Hyperstructures and Idempotent Semistructures

by

Jeffrey Tolliver

A dissertation submitted to The Johns Hopkins University in conformity with the requirements for the degree of Doctor of Philosophy.

Baltimore, Maryland

May, 2015

Abstract

Much of this thesis concerns hypergroups, multirings, and hyperfields. These are analogous to abelian groups, rings, and fields, but have a multivalued addition operation.

M. Krasner introduced the notion of a valued hyperfield; The prototypical example is $K/(1+\mathfrak{m}_K^n)$ where K is a local field. P. Deligne introduced a category of triples whose objects have the form $\mathrm{Tr}_n(K) = (\mathcal{O}_K/\mathfrak{m}_K^n, \mathfrak{m}_K/\mathfrak{m}_K^{n+1}, \epsilon)$ where $\epsilon : \mathfrak{m}_K/\mathfrak{m}_K^{n+1} \to \mathcal{O}_K/\mathfrak{m}_K^n$ is the obvious map. In this thesis I relate the category of discretely valued hyperfields to Deligne's category of triples.

An extension of a local field is arithmetically profinite if the upper ramification subgroups are open. Given such an extension L/K, J.P. Wintenberger defined the norm field $X_K(L)$ as the inverse limit of the finite subextensions of L/K along the norm maps. Wintenberger has defined an addition operation on $X_K(L)$, and shown that $X_K(L)$ is a local field of finite characteristic. Using Deligne's triples, I have given a new proof of Wintenberger's characterization of its Galois group.

The semifield $\mathbb{Z}_{\max}$ is defined as $\{0\} \cup \{u^k \mid k \in \mathbb{Z}\}$ with addition given by

ABSTRACT

$u^m + u^n = u^{\max(m,n)}$. An extension of $\mathbb{Z}_{\max}$ is a semifield containing $\mathbb{Z}_{\max}$. The extension is finite if S is finitely generated as a $\mathbb{Z}_{\max}$-semimodule. In this thesis I classify the finite extensions of $\mathbb{Z}_{\max}$.

There are two previously known methods for constructing a hypergroup from a totally ordered set. In this thesis I generalize these to a family of constructions parametrized by hypergroups H satisfying $x - x = H$ for all $x \in H$.

We say a hyperfield K is selective if $1 + 1 - 1 - 1 = 1 - 1$ and for all $x, y \in K$ one has either $x \in x + y$ or $y = x + y$. In this thesis, I show that a selective hyperfield is characterized by a totally ordered group Γ, a hyperfield H satisfying $1 - 1 = H$, and an extension $\phi \in \mathrm{Ext}^1(\Gamma, H^\times)$.

We say a triple of elements (x, y, z) of an idempotent semiring is a corner triple if $x + y = y + z = x + z$. We say an idempotent semiring is regular if whenever (x, y, a) and (z, w, a) are corner triples, there exists b such that (x, z, b) and (y, w, b) are also corner triples. I prove in this thesis that the category of regular idempotent semirings is a reflective subcategory of the category of multirings.

Readers: Caterina Consani (Advisor) and Cristian Popescu.

Acknowledgments

I'd like to express my gratitude to my advisor Caterina Consani. I would also like to thank my fellow students, especially Jai Ung Jun, Vitaly Lorman, Kalina Mincheva, and Jingjing Zhang for useful discussions. I would also like to express my appreciation to the faculty and staff at Johns Hopkins University. Finally, I want to thank my parents, Eric and Holley for their support.

Dedication

This thesis is dedicated to Jingjing Zhang.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

In this thesis, we will study the relation between hyperstructures (e.g. hypergroups, multirings, hyperrings, and hyperfields) and idempotent semistructures (e.g. idempotent semigroups, idempotent semirings, and idempotent semifields). Hyperstructures are generalizations of classical algebraic structures in which the addition is multivalued, i.e. the sum of two elements is no longer an element but a subset. In the following definition, 2^H will denote the power set of H.

Definition 1.0.1. A canonical abelian *hypergroup* consists of a set H together with a multivalued addition operation $+ : H \times H \to 2^H$ sending two elements of H to a subset of H such that the following properties hold:

(i) $(x + y) + z = x + (y + z)$ for all $x, y, z \in H$.

(ii) $x + y = y + x$ for all $x, y \in H$.

(iii) There exists $0 \in H$ such that $x + 0 = \{x\}$ for all $x \in H$.

(iv) For all $x \in H$, there exists a unique element $-x \in H$ such that $0 \in x + (-x)$.

A *multiring* is a set H together with a multivalued addition operation and a single valued multiplication operation such that H is a commutative monoid under multiplication, a canonical abelian hypergroup under addition, and such that $x(y + z) \subseteq xy + xz$ and $0x = 0$ for all $x, y, z \in H$. A *hyperring* is a multiring such that $x(y + z) = xy + xz$. A *hyperfield* is a hyperring such that every nonzero element has a multiplicative inverse.

Hyperstructures have been applied to the study of local fields by M. Krasner.[5] More recently, they have been applied to quadratic forms and real algebraic geometry by M. Marshall,[24] to tropical geometry by O. Viro,[17] and to number theory by A. Connes and C. Consani[11].[12]

In chapter 3, we will give a brief summary of Krasner's work on limits of local fields.[5] Given a natural number k, one may associate to a local field[1] K the quotient $K/(1+\mathfrak{m}_K^k)$ of K by the action of the subgroup $1+\mathfrak{m}_K^k \subseteq K^\times$. This quotient carries the structure of a hyperfield. One says that K is a limit of a sequence of discretely valued fields K_i if for every fixed k there exists N such that $K_i/1+\mathfrak{m}_{K_i}^k \cong K/1+\mathfrak{m}_K^k$ for $i > N$ and if these isomorphisms are compatible with the projections $K/1+m_K^k \to K/1+m_K^j$ for $j < k$. Krasner has shown that in this case, a finite separable extension L of K may be understood in terms of a sequence of finite separable extensions L_i of K_i.

In the discretely valued case, P. Deligne has obtained a sharper result than Kras-

[1] In fact, Krasner proved his results with assuming the valuation is discrete. In the non-discrete case, one may replace the subgroup $1 + \mathfrak{m}_K^k \subseteq K^\times$ with a ball around 1.

ner's using more classical algebraic structures.[6] We will describe his approach in chapter 4. Rather than working with the hyperfield $K/1+\mathfrak{m}_K^k$, Deligne uses a triple of data consisting of the ring $\mathcal{O}_K/\mathfrak{m}_K^k$, the module $\mathfrak{m}_K/\mathfrak{m}_K^{k+1}$, and the canonical homomorphism $\mathfrak{m}_K/\mathfrak{m}_K^{k+1} \to \mathcal{O}_K/\mathfrak{m}_K^k$. This triple will be denoted $\mathrm{Tr}_k(K)$. We shall study the relation between Deligne's triples and Krasner's valued hyperfields in chapter 5. Deligne has proven the following theorem.

Theorem 1.0.2. *[6, 2.8]*$\mathrm{Tr}_k(K)$ *determines the quotient* $\mathrm{Gal}(\bar{K}/K)/\mathrm{Gal}(\bar{K}/K)^k$ *of the absolute Galois group.*[2].

If K is the limit of a sequence of local fields K_i, then Deligne's result implies in particular that for any fixed k, the k-th upper ramification groups of K and K_i agree for sufficiently large i. Since the absolute Galois group is the union of its upper ramification filtration, this recovers Krasner's result that the absolute Galois group of K may described in terms of the fields K_i and the compatibility between them.

A construction of similar flavor has been provided by J. P. Wintenberger. This construction was given in the paper[2] and will be described in chapter 6. To a suitable infinite extension L of a characteristic 0 local field K, Wintenberger associates a field $X_K(L)$ of finite characteristic, which is called the norm field of L/K. This field is defined as the inverse limit of the finite subextensions of L/K under the norm maps. Wintenberger has proven the following surprising theorem.

Theorem 1.0.3. *[2, 3.2.3]Let L/K be an infinite arithmetically profinite extension*

[2]The definition of this filtration on the absolute Galois group of K is given in Definition 2.0.12.

of a local field. Then $\mathrm{Gal}(\overline{X_K(L)}/X_K(L)) \cong \mathrm{Gal}(\bar{L}/L)$*.*

In chapter 7, and specifically Theorem 7.4.8 we will give a new proof of Wintenberger's result using Deligne's results on limits of local fields. The local field $X_K(L)$ is a limit in the sense of Krasner and Deligne of the finite subextensions of L/K, so its Galois group may be understood in terms of these fields. In particular any given group in the upper ramification filtration of the absolute Galois group of $X_K(L)$ is determined by corresponding group for any sufficiently large intermediate field F with $K \subseteq F$. On the other hand, as in the case of any algebraic extension, L is the union of the finite subextensions of L/K. Using group-theoretic computations with the upper ramification groups, one may show that for any fixed k, the k-th upper ramification groups of L and F coincide when F is a suitably large finite subextension of L/K. Since the upper ramification groups of L and $X_K(L)$ both coincide with those of suitably large finite subextensions of L/K, all of the upper ramification groups of L agree with those of $X_K(L)$. Upon proving these identification are compatible in a certain sense, we may use the fact that the absolute Galois group is a colimit of the upper ramification groups to obtain an isomorphism between the absolute Galois groups of L and of $X_K(L)$.

The remaining part of this thesis will be devoted to the study of idempotent semistructures. An *idempotent semigroup* satisfies the axioms of an abelian group except that instead of requiring the existence of additive inverses we require that $x + x = x$ for all x. An *idempotent semiring* is like a ring, but forms an idempotent semigroup under addition rather than an abelian group. An idempotent semigroup is *selective* if for all x, y one has $x + y \in \{x, y\}$. Precise definitions will be given in Definition 8.2.1. Idempotent and selective semigroups appear naturally in the study of ordered sets. Idempotent semifields have been studied in connection with tropical geometry.

The semifield $\mathbb{Z}_{\max}$ has played a prominent role in the recent work of A. Connes and C. Consani. They have shown that the epicyclic category may be interpreted as a category of projective spaces over $\mathbb{Z}_{\max}$.[13] They have also defined a geometric object called the arithmetic site, on which the Riemann zeta function can be viewed as counting fixed points of a Frobenius operator.[26] Their arithmetic site consists of the semiring $\bar{\mathbb{N}} = (-\mathbb{N})_{\max}$ viewed as an object of the topos $\widehat{\mathbb{N}^{\times}}$. $\mathbb{Z}_{\max}$ arises as the semifield of fractions of $\bar{\mathbb{N}}$, and furthermore, the category of points of $\widehat{\mathbb{N}^{\times}}$ is equivalent to the category of subextensions of $\mathbb{Q}_{\max}/\mathbb{Z}_{\max}$.

A natural question which arises is to classify the finite subextensions of $\mathbb{Z}_{\max}$, that is the semifields which contain $\mathbb{Z}_{\max}$ and are finitely generated as a module over $\mathbb{Z}_{\max}$. Given a positive integer n, Connes and Consani obtained an extension $F^{(n)}$, which may be viewed as the subsemifield of $\mathbb{Q}_{\max}$ corresponding to rational numbers with denominator dividing n. One may also wish to understand division semirings containing $\mathbb{Z}_{\max}$ and finite dimensional as a module over $\mathbb{Z}_{\max}$. I have proven the following theorem about finite extensions and division semialgebras over $\mathbb{Z}_{\max}$. In chapter 8, we classify the finite extensions of the semifield $\mathbb{Z}_{\max}$, by proving the following theorem (c.f. Theorems 8.7.3 and 8.9.8).

Theorem 1.0.4. *Let n be a positive integer. Up to isomorphism, $\mathbb{Z}_{\max}$ has exactly one extension of degree n. Furthermore, if D is a division semiring containing $\mathbb{Z}_{\max}$ and is finitely generated as a semimodule over $\mathbb{Z}_{\max}$ then D is commutative.*

In chapters 10 and 9, we turn to the problem of relating hyperstructures with idempotent semistructures. One expects the two types of structure to be related because they both arise naturally in connection with tropical geometry, and with Connes' and Consani's work on the Riemann zeta function and the absolute point. Furthermore, there are two known methods for constructing a hypergroup from a totally ordered set, or equivalently from a selective hypergroup. The first, which was independently discovered by M. Ştefănescu and by Viro[17],[22] puts a multivalued addition on the underlying set of the selective semifield. The second, which was discovered by S. Henry,[14] involves gluing two copies of the totally ordered group together, and may be thought of as a modified version of the Grothendieck group construction.

In chapter 9, we define a class of hypergroups called idempotent hypergroups by analogy with idempotent semigroups. We show that every hypergroup H is canonically equipped with a map v to a poset Γ. In the case of idempotent hypergroups, the definition of this map resembles that of the ordering on an idempotent semiring, and we have proven the following theorem, which tells us that v behaves like a valuation (c.f. section 9.2, especially Lemma 9.2.13).

Theorem 1.0.5. *Let H be an idempotent hypergroup. Let v and Γ be as above. Then $v(x) = 0$ if and only if $x = 0$. For all $x \in H$, we have $v(x) = v(-x)$, and for all $x, y \in H$ and all $t \in \Gamma$ with $v(x) \leq t$ and $v(y) \leq t$, we have $v(x + y) \leq t$.*

However the target Γ of the valuation we define is general only partially ordered, rather than totally ordered. We then define the notion of a selective hypergroup by analogy with selective semigroups. To a selective hyperfield K, one may associate a selective hyperfield k whose valuation is trivial, and which may be viewed as the residue hyperfield. One may also associate to K it's value group Γ, which is the totally ordered that appears as the image of its valuation. To the selective hyperfield K, one may also associate a short exact sequence $1 \to k^\times \to K^\times \to \Gamma \to 1$. We will show the following theorem (c.f. Corollary 9.4.15).

Theorem 1.0.6. *Let k be a trivially valued selective hyperfield, and Γ be a totally ordered group. Then selective hyperfields with residue hyperfield k and value group Γ are classified by $\mathrm{Ext}^1(\Gamma, k^\times)$, that is by the set of isomorphism classes of short exact sequences $1 \to k^\times \to G \to \Gamma \to 1$.*

In chapter 9, we will also give a method of producing a selective hypergroup $\mathcal{T}(S, k)$ from a totally ordered set S, and a selective hypergroup k, such that the valuation on k is trivial. In the case where $k = \mathbb{K}$ is the Krasner hyperfield[3], our construction recovers the aforementioned construction of Ştefănescu and Viro. In the case where $k = \mathbb{S}$, our construction is that of Henry.

[3] c.f. Example 3.1.5.

In chapter 10, we generalize the construction of Ştefănescu and Viro in a different direction by relaxing the condition that the input to the construction must be totally ordered. We introduce a class of posets, which we call regular posets, and which serve as the setting for our construction. They are defined as follows:

Definition 1.0.7. Let S be a poset. A multiset $\{x_1, \ldots, x_n\} \subseteq S$ is called a corner set if for all $1 \leq j \leq n$ and all $z \in S$ with $x_i \leq z$ for all $i \neq j$, one has $x_j \leq z$. A poset is regular if whenever x, y, z, b are chosen such that $\{x, y, b\}$ and $\{z, w, b\}$ are corner sets, there exists a such that $\{x, z, a\}$ and $\{y, w, a\}$ are corner sets.

We prove the following theorem (c.f. Theorem 10.1.15).

Theorem 1.0.8. *Every modular lattice is a regular poset. In particular, this applies to any distributive lattice.*

We may use this theorem to show in particular that any totally ordered set is regular, that any idempotent semifield is regular, and that polynomials over a regular idempotent semiring are regular. Furthermore, the set of ideals of a ring, or subgroups of an abelian group is a regular poset when partially ordered by inclusion.

On any regular poset with a minimal element, and in particular on any regular idempotent semigroup, we define a multivalued addition operation making the poset into a hypergroup, as follows:

Theorem 1.0.9. *Let S be a regular poset with minimal element. For $x, y \in S$, let $x + y = \{z \mid \{x, y, z\}$ is a corner set.$\}$. Then under this addition operation, S*

becomes a hypergroup. This gives a functor Y from the category of regular idempotent semigroups to the category of hypergroups. Furthermore, Y induces a functor from regular idempotent semirings to multirings.

We prove the following theorem (c.f Theorems 10.2.6 and 10.3.3, as well as Proposition 10.2.12).

Theorem 1.0.10. *Let S be a regular idempotent semiring. Then ideals of $Y(S)$ correspond to strong ideals of S.*

We show there is a functor $\mathcal{S}_f$ from hypergroups to regular semigroups. This functor takes a hypergroup to the set of its finitely generated subhypergroups. We then prove the following theorem (c.f theorems 10.4.14, 10.4.15, and 10.4.13).

Theorem 1.0.11. *The functor $\mathcal{S}_f$ from hypergroups to idempotent semigroups is left adjoint to the functor Y from idempotent semigroups to hypergroups. Furthermore, Y is fully faithful and $\mathcal{S}_f \circ Y$ is naturally isomorphic to the identity via the counit of the adjunction.*

When R is a multiring, $\mathcal{S}_f(R)$ naturally caries the structure a regular idempotent semiring. In the case where R is a ring, $\mathcal{S}_f(R)$ is the target of the universal valuation introduced by J. Giansiracusa and N. Giansiracusa[25].[23] $\mathcal{S}_f$ may be viewed as a functor from multirings to idempotent semirings, while Y may be viewed as a functor in the reverse direction. In section 10.5, we prove the following theorem.

Theorem 1.0.12. *The functor $\mathcal{S}_f$ from multirings to idempotent semirings is left adjoint to the functor Y from idempotent semirings to multirings. Furthermore, Y is fully faithful and $\mathcal{S}_f \circ Y$ is naturally isomorphic to the identity via the counit of the adjunction.*

1.1 Notation

In this paper, all rings will be commutative with identity except when otherwise stated. All semigroups will be assumed abelian. All hypergroups will be assumed to be canonical and abelian. Until chapter 8, valuations will have values in a subgroup of $\mathbb{R}$ rather than an arbitrary totally ordered group. The completion of a metric space X will be denoted $\hat{X}$

If R is a local ring, we will denote its maximal ideal by $\mathfrak{m}_R$.

If K is a field, $\bar{K}$ will denote its separable closure, and we let $G_K = \mathrm{Gal}(\bar{K}/K)$. If L/K is a finite field extension, $N_{L/K}$ will denote the norm map from L to K.

We say K is a local field if it is complete with respect to a discrete valuation and has a perfect residue field of finite characteristic. Note that this is more general than the usual definition since we do not require that the residue field be finite. We will denote the residue characteristic by p. If K is a local field, we denote its ring of integers by $\mathcal{O}_K$ and the maximal ideal by $\mathfrak{m}_K = \mathfrak{m}_{\mathcal{O}_K}$. We will denote its valuation by v.

Chapter 2

Ramification Theory

In this section we give a brief review of the upper and lower ramification filtrations of the Galois group of a local field. Essentially all of the material in this section may be found in [1, IV.1,IV.3]. Throughout this section, K will denote a local field.

Definition 2.0.1. If L/K is a finite Galois extension of local fields and $i \in \mathbb{R}$, we let $\mathrm{Gal}(L/K)_i = \{\sigma \in \mathrm{Gal}(L/K) \mid v(\sigma x - x) \geq i + 1 \forall x \in L\}$. This gives a decreasing filtration by normal subgroups on $\mathrm{Gal}(L/K)$ called the lower ramification filtration.

Remark 2.0.2. For any x, let $\lceil x \rceil$ denote the smallest integer $\geq x$. Then $\mathrm{Gal}(L/K)_i = \mathrm{Gal}(L/K)_{\lceil i \rceil}$ for all i.

Example 2.0.3. $\mathrm{Gal}(L/K)_{-1} = \mathrm{Gal}(L/K)$, $\mathrm{Gal}(L/K)_0$ is the inertia group, and $\mathrm{Gal}(L/K)_1$ is the wild inertia group.

If $K \subseteq E \subseteq L$, then the canonical map $\mathrm{Gal}(L/E) \to \mathrm{Gal}(L/K)$ is compatible with the filtration in the sense that it sends $\mathrm{Gal}(L/E)_i$ to $\mathrm{Gal}(L/E)_i$. More precisely, the image of $\mathrm{Gal}(L/E)_i$ under the inclusion is $\mathrm{Gal}(L/K)_i \cap \mathrm{Gal}(L/E)$. However $\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$ is not compatible with the filtration. In order to give a precise description of what this map does to the lower ramification filtration, we will need the following definition.

Definition 2.0.4. Let L be a finite Galois extension of a local field K, and let $\phi_{L/K}(u) = \int_0^u \frac{|\mathrm{Gal}(L/K)_t|}{|\mathrm{Gal}(L/K)_0|} dt$ for $u \geq -1$.

We now list some of the basic properties of this function.

Remark 2.0.5. Let L/K be finite Galois. Because the integrand in 2.0.4 is piecewise constant, $\phi_{L/K}$ is piecewise linear and continuous. Because the integrand is positive, $\phi_{L/K}$ is strictly increasing and hence one-to-one. Because the integrand is bounded by 1, we always have $\phi_{L/K}(x) \leq x$. Since $\phi_{L/K}(-1) = -1$ and $\phi_{L/K}(x)$ tends to ∞ as $x \to \infty$, it follows from the intermediate value theorem that $\phi_{L/K} : [-1, \infty) \to [-1, \infty)$ is bijective. Also $\phi_{L/K}(x) = x$ for $-1 < x \leq 0$.

The importance of $\phi_{L/K}$ comes from the following theorem.

Theorem 2.0.6. *[1, IV.3 Lemma 5]Let L/K be finite Galois, and let E/K be a Galois subextension. The image of $\mathrm{Gal}(L/K)_i$ in $\mathrm{Gal}(E/K)$ is $\mathrm{Gal}(E/K)_{\phi_{L/E}(i)}$.*

For future convenience we would like to define $\phi_{L/K}$ for non-Galois extensions. To do this, we need the following result.

Theorem 2.0.7. *[1, IV.3 Prop 15]Let L/K be finite Galois, and let E/K be a Galois subextension. Then $\phi_{L/K} = \phi_{E/K} \circ \phi_{L/E}$*

Definition 2.0.8. Let L/K be a finite separable extension. We define $\phi_{L/K} = \phi_{M/K} \circ \phi_{M/L}^{-1}$ where M/K is any finite Galois extension containing L.

The following result follows easily from 2.0.7.

Corollary 2.0.9. *The function $\phi_{L/K}$ of 2.0.8 is well defined. Theorem 2.0.7 holds even when the extensions are not Galois. Furthermore all of the statements in 2.0.5 are true without the hypothesis that L/K is Galois.*

By 2.0.5, $\phi_{L/K}$ is invertible, so we can make the following definition.

Definition 2.0.10. Suppose L/K is finite and separable. We let $\psi_{L/K} : [-1, \infty) \to [-1, \infty)$ be the inverse of $\phi_{L/K}$.

It is worth mentioning the following facts, which are trivial consequences of the corresponding facts for $\phi_{L/K}$.

Remark 2.0.11. If E/K is a subextension of L/K, then $\psi_{L/K} = \psi_{L/E}\psi_{E/K}$. The function $\psi_{L/K}$ is continuous, piecewise linear, bijective, and strictly increasing. For all $x \in [-1, \infty)$, $\psi_{L/K}(x) \geq x$. Also, $\psi_{L/K}(x) = x$ for $-1 \leq x \leq 0$.

We will now introduce a filtration on $\mathrm{Gal}(L/K)$ which is compatible with the map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$, but is no longer compatible with $\mathrm{Gal}(L/E) \to \mathrm{Gal}(L/K)$.

Definition 2.0.12. Let L/K be a finite Galois extension of a local field. Then we define $\mathrm{Gal}(L/K)^u = \mathrm{Gal}(L/K)_{\psi_{L/K}(u)}$. This is called the upper ramification filtration.

An easy calculation using 2.0.7 and 2.0.6 shows the following standard result.

Proposition 2.0.13. [1] *Let L/K a finite Galois extension. Let E/K be a Galois subextension. Then the image of* $\mathrm{Gal}(L/K)^u$ *in* $\mathrm{Gal}(E/K)$ *is* $\mathrm{Gal}(E/K)^u$*.*

The fact that the lower ramification filtration is compatible with the inclusion $\mathrm{Gal}(L/E) \to \mathrm{Gal}(L/K)$ immediately implies the following standard result.

Proposition 2.0.14. [1] *Let L/K a finite Galois extension. Let E/K be a subextension. Then* $\mathrm{Gal}(L/E)^u = \mathrm{Gal}(L/K)^{\phi_{E/K}(u)} \cap \mathrm{Gal}(L/E)$*.*

The upper ramification filtration in fact extends to a filtration on the absolute Galois group of a local field.

Definition 2.0.15. Let $G_K^u = \varprojlim \mathrm{Gal}(L/K)^u$, where the limit is over the poset of all finite Galois extensions L/K inside a fixed separable closure, and where the maps $\mathrm{Gal}(L/K)^u \to \mathrm{Gal}(E/K)^u$ appearing in the limit are those given by 2.0.13. This will be regarded as a subgroup of $G_K = \varprojlim \mathrm{Gal}(L/K)$ in the obvious way.

Proposition 2.0.14 has the following corollary.

Corollary 2.0.16. [1] *Let L/K be a finite separable extension of a local field. Then* $G_L^u = G_K^{\phi_{L/K}(u)} \cap G_L$*.*

We now give a formula for $\psi_{L/K}$ analogous to 2.0.4.

Remark 2.0.17. If L/K is finite Galois, then $\psi_{L/K}(x) = \displaystyle\int_0^x \frac{|\mathrm{Gal}(L/K)^0|}{|\mathrm{Gal}(L/K)^u|} du$. This fact may be proven by differentiating $\psi_{L/K}$ using the inverse function theorem. In addition, for any finite separable L/K, $\psi_{L/K}(t) = \displaystyle\int_0^t \frac{|G_K^0|}{|G_L G_K^u|} du$. In the Galois case, this reduces to the previous formula. For the general case one reduces to the Galois case by using the chain rule to show that if $f_{L/K}(t)$ denotes $\int_0^t \frac{|G_K^0|}{|G_L G_K^u|} du$, then $f_{L/K} = f_{L/E} f_{E/K}$ for any intermediate extension E.

Finally we introduce some notation which will be useful in later chapters.

Definition 2.0.18. Let L/K be a separable extension of K. Let $u \in \mathbb{R}$. We will say L/K has ramification bounded above by u if $G_K^u \subseteq G_L$. We say it has ramification bounded below by u if $G_K^u G_L = G_K$.

Example 2.0.19. Let K be a local field and L/K be finite and separable. L/K has ramification bounded above by 0 iff it is unramified. It has ramification bounded below by 0 iff it is totally ramified.

The terminology is motivated by the following lemma. In fact,[6] defines L/K to have ramification bounded by u if $\mathrm{Gal}(\tilde{L}/K)^u = 1$.

Lemma 2.0.20. *Let L/K be a separable extension with Galois closure $\tilde{L}/K$. Then L/K has ramification bounded above by u if and only if* $\mathrm{Gal}(\tilde{L}/K)^u = 1$.

Proof. First suppose $\mathrm{Gal}(\tilde{L}/K)^u = 1$. Then $G_K^u \subseteq G_{\tilde{L}} \subseteq G_L$.

Conversely suppose L/K has ramification bounded above by u. Then $G_L \subseteq G_K^u$. Since G_K^u is normal and since $G_{\tilde{L}}$ is the normal closure of G_L, it follows that $G_{\tilde{L}} \subseteq G_K^u$. Hence $\mathrm{Gal}(\tilde{L}/K)^u = 1$. □

Definition 2.0.21. $\mathcal{C}_K^u$ will denote the category of finite separable extensions with ramification bounded above by u

Chapter 3

Krasner's valued hyperfields and limits of local fields

In this chapter we will present a summary of Krasner's theory about the limit of a sequence of local fields; in particular this chapter will contain no original work. Krasner defined the notion of the limit of a sequence of local fields by reference to certain quotients of the local fields. Such quotients are hyperfields, which means that they have a well behaved multivalued addition operation. Krasner has shown that if K is the limit of a sequence K_i of local fields, then extensions of K may be understood in terms of suitable sequences of extensions of the K_i.

3.1 Hyperstructures

In this section we will present a generalization of classical algebraic structures to those with a multivalued operation. These will often occur as quotients of algebraic structures by an equivalence relation. In particular, by generalizing fields to hyperfields, we will be able to obtain interesting quotients of fields. This idea was first pursued by Krasner, who showed essentially that the quotient $K/(1+\mathfrak{m}_K^i)$ of a local field retains a lot of arithmetic information about K. More recently, this idea has been studied by Connes and Consani for the development of algebraic geometry and arithmetic over hyperrings.

Definition 3.1.1 ([5, §3]). We will use $\mathcal{P}X$ to denote the power set of a set X. A hypergroup H is a set together with a subset valued binary operation $H \times H \to \mathcal{PH}$ such that for all $x, y, z \in H$, $x(yz) = (xy)z$ and $H = xH = Hx$. For $A, B \in \mathcal{P}H$, we are using AB to denote $\{xy \mid x \in A, y \in B\}$, and for $x \in H$ we write xA to denote $\{x\}A$. H is called abelian if $ab = ba$ for all $a, b \in H$.

Example 3.1.2. Let G be a group. Let $\sim$ be an equivalence relation on G. Let $H = G/\sim$. Define a subset valued binary operation on H by $ab = \{xy \mid x \in a, y \in b\}$. Then H is readily seen to be a hypergroup.

Definition 3.1.3 ([5, §3]). A commutative hypergroup is called canonical if it satisfies the following axioms:

(i) There is an element $0 \in H$ such that $x + 0 = 0 + x = \{x\} \forall x \in H$.

(ii) For any $x \in H$, there is a unique element of H (denoted $-x$) such that $0 \in x + (-x)$. We will write $x - y$ to denote the set $x + (-y)$.

(iii) For any $x, y, z \in H$, we have $x \in y + z$ if and only if $x + (-z) \in y$.

Since we will not be interested in non-canonical or non-abelian hypergroups, for the remainder of this thesis, the word hypergroup will refer to canonical abelian hypergroups.

Definition 3.1.4 ([5, §3]). A (commutative) multiring is a set H that is both a commutative canonical hypergroup and a commutative monoid, and which satisfies the following:

(i) $(x + y)z \subseteq xz + yz$, where $+$ denotes the hypergroup operation, and concatenation denotes the monoid operation.

(ii) $0x = x0 = 0$ for all $x \in H$, where 0 is the identity element of the underlying hypergroup.

(iii) $H \neq \{0\}$. A hyperring is a multiring satisfying the stronger distributive law $(x+y)z = xz+yz$. A commutative hyperring is a hyperfield if every nonzero element has a multiplicative inverse.

Example 3.1.5. Let $\mathbb{K} = \{0, 1\}$ with $1+1 = \{0, 1\}$ and with the obvious multiplication. One may think of $\mathbb{K}$ as the quotient of a ring other than $\mathbb{F}_2$ by the relation which identifies all nonzero elements. $\mathbb{K}$ is called the Krasner hyperfield. Let $\mathbb{S} = \{0, 1, -1\}$ be equipped with the obvious multiplication and with addition satisfying $1 + 1 = 1$, $-1 + (-1) = -1$, and $1 - 1 = \mathbb{S}$. One may think of $\mathbb{S}$ as the quotient of $\mathbb{R}$ by the relation identifying any two nonzero elements that have the same sign. $\mathbb{S}$ is called the hyperfield of signs. We let $\Phi = S^1 \cup \{0\}$ be the union of the circle group and the zero element with the usual multiplication. If $x, y \in S^1$ are antipodal, we let $x + y = \Phi$; otherwise $x + y$ is the shortest arc from x to y.

Example 3.1.6. Let $\mathbb{Y}_\times = \mathbb{R}_{\geq 0}$ equipped with the usual multiplication. We define $x + y = x$ if $x > y$ and $x + x = \{t \in \mathbb{Y}_\times \mid t \leq x\}$. Let $\mathcal{T}\mathbb{R} = \mathbb{R}$ with the usual multiplication. We define addition by $x + y = x$ if $|x| > |y|$, $x + x = x$, and $x - x = \{t \in \mathcal{T}\mathbb{R} \mid |t| \leq |x|\}$. Let $\mathcal{T}\mathbb{C} = \mathbb{C}$ with the usual multiplication. For $x, y \in \mathcal{T}\mathbb{C}$ with $|x| > |y|$ let $x+y = x$, and similarly for when $|y| > |x|$. For $x, y \in \mathcal{T}\mathbb{C}$ with $y = -x$ we let $x + y = \{t \in \mathcal{T}\mathbb{C} \mid |t| \leq |x|\}$. Otherwise we let $x + y$ be the shortest arc containing x and y on the circle of radius $|x|$ around 0. Then $\mathbb{Y}_\times$, $\mathcal{T}\mathbb{R}$, and $\mathcal{T}\mathbb{C}$ are hyperfields. $\mathbb{Y}_\times$, $\mathcal{T}\mathbb{R}$, and $\mathcal{T}\mathbb{C}$ were introduced by O. Viro in connection with tropical geometry.[17]

The hyperfields $\mathbb{Y}_\times$, $\mathcal{T}\mathbb{R}$, and $\mathcal{T}\mathbb{C}$ played a prominent role in Viro's work; in particular a tropical variety may be viewed as the zero set of a family of polynomials over $\mathbb{Y}_\times$.

Definition 3.1.7. A homomorphism between two multirings or hyperrings H_1 and H_2 is a map $f : H_1 \to H_2$ such that $f(1) = 1$, $f(xy) = f(x)f(y)$ and $f(x+y) \subseteq f(x)+f(y)$ for all $x, y \in H_1$.

Example 3.1.8. If R is a ring and H is a hyperring obtained as a quotient of R, then the quotient map is a homomorphism of hyperrings.

Example 3.1.9. Any real number q induces a hyperring homomorphism $\mathbb{Z}[t] \to S$ sending a polynomial $f(t)$ to the sign of $f(q)$. If q is algebraic we can also define a hyperring homomorphism $Z[t] \to S$ sending $f(t)$ to $\lim_{x \to q^+} \text{Sign}(f(x))$ as well as a homomorphism sending $f(t)$ to $\lim_{x \to q^-} \text{Sign}(f(x))$. One can also define homomorphisms $\mathbb{Z}[t] \to S$ corresponding to $\pm\infty$. Connes and Consani have shown in[11] that these are the only homomorphisms from $\mathbb{Z}[t]$ to S.

Example 3.1.10. Let $\mathbb{Y}_\times$ be as in Example 3.1.6. Let F be a field with a non-archimedean absolute value. Then the valuation $v(x) := -ln|x|$ defines a homomorphism $F \to \mathbb{Y}_\times$. The fact that v is a homomorphism of multiplicative monoids is simply a restatement of the fact that $v(xy) = v(x) + v(y)$, while the fact that $v(x + y) \subseteq v(x) \Diamond v(y)$ is a restatement of the non-archimedean triangle inequality. Given a variety V over a non-archimedean field F, one would expect that morally V should induce a 'variety over $\mathbb{Y}$' by base change. This idea is closely related to tropical geometry, where one studies algebraic geometry over the semiring $\mathbb{R} \cup \{\infty\}$, in which addition is min and multiplication is addition of real numbers.

Definition 3.1.11 ([5, pg 144])**.** A valued hyperfield is a hyperfield equipped with a map $|\cdot| : H \to \mathbb{R}$ satisfying the following axioms:

(i) $|x| \geq 0$ with equality if and only if $x = 0$.

(ii) $|xy| = |x||y|$ for all $x, y \in H$.

(iii) $|x + y| \leq \max(|x|, |y|)$.

(iv) $|x + y|$ consists of a single element unless $0 \in x + y$. This axiom in particular implies that there is a well defined metric on H given by $d(x, y) = |x - y|$ for $x \neq y$ and $d(x, x) = 0$ for any $x \in H$ (It is guaranteed to be a metric by axioms (i) and (iii)).

(v) There is a real number $\rho > 0$ such that either $x + y$ is a closed ball of radius $\rho\max(|x|, |y|)$ for all x and y, or $x + y$ is an open ball of radius $\rho\max(|x|, |y|)$ for all $x, y \in H$. The smallest such ρ is called the norm of the valued hyperfield.

Example 3.1.12 ([5, pg 146]). Let $e \in \mathbb{N}$ be at least 1. Krasner has shown that if F is a local field, then $F/(1 + \mathfrak{m}_F^e)$ is a valued hyperfield. In fact, he showed in[10] that the quotient of any commutative ring by a subgroup of its multiplicative group is a hyperring, so that $F/(1 + \mathfrak{m}_F^e)$ is a hyperfield. To define the absolute value, we note that if $x \in y(1 + \mathfrak{m}_F^e)$, then $|x| = |y|$, so $|\bar{x}| = |x|$ is well-defined. (i), (ii) and (iii) of the definition of a valued hyperfield are obvious. For (v), we note that for $x, y \in K$, $\bar{x}$ and $\bar{y}$ are balls of radius $p^{-e}|x|$ and $p^{-e}|y|$ respectively. For (iv), we apply (v) to see that $\bar{x} + \bar{y}$ is a ball around $x + y$ with radius less than $\max(|x|, |y|)$. The absolute value in K is constant on any ball not containing 0.

Example 3.1.13. Given a real number ρ_Π, we can define an equivalence relation on any valued hyperfield H, in which the equivalence class of x is the ball of radius $\rho|x|$ around x. The quotient of H by this relation will be denoted H/Π, and can be shown to be a hyperfield. In the case where H is a field, this is Example 3.1.12.

Definition 3.1.14 ([5, pg 148]). A map $f : H_1 \to H_2$ between valued hyperfields is called a homomorphism if the following axioms hold:

(i) $f(xy) = f(x)f(y)$ for all $x, y \in H_1$.

(ii) $f^{-1}(a+b) = f^{-1}(a) + f^{-1}(b)$ for all $a, b \in H_2$. Note that this axiom differs from the definition of a homomorphism of hyperrings.

(iii) $|f(x)| = |x|$ for all $x \in H_1$.

(iv) The fiber over 1 is a ball. Consequently, all fibers are balls.

3.2 Limits

In this section, we will explain how to obtain a valued field from a suitable sequence of hyperfields. We then discuss the notion of a limit of a sequence of local fields, and what it means for a sequence of elements of these fields to converge.

Theorem 3.2.1 ([5, §5]). *For each $i \in \mathbb{N}$, let H_i be a complete valued hyperfield, and let ρ_i be its norm. Suppose $\rho_i \to 0$ as $i \to \infty$, and suppose we are given surjective homomorphisms $\theta_i : H_{i+1} \to H_i$ for all i. Then $K = \varprojlim H_i$ is a complete valued field.*

Proof. Because θ_i is a monoid homomorphism, K is a monoid in which every nonzero element is a unit. Let $\alpha, \beta \in K$, and let $\alpha_i, \beta_i \in H_i$ be the corresponding elements. Since θ_k preserves absolute value for all k, $|\alpha_j|$ is independent of j. We will denote the common value by $|\alpha|$.

Let $\theta_{i,j} : H_i \to H_j$ be the map induced by the maps θ_k. I claim that for each i, $\theta_{j,i}(\alpha_j + \beta_j)$ converges in the sense that for any $\gamma_j \in \alpha_j + \beta_j$, $\theta_{j,i}(\gamma_j)$ converges to a value independent of the choice of γ_j. Let γ_j' be another choice. Then by Definition

3.1.11(v), $d(\gamma_j, \gamma_j') \leq \rho_j \max(|\alpha|, |\beta|)$. Since $\lim_{j\to\infty} \rho_j = 0$, $\lim_{j\to\infty} d(\gamma_j, \gamma_j') = 0$. This shows that the limit of $\theta_{j,i}(\gamma_j)$, if it exists, does not depend on the choice of γ_j. In particular, we can take $\gamma_j' = \theta_{k,j}(\gamma_k)$, which is in $\alpha_j + \beta_j$ by Definition 3.1.14(iii), and by the fact that $\theta_{i,j}(\alpha_i) = \alpha_j$. Doing so shows that $\theta_{j,i}(\gamma_j)$ is Cauchy (and hence convergent), and we just saw that it is independent of the choice of γ_i.

It is straightforward to check that $\theta_{i,k}(\lim_{j\to\infty} \theta_{j,i}(\gamma_j)) = \lim_{j\to\infty} \theta_{j,k}(\gamma_j)$, so that we have an element $\alpha + \beta \in K$ defined by $(\alpha+\beta)_i = \lim_{j\to\infty} \theta_{j,i}(\gamma_j)$. One then verifies that this addition and the absolute value defined above make K into a complete valued field. □

Definition 3.2.2 ([5, pg 154])**.** We retain the notation of Theorem 3.2.1 and its proof, and we let $a_i \in H_i$. We say a_i converges additively if $d(a_i, \theta_i(a_{i+1}))$ tends to 0 as $i \to \infty$. We say an element $l \in K$ is its limit if $\lim_{i\to\infty} d(l_i, a_i) = 0$. We say a_i is multiplicatively convergent if it has finitely many nonzero terms, or if it converges additively to a nonzero limit. The convergence is said to be canonical if $a_i = l_i$ for all i.

Remark 3.2.3 ([5, pg 154]). Every additively or multiplicatively convergent sequence has a limit.

Definition 3.2.4 ([5, pg 155-156])**.** Let K, F be local fields. We say that K and F are residually isomorphic of norm p^{-e} if the valued hyperfields $K/(1+\mathfrak{m}_K^e)$, and $F/(1+\mathfrak{m}_F^e)$ are isomorphic.

Definition 3.2.5 ([5, pg 156])**.** We say a sequence of local fields K_i converges if for all $i \in \mathbb{N}$, there exists ρ_i such that K_i and K_{i+1} are residually isomorphic of norm ρ_i and $\rho_i \to 0$ as $i \to \infty$. We may assume that ρ_i is decreasing. We say that the limit of the sequence K_i is $\varprojlim K_i/U_{K_i;\rho_i}$, where $U_{K;\rho}$ is the closed ball of radius ρ around 1 in K.

Example 3.2.6 ([5, pg 159-160]). Let k be a field of characteristic p. Let $K_0 = \mathrm{Frac}(\mathbf{W}(k))$.[1] Then the sequence $K_i = K_0(p^{1/i})$ converges to $k((t))$.

Definition 3.2.7 ([5, pg 161])**.** Let K_i be a sequence of local fields converging to a local field K. Let $H_i = K/(1+\mathfrak{m}_K^{\rho_i})$, where ρ_i is as in Definition 3.2.5. We say a sequence of elements $a_i \in K_i$ converges (either additively or multiplicatively) to an element $a \in K$, if the equivalence classes $\bar{a}_i \in H_i$ converge to a. A sequence $f_i \in K_i[t]$ converges to $f \in K[t]$ (additively or multiplicatively) if each coefficient of the f_i converges to the corresponding coefficient of f.

Remark 3.2.8 ([5, pg 161]). Let $f_i \in K_i[x_1, \dots, x_n]$ be a sequence of polynomials converging (additively) to a polynomial $f \in K[x_1, \dots, x_n]$. For each j between 1 and n, we let $a_{i,j} \in K_i$ be a sequence of elements converging to some $a_j \in K$. Then $f_i(a_{i,1}, \dots, a_{i,n})$ converges to $f(a_1, \dots, a_n)$. In particular if $g_i \in K_i[t]$ converges to $g \in K[t]$, then the discriminants of the g_i converge to that of g. In addition the constant terms of the g_i converge to that of g, and for large i, $\deg(g_i) = \deg(g)$.

[1] $\mathbf{W}$ denotes the ring of p-typical Witt vectors.

3.3 Extensions

Let K_i be a sequence of local fields converging to a local field K. Our goal is to relate extensions of K_i with those of K. The following theorem is used by Krasner to establish a residual isomorphism between these extensions.

Theorem 3.3.1 ([5, §9]). *Let K, K' be local fields of residue characteristic p, which are residually isomorphic of norm ρ. Let $H = K/(1+\mathfrak{m}_K^{-\frac{\log \rho}{\log p}})$ be the common quotient. Let $L = K(\alpha)$ be a finite separable extension. Let $f \in K[t]$ be the minimal polynomial of α. Let c_f and D_f be the constant term and discriminant of f respectively. Let $f' \in K'[t]$ be a polynomial whose coefficients reduce to the same element of H as the corresponding coefficients of f. Let α' be a root of f' and let $L' = K'(\alpha')$. If $\rho < |\frac{D_f^{n/2}}{c_f^{n(n-1)/2}}|$, then the given residual isomorphism extends to a residual isomorphism of norm $\rho|\frac{c_f^{n-1}}{D_f}|$ between L and L'.*

The following lemma, in conjunction with Krasner's lemma, is the main tool used by Krasner to show that the extensions he constructed are independent of any arbitrary choices.

Lemma 3.3.2 ([5, pg 161]). *Let f be a polynomial over a local field K. Let z be a zero of f, and let $r_f^{(z)}$ be the distance to the nearest other zero of f. Let $C_f^{(z)}$ be the circle around z of radius $r_f^{(z)}$. Then $C_f^{(z)} = \{\beta \in \bar{K} \mid |f(\beta)| < r_f^{(z)}|f'(z)|\}$. In particular, if $|f(\beta)| < r_f^{(z)}|f'(z)|$, then $K(z) \subseteq K(\beta)$.*

If f is irreducible, then $r_f^{(z)}$ is independent of z, and will henceforth be denoted

r_f.

Theorem 3.3.3 ([5, pg 187]). *Let K_i be a sequence of local fields converging to a local field K. Let $f_i \in K_i[t]$ be a sequence of polynomials which converges multiplicatively and canonically to a separable irreducible polynomial f. For each i we let α_i be a root of f_i. Then there exists a number N depending only on f such that for $i > N$, f_i is separable and irreducible. In addition, we can choose N so that $L_i = K_i(\alpha_i)$ is independent of arbitrary choices for $i > N$.*

In particular this allows us to canonically associate to each finite separable extension L/K an extension L_i/K_i for large i.

Corollary 3.3.4 ([5, pg 188]). *Let K_i be a sequence of local fields converging to a local field K. Let $f_i \in K_i[t]$ be a sequence of polynomials which converges multiplicatively to a separable irreducible polynomial f. Then for large i, the extension $K_i[x]/f_i$ of K_i is associated to $K[x]/f$ under the correspondence of Theorem 3.3.3.*

Proof. Let n be the degree of f. Let g_i be a sequence converging canonically to f. Let β_i be the root of g_i which minimizes $|f_i(\beta_i)|$. We wish to show that if i is large, f_i and g_i generate the same extension of K_i. Using lemma 3.3.2, it suffices to show that $|f_i(\beta_i)| \leq r_{f_i}|f_i'(\alpha_i)|$. To do this, it suffices to check $|R(f_i, g_i)| \leq (r_{f_i}|f_i'(\alpha_i)|)^n$, where R denotes the resultant. Applying 3.2.8 to the discriminant shows $|f_i'(\alpha_i)|$ is independent of i if i is large. Using the Newton polygon, Krasner has shown[2] that r_{f_i}

[2] [5, pg 187].

is independent of i if i is large. Thus we only need to bound $|R(f_i, g_i)|$ by a certain constant. But Remark 3.2.8 shows that $|R(f_i, g_i)| \to |R(f, f)| = 0$ as $i \to \infty$. $\square$

Theorem 3.3.5 ([5, pg 201])**.** *Let K_i be a sequence of local fields converging to K. Let L/K be a finite extension. Let L_i/K_i be the extensions induced by L/K under the correspondence of 3.3.3. Then L/K is Galois if and only if L_i/K_i is Galois for large i. In this case* $\mathrm{Gal}(L_i/K_i) \cong \mathrm{Gal}(L/K)$.

Chapter 4

Deligne's approach to limits of local fields

This chapter will describe a different approach to the results of 3, which is due to Deligne. In particular, this chapter will contain no original material except proposition 7.3.1. The most obvious difference between Krasner's approach and that of Deligne is that rather than associating to a local field K the valued hyperfields $K/(1+\mathfrak{m}_K^i)$, Deligne uses the triple $Tr_i(K)$ consisting of the ring $\mathcal{O}_K/\mathfrak{m}_K^i$, the module $\mathfrak{m}_K/\mathfrak{m}_K^{i+1}$ and the canonical map $\mathfrak{m}_K/\mathfrak{m}_K^{i+1} \to \mathcal{O}_K/\mathfrak{m}_K^i$. This difference is for the most part inconsequential, because this triple carries the same information as the valued hyperfield. However Deligne's definition of this triple only applies when the valuation is discrete, so Deligne's results hold in a slightly less general setting than Krasner's.

Suppose K is a limit of local fields K_i. The most significant difference between

Krasner's results and Deligne's results is that rather than merely showing that the Galois theory of K can be described in terms of all of the K_i, Deligne's theorem tells us how much of the Galois theory of K can be obtained from knowledge of a single one of the fields K_i.

More precisely, Deligne shows that G_K^v can be determined from $\mathrm{Tr}_u(K)$ for $u > v$. If $Tr_{u_i}(K) \equiv Tr_{u_i}(K_i)$ for some sequence u_i which tends to infinity, then this implies that the K_i determine G_K^v for all v, and so essentially determine the Galois theory of K.

On the other hand, rather than viewing Deligne's theorem as a result about limits of local fields, we may view it as a generalization of the fact that the unramified extensions of K can be described solely in terms of the residue field of K to a similar statement about extensions with ramification bounded by u for some fixed u.

4.1 Truncated DVRs

In this subsection, our goal is to develop an analogue of part of the theory of DVRs for the rings $\mathcal{O}_K/\mathfrak{m}_K^i$.

Definition 4.1.1 ([6, 1.1], [7, pg 3])**.** A truncated DVR[1] is a local Artinian ring with principal maximal ideal. If R is a truncated DVR and if $x \in R$, then we define $v_R(x) = \sup\{i \in \mathbb{N} \mid x \in \mathfrak{m}_R^i\}$, where $\mathfrak{m}_R$ is the maximal ideal. We will write

[1] The name truncated DVR comes from Example 4.1.2. In particular, the truncated power series ring $k[[t]]/(t^n)$ is a truncated DVR.

$l(R) = l_R(R)$ for the length of R as a module over itself.

For the remainder of this section, R will denote a truncated DVR, and π_R will be a generator of the maximal ideal.

Example 4.1.2. Let $\mathcal{O}$ be a DVR with maximal ideal $\mathfrak{m}$. Then $\mathcal{O}/\mathfrak{m}^k$ is a truncated DVR for any $k \in \mathbb{N}$ with $k \geq 1$. If L/K is a finite extension of local fields, then there is a finite flat local homomorphism $\mathcal{O}_K/\mathfrak{m}_K^k \to \mathcal{O}_L/\mathfrak{m}^{ke_{L/K}}$.

Remark 4.1.3. Let $x \in R$ have valuation $k < \infty$. Then $x = u\pi_R^k$ for some $u \in R \backslash \mathfrak{m}_R$. Hence x generates $\mathfrak{m}_R^k$. Using this, one can easily see that every ideal in R is a power of the maximal ideal. Hence $l(R)$ is the smallest nonnegative integer l such that $\mathfrak{m}_R^l = 0$.

As Example 4.1.2 suggests, much of the theory of DVRs has analogues for truncated DVRs. The following remarks are a first step in that direction.

Remark 4.1.4. Let R be a truncated DVR. Then it is easy to show that $v_R(x+y) \geq \min(v_R(x), v_R(y))$ for all $x, y \in R$. In addition, $v(xy) = v(x) + v(y)$ unless $xy = 0$. Using Nakayama's lemma, it is easy to see that $v_R(x) = \infty$ if and only if $x = 0$.

Definition 4.1.5. If $\phi : R \to A$ is a finite homomorphism of truncated DVRs, we define the ramification index to be $e_{A/R} = v_A(\phi(\pi_R))$ if $\pi_R \neq 0$ and $e_{A/R} = l(A)$ if $\phi(\pi_R) = 0$. We define $f_{A/R}$ to be the degree of the extension of residue fields.[2] We say A/R is unramified if $e_{A/R} = 1$ and totally ramified if $f_{A/R} = 1$.

[2]Note that finite homomorphisms of local rings are always local homomorphisms.

Remark 4.1.6. It is straightforward to show that if ϕ is flat (or just injective), then $v_A(x) = v_R(x)e_{A/R}$ for all $x \in R$. In general we still have $\mathfrak{m}_R A = \mathfrak{m}_A^{e_{A/R}}$.

As in the case of extensions of DVRs, the residue class degree and ramification index are related to the degree of an extension.

Lemma 4.1.7. *Let $\phi : R \to A$ be a finite flat homomorphism of truncated DVRs. Then A is a free R-module of rank $e_{A/R}f_{A/R}$.*

Proof. First we will treat the case where $\phi(\pi_R) \neq 0$. By A.1.3 of,[3] $l_R(A) = l_A(A)f_{A/R}$. By A.4.1 of,[3] $l_A(A) = l_R(R)l_A(A/\mathfrak{m}_R A) = l_R(R)l_A(A/\mathfrak{m}_A^{e_{A/R}}) = l_R(R)e_{A/R}$. Then $l_R(A) = l_R(R)(e_{A/R}f_{A/R})$, from which the result follows easily. In the case where $\phi(\pi_R) = 0$, we still have $l_R(A) = l_A(A)f_{A/R} = e_{A/R}f_{A/R}$ by the definition of $e_{A/R}$. □

The following lemma gives a useful criterion for flatness.

Lemma 4.1.8. *Suppose $\phi : R \to A$ is a finite homomorphism of truncated DVRs. Then ϕ is flat if and only if $l(A) = l(R)e_{A/R}$.*

Proof. Suppose ϕ is flat. By the proof of Lemma 4.1.7, $l(A) = l(R)e_{A/R}$.

Conversely, suppose $l_A(A) = l_R(R)e_{A/R}$. Then by Lemma A.1.4 of[3] we find that $l_{R/\mathfrak{m}_R}(A/\mathfrak{m}_R A) = l_R(A/\mathfrak{m}_R A) = l_A(A/\mathfrak{m}_R A)f_{A/R} = f_{A/R}e_{A/R}$. Thus the dimension of $A/\mathfrak{m}_R A$ as a vector space over $R/\mathfrak{m}_R$ is $f_{A/R}e_{A/R}$, so by Nakayama's lemma, A is a quotient of a free module F with $f_{A/R}e_{A/R}$ generators. Similarly, as in the proof of lemma 4.1.7, $l_R(A) = l_R(R)f_{A/R}e_{A/R} = l_R(F)$. Thus the kernel of the map $F \to A$ has length 0, so $A = F$ is free. □

Remark 4.1.9 ([6, pg 129]). Let R, A, and B be truncated DVRs with residue fields k_R, k_A, and k_B. Note that truncated DVRs are Henselian. By the proof of proposition I.4.4 in,[8] if $R \to A$ and $R \to B$ are finite étale, then $\mathrm{Hom}_R(A, B) = \mathrm{Hom}_{k_R}(k_A, k_B)$. By the same proposition we know that if $f : R \to A$ is any finite homomorphism, then there is a unique finite étale extension R_0 of R such that $k_{R_0} = k_A$. Then identifying these 2 residue fields gives a totally ramified map $A_0 \to A$ of R-algebras. Hence every finite morphism of truncated DVRs factors into a finite étale morphism and a finite totally ramified morphism.

Remark 4.1.10. We say a monic polynomial $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ over a truncated DVR is Eisenstein if $v(a_0) = 1$ and $v(a_i) \geq 1$ for all i. One can show, as in the case of DVRs, that if $f : R \to A$ is a finite flat totally ramified homomorphism, then $A \cong R[x]/P(x)$, where P is Eisenstein.

Proposition 4.1.11 ([7, 1.3]). *Let K be a local field, and $A = \mathcal{O}_K/\mathfrak{m}_K^u$. Let $f : A \to B$ be a finite flat homomorphism of truncated DVRs. Then there is a separable field extension L such that $B \cong \mathcal{O}_L/\mathfrak{m}_L^{eu}$ as A-algebras for some e.*

Proof. Suppose f factors as the composition of two finite flat morphisms $A \to C \to B$ of truncated DVRs. It is easy to see that it suffices to prove the result for $A \to C$ and $C \to B$. Thus without loss of generality, we may assume f is either étale or totally ramified, and that A is generated as an R algebra by a single element. Then $A \cong R[x]/P(x)$ for some $P(x)$. Let $\hat{P}(x) \in \mathcal{O}_K$ be a lift of P which is separable.[3] Then $\hat{P}$ is

[3] This can always be arranged by requiring the coefficient of the x term to be nonzero.

irreducible modulo $\mathfrak{m}_K$, so is irreducible by Hensel's lemma. Then $\mathcal{O}_L := \mathcal{O}_K[x]/\hat{P}(x)$ is a DVR. In the totally ramified case, $P(x)$ is Eisenstein, so we can pick $\hat{P}(x)$ to be Eisenstein, so L/K is totally ramified of degree $deg(P) = e$. Then $\mathcal{O}_L/\mathfrak{m}_L^{eu} = \mathcal{O}_K[x]/(\mathfrak{m}_K^u\mathcal{O}_K[x] + \hat{P}(x)\mathcal{O}_K[x]) = (\mathcal{O}_K/\mathfrak{m}_K^u)/P(x)$, as desired. The unramified case is similar. □

4.2 Triples

Definition 4.2.1 ([6, pg 126])**.** A triple (R, M, ϵ) consists of a truncated DVR R with perfect residue field, a free R-module M of rank 1, and a homomorphism $\epsilon : M \to R$ whose image is $\mathfrak{m}_R$. We define a integer valued function on $M^{\otimes i}$ by $v(am^{\otimes i}) = i + v_R(a)$ for $a \in R$, where m is a generator of M.

Example 4.2.2 ([6, 1.2]). Let $\mathcal{O}$ be a DVR with perfect residue field, and with maximal ideal $\mathfrak{m}$. Then for $u \in \mathbb{N}$ there is a triple $(\mathcal{O}/\mathfrak{m}^u, \mathfrak{m}/\mathfrak{m}^{u+1}, \epsilon)$, where ϵ is induced by the inclusion $\mathfrak{m} \subseteq \mathcal{O}$. If $\mathcal{O}$ is the ring of integers of a local field K, we will denote this triple $\mathrm{Tr}_u(K)$.

For $s > r$, we can define a map $\epsilon_{r,s} : M^{\otimes s} \to M^{\otimes r}$ by $\epsilon_{r,s}(x^{\otimes s}) = \epsilon(x)^{s-r}x^{\otimes r}$, where x is a generator of M.

Definition 4.2.3 ([6, 1.4])**.** A morphism of triples $(r, f, \eta) : (R, M, \epsilon) \to (R', M', \epsilon')$ consists of a homomorphism $f : R \to R'$, an integer r (called the ramification index) and an R-linear map $\eta : M \to M'^{\otimes r}$, such that $f\epsilon = \epsilon'_{0,r}\eta$ and such that $M \otimes R' \to$

$M'^{\otimes r}$ is an isomorphism. The morphism is called flat if $l(R') = l(R)r$.[4] It is finite or totally ramified if $R \to R'$ is. It is étale if it is finite, flat, and has r=1. We compose morphisms of triples by the formula $(r, f, \eta)(s, g, \theta) = (rs, fg, \eta^{\otimes s}\theta)$.

Example 4.2.4 ([6, 1.4.1]). If L/K is a finite extension of local fields with ramification index r, then $\mathcal{O}_K \to \mathcal{O}_L$ induces a finite flat morphism $\mathrm{Tr}_u(K) \to \mathrm{Tr}_{ru}(L)$.

Remark 4.2.5 ([6, pg 126]). If (R, M, ϵ) and (R', M', ϵ') are triples, then any isomorphism $R \to R'$ lifts uniquely to a isomorphism of triples.

Remark 4.2.6. Let $(r, f, \eta) : (R, M, \epsilon) \to (R', M', \epsilon')$ be a morphism such that $f(\pi_R) \neq 0$. It is easy to see that $r = e_{R'/R}$.

Proposition 4.2.7. *Let $S = (R, M, \epsilon)$ and $S' = (R', M', \epsilon')$. A morphism $(r, \phi, \eta) : S \to S'$ can be factored uniquely as $S \to S'' \to S'$ where $S \to S''$ is étale and $S'' \to S'$ is totally ramified*

Proof. By 4.1.9, there is a unique étale R-algebra R'' such that $R \to R'$ factors as a composite of an étale morphism $\theta_1 : R \to R''$ and a totally ramified morphism of truncated DVRs $\theta_2 : R'' \to R'$. Let $M'' = R'' \otimes_R M$, and let $\epsilon'' = \mathrm{id}''_R \otimes \epsilon$. It is easy to verify that $S'' = (R'', M'', \epsilon'')$ is a triple, and that the canonical maps $\theta_1 : R \to R''$ and $\eta_1 = \mathrm{id} \otimes \theta_1 : M \to M \otimes_R R'' = M''$ give an unramified morphism $(1, \theta_1, \eta_1)$ of triples. If R is a field, then R and R'' both have length 1 so the morphism is flat. Otherwise $\theta_1(\pi_R) \neq 0$. Then we can show $(1, \theta_1, \eta_1)$ is flat by noticing that θ_1 is flat and applying

[4] c.f. lemma 4.1.8

4.2.6 and 4.1.8. The map θ_2 gives an action of R'' on M' so allows us to lift η to a map $\eta_2 : M'' = M \otimes_R R'' \to M'^{\otimes r}$. Under the identification $M'; \otimes_{R''} R' = M \otimes_R R'$, the map $M'' \otimes_{R''} R' \to M'^{\otimes r}$ induced by η_2 is the isomorphism induced by η. To check that (r, θ_2, η_2) is a morphism of triples it now remains to show that $\theta_2 \epsilon'' = \epsilon'_{0,r}\eta$. This follows easily from the corresponding formula for (r, ϕ, η). This morphism is totally ramified since θ_2 is. The uniqueness of the decomposition is straightforward to verify. □

The following result is an analogue of Proposition 4.1.11 for triples.

Lemma 4.2.8 ([6, 1.4.4]). *Let K be a local field. Let $\mathrm{Tr}_e(K) \to S$, be a finite flat morphism of ramification index r. Then there is a finite separable extension L/K with ramification index r such that $S \cong \mathrm{Tr}_{re}(L)$ as objects in the coslice category*[5] *of* $\mathrm{Tr}_e(K)$.

4.3 The Newton polygon

The key to Deligne's proof is showing that one may recover a lot of information about the ramification filtration of an extension L/K from the corresponding morphism of triples. To do this we first show that in the case of a totally ramified extension, one may recover the sizes of the ramification groups from the Newton poly-

[5] Recall that if $\mathcal{C}$ is a category and $X \in \mathcal{C}$, then the objects of the coslice category of X are pairs (Y, ϕ_Y) with $Y \in \mathcal{C}$ and $\phi_Y : X \to Y$. A morphism $(Y, \phi_Y) \to (Z, \phi_Z)$ is a morphism $Y \to Z$ such that the obvious triangle commutes.

gon of a minimal polynomial of the uniformizer of L/K. We will then show that if a certain bound on ramification is satisfied, then this Newton polygon is determined by the morphism $\mathrm{Tr}_u(K) \to \mathrm{Tr}_{eu}(L)$.

Let L/K be a finite totally ramified separable extension of local fields. We will fix an embedding $L \subseteq \bar{K}$, where $\bar{K}$ is the separable closure. Then $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$, where π_L is a root of an Eisenstein polynomial $f(x) \in K[x]$. We will let $P_{L/K}(x) = \frac{f(x+\pi_L)}{x}$.

Definition 4.3.1. Given a finite collection of points $(x_i, y_i) \in \mathbb{R}^2$, the lower convex hull of the family $\{(x_i, y_i)\}$ is the supremum of all piecewise linear convex functions $\theta(t)$ such that $y_i \geq \theta(x_i)$ for all i. The Newton polygon associated to a monic polynomial $g(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0$ with coefficients in either a DVR or a truncated DVR is defined to be the lower convex hull of the points $(i, v(a_i))$ for $0 \leq i \leq n-1$.[6] For future convenience, we will extend the definition to a function on $[-1, n-1]$ by linearity.

We will need the following standard result about the Newton polygon.

Theorem 4.3.2. *Suppose g is a polynomial over a DVR. Each segment of the Newton polygon has slope equal to $-v(\rho)$ for some root ρ of g. Furthermore, the length of the projection of this segment onto the x-axis is the number of roots with valuation $v(\rho)$.*

We will let $y = n_L(x)$ be the Newton polygon of $P_{L/K}$ (with respect to the valuation v_L). We will let (d_i, f_i) be the ith vertex (so $d_1 < \ldots < d_r$, where r is

[6] Note that I am indexing the coefficients of the polynomial in the order opposite to that used by Deligne.

the number of vertices). We will let $s_i = \frac{f_i - f_{i+1}}{d_{i+1} - d_i}$.

Remark 4.3.3 ([7, pg 5]). For an embedding $\sigma : L \to \bar{K}$ which is not the standard inclusion, we will let $i_{L/K}(\sigma) = \inf_{x \in \mathcal{O}_L} v_L(\sigma x - x)$. When L/K is totally ramifed, $i_{L/K}(\sigma) = v_L(\sigma\pi_L - \pi_L)$ is the valuation of the root of $P_{L/K}$ corresponding to σ. Then the number of $\sigma \neq 1$ such that $i_{L/K}(\sigma) = s_i$ is $d_{i+1} - d_i$. If L/K is Galois, then because $\mathrm{Gal}(L/K)_i = \{\sigma \in \mathrm{Gal}(L/K) \mid i_{L/K}(\sigma) \geq i+1\}$, this determines the order of each $\mathrm{Gal}(L/K)_i$. In fact, in this case, $|\mathrm{Gal}(L/K)_i| - 1$ is the greatest integer g such that the Newton polygon has slope less than $-i-1$ on $(g, n-1]$. Since this Newton polygon can be described in terms of the ramification filtration it is independent of the choice of π_L.

Let $u \geq 0$. Let $e = e_{L/K}$. Let $S = (R, M, \epsilon) = \mathrm{Tr}_u(K)$ and $S' = (R', M', \epsilon') = \mathrm{Tr}_{eu}(L)$. Let $(e, \theta, \eta/)$ be the standard morphism between them. We will now define the Eisenstein polynomial of S'/S.

It is easy to verify that because R' is flat and totally ramified over R, R' is a free R-module with basis $1, \pi_{R'}, \ldots, \pi_{R'}^{e-1}$, where $\pi_{R'}$ is any generator of the maximal ideal, in particular when $\pi_R = \epsilon(\omega)$ where ω is a generator of M'. Then $x^{\otimes r}$ is in the image of the isomorphism $\eta : M \otimes_R R' \to M^{\otimes r}$. Hence we can write $\omega^{\otimes r} = \eta(\sum_{i=0}^{r-1} -c_i \epsilon(\omega)^i)$ with $c_i \in M$. It is easy to see that c_0 generates M. It is clear that if π_L is an element of $\mathfrak{m}_L$ lying over ω then the c_i are the reduction mod $\mathfrak{m}_K^{u+1}$ of the coefficients of the minimal polynomial of π_L over K.

At the beginning of this section, instead of taking the Newton polygon of the

Eisenstein polynomial $f(x)$ we used $f(x+\pi_L)/x$. The analogue of the coefficients of $f(x+\pi_L)$ are the elements $b_i \in M'^{\otimes(r-i)}$ defined by the following equation.

$$b_i = \binom{r}{i}\omega^x + \sum_{j\geq i}\binom{j}{j-i}\epsilon_{r-i,r}\eta(a_j)\epsilon(\omega)^{j-i}.$$

An easy argument using the binomial theorem and the fact that the elements a_i are reductions of the coefficients of $f(x)$ shows that the b_i are reductions of the coefficients of $f(x+\pi_L)$. Hence b_{i+1} is the reduction of the ith coefficient of $P_{L/K}$. This motivates the following definition.

Definition 4.3.4. Let $S \to S' = (R', M', \epsilon')$ be a flat totally ramified morphism of triples, and let b_i be defined in terms of a generator ω of M' as described above. Then we let $n_{S'}$ be the lower convex hull of the points (i, b_{i+1}) for $i \geq 0$. For convenience, we will extend $n_{S'}$ to a function on $[-1, 0]$ by declaring that it is linear on this interval and has the same slope as on $[0, 1)$.

The point of the Newton polygon we just defined is that $n_{\mathrm{Tr}_{eu}(L)}$ will hopefully determine n_L and hence the sizes of the lower ramification subgroups associated to L/K.

Proposition 4.3.5 ([6, 1.5.2]). *Suppose we are in the situation of Definition 4.3.4, and that we have a totally ramified separable extension L/K of degree e such that $S = \mathrm{Tr}_u(K)$, $S' = \mathrm{Tr}_{eu}(L)$, and such that $S \to S'$ is the morphism obtained from L/K. The following are equivalent:*

(a) The Galois closure L'/K of L/K satisfies $\mathrm{Gal}(L'/K)^e = 1$.

(b) $n_L = n_{S'}$.

(c) $n_L(-1) < e(u+1)$*, where* r *is the ramification index of the canonical morphism* $S \to T$*.*

(d) $n_{S'}(-1) < \infty$*.*

Proof. The fact that (a) and (c) are equivalent is essentially [6, A.6.2]. In the case where L/K is Galois on can prove it by using 4.3.3 to see that the numbers $|\mathrm{Gal}(L/K)_i|$ are determined by n_L and hence so are the orders of the group $\mathrm{Gal}(L/K)^e$. A bit of computation will show that (c) is the inequality obtained in this way from the equation $|\mathrm{Gal}(L/K)^e| = 1$.

To relate (b), (c), and (d), we let ω generate M', and let b_i be given by Equation 4.3. Let $\pi_L \in \mathfrak{m}_L$ be a lift of ω and let $\tilde{b_i}$ be the coefficients of $P_{L/K}$. We noted that the b_i are reductions of the $\tilde{b_i}$. Hence $v(b_i) = v(\tilde{b_i})$ if $v(\tilde{b_i}) < eu + e - i$ and $v(b_i) = \infty$ otherwise. Since we always have $v(\tilde{b_i}) \leq v(b_i)$, it follows that $n_L \leq n_{S'}$.

Assume (c) holds. Proving (b) then amounts to showing that if $(i, v(\tilde{b_{i+1}}))$ is a vertex of the Newton polygon $y = n_L(x)$, then it is also a vertex of $y = n_{S'}(x)$. If we assume (c), then using the fact that each segment has an integer slope, we get that $n_L(x) < e(u+1) - (x+1)$, so each $(i, \tilde{b_{i+1}})$ that occurs as a vertex of the Newton polygon satisfies $v(\tilde{b_{i+1}}) < eu + e - i - 1$, and hence $v(b_{i+1}) = v(\tilde{b_{i+1}})$ holds for such i. This implies (b).

Assume now that (d) holds. Then $n_{S'}(x) \leq \infty$ for all x. Hence each for each vertex $(i, v(b_{i+1}))$ we have $v(\tilde{b_{i+1}}) < \infty$ so $v(b_i) = v(\tilde{b_{i+1}})$. If n is the lower convex hull of $(i, v(\tilde{b_{i+1}}))$ for i satisfying $v(\tilde{b_{i+1}}) < \infty$, we have $n = n_{S'}$. On the other hand for all other i we have $v(\tilde{b_{i+1}}) = \infty$ so $v(b_{i+1}) \geq eu + e - i - 1 \geq n$. Hence $n_L \geq n = n_{S'}$ by the definition of the lower convex hull in terms of a supremum, and we have already seen $n_{S'} \geq n_L$. Hence (b) holds, and therefore (c) does as well. □

Corollary 4.3.6 ([6, 1.5.1]). *We retain the notation of 4.3.5. Suppose* $0 \leq f < u$. *Then the Galois closure* L'/K *of* L/K *satisfies* $\mathrm{Gal}(L'/K)^f = 1$ *if and only if* $n_T(-1) < r(f+1)$.

Remark 4.3.7. Let $S \to X$ be a finite flat totally ramified morphism of triples. Let g_i be the greatest integer such that the Newton polygon n_X has slope less than $-i-1$ on $(g_i, n-1]$. By 4.3.3, it follows that if $S \to X$ comes from a field extension satisfying the ramification bound appearing in reftripnp, then $g_i + 1$ is the order of $\mathrm{Gal}(L/K)$. We define $\phi_{X/S}(x) = \int_0^x \frac{g_t + 1}{g_0 + 1} dt$. When X/S is not totally ramified, we define $\phi_{X/S} = \phi_{X/S_0}$, where $S \to S_0 \to X$ is the factorization from 4.2.7. If X/S is $\mathrm{Tr}_{eu}(L)/\mathrm{Tr}_u(K)$ and L/K has ramification bounded by u, then $\phi_{X/S} = \phi_{L/K}$.

Definition 4.3.8. Let $S \to X$ be a finite flat morphism of triples. We let $\psi_{X/S}$ be the inverse function to the function $\phi_{X/S}$ of 4.3.7

4.4 Deligne's theorem

Embeddings of fields will correspond not to morphisms of triples, but to equivalence classes of morphisms. Let $f \geq 0$. Let X', X'' be finite flat objects of the coslice category of a triple S, with $X' = (A', I', \epsilon)$. Given two morphisms $\theta_i = (s, \phi_i, \eta_i)$; $i = 1, 2$, we say $\theta_1 \equiv \theta_2 \bmod R(f)$ if $v(\eta_1(x) - \eta_2(x)) \geq s(f+1)$ for all $x \in I'$.

Lemma 4.4.1 ([6, 2.3.1]). *Let F be a local field. Suppose $S = \mathrm{Tr}_e(F)$, and X', X'' are the extensions of S corresponding to finite separable extensions E', E'' of F. If the Galois closure K of E' satisfies $\mathrm{Gal}(K/F)^e = 1$, then the canonical map $\mathrm{Hom}_F(E', E'') \to \mathrm{Hom}_S(X', X'')/R(\psi_{X'/S}(e))$ is a bijection.*

Lemma 4.4.2 ([6, 2.4,2.5]). *(i) Let X', X'', X''' be finite flat objects of the coslice category of a triple S. Let $u_1, u_2 : X'' \to X'''$ and $v : X' \to X''$ be morphisms in this category. If $u_1 \equiv u_2$ mod $R(f)$, then $vu_1 \equiv vu_2$ mod $R(f)$.*

(ii) Let X', X'', X''' be finite and flat over a triple S. If $u_1, u_2 : X'' \to X'''$ are congruent mod $R(f)$ and $v : X' \to X''$, then $u_1 v \equiv u_2 v$ mod $R(\psi_{X'/S}(f))$.

We are now ready to state the main result of this section.

Definition 4.4.3. Let S be a triple. We define $\mathcal{C}_S^f$ to be the category whose objects are triples X equipped with a finite flat morphism $S \to X$ such that $n_X(-1) < r(f+1)$[7], and whose morphisms $X' \to X''$ are equivalence classes of morphisms $X' \to X''$ in the coslice category of S modulo the relation $R(\psi_{X'/S}(f))$.

Theorem 4.4.4 ([6, 2.8]). *Let F be a local field. Let $S = \mathrm{Tr}_e(F)$. Let $\mathcal{C}_F^f$ be the category defined in 2.0.21. Then $\mathcal{C}_F^f$ and $\mathcal{C}_S^f$ are equivalent when $f \leq e$.*

Proof. $\mathcal{C}_S^f$ is a category by lemma 4.4.2. The functor is fully faithful by lemma 4.4.1. It is essentially surjective by Corollary 4.3.6 and propositon 4.3.5. ∎

[7] see cor 4.3.6.

One can use this result to develop a notion of the a limit of local fields, analogously to Krasner's definition. Let K_i be a sequence of local fields, and u_i an increasing sequence of natural numbers. Suppose that K is a local field such that $\mathrm{Tr}_{u_i}(K) \cong \mathrm{Tr}_{u_i}(K_i)$ for all i. Then if L/K is a finite separable extension, one can construct an extension L_i/K_i for large i, which carries the same Galois-theoretic data as L/K. This is because one has $\mathcal{C}_K^{u_i} \cong \mathcal{C}^{u_i}_{\mathrm{Tr}_{u_i}(K)} \cong \mathcal{C}^{u_i}_{\mathrm{Tr}_{u_i}(K_i)} \cong \mathcal{C}^{u_i}_{K_i}$, and because L is an object of $\mathcal{C}_K^{u_i}$ for large i. If K is the limit of a sequence K_i in the sense just defined, then $\mathcal{O}_K \cong \varprojlim \mathcal{O}_K/\mathfrak{m}_K^{u_i} \cong \varprojlim \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{u_i}$, so $K \cong \mathrm{Frac}(\varprojlim \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{u_i})$. The following converse also holds.

Proposition 4.4.5. *Let u_i be an increasing sequence of integers. Let K_i be a sequence of local fields. Suppose that for each i, we are given a surjective homomorphism $\theta_i : \mathcal{O}_{K_{i+1}}/\mathfrak{m}_{K_{i+1}}^{u_{i+1}} \to \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{u_i}$. Let $K = \mathrm{Frac}(\varprojlim \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{u_i})$. Then K is a local field, and $\mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{u_i} \cong \mathcal{O}_K/\mathfrak{m}_K^{u_i}$ for all i. Furthermore $\mathrm{Tr}_{u_i}(K) \cong \mathrm{Tr}_{u_i}(K_i)$.*

Proof. Let $\mathcal{O}_K = \varprojlim \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{u_i}$. For the first part of the proposition, it suffices to show $\mathcal{O}_K$ is a complete DVR. It is clearly a ring. Let v_i be the valuation on the truncated DVR $\mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{u_i}$. For $\alpha \in \mathcal{O}_K$, let α_i be its component in $\mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{u_i}$. I claim that $v_i(\alpha_i) = v_{i+1}(\alpha_{i+1})$ for large i. Write $\alpha_i = u_i \pi_i^{v_i(\alpha_i)}$, where π_i is a uniformizer of $\mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{u_i}$. Then $\theta_i(\alpha_{i+1}) = \theta_i(u_{i+1})\theta_i(\pi_{i+1})^{v_{i+1}(\alpha_{i+1})}$. Since θ_i is a surjective homomorphism of local rings, $\theta_i(u_{i+1})$ is a unit and $\theta_i(\pi_{i+1})$ is a uniformizer. In particular, if $\alpha_i = \theta_i(\alpha_{i+1})$ is nonzero, then $v_i(\alpha_i) = v_{i+1}(\alpha_{i+1})$. If $\alpha \neq 0$, then this proves the claim. If $\alpha = 0$, then the claim is trivial.

We define $v(\alpha)$ to be the limiting value of $v_i(\alpha_i)$. If $\alpha, \beta \in \mathcal{O}_K$, then according to 4.1.4, $v_i(\alpha_i\beta_i) = v_i(\alpha_i) + v_i(\beta_i)$, as long as $v_i(\alpha_i) + v_i(\beta_i) < u_i$. Taking the limit shows that $v(\alpha\beta) = v(\alpha) + v(\beta)$ when $v(\alpha) + v(\beta) < \infty$. The other properties of a discrete valuation are proven similarly. Let $\{\alpha^{(k)}\}$ denote a Cauchy sequence in $\mathcal{O}_K$. Let N be a natural number. Then $v(\alpha^{(k)} - \alpha^{(l)}) > N$ for large k and l. Thus $v_i(\alpha_i^{(k)} - \alpha_i^{(l)}) > N$ when i, k, and l are large. Since $\mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{u_i}$ is complete, $\lim\limits_{k\to\infty} \alpha_i^{(k)}$ exists, and will be denoted α_i. Since θ_i is continuous, $\theta_i(\alpha_{i+1}) = \theta_i(\alpha_i)$, so the α_i define an element $\alpha \in \mathcal{O}_K$. It is easy to see this is the limit of the given Cauchy sequence, and so $\mathcal{O}_K$ is a complete DVR.

Let $n \in \mathbb{N}$. It is easy to see that $\mathfrak{m}_K^n = \varprojlim \mathfrak{m}_{K_i}^{\min(u_i,n)}/\mathfrak{m}_{K_i}^{u_i}$. I claim that $\varprojlim^1 \mathfrak{m}_{K_i}^{\min(u_i,n)}/\mathfrak{m}_{K_i}^{u_i} = 0$. Without loss of generality, I will assume $u_i > n$ for all i. Let $\theta_{i,j} : \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{u_i} \to \mathcal{O}_{K_j}/\mathfrak{m}_{K_j}^{u_j}$ for $i > j$ be the maps induced by the sequence $\{\theta_k\}$. By the Mittag-Leffler condition, the claim reduces to showing that for all k, there exists $j \geq k$ such that for $i \geq j$, $\theta_{i,k}(\mathfrak{m}_{K_i}^n/\mathfrak{m}_{K_i}^{u_i}) = \theta_{j,k}(\mathfrak{m}_{K_j}^n/\mathfrak{m}_{K_j}^{u_j})$. But both are generated by the image of $\pi_{K_k}^n$, so the claim holds. Then by the long exact sequence, $\mathcal{O}_K/\mathfrak{m}_K^n \cong \varprojlim \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{\min(u_i,n)}$.

If $n = u_j$, it is easy to see that all but finitely many terms in this limit are isomorphic (under the maps induced by the θ_i) to $\mathcal{O}_{K_j}/\mathfrak{m}_{K_j}^{u_j}$. Hence $\mathcal{O}_{K_j}/\mathfrak{m}_{K_j}^{u_j} \cong \mathcal{O}_K/\mathfrak{m}_K^{u_j}$. The final statement follows from Remark 4.2.5. □

Lemma 4.4.6. *Let $f : S \to S'$ be an isomorphism of triples. Let $f \in \mathbb{R}$. Pullback along f gives an equivalence of categories $\mathcal{C}_S^f \to \mathcal{C}_{S'}^f$.*

Proof. It is trivial to show that pullback along f^{-1} is the inverse up to natural isomorphism □

Chapter 5

The equivalence between triples and valued hyperfields

Deligne comments without elaboration in[6] that his triples are essentially the same as Krasner's valued hyperfields. However, to the author's knowledge, a precise statement of their relation cannot be found in the literature. The categories of triples and of valued hyperfields are not equivalent for a trivial reason: If one rescales the absolute value on a local field by replacing it with the map $x \to |x|^c$ for some constant c, then this changes the valued hyperfields, but not the triples that occur as quotients. However aside from this minor issue, the categories agree. In particular we shall show that their coslice categories are equivalent.

5.1 Basic Definitions

Definition 5.1.1. A valued hyperfield H is discrete if the image of $H - \{0\}$ under the absolute value is discrete. A uniformizer of H is an element with maximal absolute value among all elements whose absolute value is less than 1.

Definition 5.1.2. Let H be a valued hyperfield. A valued subhyperfield is a subset $H' \subseteq H$ containing 0 and -1 and an element whose absolute value is not 0 or 1, and which is closed under multiplication and inversion and satisfies $(x + y) \cap H' \neq \emptyset$ for all $x, y \in H'$.

Proposition 5.1.3. *Let H be a valued hyperfield, and H' a valued subhyperfield. Then H' is a valued hyperfield with the same multiplication and absolute value and the addition is given by $x +_{H'} y = (x +_H y) \cap H'$. The inclusion $H' \to H$ is a morphism.*

Proof. Clearly the metric on H' is the subspace metric. All of the valued hyperfield axioms are clear except associativity of addition. We will use $+$ to denote addition in H. Let $x, y, z \in H'$. Let $w \in (x +_{H'} y) +_{H'} z = (((x + y) \cap H') + z) \cap H'$. Since $w \in x + y + z$, $(y + z) \cap (w - x) \neq \emptyset$. Since $y + z$ and $w - x$ are non-disjoint balls, one of them is contained in the other. Then $(w - x) \cap (y + z) \cap H'$ is either $(w - x) \cap H'$ or $(y + z) \cap H'$, so it is nonempty. Let $a \in H' \cap (w - x) \cap (y + z)$. Then $w \in (x + a) \cap H' \subseteq (x + ((y + z) \cap H')) \cap H'$. The reverse inclusion is similar. Clearly the inclusion map is a morphism of valued hyperfields.

□

5.2 Construction of the triple $\mathrm{Tr}(H)$

Let H be a discretely valued hyperfield, which is not a field. Let ρ be it's norm. Let θ be the absolute value of a uniformizer. We will write $\mathcal{O}_H$ for the closed unit ball. $\mathfrak{m}_H^i$ will denote the closed ball of radius θ^i around 0. For $x, y \in H$ we write $x \equiv_\eta y$ when $d(x,y) \leq \eta$. Define $M_i = \mathfrak{m}_H^i / \equiv_{\rho\theta^i}$. For $x \in H$, we define $v(x) = \frac{\log |x|}{\log \theta}$.

Lemma 5.2.1. *M_i is an abelian group for all $i \in \mathbb{Z}$. M_0 is a commutative ring, and each M_i is a module over M_0.*

Proof. Let $x, y \in M_i$. Let $\hat{x}, \hat{y} \in \mathfrak{m}_H^i$ be lifts. Let $\hat{z} \in \hat{x} + \hat{y}$. Then $x + y \in M_i$ is defined to be it's equivalence class. To show this is well-defined, let $\hat{x}', \hat{y}' \in \mathfrak{m}_H^i$ be another choice of lifts. Then $|\hat{x} - \hat{x}'| \leq \rho\theta^i$ unless $0 \in \hat{x} - \hat{x}'$. On the other hand, if $0 \in \hat{x} - \hat{x'}$, then $\hat{x} - \hat{x}'$ is a ball around 0 of radius $\rho \max(\hat{x}, \hat{x}') \leq \rho\theta^i$. Thus we have $|\hat{x} - \hat{x}'| \leq \rho\theta^i$ in both cases, and similarly, $|\hat{y} - \hat{y}'| \leq \rho\theta^i$. Let $\hat{z}' \in \hat{x}' + \hat{y}'$. Then $\hat{z} - \hat{z}' \in (\hat{x} - \hat{x}') + (\hat{y} - \hat{y}')$, so $|\hat{z} - \hat{z}'| \leq \max(|\hat{x} - \hat{x}'|, |\hat{y} - \hat{y}'|) \leq \rho\theta^i$. Thus $\hat{z}$ and $\hat{z}'$ define the same element of M_i. Each of the abelian group axioms follows easily by using the corresponding facts in $\mathfrak{m}_H^i$.

We now define a bilinear multiplication map $M_i \times M_j \to M_{i+j}$. Let $x \in M_i$ and $y \in M_j$. Let $\hat{x} \in \mathfrak{m}_H^i$ and $\hat{y} \in \mathfrak{m}_H^j$ be lifts. We define $xy \in M_{i+j}$ to be the class of $\hat{x}\hat{y}$. Let $\hat{x}'$ be a different lift. Then $d(\hat{x}\hat{y}, \hat{x}'\hat{y}) = |(\hat{x} - \hat{x'})\hat{y}| = |\hat{x} - \hat{x'}||\hat{y}| \leq \rho\theta^i\theta^j$ since $\hat{y} \leq \theta^j$. Thus xy is independent of $\hat{x}$ and similarly, it is independent of $\hat{y}$. Bilinearity follows from the distributive law in H. It is easy to check, using the associativity of H, that the multiplication $M_0 \times M_0 \to M_0$ makes M_0 into a ring, and that $M_0 \times M_i \to M_i$ makes M_i into a module.

□

Henceforth we will denote M_0 by R and M_1 by M.

Lemma 5.2.2. *R is a truncated DVR. Its length is $\frac{\log \rho}{\log \theta}$.*

Proof. For $x \in R$, let $\hat{x} \in \mathcal{O}_H$ be a lift. Define $v(x) = v(\hat{x})$ if $x \neq 0$ and $v(0) = \infty$. To see this is well-defined, suppose $x \neq 0$, and let $\hat{x}'$ be another lift. Then $|\hat{x}' - \hat{x}| \leq \rho$, but $|\hat{x}| > \rho$. By the ultrametric inequality, $|\hat{x}| = |\hat{x'}|$, so $v(x)$ is well-defined.

For $x, y \in R$ such that $xy \neq 0$, $v(xy) = v(x) + v(y)$, as may be seen by picking lifts of x and y. In addition, $v(x + y) \geq \min(v(x), v(y))$. Suppose that $x, y \in R$ are such that $v(x) \leq v(y)$. Suppose $x, y \neq 0$. Pick lifts $\hat{x}, \hat{y} \in \mathcal{O}_H$. Then $v(\hat{x}) \leq v(\hat{y})$, so there is a $\hat{z} \in \mathcal{O}_H$ such that $\hat{y} = \hat{x}\hat{z}$. Let $z \in R$ be the class of $\hat{z}$. Then $y = xz$. We have shown that if $v(y) \geq v(x)$, then $y \in xR$.

Let $\pi \in R$ be such that $v(\pi) = 1$. Let I be an ideal generated by a set S. Let $i = \inf_{x \in S} v(x)$. Then $S \subseteq \pi^i R$. $\pi^i \in I$ because $S \subseteq I$ contains an element of valuation i. Hence every ideal has the form $I = \pi^i R$, so R is local and has a principal maximal ideal. Since $\pi^{\frac{\log \rho}{\log \theta}}$ is the smallest power of π which is 0, R is Artinian, and the assertion about the length holds.[1] □

We will denote the maximal ideal of R by $\mathfrak{m}_R$.

[1] This step is where we use the assumption that H is not a field. If H were a field, then $\rho = 0$, so the length would be infinite. We would then have a DVR rather than a truncated DVR. In fact, in this case the construction described just gives the ring of integers.

Lemma 5.2.3. *M is free of rank 1. Furthermore there is a canonical isomorphism $M_i \cong M^{\otimes i}$ for $i \in \mathbb{N}$.*

Proof. Let $\pi \in H$ be a uniformizer. Multiplication by π gives a bijection $\mathcal{O}_H \to \mathfrak{m}_H$. It is easily seen that this induces a well-defined bijection $\mathcal{O}_H/\equiv_\rho \to \mathfrak{m}_H/\equiv_{\theta\rho}$. Since this bijection is just multiplication by $\bar{\pi} \in M$, it is a homomorphism of modules, and so M is free of rank 1. A similar argument shows M_i is free and generated by $\overline{\pi^i}$. We define an isomorphism $M_i \cong M^{\otimes i}$ sending $\overline{\pi^i}$ to $\bar{\pi}^{\otimes i}$. It is easy to check this is canonical in the sense that it is independent of the choice of π. □

We now construct a map $\epsilon : M \to R$. Let $x \in M$. Let $\hat{x} \in \mathfrak{m}_H \subseteq \mathcal{O}_H$ be a lift. Then $\epsilon(x)$ is defined to be the class of $\hat{x}$ in R.

Lemma 5.2.4. *ϵ is a well defined R-linear map. Furthermore, its image is $\mathfrak{m}_R$.*

Proof. Let $\hat{x}, \hat{x}' \in \mathfrak{m}_H$ be lifts of $x \in R$. Then $\hat{x} \equiv_{\theta\rho} \hat{x}'$, so $\hat{x} \equiv_\rho \hat{x}'$. Thus they give the same element of R, and so ϵ is well-defined. The R-linearity is trivial. The description of its image is also easy. □

Definition 5.2.5. $\mathrm{Tr}(H) = (R, M, \epsilon)$.

We have proven the following theorem.

Theorem 5.2.6. $\mathrm{Tr}(H)$ *is a triple in the sense of Deligne.*

5.3 Functoriality

Let H, H' be discretely valued hyperfields, which are not fields. We will retain all the notation of the previous section. In addition we will define ρ', θ', ϵ', R', M', and M'_i in a manner analogous to that of the previous section, but using H' instead of H.[2] Throughout this section, we let $f : H \to H'$ be a morphism of valued hyperfields. We will let $r = \frac{\log \theta}{\log \theta'}$.

Lemma 5.3.1. *[5, pg149]$\rho' \geq \rho$.*

Proof. Let $x, y \in H$. Let $z, z' \in x + y$ be distinct. We wish to show $d(z, z') \leq \rho' \max(|x|, |y|)$.

First suppose that $f(z) \neq f(z')$. It is easily seen that $f(z), f(z') \in f(x) + f(y)$. By the definition of ρ', $|f(z) - f(z')| = d(f(z), f(z')) \leq \rho' \max(|f(x)|, |f(y)|) = \rho' \max(|x|, |y|)$. Since $f(z - z') \subseteq f(z) - f(z')$, $|z - z'| = |f(z) - f(z')| \leq \rho' \max(|x|, |y|)$.

Now we consider the case where $f(z) = f(z')$. Suppose for the sake of contradiction that $d(z, z') > \rho' \max(|x|, |y|)$. Then $d(1, \frac{z}{z'}) > \frac{\rho' \max(|x|,|y|)}{|z'|} \geq \rho'$. Let $u = \frac{z}{z'}$. Then $|1 - u| > \rho'$, and $f(u) = 1$. Since $f(1 - u) \subseteq f(1) - f(u) = 1 - 1$, and since $1 - 1$ is a ball of radius ρ' around 0, it follows that $|f(1 - u)| \leq \rho'$. This contradicts the fact that $|1 - u| > \rho'$. □

We define a map $\phi : R \to R'$ by letting $\phi(x)$ be the class of $f(\hat{x})$ where $\hat{x} \in H$ is any lift.

[2] So for example $\mathrm{Tr}(H') = (R', M', \epsilon')$.

Proposition 5.3.2. *ϕ is a well-defined ring homomorphism.*

Proof. Let $\hat{x}, \hat{x}' \in H$ be lifts of x. Then $\hat{x} \equiv_\rho \hat{x}'$, so $f(\hat{x}) \equiv_\rho f(\hat{x}')$. Then $\hat{x}$ and $\hat{x}'$ define the same class in R' by 5.3.1. Thus ϕ is well-defined. Let $x, y \in R$, and let $\hat{x}, \hat{y}$ be lifts. Then any element $\hat{z} \in \hat{x} + \hat{y}$ is a lift of $x + y$. Then $f(\hat{z}) \in f(\hat{x} + \hat{y}) \subseteq f(\hat{x}) + f(\hat{y})$, so the class of $f(\hat{z})$ is $\phi(x) + \phi(y)$. The other axioms of a ring homomorphism are easy to verify. □

Definition 5.3.3. We say $f : H \to H'$ is finite if there is a finite subset $S \subseteq H'$ such that for all $x \in H'$ there is a map $a : S \to H$ such that $x \in \sum_{s \in S} a(s)s$. We say that f is flat if $\rho = \rho'$.

It is clear that ϕ is finite if f is.

Lemma 5.3.4. *If f is flat, then $l(R') = rl(R)$ where $l(R)$ denotes the length of R as an R-module.*

Proof. This follows easily from 5.2.2 □

We will now define a map $\eta : M \to M'^{\otimes r} = M'_r$. For $x \in M$, we pick a lift $\hat{x} \in \mathfrak{m}_H$. Then $f(\hat{x}) \in \mathfrak{m}_{H'}^r$, and we let $\eta(x)$ be the class of $f(\hat{x})$.

Lemma 5.3.5. *η is a well-defined R-linear map. It induces an isomorphism $M \otimes R' \to M'^{\otimes r}$.*

Proof. This is proven in the same manner as 5.3.2. If we let $\hat{x}'$ be another lift of x, then since $\hat{x} \equiv_{\theta\rho} \hat{x}'$, $f(\hat{x}) \equiv_{\rho'\theta} f(\hat{x}')$. Since $\theta = \theta'^r$, $f(\hat{x})$ and $f(\hat{x}')$ define the same element of M'_r. R-linearity is straightforward to verify. Let $\pi \in H$ be a uniformizer. $M \otimes R'$ is free with generator $\bar{\pi}$, while M'_r is free with generator $\overline{f(\pi)} = \eta(\bar{pi})$. Thus $M \otimes R' \to M'^{\otimes r}$ maps a generator to a generator, so is an isomorphism. □

Deligne defined an R'-linear map $\epsilon'_{0,r} : M'^{\otimes r} \to R'$ by $\epsilon'_{0,r}(x^{\otimes r}) = \epsilon(x)^r$ when x generates M'. It is straightforward to verify that for $x \in M'_r$, $\epsilon'_{0,r}(x)$ is the class of $\hat{x}$ in R' where $\hat{x} \in \mathfrak{m}^r_{H'} \subseteq \mathcal{O}_{H'}$ is any lift of x.

Lemma 5.3.6. $\epsilon'_{0,r}\eta = \phi\epsilon$.

Proof. It is routine to verify that both composite maps have the following description: Let $x \in M$. Let $\hat{x} \in \mathfrak{m}_H$ be a lift. Then $\epsilon'_{0,r}\eta(x) = \phi\epsilon(x) \in R'$ is the class of $f(\hat{x}) \in \mathcal{O}_{H'}$. □

Definition 5.3.7. $\mathrm{Tr}(f)$ will denote (r, ϕ, η).

We have proven the following theorem.

Theorem 5.3.8. $\mathrm{Tr}(f)$ *is a morphism of triples. It is finite if f is. It is flat if f is.*

Theorem 5.3.9. Tr *is a functor from the category of discretely valued hyperfields which are not fields to the category of triples. It induces a functor from the category of discretely valued hyperfields which are not fields with finite flat morphisms to the category of triples and finite flat morphisms.*

Proof. We only need to show it is compatible with composition. That is, if $f : H \to H'$ and $f' : H' \to H''$ and $\mathrm{Tr(f')} = r', \phi', \eta'$, then we need to show $\mathrm{Tr}(f'f) = (rr', \phi'\phi, \eta'^{\otimes r}\eta)$. This is a straightforward computation, which will be omitted. □

5.4 Recovering the underlying set of the hyperfield

Let $T = (R, M, \epsilon)$ be any triple. We define $v : M^{\otimes i} \to \mathbb{Z} \cup \{\infty\}$[3] by $v(r\pi^i) = v(r)+i$ for $r \in R$, when π is a uniformizer. Let $\mathbf{U}(T) = \{0\} \cup \bigcup_{i \in \mathbb{Z}} \{x \in M^{\otimes i} \mid v(x) = i\}$. If $(r, \phi, \eta) : (R, M, \epsilon) \to (R', M', \epsilon')$ is a morphism of triples, then it induces maps $\eta^{\otimes i} : M^{\otimes i} \to M^{\otimes ri}$ which send elements of valuation i to those of valuation ri. These give a map $\mathbf{U}(r, \phi, \eta) : \mathbf{U}(R, M, \epsilon) \to \mathbf{U}(R', M', \epsilon)$. It is readily verified that $\mathbf{U}$ is a functor.

Proposition 5.4.1. $\mathbf{U} \circ \mathrm{Tr}$ *is naturally isomorphic to the forgetful functor from discretely valued hyperfields which are not fields to the category of sets.*

Proof. Let H be a discretely valued hyperfield which is not a field. Let $T = \mathrm{Tr}(H) = (R, M, \epsilon)$. Let M_i, ρ, and θ be as in §5.2. Let $C_i = \{x \in H \mid v(x) = i\}$. Suppose $x \in C_i$ and $y \in H$ are chosen such that $x \equiv_{\theta^i \rho} y$. Then by page 145 of Krasner, $x = y$. Thus the reduction map $C_i \to M_i$ is injective. Its image consists of elements with valuation i, so we have bijections $C_i \xrightarrow{\alpha_i} \{x \in M_i \mid v(x) = i\} \xrightarrow{\beta_i} \{x \in M^{\otimes i} \mid v(x) = i\}$. If these bijections are natural[4], then so is the induced bijection $H = \{0\} \cup \bigcup_{i \in \mathbb{Z}} C_i \to \{0\} \cup \bigcup_{i \in \mathbb{Z}} \{x \in M^{\otimes i} \mid v(x) = i\} = \mathbf{U}(\mathrm{Tr}(H))$, and the result will follow.

Let $f : H \to H'$ be a morphism to another discretely valued hyperfield which is

[3] Since M is projective of rank 1, negative tensor powers are defined.

[4] Actually, we will require that $\alpha_{\frac{\log u}{\log \rho}}$ and $\beta_{\frac{\log u}{\log \rho}}$ are natural for any fixed u, rather than fixing i.

not a field. Let $\mathrm{Tr}(H') = (R', M', \epsilon')$, and let C_i' and M_i' be like C_i and M_i, but defined in terms of H' instead of H. Let $(r, \phi, \eta) = \mathrm{Tr}(f)$. Let $x \in C_i$. Then $\alpha_{ri}(f(x))$ is the reduction of $f(x)$ modulo $\equiv_{\theta'^i \rho'}$. Let $\theta_i : M_i \to M_{ri}'$ be the map corresponding to $\eta^{\otimes i}$. It is routine to verify that $\theta_i(x)$ is obtained by lifting x, applying f, and reducing. Then $\theta_i(\alpha_i(x))$ is obtained by reducing x, picking a lift, applying f to that lift, and reducing again. Thus $\theta_i(\alpha_i(x)) = \alpha_{ri}(f(x))$, so the $\alpha_{\frac{\log u}{\log \rho}}$ are natural. The $\beta_{\frac{\log u}{\log \rho}}$ are natural by the choice of θ_i. □

Corollary 5.4.2. Tr *is faithful.*

Proof. This follows from 5.4.1 and the fact that the forgetful functor is faithful. □

5.5 Equivalence

Let H be a discretely valued hyperfield which is not a field. We have seen that there is a canonical bijection $\psi : \mathbf{U}(\mathrm{Tr}(H)) \to H$, so $\tilde{H} = \mathbf{U}(\mathrm{Tr}(H))$ is a discretely valued hyperfield[5]. We will now describe the addition, multiplication, and absolute value on $\tilde{H}$ more explicitly. We will retain the notation of the previous section. Let $S_i = \{x \in M^{\otimes i} \mid v(x) = i\}$, so $\tilde{H} = \{0\} \cup \bigcup_i S_i$. Let π_H be a uniformizer in H, and π_M be its image in M (which must generate M). Throughout this section, we will identify M_i with $M^{\otimes i}$.

For $x \in S_i$, it follows from results of the previous section that $|\psi(x)| = \theta^i$, so

[5] By decreeing ψ to be an isomorphism.

$|x| = \theta^i$. For $x \in S_i$ and $y \in S_j$, we can easily verify that $xy \in S_{i+j} \subseteq M^{\otimes i+j}$ is the image of $x \otimes y$ under $M^{\otimes i} \otimes M^{\otimes j} \to M^{\otimes i+j}$.

Let $x \in S_j$ and $y \in S_i$. Without loss of generality, we assume $i \geq j$. Let $z = x +_{M_j} \epsilon_{j,i}(y) \in M_j$footnoteWe use the notation $+_{\{}M_j\}$ to distinguish this addition from the addition $+_{\tilde{H}}$ which comes from the hyperfield structure on $\tilde{H}$., where $\epsilon_{j,i} : M^{\otimes i} \to M^{\otimes j}$ is the map induced by ϵ. Let $\hat{x}, \hat{y} \in H$ be lifts of $x \in M_j$ and $y \in M_i$. Note that $\hat{y}$ is also a lift of $\epsilon_{j,i}(y)$. Then z is by definition the reduction of any element of $\hat{x} + \hat{y}$. Since $|x| = \theta^j$, $\hat{x} + \hat{y}$ is a ball of radius $\rho\theta^j$, so it is the preimage of z under the reduction map. Let $w \in \tilde{H}$. It is easy to check that $\psi(w) \in H$ reduces to $z \in M_i$ if and only if either both $w = 0$ and $z = 0$ hold or if $w \in S_k$ for some $k \geq j$ and $\epsilon_{j,k}(w) = z$, because any element of H corresponding to $w \in M_k$ corresponds to $\epsilon_{j,k}(w) \in M_j$. Thus $x +_{\tilde{H}} y = \bigcup_{k \geq j} \{w \in S_k \mid \epsilon_{j,k}(w) = x + \epsilon_{j,i}(y)\}$, or it is the union of this set with $\{0\}$ depending on whether $x = -y$.

Let H, H' be discretely valued hyperfields which are not fields. Let $(r, \phi, \eta) : \mathrm{Tr}(H) \to \mathrm{Tr}(H')$ be a morphism of triples. Let $f = \mathbf{U}(r, \phi, \eta) : \tilde{H} \to \tilde{H}'$.

Proposition 5.5.1. *If $r = \frac{\log \theta}{\log \theta'}$, then f is a morphism of valued hyperfields.*

Proof. By construction, f maps elements of S_i to elements of S'_{ri} (via the maps $\eta^{\otimes i}$), and $r = \frac{\log \theta}{\log \theta'}$, so f preserves absolute value. f preserves multiplication, because the multiplication is defined in terms of $M^{\otimes i} \otimes M^{\otimes j} \to M^{\otimes i+j}$ and the corresponding maps for M', and because the maps $S_i \to S'_r i$ are just $\eta^{\otimes i}$. Let $x \in \tilde{H}$ be such that $f(x) = 1$. Then $x \in S_0 \subseteq R$, and $\phi(x) = 1$, so $x - 1 \in \ker(\phi)$. Conversely, if

$x - 1 \in \ker(\phi)$, then $x \in S_0$ and $f(x) = 1$ when we view x as an element of $\tilde{H}$. But the preimage of $\ker(\phi)$ (or of any other ideal of R) in $\mathcal{O}_H$ is a ball around 0. Hence the equation $f(x) = 1$ is equivalent to a bound on $d(1, x) = |x - 1|$, so the fiber of 1 is a ball. Consequently all fibers are balls.

Let $x, y \in H$. Let z be such that $f(z) \in f(x) +_{\tilde{H}'} f(y)$. For simplicity we will consider only the case where $z \neq 0$; the other case is trivial. Suppose $i = v(x) > v(y) = j$. Let $k = v(z)$. Then $v(f(z)) = rk$, and similarly for x and y. Then $\epsilon'_{rj,rk}(f(z)) = f(x) + \epsilon'_{rj,ri}(f(y))$, by the description of $+_{\tilde{H}'}$. So $epsilon'_{rj,rk}(\eta^{\otimes k}(z)) = \eta^{\otimes j} x + \epsilon'_{rj,ri}(\eta otimes i(y))$. Using the definition of a morphism of triples, $\eta^{\otimes j}(\epsilon_{j,k}(z)) = \eta^{\otimes j}(x) + \eta^{\otimes j}(\epsilon_{j,i}(y))$. Since $f(x) = \eta^{\otimes j}(x) = \eta^{\otimes j}(\epsilon_{j,k}(z) - \epsilon_{j,i}(y))$, we may replace x by $\epsilon_{j,k}(z) - \epsilon_{j,i}(y)$ without changing $f(x)$. Without loss of generality, $\epsilon_{j,k}(z) = x + \epsilon_{j,i}(y)$, and so $z \in x + y \subseteq f^{-1}(f(x)) + f^{-1}(f(y))$. Hence $f^{-1}(f(x + y)) \subseteq f^{-1}(f(x)) + f^{-1}(f(y))$. The reverse inclusion is essentially the same argument in reverse, so in fact $f^{-1}(f(x + y)) \subseteq f^{-1}(f(x)) + f^{-1}(f(y))$ for all $f(x), f(y) \in f(H)$. Hence f is a morphism of valued hyperfields. □

Corollary 5.5.2. *Let $(r, \phi, \eta) : \mathrm{Tr}(H) \to \mathrm{Tr}(H')$ be a morphism of triples such that $r = \frac{\log \theta}{\log \theta'}$. Then there is a morphism $f : H \to H'$ such that $(r, \phi, \eta)\mathrm{Tr}(f)$.*

Proof. Let $f : \tilde{H} \to \tilde{H}'$ be as above. We only need to show that $(r, \phi, \eta) = \mathrm{Tr}(f)$. Let $(\tilde{r}, \tilde{\phi}, e\tilde{t}a) = \mathrm{Tr}(f)$. It is easy to check $r = \tilde{r}$. It follows from the first sentence of the proof of 5.5.1 that $\eta^{\otimes i}$ agrees with $\tilde{\eta}^{\otimes i}$ on S_i. Let $x \in M_i$ have valuation j. Let $\hat{x} \in M_j$

be any element such that $\epsilon_{i,j}(\hat{x}) = x$. Then $\eta^{\otimes i}(x) = \eta^{\otimes i}(\epsilon_{j,i}(\hat{x})) = \epsilon'_{rj,ri}(\eta^{\otimes j})(\hat{x})$, and similarly for $\tilde{\eta}$. Then $\eta^{\otimes i}(x) = \epsilon'_{rj,ri}(\eta^{\otimes j})(\hat{x}) = \epsilon'_{rj,ri}(\tilde{\eta}^{\otimes j})(\hat{x}) = \tilde{\eta}^{\otimes i}(x)$. Taking $i = 0$ and $i = 1$ gives the result. □

Theorem 5.5.3. Tr *is essentially surjective.*

Proof. Let (R, M, ϵ) be a triple. Deligne has shown that for any truncated DVR R, there is a DVR $\mathcal{O}$ such that $R \cong \mathcal{O}/\mathfrak{m}^i$ for some i. Let $K = \mathrm{Frac}(\mathcal{O})$. Let $H = K/(1 + \mathfrak{m}^i)$. Let $(R', M', \epsilon') = \mathrm{Tr}(H)$. Then $R' \cong \mathcal{O}/\mathfrak{m}^i \cong R$. Deligne showed that an isomorphism of truncated DVRs extends to an isomorphism of triples; hence $\mathrm{Tr}(H) = (R', M', \epsilon') \cong (R, M, \epsilon)$. Thus Tr is essentially surjective. □

Theorem 5.5.4. *Let H be a discretely valued hyperfield which is not a field. Then* Tr *induces an equivalence of categories between the coslice category of H and the coslice category of* $\mathrm{Tr}(H)$*. It also induces an equivalence between the slice category of H and the slice category of* $\mathrm{Tr}(H)$*.*

Proof. We consider the case of the coslice category; the other part is proven similarly. Clearly this functor is faithful. Let $(r, \phi, \eta) : \mathrm{Tr}(H) \to S$ be an object of the coslice category of $\mathrm{Tr}(H)$. Then there exists H' such that $S \cong \mathrm{Tr}(H')$. By rescaling the absolute value (which does not affect $\mathrm{Tr}(H')$, we may assume $r = \frac{\log \theta}{\log \theta'}$. Then there is a morphism $f : H \to H'$ such that $(r, \phi, \eta) = \mathrm{Tr}(f)$. Hence the functor between coslice categories is essentially surjective.

Given a morphism $(r, \phi, \eta) : \mathrm{Tr}(H') \to \mathrm{Tr}(H'')$ in the coslice category of $\mathrm{Tr}(H)$, we have $r = \frac{\log \theta}{\log \theta'}$, because r is the ratio of the ramification indices of $\mathrm{Tr}(H) \to \mathrm{Tr}(H'')$ and $\mathrm{Tr}(H) \to \mathrm{Tr}(H')$. The functor between the coslice categories is full by 5.5.

□

Proposition 5.5.5. *f is finite and flat if and only if* $\mathrm{Tr}(f)$ *is.*

Proof. We only need to show that finite flat morphisms of discretely valued hyperfields correspond to finite flat morphisms of triples. For flatness, one uses 5.3.4 and its converse (which is proven in the same way). We have seen that if f is finite then so is $Tr(f)$. Let $f : H \to H'$ be a morphism of triples such that $\mathrm{Tr}(f)$ is finite. Let $\mathrm{Tr}(H) = (R, M, \epsilon)$ and $\mathrm{Tr}(H') = (R', M', \epsilon')$, so $\phi : R \to R'$ is finite; the generators will be denoted $\bar{\alpha_1}, \ldots, \bar{\alpha_n}$, and their lifts in H' will be denoted $\alpha_1, \ldots, \alpha_n$. Let $x \in H'$ have absolute value 1. Then there are $a_1, \ldots, a_n \in H$ such that $\bar{x} = \phi(\bar{a_1})\bar{\alpha_1} + \ldots + \phi(\bar{a_n})\bar{\alpha_n}$. Using the definition of addition in R', there exists $y \in H'$ such that $\bar{x} = \bar{y}$ and $y \in f(a_1)\alpha_1 + \ldots f(a_n)\alpha_n$. Because $|x| = 1$, x is the unique lift of $\bar{x}$, and so $x \in f(a_1)\alpha_1 + \ldots + f(a_n)\alpha_n$.

We now let $x \in H'$ be arbitrary. Let r be the ramification index. Let $\pi_H \in H$ and $\pi_{H'} \in H'$ be uniformizers. Then there exist i, j such that $|f(\pi_H)^i \pi_{H'}^{-j} x| = 1$ and $0 \leq j < r$. Then there are $a_1, \ldots, a_n$ such that $x \in f(\pi_H^{-i} a_1)\alpha_1 \pi_{H'}^j + \ldots + f(\pi_H^{-i} a_n)\alpha_n \pi_{H'}^j$, and so x is in the span of the family of elements $\alpha_k \pi_{H'}^j$. Hence f is finite. □

Chapter 6

The Fontaine-Wintenberger theory of norm fields

In this chapter, we will present Wintenberger's construction of the norm field (cf.[2]), which to a suitable infinite extension L/K of a local field, associates a local field $X_K(L)$ of characteristic p whose extensions correspond to extensions of L. We will also present the related notion of the perfect norm field. This chapter will contain no new results.

6.1 Perfect norm fields

Before constructing the norm field, we will first introduce a related construction called the perfect norm field. This is somewhat simpler because it uses the p-th power map instead of norm maps.

Definition 6.1.1. If A is a ring of characteristic p, we will let $\underline{R}(A)$ be the inverse limit of the system $\ldots \to A \to A \to A$, where all of the maps are the p-th power.

Remark 6.1.2. $\underline{R}(A)$ is a ring, because the p-th power map is a ring homomorphism. An element $\alpha = \underline{R}(A)$ is a sequence of elements $\alpha_i \in A$ such that $\alpha_i = \alpha_{i+1}^p$. $\underline{R}(A)$ is then perfect because $\beta_i = \alpha_{i+1}$ defines an element of $\underline{R}(A)$, and because the p-th power map is injective on $\underline{R}(A)$. There is a canonical map $\underline{R}(A) \to A$ sending a sequence $\{\alpha_i\}$ to α_0. It is easy to check that the map $\underline{R}(A) \to A$ is universal among maps from perfect rings of characteristic p to A in the sense that any map $B \to A$ with B perfect induces a unique map $B \to \underline{R}(A)$ such that the obvious triangle commutes. More specifically, if $f : B \to A$, then the corresponding map $B \to \underline{R}(A)$ sends x to the sequence whose i-th term is $f(x^{p^{-i}})$.

We will need the following estimate on the p-th power map.

Remark 6.1.3. Let $\mathcal{O}$ be the ring of integers of a valued field with residue field of characteristic p. Then if $x, y \in \mathcal{O}$ are congruent mod p, $v(x^p - y^p) \geq v(x-y) + v(p)$. Hence $v(x^{p^k} - y^{p^k}) \geq kv(p)$.

Proposition 6.1.4 ([9, 4.3.1]). *Let $\mathcal{O}$ be a domain which is separated and complete with respect to the p-adic valuation and which has a perfect residue field of characteristic p. Then $\varprojlim_{x \mapsto x^p} \mathcal{O} \cong \underline{R}(\mathcal{O}/p)$ as multiplicative monoids. In particular $\underline{R}(\mathcal{O}/p)$ is a domain.*

Proof. An element $x \in \varprojlim_{x \mapsto x^p} \mathcal{O}$ is the same as a sequence of elements $x_i \in \mathcal{O}$ such that $x_i = x_{i+1}^p$ for all $i \in \mathbb{N}$. A similar description holds for $\underline{R}(\mathcal{O}/p)$. We define a map $\psi : \varprojlim_{x \mapsto x^p} \mathcal{O} \to \underline{R}(\mathcal{O}/p)$ by sending x to the sequence of elements $x_i \bmod p \in \mathcal{O}/p$. Let $\overline{x_i} \in \mathcal{O}/p$ define an element of $\underline{R}(\mathcal{O}/p)$. We let $\widehat{\overline{x_i}} \in \mathcal{O}$ denote any lift of $\overline{x_i}$. Then I claim that $\lim_{i \to \infty} \widehat{\overline{x_{j+i}}}^{p^i}$ is well defined and converges. Let $\widehat{\overline{x_i}}'$ be another lift. Then $\widehat{\overline{x_{i+j}}}' \equiv \widehat{\overline{x_{i+j}}}$ modulo p, so by Remark 6.1.3, $v(\widehat{\overline{x_{i+j}}}'^{p^i} - \widehat{\overline{x_{i+j}}}^{p^i}) \geq iv(p)$, which tends to ∞. Hence the limit, if it exists, is independent of the choice of $\widehat{\overline{x_i}}$. For any $k \in \mathbb{N}$, $\widehat{\overline{x_{i+j+k}}}^{p^k} \equiv \widehat{\overline{x_{i+j}}}$ mod p, so for all j, $v(\widehat{\overline{x_{i+j+k}}}^{p^{j+k}} - \widehat{\overline{x_{i+j}}}^{p^j})$ tends to ∞. Hence the sequence is Cauchy, so it converges, as was claimed. Now we define a map $\theta : \underline{R}(\mathcal{O}/p) \to \varprojlim_{x \mapsto x^p} \mathcal{O}$ which sends a sequence $\overline{x_i}$ to the sequence $\lim_{j \to \infty} \widehat{\overline{x_{i+j}}}^{p^j}$. It is straightforward to show $\psi\theta = \mathrm{id}$. To show $\theta\psi = \mathrm{id}$, we let x_i be a sequence defining an element of $\varprojlim_{x \mapsto x^p} \mathcal{O}$, and let $\overline{x_i}$ be its reduction mod p. Then one choice of a lift is $\widehat{\overline{x_i}} = x_i$, so $\lim_{i \to \infty} \widehat{\overline{x_{j+i}}}^{p^i} = \lim_{i \to \infty} x_{j+i}^{p^i} = x_j$. □

Let K be a valued field which is complete and separated with respect to the p-adic valuation and have residue field of characteristic p. We will write R_K for $\underline{R}(\mathcal{O}_K/p)$. An element of R_K can be viewed either as a sequence $x_i \in \mathcal{O}_K/p$ satisfying $x_i = x_{i+1}^p$, or as a sequence $x^{(i)} \in \mathcal{O}_K$ satisfying $(x^{(i+1)})^p = x^{(i)}$.

Lemma 6.1.5 ([9, 4.3.3/13.2.2]). *R_K is a complete valuation ring under the valuation $v(\{x^{(i)}\}_{i \in \mathbb{N}}) = v_K(x^{(0)})$.*

The above lemma is proven by essentially the same method used for 6.2.12.

Definition 6.1.6 ([27])**.** $\mathrm{Frac}(R_K)$ is called the perfect norm field associated to K.

Theorem 6.1.7 ([9, 4.3.5])**.** *If K is a discretely valued field of characteristic 0 and of residue characteristic p, then $\mathrm{Frac}(\underline{R}(\mathcal{O}_{C_K}))$ is algebraically closed, where C_K is the completion of the algebraic closure of K.*

For any complete valued field K with residue field of characteristic p, we have a canonical valuation-preserving action of $\mathrm{Gal}(\bar{K}/K)$ on $R_{\hat{\bar{K}}}$ by acting on a sequence $x^{(i)} \in \mathcal{O}_{\bar{K}}$ component wise. We can define an embedding $R_K \subseteq R_{\hat{\bar{K}}}$ by using the embedding $\mathcal{O}_K \subseteq \mathcal{O}_{\bar{K}}$ on each component.

The following result will allow us to compare the Galois group of K with that of $\mathrm{Frac}(R_K)$.

Proposition 6.1.8 ([9, 14.2.4])**.** *Let K be a complete discretely valued field of characteristic 0 and residue characteristic p. Then $R_{\hat{\bar{K}}}^{\mathrm{Gal}(\bar{K}/K)} = R_K$. Similarly, we also have $\mathrm{Frac}(R_{\hat{\bar{K}}})^{\mathrm{Gal}(\bar{K}/K)} = \mathrm{Frac}(R_K)$.*

Proof. For the first part apply $\mathcal{O}_{\hat{\bar{K}}}^{\mathrm{Gal}(\bar{K}/K)} = \mathcal{O}_K$ to each component. For the second, let $x \in \mathrm{Frac}(R_{\hat{\bar{K}}})^{\mathrm{Gal}(\bar{K}/K)}$. Then either x or $1/x$ is in $R_{\hat{\bar{K}}}^{\mathrm{Gal}(\bar{K}/K)} = R_K$, because $R_{\hat{\bar{K}}}$ is a valuation ring. Hence $\mathrm{Frac}(R_{\hat{\bar{K}}})^{\mathrm{Gal}(\bar{K}/K)} \subseteq \mathrm{Frac}(R_K)$. The reverse inclusion is trivial. $\square$

Let K be a local field of characteristic 0 and residue characteristic p, and K_∞/K be a totally ramified $\mathbb{Z}_p$ extension, i.e. $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$. We will abuse terminology by assuming $\mathrm{Gal}(K_\infty/K) = \mathbb{Z}_p$. We write K_n for the fixed field $K_\infty^{p^n\mathbb{Z}_p}$ of the subgroup $p^n\mathbb{Z}_p \subseteq \mathrm{Gal}(K_\infty/K)$.

Theorem 6.1.9 ([9, 13.2.6])**.** *Let M_1 and M_2 be finite separable extensions of K_∞ with $M_2 \subseteq M_1$. Then $[M_1 : M_2] = [\mathrm{Frac}(R_{M_1}) : \mathrm{Frac}(R_{M_2})]$. If M_1/M_2 is Galois, then $\mathrm{Gal}(\mathrm{Frac}(R_{M_1})/\mathrm{Frac}(R_{M_2})) \cong \mathrm{Gal}(M_1/M_2)$.*

Proof. We may easily reduce this to the Galois case. Let $H_i = \mathrm{Gal}(\bar{K}/M_i) \subseteq \mathrm{Gal}(\bar{K}/K)$. Then H_1 acts trivially on $\mathrm{Frac}(R_{M_1})$, so H_2/H_1 acts on $\mathrm{Frac}(R_{M_1})$. We have $\mathrm{Frac}(R_{M_1})^{H_2/H_1} = \mathrm{Frac}(R_{\hat{\bar{K}}})^{H_2} = \mathrm{Frac}(R_{M_2})$ by Proposition 6.1.8. Then $\mathrm{Frac}(R_{M_1})/\mathrm{Frac}(R_{M_2})$ is a finite Galois extension, whose Galois group is a quotient of $H_2/H_1 \cong \mathrm{Gal}(M_1/M_2)$.[1] By 13.3.12 of,[9] $\mathrm{Gal}(\mathrm{Frac}(R_{M_1})/\mathrm{Frac}(R_{M_2})) \cong H_2/H_1$. □

6.2 Construction of the norm field

Given a suitable extension L/K of a local field, we will show that the inverse limit of finite subextensions along the norm maps is a local field. In order to do this, we will first need to relate the behaviour of the norm map to ramification.

Definition 6.2.1 ([2, 1.2.1])**.** Let K be a local field of characteristic 0. A separable extension L/K is said to be arithmetically profinite or APF if for each real number $u \geq -1$, the subfield of L fixed by G_K^u is a finite extension of K. Equivalently, L/K is APF if $G_K^u G_L$ has finite index in G_K for all $u \geq -1$.

[1] More specifically the Galois group is the image of H_2/H_1 in $Aut(\mathrm{Frac}(R_{M_1}))$.

In the language introduced in 2.0.18, the fixed field of $G_L G_K^u$ is the maximal subextension of L/K with ramification bounded by u. Then the above definition can be restated as saying that the maximal subextension of L/K with ramification bounded by u is a finite extension of K. This will often allow us to reduce questions about APF extensions to questions about finite extensions. This phenomenon will be used in 6.2.3 to show that we can give a reasonable definition for the functions $\psi_{L/K}$ when L/K is APF. To do this we first make a definition analogous to 2.0.17.

Definition 6.2.2 ([2, 1.2.1]). If L/K is totally ramified and APF, define $\psi_{L/K}(t) = \int_0^t [G_K : G_L G_K^u] du$. If L/K is any APF extension, we define $\psi_{L/K}(t) = \psi_{L/K_0}(t)$, where K_0 is the maximal unramified subextension of L/K. We let $\phi_{L/K}$ be the inverse function. For an APF extension, let $i_{L/K} = \sup\{i \mid G_K^i G_L = G_K\}$.

In the terminology of 2.0.18, $i_{L/K}$ may be thought of as the greatest lower bound for the ramification of L/K.

Remark 6.2.3. If L/K is finite, then it is trivially APF. In this case 2.0.17 says that our definition of $\psi_{L/K}$ agrees with 2.0.10. The study of $\psi_{L/K}$ in general can be reduced to the finite case. If E/K is a finite subextension containing the fixed field of $G_K^t G_L$ for some t, then for $u \leq t$, $G_L G_K^u \subseteq (G_E G_K^t) G_K^u = G_E G_K^u$, and the reverse inclusion follows from $G_L \subseteq G_E$, so $G_L G_K^u = G_L G_K^u$ for $u \leq t$. Hence $\psi_{L/K}(t) = \psi_{E/K}(t)$. If L is the union of an increasing sequence $\{E_i\}$ of finite extensions, then $\psi_{L/K} = \lim_{i\to\infty} \psi_{E_i/K}$. If F/K is a finite subextension of L, then $\psi_{L/F} \circ \psi_{F/K} = \lim_{i\to\infty} \psi_{E_i/F} \circ \psi_{F/K} = \lim_{i\to\infty} \psi_{E_i/K} = \psi_{L/K}$.

Proposition 6.2.4 ([2, 1.2.3]). *Let $K \subseteq L \subseteq M$ be fields, with K a local field. Then*

(a) Suppose M/L is finite. Then M/K is APF if and only if L/K is APF. In this case $i_{L/K} \geq i_{M/K}$.

(b) Suppose L/K is finite. Then M/K is APF if and only if M/L is APF. In this case $i_{M/L} \geq \psi_{L/K}(i_{M/K}) \geq i_{M/K}$

(c) A subextension of an APF extension is APF.

Let L/K be an infinite APF extension of a local field of residue characteristic p. Let $\mathcal{E}_{L/K}$ be the poset consisting of finite subextensions of L/K.

Definition 6.2.5. Let $X_K(L) = \varprojlim_{F \in \mathcal{E}_{L/K}} F$, where the transition maps are the norm maps. $X_K(L)$ is called the norm field of L/K.

$X_K(L)$ is a monoid under multiplication because the norm maps are monoid homomorphisms. We wish to show that $X_K(L)$ is in fact a local field. Since $X_K(L) = X_F(L)$ for any finite subextension F of L/K, we can replace K by the maximal tamely ramified subextension (which is finite over K because L/K is APF), and so we will assume without loss of generality that L/K is totally wildly ramified. The first step is to show that the norm maps approximately behave like surjective additive homomorphisms in the following sense:

Lemma 6.2.6 ([2, 2.2.1]). *Let E/F be a finite separable totally wildly ramified extension of local fields with residue characteristic p. Then*

(a) $v_F(N_{E/F}(a+b) - N_{E/F}(a) - N_{E/F}(b)) \geq \frac{(p-1)i_{E/F}}{p}$ for all $a, b \in E$.

(b) For all $\alpha \in F$, $\exists a \in E$ *such that* $v_F(N_{E/F}(a) - \alpha) \geq \frac{(p-1)i_{E/F}}{p}$.

Proof. (a) I will consider only the case where E/F is Galois. The general case is proven in 2.2.2.5 of.[2] We may assume that $\frac{a}{b}$ is integral. Since $v_F(N_{E/F}(b)) \geq 0$, it suffices to show $v_F(N_{E/F}(1 + \frac{a}{b}) - N_{E/F}(1) - N_{E/F}(\frac{a}{b})) \geq \frac{(p-1)i_{E/F}}{p}$, so we may also assume without loss of generality that $b = 1$. First we consider the case where E/F is cyclic of degree p. By definition, $G_F^t G_E = G_F$ for $t < i_{E/F}$, so $\mathrm{Gal}(E/F)^t = \mathrm{Gal}(E/F)$ for such t, and $\psi_{E/F}(u) = u$ for $u < i_{E/F}$. Then $\mathrm{Gal}(E/F)_u = \mathrm{Gal}(E/F)_{\psi_{E/F}(u)} = \mathrm{Gal}(E/F)^u = \mathrm{Gal}(E/F)$ for $u < i_{E/F}$. Similarly, $\mathrm{Gal}(E/F)_u \neq \mathrm{Gal}(E/F)$ if $u > i_{E/F}$ so $\mathrm{Gal}(E/F)_u = 1$ for such u. According to lemma V.3.5 and V.3.4 of,[1] $N_{E/F}(1 + a) - 1 - N_{E/F}(a) \in Tr(\mathcal{O}_E) \subseteq \mathfrak{p}_F^r$, where $r = \lfloor \frac{(p-1)(i_{E/F}+1)}{p} \rfloor \geq \frac{(p-1)i_{E/F}}{p}$, as desired. In general, since E/F is totally ramified, it has degree p^k for some k, and we proceed by induction on k. The base case $k = 1$ has already been done. Assume the result holds for extensions of degree less than p^k, and let E/F be totally wildly ramified of degree p^k. Then by the theory of p-groups, there is a degree p subextension K/F, and by the inductive hypothesis, the result holds for E/K and K/F. Then $N_{E/F}(1 + a) - N_{E/F}(a) - 1 = N_{K/F}(N_{E/K}(1+a)) - N_{K/F}(N_{E/K}(a)) - 1 = N_{K/F}(N_{E/K}(a) + 1 + \gamma) - N_{K/F}(N_{E/K}(a)) - 1 = N_{K/F}(N_{E/K}(a)) + 1 + N_{K/F}(\gamma) - N_{K/F}(N_{E/K}(a)) - 1 + \gamma' = N_{K/F}(\gamma) + \gamma'$, where $v_K(\gamma) \geq \frac{(p-1)i_{E/K}}{p}$, and $v_F(\gamma') \geq \frac{(p-1)i_{E/K}}{p} \geq \frac{(p-1)i_{E/F}}{p}$. But $v_F(N_{K/F}(\gamma)) = v_K(\gamma) \geq \frac{(p-1)i_{E/K}}{p} \geq \frac{(p-1)i_{E/F}}{p}$, so $v_F(N_{E/F}(1 + a) - N_{E/F}(a) - 1) = v_F(N_{K/F}(\gamma) + \gamma') \geq \frac{(p-1)i_{E/F}}{p}$, as desired. (b) Let π_E, π_F be uniformizers for E and

F respectively, such that $N_{E/F}(\pi_E) = \pi_F$. Write $\alpha = \sum_{i\geq 0}[x_i]\pi_F^i$, where $[x_i]$ is the multiplicative representative of an element x_i of the residue field of F. Let $a = \sum_{i\geq 0}[x_i]^{[E:F]^{-1}}\pi_E^i$. By part (a), we see that $N_{E/F}(a) \equiv \sum_{i\geq 0} N_{E/F}([x_i]^{[E:F]^{-1}})N_{E/F}(\pi_E^i) = \sum_{i\geq 0}[x_i]\pi_F^i = \alpha$, where $\equiv$ denotes congruence modulo elements of valuation $\geq \frac{(p-1)i_{E/F}}{p}$.

□

Definition 6.2.7. Let E/F be an APF field extension. Suppose $G_F^b G_E \neq G_F^{b+\epsilon} G_E$ for all $\epsilon > 0$. Then we say that b is a jump in the upper ramification filtration of E/F.

Definition 6.2.8. Let P be a poset such that any 2 elements have an upper bound. Let X be a topological space. Let $x \in X$ and let x_p be a sequence of elements of x indexed by P. We say $\lim_{p\in P} x_p = x$ if for every neighborhood U of x, there exists $p_U \in P$ such that $x_p \in U$ for every $p \geq p_U$.

Such limits can be seen to be unique and satisfy the standard limit laws from calculus by using the same proofs used in the classical case $P = \mathbb{N}$. In most applications of this definition we will use $P = \mathcal{E}_{L/K}$.

The following lemma shows that the accuracy of the approximations in lemma 6.2.6 can always be substantially improved by enlarging the field extension.

Lemma 6.2.9 ([2, 2.2.3.1])**.** *Let L/K be as above. Then $\lim_{E\in\mathcal{E}_{L/K}} i_{L/E} = \infty$; i.e. for every $N > 0$ there exists a finite extension E_N/K such that $i_{L/E} > N$ for every finite intermediate extension $E_N \subseteq E \subseteq L$.*

Proof. By Proposition 6.2.4, it suffices to find E_N/K such that $i_{L/E_N} > N$. Let $\{b_n\}$ be the sequence of jumps in the upper ramification filtration of L/K. It is easily seen that since L/K is infinite APF, $\lim_{n\to\infty} b_n = \infty$. Let K_n be the fixed field of $G_K^{b_n}G_L$. I claim that $i_{L/K_n} = \psi_{L/K}(b_n)$.

Let u be such that $G_{K_n}^u G_L = G_{K_n}$. Then since $G_{K_n}^u = G_{K_n} \cap G_K^{\phi_{K_n/K}(u)}$, we have $G_K^{b_n}G_L = G_{K_n} = G_{K_n}^u G_L = (G_{K_n} \cap G_K^{\phi_{K_n/K}(u)})G_L = (G_K^{b_n}G_L \cap G_K^{\phi_{K_n/K}(u)})G_L = G_K^{b_n}G_L \cap G_K^{\phi_{K_n/K}(u)}G_L$. Then $G_K^{b_n}G_L \subseteq G_K^{\phi_{K_n/K}(u)}G_L$. Since b_n is a jump in the filtration, $\phi_{K_n/K}(u) \leq b_n$, so $u \leq \psi_{K_n/K}(b_n)$. A similar argument shows that conversely, if $u \leq \psi_{K_n/K}(b_n)$, then $G_{K_n}^u G_L = G_{K_n}$. By definition of i_{L/K_n}, we have $i_{L/K_n} = \psi_{K_n/K}(b_n)$. It then suffices to show that $\psi_{K_n/K}(b_n) = \psi_{L/K}(b_n)$. Since $\psi_{L/K_n}(t) = t$ for $t \leq i_{L/K_n} = \psi_{K_n/K}(b_n)$, and since $\psi_{L/K} = \psi_{L/K_n} \circ \psi_{K_n/K}$, the claim follows.

Since b_n tends to infinity, so does $\psi_{L/K}(b_n)$, so we may pick n so that $\psi_{L/K}(b_n) \geq N$. If we take $E_N = K_n$, then the result follows from the claim above. □

The following lemma should be viewed as a sort of equicontinuity result for the norm maps.

Lemma 6.2.10 ([2, 2.3.2.2]). *Let E/F be a finite extension of local fields. Let $\alpha, \beta \in E$. Then $v_F(N_{E/F}(\alpha) - N_{E/F}(\beta)) \geq \phi_{E/F}(v_E(\alpha - \beta))$.*

Let $\{s(E)\}_{E\in\mathcal{E}_{L/K}}$ be an increasing sequence of integers indexed by finite subextensions of L/K, such that $s(E) \leq \frac{(p-1)i_{E/F}}{p}$ and $\lim_{E\in\mathcal{E}_{L/K}} s(E) = \infty$. This is possible by Lemma 6.2.9. It is easy to see that for any subextension F of E/K, the map

$N_{E/F} : \mathcal{O}_E/\mathfrak{p}_E^{s(E)} \to \mathcal{O}_F/\mathfrak{p}_F^{s(F)}$ is well defined. by Lemma 6.2.6, this map is a surjective ring homomorphism.

Definition 6.2.11. Let $A_K(L) = \varprojlim_{\mathcal{E}_{L/K}} \mathcal{O}_E/\mathfrak{p}_E^{s(E)}$, where the transition maps in the inverse system are those induced by the norm.

$A_K(L)$ is a ring because the transition maps are homomorphisms by 6.2.6.

Theorem 6.2.12 ([2, 2.2.4]). *Let L/K be a totally wildly ramified infinite APF extension.*

(a) $A_K(L)$ is a complete DVR of characteristic p.

(b) The residue field of $A_K(L)$ is canonically isomorphic to that of L.

(c) The field of fractions of $A_K(L)$ is canonically isomorphic to $X_K(L)$ as a monoid.

Proof. (a) Picking an element $x \in A_K(L)$ amounts to picking a collection of elements $x_E \in \mathcal{O}_E/\mathfrak{p}_E^{s(E)}$ for each finite subextension E of L such that $N_{E/F}(x_E) = x_F$ whenever $K \subseteq F \subseteq E \subseteq L$. We define $v(x) = \lim_{E \in \mathcal{E}_{L/K}} v_E(\widehat{x_E})$, where $\widehat{x_E} \in \mathcal{O}_E$ is any lift of x_E. It is straightforward to check that if $x \neq 0$, then $v_E(\widehat{x_E})$ is independent of $\widehat{x_E}$ if $s(E)$ is large enough. Furthermore, for such an E, we have $v_E(\widehat{x_E}) = v_F(\widehat{x_F})$ for any finite subextension F containing E because we may take $\widehat{x_E} = N_{F/E}(\widehat{x_F})$. It follows that $v(x)$ is defined, is a finite integer unless $x = 0$, and is independent of $\widehat{x_E}$. To verify that v is a discrete valuation on $A_K(L)$, one uses the definition of v and the fact that v_E is a valuation. To show $A_K(L)$ is complete, let $\{x_i\}_{i \in \mathbb{N}}$ be a Cauchy sequence. Let $x_{E;i}$ be the corresponding element of $\mathcal{O}_E/\mathfrak{p}_E^{s(E)}$. Using the continuity of the projection $A_K(L) \to \mathcal{O}_E/\mathfrak{p}_E^{s(E)}$, one sees that $\{x_{E;i}\}_{i\in\mathbb{N}}$ is Cauchy for any fixed E, and hence converges to an element $x_E \in \mathcal{O}_E/\mathfrak{p}_E^{s(E)}$. These elements are clearly compatible, as seen by using the compatibility of the $x_{E;i}$ for each i, so they give an element x in the inverse limit $A_K(L)$. To show that $A_K(L)$ has characteristic p, note that $v(p) = \lim_{E\in\mathcal{E}_{L/K}} v_E(p) = \infty$ since the ramification indices of the finite subextensions of L/K tend to infinity. Hence $p = 0$.

(b) Since L/K is totally ramified, the residue field of L agrees with that of any subextension of L/K. Let k denote this common residue field. For any finite subextension E and any $y \in \mathcal{O}_E/\mathfrak{p}_E^{s(E)}$, we let $\bar{y} \in k$ denote the reduction modulo the maximal ideal. Let E/K be any finite subextension of L/K. Define $f : A_K(L) \to k$ by $f(x) = \bar{x_E}^{1/[E:K]}$. Taking the $\frac{1}{[E:K]}$-th power makes sense because $[E:K]$ is a p-th power and k is perfect. For any $a \in E$ it is easy to check using the fact that E/K is totally ramified that $N_{E/K}(a)$ and $a^{[E:K]}$ define the same element of k. This fact allows one to easily show that f is independent of the choice of E. It is straightforward to check that f is a surjective ring homomorphism. Hence, we only need to show the kernel of f is maximal. Suppose $x \in \mathfrak{m}_{A_K(L)}$. Then $v(x) > 0$ so $v_E(\widehat{x_E}) > 0$ for all sufficiently large E. Hence $v_E(\widehat{x_E}^{1/[E:K]}) > 0$ so $f(x) = 0$.

(c) Let $a \in A_K(L)$. For each $E \in \mathcal{E}_{L/K}$, let $\widehat{(a_E)} \in \mathcal{O}_E$ be any lift of the element $a_E \in \mathcal{O}_E/\mathfrak{p}^{s(E)}$ corresponding to a. I claim that for any $F \in \mathcal{E}_{L/K}$, $\lim_{E\in\mathcal{L}/\mathcal{F}} N_{E/F}(\widehat{a_E})$ converges. To see this, note that for any $E' \in \mathcal{E}_{L/E}$, $v_E(N_{E'/E}(\widehat{a_{E'}}) - \widehat{a_E}) \geq s(E)$.

by Lemma 6.2.6a $v_F(N_{E'/F}(\widehat{a_{E'}}) - N_{E/F}(\widehat{a_E})) = v_F(N_{E/F}(N_{E'/E}(\widehat{a_{E'}})) - N_{E/F}(\widehat{a_E}))$. by Lemma 6.2.10, $v_F(N_{E/F}(N_{E'/E}(\widehat{a_{E'}})) - N_{E/F}(\widehat{a_E})) \geq \phi_{E/F}(s(E)) \geq \phi_{L/F}(s(E))$. In particular, since $s(E) \to \infty$, $\{N_{E/F}(\widehat{a_E})\}$ is Cauchy, and hence converges. An argument analogous to the above shows that the limit is independent of the choice of $\widehat{a_E}$.

Specifying an α in $X_K(L)$ is the same as specifying a choice of $\alpha_E \in E$ for each $E \in \mathcal{E}_{L/K}$ such that $N_{F/E}(\alpha_F) = \alpha_E$ for each finite extension F/E. Let $\mathcal{O}_{X_K(L)}$ be the subset of $X_K(L)$ consisting of elements α such that α_E is integral for all E. By the previous paragraph we have a map $\eta : A_K(L) \to \mathcal{O}_{X_K(L)}$ such that $\eta(a)_E = \lim_{E \in \mathcal{L}/\mathcal{F}} N_{E/F}(\widehat{a_E})$. It is easy to check that the map $\mathcal{O}_{X_K(L)} \to A_K(L)$ induced by the maps $\mathcal{O}_E \to \mathcal{O}_E/\mathfrak{p}^{s(E)}$ is its inverse. Furthermore, using the fact that every element of $X_K(L)$ is the ratio of two elements of $\mathcal{O}_{X_K(L)}$, one sees easily that this extends to a bijection between $X_K(L)$ and the field of fractions of $A_K(L)$. □

Remark 6.2.13. Instead of taking the inverse limit over all finite extensions of L/K, we can take the inverse limit over any increasing sequence K_i/K such that $L = \bigcup_i K_i$. In particular, suppose K_i is the fixed field of $G_L G_K^i$. Let $N_i = i_{L/K_i}$. Let $s(K_i) = s_i$ be any strictly increasing sequence of natural numbers such that $ps_i = (p-1)N_i$. Let $i, j \in \mathbb{N}$ be such that $j > i$. Then the maps $\mathcal{O}_{K_j}/\mathfrak{m}_{K_j}^{s_j} \to \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{s_i}$ induced by the norm N_{K_j/K_i} are well-defined surjective ring homomorphisms by 6.2.6. By a cofinality argument $A_K(L) = \varprojlim \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{s_i}$. By 6.2.12 $X_K(L)$ if the field of fractions of $\varprojlim \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{s_i}$. It is this description of $X_K(L)$ that we will use in chapter 7 to link

Wintenberger's theorem with Deligne's.

Corollary 6.2.14. *If L/K is an infinite APF extension, then $X_K(L)$ is a local field, in which the addition is given by* $(x+y)_F = \lim_{E\in\mathcal{E}_{L/F}} N_{E/F}(x_E + y_E)$.

According to Proposition 7.3.1, part (c) of Theorem 6.2.12 states that $X_K(L)$ is the limit of the finite subextensions of L/K in the sense of the discussion preceding 7.3.1. It is worth noting that we could have proven part (a) of this theorem simply by appealing to 7.3.1.

6.3 Galois theory of norm fields

In this subsection, we will study separable extensions of $X_K(L)$. The first step in this direction is to show that if M/L is finite and separable, then $X_K(M)$ is an extension of $X_K(L)$.

Remark 6.3.1 ([2, 3.1.1]). Let L/K be infinite APF, and let $\tau : L \to L'$ be a finite separable embedding. Let $\mathcal{E}'_\tau$ be the family of finite extensions E/K such that τL and E are linearly disjoint, and have compositum equal to L'. One can verify that this is cofinal in $\mathcal{E}_{L'/K}$, so can be used in place of $\mathcal{E}_{L'/K}$ to define the norm field. Then we can define a map $X_K(\tau) : X_K(L) \to X_K(L')$ by $(X_K(\tau)(x))_E = \tau x_{\tau^{-1}E}$ for $E \in \mathcal{E}'_\tau$. To check that the result gives an element of $X_K(L')$, one uses the fact that $N_{E/F}(\tau\alpha) = \tau N_{\tau^{-1}E/\tau^{-1}F}$ for any $E, F \in \mathcal{E}'_\tau$ such that $F \subseteq E$. It can be shown that $X_K(\sigma\tau) = X_K(\sigma)X_K(\tau)$.

Lemma 6.3.2 ([2, 3.1.3.1]). *If L'/L is finite and Galois, then $Gal(L'/L)$ acts faithfully on $X_K(L')$.*

Proof. Let $\sigma \in Gal(L'/L)$ act trivially on $X_K(L')$, i.e. $X_K(\sigma) = 1$. Using the fact that Galois extensions are cofinal in $\mathcal{E}_{L'/K}$, one readily checks that the action of σ and that of $X_K(\sigma)$ on the residue field of L' are identified by the correspondence in Theorem 6.2.12b. In particular, σ acts trivially on this residue field. Let $E' \in \mathcal{E}'_\tau$ be Galois and contain the maximal unramified subextension of L'/K. Let $\pi \in X_K(L')$ be a uniformizer. Then $\sigma\pi = \pi$, so $\sigma\pi_{E'} = \pi_{E'}$. Since σ acts trivially on the residue field of $E' \subseteq L'$ and on a uniformizer, it acts trivially on E'. But the collection of such E' is cofinal, so σ is trivial on all of L'. □

The following result shows that the extension $X_K(M)/X_K(L)$ is very similar to M/L.

Corollary 6.3.3 ([2, 3.1.2]). *(a) If M/L is finite and separable, then $X_K(M)/X_K(L)$ is separable and has the same degree.*

(b)If in addition M/L is Galois, then $X_K(M)/X_K(L)$ is Galois and $\mathrm{Gal}(M/L) \cong \mathrm{Gal}(X_K(M)/X_K(L))$.

Proof. Suppose M/L is Galois. It is easy to check that the fixed field of $\mathrm{Gal}(M/L)$ on $X_K(M)$ is $X_K(L)$. This together with lemma 6.3.2 shows (b). To see $X_K(M)/X_K(L)$ is separable of degree $[M : L]$, we apply (b) to M'/M and M'/L, where M'/L is the Galois closure of M. □

Definition 6.3.4. Let L'/L be any separable extension of an infinite APF extension L/K. Then we can define $X_{L/K}(L')$ as the direct limit of the fields $X_K(E)$, where E runs through the intermediate extensions $L \subseteq E \subseteq E'$ which are finite over L.

Remark 6.3.5. By 6.3.3, $X_{L/K}(M)$ is separable. If $\tau : L' \to L''$ is a separable embedding, then the maps from Remark 6.3.1 induce a map $X_{L/K}(\tau) : X_{L/K}(L') \to X_{L/K}(L'')$. $X_{L/K}$ is then a functor from the category of separable extensions of L to that of $X_K(L)$. If L'/L is finite, then clearly $X_K(L') = X_{L/K}(L')$.

Proposition 6.3.6 ([4, III.5.6])**.** *$X_{L/K}$ is fully faithful.*

Proof. Let L'/L be finite and Galois. by Lemma 6.3.2, we can embed $\mathrm{Gal}(L'/L)$ in $\mathrm{Gal}(X_{L/K}(L')/X_K(L))$. By computing the fixed field of $\mathrm{Gal}(L'/L)$ on $X_{L/K}(L')$, one sees that this is an isomorphism. From this, one can deduce the corresponding fact for infinite Galois extensions of L. To show $\mathrm{Hom}(L', L'') \cong \mathrm{Hom}(X_{L/K}(L'), X_{L/K}(L''))$, one uses the fundamental theorem of Galois theory to express the Hom sets in terms of Galois groups. □

Theorem 6.3.7 ([2, 3.2.5])**.** *$X_{L/K}$ is an equivalence of categories.*

Proof. It suffices to show $X_{L/K}$ is essentially surjective. This is proven in [2, 3.2.5]. □

Corollary 6.3.8. *The categories of finite separable extensions of L and $X_K(L)$ are equivalent.*

6.4 Relation between norm fields and perfect norm fields

We will now explore the relation between the norm field, and the perfect norm field. First we will state some results of Wintenberger, which allow us to embed the norm field inside a perfect norm field. We will then outline the construction of,[9] in which the norm field of a totally ramified $\mathbb{Z}_p$ extension is constructed from the perfect norm field.

We will let $\hat{L}$ denote the completion of a valued field L. We assume L/K is infinite APF and totally wildly ramified, and that K has characteristic 0. We let $\mathcal{E}_n$ be the subposet of $\mathcal{E}_{L/K}$ consisting of extensions of degree divisible by p^n. Given an element $\alpha \in X_K(L)$ we let $\alpha_E \in E$ denote the component corresponding to a subfield E.

Theorem 6.4.1 ([2, 4.2.1])**.** *Let $\alpha \in X_K(L)$. Then $\lim_{E \in \mathcal{E}_n} \alpha_E^{p^{-n}[E:K]}$ converges in $\hat{L}$. If we let x_n denote the limit, then the family of $x_n \in \hat{L}$ defines an element of $R_{\hat{L}}$. This construction defines a continuous embedding $X_K(L) \to R(\hat{L})$.*

Henceforth, we assume that L is a $\mathbb{Z}_p$ extension in addition to the properties above. We let F/K be a finite extension, and $F_n = FK_n$. Let $M = FK_\infty$.

Definition 6.4.2 ([9, 13.3.3])**.** We define $\mathbb{E}_M^+$ to be the set of sequences $x_n \in \hat{M}$ such that $x_n^p = x_{n+1}$ and such that $x_n \in \mathcal{O}_{F_n}$ for large n.

Then according to [9, 13.3.5], the field of fractions of $\mathbb{E}_M^+$ is the norm field associated to M/K. We will let ϕ denote the p-th power map and $\phi^{-\infty}(\mathbb{E}_M^+) = \{x \in R_{\hat{M}} \mid \exists k. \phi^k(x) \in \mathbb{E}_M^+\}$.

Proposition 6.4.3 ([9, 13.3.11])**.** *$\phi^{-\infty}(\mathbb{E}_M^+)$ is dense in $R_{\hat{M}}$.*

In fact, Wintenberger proves in [2, 4.3.4] that this holds for any infinite APF extension M/K.

Chapter 7

A link between the theories of Wintenberger and Deligne

Let L/K be an infinite APF extension as defined by 6.2.1. Let $X_K(L)$ be the norm field of section 6. Rather than using the standard description of $X_K(L)$, it is more convenient for use to use the description given in 6.2.13. Our goal is to give a new proof of 6.3.8 without using the results of 6.3. Since $X_K(L)$ is defined, not directly in terms of L, but in terms of its finite subextensions, it is natural to prove this by relating extensions of both L and $X_K(L)$ with those of a suitable sequence of finite subextensions of L/K.

In sections 7.1 and 7.2, we will use the ramification filtration to prove that finite separable extensions of L with a given bound on their ramification are equivalent to finite separable extensions of a suitable subextension K_i/K with the same bound on ramification. The argument essentially reduces to the case where $K_i = K$ has ramification bounded below by i. The key to comparing extensions of K_i and those of L is the linear disjointness provided by 7.1.4.[1]

In section 7.3, we will use Deligne's theory, which is described in section 4, to show that the finite separable extensions of K_i with an appropriate bound on ramification correspond to extensions of $X_K(L)$ with the same bound on ramification.[2] Combining these results will show that extensions of L with a bound on ramification correspond to extensions of $X_K(L)$ with the same ramification bound. This equivalence is not obviously canonical, however; It appears to depend on the choice of the subextension K_i.

In section 7.4, we will give an explicit description of the extension of $X_K(L)$ corresponding to a given extension of L for large values of i. In particular, the fact that this description does not depend on the choice of i will allow us to provide an equivalence of categories between finite separable extensions of L and those of $X_K(L)$ without needing to impose a bound on ramification.

Throughout this paper the absolute Galois group of a field K will be denoted G_K. We will define the upper and lower ramification filtrations and the function $\psi_{L/K}$ as in Chapter IV of[1]

[1] In particular, this result requires us to work with extensions of L with bounded ramification, rather than arbitrary extensions.

[2] We also need to bound the ramification of the extensions, because Deligne's theory deals with a category of extensions with a bound on their ramification.

7.1 Some results in ramification theory

If K is a field, we will denote the absolute Galois group of K by G_K. The u-th step in the upper ramification filtration on $\mathrm{Gal}(L/K)$ or G_K will be denoted $\mathrm{Gal}(L/K)^u$ or G_K^u.

Definition 7.1.1. [2]Let K be a local field. For a totally ramified APF extension L/K, we define $\psi_{L/K}(t) = \int_0^u [G_K : G_L G_K^u]du$. We define $\phi_{L/K}$ to be the inverse function. We define $G_L^u = G_L \cap G_K^{\phi_{L/K}(u)}$. For a Galois extension M/L, we define $\mathrm{Gal}(M/L)^u$ to be the image of G_L^u in $\mathrm{Gal}(M/L)$.

Remark 7.1.2. Let L/K be a totally ramified APF extension. Let E/K be a finite subextension of L/K. Then the definition of G_L^u can be easily verified to be the same if we replace L/K with L/E, since $G_K^{\phi_{E/K}(v)} \cap G_E = G_E^v$ for all v.

In what follows K may be either a local field or an APF extension of a local field, unless otherwise specified. The remainder of this section will be devoted to studying bounds on ramification in the sense of Definition 2.0.18.

Lemma 7.1.3. *Let L/K and E/K have ramification bounded above by u. Then LE/K has ramification bounded above by u.*

Proof. $G_K^u \subseteq G_L$ and $G_K^u \subseteq G_E$ so $G_K^u \subseteq G_E \cap G_L = G_{LE}$. ☐

Proposition 7.1.4. *Let L/K be have ramification bounded below by u. Let E/K have ramification bounded above by u. Then L and E are linearly disjoint.*

Proof. Let $\tilde{E}/K$ be the Galois closure of E. It suffices to show L/K and $\tilde{E}/K$ are linearly disjoint. For this, it suffices to show that $L \cap \tilde{E} = K$. We know that $G_K^u \subseteq G_L$ and $G_K^u G_{\tilde{E}} = G_K$. Hence $G_K \subseteq G_L G_{\tilde{E}}$ so $L \cap \tilde{E} \subseteq K$. The reverse inclusion is trivial. □

Lemma 7.1.5. *Let L/K be an APF extension of a local field with ramification bounded below by $u > 0$. Let E/K be finite and have ramification bounded above by u. Then LE/L has ramification bounded above by u. In addition, LE/E has ramification bounded below by u.*

Proof. $\psi_{L/K}(t) = \displaystyle\int_0^t [G_K : G_L G_K^v] dv$, and for $v \leq u$, the integrand is 1. Hence $\psi_{L/K}(t) = t$ for $t \leq u$, and so $\phi_{L/K}$ has this property as well. $G_L^u = G_L \cap G_K^{\phi_{L/K}(u)} = G_L \cap G_K^u$.

Since $G_K^u \subseteq G_E$, $G_L^u \subseteq G_L \cap G_E = G_{LE}$, and so LE/L has ramification bounded above by u.

We will show that LE/L has ramification bounded below by $\psi_{E/K}(u) \geq u$. Since $G_K^u \subseteq G_E$, $G_L G_E^{\psi_{E/K}(u)} = G_L(G_E \cap G_K^u) = G_L G_K^u = G_K$. Hence $G_E \subseteq G_L G_E^{\psi_{E/K}(u)}$, so $G_E \subseteq G_E^{\psi_{E/K}(u)}(G_E \cap G_L) = G_E^{\psi_{E/K}(u)} G_{LE}$, so EL/E has ramification bounded below by $\psi_{E/K}(u)$. □

7.2 Moderately ramified extensions of APF extensions

Until otherwise noted, L/K will denote an APF extension with ramification bounded below by $u > 0$. We fix an algebraic closure of K, and an embedding of L into this algebraic closure. Our goal is to show that $\mathcal{C}_K^u \cong \mathcal{C}_L^u$.

Proposition 7.2.1. *There is a functor* $\mathbf{V} : \mathcal{C}_K^u \to \mathcal{C}_L^u$ *sending an extension* E/K *to* EL/L*, and sending a morphism of extensions* $E \to E'$ *into the corresponding morphism* $LE \to LE'$*.*

Proof. Let $E \in \mathcal{C}_K^u$. By 7.1.5, $LE \in \mathcal{C}_L^u$. If $E \to E'$ is a morphism in $\mathcal{C}_K^u$, then by 7.1.4, E/K and E'/K are each linearly disjoint to L/K. Then we get a morphism $LE \cong L \otimes_K E \to L \otimes_K E' \cong LE'$, so the inclusion $LE \subseteq LE'$ makes sense. This clearly preserves composition. □

Lemma 7.2.2. $\mathbf{V}$ *is faithful.*

Proof. Suppose two inclusions $E \to E'$ induce the same inclusion $LE \to LE'$. Then the two inclusions are both given by restricting the codomain on the composite $E \to LE \to LE'$ to E', so they must be equal. □

Lemma 7.2.3. $\mathbf{V}$ *is full.*

Proof. Let $M, M' \in \mathcal{C}_L^u$ with $M \subseteq M'$, and suppose $M = LF$ and $M' = LF'$ for some $F, F' \in \mathcal{C}_K^u$. We have $F = K(\alpha)$ and $F' = K(\beta)$ for some α and β. Then

$L(\alpha) = M \subseteq M' = L(\beta)$ so $LF' = L(\beta) = L(\alpha, \beta) = LFF'$. By 7.1.3, FF'/K has ramification bounded by u, so by 7.1.4, F' and FF' are linearly disjoint from L/K. Thus $[FF' : F'] = [LFF' : LF'] = 1$, so $F' = FF'$ and hence $F \subseteq F'$. Clearly this inclusion induces the original inclusion $M \subseteq M'$. This deals with the case where the given map $M \to M'$ is an inclusion. In general it is the composite of an inclusion and an isomorphism $\sigma : \sigma^{-1}M' \to M'$ for $\sigma \in G_L \subseteq G_K$. But this isomorphism is induced by $\sigma : \sigma^{-1}F' \to F$. □

Lemma 7.2.4. **V** *is essentially surjective.*

Proof. Let $M \in \mathcal{C}_L^u$. Then $G_L^u \subseteq G_M$. Since M/L is finite and separable, we have $M = L(\alpha)$ where α is algebraic over K. Let E be the fixed field of $G_M G_K^u$. As in the proof of 7.1.5, $\phi_{L/K}(u) = u$. Then $G_L^u = G_L \cap G_K^{\phi_{L/K}(u)} = G_L \cap G_K^u$. $G_E \cap G_L = G_M G_K^u \cap G_L = G_M(G_K^u \cap G_L) = G_M(G_L^u) = G_M$, so $M = LE = \mathbf{V}(E)$. Hence **V** is essentially surjective. □

The above lemmas immediately imply the following.

Theorem 7.2.5. *Let $u > 0$. Let L/K be an APF extension with ramification bounded below by u. Then $\mathbf{V} : \mathcal{C}_K^u \to \mathcal{C}_L^u$ is an equivalence of categories.*

Corollary 7.2.6. *Let $u > 0$. Let L/K be any APF extension. Let K_u be the fixed subfield of $G_L G_K^u$. Then the categories $\mathcal{C}_{K_u}^v$ and $\mathcal{C}_L^v$ are equivalent for any $v \leq u$.*

Proof. I claim that L/K_u has ramification bounded below by v, that is $G_{K_u}^v G_L = G_{K_u}$. Note that $G_{K_u}^v = G_{K_u} \cap G_K^{\phi_{K_u/K}(v)} = G_L G_K^u \cap G_K^{\phi_{K_u/K}(v)}$. If $v \leq u$, then $\phi_{K_u/K}(v) \leq$

$v \leq u$, so $G^v_{K_u} \supseteq G_L G^u_K \cap G^u_K = G^u_K$. Then $G^v_{K_u} G_L \supseteq G^u_K G_L = G_{K_u}$. The reverse inclusion is trival, so the claim holds. Now we can simply apply the previous theorem to L/K_u. □

7.3 An application of Deligne's theory to norm fields

Proposition 7.3.1. *Let u_i be a nondecreasing sequence of integers which tends to infinity. Let K_i be a sequence of local fields. Suppose that for each i, we are given a surjective homomorphism $\theta_i : \mathcal{O}_{K_{i+1}}/\mathfrak{m}^{u_{i+1}}_{K_{i+1}} \to \mathcal{O}_{K_i}/\mathfrak{m}^{u_i}_{K_i}$. Let $K = \mathrm{Frac}(\varprojlim \mathcal{O}_{K_i}/\mathfrak{m}^{u_i}_{K_i})$. Then K is a local field, and $\mathcal{O}_{K_i}/\mathfrak{m}^{u_i}_{K_i} \cong \mathcal{O}_K/\mathfrak{m}^{u_i}_K$ for all i. Furthermore $\mathrm{Tr}_{u_i-1}(K) \cong \mathrm{Tr}_{u_i-1}(K_i)$.*

Proof. Let $\mathcal{O}_K = \varprojlim \mathcal{O}_{K_i}/\mathfrak{m}^{u_i}_{K_i}$. For the first part of the proposition, it suffices to show $\mathcal{O}_K$ is a complete DVR. It is clearly a ring. Let v_i be the valuation on the truncated DVR $\mathcal{O}_{K_i}/\mathfrak{m}^{u_i}_{K_i}$. For $\alpha \in \mathcal{O}_K$, let α_i be its component in $\mathcal{O}_{K_i}/\mathfrak{m}^{u_i}_{K_i}$. I claim that $v_i(\alpha_i) = v_{i+1}(\alpha_{i+1})$ for large i. Write $\alpha_i = u_i \pi_i^{v_i(\alpha_i)}$, where π_i is a uniformizer of $\mathcal{O}_{K_i}/\mathfrak{m}^{u_i}_{K_i}$. Then $\theta_i(\alpha_{i+1}) = \theta_i(u_{i+1})\theta_i(\pi_{i+1})^{v_{i+1}(\alpha_{i+1})}$. Since θ_i is a surjective homomorphism of local rings, $\theta_i(u_{i+1})$ is a unit and $\theta_i(\pi_{i+1})$ is a uniformizer. In particular, if $\alpha_i = \theta_i(\alpha_{i+1})$ is nonzero, then $v_i(\alpha_i) = v_{i+1}(\alpha_{i+1})$. If $\alpha \neq 0$, then this proves the claim. If $\alpha = 0$, then the claim is trivial. Note furthermore that $v_i(\alpha_i) = v_{i+1}(\alpha_{i+1})$

holds unless $\alpha_i = 0$, in which case we still have $v_i(\alpha_i) \geq v_{i+1}(\alpha_{i+1})$.

We define $v(\alpha)$ to be the limiting value of $v_i(\alpha_i)$. Then $v_i(\alpha_i) \geq v(\alpha)$ for all i. If $\alpha, \beta \in \mathcal{O}_K$, then $v_i(\alpha_i\beta_i) = v_i(\alpha_i) + v_i(\beta_i)$, as long as $v_i(\alpha_i) + v_i(\beta_i) < u_i$. Taking the limit shows that $v(\alpha\beta) = v(\alpha) + v(\beta)$ when $v(\alpha) + v(\beta) < \infty$. The other properties of a discrete valuation are proven similarly. Let $\{\alpha^{(k)}\}$ denote a Cauchy sequence in $\mathcal{O}_K$. Let N be a natural number. Then $v(\alpha^{(k)} - \alpha^{(l)}) > N$ for large k and l. Thus $v_i(\alpha_i^{(k)} - \alpha_i^{(l)}) \geq v(\alpha^{(k)} - \alpha^{(l)} > N$ when k, and l are large. Since $\mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{u_i}$ is complete, $\lim\limits_{k\to\infty} \alpha_i^{(k)}$ exists, and will be denoted α_i. Since θ_i is continuous, $\theta_i(\alpha_{i+1}) = \alpha_i$, so the α_i define an element $\alpha \in \mathcal{O}_K$. It is easy to see this is the limit of the given Cauchy sequence, and so $\mathcal{O}_K$ is a complete DVR.

Let $n \in \mathbb{N}$. It is easy to see that $\mathfrak{m}_K^n = \varprojlim \mathfrak{m}_{K_i}^{\min(u_i,n)}/\mathfrak{m}_{K_i}^{u_i}$. I claim that $\varprojlim^1 \mathfrak{m}_{K_i}^{\min(u_i,n)}/\mathfrak{m}_{K_i}^{u_i} = 0$. Without loss of generality, I will assume $u_i > n$ for all i. Let $\theta_{i,j} : \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{u_i} \to \mathcal{O}_{K_j}/\mathfrak{m}_{K_j}^{u_j}$ for $i > j$ be the maps induced by the sequence $\{\theta_k\}$. By the Mittag-Leffler condition, the claim reduces to showing that for all k, there exists $j \geq k$ such that for $i \geq j$, $\theta_{i,k}(\mathfrak{m}_{K_i}^n/\mathfrak{m}_{K_i}^{u_i}) = \theta_{j,k}(\mathfrak{m}_{K_j}^n/\mathfrak{m}_{K_j}^{u_j})$. But both are generated by the image of $\pi_{K_k}^n$, so the claim holds. Then by the long exact sequence, $\mathcal{O}_K/\mathfrak{m}_K^n \cong \varprojlim \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{\min(u_i,n)}$.

If $n = u_j - 1$, it is easy to see that all but finitely many terms in this limit are isomorphic (under the maps induced by the θ_i) to $\mathcal{O}_{K_j}/\mathfrak{m}_{K_j}^{u_j-1}$. Hence $\mathcal{O}_{K_j}/\mathfrak{m}_{K_j}^{u_j-1} \cong \mathcal{O}_K/\mathfrak{m}_K^{u_j-1}$, under the map induced by the projection $\mathcal{O}_K \to \mathcal{O}_{K_j}/\mathfrak{m}_{K_j}^{u_j}$. The isomorphism $\mathcal{O}_K/\mathfrak{m}_K^{u_j-1} \to \mathcal{O}_{K_j}/\mathfrak{m}_{K_j}^{u_j-1}$ will be denoted ϕ.

Using the same vanishing result on $\varprojlim^1$, $\mathfrak{m}_K/\mathfrak{m}_K^{n+1} \cong \varprojlim \mathfrak{m}_{K_i}/\mathfrak{m}_{K_i}^{\min(u_i,n+1)}$. Taking $n = u_j - 1$, we get $\mathfrak{m}_K/\mathfrak{m}_K^{u_j} \cong \varprojlim \mathfrak{m}_{K_i}/\mathfrak{m}_{K_i}^{\min(u_i,u_j)}$. Since the maps θ_i provide isomorphisms $\mathfrak{m}_{K_i}/\mathfrak{m}_{K_i}^{u_j} \cong \mathfrak{m}_{K_j}/\mathfrak{m}_{K_j}^{u_j}$, the inverse limit is $\mathfrak{m}_{K_j}/\mathfrak{m}_{K_j}^{u_j}$. Hence $\mathfrak{m}_K/\mathfrak{m}_K^{u_j} \cong \mathfrak{m}_{K_j}/\mathfrak{m}_{K_j}^{u_j}$ under the map η induced by the projection $\mathfrak{m}_K \to \mathfrak{m}_{K_j}/\mathfrak{m}_{K_j}^{u_j}$. One checks that $(1, \phi, \eta)$ is an isomorphism of triples. □

Let L/K be an infinite APF extension. Let K_i be the fixed field of $G_L G_K^i$. By 6.2.13, there is an increasing sequence of natural numbers $s_i \to \infty$ such that the norm maps induce surjective homomorphisms $\theta_i : \mathcal{O}_{K_{i+1}}/\mathfrak{m}_{K_{i+1}}^{s_{i+1}} \to \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{s_i}$. Furthermore, $X_K(L) = \mathrm{Frac}(\varprojlim \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{s_i})$. By 7.3.1, $\mathrm{Tr}_{s_i-1}(X_K(L)) \cong \mathrm{Tr}_{s_i-1}(K_i)$. Deligne's theorem gives the following.

Proposition 7.3.2. *Let $i > 0$. Let $v < s_i - 1$. Then $\mathcal{C}^v_{X_K(L)}$ and $\mathcal{C}^v_{K_i}$ are equivalent.*

Combining this with 7.2.6 and picking i large enough that $i > v$ and $s_i - 1 > v$ gives the following.

Theorem 7.3.3. *Let $v > 0$. Then $\mathcal{C}^v_{X_K(L)}$ and $\mathcal{C}^v_L$ are equivalent.*

7.4 An explicit description of the equivalence

Throughout this section we will use the following notation. Let $R \geq 1$ be a large fixed natural number. Let L/K be infinite APF. Let M/L be a finite separable extension. Let K_u be the fixed field of $G_L G_K^u$ and let K'_u be the fixed field of $G_M G_K^u$. We will soon see that the ramification index of K'_u/K_u is independent of u. We will denote the common value by r and, unless otherwise specified, will only consider extensions M/L such that $r \leq R$. We will define s_i to be any nondecreasing sequence s_i which tends to infinity such that $ps_i \leq pRs_i \leq (p-1)b_i$ where b_i is a lower bound on the ramification filtration of L/K_i, and where p is the residue characteristic. Then by footnote 6.2.13, the norm maps induce surjective homomorphisms $\mathcal{O}_{K_{i+1}}/\mathfrak{m}_{K_{i+1}}^{s_{i+1}} \to \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{s_i}$. We will soon see that the norm maps induce surjective homomorphisms $\mathcal{O}_{K'_{i+1}}/\mathfrak{m}_{K'_{i+1}}^{r(s_{i+1})} \to \mathcal{O}_{K'_i}/\mathfrak{m}_{K'_i}^{r(s_i)}$. If $\iota : L \to M$ denotes the embedding, then we define $X_K(\iota) : X_K(L) = \mathrm{Frac}(\varprojlim \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{s_i}) \to \mathrm{Frac}(\varprojlim \mathcal{O}_{K'_i}/\mathfrak{m}_{K'_i}^{r(s_i)}) = X_K(M)$ to be the map induced by the embeddings $\iota|_{K_i} : K_i \to K'_i$[3]. Similarly, for $\sigma \in G_L$, we let $X_K(\sigma) : X_K(M) \to X_K(\sigma M)$ be induced by $\sigma : K'_i \to \sigma K'_i$, which is well defined since the Galois action commutes with norm maps.

Lemma 7.4.1. *If M/L has ramification bounded above by u, then so does K'_i/K_i for $i \geq u$. In particular, K'_i/K_i and L/K_i are linearly disjoint, and the ramification index of K'_i/K_i is independent of i for $i \geq u$.*

Proof. We have $G_L^u \subseteq G_M$. Then $G_{K'_i} = G_M G_K^i \supseteq G_L^u G_K^i = (G_L \cap G_K^{\phi_{L/K}(u)}) G_K^i$. In addition, $G_{K_i}^u = G_K^{\phi_{K_i/K}(u)} \cap G_{K_i}$. Since $\phi_{K_i/K}(u) \geq \phi_{L/K}(u)$, we have $G_{K_i}^u \subseteq$

[3]The map $\varprojlim \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{s_i} \to \varprojlim \mathcal{O}_{K'_i}/\mathfrak{m}_{K'_i}^{r(s_i)}$ is well-defined by 7.4.2. The map $\mathrm{Frac}(\varprojlim \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{s_i}) \to \mathrm{Frac}(\varprojlim \mathcal{O}_{K'_i}/\mathfrak{m}_{K'_i}^{r(s_i)})$ is well defined because $\varprojlim \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{s_i} \to \varprojlim \mathcal{O}_{K'_i}/\mathfrak{m}_{K'_i}^{r(s_i-1)}$ is injective, which follows from the fact that each $\mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{s_i} \to \mathcal{O}_{K'_i}/\mathfrak{m}_{K'_i}^{r(s_i)}$ is injective.

$G_{K_i} \cap G_K^{\phi_{L/K}(u)} = G_L G_K^i \cap G_K^{\phi_{L/K}(u)}$. If $i \geq \phi_{L/K}(u)$, then $G_L G_K^i \cap G_K^{\phi_{L/K}(u)} = (G_L \cap G_K^{\phi_{L/K}(u)}) G_K^i$.[4] Hence $G_{K_i}^u \subseteq (G_L \cap G_K^{\phi_{L/K}(u)}) G_K^i \subseteq G_{K_i'}$ so the ramification of K_i'/K_i is bounded above by u. The linear disjointness follows from the fact that the ramification of L/K_i is bounded below by i, and hence by u if $i \geq u$.

□

Lemma 7.4.2. *The map* $\varprojlim \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{s_i} \to \varprojlim \mathcal{O}_{K_i'}/\mathfrak{m}_{K_i'}^{r(s_i)}$ *is well defined.*

Proof. It suffices to show that the inclusions $\mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{s_i} \to \varprojlim \mathcal{O}_{K_i'}/\mathfrak{m}_{K_i'}^{r(s_i)}$ form a morphism of projective systems; i.e. they are compatible with the norm maps. By a cofinality argument it suffices to show this for large i. But then 7.4.1 shows that K_i'/K_i and K_j/K_i are linearly disjoint for $i > j$, and the result follows from the standard result that in this case $N_{K_j K_i'/K_i'}(x) = N_{K_j/K_i}(x)$ for $x \in K_j$.

□

Lemma 7.4.3. *In the setting introduced above, the norm maps induce surjective homomorphisms* $\mathcal{O}_{K_{i+1}'}/\mathfrak{m}_{K_{i+1}'}^{r(s_{i+1})} \to \mathcal{O}_{K_i'}/\mathfrak{m}_{K_i'}^{r(s_i)}$.

Proof. By 7.1.5, M/K_i' has ramification bounded below by b_i. Since $prs_i \leq (p-1)b_i$, the result follows from Remark 6.2.13. □

Lemma 7.4.4. *Let v be such that M/L has ramification bounded above by v. Let i be large enough that $v < \min(s_i - 1, i)$. Let r be the ramification index of K_i'/K_i.*

[4] More generally if G is a group and H, K, N are subgroups with $H \subseteq K$, then $NH \cap K = (N \cap K)H$.

Suppose $r \leq R$. The map $X_K(\iota)$ induces a well-defined morphism $\mathrm{Tr}_v(X_K(L)) \to \mathrm{Tr}_{rv}(X_K(M))$. *In addition, the following diagram commutes.*

$$\begin{array}{ccc} \mathrm{Tr}_{rv}(X_K(M)) & \xrightarrow{\sim} & \mathrm{Tr}_{rv}(K_i') \\ {\scriptstyle X_K(\iota)^*}\uparrow & & {\scriptstyle \iota^*}\uparrow \\ \mathrm{Tr}_v(X_K(L)) & \xrightarrow{\sim} & \mathrm{Tr}_v(K_i) \end{array}$$

Proof. First we check that the following diagram of truncated DVRs commutes.

$$\begin{array}{ccc} \mathcal{O}_{X_K(M)}/\mathfrak{m}_{X_K(M)}^{rv} & \xrightarrow{\sim} & \mathcal{O}_{K_i'}/\mathfrak{m}_{K_i'}^{rv} \\ {\scriptstyle X_K(\iota)^*}\uparrow & & {\scriptstyle \iota^*}\uparrow \\ \mathcal{O}_{X_K(L)}/\mathfrak{m}_{X_K(L)}^{v} & \xrightarrow{\sim} & \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^{v} \end{array}$$

Let $x \in \mathcal{O}_{X_K(L)} = \varprojlim \mathcal{O}_{K_j}/\mathfrak{m}_{K_j}^{s_j}$ with components $x_j \in \mathcal{O}_{K_j}/\mathfrak{m}_{K_j}^{s_j}$. Let $\tilde{x}_j \in \mathcal{O}_{K_j}$ be a lift of x_j. The bottom arrow of the diagram sends the class of x to the class of $\tilde{x}_i$; this class gets mapped to the class of $\iota(\tilde{x}_i)$ by the right arrow. Let $y \in \mathcal{O}_{X_K(M)}$ be the element whose components $y_j \in \mathcal{O}_{K_j'}/\mathfrak{m}_{K_j'}^{s_j}$ are the classes of the elements $\tilde{y}_j = \iota(\tilde{x}_j)$. Then by definition the left arrow sends the class of x to that of y, which gets mapped by the top arrow to the class of $\tilde{y}_i$. Since $\tilde{y}_i = \iota(\tilde{x}_i)$, the diagram of truncated DVRs commutes. A similar argument shows that the diagram of free rank 1 modules commutes. Hence the diagram of triples commutes. The fact that $\mathrm{Tr}_v(X_K(L)) \to \mathrm{Tr}_{rv}(X_K(M))$ is well-defined can be seen by viewing it as a composition of other morphisms in the diagram. □

We now prove a state a similar but easier result for the Galois action.

Lemma 7.4.5. *Let v be such that M/L has ramification bounded above by v. Let i be large enough that $v < \min(s_i - 1, i)$. Let r be the ramification index of K_i'/K_i. Suppose $r \leq R$. Let $\sigma \in G_L$. The map $X_K(\sigma)$ induces a well-defined morphism*

$\mathrm{Tr}_{rv}(X_K(M)) \to \mathrm{Tr}_{rv}(X_K(\sigma M))$. *In addition, the following diagram commutes.*

$$\begin{array}{ccc} \mathrm{Tr}_{rv}(X_K(\sigma M)) & \xrightarrow{\sim} & \mathrm{Tr}_{rv}(\sigma K_i') \\ {\scriptstyle X_K(\sigma)^*}\uparrow & & {\scriptstyle \sigma^*}\uparrow \\ \mathrm{Tr}_{rv}(X_K(M)) & \xrightarrow{\sim} & \mathrm{Tr}_{rv}(K_i') \end{array}$$

Proof. The proof follows the strategy of 7.4.4. □

Lemma 7.4.6. *Let v be such that M/L has ramification bounded above by v. Let $i \geq v$. Then $K_i'L = M$.*

Proof. Since M/L has ramification bounded by v, we have $G_L^v = G_L \cap G_K^{\phi_{L/K}(v)} \subseteq G_M$. Since $i \geq v \geq \phi_{L/K}(v)$, $G_L \cap G_K^i \subseteq G_L \cap G_K^{\phi_{L/K}(v)} \subseteq G_M$. Hence $G_L \cap G_{K_i'} = G_L \cap G_M G_K^i = G_M(G_L \cap G_K^i) = G_M$. Since $K_i'L$ is the fixed field of the left side, the result follows.

□

Theorem 7.4.7. *Let M/L be a finite separable extension with ramification bounded by v and ramification index bounded by R. Choose i such that $v < \min(s_i - 1, i)$. Then the extension M/L corresponds to the extension $X_K(M)/X_K(L)$ given by $X_K(\iota)$ under the correspondence of 7.3.3. Let M'/L be another such extension and $\tau : M \to M'$. Then τ corresponds to $X_K(\tau) : X_K(M) \to X_K(M')$ under 7.3.3.*

Proof. We know that K_i'/K_i has ramification bounded above by v, so the functor $\mathcal{C}_{K_i}^v \to \mathcal{C}_L^v$ sends K_i' to $LK_i' = M$. Determining what M corresponds to under $\mathcal{C}_L^v \to \mathcal{C}_{X_K(L)}^v$ then reduces to determining what K_i' corresponds to under $\mathcal{C}_{K_i}^v \to \mathcal{C}_{X_K(L)}^v$. But using the diagram of triples of 7.4.4 shows that K_i' corresponds to $X_K(M)$.

Suppose K_i'' is the fixed field of $G_{M'}G_K^i$, and e is the ramification index of $M \to M'$. The second part is proven in a similar manner to the first, using the following diagram. The top square follows by writing τ as the composition of an inclusion and an element of the Galois group, and applying 7.4.4 and 7.4.5.

$$\begin{array}{ccc}
\mathcal{O}_{X_K(M')}/\mathfrak{m}^{rev}_{X_K(M')} & \xrightarrow{\sim} & \mathcal{O}_{K_i''}/\mathfrak{m}^{rev}_{K_i''} \\
{\scriptstyle X_K(\tau)^*}\uparrow & & \uparrow{\scriptstyle \tau^*} \\
\mathcal{O}_{X_K(M)}/\mathfrak{m}^{rv}_{X_K(M)} & \xrightarrow{\sim} & \mathcal{O}_{K_i'}/\mathfrak{m}^{rv}_{K_i'} \\
{\scriptstyle X_K(\iota)^*}\uparrow & & \uparrow{\scriptstyle \iota^*} \\
\mathcal{O}_{X_K(L)}/\mathfrak{m}^{v}_{X_K(L)} & \xrightarrow{\sim} & \mathcal{O}_{K_i}/\mathfrak{m}^{v}_{K_i}
\end{array}$$

□

Theorem 7.4.8. *The functor X_K provides an equivalence of categories between finite separable extensions of L and those of $X_K(L)$.*

Proof. First we prove it is faithful. Let $\tau, \tau' : M \to M'$ be such that $X_K(\tau) = X_K(\tau')$. Let v be a bound on the ramification of M and M'. Since v as well as the functor X_K and the maps τ, τ' are independent of R, we may suppose that we had picked R large enough that M and M' have ramification indices bounded by R. Let i be such that $v < \min(s_i - 1, i)$, where s_i is as at the beginning of the section[5]. By 7.4.7 τ, τ' both map under the equivalence of categories 7.3.3 to $X_K(\tau) = X_K(\tau')$. Hence they are equal.

Given any map $X_K(M) \to X_K(M')$ where v, R, i are as in the previous paragraph, the map has the form $X_K(\tau)$ where $\tau \in \mathrm{Hom}_{\mathcal{C}_L^v}(M, M')$ corresponds to the given map under the equivalence of 7.3.3. Hence the functor is full.

[5]In particular the sequence s_k, and hence the number i depend on the choice of R.

Let E be any finite separable extension of $X_K(L)$. We may pick v such that $E/X_K(L)$ has ramification bounded by v. Suppose R was chosen so that $E/X_K(L)$ has ramification index bounded by R. Let i be such that $v < \min(s_i - 1, i)$ and such that $i > R$. Let M/L be the extension corresponding to E under 7.3.3. Let K_j' be the fixed field of $G_K^j G_M$. Then according to Deligne's theory, the ramification index of K_i'/K_i is bounded by R (and hence by i). Since the functor $\mathbf{V}$ of section 7.2 sends $\mathcal{C}_{K_i}^R$ to $\mathcal{C}_L^R$, it follows that M/L has ramification bounded by R. Hence M/L satisfies the conditions of 7.4.7, so that it corresponds to $X_K(M)$ under the equivalence of 7.3.3. Hence $E \cong X_K(M)$, so X_K is essentially surjective. $\square$

Chapter 8

Finite Extensions of $\mathbb{Z}_{\max}$

8.1 Introduction

There has been much interest recently in geometry over the tropical semifield $\mathbb{R}_{\max} = \mathbb{R} \cup \{\infty\}$, in which the addition operation is max and multiplication is given by the usual notion of addition.[18] In this paper, we will instead work with a related semifield $\mathbb{Z}_{\max}$, which is defined in a similar manner.

The semifield $\mathbb{Z}_{\max}$ has been studied by A. Connes and C. Consani in connection with the notion of the absolute point.[13] In particular, they have studied projective spaces over $\mathbb{Z}_{\max}$ and shown that they give a realization of J. Tits' ideas on a projective geometry over the "field with one element".[20]

A natural question that arises is to study the finite extensions of $\mathbb{Z}_{\max}$, that is semifields containing $\mathbb{Z}_{\max}$ which are finitely generated as a semimodule. One reason for studying the finite extensions is geometric in nature. When studying varieties over a non-algebraically closed field K, one needs to consider points with values not only in K, but also in finite extensions of K. By analogy, one might expect that points with values in the extensions of $\mathbb{Z}_{\max}$ will be a necessary ingredient in devoloping a notion of algebraic geometry over $\mathbb{Z}_{\max}$ embodying Connes' and Consani's ideas about projective space.

In,[13] Connes and Consani have discovered that for each $n > 1$ there is a relative Frobenius map $\mathbb{Z}_{\max} \to \mathbb{Z}_{\max}$. Furthermore they showed that this map gives a rank n free semimodule $F^{(n)}$ over $\mathbb{Z}_{\max}$ which is a semifield. The goal of this paper is to show that these are all of the finite extensions of $\mathbb{Z}_{\max}$.

To each extension L of $\mathbb{Z}_{\max}$, we may associate a group $L^\times/\mathbb{Z}_{\max}^\times$. The key to understanding the finite extensions of $\mathbb{Z}_{\max}$ is Corollary 8.6.6 which states that for every finite extension L of $\mathbb{Z}_{\max}$ the group $L^\times/\mathbb{Z}_{\max}^\times$ is finite.

Section 8.2 will give the basic definitions used throughout this paper. In section 8.2 we will also classify finite extensions of the simplest idempotent semifield $\mathbb{B}$.

Section 8.3 will introduce the notion of the unit index of an extension, which is the order of the group $L^\times/\mathbb{Z}_{\max}^\times$ associated to an extension L of $\mathbb{Z}_{\max}$. To show the theory of extensions with finite unit index is nontrivial, we will give a condition in which the unit index must be finite. We will also show in Theorem 8.3.7 that for $n > 1$, any extension of $\mathbb{Z}_{\max}$ has at most one subextension of a given unit index, and we will use this fact in Corollary 8.3.9 to classify finite subextensions of $\mathbb{R}_{\max}/\mathbb{Z}_{\max}$.

Most of the results of section 8.3 will be superseded by more general results in later sections. Thus the reader may skip section 3 except for Definition 8.3.1 and the proof of Theorem 8.3.4. However section 8.3 provides useful motivation for caring about whether an extension has finite unit index.

In section 8.4, we will introduce the notion of an archimedean extension of an idempotent semifield. Roughly speaking L is archimedean over K if every element of L is bounded above by an element of K in a certain sense. We will show that every finite archimedean extension of $\mathbb{Z}_{\max}$ has finite unit index.

We would like to say that all finite extensions of $\mathbb{Z}_{\max}$ have finite unit index. To do this we will show in sections 8.5 and 8.6 that every finite extension L of any idempotent semifield K is archimedean. Then the results of section 8.4 will apply. The strategy to proving this will involve constructing the maximal archimedean subextension L_{arch} of the extension L over K. Section 8.5 is devoted to introducing a notion of convexity that will allow us to prove in section 8.6 that $L = L_{\text{arch}}$. This will imply that L is archimedean.

In section 8.7, we will classify extensions of $\mathbb{Z}_{\max}$ with finite unit index, by showing in Theorem 8.7.2 that they are all $F^{(n)}$ for some n. Since all finite extensions of $\mathbb{Z}_{\max}$ have finite unit index, this gives us a classification of the finite extensions.

Suppose L has finite unit index over $\mathbb{Z}_{\max}$. The first step to showing that $L \cong F^{(n)}$ will be to study the structure of the multiplicative group $L^{\times}$, which we will see to be isomorphic to $\mathbb{Z}$. To understand the addition, we show that the embedding $\mathbb{Z}_{\max} \to L$

tells us how to add nth powers. We then show that this completely determines the additive structure by using lemma 8.2.7, which states that the nth root operation is monotonic in a suitable sense.

After studying the finite extensions, in sections 8.8 and 8.9 we will outline how these results may be generalized to the noncommutative case of division semialgebras over $\mathbb{Z}_{\max}$.

8.2 Basic Definitions and Examples

Definition 8.2.1. A (commutative) semiring R is a set together with 2 binary operations (called addition and multplication) such that R is a commutative monoid under each operation and the distributive law holds. It is idempotent if $x + x = x$ for all $x \in R$. It is selective if for all $x, y \in R$ one has either $x + y = x$ or $x + y = y$. A semifield is a semiring R in which all nonzero elements are units.

Example 8.2.2. Let $\mathbb{B} = \{0, 1\}$ in which addition is given by $x + 0 = 0 + x = 0$ for all x and $1 + 1 = 1$, and with the obvious notion of multiplication. Then $\mathbb{B}$ is an idempotent semifield. More generally let M be a totally ordered abelian group. Then $M_{\max} = M \cup \{-\infty\}$ is an idempotent semiring in which addition is max and multiplication is the group operation of M. Then $\mathbb{B} = M_{\max}$ where M is the trivial group.

Remark 8.2.3. There is an element $u \in \mathbb{Z}_{\max}$ such that $\mathbb{Z}_{\max} = \{0\} \cup \{u^n \mid u \in \mathbb{Z}\}$ and

$u + 1 = u$. We will write elements of $\mathbb{Z}_{\max}$ this way to avoid the ambiguity between addition in $\mathbb{Z}$ and in $\mathbb{Z}_{\max}$.

Definition 8.2.4. An extension L of a semifield K consists of a semifield L and an injective homomorphism $K \to L$. The extension is finite if the homomorphism makes L into a finitely generated semimodule.

Example 8.2.5. Let M be a totally ordered abelian group and $N \subseteq M$ be a subgroup. Then $M_{\max}$ is an extension of $N_{\max}$.

Example 8.2.6. Fix a positive integer n. Define a map $\mathbb{Z}_{\max} \to \mathbb{Z}_{\max}$ sending each nonzero element u^k to u^{nk} and sending 0 to 0. Then this homomorphism is injective, so gives an extension which will be denoted $F^{(n)}$. It is easily checked that $1, u, \ldots, u^{n-1}$ generate $F^{(n)}$ as a semimodule over $\mathbb{Z}_{\max}$[1], so the extension is finite.

We will conclude this section by classifying finite extensions of $\mathbb{B}$. To do this we will need two lemmas. The first of these two lemmas can be obtained by translating a standard result on lattice ordered groups into the language of idempotent semifields. However, we will give a different, and hopefully simpler, proof.

Lemma 8.2.7. *Let K be an idempotent semifield. Let $x, y \in K$ be such that $x^n + y^n = y^n$ for some $n > 0$. Then $x + y = y$.*

Proof. We may assume $x, y \neq 0$. Then $x + y \neq 0$. We compute $(x+y)^n = x^n + x^{n-1}y + \ldots + xy^{n-1} + y^n = x^{n-1}y + \ldots + xy^{n-1} + y^n = y(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-2}) = y(x+y)^{n-1}$. Dividing by $(x+y)^{n-1}$ gives $x + y = y$. □

[1] In fact this is a minimal set of generators, so $F^{(n)}$ is a rank n semimodule over $\mathbb{Z}_{\max}$.

Lemma 8.2.8. *Let K be an idempotent semifield, and $x \in K$ be a root of unity. Then $x = 1$.*

Proof. For some n, we have $x^n = 1$. By lemma 8.2.7, it follows that $x + 1 = 1$.

x^{-1} is also a root of unity so lemma 8.2.7 gives $x^{-1} + 1 = 1$. Hence $x + 1 = x$. By transitivity of equality we have $x = 1$. □

Theorem 8.2.9. *Let L be a finite extension of the idempotent semifield $\mathbb{B}$. Then $L = \mathbb{B}$.*

Proof. Since L is finitely generated as a semimodule over $\mathbb{B}$ and $\mathbb{B}$ is finite, it follows that L is finite. Then $L^\times$ is a finite group and hence is torsion. By lemma 8.2.8, $L^\times = \{1\}$. Hence $L = \mathbb{B}$. □

8.3 Finite subextensions of $\mathbb{R}_{\max}$ over $\mathbb{Z}_{\max}$

In this section we will associate a number called the unit index to any extension of semifields. As an application, and as motivation for the approach of later sections, we will classify finite subextensions of the infinite extension $\mathbb{R}_{\max}$ over $\mathbb{Z}_{\max}$. The first step will be to show in Theorem 8.3.4 that the finite subextensions have finite unit index. We will then study the subextensions of $\mathbb{R}_{\max}$ with finite unit index by relating them to finite subgroups of the circle group $\mathbb{R}/\mathbb{Z}$.

Definition 8.3.1. Let L be an extension of a semifield K. We define the unit index of the extension to be $\text{ui}(L/K) = |L^\times/K^\times|$.

Example 8.3.2. Pick $v \in F^{(n)}$ such that $F^{(n)} = \{0\} \cup \{v^k \mid k \in \mathbb{Z}\}$. Then $\mathbb{Z}_{\max} = \{0\} \cup \{v^{kn}\}$. Then $(F^{(n)})^\times$ is cyclic with generator v while $\mathbb{Z}_{\max}^\times$ is cyclic with generator v^n. It is easily seen that $\mathrm{ui}(F^{(n)}/\mathbb{Z}_{\max}) = n$.

Definition 8.3.3. A idempotent semigroup M is selective if for all $x, y \in M$ either $x + y = x$ or $x + y = y$.

Of course $\mathbb{R}_{\max}$ is selective, as is any subsemimodule of $\mathbb{R}_{\max}$. This property will make it easy to show in the following thoerem that the finite subextensions of $\mathbb{R}_{\max}$ over $\mathbb{Z}_{\max}$ have finite unit index.

Theorem 8.3.4. *Let L be a finite extension of $\mathbb{Z}_{\max}$ in which L is selective. Then* $\mathrm{ui}(L/\mathbb{Z}_{\max}) < \infty$.

Proof. Note that because L is selective, every subset is closed under addition. Let S be a finite set generating L as a semimodule over $\mathbb{Z}_{\max}$. Without loss of generality, we may assume $0 \notin S$. $S\mathbb{Z}_{\max}$ is a subsemimodule of L over $\mathbb{Z}_{\max}$ because it is closed under scalar multiplation by construction, and because it is closed under addition. Since $S \subseteq S\mathbb{Z}_{\max}$, one has $L = S\mathbb{Z}_{\max}$. Then $L^\times = S\mathbb{Z}$, and S surjects onto $L^\times/\mathbb{Z}$. Hence $|L^\times/\mathbb{Z}| \leq |S| < \infty$. □

We will see in Theorem 8.6.6 that the above theorem holds without the hypothesis that L is selective. However it will take several sections to develop the machinery necessary to drop this hypothesis.

For an extension E of $\mathbb{Z}_{\max}$, it will be helpful to understand the group structure of the quotient group $E^\times/\mathbb{Z}$. To do this, we will need the following standard lemma.

Lemma 8.3.5. *Let G be a group. Suppose that for all $n \in \mathbb{N}$, G has at most n elements of order dividing n. Then every finite subgroup of G is cyclic, and there is at most one finite subgroup of a given order.*

We will make use of the following corollary with $M = E^\times$.

Corollary 8.3.6. *Let M be a torsionfree abelian group. Let $\mathbb{Z} \subseteq M$ be an infinite cyclic subgroup. Then for each positive integer n, $M/\mathbb{Z}$ has at most one subgroup of order n and all finite subgroups are cyclic.*

Proof. Let n be a positive integer. By lemma 8.3.5 it suffices to show that $M/\mathbb{Z}$ has at most n elements of order dividing n. Let $\bar{x} \in M/\mathbb{Z}$ have order dividing n and let $\hat{x} \in M$ be any lift. Then $n\hat{x} \in \mathbb{Z}$, and there exists $k \in \mathbb{Z}$ such that $n(\hat{x} - k) \in \{0, 1, \ldots, n-1\}$. Let $x = \hat{x} - k$, which is also a lift of $\bar{x}$ to M. Since M is torsionfree, each equation $nt = m$ with $n, m \in \mathbb{Z}$ has at most one solution t. Since there are n possibilities for nx, there are at most n choices for x and hence for $\bar{x}$. □

The following theorem is the first hint that the unit index will be relevant to the problem of classifying finite extensions of $\mathbb{Z}_{\max}$. Furthermore it will allow us to easily classify those finite extensions which are contained inside $\mathbb{R}_{\max}$.

Theorem 8.3.7. *Let E be an extension of $\mathbb{Z}_{\max}$. Let n be a positive integer. Then there is at most one subextension L of E such that $\mathrm{ui}(L/\mathbb{Z}_{\max}) = n$.*

Proof. Let A be the set of all subextensions of E over $\mathbb{Z}_{\max}$. Let B be the set of subgroups of $E^\times$ containing $\mathbb{Z}_{\max}^\times = \mathbb{Z}$. Define a map $\phi : A \to B$ by $\phi(L) = L^\times$. If $\phi(L) = \phi(M)$, then $L = \{0\} \cup L^\times = \{0\} \cup M^\times = M$, so ϕ is injective. Let C be the set of subgroups of $E^\times/\mathbb{Z}_{\max}^\times$. The fourth isomorphism theorem states that the map $\psi : B \to C$ given by $\psi(G) = G/\mathbb{Z}_{\max}^\times$ is a bijection. Hence the map $A \to C$ sending L to $L^\times/\mathbb{Z}_{\max}^\times$ is injective.

This map clearly restricts from an injection from the set of subextensions with unit index n to the set of subgroups of $E^\times/\mathbb{Z}_{\max}^\times = E^\times/\mathbb{Z}$ with order n. By lemma 8.2.8 and Corollary 8.3.6, there is at most one such subgroup. Hence there is at most one subextension with unit index n. □

Remark 8.3.8. Suppose E is selective. Then if G is a subgroup of $E^\times$ then $\{0\} \cup G$ is a subsemifield of E; it is closed under addition because every subset of a selective semigroup is closed under addition. Since $\phi(\{0\} \cup G = G$, the map ϕ from the proof of Theorem 8.3.7 is bijective in this case. Hence there is a bijective correspondence between subextensions of E over $\mathbb{Z}_{\max}$ and subgroups of $E^\times/\mathbb{Z}$.

Corollary 8.3.9. *Let L be a finite subextension of $\mathbb{R}_{\max}$ over $\mathbb{Z}_{\max}$. Then there exists n such that $L = (\frac{1}{n}\mathbb{Z})_{\max}$*[2].

Proof. Since $L \subseteq \mathbb{R}_{\max}$, L is selective. By Theorem 8.3.4, L has finite unit index. Let $n = \mathrm{ui}(L/\mathbb{Z}_{\max})$. Then $(\frac{1}{n}\mathbb{Z})_{\max}$ has unit index n over $\mathbb{Z}_{\max}$. By Theorem 8.3.7 they

[2]This is the semifield associated to the totally ordered subgroup $\frac{1}{n}\mathbb{Z} \subseteq \mathbb{R}$ via Example 8.2.5. One can easily exhibit an explicit isomorphism of extensions $(\frac{1}{n}\mathbb{Z})_{\max} \cong F^{(n)}$. If we identify $F^{(n)}$ with $\mathbb{Z})_{\max}$ as in Example 8.2.6, this isomorphism sends $\frac{a}{n}$ to u^a.

are equal. □

8.4 Finite archimedean extensions of $\mathbb{Z}_{\max}$

In this section, we will give a criterion that is useful for proving an extension has finite unit index. In later sections, we will use this criterion to prove that every finite extension of $\mathbb{Z}_{\max}$ has finite unit index.

Definition 8.4.1. Let K be an idempotent semifield. An extension L over K is called archimedean if for all $x \in L$, there exists $y \in K$ such that $x + y = y$.

The terminology comes from the following example.

Example 8.4.2. $\mathbb{R}_{\max}$ can be seen to be an archimedean extension of $\mathbb{Z}_{\max}$. This is because of the archimedean property of the real numbers, which states that for every $x \in \mathbb{R}$ there exists $n \in \mathbb{Z}$ such that $x \leq n$ or equivalently $\max x, n = n$.

Lemma 8.4.3. *Let L be an archimedean extension of an idempotent semifield K. Then for all nonzero $x \in L$ there exists nonzero $z \in K$ such that $x + z = x$.*

Proof. There is some $y \in K$ such that $x^{-1} + y = y$, which is clearly nonzero. After multiplying by xy^{-1}, we get $y^{-1} + x = x$, so we may take $z = y^{-1}$. □

For the remainder of this section, let L be finite and archimedean over $\mathbb{Z}_{\max}$, and let $S \subseteq L$ be a finite set which generates L as a $\mathbb{Z}_{\max}$-semimodule. We may assume $0 \notin S$. The goal for the remainder of the section will be to show that $\mathrm{ui}(L/\mathbb{Z}_{\max}) < \infty$.

If we can show that $S\mathbb{Z}_{\max} = \{sx \mid s \in S,\ x \in \mathbb{Z}_{\max}\}$ is closed under addition, then we can apply the proof of Theorem 8.3.4 to prove Theorem 8.4.10. Unfortunately, there is no reason to believe that it is closed under addition.[3] However, we will see that we can construct a larger, but still finite, generating set T such that $T\mathbb{Z}_{\max}$ is closed under addition.

Lemma 8.4.4. *Let S be as above and let $S^{-1}S = \{s_1^{-1}s_2 \mid s_1, s_2 \in S\}$. There exists $M \in \mathbb{Z}$ such that $x + u^M = u^M$ and $x + u^{-M} = x$ for all $x \in S^{-1}S$. Furthermore, any number larger than M also has this property*

Proof. Note that if $m > n$ and $x+u^n = u^n$ then $x+u^m = x+u^m+u^n = u^m+u^n = u^m$. Similarly if $x + u^{-n} = x$ and $m > n$ then $x + u^{-m} = x$. Since $S^{-1}S$ is finite, these remarks allow us to construct a different value of M for each of the statements, and take the maximum of all of them. Let $x \in S^{-1}S$. Then since L is archimedean over $\mathbb{Z}_{\max}$, there exists M such that $x + u^M = u^M$. By lemma 8.4.3, there exists M such that that $x + u^{-M} = x$. □

For the remainder of this section we will let M be the value constructed in the previous lemma.

Let $T_n = \{s + \sum_{i=1}^{n} u^{k_i} s_i \mid s, s_1, \ldots, s_n \in S,\ k_1, \ldots, k_n \in \{-M, \ldots, 0\}\}$. Let $T = \bigcup_{n\geq 0} T_n$.

Lemma 8.4.5. *$T_n \subseteq T_{n+1}$ for all n.*

[3] In the case $L = F^{(n)}$, one can show that $L = S\mathbb{Z}_{\max}$. The classification theorem that we are working towards will then imply that $S\mathbb{Z}_{\max}$ is always closed under addition. However, we do not know a direct way to show that $S\mathbb{Z}_{\max}$ is already closed under addition without enlarging S.

Proof. Let $s + \sum_{i=1}^{n} u^{k_i} s_i \in T_n$. $s + \sum_{i=1}^{n} u^{k_i} s_i = s + s + \sum_{i=1}^{n} u^{k_i} s_i + u^{k_n} s_n \in T_{n+1}$. □

Lemma 8.4.6. *Let $N = (M+1)|S|$. Then $T = T_N$, and T is finite.*

Proof. It suffices to show for each n that $T_n \subseteq T_N$. We know this in the case where $n \leq N$. For $n > N$, we proceed by induction. Let $s + \sum_{i=1}^{n} u^{k_i} s_i \in T_n$. Since there are $M+1$ choices for k_i, and $|S|$ choices for s_i, the pigeon hole principle implies some term is repeated. Since addition is idempotent, we can remove the repeated term, so $s + \sum_{i=1}^{n} u^{k_i} s_i \in T_{n-1}$. By the inductive hypothesis, $T_{n-1} \subseteq T_N$, so $T_n \subseteq T_N$. It is clear that T_N is finite; in fact for any n, T_n has at most $|S|^{n+1}(M+1)^n$ elements. □

Since $S \subseteq T$, T is also a finite generating set for L. The next step is to show that T is closed under addition.

Lemma 8.4.7. *Let $x = s + \sum_{i=1}^{n} u^{k_i} s_i$ for some $s, s_1, \ldots, s_n$ where $k_1, \ldots, k_n$ are non-positive integers. Then $x \in T$.*

Proof. Suppose $k_i < -M$. Then by lemma 8.4.4, $s_i^{-1} s + u^{k_i} = s_i^{-1} s$. Hence $s + u^{k_i} s_i = s$, so we may drop the term $u^{k_i} s_i$. After dropping all such terms, we may suppose without loss of generality that $k_i \geq M$ for all i. But then we trivially have $s + \sum_{i=1}^{n} u^{k_i} s_i \in T$. □

Lemma 8.4.8. *Let $n \geq 1$. Let $z = \sum_{i=1}^{n} u^{k_i} s_i$ with $s_i \in S$ and $k_i \in \mathbb{Z}$. Then $z \in T\mathbb{Z}_{\max}$. Conversely every nonzero element of $T\mathbb{Z}_{\max}$ has this form for some n.*

Proof. After rearranging terms, we may suppose without loss of generality that $k_n \geq k_i$ for all i. Then $u^{-k_n}z = s_n + \sum_{i=1}^{n-1} u^{k_i - k_n} s_i$. By lemma 8.4.7, $u^{-k_n}z \in T$. Hence $z \in T\mathbb{Z}_{\max}$.

The converse is trivial. □

Corollary 8.4.9. *$T\mathbb{Z}_{\max}$ is closed under addition.*

In what follows, the next theorem will play a similar role to that played by Theorem 8.3.4 in section 8.3. We will later see that all finite extensions are archimedean, and so this theorem is much more general than it would first appear.

Theorem 8.4.10. *Let L be a finite archimedean extension of $\mathbb{Z}_{\max}$. Then one has $\mathrm{ui}(L/\mathbb{Z}_{\max}) < \infty$.*

Proof. Let S generate L as a semimodule. Let T be the set defined earlier in this section. Since $S \subseteq T$, T also generates L. By lemma 8.4.6, T is finite. By Corollary 8.4.9, $T\mathbb{Z}_{\max}$ is closed under addition. One can apply the proof of Theorem 8.3.4 to show that T surjects onto $L^\times/\mathbb{Z}_{\max}^\times$. The result follows. □

8.5 Convex subsemifields

In this section we introduce the notion of a convex subsemifield of an idempotent semifield. A convex subsemifield $K \subseteq L$ will have the property that addition in $L/K^\times$ is well-defined. We will use this property to constrain the possible subextensions of the extension L of K.

The following definition is essentially the same as the definition of a convex ℓ-subgroup given in.[19]

Definition 8.5.1. Let L be an idempotent semifield. A subsemifield $K \subseteq L$ is called convex if for any $x \in L$ such that there exist $y, z \in K$ with $x + y = y$ and $x + z = x$, one has $x \in K$.

Example 8.5.2. Give to $\mathbb{Z} \times \mathbb{Z}$ the lexicographical order, in which $(a, b) \leq (x, y)$ if $a < x$ or if $a = x$ and $b \leq y$. Identify $\mathbb{Z}$ with a subgroup of $\mathbb{Z} \times \mathbb{Z}$ by identifying n with $(0, n)$. Then $\mathbb{Z}_{\max} \subseteq (\mathbb{Z} \times \mathbb{Z})_{\max}$ is a convex subsemifield. This follows from the fact that the inequalities $(0, a) \leq (m, n) \leq (0, b)$ imply $m = 0$, and the fact that $x \leq y$ if and only if $\max(x, y) = y$.

If $K \subseteq L$ is a convex subsemifield, we consider an equivalence relation $\sim$ on L given by $x \sim y$ if there exists $u \in K^\times$ with $x = uy$. We denote the quotient by $L/K^\times$.

Theorem 8.5.3. *[19, 2.2.1]Let L be an idempotent semifield, and K be a convex subsemifield. Then $L/K^\times$ is an idempotent semifield.*

Proof. The only thing to check is that addition is well defined. Let $x, y \in L$ and $u \in K$. We must show that $x + y \sim x + uy$. Equivalently we must show $z \in K$ where $z = (x + y)^{-1}(x + uy)$.

Suppose $u + 1 = u$. Then $ux + x = ux$. Hence $u(x + y) + (x + uy) = u(x + y)$. Then $u + z = u$. Also $uy + y = uy$ so $(x + uy) + (x + y) = x + uy$. Hence $z + 1 = z$. Since $1, u \in K$, it follows from convexity that $z \in K$. Hence $x + y \sim x + uy$.

In general, we have $(u+1)+1 = u+1$, so $x+y \sim x+(u+1)y$ and it suffices to show that $x+uy \sim x+(u+1)y$. Equivalently, it suffices to show that $u^{-1}x + y \sim u^{-1}x + (1+u^{-1}y)$. But this follows from the case already considered since $(1+u^{-1})+1 = 1+u^{-1}$. □

Theorem 8.5.4. *Let E be an extension of an idempotent semifield K. Suppose $K \subseteq E$ is convex. Then the extension E over K has no nontrivial finite subextensions.*

Proof. Let L be a finite subextension of E over K. Then K is convex in L. Since L is a finite extension, there is a finite set S such that every element $x \in L$ can be written as a finite sum $x = \sum a_i s_i$ for $a_i \in K$ and s_i in S. Then every element of $L/K^\times$ can be written as a finite sum $\bar{x} = \sum \bar{a}_i \bar{s}_i$ where $\bar{a}_i \in K/K^\times = \mathbb{B}$ and $\bar{s}_i$ ranges over a finite set $\bar{S}$. Hence $L/K^\times$ is a finite extension of $\mathbb{B}$. By Theorem 8.2.9, $L/K^\times = \mathbb{B}$. Hence for all $x \in L$, one has $x = 0$ or $x \in K^\times$. It follows that $L = K$. □

8.6 The maximal archimedean subextension

When thinking about archimedean subextensions of a given extension, a natural question that arises is whether there is a maximal archimedean subextension, which contains every other archimedean subextension. In this section we will explicitly construct this maximal archimedean subextension. Applying the results of section

8.5 in this context will imply all finite extensions are archimedean, and so we may drop the archimedean hypothesis from Theorem 8.4.10.

Definition 8.6.1. Let L be an extension of an idempotent semifield K. We define $L_{\text{arch}} = \{x \in L | \ x + y = y, x + z = x \text{ for some } z, y \in K\}$.

Lemma 8.6.2. *L_{arch} is a subsemifield of L and contains K.*

Proof. Let $x_1, x_2 \in L_{\text{arch}}$. Then there exists $y_1, y_2, z_1, z_2 \in K$ such that $x_1 + y_1 = y_1$, $x_2 + y_2 = y_2$, $x_1 + z_1 = x_1$, and $x_2 + z_2 = x_2$. Then $(x_1 + x_2) + (y_1 + y_2) = y_1 + y_2$ and $(x_1 + x_2) + (z_1 + z_2) = x_1 + x_2$. Thus $x_1 + x_2 \in L_{\text{arch}}$.

Also $x_1x_2 + y_1y_2 = x_1x_2 + (x_1 + y_1)(x_2 + y_2) = x_1x_2 + y_1x_2 + x_1y_2 + y_1y_2 = (x_1 + y_1)(x_2 + y_2) = y_1y_2$. A similar computation shows $x_1x_2 + z_1z_2 = x_1x_2$. Thus $x_1x_2 \in L_{\text{arch}}$. The rest of the proposition is trivial. □

Proposition 8.6.3. *Let L be an extension of an idempotent semifield K. L_{arch} is the maximal archimedean subextension of L; In other words, it is an archimedean subextension and every other archimedean subextension is contained in it.*

Proof. By definition, for every $x \in L_{\text{arch}}$, there exists $y \in K$ such that $x + y = y$.

For the converse let F be an archimedean subextension of L over K. Let $x \in F$. Then there exists y such that $x + y = y$. Since $x^{-1} \in F$, there exists a nonzero element $z^{-1} \in K$ such that $x^{-1} + z^{-1} = z^{-1}$ so $x + z = x$. Since $x \in L$, the above equalities show $x \in L_{\text{arch}}$. Hence $F \subseteq L_{\text{arch}}$. □

Theorem 8.6.4. *L_{arch} is a convex subsemifield of L.*

Proof. Let $x \in L$. Suppose there exist $y, z \in L_{\text{arch}}$ such that $x+y = y$ and $x+z = x$. By the definition of L_{arch}, there exist $y', z' \in K$ such that $y + y' = y'$ and $z + z' = z$. Then $x + z' = (x+z)+z' = x+z = x$ and $x+y' = x+(y+y') = y+y' = y'$. Hence $x \in L_{\text{arch}}$. □

Corollary 8.6.5. *Let L be a finite extension over an idempotent semifield K. Then L is archimedean.*

Proof. L is a finite extension over L_{arch} with L_{arch} convex inside L. By Theorem 8.5.4, $L = L_{\text{arch}}$. Hence L is archimedean over K. □

We can now prove the following generalization of theorems 8.3.4 and 8.4.10

Corollary 8.6.6. *Let L be a finite extension of $\mathbb{Z}_{\max}$. Then* $\text{ui}(L/\mathbb{Z}_{\max}) < \infty$.

Proof. Use Corollary 8.6.5 and Theorem 8.4.10 □

8.7 The classification theorem

In this section, we will finally prove the classification of finite extensions of $\mathbb{Z}_{\max}$.

The following lemma is a consequence of the classification of finitely generated abelian groups.

Lemma 8.7.1. *Let M be a torsion free abelian group, and N be a finite abelian group. Suppose there is a short exact sequence $0 \to \mathbb{Z} \to M \to N \to 0$. Then $M \cong \mathbb{Z}$.*

Theorem 8.7.2. *Let L be an extension of $\mathbb{Z}_{\max}$ with $\text{ui}(L/\mathbb{Z}_{\max}) < \infty$. Then $L \cong F^{(n)}$ as extensions of $\mathbb{Z}_{\max}$ for some n.*

Proof. Fix an element $u \in \mathbb{Z}_{\max}$ as in Remark 8.2.3.

We have a short exact sequence $0 \to \mathbb{Z}_{\max}^{\times} \to L^{\times} \to L^{\times}/\mathbb{Z}_{\max}^{\times} \to 0$. $L^{\times}$ is torsionfree by lemma 8.2.8. By assumption, $L^{\times}/\mathbb{Z}_{\max}^{\times}$ is finite. By lemma 8.7.1 $L^{\times} \cong \mathbb{Z}$. Pick a generator v of $L^{\times}$. Then $L = \{0\} \cup \{v^k \mid k \in \mathbb{Z}\}$. Since $u \in \mathbb{Z}_{\max} \subseteq L$ is nonzero there exists $n \neq 0$ such that $u = v^n$. By picking the other generator of $L^{\times}$ if neccessary, we may assume without loss of generality that $n > 0$.

To determine the addition in L, it suffices to compute $v^a + v^b$ for $a, b \in \mathbb{Z}$. We may suppose without loss of generality that $a > b$. Then $(v^a)^n + (v^b)^n = u^a + u^b = u^a = (v^a)^n$. By lemma 8.2.7, $v^a + v^b = v^a$.

Hence $L \cong \mathbb{Z}_{\max}$ under the map sending v to u. Then the extension L of $\mathbb{Z}_{\max}$ may be identified with the extension given by the composite map $\mathbb{Z}_{\max} \to L \cong \mathbb{Z}_{\max}$ sending u to u^n. But this extension is F^n. □

Combining Theorem 8.7.2 and Corollary 8.6.6 gives us the following classification of finite extensions of $\mathbb{Z}_{\max}$.

Theorem 8.7.3. *Let L be a finite extension of $\mathbb{Z}_{\max}$. Then $L \cong F^{(n)}$ as extensions of $\mathbb{Z}_{\max}$.*

8.8 Division semialgebras with finite unit index

Unlike the previous sections, throughout this section, we will use the term semiring to refer to a possibly noncommutative semiring.

Definition 8.8.1. A division semialgebra over a semifield K is a division semiring D together with an injective homomorphism from K to the center of D. It is finite if D is finite as a left semimodule over K.

We define the unit index of a division semialgebra analogously to Definition 8.3.1.

Lemma 8.8.2. *Let D be an idempotent division semiring. Let $x, y \in D$ satisfy $xy = yx$. Suppose $x^n + y^n = y^n$ for some $n \geq 1$. Then $x + y = y$*

Proof. This can be proven as in lemma 8.2.7 □

Lemma 8.8.2 provides us with the following analogues of lemma 8.2.8 and theorems 8.2.9.

Corollary 8.8.3. *Let D be an idempotent division semiring. Then $D^\times$ is torsion free.*

Proof. Let $x \in D^\times$ be torsion of order n. Since $x^n + 1 = 1$, $x + 1 = 1$. Similarly $x + 1 = x$, so $x = 1$. □

Corollary 8.8.4. *Let D be a finite division semialgebra over $\mathbb{B}$. Then $D = \mathbb{B}$.*

Theorem 8.8.5. *Let D be a division semialgebra over $\mathbb{Z}_{\max}$ with finite unit index. Then D is selective.*

Proof. Let $x, y \in D$. We wish to show either $x + y = x$ or $x + y = y$. If either of x or y is zero, we are done. It suffices to show $xy^{-1} + 1 = xy^{-1}$ or $xy^{-1} + 1 = 1$. In other words, we can assume without loss of generality that $y = 1$.

Let $n = \text{ui}(D/\mathbb{Z}_{\max})$. Then by Lagrange's theorem $x^n \in \mathbb{Z}_{\max}$. Since $\mathbb{Z}_{\max}$ is selective, $x^n + 1 = 1$ or $x^n + 1 = x^n$. Since x commutes with 1, we may apply lemma 8.8.2 to see that $x + 1 = 1$ or $x + 1 = x$. □

When D is selective, the following lemma shows we can remove the commutativity hypothesis of lemma 8.8.2.

Lemma 8.8.6. *Let D be a selective idempotent division semiring. Suppose $x, y \in D$ satisfy $x^n + y^n = y^n$ for some $n \geq 1$. Then $x + y = y$.*

Proof. The lemma is clear if $x = 0$. Let n be the smallest number satisfying the hypotheses of the lemma. Suppose $x + y \neq y$. Then $x + y = x$ since D is selective. Note that $xy^{n-1} = (x + y)y^{n-1} = xy^{n-1} + y^n = xy^{n-1} + x^n + y^n$. Consequently $xy^{n-1} + x^n = xy^{n-1}$. Dividing by x gives $y^{n-1} + x^{n-1} = y^{n-1}$, contradicting minimality. Thus $x + y = y$. □

Theorem 8.8.7. *Let D be a division semialgebra over $\mathbb{Z}_{\max}$ with finite unit index. Let $G = D^\times/\mathbb{Z}_{\max}^\times$. Then G has at most one cyclic subgroup of each order.*

Proof. Let $C \subseteq G$ be a cyclic subgroup of order n. Let g generate C. Let $\hat{g} \in D^\times$ be in the preimage of g. Then $\hat{g}^n \in \mathbb{Z}_{\max}^\times$. Let u denote the standard generator of $\mathbb{Z}_{\max}^\times$ as in Remark 8.2.3. Then there exists k such that $\hat{g}^n = u^k$.

Let $d = \gcd(n, k)$. Then $(\hat{g}^{n/d})^d = (u^{k/d})^d$. Since $u^{k/d}$ is central, $(u^{k/d}\hat{g}^{n/d})^d = 1$. Hence $u^{k/d}\hat{g}^{n/d} = 1$. By looking at the image in G, we get $g^{n/d} = 1$. Since g has order n, $d = 1$.

There exist integers a, b such that $an + bk = 1$. Let $g' = g^b$; note that g' also generates C since $\gcd(b, n) = 1$. Let $\hat{g}' = u^a\hat{g}^b$, which is a lift of g'. Then $\hat{g}'^n = u^{an}\hat{g}^{bn} = u^{an}u^{bk} = u$.

Let $H \subseteq G$ be another cyclic subgroup of order n. For any generator $h \in H$, the above argument gives us a new generator $h' \in H$ and a lift $\hat{h}' \in D^\times$ such that $\hat{h}'^n = u$.

Since $\hat{g}'^n = \hat{h}'^n$, we have $\hat{g}'^n = \hat{g}'^n + \hat{h}'^n = \hat{h}'^n$. By lemma 8.8.6, $\hat{g}' = \hat{g}' + \hat{h}' = \hat{h}'$. Projecting down to G gives $g' = h'$. Hence $C = H$. □

Corollary 8.8.8. *Let D and G be as in Theorem 8.8.7. Then G is cyclic.*

Theorem 8.8.9. *Let D be a division semialgebra over $\mathbb{Z}_{\max}$ with finite unit index. Then $D = F^{(n)}$ for some n.*

Proof. Let $G = D^\times/\mathbb{Z}_{\max}^\times$. Then G is cyclic. Since the quotient of $D^\times$ by a central subgroup is abelian, $D^\times$ is itself abelian. Apply Theorem 8.7.2. □

8.9 Finite division semialgebras over $\mathbb{Z}_{\max}$

As before, we do not assume semirings to be commutative.

Definition 8.9.1. Let K be an idempotent semifield. A division semialgebra L over an idempotent semifield K is called archimedean if for all $x \in L$, there exists $y \in K$ such that $x + y = y$.

Theorem 8.9.2. *Let D be a finite archimedean division semialgebra over $\mathbb{Z}_{\max}$. Then* $\mathrm{ui}(D/\mathbb{Z}_{\max}) < \infty$.

Proof. The reader may verify that the commutative law was never used[4] in the proof of Theorem 8.4.10, or any of the results leading up to it. □

Definition 8.9.3. Let D be an idempotent division semiring. A division subsemiring $E \subseteq D$ is called convex if for any $x \in D$ such that there exist $y, z \in E$ with $x + y = y$ and $x + z = x$, one has $x \in E$. $E \subseteq D$ is called normal if $E^\times \subseteq D^\times$ is normal.

Theorem 8.9.4. *Let D be an idempotent division semiring and $E \subseteq D$ a convex normal division subsemiring. Then $D/E^\times$ is an idempotent division semiring.*

Proof. The fact that addition is well defined does not require the multiplicative structure, so an be proven the same way as the commutative case was in Theorem 8.5.3. Multiplication is well defined because it is well defined in $D^\times/E^\times$. □

Substituting the above theorem and Theorem 8.8.4 into the proof of Theorem 8.5.4 gives the following.

[4] However the fact that $\mathbb{Z}_{\max}$ lies in the center of D was used frequently.

Theorem 8.9.5. *Let D, E be finite division semirings with $E \subseteq D$ normal and convex. Suppose D is finite as a left E-semimodule. Then $D = E$.*

Since section 8.6 never used the commutative law, we have the following.

Theorem 8.9.6. *Let D be an idempotent division semiring. There is a maximal archimedean division subsemiring $D_{\text{arch}} \subseteq D$. Furthermore $D_{\text{arch}} \subseteq D$ is convex and normal.*

Proof. We only need to show normality. Let $x \in D^{\times}_{\text{arch}}$ and $g \in D^{\times}$. Then by the construction of D_{arch}[5], we have $y, z \in K$ such that $x + y = y$ and $x + z = x$. Then we get $gxg^{-1} + gyg^{-1} = gyg^{-1}$, and a similar formula involving z. But y and z lie in K which is contained in the center of D, so we have $gxg^{-1} + y = y$ and $gxg^{-1} + z = gxg^{-1}$. Thus by the construction of D_{arch} we have $gxg^{-1} \in D_{\text{arch}}$. □

As in section 8.6, we may combine the above results to obtain the following.

Corollary 8.9.7. *Every finite division semialgebra over an idempotent semifield is archimedean.*

Theorem 8.9.8. *Let D be a finite division semialgebra over $\mathbb{Z}_{\max}$. Then $D = F^{(n)}$ for some n.*

Proof. Since D is finite over $\mathbb{Z}_{\max}$, it is archimedean over $\mathbb{Z}_{\max}$. Since it is finite and archimedean, it has finite unit index. We may now apply Theorem 8.8.9. □

[5] The construction is essentially Definition 8.6.1 with L replaced by D.

Chapter 9

Selective hyperfields

9.1 Introduction

One expects that there should be an interpretation of tropical geometry as a sort of algebraic geometry over some field-like object. However there have been multiple conflicting proposals as to what sort of object should serve as the base for tropical geometry. One of the main goals of the present work is to relate some of the objects that have been proposed as a base for tropical geometry. Hence, before discussing the results of this chapter we will describe some of these objects.

The most traditional answer is that one should work over an idempotent semifield, or perhaps more specifically over a selective semifield, as defined below.

Definition 9.1.1. A semigroup is a commutative monoid. It is idempotent if one has $x + x = x$ for all $x \in A$. It is selective if for all $x, y \in A$ one has $x + y \in \{x, y\}$. If

A is an idempotent semigroup and $x, y \in A$ one writes $x \leq y$ to mean $x + y = y$. A semiring consists of a semigroup A together with a commutative associative operation $\cdot : A \times A \to A$ and an element $1 \in A$ such that for all $x, y, z \in A$, one has $1x = x$, $(x + y)z = xz + yz$. It is a semifield if all nonzero elements are units.

Example 9.1.2. Let $\mathbb{B} = \{0, 1\}$ with the obvious multiplication and with addition satisfying $1 + 1 = 1$. Then $\mathbb{B}$ is an idempotent and selective semifield. Let $\mathbb{R}_{\max} = \{-\infty\} \cup \mathbb{R}$ have max as the addition operation, and classical addition of real numbers as the multiplication operation. Then $\mathbb{R}_{\max}$ is an idempotent and selective semifield. For a ring R we let $\mathcal{I}(R)$ be the set of ideals of R equipped with the usual notion of addition and multiplication of ideals. Then $\mathcal{I}(R)$ is an idempotent semiring. However when R is not a valuation ring, $\mathcal{I}(R)$ is not selective.

It is a standard fact that the relation $\leq$ on an idempotent semigroup is a partial ordering and that the least upper bound of two elements $x, y \in A$ is $x + y$. One easily sees that selective semigroups are precisely those idempotent semigroups which are totally ordered. In particular, removing the zero element gives an equivalence of categories between selective semigroups and totally ordered sets, as well as between selective semifields and totally ordered abelian groups.

Recently Zur Izhakian and Louis Rowen gave a treatment of tropical geometry via supertropical semirings.[15] Rather than defining supertropical semirings, we will content ourselves with noting that Izhakian and Rowen showed that supertropical semirings are equivalent to valued monoids, which we do define.

Definition 9.1.3. A valued monoid is a triple (v, A, B) where A is a commutative monoid, B is a totally ordered commutative monoid, and $v : A \to B$ is a monoid homomorphism. It is a valued group if A and B are groups.

Just as using selective semifields rather than semirings amounts to using totally ordered groups rather than totally ordered monoids, one expects here that the appropriate class of objects to use as a base for tropical geometry would be valued groups rather than valued monoids. It is noteworthy that the supertropical perspective suggests using valuations rather than orderings; we will see a similar phenomenon in the next approach we discuss.

A third view of tropical geometry, which has been championed by Oleg Viro, is that it should be viewed as geometry over a hyperfield.[17] For the definitions of hyperfields and hypergroups, see definitions 3.1.4 and 3.1.3. For the purposes of this chapter we will use the term hypergroup to mean canonical abelian hypergroup.

When studying semifields in connection with tropical geometry, it is helpful to note that we are interested in selective semifields, rather than arbitrary semifields. Here too, hyperfields are too general, and one might desire to find a more restrictive class of hyperfields which contains $\mathbb{Y}_\times$, $\mathcal{T}\mathbb{R}$, and $\mathcal{T}\mathbb{C}$. In Definition 9.2.19 we propose such a class of hyperfields which we call selective hyperfields. The definition of a selective hypergroup is analogous to the definition of a selective semigroup. However, when we attempt to mimic the construction of the ordering which we gave for selective semigroups, we are instead confronted with a valuation. This is in line with the supertropical perspective that one should be working with valued objects rather than ordered objects.

Another question which arises is how selective hyperfields relate to valued groups. Because selective hyperfields are equipped with a valuation, the multiplicative group of a selective hyperfield is a valued group. But this leaves the question of what additional structure one needs to recover a selective hyperfield from a valued group. In section 9.4, we will show that one can construct a selective hyperfield from a valued group if one has identified the kernel of the valuation with a hyperfield k satisfying the condition that $1 - 1 = k$. Furthermore, all selective hyperfields arise in this manner. By Theorem 9.4.13, k may be thought of as the residue hyperfield of the selective hyperfield we are trying to construct. We will show in Proposition 9.2.23 that the condition that $1 - 1 = k$ may be interpreted as saying that k is a selective hyperfield whose valuation is trivial.

A final motivation for the present chapter comes from Simon Henry's symmetrization functor, which is introduced in.[14] The symmetrization functor is a universal way of embedding a semigroup which satisfies a certain balancing condition into a hypergroup. If the semigroup is cancellative, the resulting hypergroup is a group and this construction is just the Grothendieck group construction. However the symmetrization functor gives more interesting results when applied to a selective semigroup. Connes and Consani have introduced the insight that the restriction of the symmetrization functor to selective semigroups should be thought of as a base change functor $-\otimes_{\mathbb{B}}\mathbb{S}$ from $\mathbb{B}$ to $\mathbb{S}$. This raises the question of whether one can produce a similar construction where $\mathbb{S}$ is replaced by another hypergroup H. In section 9.3 we show how to do this when H satisfies the condition of Proposition 9.2.23. This method of constructing hypergroups always produces selective hypergroups. This construction will be needed in section 9.4 to produce the underlying additive hypergroups of the hyperfields we are trying to construct.

9.2 Idempotent and selective hypergroups

In this section we introduce the notions of idempotence and selectivity for hypergroups. The definitions parallel those from the theory of semigroups. However rather than inducing an ordering, the idempotent structure on a hypergroup induces a valuation. These classes of hypergroups will contain several examples of interest in tropical geometry, such as $\mathbb{Y}_{\times}$, $\mathcal{T}\mathbb{R}$ and $\mathcal{T}\mathbb{C}$.

There are three reasonable definitions of idempotence for a hypergroup. Requiring that $x \in x+x$ for all x is too weak for our purposes. On the other hand, requiring that $x = x+x$ is strong enough to exclude many of the examples we are interested in, such as $\mathbb{K}$. Instead we will use the following intermediate definition.

Definition 9.2.1. H is non-archimedean if $x - x = (x+x) - (x+x)$ holds for all $x \in H$. H is called idempotent if it is non-archimedean and for all $x \in H$, one has $x \in x+x$.

Example 9.2.2. $\mathbb{K}$, $\mathbb{S}$, Φ, $\mathbb{Y}_\times$, $\mathcal{T}\mathbb{R}$, and $\mathcal{T}\mathbb{C}$ are all idempotent hyperfields. In fact they are all selective hyperfields as defined below in Definition 9.2.19.

Example 9.2.3. Let K be a local field. Let n be a positive integer. Krasner introduced the hyperfield $K/(1+\mathfrak{m}^n)$. This hyperfield is non-archimedean, but doesn't satisfy $1 \in 1+1$, and hence is not idempotent.

Example 9.2.4. Let R be a local ring with maximal ideal $\mathfrak{m}$. Then the quotient $H = R/R^\times$ is a hyperring. There are two distinct cases: Either $R/\mathfrak{m} \cong \mathbb{F}_2$ or $R/\mathfrak{m} \ncong \mathbb{F}_2$. In the first case one has $R^\times - R^\times = \mathfrak{m}$, which is closed under addition. This implies $(1-1)+(1-1) = 1-1$, so H is non-archimedean in this case. However H is not idempotent if $R/\mathfrak{m} \cong \mathbb{F}_2$, since $1 \notin \mathfrak{m}/R^\times = 1-1$. In the second case where $R/\mathfrak{m}$ has more than two elements, one checks $R^\times - R^\times = R$. This implies H satisfies the equation $1-1 = H$. One easily sees that $1-1=H$ implies idempotence.

Let H be an idempotent hypergroup and $x, y \in H$. To mimic the definition of the order on an idempotent semigroup, it is natural to define $x \leq y$ to mean $y \in x+y$. However, for the sake of greater generality we will give a different definition which is equivalent to this one in the special case of idempotent hypergroups.

Lemma 9.2.5. *Let H be an idempotent hypergroup. Let $x, y \in H$. Then $y \in x+y$ if and only if $x - x \subseteq y - y$.*

Proof. Suppose $y \in x+y$. Then $x \in y-y$. Hence $x - x \subseteq (y-y)-(y-y) = (y+y)-(y+y) = y-y$. Conversely, suppose $x-x \subseteq y-y$. Since $x \in x+x$, we have $x \in x-x \subseteq y-y$. Hence $y \in x+y$. □

Definition 9.2.6. If H is a hypergroup and $x, y \in H$, we say $x \leq y$ if $x - x \subseteq y - y$.

The relation $\leq$ on a hypergroup H is reflexive and transitive. However unlike in the case of idempotent semigroups, it is not a partial order, because it is possible that $x \leq y \leq x$ without $x = y$. For example in $\mathbb{S}$ we have $1 \leq -1 \leq 1$. However, we may obtain a partially ordered set as follows.

Definition 9.2.7. Let H be a hypergroup. For $x, y \in H$ we write $x \sim y$ to mean $x \leq y \leq x$. We also use $\leq$ to denote the induced relation on $H/\sim$. The quotient map $v : H \to H/\sim$ is called the valuation on H.

Lemma 9.2.8. *$\sim$ is an equivalence relation. $\leq$ is a partial order on $H/\sim$.*

Proof. This is a standard fact about preordered sets. □

Example 9.2.9. If H is one of $\mathbb{S}$, $\mathbb{K}$, or Φ, then $H/\sim = \{0, 1\}$ with $v(0) = 0$ and $v(x) = 1$ for all other x. This valuation is called the trivial valuation. On $\mathbb{Y}_\times$, $\sim$ is equality, and v is the identity map. If H is either $\mathcal{T}\mathbb{R}$ or $\mathcal{T}\mathbb{C}$ then $H/\sim \cong \mathbb{R}_{\geq 0}$, and v is the ordinary real or complex absolute value.

Example 9.2.10. Let K be a local field, and $n > 0$. Let $H = K/(1+\mathfrak{m}^n)$. Let $x, y \in K$ and $\bar{x}, \bar{y}$ be their classes in H. Then one may check that $v(\bar{x}) \leq v(\bar{y})$ if and only if $|x| \leq |y|$, using the equation $x - x = x\mathfrak{m}^{\mathfrak{n}}/(1 + m^n)$. Hence, one may identify v with the non-archimedean absolute value induced by the one on K.

Example 9.2.11. Let R be a local ring with maximal ideal $\mathfrak{m}$ such that $R/\mathfrak{m} \neq \mathbb{F}_2$. Let $H = R/R^\times$. One has $x - x = xH$ for all $x \in H$. From this one can show that $\sim$

is equality, that v is the identity, and that the partial ordering on $H/\sim = R/R^\times$ is given by divisibility.

Remark 9.2.12. Let H be an idempotent hypergroup and $x \in H$. Then $x - x = \{y \mid x \in x + y\} = \{y \mid v(y) \leq v(x)\}$ is the ball of radius $v(x)$ around 0.

Calling $v : H \to H/\sim$ a valuation is motivated by the fact that $H/\sim$ is partially ordered and by the following lemma. Note that if $\max(v(x), v(y))$ exists then the lemma is simply the ultrametric inequality, $v(x + y) \leq \max(v(x), v(y))$.

Lemma 9.2.13. *Let H be a non-archimedean hypergroup. Let v be its valuation. Let $x, y \in H$ and $t \in H/\sim$ be such that $v(x) \leq t$ and $v(y) \leq t$. Then for all $z \in x + y$, $v(z) \leq t$.*

Proof. Let w be such that $v(w) = t$. Then $x - x \subseteq w - w$ and $y - y \subseteq w - w$. Then $z - z \subseteq (x+y)-(x+y) = (x-x)+(y-y) \subseteq (w-w)+(w-w) = w+w-w-w = w-w$. Hence $v(z) \leq v(w) = t$. ☐

Lemma 9.2.13 fails for hypergroups which aren't non-archimedean, as the following example shows.

Example 9.2.14. We will let Δ be the triangle hyperfield introduced by Viro. Specifically $\Delta = \mathbb{R}_{\geq 0}$ equipped with the multivalued operation $\triangledown$, which is given by declaring $x \triangledown y$ to be the closed interval from $|x - y|$ to $x + y$. Then Δ isn't non-archimedean. The valuation on Δ is the identity map $v : \Delta \to \mathbb{R}_{\geq 0}$, which doesn't satisfy the ultrametric inequality. For instance $2 \in 1 \triangledown 1$ but $v(2) = 2 > \max(v(1), v(1))$.

For a general hypergroup, it is not true that if $v(x) = v(0)$ then $x = 0$, as can be seen by considering any abelian group. However, for an idempotent hypergroup, this is true. It is also true for any hyperdomain which is not a ring, as the following proposition shows.

Proposition 9.2.15. *Let H be a hypergroup. Let $x \in H$. Then $v(x) = v(0)$ if and only if $x + y$ is a singleton set for all $y \in H$. If H is idempotent and $v(x) = v(0)$ then $x = 0$. If H is a hyperring, which is not a ring, and if $v(x) = v(0)$, then x is a zero-divisor.*

Proof. For the first part, suppose $v(x) = v(0)$. Then $x - x = 0$. Let $y, z \in H$, with $z \in x + y$. Then $y \in z - x$, so $x + y \subseteq z - x + x = z$. Hence $x + y$ is a singleton set. Conversely suppose that $x + y$ is a singleton for all $y \in H$, in particular for $y = -x$. Then $x - x = 0$, so $v(x) = v(0)$.

For the second part of the lemma, let H be idempotent and $v(x) = v(0)$. Then $x \leq 0$ so $x = x + 0 = 0$.

For the third part, suppose H is a non-archimedean hyperring. We assume x is not a zero-divisor. Since $v(x) = v(0)$, we have $x(1 - 1) = x - x = 0$. Since x is not a zero-divisor, $1 - 1 = 0$, and hence $a - a = 0$ for all $a \in H$. Hence $v(a) = v(0)$ for all $a \in H$. By the first part of the lemma $a + b$ is single valued for all a, b, so H is a ring.

□

We will show that if H is a hyperring, the valuation is multiplicative. First, we will prove the following lemma.

Lemma 9.2.16. *Let H be a hyperring. Let $x, y, z \in H$ and suppose $v(x) \leq v(y)$. Then $v(xz) \leq v(yz)$.*

Proof. We are given that $x - x \subseteq y - y$. Any element of $xz - xz = z(x - x)$ has the form $z\alpha$ where $\alpha \in x - x \subseteq y - y$. Hence $z\alpha \in z(y - y) = yz - yz$, so $xz - xz \subseteq yz - yz$ as desired. □

Proposition 9.2.17. *Let H be a non-archimedean hyperring. Then there is a unique monoid structure on $H/\sim$ such that $v : H \to H/\sim$ is a homomorphism of monoids.*

Proof. Note every element of $H/\sim$ has the form $v(x)$ for some $x \in H$. We must define multiplication by $v(x)v(y) = v(xy)$. We now check is that this multiplication is well defined. That is, we must show that if $v(x) = v(a)$ and $v(y) = v(b)$ then $v(xy) = v(ab)$. Since $v(x) \leq v(a)$ and $v(y) \leq v(b)$, lemma 9.2.16 gives $v(xy) \leq v(ay) \leq v(ab)$. Similarly $v(ab) \leq v(xy)$. Hence $v(xy) = v(ab)$, so multiplication is well defined. Clearly this multiplication makes $H/\sim$ into a monoid and makes v a homomorphism. The quotient monoid structure is the only monoid structure on $H/\sim$ such that v is a homomorphism, and hence this multiplicative structure is unique. □

As an application of the valuation on an idempotent multiring, we prove the following theorem which allows us to relate the ideals of certain multirings to strong ideals in idempotent semirings. Recall that an ideal I in an idempotent semiring is strong if whenever $x + y \in I$, one has $x \in I$. The special case of this theorem where

H is the symmetrization of a selective semigroup was proven by Jai Ung Jun.[21]

Theorem 9.2.18. *Let H be an idempotent multiring. Suppose that for all $x, y \in H$ there exists $z \in H$ with $v(z) = \sup(v(x), v(y))$. Then $H/\sim$ is an idempotent semigroup. Suppose we equip $H/\sim$ with a multiplication making it an idempotent semiring such that for all $x, y \in H$ one has $v(xy) \leq v(x)v(y)$ and there exists $x' \sim x$ and $y' \sim y$ with $v(x'y') = v(x)v(y)$[1]. Then there is a one-to-one correspondence between ideals of H and strong ideals of the idempotent semiring $H/\sim$.*

Proof. It is clear that $H/\sim$ is an idempotent semigroup since we assumed the existence of least upper bounds. Let $J \subseteq H/\sim$ be a strong ideal. Let $I \subseteq H$ be its preimage under v. If $x, y \in I$ then $v(x), v(y) \in J$ so $\sup(v(x), v(y)) \in J$. Since the ideal J is strong, by the ultrametric inequality one gets $v(x + y) \subseteq J$, so $x + y \subseteq I$. Suppose $x \in I$ and $r \in H$. Then $v(x) \in J$ so $v(r)v(x) \in J$. Since J is strong and $v(rx) \leq v(r)v(x)$, $v(rx) \in J$ so $rx \in I$.

For the converse, suppose $I \subseteq H$ is an ideal. Let $J \subseteq H/\sim$ be its image under v. Suppose $x \in I$ and $v(y) \leq v(x)$. Then $y \in y - y \subseteq x - x \subseteq I$. In particular if $v(y) \in J$ one has some $x \in I$ with $v(x) = v(y)$, so $y \in I$, which implies that $I = v^{-1}(J)$. The above fact also implies that if $s, t \in H/\sim$ with $t \in J$ and $s \leq t$ then $s \in J$. It remains to show that J is an ideal. To show it is closed under supremum, let $s, t \in J$. Pick $x, y \in I$ with $s = v(x)$ and $t = v(y)$. Then there exists $z \in x + y \subseteq I$ with $\sup(s, t) = v(z)$. Hence $\sup(s, t) \in J$. We now show J is closed under multiplication.

[1] These conditions on the multiplicative structure are automatic if we assume that H is a hyperring rather than just a multiring.

Let $s = v(x) \in J$ and let $t = v(y) \in H/\sim$. Then there exists x', y' with $s = v(x')$, $t = v(y')$ and $st = v(x'y')$. Since $x' \in I$, it follows that $x'y' \in I$ so $st \in J$, as desired. □

We now consider a hypergroup analogue of the notion of a selective semigroup. Note that x and y are treated differently in the definition.

Definition 9.2.19. A hypergroup H is selective if it is idempotent and for all $x, y \in H$ one has either $x = x + y$ or $y \in x + y$.

Note that the second part of the definition of selectivity implies that $x \in x + x$, so instead of requiring selective hypergroups to be idempotent, we can instead require that they are non-archimedean.

Just as a selective semigroup corresponds to a totally ordered set, selective hypergroups induce totally ordered sets.

Lemma 9.2.20. *Let H be a selective hypergroup. Then $H/\sim$ is totally ordered.*

Proof. If $x = x + y$ then $y \leq x$. If $y \in x + y$ then $x \leq y$. □

The asymmetry between x and y in the definition of a selective hypergroup is used in the first part of the following lemma. The first part of the lemma tells us that the valuation tells us how to add two elements with unequal valuation. The valuation also tells us how to subtract an element from itself. The only part of the additive law that is not determined by the valuation is how to add two elements of equal valuation which are not negatives of each other. The second part of the lemma shows how the valuation constrains this part of the additive law.

Lemma 9.2.21. *Let H be a selective hypergroup. Let $x, y \in H$. If $v(x) > v(y)$, then $x + y = x$. If $v(x) = v(y)$ and $x \neq -y$ then for all $z \in x + y$, we obtain $v(z) = v(x)$.*

Proof. Suppose $v(x) > v(y)$. Then $y \notin x + y$. Hence, by selectivity, $x = x + y$. On the other hand, suppose that $v(x) = v(y)$ and $x \neq -y$, and let $z \in x + y$. One has $v(z) \leq v(x)$ by lemma 9.2.13. One also has that $x \in z - y$. Since $x \neq -y$, $-y \neq z - y$. Hence by selectivity, $z \in z - y$ so $v(x) = v(-y) \leq v(z)$. Thus $v(x) = v(z)$. □

We now give a characterization of selective hypergroups as hypergroups with a valuation map satisfying certain hypotheses.

Theorem 9.2.22. *Let H be a hypergroup. Suppose H is equipped with a surjective map $v : H \to \Gamma$ to a totally ordered set Γ. Suppose that for all $x, y \in H$, and all $z \in x + y$, one has $v(z) \leq \max(v(x), v(y))$. Suppose also that for all $x, y \in H$ with $v(x) < v(y)$, one has $x + y = y$. Suppose that for all $x \in H$, one has $x - x = \{y \in H \mid v(y) \leq v(x)\}$. Then H is selective. There is an order preserving bijection $H/\sim \cong \Gamma$, and upon identifying the two totally ordered sets the map v becomes the valuation of H. Conversely, if H is selective, then its valuation satisfies all of the above hypotheses.*

Proof. We have already proven the converse. Suppose $v : H \to \Gamma$ satisfies the hypotheses of the theorem. Let $x \in H$. We first check that $x - x = (x + x) - (x + x)$, or equivalently $x - x = (x - x) + (x - x)$. One inclusion is clear from $0 \in x - x$. On the other hand, suppose $w, z \in x - x$. If $t \in w + z$ then $v(t) \leq \max(v(w), v(z)) \leq v(x)$ so $t \in x - x$. Hence $w + z \subseteq x - x$ so $(x - x) + (x - x) \subseteq x - x$. Now suppose $x, y \in H$. We claim that either $x = x + y$ or $y \in x + y$. In other words, we wish to show either $x = x + y$ or $v(x) \leq v(y)$. This follows from the hypothesis that if $v(x) > v(y)$ then $x = x + y$.

To show there is an order preserving bijection $H/\sim \to \Gamma$ which identifies v with the valuation of the selective hyperfield H, it suffices to show that $v(x) \leq v(y)$ if and only if $x \leq y$ with respect to the relation $\leq$ of Definition 9.2.6. Suppose $x \leq y$. Then $x \in y - y$, so $v(x) \leq v(y)$. Conversely, suppose $v(x) \leq v(y)$. Then $x \in y - y$ so $x \leq y$. □

Finally we characterize those idempotent hypergroups which are equipped with the trivial valuation. Such hypergroups will play a prominent role in the constructions given in future sections of this paper.

Proposition 9.2.23. *Let H be hypergroup. Suppose H is idempotent and one has $v(x) = v(y) \neq v(0)$ for all $x, y \in H$ satisfying $x, y \neq 0$. Then $x - x = H$ for all nonzero $x \in H$. Conversely suppose that $x - x = H$ for all nonzero $x \in H$. Then H is selective and $v(x) = v(y)$ whenever $x, y \neq 0$.*

Proof. Let H be idempotent with $v(x) = v(y)$ for all $x, y \neq 0$. Let $x \neq 0$. Then $v(y) \leq v(x)$ for all $y \in H$. Hence $y \in x - x$ for all $y \in H$. This implies $x - x = H$.

Conversely, suppose $x - x = H$ for all $x \neq 0$. Let $x, y \in H$. If $y = 0$, $x = x + y$. If $y \neq 0$, then $x \in y - y$ so $y \in x + y$. Hence either $x = x + y$ or $y \in x + y$. Also, $(x+x) - (x+x) = (x-x) + (x-x) = H + H = H = x - x$. Hence H is selective. If $x, y \neq 0$, then $x \in y - y$ so $v(x) \leq v(y)$ and similarly $v(y) \leq v(x)$ so $v(x) = v(y)$. □

9.3 Constructing hypergroups from totally ordered sets

In,[14] Simon Henry has produced a construction which takes a semigroup to a hypergroup, and which restricts to the Grothendieck group construction on cancellative semigroups. This construction is perhaps most interesting when applied to a selective semigroup. The construction should perhaps be thought of as a sort of base change from $\mathbb{B}$ to $\mathbb{S}$. It is natural to wonder whether one can do a similar construction with a different hypergroup in place of $\mathbb{S}$. We now give such a construction.

Definition 9.3.1. Let S be a totally ordered set. Let k be a canonical abelian hypergroup in which $x - x = k$ for all nonzero $x \in k$. We will write $k^\times$ for the set of nonzero elements of k. We define $\mathcal{T}(S, k) = \{0\} \cup S \times k^\times$. We define a multivalued addition on $\mathcal{T}(S, k)$ as follows. $0 + x = x + 0 = x$ for all $x \in \mathcal{T}(S, k)$. If $(x, a), (y, b) \in S \times k^\times$ with $x > y$, we let $(x, a) + (y, b) = (y, b) + (x, a) = (x, a)$. If $(x, a), (y, b) \in \mathcal{T}(S, k)$ satisfy $x = y$ and $a \neq -b$ then we let $(x, a) + (y, b) = \{(x, c) \mid$

$c \in a + b\}$. We let $(x, a) + (x, -a) = \{(y, c) \mid y \leq x\}$. We will let v denote the map $v : \mathcal{T}(S, k) \to S \cup \{0\}$ given by $v(0) = 0$ and $v((x, a)) = x$.

Example 9.3.2. Let $\mathbb{S}$ denote the hyperfield of signs. Let S be a totally ordered set. Then $\mathcal{T}(S, \mathbb{S})$ gives the same result as applying Simon Henry's symmetrization functor to the idempotent semigroup $S_{\max}$.

Some more examples will be given in section 9.4, where we will use this construction to produce hyperfields.

In Theorem 9.3.9, we shall show that, $\mathcal{T}(S, k)$ is a canonical abelian hypergroup. As a first step we will state some basic properties of it's multivalued addition operation.

Remark 9.3.3. Let $x, y \in \mathcal{T}(S, k)$ be nonzero. Then we may write $x = (u, a)$ and $y = (v, b)$. Then it is easy to see that $0 \in x +_K y$ if and only if $u = v$ and $a = -b$. Hence we will write $-x$ instead of $(u, -a)$.

Lemma 9.3.4. *Let S, k be as in Definition 9.3.1. Let $x, y \in \mathcal{T}(S, k)$. Then for all $z \in x + y$, $v(z) \leq \max(v(x), v(y))$, and equality holds unless $x = -y$.*

Proof. This is clear from the definition. □

We will write $v(x + y) = \{v(z) \mid z \in x + y\}$. For $S, T \subseteq H \cup 0$, we write $S \leq T$ to mean that for all $s \in S, t \in T$ we have $s \leq t$. With this notation, the above lemma states that $v(x + y) \leq \max(v(x), v(y))$ with equality when $x \neq -y$.

Lemma 9.3.5. *Let S, k be as in Definition 9.3.1. Let $s \in S \cup \{0\}$. Let $B = \{y \in \mathcal{T}(S,k) \mid v(y) \leq s\}$. Then if $v(x) \leq s$ then $x + B = B$. If $v(x) > s$ then $x + B = x$. Let $B' = \{y \in \mathcal{T}(S,k) \mid v(y) < s\}$. If $v(x) < s$, $x + B' = B'$. If $v(x) \geq s$, $x + B' = x$.*

Proof. If $v(x) > s$, this follows from the definition, so we suppose $v(x) \leq s$. Lemma 9.3.4 implies that $x + B \subseteq B$, so we prove the reverse inclusion. Let $b \in B$. First suppose $v(b) \leq v(x)$. This implies that $b \in x - x \subseteq x + B$, where the second inclusion uses the fact that $-x \in B$ since $v(x) \leq h$. It remains to consider b with $v(b) > v(x)$. But then $b = x + b \in x + B$. Thus $B \subseteq x + B$ as desired. The claim about B' is proved similarly. □

We can now prove associativity.

Proposition 9.3.6. *The addition on $\mathcal{T}(S,k)$ is associative.*

Proof. Let $x, y, z \in \mathcal{T}(S,k)$. We wish to show $(x+y)+z = x+(y+z)$. If any of the variables is zero, it is clear, so we may assume otherwise.

Suppose that one of $v(x), v(y), v(z)$ is strictly larger than the other two. If $v(y) > v(x)$ and $v(y) > v(z)$ then $(x+y)+z = y+z = y$ and $x+(y+z) = x+y = y$. The cases where $v(z) > \max(v(x), v(y))$ or $v(x) > \max(v(y), v(z))$ are treated similarly. Thus associativity holds unless there is a tie for the largest element of $\{v(x), v(y), v(z)\}$.

Suppose now that one of $v(x), v(y), v(z)$ is strictly smaller than the other two. First we consider the case $v(x) < \min(v(y), v(z))$. Then $(x+y)+z = y+z$, so we must show that $x + (y+z) = y+z$. If $y \neq -z$, this follows from lemma 9.3.4, which tells us that $v(y+z) = \max(v(y), v(z)) > v(x)$. If $y = -z$, then we may let $s = v(y)$ in lemma 9.3.5. The set B in lemma 9.3.5 is then $y + z$, so the lemma states that $x + (y + z) = y + z$. The case where $v(z) < \min(v(y), v(x))$ is similar, so we now consider the case where $v(y) < \min(v(z), v(x))$. Then $(x+y)+z = x+z = x+(y+z)$.

In all of the remaining cases we have $v(x) = v(y) = v(z)$. We write $x = (s, a)$, $y = (s, b)$ and $z = (s, c)$. If $x \neq -y$, $z \neq -y$, $-x \notin y + z$ and $-z \notin x + y$, then the associative law never involves adding an element to it's negative. In this case $(x + y) + z = (s,(a + b) + c) = (s,(a + (b + c)) = x + (y + z)$.

We are now reduced to the four cases where $x = -y$, $z = -y$, $-x \in y + z$ or $-z \in x + y$. Before addressing associativity in these cases, we will show that if either $x = -y$ or $-z \in x+y$, then either $-x \in y+z$ or $z = -y$. A similar argument will show conversely that if $z = -y$ or $-x \in y + z$ then either $x = -y$ or $-z \in x + y$. Suppose first that $x = -y$, so that $a = -b$. We may suppose $z \neq -y$ since otherwise this claim holds. Since $a + b = k$, $a + (b + c) = (a + b) + c = k + z = k$. Thus $0 \in a + (b + c)$, so $-a \in b + c$. Since $z \neq -y$, $y + z = (s, b + c)$, so $-x = (s, -a) \in y + z$. Suppose instead that $-z \in x + y$ but $x \neq -y$. Then $x + y = (s, a + b)$, so $-c \in a + b$. Thus $0 \in (a + b) + c = a + (b + c)$. We may proceed as in the case $x = -y$, to see that the claim holds.

Now we may assume that either $x = -y$ or $-z \in x + y$ and that either $z = -y$ or $-x \in y + z$. Let $B = \{t \in \mathcal{T}(S, k) \mid v(t) \leq s\}$. If $x = -y$ then lemma 9.3.5 implies $(x + y) + z = B + z = B$. On the other hand if $-z \in x + y$ then $B = (-z) + z \subseteq$

$(x+y)+z \subseteq B$, where the last inclusion follows from lemma 9.3.4. Thus we see that in either of the two cases, $(x+y)+z = B$. A similar argument using the fact that either $z = -y$ or $-x \in y+z$ shows that $x+(y+z) = B$. Hence $x+(y+z) = (x+y)+z$. □

To prove that the hypergroup $\mathcal{T}(S, k)$ is canonical we need the following lemma.

Lemma 9.3.7. *Let S, k be as in Definition 9.3.1. Let $x, y \in \mathcal{T}(S, k)$. Suppose $v(x) \leq v(y)$. Then $y \in x + y$.*

Proof. This is trivial except when $v(x) = v(y) \neq 0$ and $x \neq -y$. Let $x = (s, a)$ and $y = (s, b)$. Since $a \in b - b$, we obtain $b \in a + b$. Then $y = (s, b) \in (s, a + b) = x + y$, where the last equality uses $a \neq -b$. □

Proposition 9.3.8. *Let S, k be as in Definition 9.3.1. Let $x, y, z \in \mathcal{T}(S, k)$. Suppose $x \in y + z$. Then $z \in x - y$.*

Proof. If any variable is zero, the result is clear by using the fact that zero is the additive identity and using Remark 9.3.3. Suppose $v(z) < v(y)$. Then $y + z = y$ so $x = y$. Then $z \in x - y = y - y$ follows since $v(z) < v(y)$. If $v(z) > v(y)$, the same argument holds. Thus we may assume $v(y) = v(z)$. Write $y = (s, a)$ and $z = (s, b)$ and $x = (t, c)$. Let $B = \{u \in \mathcal{T}(S, k) \mid v(u) \leq s\}$. Suppose first that $y \neq -z$. Then $x \in y+z = (s, a+b)$, so $s = t$ and $c \in a+b$. Hence $b \in c-a$. If in addition $x \neq y$, then $x - y = (s, c - a)$ so $z \in x - y$ as desired. If $x = y$, then $x - y = B$ contains z. Now we consider the case $y = -z$. We have $v(x) \leq v(z)$. By 9.3.7, $z \in x + z = x - y$. □

We have now proved the following theorem.

Theorem 9.3.9. *Let S, k be as in Definition 9.3.1. Then $\mathcal{T}(S, k)$ is a canonical abelian hypergroup.*

In fact, this hypergroup is selective.

Theorem 9.3.10. *The hypergroup $\mathcal{T}(S, k)$ is selective. Furthermore, one may identify S with $\mathcal{T}(S, k)/\sim$ and v with the valuation of Definition 9.2.7.*

Proof. We check the hypotheses of Theorem 9.2.22. Lemma 9.3.4 gives the ultrametric inequality. Let $(x, a), (y, b) \in \mathcal{T}(S, k)$. Suppose $v((x, a)) > v((y, b))$ so $x > y$. Then by definition, $(x, a) = (x, a) + (y, b)$ as desired. Also $(x, a) - (x, a) = (x, a) + (x, -a) = \{(y, c) \mid v((y, c)) = y \leq x = v((x, a))\}$. Clearly, v is surjective. Thus all hypotheses hold and Theorem 9.2.22 can be applied. $\square$

9.4 The hyperfields $\mathbf{T}(G, H, v, k, \alpha)$ and $\mathcal{T}(H, k)$

Definition 9.4.1. Let G and H be abelian groups with H totally ordered. Let $v : G \to H$ be a homomorphism. Let k be a hyperfield such that $1 - 1 = k$. Let $\alpha : k^\times \to \ker v$ be an isomorphism. We define $\mathbf{T}(G, H, v, k, \alpha) = G \cup \{0\}$. We extend v to a map $\mathbf{T}(G, H, v, k, \alpha) \to H \cup \{0\}$. $\mathbf{T}(G, H, v, k, \alpha)$ will be given the obvious notion of multiplication, and a multivalued addition operation defined as follows. For $x \in K$, we let $x + 0 = 0 + x = x$. For $x, y \in G$ with $v(x) < v(y)$, we let $x + y = y + x = y$. For $x, y \in G$ with $v(x) = v(y)$ and $x \neq \alpha(-1)y$, we let $x + y = u(\alpha(\alpha^{-1}(u^{-1}x) +_k \alpha^{-1}(u^{-1}y))$ where $u \in G$ is any element with $v(u) = v(x)$, and $+_k$ denotes addition in k. If $x = \alpha(-1)y$, we let $x + y = \{z \in K \mid v(z) \leq v(x)\}$. $\mathcal{O}_{\mathbf{T}(G,H,v,k,\alpha)}$ will denote the set of $x \in \mathbf{T}(G, H, v, k, \alpha)$ with $v(x) \leq 1$. $\mathfrak{m}_{\mathbf{T}(G,H,v,k,\alpha)}$ will denote the set of $x \in \mathbf{T}(G, H, v, k, \alpha)$ with $v(x) < 1$.

One of our main goals for this section is to show $\mathbf{T}(G, H, v, k, \alpha)$ is a selective hyperfield. We will then consider the question of which selective hyperfields arise in this way. However, before doing these this, we will give some examples of this construction. First we will consider a special case which contains some of the most interesting examples.

Definition 9.4.2. Let H be a totally ordered abelian group. Let k be a hyperfield in which $1 - 1 = k$. We will let $\mathcal{T}(H, k) = \mathbf{T}(H \times k^\times, H, p, k, j)$ where $p : H \times k^\times \to H$ is the projection and $j : k^\times \to \{1\} \times k^\times$ is the obvious isomorphism.

This notation appears to conflict with that of Definition 9.3.1, but we will see in Corollary 9.4.9 that they describe the same object.

Example 9.4.3. Let H be a totally ordered group. Then $\mathcal{T}(H, \mathbb{K}) = H \cup \{0\}$ with the addition given by $x + y = \max(x, y)$ if $x \neq y$, and $x + x = \{z \in H \cup \{0\} \mid z \leq x\}$. By inspection this is the same

Example 9.4.4. Let H be a totally ordered abelian group. Then $\mathcal{T}(H, \mathbb{S}) = H \times \{1, -1\} \cup \{0\}$. The addition is given by $(x, s) + (y, t) = (x, s)$ if $x > y$, $(x, s) + (y, t) = (y, t)$ if $x < y$, $(x, s) + (x, s) = (x, s)$ and $(x, s) + (x, -s) = \{0\} \cup \{(z, t) \in H \times \{1, -1\} \mid z \leq x$. One may check that this agrees with the result of applying Simon

Henry's symmetrization functor to the idempotent semifield $H_{\max}$. As a special case, we note that the real tropical hyperfield can be described as $\mathcal{T}\mathbb{R} = \mathcal{T}(\mathbb{R}_{\geq 0}, \mathbb{S}) = \mathbf{T}(\mathbb{R}^\times, \mathbb{R}_{\geq 0}, |\ \ |, \mathbf{S}, \mathrm{id})$.

Example 9.4.5. Let T be the circle group. Let $k = T \cup \{0\}$. We define a multivalued addition on k as follows. For all $x \in k$, we let $x + 0 = 0 + x = x$. For $x \neq 0$, let $-x$ denote the antipode of x on the circle. Then we define $x - x = k$. For $x \neq -y$, where x and y are nonzero, we let $x + y$ denote the shortest arc of the circle containing x and y. Then the complex tropical hyperfield is $\mathcal{T}(\mathbb{R}_{\geq 0}, k) = \mathbf{T}(\mathbb{C}^\times, \mathbb{R}_{\geq 0}, |\ \ |, k, \mathrm{id})$.

Remark 9.4.6. If $x, y \in \mathbf{T}(G, H, v, k, \alpha)$ then it is easy to see that $0 \in x +_K y$ if and only if $y = \alpha(-1)x$. Hence we will write $-x$ instead of $\alpha(-1)y$.

Lemma 9.4.7. *Let G, H, v, k, α be as in Definition 9.4.1. Then the addition on $\mathbf{T}(G, H, v, k, \alpha)$ is well defined.*

Proof. Addition is clearly well-defined except when $v(x) = v(y)$ and $x \neq -y$, so we will assume this is the case. Let $u, u' \in G$ with $v(u) = v(u') = v(x)$. Then $uu'^{-1} \in kerv$, so $u(\alpha(\alpha^{-1}(u^{-1}x) +_k \alpha^{-1}(u^{-1}y)) = u'(uu'^{-1})(\alpha(\alpha^{-1}(u^{-1}x) +_k \alpha^{-1}(u^{-1}y)) = u'(\alpha(\alpha^{-1}(uu'^{-1})(\alpha^{-1}(u^{-1}x) +_k \alpha^{-1}(u^{-1}y)) = u'(\alpha(\alpha^{-1}(u'^{-1}x) +_k \alpha^{-1}(u'^{-1}y))$. Here the second equality uses that α is a group homomorphism and the third uses the distributive law on k. □

Proposition 9.4.8. *Let G, H, v, k, α be as in Definition 9.4.1. Suppose that $v : G \to H$ is surjective. Let $\mathcal{T}(H, k)$ be defined as in Definition 9.3.1 rather than Definition*

9.4.2. Let $i : H \to G$ be any function such that $v \circ i = \mathrm{id}$. The choice of i gives a bijection of sets $\eta : G \to H \times k^\times$, which induces a bijection $\eta : \mathbf{T}(G, H, v, k, \alpha) \to \mathcal{T}(H, k)$. This bijection is an isomorphism of hypergroups. Furthermore, for all $x \in \mathbf{T}(G, H, v, k, \alpha)$, we have $v(\eta(x)) = v(x)$, where the v on the left is as in Definition 9.3.1 and on the right, v is as in Definition 9.4.1.

Proof. One has a bijection $G \to H \times \ker v$ given by $x \mapsto (v(x), i(v(x))^{-1}x)$. Using α to identify $\ker v$ with $k^\times$ gives the bijection $\eta(x) = (v(x), \alpha^{-1}(i(v(x))^{-1}x))$, which is extended by defining $\eta(0) = 0$. It is clear from definitions that $v(\eta(x)) = v(x)$ in both cases. It remains to show the map η is an isomorphism of hypergroups.

Let $x, y \in \mathbf{T}(G, H, v, k, \alpha)$. We must show $\eta(x) + \eta(y) = \eta(x + y)$. If $x = 0$ or $y = 0$, this is clear. If $v(x) < v(y)$ then $v(\eta(x)) < v(\eta(y))$. Then $x + y = y$ and $\eta(x) + \eta(y) = \eta(y) = \eta(x + y)$. If $v(x) > v(y)$ a similar argument applies. So we can now assume $v(x) = v(y)$, and hence $v(\eta(x)) = v(\eta(y))$. One easily sees that $\eta(-x) = (v(x), i(v(x))^{-1}(-x)) = -\eta(x)$. We have two cases: Either $y = -x$ and hence $\eta(y) = -\eta(x)$ or $y \neq -x$ and hence $\eta(y) \neq \eta(x)$. Suppose first that $y = -x$. Then $x + y = \{t \in \mathbf{T}(G, H, v, k, \alpha) \mid v(t) \leq v(x)\}$, so $\eta(x + y) = \{\eta(t) \mid v(\eta(t)) \leq v(\eta(x))\} = \eta(x) + \eta(y)$. Now we consider the last case where $v(x) = v(y)$ and $y \neq -x$. Let $u = i(v(x)) = \eta^{-1}((v(x), 1))$. We easily see $v(u) = v(x)$. Then $x + y = u(\alpha(\alpha^{-1}(u^{-1}x) +_k \alpha^{-1}(u^{-1}y)))$. One easily sees that all $z \in x + y$ have $v(z) = v(u) = v(x)$. Hence for $z \in x+y$ we have $\eta(z) = (v(x), \alpha^{-1}(i(v(x))^{-1}z)) = (v(x), \alpha^{-1}(u^{-1}z))$. Thus $\eta(x+y) = (v(x), \alpha^{-1}(u^{-1}u(\alpha(\alpha^{-1}(u^{-1}x)+_k\alpha^{-1}(u^{-1}y))))) = (v(x), \alpha^{-1}(u^{-1}x)+_k$

$\alpha^{-1}(u^{-1}y))) = (v(x), \alpha^{-1}(u^{-1}x)) + (v(x), \alpha^{-1}(u^{-1}y)) = \eta(x) + \eta(y)$, as desired. □

Corollary 9.4.9. *Let H, k be as in Definition 9.4.2. Then definitions 9.4.2 and 9.3.1 produce the same selective hypergroup $\mathcal{T}(H, k)$.*

Proof. For the moment, we use the notation of Definition 9.3.1 rather than 9.4.2. We wish to show that $\mathcal{T}(H, k) = \mathbf{T}(H \times k^\times, H, p, k, j)$ as hypergroups. As sets, both equal $H \times k^\times \cup \{0\}$. Clearly $v : H \times k^\times \to H$ is surjective. Thus by Proposition 9.4.8, $\eta : \mathbf{T}(G, H, v, k, \alpha) \to \mathcal{T}(H, k)$ is an isomorphism. One ready checks that η is the identity map. □

Lemma 9.4.10. *Let G, H, v, k, α be as in Definition 9.4.1. Let $x, y \in \mathbf{T}(G, H, v, k, \alpha)$. Then for all $z \in x + y$, $v(z) \leq \max(v(x), v(y))$, and equality holds when $y \neq -x$. Furthermore $v(xy) = v(x)v(y)$.*

Proof. This is a consequence of lemma 9.3.4. □

We are now ready to prove distributivity.

Proposition 9.4.11. *Let G, H, v, k, α be as in Definition 9.4.1. The addition on $\mathbf{T}(G, H, v, k, \alpha)$ distributes over multiplication.*

Proof. Without loss of generality, we will assume that $k^\times = \ker v$, and $\alpha = \mathrm{id}$. Let $x, y, z \in \mathbf{T}(G, H, v, k, \alpha)$. We wish to show $z(x + y) = zx + zy$. If any of x, y, z is zero, it is clear. Suppose $v(x) < v(y)$. Then $v(zx) = v(z)v(x) < v(z)v(y) = v(zy)$, so $zx + zy = zy = z(x + y)$. The case where $v(x) > v(y)$ is similar, so we consider the case where $v(x) = v(y)$. Suppose first that $x \neq -y$. Then $x + y = x(1 +_k x^{-1}y)$, so that $z(x+y) = zx(1+_k x^{-1}y)$. Applying this argument to zx and zy instead of x and y gives $zx + zy = zx(1 +_k (zx)^{-1}zy) = zx(1 +_k x^{-1}y)$, so distributivity holds in this case. In the remaining case $x = -y$ so $zx = -zy$. Then $x+y = \{t \in \mathbf{T}(G, H, v, k, \alpha) \mid v(t) \leq v(x)\}$, and $zx + zy = \{s \in \mathbf{T}(G, H, v, k, \alpha) \mid v(s) \leq v(z)v(x)\}$. One easily sees that the map $t \mapsto zt$ and it's inverse $s \mapsto z^{-1}s$ give a bijective correspondence between $x + y$ and $zx + zy$, so $zx + zy = z(x + y)$. □

We can now conclude that $\mathbf{T}(G, H, v, k, \alpha)$ is a hyperfield.

Theorem 9.4.12. *Adopt the notation of Definition 9.4.1. Let $K = \mathbf{T}(G, H, v, k, \alpha)$. Then K is a selective hyperfield. Furthermore $\mathcal{O}_K$ is a subhyperring.*

Proof. We may assume without loss of generality that v is surjective because replacing H with image(v) leaves $\mathbf{T}(G, H, v, k, \alpha)$ unchanged. K is a selective hypergroup by Theorem 9.3.10 and Proposition 9.4.8. The distributive law is Proposition 9.4.11. The hyperfield axioms which only involve multiplication hold because $K = G \cup \{0\}$ with G a group. Showing that $\mathcal{O}_K$ is a subhyperring reduces to showing that it is closed under multiplication and is closed under addition in the sense that for $x, y \in \mathcal{O}_K$, $x + y \subseteq \mathcal{O}_K$. □

We will now compute the residue hyperfield of $\mathcal{O}_K$.

Proposition 9.4.13. *Use the notation of Definition 9.4.1. Let $K = \mathbf{T}(G, H, v, k, \alpha)$. Then $\mathfrak{m}_K \subseteq \mathcal{O}_K$ is the unique maximal ideal consisting of all non-units in $\mathcal{O}_K$. There* *is a canonical isomorphism* $\mathcal{O}_K/\mathfrak{m}_K \cong k$*.*

Proof. $\mathfrak{m}_K$ is an ideal by lemma 9.4.10. Let $x \in \mathcal{O}_K$. This means that $v(x) \leq 1$. Then $x \in \mathcal{O}_K^\times$ if and only if $v(x^{-1}) = v(x)^{-1} \leq 1$, which is true if and only if $v(x) \geq 1$. Also $x \in \mathfrak{m}_K$ if and only if $v(x) \geq 1$ does not hold. Then $x \in \mathcal{O}_K^\times$ if and only if $x \notin \mathfrak{m}_K$. From this it follows that $\mathfrak{m}_K$ is the unique maximal ideal.

Define a map $\pi : \mathcal{O}_K \to k$ by $\pi(x) = 0$ if $x \in \mathfrak{m}_K$, and $\pi(x) = \alpha^{-1}(x)$ if $x \in \ker v = \mathcal{O}_K^\times$. It is easy to see that π is a multiplicative homomorphism. π is surjective since $\mathcal{O}_K^\times$ surjects onto $k^\times$ and 0 maps to 0. I claim that for $x, y \in \mathcal{O}_K$, $\pi(x) = \pi(y)$ if and only if $x + \mathfrak{m}_K = y + \mathfrak{m}_K$.4 In fact, by lemma 9.3.5, $x + \mathfrak{m}_K = \mathfrak{m}_K$ if $x \in \mathfrak{m}_K$ and $x + \mathfrak{m}_K = x$ otherwise. The claim follows easily from this statement. Thus we have an induced bijection $\bar{\pi} : \mathcal{O}_K/\mathfrak{m}_K \to k$, which is easily seen to be multiplicative. Thus we must only check that the addition on both sides of the desired isomorphism agree.

Let $\bar{x}, \bar{y} \in \mathcal{O}_K/\mathfrak{m}_K$ be the classes of elements $x, y \in \mathcal{O}_K$. We wish to show $\bar{\pi}(\bar{x} + \bar{y}) = \bar{\pi}(\bar{x}) + \bar{\pi}(\bar{y})$. If $\bar{x} = 0$ or $\bar{y} = 0$, then this is clear. Hence we may assume they are nonzero, so that $v(x) = v(y) = 1$. Let $\bar{z} \in \bar{x} + \bar{y}$. By definition of the quotient hyperring, this is equivalent to saying that $\bar{z}$ is the class of some $z \in \mathcal{O}_K$ such that $z \in x + y$. Suppose first that $x \neq -y$. Then $v(z) = 1$ by lemma 9.4.10, so that $\bar{\pi}(\bar{z}) = \pi(z) = \alpha^{-1}(z)$. The assumption that $x \neq -y$ also implies $x + y = \alpha(\alpha^{-1}(x) +_k \alpha^{-1}(y))$. Hence $z \in \alpha(\alpha^{-1}(x) +_k \alpha^{-1}(y))$ so $\bar{\pi}(\bar{z}) = \alpha^{-1}(z) \in \alpha^{-1}(x) +_k \alpha^{-1}(y) = \bar{\pi}(\bar{x}) + \bar{\pi}(\bar{x})$. On the other hand suppose that $x = -y$.

Then $\alpha^{-1}(x) = -\alpha^{-1}(y)$, so $\bar{\pi}(\bar{z}) \in k = \alpha^{-1}(x) +_k \alpha^{-1}(y) = \bar{\pi}(\bar{x}) + \bar{\pi}(\bar{x})$. Hence $\bar{\pi}(\bar{x}+\bar{y}) \subseteq \bar{\pi}(\bar{x})+\bar{\pi}(\bar{y})$. For the reverse inclusion, let $\pi(z) \in \bar{\pi}(\bar{x})+\bar{\pi}(\bar{y}) = \pi(x)+\pi(y)$[2]. Suppose first that $x \neq -y$. Then $x + y = \alpha(\alpha^{-1}(x) +_k \alpha^{-1}(y)) = \alpha(\pi(x) + \pi(y))$. Then $\alpha(\pi(z)) \in x + y$. Furthermore $\pi(x) = \alpha^{-1}(x) \neq \alpha^{-1}(-y) = -\pi(y)$, so the fact that $\pi(z) \in \pi(x) + \pi(y)$ implies $\pi(z) \neq 0$. Then $v(z) = 1$, so $z = \alpha(\pi(z)) \in x + y$. Then $\pi(z) = \bar{\pi}(\bar{z}) \in \bar{\pi}(\bar{x} + \bar{y})$ as desired. Now suppose instead that $x = -y$. Then $\bar{\pi}(\bar{x}) = -\bar{\pi}(\bar{y})$ so $\bar{\pi}(\bar{x} + \bar{y}) = k$. Hence $\bar{\pi}(\bar{x}) + \bar{\pi}(\bar{y}) \subseteq \bar{\pi}(\bar{x} + \bar{y})$ in either case.

□

We now consider the question of which hyperfields arise via the construction of Definition 9.4.1. The answer is provided by the following theorem.

Theorem 9.4.14. *Let K be a hyperfield. Let H be a totally ordered group. Let $v : K^\times \to H$ be a group homomorphism, which we extend to a map $v : K \to H \cup \{0\}$. Suppose that for all $x, y \in K$, we have $v(x+y) \leq max(v(x), v(y))$. Suppose in addition that for all $x, y \in K$ with $v(x) < v(y)$ we have $x + y = y$. Suppose that for all $x \in K$, $x - x = \{y \in K \mid v(y) \leq v(x)\}$. Let $\alpha : \mathcal{O}_K/\mathfrak{m}_K^\times \to \ker v$ be given by $\alpha(\bar{x}) = x$ where $\bar{x}$ is the coset of $x \in \mathcal{O}_K$. Then α is a well defined isomorphism, $k = \mathcal{O}_K/\mathfrak{m}_K$ is a hyperfield satisfying $1 +_k (-1) = k$, and $K = \mathbf{T}(K^\times, H, v, \mathcal{O}_K/\mathfrak{m}_K, \alpha)$.*

Proof. Note that $v(-1)^2 = v(1) = v(1)^2$. Since Γ is totally ordered, $v(-1) = v(1)$. The properties of v imply that $\mathcal{O}_K = \{x \in K \mid v(x) \leq 1\}$ is closed under addition, multiplication, and negation, and contains 0 and 1, and so is a hyperring. Similarly

[2] By surjectivity of π, every element has this form.

$\mathfrak{m}_K = \{x \in K \mid v(x) < 1\}$ is an ideal. It is easily seen that it contains all non-units, so is maximal and $k = \mathcal{O}_K/\mathfrak{m}_K$ is thus a hyperfield as claimed. In $\mathcal{O}_K$ we have $1 + (-1) = \mathcal{O}_K$. This can easily be seen to imply that $1 +_k (-1) = k$.

Let $\beta : \ker v \to \mathcal{O}_K/\mathfrak{m}_K^\times$ be the map $\beta(x) = \bar{x}$ where $\bar{x}$ is the coset of x. We will show β is an isomorphism which will imply the claim about $\alpha = \beta^{-1}$. Let $x \in \mathcal{O}_K$. If $x \in \ker v$ then $\bar{x} = \beta(x)$ is in the image of β. Otherwise $v(x) < 1$, so $x \in \mathfrak{m}_K$. Then $\bar{x} = 0$ is not a unit. Hence β is surjective. Now suppose $\beta(x) = \beta(y)$ for some $x, y \in \ker v$. Then $\bar{x} = \bar{y}$ so $x + \mathfrak{m}_K = y + \mathfrak{m}_K$. But $v(x) = v(y) = 1 > v(\mathfrak{m}_K$. Thus by our hypothesis on adding elements with different valuation, $x = x + \mathfrak{m} = y + \mathfrak{m} = y$, so β is injective. Clearly β is multiplicative, so is a group isomorphism as desired.

Let $T = \mathbf{T}(K^\times, H, v, \mathcal{O}_K/\mathfrak{m}_K, \alpha)$. Clearly $K = T$ as sets, or even as multiplicative monoids, since both are $\{0\} \cup K^\times$. Furthermore, the valuations on K and T coincide. To show they are equal as hyperfields, we must show the addition operations on both agree. We denote the addition on K by $+_K$ and on T by $+_T$. If $v(x) > v(y)$ then $x +_K y = x = x +_T y$. A similar situation holds if $v(y) > v(x)$. Thus we may assume that $v(x) = v(y)$. Note that $X +_K y = x(1 +_K x^{-1}y)$ and similarly for T. Thus it suffices to show that $1 +_K x^{-1}y = 1 +_T x^{-1}y$. Since $v(x^{-1}y) = 1$, it suffices to show that for all $z \in K$ with $v(z) = 1$ we have $1 +_K z = 1 +_T z$. If $z = -1$, then both sides are $\mathcal{O}_K$. We assume otherwise. Then $\alpha(1 +_k \bar{z}) = \alpha(1 +_k \alpha^{-1}(z)) = 1 +_T z$. Let $t \in 1 +_T z$. Then $v(t) = 1$ and $\bar{t} = \alpha^{-1}(t) \in 1 +_k \bar{z}$. Since $k = \mathcal{O}_K/\mathfrak{m}_K$, there exists $t' \in \mathcal{O}_K$ which reduces to $\bar{t}$ modulo $\mathfrak{m}_K$ such that $t' \in 1 +_K z$. Since $\bar{t} \neq 0$,

$v(t) = v(t') = 1$. Consequently $t' = t' +_K \mathfrak{m}_K = t +_K \mathfrak{m}_K = t$. Thus $t \in 1 +_K z$, and $1 +_T z \subseteq 1 +_K z$. Conversely let $t \in 1 +_K z$. If $v(t) < 1$, then $0 \in 1 +_k \bar{z}$, so $\bar{z} = -1$. Then $-1 = -1 +_K \mathfrak{m}_K = z +_K \mathfrak{m}_K = z$, which we assumed did not occur. Hence $v(t) = 1$. Now $\beta(t) = \bar{t} \in 1 +_k \bar{z} = 1 +_k \beta(z)$. Then $t \in \alpha(1 +_k \alpha^{-1}(z)) = 1 +_T z$ as desired. □

Corollary 9.4.15. *Every selective hyperfield arises via the construction of Definition 9.4.1.*

Proof. Let K be a selective hyperfield. Let $H = K/\sim$. Let v be the valuation associated to the selective hyperfield K. Apply Theorem 9.4.14. □

Chapter 10

The hypergroup structure on a modular lattice

Ştefănescu and Viro have independently discovered that if S is a totally ordered set, then one may make $\{0\} \cup S$ into a hypergroup by defining $x + x = \{t \mid t \leq x\}$ and $x + y = \max(x, y)$ for $x \neq y$.[17,22] In the notation of the previous chapter, this hypergroup is $\mathcal{T}(S, \mathbb{K})$. In this chapter we will show that this construction may be extended to a much larger class of posets, including modular lattices.

10.1 Regular posets

Definition 10.1.1. Let S be a poset. A multiset $\{x_1, \ldots, x_n\} \subseteq S$ is called a corner set if for all j and any $z \in S$ satisfying $x_i \leq z$ for all $i \neq j$, one has $x_j \leq z$.

Remark 10.1.2. Let S be totally ordered. $\{x_1, \ldots, x_n\}$ is a corner set if and only if the maximum occurs at least twice.

Definition 10.1.3. Let S be a poset, and let $x, y \in S$. We write $x \vee y$ for the least upper bound of x and y if it exists, and $x \wedge y$ for the greatest lower bound if it exists.

When least upper bounds exist, we have the following alternate description of a corner set.

Lemma 10.1.4. *Suppose that any two elements of a poset S have a least upper bound. Then $\{x_1, \ldots, x_n\}$ is a corner set if and only if for all j, $\bigvee_{i=1}^{n} x_i = \bigvee_{i \neq j} x_i$.*

Proof. Suppose $\{x_1, \ldots, x_n\}$ is a corner set. Fix j between 1 and n. Let $y = \bigvee_{i \neq j} x_i$. Since $\{x_1, \ldots, x_n\}$ is a corner set, $x_j \leq y$, so $y = y \vee j = \bigvee_{i=1}^{n} x_i$. Conversely suppose that for all j, $\bigvee_{i=1}^{n} x_i = \bigvee_{i \neq j} x_i$. Pick an index j, and suppose $z \in S$ is chosen so $x_i \leq z$ for $i \neq j$. Then $x_j \leq \bigvee_{i=1}^{n} x_i = \bigvee_{i \neq j} x_i \leq z$. Hence $\{x_1, \ldots, x_n\}$ is a corner set. □

We will now show it is possible to glue two corner sets together by deleting an element they have in common.

Lemma 10.1.5. *Let S be a poset. Let $x_1, \ldots, x_t, y_1, \ldots, y_s, a \in S$. Suppose that $\{x_1, \ldots, x_s, a\}$ and $\{y_1, \ldots, y_t, a\}$ are corner sets. Then $\{x_1, \ldots, x_t, y_1, \ldots, y_s\}$ is a corner poset.*

Proof. Let $z \in S$ be an upper bound for all but one element of $\{x_1, \ldots, x_t, y_1, \ldots, y_s\}$. We have 2 cases: either the missing element has the form x_j for some j or it has the form y_j for some j. Without loss of generality we may assume we are in the first case, so $x_i \leq z$ for $i \neq j$ and $y_i \leq z$ for all i. Since $\{y_1, \ldots, y_t, a\}$ is a corner set, we may conclude $a \leq z$. We now know every element of $\{x_1, \ldots, x_s, a\}$ except x_j is bounded by z. Since $\{x_1, \ldots, x_s, a\}$ is a corner set, we also have $x_j \leq z$, so every element of $\{x_1, \ldots, x_t, y_1, \ldots, y_s\}$ is bounded by z, as desired. □

We now introduce regularity conditions on posets that will be used to construct hypergroups. A strongly regular poset is one in which the converse to lemma 10.1.5 holds.

Definition 10.1.6. A poset S is regular if whenever $x, y, z, w, b \in S$ are chosen so that $\{x, y, b\}$ and $\{z, w, b\}$ are corner sets, then there exists $a \in S$ such that $\{x, w, a\}$ and $\{y, z, b\}$ are also corner sets. S is strongly regular if for any $s, t \in \mathbb{N}$, whenever $x_1, \ldots, x_t, y_1, \ldots, y_s$ are chosen to make $\{x_1, \ldots, x_t, y_1, \ldots, y_s\}$ a corner set there exists $a \in S$ such that $\{x_1, \ldots, x_t, a\}$ and $\{y_1, \ldots, y_s, a\}$ a corner set.

Proposition 10.1.7. *A strongly regular poset is regular.*

Proof. Let S be strongly regular. Let $x, y, z, w, b \in S$ be such that $\{x, y, b\}$ and $\{z, w, b\}$ are corner sets. By lemma 10.1.5, $\{x, y, z, w\}$ is a corner set. By strong regularity, there exists a such that $\{x, w, a\}$ and $\{y, z, a\}$ are corner sets. □

One may worry that a poset has too few corner sets for their study to be interesting. The following lemma shows that for a regular poset with a minimal element, this is not the case.

Lemma 10.1.8. *Let S be a regular poset. Suppose either that S has a minimal element 0[1], or that S is strongly regular. Let $x, y \in S$. Then there exists $a \in S$ such that $\{x, y, a\}$ is a corner set.*

Proof. If S has a minimal element, then $\{x, x, 0\}$ and $\{y, y, 0\}$ are corner sets. Hence by regularity, there exists $a \in S$ such that $\{x, y, a\}$ and $\{x, y, a\}$ are corner sets. The strongly regular case is similar, but uses the fact that $\{x, y, x, y\}$ is a corner set. □

We will now recall some definitions from the theory of lattices, which will allow us to produce a large class of regular posets.

Definition 10.1.9. A poset S is a lattice if the least upper bound and greatest lower bound of any two elements exists. A lattice S is distributive if for all $x, y, z \in S$ one has $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$. A lattice S is modular if for all $x, y, z \in S$ with $x \leq z$, one has $x \vee (y \wedge z) = (x \vee y) \wedge z$.

Example 10.1.10. Any totally ordered set is a distributive lattice.

Example 10.1.11. Any idempotent semifield is a distributive lattice under its canonical order. To see this, let S be an idempotent semifield and $x, y, z \in S$. One may check that $x \vee y = x + y$ and $x \wedge y = (x^{-1} + y^{-1})^{-1} = (x + y)^{-1}xy$. Then $x \vee (y \wedge z) = x + (y + z)^{-1}yz = (y + z)^{-1}(xy + xz + yz)$. On the other hand $(x \vee y) \wedge (x \vee z) = (x + y + x + z)^{-1}(x + y)(x + z) = (x + y + z)^{-1}(x^2 + xy + xz + yz)$. Thus we must check that $(y + z)^{-1}(xy + xz + yz) = (x + y + z)^{-1}(x^2 + xy + xz + yz)$, or

[1] Instead of assuming the existence of a minimal element, we actually only need to assume that any two elements have some lower bound.

that $(x + y + z)(xy + xz + yz) = (y + z)(x^2 + xy + xz + yz)$. But both equal $x^2y + xy^2 + xyz + x^2z + xz^2 + y^2z + yz^2$.

Example 10.1.12. Let K be an idempotent semifield, or more generally an idempotent semiring which is a distributive lattice under its canonical order. Then the polynomial semiring $K[x_1, \ldots, x_n]$ is a distributive lattice under its canonical order. In fact least upper bounds and greatest lower bounds may computed coefficient-wise, and the distributivity of $\vee$ and $\wedge$ may be checked coefficient-wise using the corresponding distributive law for K.

Example 10.1.13. Let R be a multiring. Let $\mathcal{I}(R)$ be the set of ideals of R, partially ordered by inclusion. Then for $I, J \in \mathcal{I}(R)$, $I \vee J = I + J$ and $I \wedge J = I \cap J$. Suppose $I, J, N \in \mathcal{I}(R)$ with $I \subseteq N$. Then one trivially has $I + (J \cap N) \subseteq (I + J) \cap N$. For the reverse inclusion, if $x \in (I + J) \cap N$ one may write $x = y + z$ for $y \in I \subseteq N$ and $z \in J$. Then $z \in x - y$, so $z \in N - N = N$. Thus $z \in J \cap N$ and $x = y + z \in I + (J \cap N)$. Hence $\mathcal{I}(R)$ is modular. Similarly, if A is a hypergroup, we may let $\mathcal{S}(A)$ be the set of subhypergroups. Then $\mathcal{S}(A)$ is modular for the same reason.

We recall the following standard result.

Proposition 10.1.14. *Let S be a distributive lattice. Then S is modular.*

Proof. Let $x, y, z \in S$, with $x \leq z$. Then $(x \vee y) \wedge z = (x \vee y) \wedge (x \vee z) = x \vee (y \wedge z)$. □

We now prove a result which provides a large class of strongly regular posets. The choice of a in the proof was suggested to the author by V. Lorman.

Theorem 10.1.15. *Let S be a modular lattice. Then S is strongly regular.*

Proof. Let $x_1, \ldots, x_t \in S$ and $y_1 \ldots, y_s \in S$ be such that $\{x_1, \ldots, x_t, y_1, \ldots, y_s\}$ is a corner set. Let $a = (\bigvee_{i=1}^{t} y_i) \wedge (\bigvee_{i=1}^{s} x_i)$. We wish to show that $\{x_1, \ldots, x_t, a\}$ and $\{y_1, \ldots, y_s, a\}$ are corner sets. Without loss of generality it suffices to do it for $\{x_1, \ldots, x_t, a\}$. Note that if $x_i \leq z$ for all i, then $a \leq \bigvee_{i=1}^{t} x_i \leq z$. Thus we may assume that $a \leq z$ and that there exists j such that $x_i \leq z$ for $i \neq j$, and we must show $x_j \leq z$. It suffices to do this for $z = \bigvee_{i \neq j} x_i \vee a$. But then $z = \bigvee_{i \neq j} x_i \vee ((\bigvee y_i) \wedge (\bigvee x_i)) = (\bigvee_{i \neq j} x_i \vee \bigvee y_i) \wedge (\bigvee x_i)$, since S is modular. It then suffices to show that $x_j \leq \bigvee x_i$, and that $x_j \leq \bigvee y_i \vee \bigvee_{i \neq j} x_i$. The first of these inequalities is trivial because x_j appears as a term on the right. The inequality $x_j \leq \bigvee y_i \vee \bigvee_{i \neq j} x_i$ follows from the fact that $\{x_1, \ldots, x_t, y_1, \ldots, y_s\}$ is a corner set. □

10.2 The hypergroup structure on a regular poset

Definition 10.2.1. Let S be a regular poset with a minimal element denoted 0. Then for $x, y \in S$, we write $x + y = \{a \mid \{a, x, y\}$ is a corner set$\}$.

Remark 10.2.2. If S is totally ordered, and $x \neq y$ then $x + y = \max(x, y)$. If $x = y$, then $x + y = \{a \mid a \leq x\}$. Thus for a totally ordered set this construction agrees with that of Viro.

We wish to show that Definition 10.2.1 makes every regular poset into a canonical abelian hypergroup, and in fact into an idempotent hypergroup.

Remark 10.2.3. It is easy to see that the addition of Definition 10.2.1 is commutative and has identity 0. If $x \in S$ then $0 \in x + x$. On the other hand if $0 \in x + y$ then $\{0, x, y\}$ is a corner set so that $x \leq y$ and $y \leq x$ so $x = y$. Thus each element x has a unique additive inverse, which is equal to x. Furthermore, for all $x, y \in S$, lemma 10.1.8 implies that $x + y$ is nonempty.

Proposition 10.2.4. *Let S be a regular poset with minimal element 0. Then the addition of Definition 10.2.1 is associative.*

Proof. Let $x, y, z \in S$. We will first show that $(x + y) + z \subseteq x + (y + z)$. Let $w \in (x + y) + z$. Then there exists $b \in x + y$ such that $w \in b + z$. Hence $\{x, y, b\}$ and $\{z, w, b\}$ are corner sets. Hence, by regularity, there exists $a \in S$ such that $\{x, w, a\}$ and $\{y, z, a\}$ are corner sets. Then $a \in y + z$, and $w \in x + a$. Hence $(x + y) + z \subseteq x + (y + z)$. By relabelling variables, we get $(z + y) + x \subseteq z + (y + x)$. Using the commutative law we get $x + (y + z) \subseteq (x + y) + z$. Hence associativity holds. □

Proposition 10.2.5. *Let S be a regular poset with a minimal element, equipped with the addition of Definition 10.2.1. Let $x, y, z \in S$ and suppose $x \in y + z$. Then $y \in z - x$.*

Proof. Since $x = -x$, it suffices to show that $y \in z + x$. We are given that $x \in y + z$, or equivalently that $\{x, y, z\}$ is a corner set. But this directly implies that $y \in z+x$. $\square$

We have verified all of the axioms of a canonical abelian hypergroup. Thus we have proved the following.

Theorem 10.2.6. *Let S be a regular poset with minimal element 0. Equip S with the addition of Definition 10.2.1. Then S is a canonical abelian hypegroup.*

In fact such hypergroups are idempotent hypergroups, as defined in 9.2.1.

Theorem 10.2.7. *Let S be as in Theorem 10.2.6. Then S is an idempotent hypergroup.*

Proof. One has $x - x = x + x = \{a \mid \{a, x, x\} \text{ is a corner set}\} = \{a \mid a \leq x\}$. Clearly $x \in x + x$. If $a, b \in x - x$ and $c \in a + b$, then $\{a, b, c\}$ is a corner set and $a, b \leq x$. But this implies $c \leq x$, so $c \in x - x$. Hence $(x - x) + (x - x) \subseteq x - x$. The reverse inclusion follows from $0 \in x-x$, so $x+x-x-x = x-x$. Hence S is idempotent. $\square$

On an idempotent hypergroup we defined a valuation induced by the relation $x \leq y$ if $y \in x + y$. In this case the relation is the partial ordering we started with.

Proposition 10.2.8. *Let S be as in Theorem 10.2.6. Let $x, y \in S$. Then $x \leq y$ if and only if $y \in x + y$.*

Proof. It suffices to show that $x \leq y$ if and only if $\{x, y, y\}$ is a corner set. If $\{x, y, y\}$ is a corner set then $x \leq y$ follows from $y \leq y$. On the other hand, suppose $x \leq y$. If $x \leq z$ and $y \leq z$ then $y \leq z$. If $y \leq z$ then $x \leq y \leq z$ so $\{x, y, y\}$ is a corner set. $\square$

Corollary 10.2.9. *Let S be as in Theorem 10.2.6 and let v be as in Definition 9.2.7. Then v is bijective and $v(x) \leq v(y)$ if and only if $x \leq y$.*

The hypergroup structure on a regular poset with minimal element satisfies the following universal property. By a hypergroup homomorphism we mean a map satisfying $v(0) = 0$ and $v(x + y) \subseteq v(x) + v(y)$.

Theorem 10.2.10. *Let S be as in Theorem 10.2.6. Let A be a canonical abelian hypergroup. Suppose $v : A \to S$ is such that for any $x, y \in A$ and any $t \in S$ with $v(x) \leq t$ and $v(y) \leq t$, one has $v(x + y) \leq t$*[2]*. Suppose furthermore that for all $x \in A$ one has $v(x) = v(-x)$ and that $v(0) = 0$. Then v is a homomorphism of hypergroups. Conversely any hypergroup homomorphism $v : A \to S$ has the properties described.*

Proof. Let v satisfy the hypotheses described in the statement of the theorem. Let $x, y \in A$. We must show that $v(x+y) \subseteq v(x)+v(y)$. Thus for any $z \in x+y$, we must show that $v(z) \subseteq v(x)+v(y)$, or that $\{v(z), v(x), v(y)\}$ is a corner set. If $v(x) \leq t$ and $v(y) \leq t$ then $v(z) \in v(x+y) \leq t$. If $v(x) \leq t$ and $v(z) \leq t$, then $v(y) \in v(z-x) \leq t$, since $y \in z - x$ and since $v(-x) = v(x) \leq t$. Similarly if $v(y) \leq t$ and $v(z) \leq t$, then $v(x) \leq t$. Hence $\{v(x), v(y), v(z)\}$ is a corner set so $v(x + y) \subseteq v(x) + v(y)$. We have $v(0) = 0$ by assumption, so v is a homomorphism.

For the converse, suppose $v : A \to S$ is a homomorphism. Then $v(0) = 0$. Since $0 = v(0) \in v(x - x) \subseteq v(x) + v(-x)$, we see that $v(-x) = -v(x) = v(x)$ for all $x \in A$. Suppose $x, y \in A$ and $t \in S$ with $v(x) \leq t$ and $v(y) \leq t$. Let $z \in x + y$. Then

[2] By $v(x + y) \leq t$ we mean that $v(z) \leq t$ for all $z \in x + y$.

$v(z) \in v(x+y) \subseteq v(x)+v(y)$, so $\{v(x), v(y), v(z)\}$ is a corner set. Hence $v(z) \leq t$. Thus $v(x+y) \leq t$, so all of the desired properties have been verified. □

In a strongly regular poset, the sum of more than two elements has a particularly nice form.

Proposition 10.2.11. *Let S be a strongly regular poset with minimal element 0. Let $x_1, \ldots, x_n \in S$. Then $x_1 + \ldots + x_n = \{a \mid \{x_1, \ldots, x_n, a\}$ is a corner set$\}$.*

Proof. We proceed by induction on n. The case $n = 2$ is Definition 10.2.1. Suppose the result holds for $n-1$. Suppose that $\{x_1, \ldots, x_n, a\}$ is a corner set. Then by strong regularity, there exists $b \in S$ such that $\{b, x_n, a\}$ and $\{x_1, \ldots, x_{n-1}\}$ are corner sets. Then $b \in x_1 + \ldots + x_{n-1}$ by the inductive hypothesis, and $a \in b + x_n$. Hence $a \in x_1 + \ldots + x_n$. Conversely, suppose that $a \in x_1 + \ldots + x_n$. We will show that $\{x_1, \ldots, x_n, a\}$ is a corner set. There exists $b \in x_1 + \ldots + x_{n-1}$ such that $a \in b + x_n$. Then $\{b, x_1, \ldots, x_{n-1}\}$ and $\{b, a, x_n\}$ are corner sets. The result follows from lemma 10.1.5. □

Using the above method to construct hypergroups from regular idempotent semigroups is functorial, as the following proposition shows.

Proposition 10.2.12. *Let S, S' be regular idempotent semigroups, which we endow with the hypergroup structure of Theorem 10.2.6. Let $f : S \to S'$ be a semiring homomorphism. Then f is a hypergroup homomorphism.*

Proof. Clearly $f(0) = 0$. Let $x, y, z \in S$ be chosen so $z \in x + y$, or equivalently $\{x, y, z\}$ is a corner set. We must show that $f(z) \in f(x) + f(y)$, or equivalently that $\{f(x), f(y), f(z)\}$ is a corner set. Since $\{x, y, z\}$ is a corner set, by lemma 10.1.4, $x \vee y = x \vee z = y \vee z$. Hence $f(x) \vee f(y) = f(x) \vee f(z) = f(y) \vee f(z)$, which gives the desired result by lemma 10.1.4. □

10.3 Regular idempotent semirings

In this section the addition in an idempotent semiring will be denoted $x \vee y$ to indicate that the sum is the least upper bound, as well as to avoid confusion with the addition in the hypergroup of Definition 10.2.1.

Lemma 10.3.1. *Let S be a regular idempotent semiring. Let $x_1, \ldots, x_n, y \in S$. Suppose $\{x_1, \ldots, x_n\}$ is a corner set. Then $\{x_1 y, \ldots, x_n y\}$ is a corner set.*

Proof. We use the criterion of lemma 10.1.4 to see that $\bigvee_{i=1}^{n} x_i = \bigvee_{i \neq j} x_i$. Multiplying by y gives $\bigvee_{i=1}^{n} x_i y = \bigvee_{i \neq j} x_i y$ as desired. □

We now prove a distributive law for regular idempotent semirings.

Proposition 10.3.2. *Let S be a regular idempotent semiring. Use $+$ to denote the operation of Definition 10.2.1, and write the semiring multiplication as ordinary multiplication. Then $(x + y)z \subseteq xz + yz$.*

Proof. Any element of $(x+y)z$ has the form az for $a \in x+y$. Then $\{a, x, y\}$ is a corner set. Hence $\{az, xz, yz\}$ is a corner set. Then $az \in xz+yz$, so $(x+y)z \subseteq xz+yz$. $\square$

Theorem 10.3.3. *Let S be a regular idempotent semiring. Then S is a multiring under the addition of Definition 10.2.1 and the multiplication coming from its semiring structure.*

Proof. We have proven it is a canonical abelian hypergroup in Theorem 10.2.6. We have shown the distributive law in Proposition 10.3.2. The associativity of multiplication and the existence of the multiplicative identity follow from the semiring axioms. $\square$

We now show the ideals of the multiring structure on S may be expressed in terms of the semiring structure on S.

Theorem 10.3.4. *Let S be a regular idempotent semiring. Let $I \subseteq S$. Then I is an strong ideal of the semiring S if and only if it is an ideal of S regarded as a multiring via Theorem 10.3.3.*

Proof. We use Theorem 9.2.18. Note that by Corollary 10.2.9, the map $v : S \to S/\sim = S$ is the identity map from the multiring S to the semiring S. Since both have the same multiplication, $v(xy) = v(x)v(y)$ for all $x, y \in S$. If $x, y \in S$, then $x \vee y \in x + y$, so there exists $z \in x + y$ with $v(z) = \sup(v(x), v(y))$. All of the hypotheses of Theorem 9.2.18 hold, so the result follows from that theorem. $\square$

We define the notion of a valuation from a multiring to an idempotent semiring.

Definition 10.3.5. Let R be a multiring, and let S be an idempotent semiring. A map $v : R \to S$ is a valuation if it satisfies the following properties.

(i) $v(0) = 0$.

(ii) $v(1) = 1$.

(iii) $v(x) = v(-x)$ for all $x \in R$.

(iv) $v(xy) = v(x)v(y)$ for all $x, y \in R$.

(v) For all $x, y \in R$ and all $z \in x + y$, $v(z) \leq v(x) \vee v(y)$.

We now prove a universal property for the multiring associated to a regular idempotent semiring.

Theorem 10.3.6. *Let S be a regular idempotent semiring. Let R be a multiring. A map $v : R \to S$ is a valuation if and only if it is a homomorphism of multirings, where S is equipped with the multiring structure of Theorem 10.3.3.*

Proof. By Theorem 10.2.10, v satisfies properties (i), (iii) and (v) of Definition 10.3.5 if and only if it is a hypergroup homomorphism. Since a multiring homomorphism is the same as a hypergroup homomorphism that satisfies (ii) and (iv) of Definition 10.3.5, it is the same as a map that satisfies (i)-(v) of that definition. Thus v is a multiring homomorphism if and only if it is a valuation. □

10.4 The semigroup of finitely generated subhypergroups

In this section, we return to writing the addition in an idempotent semigroup using the symbol $+$. The goal for this section is to construct a left adjoint to the construction detailed in the previous sections of this chapter. Elements of the idempotent semigroup we construct will be finitely generated subhypergroups of a given hypergroup.

Definition 10.4.1. Let A be a hypergroup and $B \subseteq A$. B is a subhypergroup if the following hold:

(a) $0 \in B$.

(b) $-x \in B$ for all $x \in B$.

(c) $x + y \subseteq B$ holds for all $x, y \in B$.

Definition 10.4.2. Let A be a hypergroup and $S \subseteq A$. The subhypergroup generated by A is the intersection of all subhypergroups containing A. We write $\langle x \rangle$ for the subhypergroup generated by x.

Lemma 10.4.3. *Let A be a hypergroup. Let $B, C \subseteq A$ be subhypergroups. Then $B + C$ is the intersection of all subhypergroups of A which contain both B and C. Hence if the subhypergroups are partially ordered by inclusion, then $B + C$ is the least upper bound of B and C.*

Proof. $B + C$ contains B and C. Any subhypergroup containing both B and C contains $B + C$ because the subhypergroup is closed under addition. □

Proposition 10.4.4. *Let A be a hypergroup. Let $x_1, \ldots, x_n \in A$. Then the subhypergroup generated by $\{x_1, \ldots, x_n\}$ is $\langle x_1 \rangle + \ldots + \langle x_n \rangle$.*

Proof. This is clearly true for $n = 1$ so we suppose it holds for $n - 1$. Let B be the subhypergroup generated by $\{x_1, \ldots, x_n\}$. Since $x_n \in B$, $\langle x_n \rangle \subseteq B$. Since $\{x_1, \ldots, x_{n-1}\} \subseteq B$, the inductive hypothesis implies $\langle x_1 \rangle + \ldots + \langle x_{n-1} \rangle \subseteq B$. Hence by lemma 10.4.3,$\langle x_1 \rangle + \ldots + \langle x_n \rangle \subseteq B$. Conversely, to show $B \subseteq < x_1 > + \ldots + < x_n >$, it suffices to show that $\{x_1, \ldots, x_n\} \subseteq \langle x_1 \rangle + \ldots + \langle x_n \rangle$, which is trivial. □

Definition 10.4.5. For a hypergroup A, we let $\mathcal{S}_f(A)$ be the set of finitely generated subhypergroups of A, which we view as a poset partially ordered by inclusion.

Remark 10.4.6. $\mathcal{S}_f(A)$ has a minimal element 0. If $B, C \in \mathcal{S}_f(A)$, then it follows from Proposition 10.4.4 that $B + C \in \mathcal{S}_f(A)$. Furthermore, this fact together with lemma 10.4.3 imply that B and C have a least upper bound given by $B + C$. Hence $\mathcal{S}_f(A)$ is an idempotent semigroup equipped with its canonical order

We wish to show that the poset $\mathcal{S}_f(A)$ is regular. The poset $\mathcal{S}(A)$ of all subhypergroups is regular by Example 10.1.13 and Theorem 10.1.15. We will deduce the case of $\mathcal{S}_f(A)$ from this fact.

Theorem 10.4.7. *Let A be a hypergroup. Then $\mathcal{S}_f(A)$ is regular.*

Proof. Let X, Y, Z, W, B be finitely generated subhypergroups of A. Suppose that $\{X, Y, B\}$ and $\{Z, W, B\}$ are corner sets in $\mathcal{S}_f(A)$. We wish to construct $N \in \mathcal{S}_f(A)$ such that $\{X, W, N\}$ and $\{Y, Z, N\}$ are corner sets in $\mathcal{S}_f(A)$. Note that $\{X, Y, B\}$ and $\{Z, W, B\}$ are corner sets in $\mathcal{S}(A)$, as can be seen using lemma 10.1.4. Hence we get $N' \in \mathcal{S}(A)$ such that $\{X, W, N'\}$ and $\{Y, Z, N'\}$ are corner sets in $\mathcal{S}(A)$. That $\{X, W, N'\}$ is a corner set means $X + W = X + N' = W + N'$. Similarly $Y + Z = Y + N' = Z + N'$.

Let $a_1, \ldots, a_t$ be generators for the finitely generated subhypergroup $X + W = X + N'$ of A. For each i, write $a_i = u_i + v_i$ with $u_i \in X$ and $v_i \in N'$. Let N_1 be the subhypergroup generated by $v_1, \ldots, v_t$. Then $a_i = u_i + v_i \in X + N_1$ for all i, so $X + W \subseteq X + N_1$. We similarly construct finitely generated subhypergroups $N_2, N_3, N_4 \subseteq N'$ such that $Y + Z \subseteq Y + N_2$, $Y + Z \subseteq Z + N_3$ and $X + W \subseteq W + N_4$. Let $N = N_1 + N_2 + N_3 + N_4 \subseteq N'$, which is clearly finitely generated. Because $N_1, N_2, N_3, N_4 \subseteq N$, $X + W \subseteq X + N$, $Y + Z \subseteq Y + N$, $Y + Z \subseteq Z + N$ and $X + W \subseteq W + N$. On the other hand, since $N \subseteq N'$, $X + N \subseteq X + N' = X + W$, $Y + N \subseteq Y + Z$, $Z + N \subseteq Y + Z$, and $W + N \subseteq X + W$. Hence $X + W = X + N = W + N$ and $Y + Z = Y + N = Z + N$, so $\{X, W, N\}$ and $\{Y, Z, N\}$ are corner sets in $\mathcal{S}_f(A)$, as desired. □

Definition 10.4.8. Let A be a hypergroup. Let S be an idempotent semigroup. An nonmultiplicative valuation from A to S is a map such that for all $x, y \in A$, $v(x+y) \leq v(x) + v(y)$, $v(x) = v(-x)$ and $v(0) = 0$. We denote the set of nonmultiplicative valuations from A to S by $\mathrm{Val}(A, S)$.

We will relate nonmultiplicative valuations to the semigroup $\mathcal{S}_f(A)$.

Lemma 10.4.9. *Let A be a hypergroup and $x \in A$. Let $v : A \to S$ be an non-multiplicative valuation from A to an idempotent semigroup S. Let $t \in \langle x \rangle$. Then $v(t) \leq v(x)$.*

Proof. First I claim that for any $s \in S$, the set $\{y \in A \mid v(y) \leq s\}$ is a subhypergroup. In fact it is closed under negation because $v(y) = v(-y)$, and contains 0, and it is closed under addition by the ultrametric inequality. For any $x \in A$, we have $x \in \{y \in A \mid v(y) \leq v(x)\}$, so $\langle x \rangle \subseteq \{y \in A \mid v(y) \leq v(x)\}$. □

Lemma 10.4.10. *Let A be a hypergroup. Let $B \subseteq A$ be the subhypergroup generated by a finite set $\{x_1, \ldots, x_n\}$. Let S be an idempotent semigroup and $v : A \to S$ be an nonmultiplicative valuation. Then $v(x_1) + \ldots + v(x_n)$ is the least upper bound of $\{v(b) \mid b \in B\}$.*

Proof. We have $B = \langle x_1 \rangle + \ldots + \langle x_n \rangle$. Let $b \in B$. Then there are elements $b_i \in \langle x_i \rangle$ such that $b = b_1 + \ldots + b_n$. By lemma 10.4.9, $v(b_i) \leq v(x_i)$ for all i. Hence $v(b) \leq v(b_1) + \ldots + v(b_n) \leq v(x_1) + \ldots + v(x_n)$. Hence $v(x_1) + \ldots + v(x_n)$ is an upper bound for $\{v(b) \mid b \in B\}$. Suppose η is another upper bound. Then $v(x_i) \subseteq \{v(b) \mid b \in B\}$, so $v(x_i) \leq \eta$ for all i. Hence $v(x_1) + \ldots + v(x_n) \leq \eta$, so $v(x_1) + \ldots + v(x_n)$ is the least upper bound. □

We now prove a universal property for $\mathcal{S}_f(A)$, which states that the map $A \to \mathcal{S}_f(A)$ sending x to $\langle x \rangle$ is the universal nonmultiplicative valuation on A. An analogue for rings is proven in[23]

Theorem 10.4.11. *Let A be a hypergroup. The map $w : A \to \mathcal{S}_f(A)$ given by $w(x) = \langle x \rangle$ is an nonmultiplicative valuation. Let S be an idempotent semigroup, and let $v : A \to S$ be an nonmultiplicative valuation. Then there is a unique semigroup homomorphism $\phi : \mathcal{S}_f(A) \to S$ such that $\phi \circ w = v$.*

Proof. Let $x, y \in A$. Then $x, y \in \langle x \rangle + \langle y \rangle$, so $x + y \in \langle x \rangle + \langle y \rangle$. Hence $w(x + y) \leq w(x) + w(y)$. Also $w(x) = \langle x \rangle = \langle -x \rangle = w(-x)$, since subhypergroups are closed under negation. Furthermore, $w(0) = \langle 0 \rangle = 0$. Hence w is an nonmultiplicative valuation.

For $B \in \mathcal{S}_f(A)$, let $\phi(B)$ be the least upper bound of $\{v(b) \mid b \in B\}$, which exists by lemma 10.4.10. Let $B' \in \mathcal{S}_f(A)$ be another element. Let $x_1, \ldots, x_n$ be generators for B, and let $y_1, \ldots, y_m$ be generators for B'. Then $x_1, \ldots, x_n, y_1, \ldots, y_m$ generates $B + B'$. Hence by lemma 10.4.10, $\phi(B) = v(x_1) + \ldots + v(x_n)$, $\phi(B') = v(y_1) + \ldots + v(y_m)$, and $\phi(B + B') = v(x_1) + \ldots + v(x_n) + v(y_1) + \ldots + v(y_m)$. Hence $\phi(B + B') = \phi(B) + \phi(B')$. Since we also have $\phi(0) = v(0) = 0$, ϕ is a semigroup homomorphism. Also, by lemma 10.4.10, $\phi(w(x)) = \phi(\langle x \rangle) = v(x)$.

Let $\psi : \mathcal{S}_f(A) \to S$ be another semigroup homomorphism such that $\psi \circ w = v$. Let $B \in \mathcal{S}_f(A)$. Let $x_1, \ldots, x_n$ be generators for B. Then $\psi(B) = \psi(\langle x_1 \rangle + \ldots + \langle x_n \rangle) = \psi(\langle x_1 \rangle) + \ldots + \psi(\langle x_n \rangle) = \psi(w(x_1)) + \ldots + \psi(w(x_n)) = v(x_1) + \ldots + v(x_n)$. By lemma

10.4.10, we now have $\psi(B) = \phi(B)$, so ϕ is unique. □

Definition 10.4.12. For a regular idempotent semigroup S, we let $Y(S)$ be the hypergroup $Y(S) = S$ constructed in Theorem 10.2.6. For a morphism ϕ of regular idempotent semigroups, we let $Y(\phi) = \phi$.

By lemma 10.2.12, Y is a functor from the category of regular idempotent semigroups[3] to the category of hypergroups. We have seen in Theorem 10.4.7 that $\mathcal{S}_f$ sends hypergroups to regular idempotent semigroups. We would like to say that $\mathcal{S}_f$ is left adjoint to Y. However, we have not described $\mathcal{S}_f$ on morphisms, so $\mathcal{S}_f$ is not yet a functor. Nonetheless, we can still accomplish our goal.

Theorem 10.4.13. *There is a way to associate to each hypergroup homomorphism $\eta : A \to B$ a semigroup homomorphism $\mathcal{S}_f(\eta)$ so that $\mathcal{S}_f$ is a functor and is left adjoint to the functor Y.*

Proof. Given a hypergroup A and a morphism $\phi : S \to S'$ of regular idempotent semigroups, we define $\mathrm{Val}(A, \phi) : \mathrm{Val}(A, S) \to \mathrm{Val}(A, S')$ to send $f \in \mathrm{Val}(A, S)$ to $\phi \circ f$. Given a regular idempotent semigroup S and a morphism $\eta : A \to B$ of hypergroups, define $\mathrm{Val}(\eta, S) : \mathrm{Val}(B, S) \to \mathrm{Val}(A, S)$ to send f to $f \circ \eta$. Then one readily sees that $\mathrm{Val}(A, S)$ is a covariant functor in S and a contravariant functor in A. By Theorem 10.2.10, we have an isomorphism $\alpha : \mathrm{Val}(A, S) \to \mathrm{Hom}(A, Y(S))$ sending a map $f : A \to S$ to f. One easily sees that this is natural in A and in S.

[3]Morphisms in this category are simply semigroup homomorphisms.

By Theorem 10.4.11, we have an isomorphism $\beta : \mathrm{Hom}(\mathcal{S}_f(A), S) \to \mathrm{Val}(A, S)$. If w is as in Theorem 10.4.11 then $\beta(u) = u \circ w$. To check naturality in S, let $\phi : S \to S'$ be a morphism of regular idempotent semigroups. Let $u \in \mathrm{Hom}(\mathcal{S}_f(A), S)$. Then $(\beta_{S'} \circ \mathrm{Hom}(\mathcal{S}_f(A), \phi))(u) = \beta_{S'}(\phi \circ u) = \phi \circ u \circ w$. Also $(\mathrm{Val}(A, \phi) \circ \beta_S)(u) = \mathrm{Val}(A, \phi)(u \circ w) = \phi \circ u \circ w$. Thus the naturality square commutes and β is natural in S. By the Yoneda lemma, there is a unique way of defining $\mathcal{S}_f$ on morphisms such that β is natural in A, and furthermore this makes $\mathcal{S}_f$ a functor. Since α and β are natural in A and S, so is their composite. Thus $\mathrm{Hom}(\mathcal{S}_f(A), S) \cong \mathrm{Hom}(A, Y(S))$ naturally in A and S, as desired. □

We would also like to show that $\mathcal{S}_f$ provides a one-sided inverse to Y. We will use the following theorem.

Theorem 10.4.14. *The functor Y is fully faithful.*

Proof. Let S and S' be regular idempotent semigroups. Let $f : Y(S) \to Y(S')$ be a hypergroup homomorphism. Then we may view f as a function from S to S', and we wish to show this function is a semigroup homomorphism. If $\{a, b, c\}$ is a corner set in S then $c \in a + b$ in $Y(S)$ so $f(c) \in f(a) + f(b)$ holds in $Y(S')$, which implies that $\{f(a), f(b), f(c)\}$ is a corner set in S'. Thus f maps corner sets with three elements to corner sets. Let $x, y \in S$ with $y \leq x$. Then $\{x, x, y\}$ is a corner set in S, so $\{f(x), f(x), f(y)\}$ is a corner set. Hence $f(y) \leq f(x)$ so f is monotonic. Write $\vee$ for the addition in S or in S'. Then for any $x, y \in S$, $\{x, y, x \vee y\}$ is a corner set. Hence $\{f(x), f(y), f(x \vee y)\}$ is a corner set in S'. Since $f(x) \leq f(x) \vee f(y)$, and $f(y) \leq f(x) \vee f(y)$, it follows that $f(x \vee y) \leq f(x) \vee f(y)$. Conversely $f(x) \leq f(x \vee y)$ and $f(y) \leq f(x \vee y)$ since f is monotonic. Hence $f(x) \vee f(y) \leq f(x \vee y)$ so $f(x) \vee f(y) = f(x \vee y)$. Hence f is a semigroup homomorphism, so that Y is full. The fact that Y is faithful holds because f and $Y(f)$ are the same function on the level of sets. □

Theorem 10.4.15. *The counit of the adjunction between $\mathcal{S}_f$ and Y provides a natural isomorphism between $\mathcal{S}_f \circ Y$ and the identity functor. The category of regular idempotent semigroups is equivalent to a reflective subcategory*[4] *of the category of hypergroups.*

Proof. This follows via category theory from theorems 10.4.14 and 10.4.13. The first statement is a consequence of the Yoneda lemma, while the second follows from the definition of a reflective subcategory. □

10.5 The functor $\mathcal{S}_f$ on multirings

In this section we prove analogues of the results of section 10.4 for multirings. The key difficulty lies in showing that $\mathcal{S}_f$ is a semiring. First we define the multiplication operation.

[4]A reflective subcategory is a full subcategory such that the inclusion functor has a left adjoint. This adjoint is called the reflector. For example the category of complete metric spaces is a reflective subcategory of the category of metric spaces with the reflector being the completion functor.

Definition 10.5.1. Let R be a multiring. Let $A, B \subseteq R$. Then we write AB for the intersection of all subhypergroups of R which contain the set $\{ab \mid a \in A, b \in B\}$.

The following lemma describes this multiplication operation on subhypergroups with one generator.

Lemma 10.5.2. *Let R be a multiring and $x, y \in R$. Let $A = \langle x \rangle$ and $\langle y \rangle$. Then $AB = \langle xy \rangle$*

Proof. Let $C = \{t \mid ty \in \langle xy \rangle\}$. If $s, t \in C$ and $c \in s + t$ then $cy \in (s+t)y \subseteq sy + ty$. Since $sy, ty \in \langle xy \rangle$, $cy \in \langle xy \rangle$ so $c \in C$. Hence C is closed under addition. It is easily seen to be closed under negation, so it is a subhypergroup. Clearly $x \in C$ so $A = \langle x \rangle \subseteq C$. Thus for any $a \in A$ we have $ay \in \langle xy \rangle$. For each $a \in A$, let $D_a = \{t \mid at \in \langle xy \rangle\}$. One sees, as in the case of C that D is a subhypergroup. We have seen that $y \in D_a$ for all $a \in A$. Hence $B = \langle y \rangle \subseteq D_a$ for all $a \in A$. Thus for all $a \in A$ and all $b \in B$, $b \in D_a$ so $ab \in \langle xy \rangle$. Thus $\langle x \rangle \langle y \rangle \subseteq \langle xy \rangle$. For the converse, note that $x \in \langle x \rangle$ and $y \in \langle y \rangle$ so $xy \in \langle x \rangle \langle y \rangle$. Hence $\langle xy \rangle \subseteq \langle x \rangle \langle xy \rangle$. □

We now prove this multiplication on subhypergroups distributes over addition.

Lemma 10.5.3. *Let R be a multiring. Let $A, B, C \subseteq R$ be subhypergroups. Then $A(B + C) = AB + AC$.*

Proof. Because $B \subseteq B + C$ we have $AB \subseteq A(B + C)$ and similarly $AC \subseteq A(B + C)$. Hence $AB + AC \subseteq A(B + C)$. For the reverse inclusion let $a \in A$ and $y \in B + C$.

It suffices to show $ay \subseteq AB + AC$. Let $y \in b + c$ where $b \in B$ and $c \in C$. Then $ay \in a(b + c) \subseteq ab + ac \subseteq AB + AC$. ☐

We now prove this multiplication is associative.

Lemma 10.5.4. *Let R be a multiring. Let $A, B, C \subseteq R$ be subhypergroups. Then $(AB)C = A(BC)$.*

Proof. Let ABC be the smallest subhypergroup containing $\{abc \mid a \in A, b \in B, c \in C\}$. Then $ABC \subseteq (AB)C$. For an element $c \in C$, let $D_c = \{t \in R \mid tc \in ABC\}$. Then as in the proof of lemma 10.5.2, D_c is a subhypergroup. Furthermore for $a \in A$, $b \in B$ and $c \in C$, one has $ab \in D_c$. Hence for $c \in C$, one has $AB \subseteq D_c$. Thus for $x \in AB$ and $y \in C$ one has $xy \in ABC$ so that $(AB)C = ABC$. Similarly one can show $A(BC) = ABC$. ☐

We now show multiplication of subhypergroups preserves the property of being finitely generated.

Lemma 10.5.5. *Let R be a multiring. Let $A, B \subseteq R$ be finitely generated subhypergroups. Then AB is a finitely generated subhypergroup.*

Proof. Using Proposition 10.4.4 we may write $A = \langle x_1 \rangle + \ldots + \langle x_m \rangle$ and $B = \langle y_1 \rangle + \ldots + \langle y_n \rangle$ for some $x_1 \ldots, x_m, y_1, \ldots, y_n \in R$. By lemmas 10.5.3 and 10.5.2 we may write $AB = (\langle x_1 \rangle + \ldots + \langle x_m \rangle)(\langle y_1 \rangle + \ldots + \langle y_n \rangle) = \langle x_1 y_1 \rangle + \ldots + \langle x_m y_1 \rangle + \ldots + \langle x_1 y_n \rangle + \ldots + \langle x_m y_n \rangle$. ☐

Theorem 10.5.6. *Let R be a multiring. Then $\mathcal{S}_f(R)$ is a regular idempotent semiring.*

Proof. It is a regular idempotent semiring by Theorem 10.4.7. It is closed under multiplication by lemma 10.5.5. It satisfies the distributive law by lemma 10.5.3, and the associative law by lemma 10.5.4. □

Definition 10.5.7. Let R be a multiring. Let S be an idempotent semiring. A multiplicative valuation $v : R \to S$ is a nonmultiplicative valuation such that $v(xy) = v(x)v(y)$ for all $x, y \in R$. The set of multiplicative valuations is denoted $\mathrm{Val}_m(R, S)$.

We now turn to the problem of showing that the map $R \to \mathcal{S}_f(R)$ is universal among multiplicative valuations. In the case of rings, this was observed by Macpherson.[23]

Theorem 10.5.8. *Let R be a multiring. The map $w : R \to \mathcal{S}_f(R)$ given by $w(x) = \langle x \rangle$ is an nonmultiplicative valuation. Let S be an idempotent semiring, and let $v : A \to S$ be an multiplicative valuation. Then there is a unique semiring homomorphism $\phi : \mathcal{S}_f(R) \to S$ such that $\phi \circ w = v$.*

Proof. By Theorem 10.4.11, w is a nonmultiplicative valuation. It is multiplicative by lemma 10.5.2. By Theorem 10.4.11 there is a semigroup homomorphism $\phi : \mathcal{S}_f(R) \to S$ such that $\phi \circ w = v$. Let $A, B \in \mathcal{S}_f(R)$. Let A be generated by $x_1, \ldots, x_m$ and B be generated by $y_1, \ldots, y_n$, so that by the proof of lemma 10.5.5, AB must be generated by $\{x_i y_j \mid 1 \le i \le m, 1 \le j \le n\}$. Then by the description of ϕ given in the proof of Theorem 10.4.11, $\phi(A)\phi(B) = (v(x_1)+\ldots+v(x_m))(v(y_1)+\ldots+v(y_n)) = v(x_1)v(y_1)+\ldots+v(x_m)v(y_n) = v(x_1y_1)+\ldots v(x_my_n) = \phi(AB)$. Hence ϕ is a semiring homomorphism. □

We now turn our attention to the functor Y.

Theorem 10.5.9. *The functor Y restricts to a fully faithful from the category of regular idempotent semirings to the category of multirings.*

Proof. If R is a regular idempotent semiring, then Theorem 10.3.3 implies $Y(R)$ is a multiring. On the level of sets we take $Y(f) = f$. To show Y is a fully faithful functor we must show that f is a multiring homomorphism if and only if it is a semiring homomorphism. We know by Proposition 10.2.12 and Theorem 10.4.14 that f is a hypergroup homomorphism if and only if it is a semigroup homomorphism. Thus f is a hypergroup homomorphism which preserves multiplication if and only if it is a semigroup homomorphism which preserves multiplication. The result follows. □

Theorem 10.5.10. *Let Y be the functor from regular idempotent semirings to multirings described above. $\mathcal{S}_f$ may defined on morphisms in such a way that $\mathcal{S}_f$ is left adjoint to Y.*

Proof. The proof is essentially identical to that of Theorem 10.4.13. Instead of using theorems 10.4.11 and 10.2.10, we use theorems 10.5.8 and 10.3.6. □

Theorem 10.5.11. *The counit of the adjunction between $\mathcal{S}_f$ and Y provides a natural isomorphism between $\mathcal{S}_f \circ Y$ and the identity functor. The category of regular* *idempotent semirings is equivalent to a reflective subcategory of the category of multirings.*

Proof. This is proven in the same way as Theorem 10.4.15. □

Bibliography

[1] Jean-Pierre Serre, *Local Fields*. Springer-Verlag, 2nd edition, 1995.

[2] J.-P. Wintenberger, *Le corps des normes de certaines extensions infinies des corps locaux; applications*, Annales scientifiques de l'école Normale Supérieure, Sér. 4, 16 no. 1 (1983), p. 59-89.

[3] William Fulton, *Intersection Theory*. Springer-Verlag, 2nd edition, 1998.

[4] I.B. Fesenko and S.V. Vostokov, *Local Fields and Their Extensions.* American Mathematical Society, 2nd edition, 2002.

[5] Marc Krasner, *Approximation des corps valués complets de caractéristique* $p \neq 0$ *par ceux caractéristique 0*, 1957 Colloque d'algébre supérieure, tenu á Bruxelles du 19 au 22 décembre.

[6] P. Deligne, *Les corps locaux de caractéristique p, limits de corps locaux de caractéristique 0*, J.-N. Bernstein, P. Deligne, D. Kazhdan, M.-F. Vigneras, Repre-

sentations des groupes reductifs sur un corps local, Travaux en cours, Hermann, Paris, 119-157, 1984).

[7] Manabu Yoshida, *An introduction to the theory of Deligne on truncated discrete valuation rings*. http://www2.math.kyushu-u.ac.jp/~m-yoshida/pdf/an_introduction_to_the.pdf.

[8] J.S. Milne, *Étale Cohomology*. Princeton University Press, 1st edition, 1980.

[9] Oliver Brinon and Brian Conrad, *CMI summer school notes on p-adic Hodge theory*. http://math.stanford.edu/~conrad/papers/notes.pdf.

[10] Marc Krasner, *A class of hyperrings and hyperfields*, Internat. J. Math. Math. Sci. 6 (1983), no. 2, 307311.

[11] A. Connes, C. Consani, *From monoids to hyperstructures: in search of an absolute arithmetic*, in Casimir Force, Casimir Operators and the Riemann Hypothesis, de Gruyter (2010), pg 147-198.

[12] A. Connes, C. Consani, *The universal thickening of the field of real numbers*, arXiv:0420079v1 [mathNT] (2012).

[13] A. Connes, C. Consani, *Projective geometry in characteristic one and the epicyclic category*, arXiv:1309.0406 [Math.AG] (2013), to appear in Nagoya Math. J.

[14] S. Henry, *Symmetrization of monoids as hypergroups*, arXiv:1309.1963 [math.AG] (2013)

[15] Z. Izhakian, L. Rowen, *Supertropical Algebra*, Adv. in Math., 225(4): 2222-2286, 2010. Librairie Gauthier-Villars, Paris.

[16] F. Marty, *Sur une généralization de la notion de group*, Eight Congress Math. Scandenaves, Stockholm, (1934), 4549.

[17] O. Viro, *Hyperfields for tropical geometry I, hyperfields and dequantization*, available as arXiv:1006.3034v2.

[18] A. Gathmann, *Tropical algebraic geometry*, Jahresber. Deutsch. Math.-Verein **108** 1 (2006), 3-32.

[19] S. A. Steinberg, *Lattice-ordered Rings and Modules*, Springer-Verlag, New York (2010)

[20] J. Tits, *Sur les analogues algébriques des groupes semi-simples complexes.* Colloque dálgébre supérieure, Bruxelles 1922 decembre 1956, Centre Belge de Recherches Mathématiques Etablissements Ceuterick, Louvain; Librairie Gauthier-Villars, Paris (1957), pg 261289.

[21] J. Jun, PhD Thesis, Johns Hopkins University, 2015

[22] M. Ştefănescu, *Constructions of hyperfields and hyperrings*, Studii i Cercetări

Stiintifice, Seria: Matematică, Universitatea din Bacău, no. 16, supplement, pg 563-571, 2006.

[23] A. Macpherson *Skeleta in non-Archimedean and tropical geometry*, available as arXiv:1311.0502 [math.AG]

[24] M. Marshall, *Real reduced multirings and multifields*, Journal of Pure and Applied Algebra, Volume 205, Issue 2, pg 452-468, 2006.

[25] N.Giansiracusa, J. Giansiracusa, *Equations of tropical varieties*, arXiv:1308.0042 (2013).

[26] A. Connes, C. Consani, *The arithmetic site*, arXiv:1405.4527 [math.NT] (2014). To appear in Comptes rendus de l'Académie des sciences.

[27] J.-M. Fontaine and J.-P. Wintenberger, Le "corps des normes" de certaines extensions algébriques de corps locaux, C.R. Acad. Sci. Paris S'er. A-B 288 (1979), A367A370.

Vita

Jeffrey Tolliver was born in 1985 in California. He received a B.A. degree in Mathematics from the California State University at Northridge in 2008, and an M.A. in Mathematics from the University of California at San Diego in 2009. He was admitted to the PhD program at Johns Hopkins in 2009. He completed his thesis under the direction of Professor Caterina Consani, and defended the thesis on February 23, 2015.