $g \otimes_{\mathcal{H}} 1 \neq 1 \otimes_{\mathcal{H}} g$. □

Lemma 10.2. *Every zero divisor of $\mathcal{P}$ is contained in some minimal prime Δ-ideal of $\mathcal{P}$.*

Proof. Suppose that $rs = 0$ with $r, s \in \mathcal{P}$, and $s \neq 0$. Because $\mathcal{P}$ is reduced, s^{∞} is a multiplicative set that does not contain 0. Let $\mathfrak{m}$ be a Δ-ideal that is maximal with respect to avoiding s^{∞}. By Proposition 2.5, $\mathfrak{m}$ is prime. Let $\mathfrak{p}$ be a minimal prime Δ-ideal contained in $\mathfrak{m}$. Since $s \notin \mathfrak{p}$, we must have $r \in \mathfrak{p}$. □

Definition 10.3. $\mathfrak{p}^{\circ}$ is the unique minimal prime Δ-ideal contained in $\mathfrak{p}_{\mathrm{id}}$.

Proposition 10.4. *Let $\mathcal{F}^{\circ}$ be the algebraic closure of $\mathcal{F}$ in $\mathcal{G}$. Then $\mathfrak{p}^{\circ}$ is generated by $f \otimes 1 - 1 \otimes f$ ($f \in \mathcal{F}^{\circ}$). Moreover, $\mathcal{P}/\mathfrak{p}^{\circ}$ is isomorphic to $\mathcal{G} \otimes^{\circ}_{\mathcal{F}} \mathcal{G}$.*

Proof. By Proposition 10.1, the ideal $\mathfrak{q}$ generated by $f \otimes 1 - 1 \otimes f$ ($f \in \mathcal{F}^{\circ}$) is a Δ-ideal and $\mathcal{R}/\mathfrak{q} \approx \mathcal{G} \otimes^{\circ}_{\mathcal{F}} \mathcal{G}$. By Corollary 8.2, $\mathfrak{q} \subset \mathfrak{p}_{\mathrm{id}}$. Since $\mathcal{G} \otimes^{\circ}_{\mathcal{F}} \mathcal{G}$ is an integral domain, $\mathfrak{q}$ is prime. We claim that $\mathfrak{q}$ consists entirely of zero divisors, which will imply that $\mathfrak{q}$ is the unique minimal prime Δ-ideal contained in $\mathfrak{p}_{\mathrm{id}}$.

For $f \in \mathcal{F}^{\circ}$, let $P_n X^n + \cdots + P_0$ be a minimal polynomial for f over $\mathcal{F}$. Then

$$\begin{aligned} \big(f \otimes 1 - 1 \otimes f\big) \, \big(\sum_{i=1}^{n} P_i \sum_{k=0}^{i-1} (f^k \otimes f^{i-1-k}) \big) \\ = \big(\sum_{i=1}^{n} P_i f^i \big) \otimes 1 - 1 \otimes \big(\sum_{i=1}^{n} P_i f^i \big) \\ = (-P_0) \otimes 1 - 1 \otimes (-P_0) = 0. \end{aligned}$$

Since $f^i \otimes f^j$ ($0 \leq i, j < n$) are linearly independent over $\mathcal{F}$, the second factor is non-zero and therefore $f \otimes 1 - 1 \otimes f$ is a zero divisor. □

11. Strong isomorphisms

Definition 11.1. If σ is a Δ-isomorphism of $\mathcal{G}$ over $\mathcal{F}$, then $\mathcal{C}(\sigma) = (\mathcal{G}\sigma\mathcal{G})^{\Delta}$.

Recall the following definition from Kolchin [12, pp. 388-389].

Definition 11.2. Let σ be a Δ-isomorphism $\mathcal{G}$ over $\mathcal{F}$. Then σ is *strong* if

(1) $\sigma \,|\, \mathcal{G}^{\Delta} = \mathrm{id}$,
(2) $\mathcal{G}\sigma\mathcal{G} = \mathcal{G}\mathcal{C}(\sigma) = \sigma\mathcal{G}\mathcal{C}(\sigma)$.

Note that the field compositums $\mathcal{G}\sigma\mathcal{G}$, etc., are defined since, by Definition 6.1, $\sigma\mathcal{G}$ is contained in some extension $\mathcal{E}$ of $\mathcal{G}$. In the Kolchin treatment, the image of a Δ-isomorphism is always contained in a fixed universal Δ-field $\mathcal{U}$.

Definition 11.3. Let $\mathfrak{p} \subset \mathcal{P}$ be a prime Δ-ideal. Then:

(1) $\kappa(\mathfrak{p}) = \mathrm{qf}(\mathcal{P}/\mathfrak{p})$, the quotient field of $\mathcal{P}/\mathfrak{p}$,
(2) $\mathcal{C}(\mathfrak{p}) = \kappa(\mathfrak{p})^{\Delta}$,
(3) $\mathcal{G}$ denotes the image of $\mathcal{G} \otimes_{\mathcal{F}} 1$ in $\kappa(\mathfrak{p})$, and
(4) $\mathcal{G}(\mathfrak{p})$ denotes the image of $1 \otimes_{\mathcal{F}} \mathcal{G}$ in $\kappa(\mathfrak{p})$.

Thus $\kappa(\mathfrak{p}) = \mathcal{G}(\mathfrak{p})\mathcal{G}$ and $\mathcal{P}/\mathfrak{p} = \mathcal{G}[\mathcal{G}(\mathfrak{p})]$.

Definition 11.4. Let $\mathfrak{p}$ be a prime Δ-ideal of $\mathcal{P}$. Then $\mathfrak{p}$ is *strong* if

(1) $c \otimes 1 - 1 \otimes c \in \mathfrak{p}$ for every $c \in \mathcal{G}^{\Delta}$,
(2) $\kappa(\mathfrak{p}) = \mathcal{G}(\mathfrak{p})\mathcal{G} = \mathcal{G}\mathcal{C}(\mathfrak{p}) = \mathcal{G}(\mathfrak{p})\mathcal{C}(\mathfrak{p})$.

Proposition 11.5. *Let σ be a Δ-isomorphism of $\mathcal{G}$ over $\mathcal{F}$. Then σ is strong if and only if $\mathfrak{p}_\sigma$ is strong.*

12. Strongly normal extensions

Definition 12.1. By a *strongly normal* extension of $\mathcal{F}$ is meant a finitely Δ-generated extension $\mathcal{G}$ such that every Δ-isomorphism of $\mathcal{G}$ over $\mathcal{F}$ is strong, or equivalently, such that every prime Δ-ideal of $\mathcal{P}$ is strong.

Proposition 12.2. *Let $\mathcal{G}$ be a strongly normal extension of $\mathcal{F}$. Then $\mathcal{G}^{\Delta} = \mathcal{C}$.*

Proof. If $c \in \mathcal{G}^{\Delta}$, then $c \otimes 1 - 1 \otimes c$ is in every prime Δ-ideal $\mathfrak{p}$ of $\mathcal{P}$, and hence, by Proposition 2.8, in every prime ideal. But the intersection of these is (0), since $\mathcal{P}$ is reduced. Therefore $c \in \mathcal{F}$. □

In Kolchin [11, p. 772] a strongly normal extension was assumed to have finite transcendence degree over $\mathcal{F}$. In Kolchin-Lang [15, p. 105], even more was assumed, namely that $\mathcal{G}$ was finitely generated as a field over $\mathcal{F}$. In [12] Kolchin dropped both those assumptions and proved them instead.

Lemma 12.3. *Let $\mathcal{G}$ be a finitely Δ-generated Δ-extension field of $\mathcal{F}$ having finite transcendence degree over $\mathcal{F}$. Then $\mathcal{G}$ is finitely generated as a field over $\mathcal{F}$.*

Proof. Using induction on the number of Δ-generators of $\mathcal{G}$ over $\mathcal{F}$, we may assume that $\mathcal{G} = \mathcal{F}\langle\eta\rangle$. For $s \in \mathbb{N}$ denote by $\Theta(s)$ the set of derivation operators $\theta = \delta_1^{e_1} \cdots \delta_m^{e_m}$ with $e_1 + \cdots + e_m \leq s$. Also denote by $\mathcal{G}_s$ the field (not a Δ-field) generated over $\mathcal{F}$ by $\theta\eta$ for $\theta \in \Theta(s)$. Thus

$$\mathcal{G}_s = \mathcal{F}\big((\theta\eta)_{\theta \in \Theta(s)}\big).$$

Observe that $\mathcal{G}_s$ is finitely generated over $\mathcal{F}$. Because $\mathcal{G}$ has finite transcendence degree over $\mathcal{F}$, there exists $s \in \mathbb{N}$ such that each $\theta\eta$ ($\theta \in \Theta(s)$) is algebraic over $\mathcal{G}_{s-1}$. We claim that $\mathcal{G} = \mathcal{G}_s$.

Let $\theta' \in \Theta(s+1)$, say $\theta' = \delta_i\theta$, where $\theta \in \Theta(s)$, and let $P \in \mathcal{G}_{s-1}[X]$ be a minimal polynomial of $\theta\eta$ over $\mathcal{G}_{s-1}$. Then

$$\theta'\eta = \delta_i\theta\eta = -\frac{P^{\delta_i}(\theta\eta)}{P'(\theta\eta)},$$

where $P^{\delta_i} \in \mathcal{G}_s[X]$ is the result of applying δ_i to the coefficients of P, and $P' = dP/dX$. We see that $\theta'\eta \in \mathcal{G}_s$, so $\mathcal{G}_{s+1} \subset \mathcal{G}_s$. Next let $\theta' \in \Theta(t)$ with $t > s+1$, say $\theta' = \delta_i\theta$. Using induction, we may assume that $\theta\eta \in \mathcal{G}_s$, so

$$\theta'\eta = \delta_i\theta\eta \in \mathcal{G}_{s+1} \subset \mathcal{G}_s$$

by what we have already proven. □

Proposition 12.4. *Suppose that $\mathcal{G}$ is strongly normal over $\mathcal{F}$. Then $\mathcal{G}$ is finitely generated as a field over $\mathcal{F}$. If σ is a Δ-isomorphism of $\mathcal{G}$ over $\mathcal{F}$, then $\mathcal{C}(\sigma)$ is finitely generated over $\mathcal{C}$.*

Proof. For the second statement note that $\mathcal{G}$ is finitely Δ-generated over $\mathcal{F}$ by hypothesis, hence $\mathcal{G}\sigma\mathcal{G}$ is finitely Δ-generated over $\mathcal{G}$. By Kolchin [12, Corollary 1, p. 113], $\mathcal{C}(\sigma)$ is finitely generated over $\mathcal{C}$.

For the first statement, consider the minimal prime Δ-ideal $\mathfrak{p}^\circ$ of Definition 10.3. Since $\mathcal{C}(\mathfrak{p}^\circ)$ is finitely generated over $\mathcal{C}$, $\mathcal{G}(\mathfrak{p}^\circ)\mathcal{G} = \mathcal{G}\mathcal{C}(\mathfrak{p}^\circ)$ is finitely generated over $\mathcal{G}$. By Proposition 10.4, $\mathcal{G}(\mathfrak{p}^\circ)\mathcal{G} = \mathrm{qf}(\mathcal{G} \otimes^\circ_{\mathcal{F}} \mathcal{G})$, so $\mathcal{G}$ has finite transcendence degree over $\mathcal{F}^\circ$ and hence over $\mathcal{F}$. Now we can use the lemma. □

Proposition 12.5. *Let $\mathcal{G}$ be a finitely Δ-generated Δ-extension of $\mathcal{F}$ such that $\mathcal{G}^\Delta = \mathcal{C}$. Suppose that every Δ-isomorphism σ of $\mathcal{G}$ over $\mathcal{F}$ satisfies*

$$\sigma\mathcal{G} \subset \mathcal{G}\mathcal{D}_\sigma,$$

where $\mathcal{D}_\sigma$ is a field of constants. Then $\mathcal{G}$ is strongly normal over $\mathcal{F}$.

Proof. We first show that $\mathcal{G} \subset \sigma\mathcal{G}\mathcal{E}_\sigma$ for some field of constants $\mathcal{E}_\sigma$. The Δ-isomorphism $\sigma^{-1} : \sigma\mathcal{G} \to \mathcal{G}$ extends to some Δ-isomorphism ϕ:

$$\begin{array}{ccc} \mathcal{G}\sigma\mathcal{G} & \xrightarrow{\phi} & \mathcal{E} \\ \uparrow & & \uparrow \\ \sigma\mathcal{G} & \xrightarrow{\sigma^{-1}} & \mathcal{G}. \end{array}$$

Then $\tau = \phi \,|\, \mathcal{G}$ is an isomorphism of $\mathcal{G}$ over $\mathcal{F}$, and we have

$$\mathcal{G} = \phi^{-1}\tau\mathcal{G} \subset \phi^{-1}(\mathcal{G}\mathcal{D}_\tau) = (\phi^{-1}\mathcal{G})(\phi^{-1}\mathcal{D}_\tau) = \sigma\mathcal{G}\mathcal{E}_\sigma.$$

Next we show that $\sigma\mathcal{G} \subset \mathcal{G}\mathcal{D}_\sigma$ implies $\sigma\mathcal{G} = \mathcal{G}\mathcal{C}(\sigma)$. We may assume that $\mathcal{C}(\sigma) \subset \mathcal{D}_\sigma$. If $x \in \sigma\mathcal{G}$, then

$$x = \frac{\sum_i f_i c_i}{\sum_j g_j d_j},$$

where $f_i, g_j \in \mathcal{G}$, $c_i, d_j \in \mathcal{D}$, and the g_j are linearly independent over $\mathcal{C}(\sigma)$. The family (f_i, xg_j) is linearly dependent over $\mathcal{D}_\sigma$ and therefore, by Proposition 2.1, over $\mathcal{C}(\sigma)$. Similarly $\mathcal{G} = \sigma\mathcal{G}\mathcal{C}(\sigma)$. □

13. Constrained extensions

A Galois (not differential) extension is contained in an algebraic closure of the base field. There is an analogous statement in differential algebra, namely that a strongly normal extension is constrained or, in model-theoretic terms, is contained in a "differential closure" of the base field (Scanlon [28, Section 4]).

This was proven in Kolchin [13, Theorem 3], but his proof uses knowledge of the Galois group that we do not yet have, as well as group cohomology, which we

prefer to avoid in this presentation. Therefore we review the notions and give a more elementary proof here. As our only interest is in finite constrained families, we restrict our attention to that case. For a more general treatment, see Kolchin [12, Section 10, p. 142] and [13].

In this section $\eta = (\eta_1, \ldots, \eta_n)$ denotes a finite family of elements of some Δ-extension field of $\mathcal{F}$. This implies that $\mathcal{F}\{\eta\}$ is an integral domain.

Definition 13.1. η is *constrained over* $\mathcal{F}$ if there exists $C \in \mathcal{F}\{\eta\}$, $C \neq 0$, such that C goes to 0 under every non-generic specialization of η. C is called the *constraint*. We also say that η is *C-constrained over* $\mathcal{F}$.

This means that if $\mathcal{H}$ is some Δ-extension field of $\mathcal{F}$ and $\phi\colon \mathcal{F}\{\eta\} \to \mathcal{H}$ is a Δ-homomorphism over $\mathcal{F}$, then either ϕ is injective or else $\phi(C) = 0$. We say that a Δ-integral domain $\mathcal{R}$ containing $\mathcal{F}$ is constrained over $\mathcal{F}$ if every finite family of elements of $\mathcal{R}$ is constrained over $\mathcal{F}$.

Proposition 13.2. *Suppose that $\eta = (\eta_1, \ldots, \eta_n)$ is constrained over $\mathcal{F}$. Then $\mathcal{F}\{\eta\}$ is constrained over $\mathcal{F}$.*

Proof. Kolchin [12, Proposition 7, p. 142]. See also [13, Proposition 1, p. 144]. (The assumption that the family η is finite is required for this proposition.) □

Proposition 13.3. *η is C-constrained over $\mathcal{F}$ if and only if every non-zero prime Δ-ideal of $\mathcal{F}\{\eta\}$ contains C.*

Proof. Non-zero prime Δ-ideals are kernels of non-generic specializations. □

An interesting special case occurs when $C = 1$. Recall that $\mathcal{R}$ is said to be Δ-simple if $\mathcal{R}$ contains no non-zero proper Δ-ideal. For Ritt algebras, as we are assuming, this is equivalent to saying that $\mathcal{R}$ has no non-zero prime Δ-ideal by Proposition 2.5. It follows that (0) is a prime Δ-ideal, so $\mathcal{R}$ is an integral domain.

Proposition 13.4. *Let $\mathcal{R} = \mathcal{F}\{\eta\}$. Then the following are equivalent.*

(1) *η is 1-constrained over $\mathcal{F}$.*
(2) *$\mathcal{R}$ is Δ-simple.*
(3) *Every non-zero element of $\mathcal{R}$ is a Δ-unit (Definition 4.3).*

Proof. (1) ⇒ (2): The previous proposition.
(2) ⇒ (3): If $r \in \mathcal{R}$, $r \neq 0$, then the Δ-ideal $[r]$ is non-zero and hence contains 1.
(3) ⇒ (1): If $\mathfrak{a} \subset \mathcal{R}$ is a non-zero Δ-ideal and $r \in \mathfrak{a}$, $r \neq 0$, then $1 \in [r] \subset \mathfrak{a}$. □

Corollary 13.5. *If η is C-constrained, then $\mathcal{R}_C$ is Δ-simple.*

Proof. Evidently $(\eta_1, \ldots, \eta_n, \frac{1}{C})$ is 1-constrained. □

Corollary 13.6. *Suppose that $\Sigma \subset \mathcal{R}$ is a multiplicative set consisting of Δ-units. Then $\mathcal{R}\Sigma^{-1}$ is Δ-simple if and only if $\mathcal{R}$ is.*

Proof. By Proposition 4.2 there is a bijection between $\mathtt{P}(\mathcal{R}\Sigma^{-1})$ and $\mathtt{P}(\mathcal{R}, \Sigma)$, which is $\mathtt{P}(\mathcal{R})$ by Proposition 4.4. □

The following proposition uses the assumption that $\mathcal{C}$ is algebraically closed. This simple proof was suggested by Alberto Baider.

Proposition 13.7. *Suppose that $\mathcal{R}$ is a Δ-simple ring containing $\mathcal{F}$ that is finitely generated over $\mathcal{F}$ (not finitely Δ-generated). Then $\mathrm{qf}(\mathcal{R})^{\Delta} = \mathcal{C}$.*

Proof. Suppose that $c \in \mathrm{qf}(\mathcal{R})^\Delta$. Let

$$\mathfrak{a} = \{b \in \mathcal{R} \mid bc \in \mathcal{R}\}.$$

Evidently $\mathfrak{a}$ is a non-zero ideal, and it is a Δ-ideal because c is constant. Therefore $1 \in \mathfrak{a}$ and $c \in \mathcal{R}^\Delta$. Because $\mathrm{qf}(\mathcal{R})^\Delta$ is a field, every non-zero element of $\mathcal{R}^\Delta$ is invertible.

Suppose that c is transcendental over $\mathcal{F}$. We know (e.g., by Atiyah-MacDonald [1, Proposition 5.23, p. 66]) that there exists $P \in \mathcal{F}[c]$ such that any homomorphism $\phi\colon \mathcal{F}[c] \to \mathcal{F}$ with $\phi(P) \neq 0$ extends to a homomorphism (not a Δ-homomorphism) of $\mathcal{R}$ into an algebraic closure of $\mathcal{F}$. Choose $d \in \mathcal{C}$ with $P(d) \neq 0$, and let ϕ be the substitution homomorphism $c \mapsto d$ over $\mathcal{F}$. Then $c - d \mapsto 0$. But $c - d$ is a constant and therefore is either 0 or invertible in $\mathcal{R}$. Since it cannot be invertible, $c = d$.

It is well known that if c is algebraic over $\mathcal{F}$ then it is algebraic over $\mathcal{C}$ (and therefore is in $\mathcal{C}$). Indeed, if P is the minimal monic polynomial for c over $\mathcal{F}$, then δP vanishes at c and has strictly smaller degree, and hence is 0. □

In the above proposition we could have used extensions of Δ-homomorphisms (Kolchin [12, Theorem 3, p. 140]) and obtained the same result for the case in which $\mathcal{R}$ finitely Δ-generated over $\mathcal{F}$. But the extension theorem for Δ-homomorphisms is quite deep, and we do not need the added generality here.

Proposition 13.8. *Let $\mathcal{G}$ be a strongly normal extension of $\mathcal{F}$. Then there is a finite family $\eta = (\eta_1, \ldots, \eta_n)$ such that $\mathcal{G} = \mathcal{F}(\eta)$ and $\mathcal{R} = \mathcal{F}[\eta]$ is constrained. In particular, η may be chosen so that $\mathcal{R}$ is Δ-simple.*

Proof. The last statement is immediate from Corollary 13.5. Let $\mathcal{F}^\circ$ denote the algebraic closure of $\mathcal{F}$ in $\mathcal{G}$. Since $\mathcal{G}$ is finitely generated over $\mathcal{F}$, by Proposition 12.4, so is $\mathcal{F}^\circ$. We may assume that the family η includes generators for $\mathcal{F}^\circ$ over $\mathcal{F}$, thus reducing the problem to the case where $\mathcal{F} = \mathcal{F}^\circ$, which we assume. The advantage is that $\mathcal{P}$ is then an integral domain and (0) is the minimal prime $\mathfrak{p}^\circ$ of Section 10 and Proposition 10.4. We write $\otimes$ for $\otimes_{\mathcal{F}}$.

Choose finite families η with $\mathcal{G} = \mathcal{F}(\eta)$ and γ with $\mathcal{C}(\mathfrak{p}^\circ) = \mathcal{C}(\gamma)$, and let $\mathcal{R} = \mathcal{F}[\eta]$. Increase the family if necessary to ensure that $\mathcal{R}$ is a Δ-ring. Because $\mathfrak{p}^\circ = (0)$ is strong, we may write

$$\eta_i \otimes 1 = \frac{A_i}{B}, \qquad A_i, B \in (1 \otimes \mathcal{R})[\gamma],$$
$$\gamma_j = \frac{C_j}{D}, \qquad C_j, D \in \mathcal{R} \otimes \mathcal{R}.$$

"Plugging" the second formula into the first, we see that there exists $e \in \mathbb{N}$ such that $D^e B \in \mathcal{R} \otimes \mathcal{R}$. If we choose a vector space basis Λ of $\mathcal{R}$ over $\mathcal{F}^\circ$, then $D^e B$ can be written uniquely in the form

$$D^e B = \sum_{\lambda \in \Lambda} \lambda \otimes r_\lambda, \qquad r_\lambda \in \mathcal{R}.$$

Choose some non-zero r_λ, which we denote by C. We claim that η is C-constrained.

Suppose that ϕ is a Δ-homomorphism of $\mathcal{R}$ over $\mathcal{F}$ (into some Δ-field) such that $\phi(C) \neq 0$, and let $\mathfrak{p} = \ker \phi$. Note that $\mathcal{G} \otimes \mathfrak{p} \subset \mathcal{G} \otimes \mathcal{R}$ is a prime Δ-ideal. Indeed, the quotient is $\mathcal{G} \otimes \mathcal{R}/\mathfrak{p}$, by Zariski-Samuel [38, Theorem 35, p. 184], which is an integral domain because $\mathcal{F}(= \mathcal{F}^\circ)$ is algebraically closed in $\mathcal{G}$. By construction,

$D^eB \notin \mathcal{G} \otimes \mathfrak{p}$. Choose a maximal Δ-ideal $\mathfrak{m} \subset (\mathcal{G} \otimes \mathcal{R})_{D^eB}$ containing $\mathcal{G} \otimes \mathfrak{p}$, and let

$$\phi : (\mathcal{G} \otimes \mathcal{R})_{D^eB} \to \mathcal{S}$$

be the canonical Δ-homomorphism. We identify $\mathcal{G}$ with the image of $\mathcal{G} \otimes 1$ and let $\xi_i = \phi(1 \otimes \eta_i)$.

Because the kernel is a maximal Δ-ideal, $\mathcal{S}$ is Δ-simple. Also $\mathcal{S}$ is finitely generated over $\mathcal{G}$, and hence, by Proposition 13.7, $(\operatorname{qf} \mathcal{S})^\Delta = \mathcal{C}$. This implies that $\phi(\gamma_j) \in \mathcal{C}$. Therefore

$$\eta_i = \phi(\eta_i) = \frac{\phi A_i}{\phi B} \in \mathcal{F}(\xi).$$

Therefore the transcendence degree of $\mathcal{F}(\xi)$ is at least that of $\mathcal{G} = \mathcal{F}(\eta)$. By Zariski-Samuel [38, Theorem 29, p. 101] the mapping $\mathcal{F}[\eta] \to \mathcal{F}[\xi]$ is an isomorphism, which implies that $\mathfrak{p} = (0)$. □

14. The Galois group

In the remainder of this part, $\mathcal{G}$ is a strongly normal extension of $\mathcal{F}$.

Definition 14.1. By the *Galois group of* $\mathcal{G}$ *over* $\mathcal{F}$ we mean the group of all Δ-automorphisms of $\mathcal{G}$ over $\mathcal{F}$. We denote it by $\operatorname{Gal}(\mathcal{G}/\mathcal{F})$.

In Proposition 8.1 we showed that if σ is a Δ-automorphism of $\mathcal{G}$ over $\mathcal{F}$, then $\mathfrak{p}_\sigma$ is a maximal Δ-ideal of $\mathcal{P}$. For strongly normal extensions we have the converse. Here we use the assumption that $\mathcal{C}$ is algebraically closed.

Proposition 14.2. *Let $u \in \mathcal{P}$, $u \neq 0$, and $\mathfrak{p}$ a Δ-ideal of $\mathcal{P}$ that is maximal with respect to avoiding $u^\infty = \{u^e \mid e \in \mathbb{N}\}$. Then $\mathcal{C}(\mathfrak{p}) = \mathcal{C}$.*

Proof. By Proposition 2.5, $\mathfrak{p}$ is a prime Δ-ideal. Let v be the image of u in $\mathcal{G}[\mathcal{G}(\mathfrak{p})]$. Then every non-zero Δ-ideal of $\mathcal{G}[\mathcal{G}(\mathfrak{p})]$ contains some power of v, i.e. $\mathcal{G}[\mathcal{G}(\mathfrak{p})]_v$ is Δ-simple. If this ring were finitely generated over $\mathcal{G}$, we would be done by Proposition 13.7. However, it is not.

By Proposition 13.8 we may choose a finite family ξ with $\mathcal{G}(\mathfrak{p}) = \mathcal{F}(\xi)$ such that $\mathcal{F}[\xi]$ is Δ-simple. By Proposition 13.4, the multiplicative set $\mathcal{F}[\xi]^*$ consists of Δ-units. We also choose $r \in \mathcal{F}[\xi]^*$ such that $rv \in \mathcal{G}[\xi]$. Then

$$\mathcal{G}[\mathcal{G}(\mathfrak{p})]_v = \mathcal{G}[\xi]_{rv}(\mathcal{F}[\xi]^*)^{-1}.$$

By Corollary 13.6 $\mathcal{G}[\xi]_{rv}$ is Δ-simple, and by Proposition 13.7

$$\mathcal{C}(\mathfrak{p}) = \mathcal{G}\mathcal{G}(\mathfrak{p})^\Delta = (\operatorname{qf} \mathcal{G}[\xi]_{rv})^\Delta = \mathcal{G}^\Delta = \mathcal{C}.$$

□

Corollary 14.3. *Let $u \in \mathcal{P}$, $u \neq 0$, and $\mathfrak{p}$ a prime Δ-ideal that is maximal with respect to avoiding u. Then $\mathfrak{p}$ is a maximal ideal. If $\mathfrak{p} = \mathfrak{p}_\sigma$, then $\sigma \in \operatorname{Gal}(\mathcal{G}/\mathcal{F})$.*

Proof. By the proposition, $\mathcal{G}\mathcal{C}(\mathfrak{p}) = \mathcal{G}$. Therefore $\mathcal{P}/\mathfrak{p} = \mathcal{G}$, so $\mathfrak{p}$ is a maximal ideal. Also $\sigma\mathcal{G} = \mathcal{G}\mathcal{C}(\sigma) = \mathcal{G}$, so σ is a Δ-automorphism. □

Thus every maximal Δ-ideal of $\mathcal{P}$ is a maximal ideal. But not conversely. There may be automorphisms of $\mathcal{G}$ over $\mathcal{F}$ that are not Δ-automorphisms. The next corollary states that the set of closed points of $\operatorname{diffspec} \mathcal{P}$ is canonically identified with $\operatorname{Gal}(\mathcal{G}/\mathcal{F})$.

Corollary 14.4. *A Δ-isomorphism σ is a Δ-automorphism if and only if $\mathfrak{p}_\sigma$ is a maximal Δ-ideal.*

Proof. Proposition 8.1. □

15. Jacobson rings

We continue to assume that $\mathcal{G}$ is a strongly normal extension of $\mathcal{F}$. The material of this section shows that the set of Δ-automorphisms carries the same information as the set of Δ-isomorphisms, or, more precisely, that the maximal Δ-ideals of $\mathcal{P}$ are very dense in $P = \operatorname{diffspec} \mathcal{P}$, i.e., every non-empty locally closed subset of P contains a closed point. Recall (Bourbaki [2, pp. 351–354]) that a Jacobson ring is one in which every prime ideal is the intersection of a family of maximal ideals.

Definition 15.1. A Δ-ring $\mathcal{R}$ is Δ-*Jacobson* if every prime Δ-ideal is the intersection of a family of maximal Δ-ideals.

Proposition 15.2. *$\mathcal{P}$ is a Δ-Jacobson ring.*

Proof. Corollary 14.3. □

By an intermediate Δ-field $\mathcal{H}$ we mean one with $\mathcal{F} \subset \mathcal{H} \subset \mathcal{G}$. Evidently $\mathcal{G}$ is a strongly normal extension of $\mathcal{H}$. The following proposition shows that $\mathcal{G}$ is a *normal* extension of $\mathcal{F}$ in the sense of Kolchin [11, p. 791]. It is a (very small) part of the fundamental theorem, which we shall prove in Section 19; however, it is easy to prove at this point and worth recording.

Proposition 15.3. *Let $\mathcal{H}$ be an intermediate Δ-field and $g \in \mathcal{G}$. If $\sigma g = g$ for all $\sigma \in \operatorname{Gal}(\mathcal{G}/\mathcal{H})$, then $g \in \mathcal{H}$.*

Proof. By Proposition 8.1, $g \otimes 1 - 1 \otimes g \in \mathfrak{p}_\sigma$ for all $\sigma \in \operatorname{Gal}(\mathcal{G}/\mathcal{H})$. It follows from Corollary 14.4 and the previous proposition that $g \otimes 1 - 1 \otimes g$ is in every prime Δ-ideal of $\mathcal{P}$. Since $\mathcal{P}$ is reduced, $g \otimes 1 - 1 \otimes g = 0$. By Proposition 10.1, $g \in \mathcal{H}$. □

Later we shall need the following "lying over" result.

Proposition 15.4. *Let $\mathcal{H}$ be an intermediate Δ-field. If $\mathfrak{p}$ is a maximal Δ-ideal of $\mathcal{H} \otimes_{\mathcal{F}} \mathcal{H}$, then there exists a maximal Δ-ideal $\mathfrak{q}$ of $\mathcal{P}$ such that $\mathfrak{q} \cap (\mathcal{H} \otimes_{\mathcal{F}} \mathcal{H}) = \mathfrak{p}$.*

Proof. $\sqrt{\mathfrak{p}\mathcal{P}}$ is a radical Δ-ideal of $\mathcal{P}$, so, by Proposition 2.7, the intersection of prime Δ-ideals and therefore the intersection of maximal Δ-ideals. If $\mathfrak{q}$ is any one of them, then $\mathfrak{q} \cap (\mathcal{H} \otimes_{\mathcal{F}} \mathcal{H}) = \mathfrak{p}$ since $\mathfrak{p}$ is a maximal Δ-ideal. □

16. Δ-corings

The material in this section is based on Sweedler [31] and Cohn [4, Section 3.2]. In this section $\mathcal{R}$ is any Δ-ring.

Definition 16.1. Let $\mathcal{M}$ be a left and right Δ-$\mathcal{R}$-module. We say that $\mathcal{M}$ is a Δ-$\mathcal{R}$-*bimodule* if, for every $a, b \in \mathcal{R}$ and $m \in \mathcal{M}$,

$$(am)b = a(mb) \quad \text{and} \quad 1m = m = m1.$$

Observe that $\mathcal{P} = \mathcal{G} \otimes_{\mathcal{F}} \mathcal{G}$ is a Δ-$\mathcal{G}$-bimodule, and that the left and right $\mathcal{G}$-module structures are *not* the same.

Definition 16.2. A Δ-$\mathcal{R}$-bimodule $\mathcal{M}$, together with Δ-$\mathcal{R}$-bimodule mappings $\mu : \mathcal{M} \to \mathcal{M} \otimes_{\mathcal{R}} \mathcal{M}$ and $\epsilon : \mathcal{M} \to \mathcal{R}$, is a Δ-*coring* if the following diagrams are commutative:

Coassociative:

$$\begin{array}{ccc} \mathcal{M} & \xrightarrow{\mu} & \mathcal{M} \otimes_{\mathcal{R}} \mathcal{M} \\ {\scriptstyle\mu}\downarrow & & \downarrow{\scriptstyle \mathrm{id}\otimes\mu} \\ \mathcal{M} \otimes_{\mathcal{R}} \mathcal{M} & \xrightarrow[\mu\otimes\mathrm{id}]{} & \mathcal{M} \otimes_{\mathcal{R}} \mathcal{M} \otimes_{\mathcal{R}} \mathcal{M} \end{array}$$

Counit:

$$\begin{array}{ccc} \mathcal{M} & \xrightarrow{\mu} & \mathcal{M} \otimes_{\mathcal{R}} \mathcal{M} \\ {\scriptstyle\mu}\downarrow & \searrow^{\mathrm{id}} & \downarrow{\scriptstyle \mathrm{id}\cdot\epsilon} \\ \mathcal{M} \otimes_{\mathcal{R}} \mathcal{M} & \xrightarrow[\epsilon\cdot\mathrm{id}]{} & \mathcal{M} \end{array}$$

The counit diagram means that if $m \in \mathcal{M}$ and $\mu(m) = \sum_{i=1}^{n} a_i \otimes b_i$, then

$$\sum_{i=1}^{n} \epsilon(a_i) b_i = m = \sum_{i=1}^{n} a_i \epsilon(b_i).$$

Note that the left-hand side uses the left module structure and the right-hand side uses the right module structure. If the left and right module structures were the same, we would have a Hopf algebra.

Definition 16.3. Let $\mathcal{M}$ be a Δ-$\mathcal{R}$-coring. A Δ-*coideal* $\mathfrak{a}$ is a Δ-$\mathcal{R}$-subbimodule of $\mathcal{M}$ satisfying $\epsilon(\mathfrak{a}) = 0$ and $\mu(\mathfrak{a}) \subset \mathfrak{a} \otimes_{\mathcal{R}} \mathcal{M} + \mathcal{M} \otimes_{\mathcal{R}} \mathfrak{a}$.

Definition 16.4. Define $\mu : \mathcal{P} \to \mathcal{P} \otimes_{\mathcal{G}} \mathcal{P}$ by

$$\mu(a \otimes_{\mathcal{F}} b) = (a \otimes_{\mathcal{F}} 1) \otimes_{\mathcal{G}} (1 \otimes_{\mathcal{F}} b) \qquad (a, b \in \mathcal{G}),$$

and $\epsilon : \mathcal{P} \to \mathcal{G}$ by

$$\epsilon(a \otimes_{\mathcal{F}} b) = ab \qquad (a, b \in \mathcal{G}).$$

Proposition 16.5. *$\mathcal{P}$ is a Δ-coring.*

Proof. Straightforward. □

Cohn [4, p. 33] calls this the *standard coring of $\mathcal{P}$ over $\mathcal{G}$*. Recall that an intermediate Δ-field is a Δ-field $\mathcal{H}$ with $\mathcal{F} \subset \mathcal{H} \subset \mathcal{G}$.

Definition 16.6. Let $\mathcal{H}$ be an intermediate Δ-field. Then we define

$$C(\mathcal{H}) = \ker : \mathcal{G} \otimes_{\mathcal{F}} \mathcal{G} \to \mathcal{G} \otimes_{\mathcal{H}} \mathcal{G}.$$

If $\mathfrak{a} \subset \mathcal{P}$ is a Δ-coideal, then we define

$$I(\mathfrak{a}) = \{g \in \mathcal{G} \mid g \otimes 1 - 1 \otimes g \in \mathfrak{a}\}.$$

Clearly $C(\mathcal{H})$ is a Δ-coideal and $I(\mathfrak{a})$ is an intermediate Δ-field.

Proposition 16.7. *Let $\mathfrak{a} \subset \mathcal{P}$ be a Δ-coideal and let $\mathcal{H} = I(\mathfrak{a})$. Then $\mathfrak{a} = \ker \phi$, where $\phi : \mathcal{P} \to \mathcal{G} \otimes_{\mathcal{H}} \mathcal{G}$.*

Proof. By Proposition 10.1, $\ker\phi$ is generated as an ideal by $h\otimes_{\mathcal{F}}1-1\otimes_{\mathcal{F}}h$ ($h\in\mathcal{H}$). But $h\otimes_{\mathcal{F}}1-1\otimes_{\mathcal{F}}h\in\mathfrak{a}$ by definition of $\mathcal{H}$; hence $\ker\phi\subset\mathfrak{a}$.

Let $\mathcal{N}=\mathcal{G}\otimes_{\mathcal{H}}\mathcal{G}$, $\mathcal{M}=\mathcal{P}/\mathfrak{a}$ and $\pi:\mathcal{P}\to\mathcal{M}$ be the canonical homomorphisms of Δ-corings, and consider the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker\phi & \longrightarrow & \mathcal{P} & \xrightarrow{\phi} & \mathcal{N} & \longrightarrow & 0 \\ & & \downarrow & & \| & & \vdots\,\zeta & & \\ 0 & \longrightarrow & \mathfrak{a} & \longrightarrow & \mathcal{P} & \xrightarrow{\pi} & \mathcal{M} & \longrightarrow & 0. \end{array}$$

By Sweedler [31, Fundamental Lemma, p. 397] or Cohn [4, Proposition 3.2.2, p. 34], ζ is injective. Hence $\ker\phi=\mathfrak{a}$. □

The following is a differential version of the fundamental theorem of Sweedler corings (Sweedler [31, Theorem 2.1 p. 395] or Cohn [4, Theorem 3.2.3, p. 35].

Proposition 16.8. *The mappings $\mathcal{H}\to C(\mathcal{H})$ and $\mathfrak{a}\to I(\mathfrak{a})$ are bijective and inverse to each other.*

Proof. Let $\mathcal{H}$ be an intermediate Δ-field and let $\phi:\mathcal{P}\to\mathcal{G}\otimes_{\mathcal{H}}\mathcal{G}$. Then, by Proposition 10.1, $h\in\mathcal{H}$ if and only if $h\otimes 1-1\otimes h\in\ker\phi=C(\mathcal{H})$. By definition, $h\otimes 1-1\otimes h\in C(\mathcal{H})$ if and only if $h\in I(C(\mathcal{H}))$. Let $\mathfrak{a}$ be a Δ-coideal. If $\phi:\mathcal{P}\to\mathcal{G}\otimes_{I(\mathfrak{a})}\mathcal{G}$, then, by the preceding proposition, $\mathfrak{a}=\ker\phi=C(I(\mathfrak{a}))$. □

Definition 16.9. Define an additive map $\mathrm{T}:\mathcal{P}\to\mathcal{P}$, called the *twist*, by

$$\mathrm{T}(a\otimes_{\mathcal{F}}b)=b\otimes_{\mathcal{F}}a.$$

Note that T is *not* a $\mathcal{G}$-bimodule mapping.

Proposition 16.10. *Suppose that $\mathfrak{a}$ is a Δ-coideal of $\mathcal{P}$. Then $\mathfrak{a}$ is a radical Δ-ideal that is stable under the twist.*

Proof. If $\mathcal{H}=I(\mathfrak{a})$, then $\mathfrak{a}$ is the kernel of $\mathcal{P}\to\mathcal{G}\otimes_{\mathcal{H}}\mathcal{G}$. Since the image is reduced, $\mathfrak{a}$ is a radical Δ-ideal. By Proposition 10.1, $\mathrm{T}(\mathfrak{a})\subset\mathfrak{a}$. □

17. Coideals and automorphisms

In Proposition 8.1 we characterized Δ-primes $\mathfrak{p}_\sigma$ where σ is a Δ-automorphism. In this section we relate those ideals to the coring operations and the twist.

Proposition 17.1. *Let $\sigma,\tau\in\mathrm{Gal}(\mathcal{G}/\mathcal{F})$. Then*

(1) $\mathfrak{p}_{\mathrm{id}}=\epsilon^{-1}(0)$,
(2) $\mathfrak{p}_{\sigma\tau}=\mu^{-1}(\mathfrak{p}_\sigma\otimes_{\mathcal{F}}\mathcal{G}+\mathcal{G}\otimes_{\mathcal{F}}\mathfrak{p}_\tau)$,
(3) $\mathfrak{p}_{\sigma^{-1}}=\mathrm{T}^{-1}(\mathfrak{p}_\sigma)$.

Proof. The first statement is immediate from Corollary 8.2. The third comes from the formula

$$\overline{\sigma^{-1}}=\sigma^{-1}\circ\overline{\sigma}\circ\mathrm{T}.$$

For the second, note that any $x\in\mathcal{P}$ may be written in the form

$$x=\sum_{i=1}^{n}\sigma a_i\otimes_{\mathcal{F}}b_i\qquad\text{for some } a_i,b_i\in\mathcal{G}.$$

Then

$$\begin{aligned}\mu(x) &= \sum_{i=1}^{n}(\sigma a_i \otimes_{\mathcal{F}} 1) \otimes_{\mathcal{G}} (1 \otimes_{\mathcal{F}} b_i)\\ &= \sum_{i=1}^{n}\big(\sigma a_i \otimes 1 - 1 \otimes a_i\big) \otimes_{\mathcal{G}} \big(1 \otimes_{\mathcal{F}} b_i\big)\\ &\qquad - \sum_{i=1}^{n}\big(1 \otimes_{\mathcal{F}} a_i\big) \otimes_{\mathcal{G}} \big(\tau b_i \otimes 1 - 1 \otimes b_i\big)\\ &\qquad + (1 \otimes_{\mathcal{F}} 1) \otimes_{\mathcal{G}} \big(\sum_{i=1}^{n} a_i \tau b_i \otimes_{\mathcal{F}} 1\big).\end{aligned}$$

The last term is 0 if and only if

$$\sigma\big(\sum_{i=1}^{n} a_i \tau b_i\big) = \overline{\sigma\tau}\big(\sum_{i=1}^{n} \sigma a_i \otimes b_i\big) = \overline{\sigma\tau}(x) = 0.$$

The result now follows from Proposition 8.1. □

18. Kolchin topology

The Kolchin (or differential Zariski) topology on $P = \operatorname{diffspec} \mathcal{P}$ induces a topology on the set of maximal Δ-ideals of $\mathcal{P}$, which, because of Corollary 14.4, is canonically identified with $\operatorname{Gal}(\mathcal{G}/\mathcal{F})$.

Definition 18.1. If $\mathfrak{a}$ is a radical Δ-ideal of $\mathcal{P}$, we define

$$v(\mathfrak{a}) = \{\sigma \in \operatorname{Gal}(\mathcal{G}/\mathcal{F}) \mid \mathfrak{a} \subset \mathfrak{p}_\sigma\}.$$

If H is a subset of $\operatorname{Gal}(\mathcal{G}/\mathcal{F})$, we define

$$z(H) = \bigcap_{\sigma \in H} \mathfrak{p}_\sigma.$$

Definition 18.2. A subset H of $\operatorname{Gal}(\mathcal{G}/\mathcal{F})$ is *closed* if $H = v(\mathfrak{a})$ for some radical Δ-ideal $\mathfrak{a} \subset \mathcal{P}$.

Evidently v is an order-reversing map from the set of radical Δ-ideals of $\mathcal{P}$ to the set of closed subsets of $\operatorname{Gal}(\mathcal{G}/\mathcal{F})$, and z goes the other way.

Proposition 18.3. *v and z are bijective and inverse to each other.*

Proof. Let $\mathfrak{a}$ be a radical Δ-ideal of $\mathcal{P}$, and set $H = v(\mathfrak{a})$. Since H consists of those σ with $\mathfrak{a} \subset \mathfrak{p}_\sigma$, we evidently have

$$\mathfrak{a} \subset \bigcap_{\sigma \in H} \mathfrak{p}_\sigma = z(H).$$

We also know, by Proposition 15.2 and Corollary 14.4, that there is a set $S \subset \operatorname{Gal}(\mathcal{G}/\mathcal{F})$ with

$$\mathfrak{a} = \bigcap_{\tau \in S} \mathfrak{p}_\tau.$$

Because $\mathfrak{a} \subset \mathfrak{p}_\tau$ for every $\tau \in S$, $S \subset H$. But then $\mathfrak{a} = z(S) \supset z(H)$.

Let H be a closed subset of $\operatorname{Gal}(\mathcal{G}/\mathcal{F})$, say $H = v(\mathfrak{a})$. By the above, $\mathfrak{a} = z(v(\mathfrak{a})) = z(H)$. Hence

$$H = v(\mathfrak{a}) = v(z(H)).$$ □

Proposition 18.4. *Let H be a closed subset of* $\mathrm{Gal}(\mathcal{G}/\mathcal{F})$. *Then H is a subgroup if and only if $z(H)$ is a Δ-coideal of $\mathcal{P}$.*

Proof. Let $\mathfrak{a} = z(H)$. Suppose first that $\mathfrak{a}$ is a Δ-coideal; we use Proposition 17.1. Since $\mathfrak{a} \subset \ker \epsilon = \mathfrak{p}_{\mathrm{id}}$, $\mathrm{id} \in H$. If σ and τ are in H, then

$$\mathfrak{a} \subset \mu^{-1}(\mathfrak{a} \otimes_{\mathcal{G}} \mathcal{P} + \mathcal{P} \otimes_{\mathcal{G}} \mathfrak{a}) \subset \mu^{-1}(\mathfrak{p}_\sigma \otimes_{\mathcal{G}} \mathcal{P} + \mathcal{P} \otimes_{\mathcal{G}} \mathfrak{p}_\tau) = \mathfrak{p}_{\sigma\tau},$$

so $\sigma\tau \in H$. By Proposition 16.10,

$$\mathfrak{a} \subset T^{-1}\mathfrak{a} \subset T^{-1}(\mathfrak{p}_\sigma) = \mathfrak{p}_{\sigma^{-1}},$$

which implies that $\sigma^{-1} \in H$.

Now assume that H is a subgroup of $\mathrm{Gal}(\mathcal{G}/\mathcal{F})$. Since $\mathrm{id} \in H$, $\mathfrak{a} \subset \mathfrak{p}_{\mathrm{id}} = \ker \epsilon$. Also

$$\begin{aligned}
\mu(\mathfrak{a}) &= \mu\Big(\bigcap_{\sigma,\tau \in H} \mathfrak{p}_{\sigma\tau}\Big) \\
&\subset \Big(\bigcap_{\sigma \in H} \mathfrak{p}_\sigma\Big) \otimes_{\mathcal{G}} \mathcal{P} + \mathcal{P} \otimes_{\mathcal{G}} \Big(\bigcap_{\tau \in H} \mathfrak{p}_\tau\Big) \\
&= \mathfrak{a} \otimes_{\mathcal{G}} \mathcal{P} + \mathcal{P} \otimes_{\mathcal{G}} \mathfrak{a}.
\end{aligned}$$

□

19. First fundamental theorem

As before, $\mathcal{G}$ is a strongly normal extension of $\mathcal{F}$.

Definition 19.1. If H is a subset of $\mathrm{Gal}(\mathcal{G}/\mathcal{F})$, we denote by $\mathcal{G}^H$ the *fixed field* of H, so

$$\mathcal{G}^H = \{h \in \mathcal{G} \mid \sigma h = h, \text{ for all } \sigma \in H\}.$$

If $\mathcal{H}$ is an intermediate Δ-field, then it is easy to check that $\mathcal{G}$ is strongly normal over $\mathcal{H}$, so we have a subgroup $\mathrm{Gal}(\mathcal{G}/\mathcal{H})$ of $\mathrm{Gal}(\mathcal{G}/\mathcal{F})$. In the following we use the notation of Proposition 16.8 as well as that of the previous section.

Proposition 19.2. *If H is a closed subgroup of* $\mathrm{Gal}(\mathcal{G}/\mathcal{F})$, *then*

$$\mathcal{G}^H = I(z(H)).$$

If $\mathcal{H}$ is an intermediate Δ-field, then

$$\mathrm{Gal}(\mathcal{G}/\mathcal{H}) = v(C(\mathcal{H})).$$

In particular, $\mathrm{Gal}(\mathcal{G}/\mathcal{H})$ *is closed.*

Proof. By definition

$$I(z(H)) = \{g \in \mathcal{G} \mid g \otimes 1 - 1 \otimes g \in \bigcap_{\sigma \in H} \mathfrak{p}_\sigma\}.$$

By Proposition 8.1, $g \otimes 1 - 1 \otimes g \in \mathfrak{p}_\sigma$ if and only if $\sigma(g) = g$, which gives the first equality. By Proposition 10.1, $C(\mathcal{H})$ is generated by $h \otimes 1 - 1 \otimes h$ for $h \in \mathcal{H}$. Thus $\sigma \in v(C(\mathcal{H}))$ if and only if $g \otimes 1 - 1 \otimes g \in \mathfrak{p}_\sigma$, i.e. $\sigma g = g$. □

Theorem 19.3 (First fundamental theorem)**.** *The mappings*

$$H \longmapsto \mathcal{G}^H$$

from closed subgroups to intermediate Δ-fields and

$$\mathcal{H} \longmapsto \mathrm{Gal}(\mathcal{G}/\mathcal{H})$$

from intermediate Δ-fields to closed subgroups are bijective and inverse to each other.

Proof. Propositions 16.8, 18.3 and 19.2. □

20. Second fundamental theorem

Proposition 20.1. *Let $\mathcal{H}$ be an intermediate Δ-field that is strongly normal over $\mathcal{F}$. If $\sigma \in \mathrm{Gal}(\mathcal{G}/\mathcal{F})$, then the restriction of σ to $\mathcal{H}$ is an automorphism of $\mathcal{H}$, and the mapping*

$$\mathrm{Gal}(\mathcal{G}/\mathcal{F}) \to \mathrm{Gal}(\mathcal{H}/\mathcal{F}), \qquad \sigma \mapsto \sigma|\mathcal{H},$$

is a surjective homomorphism with kernel $\mathrm{Gal}(\mathcal{G}/\mathcal{H})$.

Proof. Let $\sigma \in \mathrm{Gal}(\mathcal{G}/\mathcal{F})$. Then $\sigma|\mathcal{H}$ is a Δ-isomorphism of $\mathcal{H}$ onto $\sigma\mathcal{H}$, and it is strong. Therefore

$$\sigma\mathcal{H} = \mathcal{H}(\mathcal{H}\sigma\mathcal{H})^{\Delta}.$$

However,

$$(\mathcal{H}\sigma\mathcal{H})^{\Delta} \subset \mathcal{C}(\sigma) = (\mathcal{G}\sigma\mathcal{G})^{\Delta} = \mathcal{C},$$

since σ is an automorphism of $\mathcal{G}$; hence $\sigma|\mathcal{H}$ is an automorphism of $\mathcal{H}$. By Theorem 19.3, the kernel is $\mathrm{Gal}(\mathcal{G}/\mathcal{H})$. Surjectivity comes from Proposition 15.4. □

Definition 20.2. Let $\mathcal{D}$ be a field of constants containing $\mathcal{C}$. If $\sigma \in \mathrm{Gal}(\mathcal{G}/\mathcal{F})$, we denote by $\sigma_{\mathcal{D}}$ the unique automorphism of $\mathcal{G}\mathcal{D}$ over $\mathcal{F}\mathcal{D}$ extending σ.

The existence is because of Proposition 2.1. Uniqueness is clear.

Lemma 20.3. *Let $\mathcal{H}$ be an intermediate Δ-field and let $\mathcal{D}$ be a field of constants containing $\mathcal{C}$. If $x \in \mathcal{G}\mathcal{D}$ has the property that $\sigma_{\mathcal{D}}(x) = x$ for every $\sigma \in \mathrm{Gal}(\mathcal{G}/\mathcal{H})$, then $x \in \mathcal{H}\mathcal{D}$.*

Proof. We follow the argument of Kolchin [11, p. 798]. We may assume that $\mathcal{D} = \mathcal{C}(c_1, \ldots, c_r, d)$, where $c_1, \ldots, c_r$ are algebraically independent over $\mathcal{C}$ and d is algebraic over $\mathcal{C}(c_1, \ldots, c_r)$ of degree s. Write $c = (c_1, \ldots, c_r)$. Then there exist polynomials $A_i, B \in \mathcal{G}[X_1, \ldots, X_n]$ such that

(1) $x\,B(c) = \sum_{i=0}^{s-1} A_i(c) d^i$,
(2) $A_0, \ldots, A_{s-1}, B$ have no common factor,
(3) some coefficient of B is 1.

For $\sigma \in \mathrm{Gal}(\mathcal{G}/\mathcal{H})$ denote by A_i^{σ}, B^{σ} the result of applying σ to the coefficients of A_i, B. Then

$$\sum_{i=0}^{s-1} \big(B^{\sigma}(c)A_i(c) - B(c)A_i^{\sigma}(c)\big) d^i = 0;$$

therefore

$$B^{\sigma}(c)A_i(c) = B(c)A_i^{\sigma}(c) \quad (i = 1, \ldots, s-1).$$

By the second condition, B must divide B^{σ}, by the third $B = B^{\sigma}$, and therefore $A_i = A_i^{\sigma}$. The first fundamental theorem (Theorem 19.3) implies $A_0, \ldots, A_{s-1}, B \in \mathcal{H}[X_1, \ldots, X_r]$. □

Lemma 20.4. *Suppose that σ is a Δ-isomorphism of $\mathcal{G}$ over $\mathcal{F}$. Suppose that $\theta \in \mathrm{Gal}(\mathcal{G}/\mathcal{F})$ and $h \in \mathcal{G}$ satisfy $\theta_{\mathcal{C}(\sigma)}\sigma h \neq \sigma h$. Then there exists $\tau \in \mathrm{Gal}(\mathcal{G}/\mathcal{F})$ such that $\theta\tau h \neq \tau h$.*

Proof. Let $\mathcal{G} = \mathcal{F}(\eta)$, $\eta = (\eta_1, \dots, \eta_n)$, and $\mathcal{C}(\sigma) = \mathcal{C}(\gamma)$, $\gamma = (\gamma_1, \dots, \gamma_r)$. Since $\mathcal{G}$ is strongly normal over $\mathcal{F}$,

$$\begin{aligned} \gamma_j &= \frac{A_j}{B}, \qquad A_j, B \in \mathcal{F}[\eta, \sigma\eta], \\ \sigma h &= \frac{C}{D}, \qquad C, D \in \mathcal{F}[\eta, \gamma], \text{ and} \\ \theta_{\mathcal{C}(\sigma)}\sigma h - \sigma h &= \frac{E}{F}, \qquad E, F \in \mathcal{F}[\eta, \sigma\eta]. \end{aligned}$$

Using the first equation, choose $e \in \mathbb{N}$ such that

$$B^e D \in \mathcal{F}[\eta, \sigma\eta],$$

and $u \in \mathcal{P}$ with

$$\overline{\sigma} u = B\,(B^e D)\,E\,F.$$

Of course $u \notin \mathfrak{p}_\sigma$.

Next choose a Δ-ideal $\mathfrak{m}$ containing $\mathfrak{p}_\sigma$ that is maximal with respect to avoiding u^∞. By Corollary 14.3 and Proposition 14.2, $\mathfrak{m} = \mathfrak{p}_\tau$ for some $\tau \in \mathrm{Gal}(\mathcal{G}/\mathcal{F})$. Then σ specializes to τ, by Proposition 7.2, so there is a Δ-homomorphism

$$\phi\colon \mathcal{G}[\sigma\mathcal{G}] \to \mathcal{G}[\tau\mathcal{G}] = \mathcal{G}$$

over $\mathcal{G}$ with $\phi(\sigma g) = \tau g$ for $g \in \mathcal{G}$. Because $\phi(B(\eta, \sigma\eta) \neq 0$, we may extend ϕ to

$$\phi\colon \mathcal{G}[\sigma\mathcal{G}][\gamma] \to \mathcal{G}.$$

Observe that $\phi \circ \theta_{\mathcal{C}(\sigma)} = \theta = \theta \circ \phi$ on $\mathcal{F}[\eta]$, and $\phi \circ \theta_{\mathcal{C}(\sigma)} = \phi = \theta \circ \phi$ on $\mathcal{C}[\gamma]$; therefore

$$\phi \circ \theta_{\mathcal{C}(\sigma)} = \theta \circ \phi \quad \text{on } \mathcal{F}[\eta, \gamma].$$

Since $\phi(D) \neq 0$, it follows that

$$\phi\big(\theta_{\mathcal{C}(\sigma)}(\sigma h)\big) = \theta\big(\phi(\sigma h)\big) = \theta(\tau h),$$

and therefore

$$\theta\tau h - \tau h = \phi\big(\theta_{\mathcal{C}(\sigma)}\sigma h - \sigma h\big) = \frac{\phi E}{\phi F} \neq 0.$$

□

Theorem 20.5 (Second fundamental theorem)**.** *Let $\mathcal{H}$ be an intermediate Δ-field. Then $\mathcal{H}$ is strongly normal over $\mathcal{F}$ if and only if* $\mathrm{Gal}(\mathcal{G}/\mathcal{H})$ *is a normal subgroup of* $\mathrm{Gal}(\mathcal{G}/\mathcal{F})$*. When this is the case,* $\mathrm{Gal}(\mathcal{H}/\mathcal{F})$ *is isomorphic to the quotient group* $\mathrm{Gal}(\mathcal{G}/\mathcal{F})/\mathrm{Gal}(\mathcal{H}/\mathcal{F})$.

Proof. Suppose that $H = \mathrm{Gal}(\mathcal{G}/\mathcal{H})$ is normal in $\mathrm{Gal}(\mathcal{G}/\mathcal{F})$. We must show that every Δ-isomorphism σ of $\mathcal{H}$ over $\mathcal{F}$ is strong. By Proposition 12.2, $\sigma(c) = c$ for every constant c. Extend σ to a Δ-isomorphism of $\mathcal{G}$ over $\mathcal{F}$, which we also call σ. Then, since σ is strong, $\sigma(\mathcal{H}) \subset \mathcal{G}\mathcal{C}(\sigma)$. We claim that $\sigma(\mathcal{H}) \subset \mathcal{H}\mathcal{C}(\sigma)$.

Suppose not. Let $h \in \mathcal{H}$, with $\sigma h \notin \mathcal{H}\mathcal{C}(\sigma)$. Then there exists, by Lemma 20.3, $\theta \in \mathrm{Gal}(\mathcal{G}/\mathcal{H})$ such that $\theta_{\mathcal{C}(\sigma)}\sigma h \neq \sigma h$. By Lemmma 20.4, there exists $\tau \in \mathrm{Gal}(\mathcal{G}/\mathcal{F})$ with $\theta\tau(h) \neq \tau(h)$. But this is impossible since $\tau^{-1}\theta\tau \in \mathrm{Gal}(\mathcal{G}/\mathcal{H})$. We conclude that $\sigma\mathcal{H} \subset \mathcal{H}\mathcal{C}(\sigma)$ for every Δ-isomorphism σ of $\mathcal{H}$ over $\mathcal{F}$, and, by Proposition 12.5, that $\mathcal{H}$ is strongly normal over $\mathcal{F}$. The remainder of the proof comes from Proposition 20.1. □

Part III. Differential schemes

We assume familiarity with the basic properties of differential schemes as found in Kovacic [16]. We are primarily interested in reduced rings; however, we always explicitly state that hypothesis when needed. A reduced ring is AAD by [16, Proposition 9.9], so we may use the results of that paper. In this part $\mathcal{R}$ is a Δ-$\mathcal{F}$-algebra, $X = \operatorname{diffspec} \mathcal{R}$, $F = \operatorname{diffspec} \mathcal{F}$ and $C = \operatorname{diffspec} \mathcal{C}$.

21. Global sections

Definition 21.1. By an *affine Δ-$\mathcal{F}$-scheme* we mean an affine Δ-scheme $(X, \mathcal{O}_X)$, where $X = \operatorname{diffspec} \mathcal{R}$, $\mathcal{R}$ is a Δ-$\mathcal{F}$-algebra, and $\mathcal{O}_X$ a sheaf of Δ-$\mathcal{F}$-algebras. A morphism $(f, f^\#)$ of affine Δ-$\mathcal{F}$-schemes is a morphism of Δ-schemes in which $f^\#$ is a morphism of sheaves of Δ-$\mathcal{F}$-algebras. A *Δ-$\mathcal{F}$-scheme* is a Δ-scheme that has an open cover by affine Δ-$\mathcal{F}$-schemes.

It could happen that $Y = \operatorname{diffspec} \mathcal{S}$ is an affine Δ-$\mathcal{F}$-scheme without $\mathcal{S}$ being a Δ-$\mathcal{F}$-algebra. For example, $\mathcal{S} = \mathbb{C}[x]$ and $\mathcal{F} = \mathbb{C}(x)$ (where $\delta x = 1$), since $Y \approx F$. However, in this paper we assume that all rings encountered are Δ-$\mathcal{F}$-algebras, except where noted. For reduced schemes the notion of Δ-$\mathcal{F}$-scheme is the same as that of Δ-scheme over F. This follows from [16, Proposition 10.6].

As in [16, Definitions 4.3 and 4.4], the Δ-$\mathcal{F}$-algebra of global sections of X is denoted by

$$\widehat{\mathcal{R}} = \mathcal{O}_X(X) = \Gamma(X, \mathcal{O}_X),$$

and the canonical mapping by

$$\iota_{\mathcal{R}} \colon \mathcal{R} \to \widehat{\mathcal{R}}.$$

In general, $\iota_{\mathcal{R}}$ is neither injective nor surjective, see Kovacic [17] for details. However, the situation is much better for reduced rings.

Proposition 21.2. *If $\mathcal{R}$ is reduced, then $\iota_{\mathcal{R}} \colon \mathcal{R} \to \widehat{\mathcal{R}}$ is injective.*

Proof. [16, Proposition 10.1]. □

Because of this we may identify $\mathcal{R}$ with a subring of $\widehat{\mathcal{R}}$, making $\iota_{\mathcal{R}}$ the inclusion. The following proposition can be used in lieu of surjectivity. Proposition 21.5 also gives a kind of surjectivity, but is it less useful in practice.

Proposition 21.3. *Suppose that $\mathcal{R}$ is reduced and $s \in \widehat{\mathcal{R}}$. Then, for some $n \in \mathbb{N}$, there exist $a_1, b_1, \dots, a_n, b_n \in \mathcal{R}$ such that $1 \in \{b_1, \dots, b_n\}$ and $b_i\, s = a_i$ for each $i = 1, \dots, n$. In particular, for every $\mathfrak{p} \in X$ there exist $a, b \in \mathcal{R}$ with $b \notin \mathfrak{p}$ and $b\, s = a$.*

Proof. [16, Theorem 10.3]. □

Beware: this does *not* mean that $s = a/b$, since b need not be invertible in $\widehat{\mathcal{R}}$; in fact b might even be a zero divisor.

Proposition 21.4. *Suppose that $\mathcal{R}$ is reduced. Then $\widehat{\mathcal{R}}$ is also reduced.*

Proof. Assume that $s^e = 0$. In the notation of the previous proposition, $a_i^e = 0$ and hence $a_i = 0$ for each $i = 1, \dots, n$. For every $\mathfrak{p} \in X$, there exists i such that $b_i \notin \mathfrak{p}$, and therefore

$$s(\mathfrak{p}) = \frac{a_i}{b_i} = 0 \in \mathcal{R}_{\mathfrak{p}}.$$

This means that $s = 0$. □

Recall that a morphism $\phi\colon A \to B$ in a category is *epi* if whenever $f, g\colon B \to C$ agree on $\phi(A)$ then $f = g$, see for example MacLane [19, Section 5, p. 19].

Proposition 21.5. *Suppose that $\mathcal{R}$ is reduced. Then $\iota_{\mathcal{R}}$ is epi in the category of reduced Δ-$\mathcal{F}$-algebras.*

Proof. Suppose that $f, g\colon \widehat{\mathcal{R}} \to \mathcal{S}$ agree on $\mathcal{R} \subset \widehat{\mathcal{R}}$, and let $s \in \widehat{\mathcal{R}}$. If $\mathfrak{q}$ is any prime Δ-ideal of $\mathcal{S}$, then by Proposition 21.3 there exist $a, b \in \mathcal{R}$ with $b \notin f^{-1}(\mathfrak{q})$ and $b\,s = a$. Therefore

$$f(b)(f(s) - g(s)) = f(a) - g(a) = 0.$$

Since $f(b) \notin \mathfrak{q}$, $f(a) - g(a) \in \mathfrak{q}$. This is so for every prime ideal by Proposition 2.8. However, the intersection of these is (0) because $\mathcal{S}$ is reduced. □

In fact, $\iota_{\mathcal{R}}$ is epi in the category of Δ-rings having no non-zero Δ-zeros ([16, Section 7]), by essentially the same proof.

22. Homomorphisms

If $\phi\colon \mathcal{R} \to \mathcal{S}$ is a Δ-$\mathcal{F}$-algebra homomorphism, then the adjoint ${}^a\phi\colon Y \to X$, ${}^a\phi(\mathfrak{p}) = {}^p\phi(\mathfrak{p}) = \phi^{-1}(\mathfrak{p})$, is continuous by [16, Proposition 3.8].

Proposition 22.1. *Let $\phi\colon \mathcal{R} \to \mathcal{S}$ be a Δ-$\mathcal{F}$-homomorphism. Then ${}^a\phi$ is a homeomorphism if and only if ${}^r\phi$ is bijective.*

Proof. By [16, Proposition 3.9], ${}^a\phi$ is a homeomorphism onto its image if and only if ${}^r\phi$ is injective. By Proposition 3.3, ${}^a\phi$ is surjective if and only if ${}^r\phi$ is surjective. □

Proposition 22.2. *Suppose that $\mathcal{R}$ is reduced, and that $\Sigma \subset \mathcal{R}$ is a multiplicative subset consisting of Δ-units. Then the canonical mapping $\phi\colon \mathcal{R} \to \mathcal{R}\Sigma^{-1}$ induces an isomorphism*

$$({}^a\phi, \phi^{\#})\colon \operatorname{diffspec} \mathcal{R}\Sigma^{-1} \to \operatorname{diffspec} \mathcal{R}.$$

Proof. By Propositions 4.2 and 4.4,

$${}^r\phi\colon \mathtt{R}(\mathcal{R}\Sigma^{-1}) \to \mathtt{R}(\mathcal{R}, \Sigma) = \mathtt{R}(\mathcal{R})$$

is bijective; hence ${}^a\phi$ is a homeomorphism. Let $\mathfrak{q} \in \operatorname{diffspec} \mathcal{R}\Sigma^{-1}$ and $\mathfrak{p} = {}^a\phi(\mathfrak{q})$. By Proposition 3.5

$$\phi_{\mathfrak{q}}\colon \mathcal{R}_{\mathfrak{p}} \to \mathcal{S}_{\mathfrak{q}}, \qquad a/b \longmapsto \phi(a)/\phi(b),$$

is injective. Every element of $\mathcal{S}_{\mathfrak{q}}$ is of the form

$$\frac{a/s}{b/t} = \frac{at/1}{bs/1},$$

where $a, b \in \mathcal{R}$ and $s, t \in \Sigma$ and $b/t \notin \mathfrak{q}$. Because s is a Δ-unit, $bs \notin \mathfrak{p}$. Therefore $\phi_{\mathfrak{q}}$ is also surjective. □

23. Adjoints

For the study of closed subschemes we need a more general "adjoint" than simply ${}^a\phi$. Keigher [8, Corollary 5.7, p. 111] shows that the global sections functor has a left adjoint, which would give us what we need. Unfortunately his proof is not constructive, it uses results from category theory, and we need precise formulas. Therefore we sketch a direct proof here.

In this discussion we fix a Δ-$\mathcal{F}$-scheme Z (not necessarily affine) along with a Δ-$\mathcal{F}$-homomorphism $\phi\colon \mathcal{R} \to \mathcal{O}_Z(Z)$. From these data we shall construct a morphism $({}^{\mathbf{a}}\phi, \phi^\sharp)\colon Z \to X$ of Δ-$\mathcal{F}$-schemes. (Compare the notation ${}^{\mathbf{a}}\phi$ and $\phi^\sharp$ of this section with ${}^a\phi$ and $\phi^\#$ of the previous section.)

We use the following notation: $s \mapsto s|U$ is the restriction $\rho_{Z,U}\colon \mathcal{O}_Z(Z) \to \mathcal{O}_Z(U)$ and s_z is the image of s in the stalk, $s_z = \rho_z(s) \in \mathcal{O}_{Z,z}$. The maximal ideal of $\mathcal{O}_{Z,z}$ is denoted by $\mathfrak{m}_z$.

Definition 23.1. For $s \in \mathcal{O}_Z(Z)$ we define $Z_s = \{\, z \in Z \mid s_z \notin \mathfrak{m}_z \,\}$.

Lemma 23.2. *If $s \in \mathcal{O}_Z(Z)$, then Z_s is open and $s|Z_s$ is invertible in $\mathcal{O}_Z(Z_s)$.*

Proof. For each $z \in Z_s$, $s_z \notin \mathfrak{m}_z$, and hence s_z is invertible in $\mathcal{O}_{Z,z}$. This implies that there is an open neighborhood U of z such that $s|U$ is invertible. Hence $s_w \notin \mathfrak{m}_w$ for every $w \in U$, so $U \subset Z_s$. It follows that Z_s is open.

We know that s is invertible on an open cover of Z_s. Since inverses are unique, $s|Z_s$ is invertible. □

Definition 23.3. For $z \in Z$ define ${}^{\mathbf{a}}\phi(z) \in X$ by

$$ {}^{\mathbf{a}}\phi(z) = {}^p\phi\, {}^p\rho_z(\mathfrak{m}_z) = \phi^{-1}\rho_z^{-1}(\mathfrak{m}_z). $$

Proposition 23.4. *${}^{\mathbf{a}}\phi\colon Z \to X$ is continuous. More precisely, if $b \in \mathcal{R}$, then ${}^{\mathbf{a}}\phi^{-1}(D(b)) = Z_{\phi(b)}$.*

Proof. $z \in Z_{\phi(b)} \iff \phi(b)_z \notin \mathfrak{m}_z \iff b \notin {}^{\mathbf{a}}\phi(z) \iff {}^{\mathbf{a}}\phi(z) \in D(b)$. □

Our next goal is to define $\phi^\sharp\colon \mathcal{O}_X \to {}^{\mathbf{a}}\phi_*\mathcal{O}_Z$. Let $U \subset X$ be open and $s \in \mathcal{O}_X(U)$. For every $\mathfrak{p} \in U$ there exist $f, a, b \in \mathcal{R}$ such that

(1) $\mathfrak{p} \in D(f)$,
(2) if $q \in D(f)$ then $b \notin \mathfrak{q}$, and
(3) $s(\mathfrak{q}) = a/b \in \mathcal{R}_\mathfrak{q}$.

We call the triple (f, a, b) *local data* for s. Define $U_f = {}^{\mathbf{a}}\phi^{-1}(U) \cap Z_{\phi(f)}$ and

$$ t(f, a, b) = \frac{\phi(a)|U_f}{\phi(b)|U_f} \in \mathcal{O}_Z(U_f). $$

Note that $D(f) \subset D(b)$, so, by Proposition 23.4, $Z_{\phi(f)} \subset Z_{\phi(b)}$. By Lemma 23.2, $\phi(b)|U_f$ is invertible. Also note that the set of all U_f is an open cover of ${}^{\mathbf{a}}\phi^{-1}(U)$.

Lemma 23.5. *Suppose that (f, a, b) and (g, c, d) are local data for s. If $z \in U_f \cap U_g$, then $t(f, a, b)_z = t(g, c, d)_z$.*

Proof. Let $\mathfrak{q} = {}^{\mathbf{a}}\phi(z) \in D(f) \cap D(g) \cap U$. Then

$$ s(\mathfrak{q}) = \frac{a}{b} = \frac{c}{d} \in \mathcal{R}_\mathfrak{q}, $$

so there exists $x \in \mathcal{R}$, $x \notin \mathfrak{q}$, with $x(ad - bc) = 0$. Hence

$$ \phi(x)_z\big(\phi(a)_z\phi(d)_z - \phi(b)_z\phi(c)_z\big) = 0. $$

But $\mathfrak{q} \in D(x)$ implies that $z \in Z_{\phi(x)}$, so $\phi(x)_z$ is invertible. Hence

$$t(f,a,b)_z = \frac{\phi(a)_z}{\phi(b)_z} = \frac{\phi(c)_z}{\phi(d)_z} = t(g,c,d)_z.$$

□

We can now define $\phi^\sharp(s)$ to be the unique element $t \in \mathcal{O}_Z({}^{\mathbf{a}}\phi^{-1}(U))$ such that $t|U_f = t(f,a,b)$ for each triple (f,a,b) of local data for s. The construction shows that $\phi^\sharp(s)$ has the following property: if $z \in {}^{\mathbf{a}}\phi^{-1}(U)$, $\mathfrak{q} = {}^a\phi(z)$, and

$$s(\mathfrak{q}) = \frac{a}{b} \in \mathcal{R}_\mathfrak{p},$$

then

$$\phi^\sharp(s)_z = \frac{\phi(a)_z}{\phi(b)_z} \in \mathcal{O}_{Z,z}.$$

Proposition 23.6. *$({}^{\mathbf{a}}\phi, \phi^\sharp)\colon Z \to X$ is a morphism of Δ-$\mathcal{F}$-schemes.*

Proof. This is straightforward (but tedious), using the above characterization of $t = \phi^\sharp(s)$ by its value on the stalks. □

Proposition 23.7. *Let $(f, f^\#)\colon Z \to X$ be a morphism of Δ-$\mathcal{F}$-schemes and let $\phi = f^\#(X) \circ \iota_\mathcal{R}\colon \mathcal{R} \to \mathcal{O}_Z(Z)$. Then $f = {}^{\mathbf{a}}\phi$ and $f^\# = \phi^\sharp$.*

Proof. Let $z \in Z$ and $\mathfrak{p} = f(z)$. Then we have the following commutative diagram:

$$\begin{array}{ccccc} \mathcal{R} & \xrightarrow{\iota_\mathcal{R}} & \widehat{\mathcal{R}} & \xrightarrow{f^\#(X)} & \mathcal{O}_Z(Z) \\ & \searrow & \downarrow & & \downarrow \\ & & \mathcal{R}_\mathfrak{p} & \xrightarrow{f_z^\#} & \mathcal{O}_{Z,z} \end{array}$$

with ${f_z^\#}^{-1}(\mathfrak{m}_z) = \mathfrak{p}\mathcal{R}_\mathfrak{p}$. It follows that ${}^{\mathbf{a}}\phi(z) = \mathfrak{p} = f(z)$. The commutative diagram also shows that

$$f_z^\#\left(\frac{a}{b}\right) = \frac{\phi(a)_z}{\phi(b)_z},$$

which, by the remarks preceding Proposition 23.6, is the same as $\phi_z^\sharp(a/b)$. □

Proposition 23.8. *Let $\phi\colon \mathcal{R} \to \mathcal{O}_Z(Z)$ be a Δ-$\mathcal{F}$-homomorphism. Then $\phi = \phi^\sharp(X) \circ \iota_\mathcal{R}$.*

Proof. Since $\iota_\mathcal{R}(a) = a/1 \in \mathcal{R}_\mathfrak{p}$ for every $\mathfrak{p} \in X$, we have $\phi^\sharp(X)(\iota_\mathcal{R}(a))_z = \phi(a)_z \in \mathcal{O}_{Z,z}$ for every $z \in Z$. □

The previous two propositions show that there is a bijection between morphisms $Z \to X$ and homomorphisms $\mathcal{R} \to \mathcal{O}_Z(Z)$. This is the adjunction of Keigher [8, Corollary 5.7, p. 111].

Proposition 23.9. *Let $\mathcal{S}$ be a Δ-$\mathcal{F}$-algebra and Z a Δ-$\mathcal{F}$-scheme. Suppose that $\alpha\colon \mathcal{S} \to \mathcal{R}$ and $\phi\colon \mathcal{R} \to \mathcal{O}_Z(Z)$ are Δ-$\mathcal{F}$-homomorphisms. Then*

$${}^{\mathbf{a}}(\phi \circ \alpha) = {}^a\alpha \circ {}^{\mathbf{a}}\phi \qquad \textit{and}$$
$$(\phi \circ \alpha)^\sharp = \phi^\sharp \circ \alpha^\#.$$

Proof. Straightforward from the definitions. □

24. Closed subschemes

Definition 24.1. Let Z be a Δ-$\mathcal{F}$-scheme. A *closed immersion* is a Δ-$\mathcal{F}$-scheme Y and a morphism $(f, f^{\#})\colon (Y, \mathcal{O}_Y) \to (Z, \mathcal{O}_Z)$ such that f is a homeomorphism of Y onto a closed subset of Z and $f^{\#}$ is surjective.

Definition 24.2. Let Z be a Δ-$\mathcal{F}$-scheme. By a *closed subscheme* is meant a closed immersion $(f, f^{\#})\colon (Y, \mathcal{O}_Y) \to (Z, \mathcal{O}_Z)$ such that Y is a closed subset of Z and $f\colon Y \to Z$ is the inclusion.

Proposition 24.3. *Let $\mathfrak{a}$ be a Δ-ideal of $\mathcal{R}$ and $\pi\colon \mathcal{R} \to \mathcal{R}/\mathfrak{a}$ the canonical homomorphism. Then ${}^a\pi\colon \operatorname{diffspec}(\mathcal{R}/\mathfrak{a}) \to X$ is a closed immersion. The image is $V(\mathfrak{a}) \subset X$.*

Proof. ${}^r\pi$ is injective, so, by [16, Proposition 3.9], ${}^a\pi$ is a homeomorphism onto its image $V(\mathfrak{a})$. The surjectivity of π implies that $\pi^{\#}$ is surjective. □

Thus $V(\mathfrak{a})$ has the structure of closed subscheme of X. However, there may be other structures, since $V(\mathfrak{a}) = V(\mathfrak{b})$ does not imply that $\mathfrak{a} = \mathfrak{b}$. If we require that $\mathfrak{a}$ be a radical Δ-ideal, we get what Hartshorne [6, Example 3.2.6, p. 86] calls the *reduced induced closed subscheme*. In this case we have the converse: if Y is a reduced closed subscheme of X, then there a radical Δ-ideal $\mathfrak{a}$ such that Y is isomorphic to $\operatorname{diffspec}(\mathcal{R}/\mathfrak{a})$.

Lemma 24.4. *Let Y be a reduced Δ-$\mathcal{F}$-scheme and $s \in \mathcal{O}_Y(Y)$. If $Y_s = \emptyset$, then $s = 0$.*

Proof. We first assume that Y is affine, say $Y = \operatorname{diffspec} \mathcal{R}$. We claim that s is contained in every prime Δ-ideal of $\widehat{\mathcal{R}}$. Because minimal prime ideals are Δ-ideals (Proposition 2.8), it follows that s is contained in every prime ideal of $\widehat{\mathcal{R}}$. But $\widehat{\mathcal{R}}$ is reduced by Proposition 21.4, and hence $s = 0$.

Let $\mathfrak{q}$ be any prime Δ-ideal of $\widehat{\mathcal{R}}$ and let $\mathfrak{p} = \mathfrak{q} \cap \mathcal{R}$. By Proposition 21.3 there exist $a, b \in \mathcal{R}$ with $b\,s = a$ and $b \notin \mathfrak{p}$. Because $Y_s = \emptyset$, $s(\mathfrak{p}) \in \mathfrak{p}\mathcal{R}_{\mathfrak{p}}$; hence $a \in \mathfrak{p} \subset \mathfrak{q}$. But $b \notin \mathfrak{q}$, and therefore $s \in \mathfrak{q}$, which proves the claim.

If Y is not affine, we cover Y by reduced affine open subsets U_i, $i \in I$. From the affine case, $s|U_i = 0$ for each $i \in I$; hence $s = 0$. □

Lemma 24.5. *Let Y be a reduced Δ-$\mathcal{F}$-scheme and $s, t \in \mathcal{O}_Y(Y)$. Suppose that $s_y = 0$ whenever $y \in Y_t$. Then $st = 0$.*

Proof. If $y \in Y_t$, then $(st)_y \in \mathfrak{m}_y$, since $s_y = 0$ by hypothesis. If $y \notin Y_t$, then $(st)_y \in \mathfrak{m}_y$, since $t_y \in \mathfrak{m}_y$ by definition of Y_t. But this means that $Y_{st} = \emptyset$, and therefore $st = 0$ by the previous lemma. □

Proposition 24.6. *Suppose that $\mathcal{R}$ is reduced and Y is a reduced closed subscheme of X. Then there is a radical Δ-ideal $\mathfrak{a} \subset \mathcal{R}$ such that Y is isomorphic to* $\operatorname{diffspec}(\mathcal{R}/\mathfrak{a})$.

Proof. Let $(f, f^{\#})\colon (Y, \mathcal{O}_Y) \to (X, \mathcal{O}_X)$ be a closed immersion with $f\colon Y \to X$ being the inclusion. Let

$$\phi = f^{\#}(X) \circ \iota_{\mathcal{R}}\colon \mathcal{R} \to \mathcal{O}_Y(Y),$$

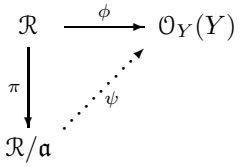
and $\mathfrak{a} = \ker \phi$. Because $\mathcal{O}_Y(Y)$ is reduced, $\mathfrak{a}$ is a radical Δ-ideal of $\mathcal{R}$. We claim that $Y = V(\mathfrak{a})$.

For every $\mathfrak{p} \in Y$, $\mathfrak{p} = f(\mathfrak{p}) = {}^{\mathbf{a}}\phi(\mathfrak{p}) = \phi^{-1}(\mathfrak{p})$ by Proposition 23.7, so $\mathfrak{a} \subset \mathfrak{p}$ and $Y \subset V(\mathfrak{a})$. Assume $Y \neq V(\mathfrak{a})$. Because Y is closed, there exists $b \in \mathcal{R}$ such that $D(b) \subset V(\mathfrak{a}) \setminus Y$ and $D(b) \neq \emptyset$. Then, using Proposition 23.4,

$$z_{\phi(b)} = f^{-1}(D(b)) = \emptyset,$$

and, by Lemma 24.4, $\phi(b) = 0$. Therefore $b \in \mathfrak{a} = \ker \phi$. But this, together with the assumption $D(b) \subset V(\mathfrak{a})$, implies that $D(b) = \emptyset$, which is a contradiction.

Let $\pi\colon \mathcal{R} \to \mathcal{R}/\mathfrak{a}$ be the canonical Δ-homomorphism, and define ψ by the following commutative diagram:



Then, using Propositions 23.7 and 23.9, $f = {}^{\mathbf{a}}\phi = {}^{a}\pi \circ {}^{\mathbf{a}}\psi$. Since f and ${}^{a}\pi$ are both homeomorphisms onto their image, ${}^{\mathbf{a}}\psi\colon Y = V(\mathfrak{a}) \to Z = \operatorname{diffspec}(\mathcal{R}/\mathfrak{a})$ is a homeomorphism. We must show that

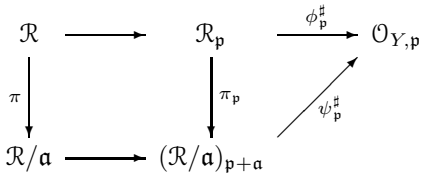
$$\psi^{\sharp}\colon \mathcal{O}_Z \to {}^{\mathbf{a}}\psi_* \mathcal{O}_Y$$

is an isomorphism, which we do by showing that the mapping on stalks

$$\psi^{\sharp}_{\mathfrak{p}}\colon (\mathcal{R}/\mathfrak{a})_{\mathfrak{p}+\mathfrak{a}} \to \mathcal{O}_{Y,\mathfrak{p}}, \quad \mathfrak{p} \in Y = V(\mathfrak{a}),$$

is an isomorphism.

Consider the following commutative diagram:



By Proposition 23.7, $\phi^{\sharp}_{\mathfrak{p}} = f^{\#}_{\mathfrak{p}}$, which is surjective by hypothesis. Therefore $\psi^{\sharp}_{\mathfrak{p}}$ is surjective. Suppose that $a \in \mathcal{R}$ is such that

$$0 = \psi^{\sharp}_{\mathfrak{p}}(\pi_{\mathfrak{p}}(a/1)) = \phi^{\sharp}_{\mathfrak{p}}(a/1) = \phi(a)_{\mathfrak{p}} \in \mathcal{O}_{Y,\mathfrak{p}}.$$

There exists an open neighborhood U of $\mathfrak{p}$ in Y such that $\phi(a)_{\mathfrak{q}} = 0$ for every $\mathfrak{q} \in U$, and we assume that $U = D(b) \cap Y$ for some $b \in \mathcal{R}$. Hence $b \notin \mathfrak{p}$. By Proposition 23.4, $Y_{\phi b} = f^{-1}(D(b)) = U$. Therefore $\phi(a)_{\mathfrak{q}} = 0$ for every $\mathfrak{q} \in Y_{\phi b}$, and $\phi(a)\phi(b) = 0$ by Lemma 24.5. It follows that $ab \in \mathfrak{a}$ and $\pi(ab) = 0$. Because $b \notin \mathfrak{p}$, $\pi_{\mathfrak{p}}(a/1) = 0 \in (\mathcal{R}/\mathfrak{a})_{\mathfrak{p}+\mathfrak{a}}$. This gives injectivity. □

25. Products

Keigher [8] has shown that products exist for Δ-$\mathcal{F}$-schemes, using a categorical argument. Here we sketch a direct proof. But first we state a lemma concerning rings (not Δ-rings).

Lemma 25.1. *Let K be a field of characteristic 0, and let R and S be reduced K-algebras. Then $R \otimes_K S$ is reduced.*

Proof. Assume the contrary, and let $x \in R \otimes_K S$ be a non-zero nilpotent. Choose bases Λ for R over K and M for S over k, and write

$$x = \sum_{\lambda\in\Lambda,\mu\in\mathrm{M}} a_{\lambda\mu}\lambda \otimes \mu,$$

where $a_{\lambda\mu} \in k$. Choose λ_o and μ_o such that $a_{\lambda_o\mu_o} \neq 0$. Let $\mathfrak{p} \subset R$ and $\mathfrak{q} \subset S$ be ideals that are maximal with respect to avoiding λ_o^∞ and μ_o^∞. Then $\mathfrak{p}$ and $\mathfrak{q}$ are prime. By Zariski-Samuel [38, Theorem 35, p. 184]

$$(R \otimes_K S)/(\mathfrak{p} \otimes_K S + R \otimes_K \mathfrak{q}) \approx (R/\mathfrak{p}) \otimes_K (S/\mathfrak{q}).$$

The image of x in this quotient is non-zero and nilpotent. Replacing R and S by $\mathrm{qf}(R/\mathfrak{p})$ and $\mathrm{qf}(S/\mathfrak{q})$, we reduce to the case where R and S are fields, where the result is well-known, e.g. Zariski-Samuel [38, Theorem 39, p. 195]. □

In the following, X is an arbitrary Δ-$\mathcal{F}$-scheme, not necessarily $\operatorname{diffspec}\mathcal{R}$, although we do set $X = \operatorname{diffspec}\mathcal{R}$ in part of the proof.

Proposition 25.2. *Let X and Y be Δ-$\mathcal{F}$-schemes. Then the product $X \times_F Y$, in the category of Δ-$\mathcal{F}$-schemes, exists. If X and Y are reduced, then so is $X \times_F Y$.*

Proof. First assume that X and Y are affine, say $X = \operatorname{diffspec}\mathcal{R}$ and $Y = \operatorname{diffspec}\mathcal{S}$, where $\mathcal{R}$ and $\mathcal{S}$ are Δ-$\mathcal{F}$-algebras. Let $T = \operatorname{diffspec}(\mathcal{R} \otimes_{\mathcal{F}} \mathcal{S})$. If

$$\alpha_{\mathcal{R}} \colon \mathcal{R} \to \mathcal{R} \otimes_{\mathcal{F}} \mathcal{S} \qquad \text{and} \qquad \alpha_{\mathcal{S}} \colon \mathcal{S} \to \mathcal{R} \otimes_{\mathcal{F}} \mathcal{S}$$

are the canonical mappings, then we define

$$\pi_X = ({}^a\alpha_{\mathcal{R}}, \alpha_{\mathcal{R}}^{\#}) \colon T \to X \qquad \text{and} \qquad \pi_Y = ({}^a\alpha_{\mathcal{S}}, \alpha_{\mathcal{S}}^{\#}) \colon T \to Y.$$

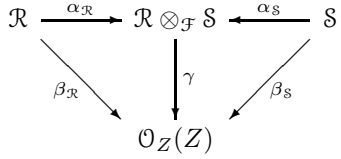
Suppose that Z is a Δ-$\mathcal{F}$-scheme and there are morphisms $f_X \colon Z \to X$ and $f_Y \colon Z \to Y$. Let

$$\beta_{\mathcal{R}} = f_X^{\#}(X) \circ \iota_{\mathcal{R}} \colon \mathcal{R} \to \mathcal{O}_Z(Z) \quad \text{and}$$
$$\beta_{\mathcal{S}} = f_Y^{\#}(Y) \circ \iota_{\mathcal{S}} \colon \mathcal{S} \to \mathcal{O}_Z(Z).$$

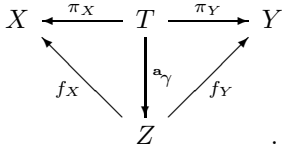
Evidently there is a unique mapping

$$\gamma \colon \mathcal{R} \otimes_{\mathcal{F}} \mathcal{S} \to \mathcal{O}_Z(Z)$$

such that



commutes. Using Propositions 23.7 and 23.9, we get



.

For the general case one patches exactly as in Hartshorne [6, p. 88]. □

26. Local ringed space of constants

Definition 26.1. Define a presheaf $\mathcal{O}_X^\Delta$ on X by the formula

$$\mathcal{O}_X^\Delta(U) = \mathcal{O}_X(U)^\Delta,$$

where $U \subset X$ is open.

Proposition 26.2. *$\mathcal{O}_X^\Delta$ is a sheaf of $\mathcal{C}$-algebras.*

Proof. Suppose that $(U_i)_{i\in I}$ is an open cover of U and $s_i \in \mathcal{O}_X^\Delta(U_i)$ agree on the intersections. Then there exists a unique $t \in \mathcal{O}_X(U)$ with $t|U_i = s_i$. For each $\delta \in \Delta$, $\delta t|U_i = \delta s_i = 0$; hence $\delta t = 0$. Therefore $t \in \mathcal{O}_X^\Delta(U)$. The mapping $\mathcal{F} \to \mathcal{O}_X(U)$ induces a mapping $\mathcal{C} \to \mathcal{O}_X^\Delta(U)$ which makes it a $\mathcal{C}$-algebra. The restrictions are clearly $\mathcal{C}$-algebra homomorphisms. □

Proposition 26.3. *Let $\mathfrak{p} \in X$. Then the stalk of $\mathcal{O}_{X,\mathfrak{p}}^\Delta$ is isomorphic to $\mathcal{R}_\mathfrak{p}^\Delta$ and is a local ring.*

Proof. By [16, Proposition 4.2], $\mathcal{O}_{X,\mathfrak{p}}$ is isomorphic to $\mathcal{R}_\mathfrak{p}$, which gives the first statement. The second is Proposition 2.9. □

Definition 26.4. We denote the local ringed space $(X, \mathcal{O}_X^\Delta)$ by X^Δ. It is called the *local ringed space of constants of X*.

Note that the topological spaces of X and X^Δ are the same; it is only the sheaves that are different.

Proposition 26.5. *F^Δ is isomorphic to C.*

Proof. Both spaces consist of a single point. Also, $\mathcal{O}_C(C) = \mathcal{C}$ and $\mathcal{O}_F^\Delta(F) = \mathcal{F}^\Delta = \mathcal{C}$. □

Proposition 26.6. *If $\mathcal{R}$ is reduced, then $\widehat{\mathcal{R}}^\Delta = \mathcal{R}^\Delta = \widehat{\mathcal{R}^\Delta}$.*

Proof. Of course $\mathcal{R}^\Delta \subset \widehat{\mathcal{R}}^\Delta$. For $s \in \widehat{\mathcal{R}}^\Delta$, $\mathfrak{a} = \{\, b \in \mathcal{R} \mid bs \in R \,\}$ is a Δ-ideal of $\mathcal{R}$ because s is a constant. By Proposition 21.3, $\mathfrak{a}$ is not contained in any prime Δ-ideal of $\mathcal{R}$; so, by Proposition 2.5, $1 \in \mathfrak{a}$ and $s \in \mathcal{R}^\Delta$. This gives $\widehat{\mathcal{R}}^\Delta = \mathcal{R}^\Delta$. The second equality is a well-known result concerning schemes:

$$\widehat{\mathcal{R}^\Delta} = \Gamma(\operatorname{spec}\mathcal{R}^\Delta, \mathcal{O}_{\operatorname{spec}\mathcal{R}^\Delta}) = \mathcal{R}^\Delta.$$

□

Definition 26.7. Suppose that $(f, f^\#)\colon X \to Y$ is a morphism of Δ-$\mathcal{F}$-schemes. Then $(f^\Delta, f^{\#\Delta})\colon X^\Delta \to Y^\Delta$ is defined as follows:

(1) $f^\Delta = f$.
(2) $f^{\#\Delta}(U)$ is the restriction of $f^\#(U)$ to $\mathcal{O}_Y^\Delta(U)$.

Proposition 26.8. *Suppose that $(f, f^\#)\colon X \to Y$ is a morphism of Δ-$\mathcal{F}$-schemes. Then $(f^\Delta, f^{\#\Delta})\colon X^\Delta \to Y^\Delta$ is a morphism of local ringed spaces over C.*

Proof. We need to show that $f_x^{\#\Delta}\colon \mathcal{O}_{Y,f(x)}^\Delta \to \mathcal{O}_{X,x}^\Delta$ is a local homomorphism. But that follows from Propositions 26.3 and 2.9. □

27. Almost constant differential schemes

In general X^Δ is simply a local ringed space, but in certain fortuitous cases it is a scheme or even an affine scheme. We examine that circumstance in this section. For the following, recall Definition 5.1.

Proposition 27.1. *Suppose that $\mathcal{R}$ is reduced. Then $\mathcal{R}$ is almost constant if and only if X^Δ is an affine scheme. In that case $X^\Delta \approx \operatorname{spec} \mathcal{R}^\Delta$.*

Proof. Suppose that $\mathcal{R}$ is almost constant, and let $j\colon \mathcal{R}^\Delta \to \mathcal{R}$ be the inclusion. By Proposition 22.1, ${}^a j\colon X^\Delta \to \operatorname{spec} \mathcal{R}^\Delta$ is a homeomorphism, and by Proposition 5.2, $j^{\#\Delta}$ is an isomorphism.

Now suppose that $(f, f^\#)\colon X^\Delta \to Y = \operatorname{spec} \mathcal{D}$ is an isomorphism. Using Proposition 26.6, we see that

$$f^\#(Y) : \mathcal{D} \to \widehat{\mathcal{R}}^\Delta = \mathcal{R}^\Delta$$

is an isomorphism. That gives the last statement of the proposition. For every $\mathfrak{p} \in X^\Delta$ we have the following commutative diagram by Proposition 26.3:

$$\begin{array}{ccccc} \mathcal{D} & \xrightarrow{f^\#(Y)} & \mathcal{R}^\Delta & \xrightarrow{\subset\ j} & \mathcal{R} \\ \downarrow & & \downarrow & & \downarrow \\ \mathcal{D}_{f(\mathfrak{p})} & \xrightarrow{f^\#_{\mathfrak{p}}} & \mathcal{R}^\Delta_{\mathfrak{p}} & \xrightarrow{\subset} & \mathcal{R}_{\mathfrak{p}} \end{array}$$

It follows that

$$f(\mathfrak{p}) = f^\#(Y)^{-1}\big(j^{-1}(\mathfrak{p})\big) = \big({}^a f^\#(Y) \circ {}^a j\big)(\mathfrak{p}).$$

Because $f^\#(Y)$ is an isomorphism, ${}^a f^\#(Y)$ is a homeomorphism and therefore so is ${}^a j$. By Proposition 22.1 $\mathtt{R}(j)$ is bijective, i.e. $\mathcal{R}$ is almost constant. □

Definition 27.2. If the local ringed space X^Δ is a scheme, we call it the *scheme of constants of X*. We also say that X is *almost constant*.

If X is reduced and almost constant, then every point has an open neighborhood of the form $\operatorname{diffspec} \mathcal{S}$, where $\mathcal{S}$ is reduced and almost constant.

Proposition 27.3. *Every open subset of a reduced almost constant Δ-$\mathcal{F}$-scheme is almost constant.*

Proof. We may assume that $X = \operatorname{diffspec} \mathcal{R}$, where $\mathcal{R}$ is almost constant. Suppose that $U \subset X$ is open and let $\mathfrak{p} \in U$. If $X \setminus U = V(\mathfrak{a})$, with $\mathfrak{a} \in \mathtt{R}(\mathcal{R})$, then $\mathfrak{a}^\Delta$ is not contained in $\mathfrak{p}^\Delta$. So we may choose $c \in \mathfrak{a}^\Delta$, $c \notin \mathfrak{p}^\Delta \subset \mathfrak{p}$. Evidently $\mathfrak{p} \in D(c) \subset U$, and by Proposition 5.3, $\mathcal{R}_c$ is almost constant. □

However, we do not claim that every open *affine* subset is an almost constant *affine* Δ-$\mathcal{F}$-scheme. Indeed, it might happen that X^Δ is a scheme but not affine. In that case there would exist $b_1, \dots, b_n \in \mathcal{R}$ such that $1 \in \{b_1, \dots, b_n\}$ and each $\mathcal{R}_{b_i}$ is almost constant; however, $\mathcal{R}$ itself would not be almost constant. We give an example of this in Section 29.

28. Split differential schemes

In this section we also consider schemes over $C = \operatorname{spec} \mathcal{C}$ as well as $F = \operatorname{diffspec} \mathcal{F}$. Since a $\mathcal{C}$-algebra has a trivial structure of Δ-ring ($\delta c = 0$ for every $\delta \in \Delta$), a scheme Y over C has a trivial structure of Δ-$\mathcal{C}$-scheme. Note that F is itself a Δ-C-scheme, and therefore we can form the product $F \times_C Y$ in the category of Δ-$\mathcal{C}$-schemes. It has a natural structure of Δ-$\mathcal{F}$-scheme. This construction is often called "base change". If Y is reduced, then $F \times_C Y$ is reduced by Proposition 25.2.

Definition 28.1. X is said to be *split* if there is a scheme Y over C such that X is isomorphic (as Δ-$\mathcal{F}$-schemes) to $F \times_C Y$.

Buium [3, p. 6] has a related notion. However, he takes the product $F \times_C Y$ in the category of schemes (not Δ-schemes) and gets what one might call a "scheme with differentiation" (Umemura [33, Definition 1.6, p. 8]). This is a scheme (not a Δ-scheme) whose sheaf is a sheaf of Δ-rings. Indeed, if $Y = \operatorname{spec} \mathcal{D}$, then Buium's product is $\operatorname{spec}(\mathcal{F} \otimes_{\mathcal{C}} \mathcal{D})$ whereas ours is $\operatorname{diffspec}(\mathcal{F} \otimes_{\mathcal{C}} \mathcal{D})$.

Proposition 28.2. *If X is reduced and split, then X is almost constant and is isomorphic to $F \times_C X^\Delta$.*

Proof. Write $X = F \times_C Y$, where Y is a scheme over C, which we may assume to be affine, say $Y = \operatorname{spec} \mathcal{D}$. Let $\mathcal{S} = \mathcal{F} \otimes_{\mathcal{C}} \mathcal{D}$. Since $\mathcal{S}^\Delta = 1 \otimes_{\mathcal{C}} \mathcal{D}$, Proposition 5.6 implies that $\mathcal{S}$ is almost constant, and Proposition 27.1 implies that $\mathcal{D} = \mathcal{S}^\Delta$. □

Proposition 28.3. *Suppose that $\mathcal{R}$ is reduced and almost constant. Then X is split if and only if*

$$\mathcal{R}_{\mathfrak{p}} = \mathcal{F}[\mathcal{R}^\Delta]_{\mathfrak{p}}$$

for every $\mathfrak{p} \in X$.

Proof. The assumption that $\mathcal{R}$ is almost constant implies that X^Δ is an affine scheme. Let

$$\phi \colon \mathcal{F} \otimes_{\mathcal{C}} \mathcal{R}^\Delta \to \mathcal{R}, \quad \phi(f \otimes c) = fc.$$

If X is split, then $({}^a\phi, \phi^\#) \colon X \to F \times_C X^\Delta$ is an isomorphism. Thus, for $\mathfrak{p} \in X$ and $\mathfrak{q} = {}^a\phi(\mathfrak{p})$,

$$\phi^\#_{\mathfrak{p}} \colon (\mathcal{F} \otimes_{\mathcal{C}} \mathcal{R}^\Delta)_{\mathfrak{q}} \to \mathcal{R}_{\mathfrak{p}}, \quad a/b \mapsto \phi(a)/\phi(b),$$

is a Δ-$\mathcal{F}$-isomorphism. The surjectivity shows that $\mathcal{R}_{\mathfrak{p}} = \mathcal{F}[\mathcal{R}^\Delta]_{\mathfrak{p}}$.

For the converse, first observe that ${}^r\phi$ is bijective by Proposition 5.6. Proposition 3.5 then tells us that $\phi^\#_{\mathfrak{p}}$ is injective. The hypothesis gives surjectivity. □

However, we do not claim that $\mathcal{R}$ is isomorphic to $\mathcal{F} \otimes_{\mathcal{C}} \mathcal{R}^\Delta = \mathcal{F}[\mathcal{R}^\Delta]$. The mapping ϕ of the proposition is certainly injective by Proposition 2.1 (or use Proposition 5.6 to see that the kernel is (0)). But surjectivity is not obvious. Indeed, an isomorphism of affine Δ-schemes does not imply that the rings are isomorphic, for example, $\operatorname{diffspec} \mathbb{C}[x] \approx \operatorname{diffspec} \mathbb{C}(x)$ (where $\delta x = 1$).

For (not differential) modules, if $\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is surjective for every prime ideal, then $\phi : M \to N$ is also surjective by Atiyah-MacDonald [1, Proposition 3.9]. However, the proof fails for Δ-modules, because annihilators are not necessarily Δ-ideals.

Proposition 28.4. *Suppose that X and Y are split. Then $X \times_F Y$ is split and is isomorphic to $F \times_C (X^\Delta \times_C Y^\Delta)$.*

Proof. $X = F \times_C X^\Delta$ and $Y = F \times_C Y^\Delta$. □

Proposition 28.5. *Suppose that X is split. If Y is a reduced closed Δ-subscheme of X, then Y is split and Y^Δ is a reduced closed subscheme of X^Δ. Conversely, if Z is a reduced closed subscheme of X^Δ, then $F \times_C Z$ is a reduced closed Δ-$\mathcal{F}$-subscheme of X.*

Proof. First assume that X^Δ is an affine scheme. Because X is split, we may assume that $\mathcal{R} = \mathcal{F} \otimes_\mathcal{C} \mathcal{R}^\Delta$ and that $\mathcal{R}$ is almost constant. If Y is a reduced closed subscheme, then by Proposition 24.6 there is a radical Δ-ideal $\mathfrak{a} \subset \mathcal{R}$ with $Y = \operatorname{diffspec}(\mathcal{R}/\mathfrak{a})$. By Proposition 5.6, $\mathfrak{a} = \mathcal{F} \otimes_\mathcal{C} a^\Delta$. But $\mathcal{F} \otimes_\mathcal{C} (\mathcal{R}^\Delta/\mathfrak{a}^\Delta)$ is isomorphic to $\mathcal{R}/\mathfrak{a} = (\mathcal{F} \otimes_\mathcal{C} \mathcal{R}^\Delta)/\mathfrak{a}$ by Zariski-Samuel [38, Theorem 35, p. 184]. Hence $Y = \operatorname{diffspec}(\mathcal{F} \otimes_\mathcal{C} (\mathcal{R}^\Delta/\mathfrak{a}^\Delta))$.

Conversely, if $Z \subset X^\Delta$ is a closed subscheme, then there is a radical Δ-ideal $\mathfrak{b} \subset \mathcal{R}^\Delta$ with $Z = \operatorname{spec}(\mathcal{R}^\Delta/\mathfrak{b})$. Evidently $F \times_\mathcal{C} Z = \operatorname{diffspec}(\mathcal{R}/(\mathcal{F} \otimes_\mathcal{C} \mathfrak{b}))$. The general case follows from this one by the usual patching procedure. □

29. Examples

In this section $\otimes$ means $\otimes_\mathcal{F}$. In both of the examples, we consider $\mathcal{P} = \mathcal{G} \otimes \mathcal{G}$, where $\mathcal{G}$ is a Δ-extension of $\mathcal{F}$. In fact $\mathcal{G}$ is a strongly normal extension of $\mathcal{F}$, but that fact is not important to the examples. In the first example $\mathcal{P}$ is almost constant, and therefore P^Δ is an affine scheme. In the second example, P^Δ is also a scheme, but *not* affine.

Example 29.1. Let $\mathcal{F} = \mathcal{C}$ and $\mathcal{G} = \mathcal{C}(x)$, where $\delta x = x' = 1$.

Observe that $\mathcal{R} = \mathcal{C}[x]$ is Δ-simple and $1 \otimes \mathcal{R}^*$ is a multiplicative subset of $\mathcal{G} \otimes \mathcal{R}$ consisting of Δ-units. By Proposition 22.2

$$P = \operatorname{diffspec} \mathcal{P} \approx \operatorname{diffspec}(\mathcal{G} \otimes \mathcal{R}).$$

Let $\gamma = x \otimes 1 - 1 \otimes x$; then $\gamma' = 0$ and $\mathcal{G} \otimes \mathcal{R} = (\mathcal{G} \otimes 1)[\gamma]$. Therefore

$$P \approx \operatorname{diffspec}((\mathcal{G} \otimes 1)[\gamma]) \approx \operatorname{diffspec}(\mathcal{G} \otimes_\mathcal{C} \mathcal{C}[\gamma]) \approx G \times_C \operatorname{spec} \mathcal{C}[\gamma],$$

where $G = \operatorname{diffspec} \mathcal{G}$ and $C = \operatorname{spec} \mathcal{C}$. This says that P is split over G and $P^\Delta = \operatorname{spec} \mathcal{C}[\gamma]$ (which is the affine line).

Example 29.2. Let $\mathcal{F} = \mathcal{C} = \mathbb{C}$, $\eta = \wp(\frac{1}{2}x)$, and $\mathcal{G} = \mathcal{C}\langle\eta\rangle$.

Here $\wp(x)$ is the Weierstrass $\wp$-function, see for example Silverman [30, Section 3, p. 153]. We have $\wp(x)'^2 = 4\wp(x)^3 - g_2\wp(x) - g_3$, so

$$\eta'^2 = \eta^3 - \tfrac{1}{4}g_2\eta - \tfrac{1}{4}g_3 = \eta^3 + a_4\eta + a_6,$$

where we have used the notation of [30, Section 1, p. 46]. The discriminant of the cubic is non-zero.

Proposition 29.3. *$\mathcal{R} = \mathcal{C}[\eta, \eta']$ is Δ-simple.*

Proof. Let $f(\eta) = \eta^3 + a_4\eta + a_6$. Suppose that $\mathfrak{p} \subset \mathcal{R}$ is a non-zero prime Δ-ideal. First observe that $\mathfrak{p}$ does not contain η'. If it did, then it would contain both $\eta'^2 = f(\eta)$ and $\eta'' = \frac{1}{2}f'(\eta)$, which contradicts the fact that the discriminant of f is non-zero.

Next observe that $\mathfrak{p}$ does not contain any non-zero polynomial in η alone. If it did, and $A(\eta) \in \mathfrak{p}$ were of lowest degree, then $A'(\eta)\eta'$ would also be in $\mathfrak{p}$. But $A'(\eta)$ has lower degree.

Finally suppose that A, B are relatively prime polynomials with $B \neq 0$ and $A(\eta) + B(\eta)\eta' \in \mathfrak{p}$. Then

$$\big(A(\eta) + B(\eta)\eta'\big)\big(A(\eta) - B(\eta)\eta'\big) = A^2(\eta) - B^2(\eta)f(\eta) \in \mathfrak{p}.$$

This must be 0, so f divides A and therefore B, which is a contradiction. □

The following proposition shows that $\mathcal{P}$ is *not* almost constant.

Proposition 29.4. $\mathcal{P}^\Delta = \mathcal{C}$.

Proof. Suppose that $c \in \mathcal{P}^\Delta$. Let $\mathfrak{b} = \{r \in \mathcal{R} \mid r\,c \in \mathcal{G} \otimes \mathcal{R}\}$. Then $\mathfrak{b}$ is a non-zero ideal of $\mathcal{R}$ and a Δ-ideal, because c is a constant. Because $\mathcal{R}$ is Δ-simple, $1 \in \mathfrak{b}$, i.e. $c \in \mathcal{G} \otimes \mathcal{R}$. Therefore

$$c = \sum_{i=0}^{r} a_i \otimes \eta^i + \sum_{j=0}^{s} b_j \otimes \eta^j \eta'$$

for some $a_i, b_j \in \mathcal{G}$. We may assume that $a_r = 0$ only if $r = 0$. Assume for the moment that $b_s \neq 0$. Differentiating this equation, we obtain

$$\begin{aligned} 0 = &\sum_{i=0}^{r} a_i' \otimes \eta^i + \sum_{i=0}^{r} i a_i \otimes \eta^{i-1}\eta' \\ &+ \sum_{j=0}^{s} b_j' \otimes \eta^j \eta' + \sum_{j=0}^{s} j b_j \otimes \eta^{j-1}\left(\eta^3 + a_4\eta + a_6\right) \\ &+ \sum_{j=0}^{s} b_j \otimes \eta^j \left(\tfrac{3}{2}\eta^2 + \tfrac{1}{2}a_4\right). \end{aligned}$$

If $s + 2 > r$, then the coefficient of $1 \otimes \eta^{s+2}$ is $(s + \frac{3}{2})\, b_s \otimes 1$. This must be zero, so $b_s = 0$, which contradicts our assumption. If $s + 2 \leq r$, then the coefficient of $1 \otimes \eta^{r-1}\eta'$ is $r\, a_r \otimes 1$, which gives $r = 0$. But then $s \leq -2$, which is absurd.

We conclude that $b_s = 0$, i.e. c is free of $1 \otimes \eta'$. Therefore

$$0 = \sum_{i=1}^{r} a_i' \otimes \eta^i + \sum_{i=0}^{r} i a_i \otimes \eta^{i-1}\eta'.$$

The coefficient of $\eta^{r-1}\eta'$ is rA_r, so we must have $r = 0$ and $c \in (\mathcal{G} \otimes 1)^\Delta = \mathcal{C}$. □

Let $E \subset \mathbb{P}^2$ be the non-singular elliptic curve with Weierstrass equation

$$Y^2 Z = X^3 + a_4 X Z^2 + a_6 Z^3.$$

Then $[1 \otimes \eta, 1 \otimes \eta', 1]$ and $[\eta \otimes 1, \eta' \otimes 1, 1]$ are two points on E, and we can form their difference, using the formulas of [30, Group Law Algorithm 2.3, p. 58]. Define

$$\begin{aligned} \gamma &= \Big(\frac{\eta' \otimes 1 + 1 \otimes \eta'}{\eta \otimes 1 - 1 \otimes \eta}\Big)^2 - \eta \otimes 1 - 1 \otimes \eta, \\ \mu &= -\Big(\frac{\eta' \otimes 1 + 1 \otimes \eta'}{\eta \otimes 1 - 1 \otimes \eta}\Big)\gamma + \frac{\eta \otimes \eta' + \eta' \otimes \eta}{\eta \otimes 1 - 1 \otimes \eta}. \end{aligned} \tag{29.1}$$

Proposition 29.5. *γ and μ are constants.*

Proof. If we first compute

$$\Big(\frac{\eta'\otimes 1+1\otimes\eta'}{\eta\otimes 1-1\otimes\eta}\Big)' = \tfrac{1}{2}\big(\eta\otimes 1-1\otimes\eta\big),$$

it easily follows that $\gamma'=0$. Because $\mu^2=\gamma^3+a_4\gamma+a_6$, we have $\mu'=0$. □

Proposition 29.6. *$\mathfrak{p}_{\mathrm{id}}$ is the unique prime Δ-ideal of $\mathcal{P}$ containing $\eta\otimes 1-1\otimes\eta$.*

Proof. If $\mathfrak{p}$ is a prime Δ-ideal containing $\eta\otimes 1-1\otimes\eta$, then, by Proposition 6.4, $\mathfrak{p}=\mathfrak{p}_\sigma$ for some Δ-isomorphism σ of $\mathcal{G}$ over $\mathcal{F}$. Since $\sigma\eta=\eta$, $\sigma=\mathrm{id}$. □

Thus $P=\operatorname{diffspec}\mathcal{P}$ is the disjoint union of the open set $D(\eta\otimes 1-1\otimes\eta)$ and the single point $\mathfrak{p}_{\mathrm{id}}$. We claim that $D(\eta\otimes 1-1\otimes\eta)\approx\operatorname{diffspec}(\mathcal{P}_{\eta\otimes 1-1\otimes\eta})$ is almost constant, and in fact $D(\eta\otimes 1-1\otimes\eta)^\Delta\approx\operatorname{spec}\mathcal{C}[\gamma,\mu]$.

Lemma 29.7. $\operatorname{diffspec}(\mathcal{P}_{\eta\otimes 1-1\otimes\eta})\approx\operatorname{diffspec}(\mathcal{G}\otimes\mathcal{R})[\gamma,\mu]$.

Proof. $\mathcal{P}$ is the ring of fractions of $\mathcal{G}\otimes\mathcal{R}$ by the multiplicative set $1\otimes\mathcal{R}^*$, which consists of Δ-units by Propositions 29.3 and 13.4. By Proposition 22.2,

$$\operatorname{diffspec}(\mathcal{P}_{\eta\otimes 1-1\otimes\eta})\approx\operatorname{diffspec}(\mathcal{G}\otimes\mathcal{R})_{\eta\otimes 1-1\otimes\eta}.$$

But by equation (29.1)

$$(\mathcal{G}\otimes\mathcal{R})_{\eta\otimes 1-1\otimes\eta}=(\mathcal{G}\otimes\mathcal{R})[\gamma,\mu]_{\eta\otimes 1-1\otimes\eta}.$$

We claim that $\eta\otimes 1-1\otimes\eta$ is a Δ-unit in $(\mathcal{G}\otimes\mathcal{R})[\gamma,\mu]$. Suppose not, and let $\mathfrak{p}$ be a prime Δ-ideal of $(\mathcal{G}\otimes\mathcal{R})[\gamma,\mu]$ that contains $\eta\otimes 1-1\otimes\eta$. By equation (29.1)

$$(\eta'\otimes 1+1\otimes\eta')^2=(\gamma+\eta\otimes 1+1\otimes\eta)\,(\eta\otimes 1-1\otimes\eta)^2\in\mathfrak{p},$$

and therefore $\eta'\otimes 1+1\otimes\eta'\in\mathfrak{p}$. But it also contains $\eta'\otimes 1-1\otimes\eta'$ and therefore $\eta'\otimes 1$, which is a unit in $(\mathcal{G}\otimes\mathcal{R})[\gamma,\mu]$. We can now use Proposition 22.2. □

Lemma 29.8. $\operatorname{diffspec}(\mathcal{G}\otimes\mathcal{R})[\gamma,\mu]\approx\operatorname{diffspec}(\mathcal{G}\otimes 1)[\gamma,\mu]$.

Proof. Because $[1\otimes\eta,1\otimes\eta',1]=[\eta\otimes 1,\eta'\otimes 1,1]+[\gamma,\mu,1]$, we have

$$1\otimes\eta=\Big(\frac{\mu-\eta'\otimes 1}{\gamma-\eta\otimes 1}\Big)-\eta\otimes 1-\gamma.$$

The denominator, $\gamma-\eta\otimes 1$, is a Δ-unit in $(\mathcal{G}\otimes 1)[\gamma,\mu]$ because its derivative is $\eta'\otimes 1$. Therefore

$$\operatorname{diffspec}(\mathcal{G}\otimes\mathcal{R})[\gamma,\mu]\approx\operatorname{diffspec}(\mathcal{G}\otimes\mathcal{R})[\gamma,\mu]_{\gamma-\eta\otimes 1}.$$

From the above equation, we get

$$(\mathcal{G}\otimes\mathcal{R})[\gamma,\mu]_{\gamma-\eta\otimes 1}=(\mathcal{G}\otimes 1)[\gamma,\mu]_{\gamma-\eta\otimes 1}.$$

Again using the fact that $\gamma-\eta\otimes 1$ is a Δ-unit, we get

$$\operatorname{diffspec}(\mathcal{G}\otimes 1)[\gamma,\mu]_{\gamma-\eta\otimes 1}\approx\operatorname{diffspec}(\mathcal{G}\otimes 1)[\gamma,\mu].$$

□

Proposition 29.9. *$\mathcal{P}_{\eta\otimes 1-1\otimes\eta}$ is almost constant. The open subset $D(\eta\otimes 1-1\otimes\eta)$ of $P=\operatorname{diffspec}\mathcal{R}$ is split over $\mathcal{G}$, and $D(\eta\otimes 1-1\otimes\eta)^\Delta=\mathcal{C}[\gamma,\mu]$.*

Therefore P^Δ has a dense open subset whose complement is the single point $\mathfrak{p}_{\mathrm{id}}$, and is isomorphic to the finite part of the elliptic curve E. We can find a second open subset which contains $\mathfrak{p}_{\mathrm{id}}$, i.e. the "point at infinity" $[0,1,0]\in E$, and thereby show that P^Δ is indeed a scheme, but not an affine scheme. We omit the details.

Part IV. Differential Galois group

Throughout this part we assume that $\mathcal{C} = \mathcal{F}^\Delta$ is *algebraically closed* and that $\mathcal{G}$ is a strongly normal extension of $\mathcal{F}$.

30. Homogeneity

Grothendieck-Dieudonne [5, Definition 2.8.1, p. 67] defines a *Jacobson space* to be a topological space whose set of closed points is *very dense*, i.e. every non-empty locally closed set contains a closed point.

Proposition 30.1. *$P = \operatorname{diffspec} \mathcal{P}$ is a Jacobson space.*

Proof. This follows from the fact that $\mathcal{P}$ is a Jacobson ring (Proposition 15.2). But it is easier to note that if $\mathfrak{a} \subset \mathcal{P}$ is a radical Δ-ideal and $a \in \mathcal{P}$, $a \notin \mathfrak{a}$, then, by Corollary 14.3, $D(a) \cap V(\mathfrak{a})$ contains a maximal Δ-ideal. □

Corollary 30.2. *$\operatorname{Gal}(\mathcal{G}/\mathcal{F})$ is very dense in P.*

Proof. Corollaries 14.3 and 14.4 allow us to identify $\operatorname{Gal}(\mathcal{G}/\mathcal{F})$ with the set of closed points of P. □

Proposition 30.3. *Let $\mathfrak{p}$ and $\mathfrak{q}$ be two maximal Δ-ideals of $\mathcal{P}$. Then there is a Δ-automorphism $\phi\colon \mathcal{P} \to \mathcal{P}$ such that $\phi(\mathfrak{p}) = \mathfrak{q}$.*

Proof. By Corollary 14.3, $\mathfrak{p} = \mathfrak{p}_\sigma$ and $\mathfrak{q} = \mathfrak{p}_\tau$, where $\sigma, \tau \in \operatorname{Gal}(\mathcal{G}/\mathcal{F})$. By Proposition 8.1, $\mathfrak{p}_\sigma$ is generated by $\sigma g \otimes 1 - 1 \otimes g$ and $\mathfrak{p}_\tau$ by $\tau g \otimes 1 - 1 \otimes g$ ($g \in \mathcal{G}$). Hence

$$\phi\colon \mathcal{P} \to \mathcal{P}, \quad \phi(a \otimes b) = \tau\sigma^{-1} a \otimes b,$$

carries $\mathfrak{p}$ into $\mathfrak{q}$. □

Proposition 30.4. *Suppose that U is a non-empty open subset of P. Then, for any $\mathfrak{p} \in P$ there is an isomorphism $f\colon P \to P$ such that $\mathfrak{p} \in f(U)$.*

Proof. Let $\mathfrak{q} \in U$ be a closed point and $\mathfrak{r}$ a closed point in the closure of $\{\mathfrak{p}\}$. By the previous proposition there is an automorphism ϕ of $\mathcal{P}$ that takes $\mathfrak{r}$ into $\mathfrak{q}$. Then $({}^a\phi, \phi^\#)\colon P \to P$ takes U onto an open subset containing $\mathfrak{r}$ and therefore containing $\mathfrak{p}$. □

In Section 33 we shall show that P is split by finding a non-empty split open subset $U \subset P$, then covering all of P with copies of U.

31. Component of the identity

Proposition 31.1. *The components of P are the sets $V(\mathfrak{p})$, where $\mathfrak{p}$ is a minimal prime Δ-ideal of $\mathcal{R}$.*

Proof. The proof is similar to Bourbaki [2, Corollary 2, p. 102]. □

Proposition 31.2. *P has a finite number of components, and they are disjoint.*

Proof. Proposition 9.5. □

Recall from Definition 10.3 that $\mathfrak{p}^\circ$ is the unique minimal prime Δ-ideal of $\mathcal{P}$ that is contained in $\mathfrak{p}_{\mathrm{id}}$. This is the "generic point" of the component containing the identity.

Proposition 31.3. *$V(\mathfrak{p}^\circ)$ is open and closed. It is isomorphic to* $\operatorname{diffspec}(\mathcal{G}\otimes_{\mathcal{F}^\circ}\mathcal{G})$, *where $\mathcal{F}^\circ$ is the algebraic closure of $\mathcal{F}$ in $\mathcal{G}$.*

Proof. By Proposition 10.4, $\mathcal{P}/\mathfrak{p}^\circ \approx \mathcal{G}\otimes_{\mathcal{F}^\circ}\mathcal{G}$. Kovacic [16, Proposition 3.10] gives $V(\mathfrak{p}^\circ) = \operatorname{diffspec}(\mathcal{P}/\mathfrak{p}^\circ)$. □

As we remarked above, we wish to find a non-empty open subset U of P that is split. Because of the previous proposition we may look for that set inside of $V(\mathfrak{p}^\circ)$. This is equivalent to assuming that $\mathcal{F} = \mathcal{F}^\circ$.

32. A preliminary result

In this section we assume that $\mathcal{F}$ is algebraically closed in $\mathcal{G}$, i.e. $\mathcal{F}^\circ = \mathcal{F}$. Then $\mathcal{P}$ is an integral domain by Zariski-Samuel [38, Corollary 2, p. 198], and we can identify $\mathcal{P}$ with a subring of its quotient field $\operatorname{qf}(\mathcal{P})$. We write $\otimes$ for $\otimes_{\mathcal{F}} = \otimes_{\mathcal{F}^\circ}$.

Because $\mathfrak{p}^\circ = (0)$ is strong (Definition 11.4), we have

$$\operatorname{qf}(\mathcal{P}) = \kappa(\mathfrak{p}^\circ) = (\mathcal{G}\otimes 1)(1\otimes\mathcal{G}) = (\mathcal{G}\otimes 1)\mathcal{C}(\mathfrak{p}^\circ) = (1\otimes\mathcal{G})\mathcal{C}(\mathfrak{p}^\circ),$$

where $\mathcal{C}(\mathfrak{p}^\circ) = \kappa(\mathfrak{p}^\circ)^\Delta$.

By Proposition 13.8 we may choose a finite family $\eta = (\eta_1,\dots,\eta_m)$ such that $\mathcal{G} = \mathcal{F}(\eta)$ and $\mathcal{R} = \mathcal{F}[\eta]$ is Δ-simple. Observe that $\mathcal{R}^*$ is a multiplicative subset of $\mathcal{R}$ which, by Proposition 13.4, consists of Δ-units. The ring of fractions is $\mathcal{G}$.

Also, by Proposition 12.4 we may choose $\gamma = (\gamma_1,\dots,\gamma_r)$ with $\mathcal{C}(\mathfrak{p}^\circ) = \mathcal{C}(\gamma)$. Then

$$1\otimes\eta_i = \frac{A_i}{B}, \qquad \text{for some } A_i, B \in (\mathcal{R}\otimes 1)[\gamma].$$

Lemma 32.1. *There exists $b\in\mathcal{C}[\gamma]$, $b\neq 0$, such that if $\mathcal{D} = \mathcal{C}[\gamma,\frac{1}{b}]$, then*

1. *$(\mathcal{G}\otimes 1)[\mathcal{D}]_B$ is almost constant,*
2. *B is a Δ-unit of $(\mathcal{G}\otimes 1)[\mathcal{D}]$, and*
3. *$(\mathcal{G}\otimes 1)[\mathcal{D}]^\Delta = \mathcal{D}$.*

Proof. Because of Proposition 5.6, $(\mathcal{G}\otimes 1)[\gamma]$ is almost constant, and therefore we can use Proposition 5.5. □

Note that $\mathcal{D} = \mathcal{C}[\gamma,\frac{1}{b}]$ is a finitely generated algebra over $\mathcal{C}$.

Lemma 32.2. *$\mathcal{P}[\mathcal{D}]$ is almost constant. In addition, $\mathcal{P}[\mathcal{D}]^\Delta = \mathcal{D}$.*

Proof. By the previous lemma $(\mathcal{G}\otimes 1)[\mathcal{D}]_B$ has ring of constants $\mathcal{D}$ and is almost constant. But

$$(\mathcal{G}\otimes\mathcal{R})[\mathcal{D}]_B = (\mathcal{G}\otimes 1)[\mathcal{D}]_B,$$

and therefore, by Proposition 5.4, $(\mathcal{G}\otimes\mathcal{R})[\mathcal{D}]$ has constants $\mathcal{D}$ and is almost constant. Using that same proposition, and the fact that $1\otimes\mathcal{R}^*$ consists of Δ-units, we get the lemma. □

We also have

$$\gamma_j = \frac{C_j}{D} \qquad \text{and} \qquad \frac{1}{b} = \frac{E}{D} \qquad \text{for some } C_j, D, E \in \mathcal{R}\otimes\mathcal{R}.$$

Proposition 32.3. *There exists $d\in\mathcal{D}$ such that $(\mathcal{P}_D)_d$ is almost constant. In addition, $(\mathcal{P}_D)_d^\Delta = \mathcal{D}_d$.*

Proof. By Proposition 5.5 there exists $d \in \mathcal{D}$ such that $\mathcal{P}[\mathcal{D}_d]_D$ is almost constant and $\mathcal{P}[\mathcal{D}_d]_D)^\Delta = \mathcal{D}_d$. However,

$$\mathcal{D} = \mathcal{P}^\Delta[\gamma, \tfrac{1}{b}] \subset \mathcal{P}_D,$$

so $\mathcal{P}[\mathcal{D}_d]_D = (\mathcal{P}_D)_d$. □

33. P splits

In this section we no longer assume that $\mathcal{F}$ is algebraically closed in $\mathcal{G}$, as we did in the previous section. We first show that P is almost constant. Note that we do not claim that $\mathcal{P}$ is almost constant—in other words, we shall show that P^Δ is a scheme, but it is not necessarily affine. We use the notation of the previous section.

Proposition 33.1. *P^Δ is a scheme of finite type over $C = \operatorname{spec} \mathcal{C}$. In particular, P is almost constant.*

Proof. Let $\mathcal{P}^\circ = \mathcal{G} \otimes^\circ_{\mathcal{F}} \mathcal{G}$ and $\mathcal{S} = (\mathcal{P}^\circ_D)_d$. By Proposition 32.3, $\mathcal{S}$ is almost constant. Let $U = \operatorname{diffspec} \mathcal{S}$. Then, by Kovacic [16, Proposition 5.5], U is open in $\operatorname{diffspec} \mathcal{P}^\circ = V(\mathfrak{p}^\circ)$, which is itself open in P by Proposition 31.3. By Proposition 30.4 we can cover P^Δ with copies of U. Therefore P^Δ is a scheme.

Proposition 32.3 also shows that $\mathcal{S}^\Delta$ is an algebra of finite type over $\mathcal{C}$; hence $U^\Delta = \operatorname{spec} \mathcal{S}^\Delta$ is of finite type. Because P is quasi-compact (Kovacic [16, Proposition 3.6]), P^Δ is of finite type over C. □

Theorem 33.2. *P is split.*

Proof. To use Proposition 28.3, we need to show that

$$\mathcal{S}_\mathfrak{p} = (\mathcal{G} \otimes^\circ_{\mathcal{F}} 1)[\mathcal{S}^\Delta]_\mathfrak{p}$$

for every $\mathfrak{p} \in U$. Let $a/b \in \mathcal{S}_\mathfrak{p}$. Because of the last formula of the preceding section we may assume that $a, b \in \mathcal{G} \otimes^\circ_{\mathcal{F}} \mathcal{F}[\eta]$. Then there exists $e \in \mathbb{N}$ with

$$\frac{a}{b} = \frac{B^e a}{B^e b} \in (\mathcal{G} \otimes 1)[\mathcal{S}^\Delta]_\mathfrak{p}.$$

□

34. P^Δ is a group scheme

For the basic theory of group schemes, see Mumford [22, Section 11]. In Section 16 we saw that $\mathcal{P}$ has a natural structure of a coring, where we thought of $\mathcal{P}$ as both a left and right algebra over $\mathcal{G}$. Here, however, we think of $\mathcal{P}$ only as a left algebra. To clarify the formulas we explicitly define the two operations:

$$\phi\colon \mathcal{G} \to \mathcal{P}, \qquad a \mapsto a \otimes_{\mathcal{F}} 1, \text{ and}$$
$$\psi\colon \mathcal{G} \to \mathcal{P}, \qquad b \mapsto 1 \otimes_{\mathcal{F}} b\,.$$

Thus ϕ defines the algebra structure on $\mathcal{P}$ and the structure mappings $({}^a\phi, \phi^\#)\colon P \to G$ and $({}^a\phi^\Delta, \phi^{\#\Delta})\colon P^\Delta \to C$, whereas ψ is simply a Δ-homomorphism. In fact, ψ is not even a Δ-$\mathcal{G}$-homomorphism; however, it is a $\mathcal{C}$-homomorphism because $\mathcal{C} \subset \mathcal{F}$.

Proposition 34.1. *The $\mathcal{C}$-morphisms*

$$({}^a\psi^\Delta, \psi^{\#\Delta})\colon P^\Delta \to C \qquad \textit{and} \qquad ({}^a\phi^\Delta, \phi^{\#\Delta})\colon P^\Delta \to C$$

are the same.

Proof. Evidently ${}^a\psi^\Delta = {}^a\phi^\Delta$, since they both take any $\mathfrak{p} \in P^\Delta$ to (0). For the mapping on stalks, $\psi_{\mathfrak{p}}^{\#\Delta}\colon \mathcal{C} \to \mathcal{P}_{\mathfrak{p}}^\Delta$, we have

$$\psi_{\mathfrak{p}}^{\#\Delta}(c) = \frac{1 \otimes_{\mathcal{F}} c}{1 \otimes_{\mathcal{F}} 1} = \frac{c \otimes_{\mathcal{F}} 1}{1 \otimes_{\mathcal{F}} 1} = \phi_{\mathfrak{p}}^{\#\Delta}(c),$$

since $c \in \mathcal{F}$. □

Recall the definitions of μ, ϵ and T from Definitions 16.4 and 16.9. Proposition 28.4 asserts that

$$(P \times_G P)^\Delta = P^\Delta \times_C P^\Delta.$$

Thus we can make the following definition.

Definition 34.2. The $\mathcal{C}$-morphism

$$({}^a\mu^\Delta, \mu^{\#\Delta})\colon P^\Delta \times_C P^\Delta \to P^\Delta$$

is denoted by $(m, m^\#)$ and is called the *multiplication of* P^Δ.

In all of the following diagrams we write $\times$ for $\times_C$ and $\otimes$ for $\otimes_{\mathcal{G}}$.

Proposition 34.3. *Multiplication is associative, i.e., the diagram*

$$\begin{array}{ccc} P^\Delta \times P^\Delta \times P^\Delta & \xrightarrow{m\times\mathrm{id}} & P^\Delta \times P^\Delta \\ \downarrow{\scriptstyle \mathrm{id}\times m} & & \downarrow{\scriptstyle m} \\ P^\Delta \times P^\Delta & \xrightarrow[m]{} & P^\Delta \end{array}$$

commutes.

Proof. This is because μ is coassociative, i.e., the diagram

$$\begin{array}{ccc} \mathcal{P} \otimes \mathcal{P} \otimes \mathcal{P} & \xleftarrow{\mu\otimes\mathrm{id}} & \mathcal{P} \otimes \mathcal{P} \\ \uparrow{\scriptstyle \mathrm{id}\otimes\mu} & & \uparrow{\scriptstyle \mu} \\ \mathcal{P} \otimes \mathcal{P} & \xleftarrow[\mu]{} & \mathcal{P} \end{array}$$

commutes by Proposition 16.5. □

Definition 34.4. The $\mathcal{C}$-morphism

$$({}^a\epsilon^\Delta, \epsilon^{\#\Delta})\colon C \to P^\Delta$$

is denoted by $(e, e^\#)$ and is called the *identity of* P^Δ.

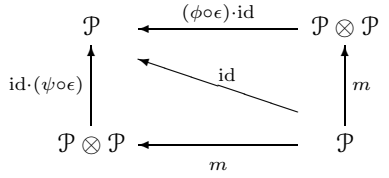
Of course C consists of the single point (0) and, by Proposition 17.1,

$$e((0)) = \epsilon^{-1}(0) = \mathfrak{p}_{\mathrm{id}}\,.$$

Proposition 34.5. *The following diagram is commutative:*

$$\begin{array}{ccc} P^\Delta & \xrightarrow{(e\circ {}^a\phi^\Delta,\ \mathrm{id})} & P^\Delta \times P^\Delta \\ \downarrow{\scriptstyle (\mathrm{id},\ e\circ {}^a\phi^\Delta)} & \searrow^{\mathrm{id}} & \downarrow{\scriptstyle m} \\ P^\Delta \times P^\Delta & \xrightarrow[m]{} & P^\Delta \end{array}$$

Proof. This comes from Proposition 34.1 and the following commutative diagram, which is Proposition 16.5:



□

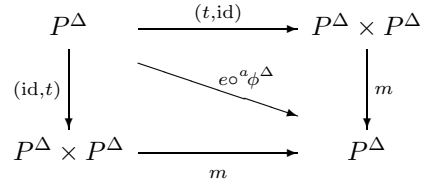
Note that the bialgebra structure of $\mathcal{P}$ is evident in the preceding diagram, because both ϕ and ψ appear. Next we come to T. It is not a Δ-$\mathcal{G}$-homomorphism, but it is a $\mathcal{C}$-homomorphism, so we can make the following definition.

Definition 34.6. The $\mathcal{C}$-morphism

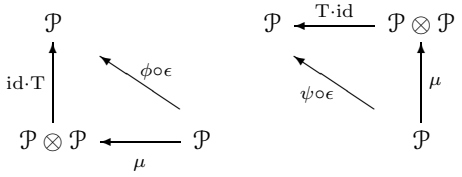
$$({}^a\mathrm{T}^\Delta, \mathrm{T}^{\#\Delta})\colon P \to P^\Delta$$

is denoted by $(t, t^\#)$ and is called the *inverse of* P^Δ.

Proposition 34.7. *The following diagram is commutative:*



Proof. We use Proposition 34.1 and the following two commutative diagrams:



□

Theorem 34.8. *P^Δ with multiplication m, identity e and inverse t is a group scheme over C.*

Proof. Propositions 34.3, 34.5 and 34.7. □

35. The Galois group

In this section we denote the group scheme P^Δ, as defined in the previous section, by G. In Corollaries 14.3 and 14.4 we identified $\mathrm{Gal}(\mathcal{G}/\mathcal{F})$ with the set of closed points of G. We claim that these are precisely the $\mathcal{C}$-rational points, which we denote by $G_\mathcal{C}$.

The $\mathcal{C}$-rational points are closed points by Grothendieck-Dieudonne [5, Proposition 3.5.6]. Conversely, if $\mathfrak{p} \in G$ is a closed point, then $\mathfrak{p}$ is a maximal Δ-ideal of $\mathcal{P}$. By Corollary 14.4, $\mathfrak{p}$ is a maximal ideal and $\mathfrak{p} = \mathfrak{p}_\sigma$ for some $\sigma \in \mathrm{Gal}(\mathcal{G}/\mathcal{F})$. Therefore $\mathcal{P}/\mathfrak{p} = \mathcal{P}_\mathfrak{p}/\mathfrak{p}\mathcal{P}_\mathfrak{p} = \mathcal{G}\sigma\mathcal{G} = \mathcal{G}$ and $\mathcal{P}_\mathfrak{p}^\Delta/(\mathfrak{p}\mathcal{P}_\mathfrak{p})^\Delta = \mathcal{C}$, so $\mathfrak{p}$ is $\mathcal{C}$-rational.

Theorem 35.1. *The mapping*

$$\Phi\colon\ \mathrm{Gal}(\mathcal{G}/\mathcal{R}) \to G_{\mathcal{C}}, \quad \sigma \mapsto \mathfrak{p}_\sigma,$$

is an isomorphism of groups.

Proof. Proposition 17.1. □

If $\mathfrak{a}$ is a radical Δ-ideal of $\mathcal{P}$, then, by Definition 18.1,

$$v(\mathfrak{a}) = \{\, \sigma \in \mathrm{Gal}(\mathcal{G}/\mathcal{F}) \mid \mathfrak{a} \subset \mathfrak{p}_\sigma \,\}.$$

Evidently $\Phi(v(\mathfrak{a}))$ is the set of $\mathcal{C}$-rational (or closed) points of $V(\mathfrak{a})^\Delta$.

As we have seen in Section 24, every radical Δ-ideal $\mathfrak{a} \subset \mathcal{P}$ induces a reduced closed subscheme $V(\mathfrak{a}) = \mathrm{diffspec}\, \mathcal{P}/\mathfrak{a}$ of P, and every reduced closed subscheme is of this form. Proposition 28.5 implies that $V(\mathfrak{a})^\Delta$ is a reduced closed subscheme of $G = P^\Delta$, and every reduced closed subscheme is of that form.

Proposition 35.2. *Let $\mathfrak{a} \subset \mathcal{P}$ be a Δ-coideal. Then $V(\mathfrak{a})^\Delta$ is a closed subgroup scheme of G. Conversely, if H is a closed subgroup scheme of G, then there is a Δ-coideal $\mathfrak{a}$ such that $H = V(\mathfrak{a})^\Delta$.*

Proof. Suppose that $\mathfrak{a}$ is a Δ-coideal, and let $H = V(\mathfrak{a})^\Delta$. Using the assumption that $\epsilon(\mathfrak{a}) = 0$ and Proposition 17.1, we have

$$\mathfrak{a} \subset \epsilon^{-1}(0) = \mathfrak{p}_{\mathrm{id}} = e((0));$$

hence $\mathfrak{p}_{\mathrm{id}} \in H$.

Next we show that the multiplication m restricts to H, i.e. $m(H \times_C H) \subset H$. By Proposition 16.10, $\mathfrak{a}$ is a radical ideal, so we may use Proposition 28.5. Thus it suffices to show that μ induces a mapping

$$\mathcal{P}/\mathfrak{a} \otimes_{\mathcal{G}} \mathcal{P}/\mathfrak{a} \to \mathcal{P}/\mathfrak{a},$$

which is true because

$$\mu(\mathfrak{a}) \subset \mathfrak{a} \otimes_{\mathcal{G}} \mathcal{P} + \mathcal{P} \otimes_{\mathcal{G}} \mathfrak{a}\,.$$

Finally, we need to show that $t(H) \subset H$, i.e.,

$$\mathrm{T}(\mathfrak{a}) \subset \mathfrak{a},$$

which follows from Proposition 16.10.

Conversly, assume that H is a closed subgroup scheme of G. It is known that any group scheme over a field of characteristic zero is reduced, e.g. Mumford [22, Theorem, p. 101], so H is reduced and we may use Propositions 24.6 and 28.5. Hence there exists a radical Δ-ideal $\mathfrak{a} \subset \mathcal{P}$ such that $H = V(\mathfrak{a})^\Delta$. We must show that $\mathfrak{a}$ is a Δ-coideal. Since $\mathfrak{p}_{\mathrm{id}} \in H$, $\mathfrak{a} \subset \epsilon^{-1}(0)$, as above, so $\epsilon(\mathfrak{a}) = 0$. Similarly, the fact that H is closed under multiplication gives

$$\mu(\mathfrak{a}) \subset \mathfrak{a} \otimes_{\mathcal{G}} \mathcal{P} + \mathcal{P} \otimes_{\mathcal{G}} \mathfrak{a}.$$

□

36. The fundamental theorem

In Section 19 we proved the fundamental theorem of differential Galois theory, relating intermediate Δ-fields to closed subgroups of $\mathrm{Gal}(\mathcal{G}/\mathcal{F})$. However, we did not yet know of the group scheme G, so we did not present the theorem in its usual form. This section remedies that flaw. As in Theorem 35.1, we define

$$\Phi\colon \mathrm{Gal}(\mathcal{G}/\mathcal{R}) \to G_{\mathcal{C}}, \quad \sigma \mapsto \mathfrak{p}_\sigma\,.$$

Definition 36.1. Let $H \subset G$ be a subgroup scheme. Then the fixed field of $H_{\mathcal{C}}$ is denoted by

$$\mathcal{G}(H) = \{\, h \in \mathcal{G} \mid \sigma h = h \text{ whenever } \Phi(\sigma) = \mathfrak{p}_\sigma \in H_{\mathcal{C}} \,\}.$$

In the notation of Definition 19.1,

$$\mathcal{G}(H) = \mathcal{G}^{\Phi^{-1}(H_{\mathcal{C}})}.$$

Definition 36.2. Let $\mathcal{H}$ be an intermediate Δ-field, i.e. $\mathcal{F} \subset \mathcal{H} \subset \mathcal{G}$, and let $\mathfrak{a}$ be the kernel of

$$\mathcal{P} = \mathcal{G} \otimes_{\mathcal{F}} \mathcal{G} \to \mathcal{G} \otimes_{\mathcal{H}} \mathcal{G}, \quad a \otimes_{\mathcal{F}} b \mapsto a \otimes_{\mathcal{H}} b.$$

Then $V(\mathfrak{a})^{\Delta}$ is denoted by $G(\mathcal{H})$.

By Proposition 35.2, $\mathfrak{a}$ is a Δ-coideal; so $G(\mathcal{H})$ is a subgroup scheme of G. In the notation of Definition 18.1,

$$\mathrm{Gal}(\mathcal{G}/\mathcal{H}) = v(\mathfrak{a}) = G(\mathcal{H})_{\mathcal{C}}.$$

Theorem 36.3 (First fundamental theorem)**.** *The mappings*

$$H \to \mathcal{G}^H$$

from subgroup schemes of G to intermediate Δ-fields and

$$\mathcal{H} \to G(\mathcal{H})$$

from intermediate Δ-fields to subgroup schemes are bijective and inverse to each other.

Proof. Theorem 19.3. □

37. Equivalence classes of Δ-isomorphisms

In Kolchin [12, Chapter VI] the Galois group is the set of all Δ-*isomorphisms* of $\mathcal{G}$ over $\mathcal{F}$, not merely automorphisms. In order that these form a set we must fix a universal Δ-field $\mathcal{U}$, as Kolchin did, and define a Δ-isomorphism of $\mathcal{G}$ to be a Δ-isomorphism into $\mathcal{U}$. In this section we shall see that the set of Δ-isomorphism classes under a certain equivalence is the entire group scheme G.

Definition 37.1. Let σ and τ be Δ-isomorphisms of $\mathcal{G}$ over $\mathcal{F}$ (into $\mathcal{U}$). We say that σ and τ are *equivalent* if there is a Δ-isomorphism

$$\mathcal{G}\sigma\mathcal{G} \to \mathcal{G}\tau\mathcal{G}$$

over $\mathcal{G}$ (i.e., $g \mapsto g$) with $\sigma g \mapsto \tau g$.

In the language of Section 7, σ and τ are equivalent if and only if they are generic specializations of each other. Evidently this is an equivalence relation.

Definition 37.2. Let $\mathrm{Iso}(\mathcal{G}/\mathcal{F})$ be the set of equivalence classes of Δ-isomorphisms of $\mathcal{G}$ over $\mathcal{F}$. The class containing σ is denoted by $[\sigma]$.

Proposition 37.3. *Let $\sigma, \tau \in \mathrm{Gal}(\mathcal{G}/\mathcal{F})$. Then $[\sigma] = [\tau]$ if and only if $\sigma = \tau$.*

Proof. $\mathcal{G}\sigma\mathcal{G} = \mathcal{G}$. □

Thus we may identify $\mathrm{Gal}(\mathcal{G}/\mathcal{F})$ with a subset of $\mathrm{Iso}(\mathcal{G}/\mathcal{F})$.

Proposition 37.4. *Let σ and τ be Δ-isomorphisms of $\mathcal{G}$ over $\mathcal{F}$. Then $[\sigma] = [\tau]$ if and only if $\mathfrak{p}_\sigma = \mathfrak{p}_\tau$.*

Proof. Proposition 7.2. □

Proposition 37.5. *The mapping*

$$\mathrm{Iso}(\mathcal{G}/\mathcal{F}) \to G = P^{\Delta}, \quad [\sigma] \mapsto \mathfrak{p}_\sigma,$$

is bijective.

Proof. G, as a set, is nothing other than $\operatorname{diffspec} \mathcal{P}$. □

Thus $\mathrm{Iso}(\mathcal{G}/\mathcal{F})$ may be identified with the group scheme $G = P^{\Delta}$, and the subset $\mathrm{Gal}(\mathcal{G}/\mathcal{F})$ with $G_{\mathcal{C}}$. However, it is not readily apparent how to *intrinsically* describe the topology, multiplication, inverse, etc., on $\mathrm{Iso}(\mathcal{G}/\mathcal{F})$. It appears we must introduce $\mathcal{P} = \mathcal{G} \otimes_{\mathcal{F}} \mathcal{G}$, and use the Kolchin topology on $P = \operatorname{diffspec} \mathcal{R}$ and the coring structure on $\mathcal{P}$.

References

[1] **Atiyah, M. F.; MacDonald, I. G.** Introduction to commutative algebra. *Addison-Wesley, Reading, Mass.* 1969, MR **39:**4129.

[2] **Bourbaki, Nicolas.** Commutative algebra. Chapters 1–7. Translated from the French, *Addison-Wesley, Reading, Mass.*, 1972; latest reprint, *Springer-Verlag, Berlin,* 1998, MR **50:**12997; MR **2001g:**13001.

[3] **Buium, Alexandru.** Differential function fields and moduli of algebraic varieties. Lecture Notes in Mathematics, 1226. *Springer-Verlag, Berlin,* 1986, MR **88e:**14010.

[4] **Cohn, Paul Moritz.** Skew field constructions. London Mathematical Society Lecture Note Series, No. 27. *Cambridge University Press, Cambridge*, 1977, MR **57:**3190.

[5] **Grothendieck, A.; Dieudonné, J.** Éléments de Géométrie Algébrique I. Seconde édition, *Springer-Verlag, Berlin,* 1971, MR **36:**177a.

[6] **Hartshorne, Robin.** Algebraic geometry. Graduate Texts in Mathematics, No. 52. *Springer-Verlag, Berlin,* 1977, MR **57:**3116.

[7] **Kaplansky, Irving.** An introduction to differential algebra. Second edition. Actualités Scientifiques et Industrielles, No. 1251. Pulications de l'Institut de Mathématique de l'Université de Nancago, No. V. *Hermann, Paris,* 1996, MR **57:**297.

[8] **Keigher, William F.** Adjunctions and comonads in differential algebra. *Pacific J. Math.* **59** (1975), no. 1, 99–112, MR **52:**13770.

[9] ———— Prime differential ideals in differential rings. *Contributions to algebra (collection of papers dedicated to Ellis Kolchin),* 239–249. *Academic Press, New York,* 1977, MR **58:**5610.

[10] **Kolchin E. R.** Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations. *Ann. of Math. (2)* **49**, (1948). 1–42, MR **9:**561c. (Reprinted in [14].)

[11] ———— Galois theory of differential fields. *Amer. J. Math.* **75**, (1953). 753–824, MR **15:**394a. (Reprinted in [14].)

[12] ———— Differential algebra and algebraic groups. Pure and Applied Mathematics, Vol. 54. *Academic Press, New York-London,* 1973, MR **58:**27929

[13] ———— Constrained extensions of differential fields. *Advances in Math.* **12**, (1974). 141–170, MR **49:**4982. (Reprinted in [14].)

[14] **Kolchin, Ellis.** Selected works of Ellis Kolchin with commentary. Commentaries by Armand Borel, Michael F. Singer, Bruno Poizat, Alexandru Buium and Phyllis J. Cassidy. Edited and with a preface by Hyman Bass, Buium and Cassidy. *American Mathematical Society, Providence, RI,* 1999, MR **2000g:**01042.

[15] **Kolchin, Ellis; Lang, Serge.** Algebraic groups and the Galois theory of differential fields. *Amer. J. Math.* **80** (1958). 103–110, MR **20:**1109. (Reprinted in [14].)
[16] **Kovacic, Jerald J.** Differential schemes. In [39], pp. 71–94.
[17] ———— Global sections of diffspec, *Journal of Pure and Applied Algebra,* **171** (2002), No 2–3, 265–288, MR **2003c:**12008.
[18] **Levelt, A. H. M.** Differential Galois theory and tensor products. *Indag. Math. (N.S.)* **1** (1990), no. 4, 439–449, MR **92f:**12012.
[19] **Mac Lane, Saunders.** Categories for the working mathematician. Second edition. Graduate Texts in Mathematics, 5. *Springer-Verlag, New York,* 1998, MR **2001j:**18001.
[20] **Magid, Andy R.** Lectures on differential Galois theory. University Lecture Series, 7. *American Mathematical Society, Providence, RI,* 1994, MR **95j:**12008.
[21] **Marker, David; Pillay, Anand.** Differential Galois theory. III. Some inverse problems. *Illinois J. Math.* **41** (1997), no. 3, 453–461, MR **99m:**12011.
[22] **Mumford, David.** Abelian varieties. Tata Institute of Fundamental Research Studies in Mathematics, No. 5, *Published for the Tata Institute of Fundamental Research, Bombay, Oxford University Press, London* 1970, MR **44:**219.
[23] **Okugawa, Kôtaro.** Differential algebra of nonzero characteristic. Lectures in Mathematics, 16. *Kinokuniya Company Ltd., Tokyo,* 1987, MR **92e:**12007.
[24] **Pillay, Anand.** Differential Galois theory. I. *Illinois J. Math.* **42** (1998), no. 4, 678–699, MR **99m:**12009.
[25] ———— Differential Galois theory. II. Joint AILA-KGS Model Theory Meeting (Florence, 1995). *Ann. Pure Appl. Logic* **88** (1997), no. 2-3, 181–191, MR **99m:**12010.
[26] **Poizat, Bruno.** Une théorie de Galois imaginaire. *J. Symbolic Logic* **48** (1983), no. 4, 1151–1170, MR **85e:**03083.
[27] ———— Stable groups. Translated from the 1987 French original by Moses Gabriel Klein. Mathematical Surveys and Monographs, 87. *American Mathematical Society, Providence, RI,* 2001, MR **2002a:**03067.
[28] **Scanlon, Thomas.** Model theory and differential algebra. In [39], pp. 125–150, MR **2003g:**03062.
[29] **Sharp, Rodney Y.** The dimension of the tensor product of two field extensions. *Bull. London Math. Soc.* **9** (1977), no. 1, 42–48, MR **55:**10435.
[30] **Silverman, Joseph H.** The arithmetic of elliptic curves. Graduate Texts in Mathematics, 106. *Springer-Verlag, New York,* 1986. MR **87g:**11070
[31] **Sweedler, Moss.** The predual theorem to the Jacobson-Bourbaki theorem. *Trans. Amer. Math. Soc.* **213** (1975), 391–406, MR **52:**8188.
[32] **Takeuchi, Mitsuhiro.** A Hopf algebraic approach to the Picard-Vessiot theory. *J. Algebra* **122** (1989), no. 2, 481–509, MR **90j:**12016.
[33] **Umemura, Hiroshi.** Galois theory of algebraic and differential equations. *Nagoya Math. J.* **144** (1996), 1–58, MR **98c:**12009.
[34] ———— Differential Galois theory of infinite dimension. *Nagoya Math. J.* **144** (1996), 59–135, MR **98c:**12010.
[35] **Vámos, P.** On the minimal prime ideals of a tensor product of two fields. *Math. Proc. Cambridge Philos. Soc.* **84** (1978), no. 1, 25–35, MR **80j:**12016.
[36] **van der Put, Marius.** Differential Galois theory, universal rings and universal groups. In [39], pp. 171–189.
[37] **Weil, André.** Foundations of algebraic geometry. *American Mathematical Society, Providence, R.I.* 1962, MR **26:**2439.
[38] **Zariski, Oscar; Samuel, Pierre.** Commutative algebra, Vol. 1. With the cooperation of I. S. Cohen. Corrected reprinting of the 1958 edition. Graduate Texts in Mathematics, No. 28. *Springer-Verlag, New York-Heidelberg-Berlin,* 1975, MR **52:**5641.
[39] **Guo, Li et al. (editors)**, Differential algebra and related topics (Proc. Internat. Workshop, Newark, NJ, 2000), *World Sci. Publishing, River Edge, NJ*, 2002, MR **2003b:**12001.

Department of Mathematics, The City College of The City University of New York, New York, New York 10031
E-mail address: jkovacic@member.ams.org
URL: http://mysite.verizon.net/jkovacic