CWI Tracts

CWI
P.O. Box 94079, 1090 GB Amsterdam, The Netherlands
Telephone 31 - 20 592 9333, telex 12571 (mactr nl),
telefax 31 - 20 592 4199

CWI is the nationally funded Dutch institute for research in Mathematics and Computer Science.

Covariant formal group theory and some applications

I. Helsloot

1991 Mathematics Subject Classification: 14L05, 13K05, 14J10, 14J70, 14P99.
ISBN 90 6196 455 5
NUGI-code: 811

Printed in the Netherlands

Acknowledgement

This work on covariant formal group theory evolved from a thesis written at the Free University in Amsterdam. I therefore like to thank de Vrije Universiteit for its hospitality during the preparation of this manuscript.

I want to thank Bert Ditters, Jan Stienstra, Simen Hoving and Noriko Yui for their careful reading of the manuscript.

My special thanks are due to Astrid Scholtens. She knows what for.

Ira Helsloot

Contents

Introduction

Much has been written on commutative formal group theory and undoubtedly much more will be written. This work is another contribution to the theory of commutative formal groups. The main body of this work consists of a) a more or less self-contained presentation of commutative formal group theory in a covariant way, b) a theorem on the classification up to isomorphism of commutative formal groups defined over an algebraically closed field of positive characteristic. In the last chapter various applications are given.

In the first chapter the concept of DPS-Hopf algebras is introduced. The category DPS−cHopf of DPS-Hopf algebras will turn out to be equivalent to the category of commutative formal group laws. Classical concepts as curvilinearity and S-typicality have well defined counterparts in DPS−cHopf. Within one chapter we will develop most of the classical theory found in [Haz] or [Laz]. New is the emphasis on the universal object $C(\mathcal{A})$, whose group structure seems to reflect the menagerie of integrality lemmas necessary in the theory of commutative formal group laws. Witt and Hilbert rings will be seen to arise naturally in this setting.

The second chapter deals with F-types. We will show that the Witt and Hilbert (if they exist) F-types of a curvilinear commutative formal group law G fully describe the formal group law G. In the process we will construct a universal DPS-Hopf algebra over a polynomial ring L, and thus give a new proof of the fact that the Lazard ring is a polynomial ring. We proceed to give connections with the theory of Dieudonné [Dieu] and of Honda [Hon]. We adapt a lemma of Dieudonné in order to obtain a very computable algorithm for finding the isogeny type of a commutative formal group law given by its F-type.

In the third chapter we prove our main result: A commutative formal group law defined over an algebraically closed field k of positive characteristic of finite height is isomorphic to a commutative formal group law having a finite F-type. This finite F-type is described by a new set of invariants, called the jump data. Thus as a corollary we obtain: there is a catalogue of finite dimension over k of commutative formal group laws defined over k with bounded height.

In this chapter we also prove a theorem on the reduction of formal group laws defined over $W(k)$ given by their Hilbert F-types. This theorem will then be used to lift the problem of classification up to isomorphism over k to a well-described classification problem over $W(k)$.

The last chapter then gives several applications: We give a complete classification in the 2-dimensional case (this has also been done by Manin [Man] and Kneppers [Kne]). In the 2- and 3-dimensional case we give the isogeny types as function of the parameters in the finite F-type. In the 2-dimensional case this has been already be done by Kneppers [Kne90], but this is new in the 3-dimensional case. Moreover using our theory there is now no obstruction for doing the same in any dimension. The chapter ends by treating a problem suggested by N. Yui: describe the structure (of the isomorphism classes) of the formal Brauer groups of Fermat hypersurfaces defined over an algebraically closed field k of positive characteristic. Again the solution of this problem lies in lifting the problem to a problem over $W(k)$, solving that problem using the theory of Hilbert F-types (and the Serre-Witt cohomology as described in [SPM]) and then reducing the solution using a reduction theorem from chapter II.

Some notation and conventions

0.1 General conventions: We use the well known notation $\mathbb{N} = \{1, 2, ...\}$, $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{F}_q, (q = p^a)$. By $\mathcal{P}$ we will denote the set of all rational primes.

0.2 For a given totally ordered finite (!) set E, we denote by $\mathsf{MI}(E)$ the set of multi-indices on E, i.e., $\mathsf{MI}(E) := (\mathbb{N} \cup \{0\})^E$. The set $\mathsf{MI}(E)$ becomes an abelian monoid under entrywise addition, and an ordered set under the lexicographic order.

0.3 All rings and algebras are considered to be commutative and unitary. Therefore, a ring homomorphism $\phi : R_1 \to R_2$ will always satisfy the property $\phi(1) = 1$.
Let R be a commutative unitary ring and let CUR_R be the category of commutative unitary R-algebras. Especially, $\mathsf{CUR} := \mathsf{CUR}_{\mathbb{Z}}$ is the category of all commutative unitary rings. For $K \in \mathsf{CUR}_R$ we will denote the multiplication by $\mu : K \otimes K \to K$ and the unit map by $\eta : R \to K$ (unless otherwise stated, all tensor products are over the base ring R).

0.4 If $R \in \mathsf{CUR}$ and x is a subset of an R-module M, then we denote by $R\{x\}$ the R-module span of all $x_i \in x$ in M. In this context $R[x]$ denotes the R-algebra generated by all $x_i \in x$ in M. By $R[[x]]$ we denote the formal power series ring over R in the generic variables $x_i \in x$.

0.5 A sum of the form $\sum_{i=a}^{b} f_i$ with $a > b$ will be considered to be zero.

0.6 By (a, b) we denote the greatest common divisor of a and b.

0.7 If M is an R-module, then we denote by M^* the linear dual of M. If $f \in M^*$ and $m \in M$ then we define $\langle f, m \rangle := f(m)$.

Chapter 1

Generalities on DPS-Hopf algebras

1 DPS-Hopf algebras

1.1 For the definitions of coalgebra, bialgebra and Hopf algebra we follow closely [Haz], §37. Other references for the general theory of these concepts are [Abe] and [Yan].

1.2 Let $R \in \mathsf{CUR}$. A *coalgebra* over R is an R-module C together with two R-module homomorphisms $\Delta : C \to C \otimes C$ (the *comultiplication*) and $\epsilon : C \to R$ (the *counit* or the *augmentation*) such that

(i) $(\mathsf{Id} \otimes \Delta) \circ \Delta = (\Delta \otimes \mathsf{Id}) \circ \Delta$,

(ii) $(\epsilon \otimes \mathsf{Id}) \circ \Delta = (\mathsf{Id} \otimes \epsilon) \circ \Delta = \mathsf{Id}$

(where we have identified $R \otimes C \cong C \cong C \otimes R$). In categorical terms a coalgebra over R is a comonoid object in Mod_R, the category of R-modules, with two-sided counit. Let $\tau : C \otimes C \to C \otimes C$ denote the switching morphism which interchanges the two factors. The coalgebra C is said to be *cocommutative* if

(iii) $\tau \circ \Delta = \Delta$.

Let $R_2 \in \mathsf{CUR}_{R_1}$ with canonical ring homomorphism $\imath : R_1 \to R_2$. Let C_1 and C_2 be coalgebras over R_1 and R_2 respectively. An R_1-module homomorphism $f : C_1 \to C_2$ is said to be a morphism of coalgebras if and only if $(f \otimes f) \circ \Delta_1 = \Delta_2 \circ f$ and $\epsilon_2 \circ f = \imath \circ \epsilon_1$ (in Mod_{R_1}). Observe that we defined a coalgebra homomorphism between coalgebras over different base rings. In case the base rings are equal, we will sometimes say that f is an R-coalgebra homomorphism.

1.3 An R-module B is a called a *bialgebra* if

(i) B is a commutative R-algebra (with structural morphisms μ, η),

(ii) B is a coalgebra over R (with structural morphisms Δ, ϵ),

such that

(iii) μ and η are R-coalgebra morphisms,

(iv) Δ and ϵ are R-algebra morphisms.

There is some redundancy in these requirements, see [Haz] 37.1.2 for details. An algebra homomorphism between two bialgebras (possibly over different base rings) is a morphism of bialgebras if it also is a morphism of coalgebras. A bialgebra is called cocommutative if the underlying coalgebra is cocommutative. Denote by cBialg_R the category of cocommutative bialgebras over R.
Let H be a bialgebra and let $x = \{x_1, x_2, \ldots\}$ be a set of generic variables. Then we denote by $H_{x_1,x_2,\ldots} := H_x := \mathbb{Z}[x] \otimes H$ the bialgebra over $\mathbb{Z}[x]$ obtained by extension of scalars.
A *topological* bialgebra is a bialgebra B together with a topology on B such that the structural morphisms of B are continuous.

1.4 Let H be a bialgebra over R. Then the R-module homomorphism $\gamma : H \to H$ is called an *antipode* if

(i) $\mu \circ (\gamma \otimes \mathsf{Id}) \circ \Delta = \eta \circ \epsilon = \mu \circ (\mathsf{Id} \otimes \gamma) \circ \Delta$.

A *Hopf algebra* is a pair consisting of a bialgebra H with an antipode γ. If H is (co)commutative, then γ is a morphism of (co)algebras ([Haz], proposition 37.1.8). A morphism of Hopf algebras simply is a morphism of the underlying bialgebras (but by [Haz], proposition 37.1.10 we know that a morphism of bialgebras commutes with the antipode). We denote by cHopf_R the category of commutative and cocommutative Hopf algebras over R.
In categorical terms we may say that cHopf_R is the category of commutative cogroup objects of CUR_R. Equivalently $H \in \mathsf{cHopf}_R$ if and only if $Spec(H)$ is an affine commutative group scheme over R.

1.5 We give an easy example: Let $X = \{X_i | i \in I\}$ be a set of indeterminates. Then $R[X]$ becomes a Hopf algebra if we define $\Delta(X_i) := X_i \otimes 1 + 1 \otimes X_i$, $\epsilon(X_i) := 0$ and $\gamma(X_i) := -X_i$.

1.6 An element x in a bialgebra H such that $\Delta(x) = x \otimes 1 + 1 \otimes x$, is called *primitive*. The abelian group of primitive elements of H will be denoted $P(H)$.

1.7 A sequence $x = \{x_i | i \geq 0\} \subset H$ is called a *sequence of divided powers*, if and only if $x_0 = 1$ and $\Delta(x_n) = \sum_{i+j=n} x_i \otimes x_j$ for all n.
In the terminology of [Haz], 38.2.1 this would be a divided power sequence over 1. The name "divided powers" arises from the fact that this notion in a way

generalizes $x^n/n!$ (as does another, different, notion in algebra that also goes by the name "divided powers"). For details, see [Haz], 38.2.2.

1.8 For $H \in \mathsf{cBialg}_R$ (resp. $H \in \mathsf{cHopf}_R$) we define $\Delta := \Delta_t : H[[t]] \to (H \otimes H)[[t]]$ by

$$\Delta\left(\sum_{i\geq 0} h_i t^i\right) := \sum_{i\geq 0} \Delta(h_i) t^i.$$

Thus Δ is continuous with respect to the t-adic topologies. We then have the following basic relation between divided power sequences and primitive elements.

1.9 Lemma. *Let $H \in \mathsf{cBialg}_{\mathbb{Q}}$. Suppose given in H two sequences of elements $(x_i)_{i\geq 0}, (r_j)_{j\geq 0}$ such that $x_0 = 1, r_0 = 0$ and such that the following relation holds for $n \geq 0$*

$$nx_n = \sum_{i+j=n} x_i r_j. \tag{1.9.1}$$

(So in particular we have for all m that $r_m \in \mathbb{Z}[x_1, ..., x_m]$.) Then relation 1.9.1 is equivalent to the following relation in $H[[t]]$

$$\sum_{i=0}^{\infty} x_i t^i = exp\left(\sum_{m=1}^{\infty} \frac{r_m}{m} t^m\right). \tag{1.9.2}$$

Moreover, the sequence $x = \{x_i | i \geq 0\}$ is a sequence of divided powers in H, if and only if all r_m ($m \geq 1$) are primitive.

Relation (1.9.1) is called the *Newton relation.*

proof: For the equivalence of relations 1.9.1 and 1.9.2: Differentiate both sides of 1.9.2 with respect to t. Then compare the coefficients of powers of t.
In order to obtain the second assertion apply Δ to both sides of 1.9.2, and compare the coefficients of powers of t. Note that we need the commutativity of a and b for the relation $exp(a+b) = exp(a).exp(b)$.

□

1.10 We use the previous lemma to construct an important example of a Hopf algebra: $\mathcal{A}$, the *bialgebra of the symmetric functions.* Let $\sigma = \{\sigma_m | m \in \mathbb{N}\}$ be the set of indeterminates σ_m. Define $\mathsf{A} = \{\mathsf{a}_i | i \in \mathbb{N}\} \subset \mathbb{Q}[\sigma]$ by the following relation in $\mathbb{Q}[\sigma][[t]]$:

$$\sum_{i=0}^{\infty} \mathsf{a}_i t^i = exp\left(\sum_{m=1}^{\infty} \frac{\sigma_m}{m} t^m\right)$$

(so $\mathsf{a}_0 = 1$). Then it is easily verified using (1.9.1) that $\mathbb{Q}[\mathsf{A}] = \mathbb{Q}[\sigma]$. We now give $\mathbb{Q}[\sigma]$ the structure of a Hopf algebra as in example 1.5. By lemma 1.9 this means that $\mathsf{a} := \{\mathsf{a}_i | i \geq 0\}$, is a sequence of divided powers. Thus in particular, if we

define $\mathcal{A} := \mathbb{Z}[\mathsf{A}]$, then $\Delta(\mathsf{a}_i) \in \mathcal{A} \otimes \mathcal{A}$. Notice that the Newton relation holds in $\mathcal{A}$:

$$n\mathsf{a}_n = \sum_{i+j=n} \mathsf{a}_i \sigma_j.$$

Thus in particular $\sigma_m \in \mathcal{A}$. In order to show that $\gamma|_{\mathcal{A}}$ is an endomorphism of $\mathcal{A}$, consider the following relation in $\mathbb{Q} \otimes \mathcal{A}[[t]]$

$$\sum \gamma(\mathsf{a}_i)t^i = exp\left(\sum \frac{\gamma(\sigma_m)}{m} t^m\right) = \left(exp\left(\sum \frac{\sigma_m}{m} t^m\right)\right)^{-1} = \left(\sum \mathsf{a}_i t^i\right)^{-1} \in \mathcal{A}[[t]]$$

So $\mathcal{A}$ is a subHopf algebra of $\mathbb{Q}[\sigma]$. One easily finds that $P(\mathcal{A}) = \mathbb{Z}\{\sigma\}$, the $\mathbb{Z}$-module span of all σ_m.
The name "symmetric functions" stems from the fact that, introducing a new set of generic variables $y_i, i \in \mathbb{N}$, the a_n may be considered as the elementary symmetric functions in the y_i. The σ_j then turn out to be symmetric functions in the y_i. The classical proof of the equivalence between relations 1.9.1 and 1.9.2 is based on this fact (see [Haz], §17).

1.11 We generalize 1.10 as follows: Let $S \subset \mathcal{P}$ be an arbitrary set of rational primes, possibly empty, and let $\mathbb{N}(S)$ be the multiplicative submonoid of the natural numbers, generated by $S \cup \{1\}$. Let $\mathbb{Z}_S$ be the intersection of all localized rings $\mathbb{Z}_{(p)}, p \in S$. Here $\mathbb{Z}_\emptyset = \mathbb{Q}$, by definition. Put $\sigma_S = \{\sigma_m | m \in \mathbb{N}(S)\}$ for indeterminates σ_m. Consider the relation

$$\sum_{n \geq 0} E_n t^n = exp\left(\sum_{m \in \mathbb{N}(S)} \frac{\sigma_m}{m} t^m\right), \qquad 1.11.1$$

in the bialgebra $\mathbb{Q}[\sigma_S]$, where we assume that all σ_m are primitive. If $m \in \mathbb{N}(S)$, then we define $\mathsf{a}_m := \mathsf{a}_{m,S} := E_m$. (Notice the double meaning of the a_m.) Let A_S denote the set $\{\mathsf{a}_m | m \in \mathbb{N}(S)\}$. Let a_m have weight m. We easily see that $\mathbb{Q}[\sigma_S] = \mathbb{Q}[\mathsf{A}_S]$, and the E_n, for natural numbers n, then become isobaric polynomials of weight n over $\mathbb{Q}$ in the indeterminates a_m for $m \in \mathbb{N}(S)$. However, the following generalization of a theorem of Dieudonné ([Dieu52]) shows, that actually all E_n have coefficients in $\mathbb{Z}_S$.

1.12 Lemma. *The sequence $\{E_n | n \geq 0\}$ is a sequence of divided powers in $\mathcal{A}_S := \mathbb{Z}_S[\mathsf{A}_S]$. Consequently $\mathcal{A}_S$ is a bialgebra over $\mathbb{Z}_S$. Also, $P(\mathcal{A}_S) = \mathbb{Z}_S\{\sigma_S\}$, the $\mathbb{Z}_S$-module span of all $\sigma_m, m \in \mathbb{N}(S)$.*

proof: Let m be the smallest integer such that $E_m = \sum_\beta e_\beta \mathsf{a}^\beta \notin \mathbb{Z}_S[\mathsf{A}_S]$, and let β be a multi-index such that $e_\beta \notin \mathbb{Z}_S$. Then $m \notin \mathbb{N}(S)$. Consider the following relation:

$$\Delta E_m - E_m \otimes 1 - 1 \otimes E_m = \sum_{i+j=m,\, i,j \neq 0} E_i \otimes E_j \in \mathbb{Z}_S[\mathsf{A}_S] \otimes \mathbb{Z}_S[\mathsf{A}_S]$$

We have the following two possibilities:
1^o) There is an index i such that $\beta = (\beta_1, ..., \beta_r)$ with $\beta_i, \beta_r \neq 0, i \neq r$. We then find that the coefficient of $\mathsf{a}_1^{\beta_1} \dots \mathsf{a}_{r-1}^{\beta_{r-1}} \otimes \mathsf{a}_r^{\beta_r}$ in the left hand side of this relation is e_β. Therefore e_β is an element of $\mathbb{Z}_S$. This is a contradiction.
2^o) $\beta = (\beta_r)$, so because of weight considerations $\beta_r = m/r$. Now the coefficient c_a of $\mathsf{a}_r^a \otimes \mathsf{a}_r^{\beta_r - a}$ in the left hand side of the relation is seen to be

$$c_a = e_\beta \begin{pmatrix} \beta_r \\ a \end{pmatrix} \in \mathbb{Z}_S, \quad a = 1, ..., \beta_r - 1.$$

The gcd of all c_a is pe_β if $\beta_r = p^n$ (for some prime p and $n \in \mathbb{N}$) and is e_β otherwise. But in any event $\beta_r \notin \mathbb{N}(S)$ (as $r\beta_r = m \notin \mathbb{N}(S)$ already) so in the first situation p is invertible in $\mathbb{Z}_S$. Therefore $e_\beta \in \mathbb{Z}_S$ and this again leads us to a contradiction. □

We call $\mathcal{A}_S$ the *bialgebra of the S-typical symmetric functions.* Notice that we have a homomorphism of bialgebras $\mathcal{A} \to \mathcal{A}_S$ defined by $\sigma_n \mapsto 0$ if $n \notin \mathbb{N}(S)$ and $\sigma_n \mapsto \sigma_n$ for $n \in \mathbb{N}(S)$.

1.13 Let $H \in \mathsf{cHopf}_R$. A basis $\phi = \{\phi_I | I \in \mathsf{MI}(E)\}$ for H considered as an R-module is called *a structural basis* if

$$\Delta\phi_I = \sum_{L+K=I} \phi_L \otimes \phi_K. \qquad 1.13.1$$

A *DPS-Hopf algebra* over R is a pair (H, ϕ), where $H \in \mathsf{cHopf}_R$ and ϕ is a structural basis for H. But we usually just say H is a DPS-Hopf algebra. A morphism of DPS-Hopf algebras is a morphism between the underlying Hopf algebras. Especially an isomorphism of DPS-Hopf algebras may be considered as a change of structural basis. The category of DPS-Hopf algebras over R will be denoted as $\mathsf{DPS{-}cHopf}_R$. The *dimension* of a DPS-Hopf algebra is defined as the cardinality of E. Notice that for $H \in \mathsf{DPS{-}cHopf}_R$ we have that $P(H) = R\{\phi_{\epsilon_i}\}$ ($i \in E, \epsilon_i$ is the i-th unit multi-index).

1.14 Remark. —Recall that we have (subsection 0.2) adopted the convention that the index set E is finite. One might also define the notion of a DPS-Hopf algebra for infinite index sets E. A non-trivial example of such a DPS-Hopf algebra is $\mathcal{A}$ (note that the $\mathbb{Z}$-module basis $\{\mathsf{a}^I | I \in \mathsf{MI}(\mathbb{N})\}$ is not structural). For a proof of this fact see [Scho].
—We might define a DPS-bialgebra as a bialgebra which admits a structural basis. In the sequel we will see, however, that a DPS-bialgebra always admits an antipode.

1.15 Let $H \in \mathsf{DPS{-}cHopf}_R$ and $f : R \to R'$ a ring homomorphism. Then we define $f_*(H) \in \mathsf{DPS{-}cHopf}_{R'}$ by the following procedure: Let $\{\phi_I | I \in \mathsf{MI}(E)\}$ be

a structural basis for H with algebra structure defined by

$$\phi_I \phi_J = \sum_K a_{I,J,K} \phi_K.$$

Then $f_*(H)$ is the DPS-Hopf algebra over R' defined as the free R'-module on the structural basis $\{\phi_I | I \in \mathsf{MI}(E)\}$ and with algebra structure defined by

$$\phi_I \phi_J = \sum_K f(a_{I,J,K}) \phi_K.$$

One easily checks that $f_*(H)$ is indeed a Hopf algebra.

1.16 Denote for $H \in \mathsf{cBialg}_R$ the linear dual as H^*, and for a topological bialgebra H the continuous linear dual as H^{*c}. (The continuous linear dual consists of all linear functionals which are continuous.) Let X_E be the set $\{X_e | e \in E\}$. For an $H \in \mathsf{DPS{-}cHopf}_R$ with structural basis $\{\phi_I | I \in \mathsf{MI}(E)\}$ the linear dual H^* has the following properties.

1.17 Proposition. *Let $H \in \mathsf{DPS{-}cHopf}_R$ with structural basis $\{\phi_I | I \in \mathsf{MI}(E)\}$. Then*

(i) *$H^* \cong R[[X_E]]$ as R-algebras.*

(ii) *H^* is a topological bialgebra under the X_E-adic topology.*

(iii) *$(H^*)^{*c} \cong H$.*

proof: (i): Let $H \in \mathsf{DPS{-}cHopf}_R$ with structural basis $\{\phi_I | I \in \mathsf{MI}(E)\}$. Let $\delta_{I,\bullet} : H \to R$ be defined by $\delta_{I,\bullet}(\phi_J) := \delta_{I,J}$. (Thus $\delta_{I,J} = 1$ if $I = J$ and $\delta_{I,J} = 0$ if $I \neq J$.) Then the isomorphism of R-algebras between H^* and $R[[X_E]]$ is given by $\delta_{I,\bullet} \mapsto X^I$. (Indeed use:

$$\delta_{I,\bullet}.\delta_{J,\bullet} = (\delta_{I,\bullet} \otimes \delta_{J,\bullet}) \circ \Delta = \delta_{I+J,\bullet} \qquad .)$$

(ii) Straightforward dualization. (Notice $(H \otimes H)^* \cong H^* \hat{\otimes} H^*$ as topological R-algebras because of (i).)
(iii): Continuous linear functionals on H^* are zero on monomials of sufficiently high degree, so an R-module basis for $(H^*)^{*c}$ is given by $\delta_{X^I,\bullet}, (I \in \mathsf{MI}(E))$. This basis is easily seen to be structural. The isomorphism $(H^*)^{*c} \cong H$ now is given by $\delta_{X^I,\bullet} \mapsto \phi_I$.
Note that we have used the cocommutativity. □

1.18 Let $H, H' \in \mathsf{DPS{-}cHopf}_R$ and $f : H \to H'$ a homomorphism of Hopf algebras. Then $f^* : H'^* \to H^*$ is a homomorphism of topological Hopf algebras, completely determined by $f^*(X'_e), e \in E'$.

Conversely: Of course, if T, T' are topological Hopf algebras over R, isomorphic as topological algebras to $R[[X_E]]$ respectively $R[[X_{E'}]]$, then any homomorphism $f : T \to T'$ induces a homomorphism of DPS-Hopf algebras $f^* : T'^* \to T^*$.
We denote the full subcategory of cHopf_R consisting of all topological Hopf algebras over R, isomorphic as topological R-algebras to $R[[X_E]]$, for some finite index set E, as $\mathsf{smooth{-}cHopf}_R$. As we have seen in the proof of proposition 1.17, part (iii), if $H \in \mathsf{smooth{-}cHopf}_R$, then $H^{*c} \in \mathsf{DPS{-}cHopf}_R$.

1.19 Corollary. *(Cartier) The categories* $\mathsf{DPS{-}cHopf}_R$ *and* $\mathsf{smooth{-}cHopf}_R$ *are anti-equivalent.* □

1.20 The following will often be useful to us: Let $Y_i \in H^*, i \in E$ be algebraically independent such that $R[[Y_E]] = H^*$. Then we define an isomorphism of topological algebras $\Phi : R[[Z_E]] \to H^*$ by $\Phi(Z_i) := Y_i (i \in E)$. We extend this to an isomorphism of topological Hopf algebras by defining $\Delta(Z_i) := \Phi^{-1}(\Delta(Y_i))$.

2 Curves

2.1 A *curve* in a bialgebra H over R is a bialgebra morphism $\phi : \mathcal{A} \to H$, or equivalently, ϕ is given by a sequence of divided powers $\{\phi_i := \phi(\mathsf{a}_i) | i \geq 0\}$ in H. We will usually write ϕ as an element of $H[[t]]$: $\phi = \sum_{i \geq 0} \phi_i t^i$. We denote the set of curves as $C(H)$. We define the m-th *ghost component* of $\phi \in C(H)$ as $r_m(\phi) := \phi(\sigma_m)$ (recall $\sigma_m \in \mathcal{A}$). We give the set $C(H)$ a topology by considering $C(H)$ as a subset of $H[[t]]$, endowed with the t-adic topology.

2.2 If $H \in \mathsf{cBialg}_R$ and H has no additive torsion (or equivalently, H flat over $\mathbb{Z}$), then as in lemma 1.9 we may write in $\mathbb{Q} \otimes H[[t]]$

$$\phi = \sum_{i \geq 0} \phi_i t^i = exp\left(\sum_{m \in \mathbb{N}} \frac{r_m(\phi)}{m} t^m \right). \qquad 2.2.1$$

So in this case the curve ϕ is determined by the set $\{r_m(\phi) | m \geq 1\}$ of (primitive) ghost components.

2.3 Lemma. *$C(H)$ becomes an abelian group if we define*

$$\phi + \psi := \mu_H \circ (\phi \otimes \psi) \circ \Delta_{\mathcal{A}},\ 1_{C(H)}(\mathsf{a}_i) := \delta_{0,i} \text{ and } -\phi := \phi \circ \gamma_{\mathcal{A}}.$$

As an element of $H[[t]]$ the curve $\phi + \psi$ is obtained by multiplication of power series. For the ghost components we have the relations:

$$r_m(\phi + \psi) = r_m(\phi) + r_m(\psi),\ r_m(-\phi) = -r_m(\phi).$$

□

2.4 The following obvious observation will often be useful: Let H have no additive torsion, $\phi \in C(H)$ and suppose $\phi_i = 0$ $(1 \leq i < n)$ or equivalently $r_m(\phi) = 0$ $(1 \leq m < n)$. Then $\phi_n = r_n(\phi)/n \in P(H)$ (Newton relation).

2.5 If $H \in \mathsf{DPS{-}cHopf}_R$ with structural basis $\{\phi_I | I \in \mathsf{MI}(E)\}$ we still have another presentation of curves. Notice that R-algebra morphisms of H^* to $R[[t]]$ (with the t-adic topology) are necessarily continuous.

2.6 Lemma. *Let $H \in \mathsf{DPS{-}cHopf}_R$. We have an isomorphism of groups*

$$C(H) \cong \mathsf{Alg}_R(H^*, R[[t]]).$$

proof: By lemma 1.17 we know that $H^* \cong R[[X_E]]$ as topological R-algebras.
If $\phi = \sum \phi_i t^i \in C(H)$, we define $\tilde{\phi} \in \mathsf{Alg}_R(H^*, R[[t]])$ by $\tilde{\phi}(X_e) := \sum \langle X_e, \phi_i \rangle t^i$, $e \in E$.
Conversely: Assume that $\psi \in \mathsf{Alg}_R(H^*, R[[t]])$. Then we may write $\psi = \sum \psi_i t^i$ for $\psi_i \in H^{**}$. Since ψ necessarily is continuous, we have that $\psi(X_e) \in tR[[t]]$, and therefore that ψ_i is zero on monomials of total degree greater than i. So especially ψ_i is continuous and thus may be considered as an element of H. That the sequence $\{\psi_i | i \geq 0\}$ is a sequence of divided powers follows from

$$\sum_n \langle \Delta\psi_n, x \otimes y \rangle t^n = \psi(xy) = \psi(x)\psi(y) = \sum_n \langle \sum_{i+j=n} \psi_i \otimes \psi_j, x \otimes y \rangle t^n.$$

□

2.7 An *S-typical curve* in a $\mathbb{Z}_S$-bialgebra H is a curve which factors via $\mathcal{A}_S$ or equivalently a morphism of bialgebras $\mathcal{A}_S \to H$. Such a curve is determined by the values on the elements of A_S. If moreover H has no additive torsion, an S-typical curve can therefore be written as

$$\phi = \sum_{i \geq 0} \phi_i t^i = exp\left(\sum_{m \in \mathbb{N}(S)} \frac{r_m(\phi)}{m} t^m \right).$$

The set of all S-typical curves is denoted $C_S(H)$. We will usually write $\sum_S$ or $\sum_{S,m}$ instead of $\sum_{m \in \mathbb{N}(S)}$. Since $\mathcal{A}_S$ is a subHopf algebra of $\mathbb{Z}_S \otimes \mathcal{A}$ we see from lemma 2.3 that $C_S(H)$ is a subgroup of $C(H)$.

2.8 If $f : H \to H'$ is a homomorphism of bialgebras, then we denote by $C(f) : C_S(H) \to C_S(H')$ the induced homomorphism of groups sending $\phi \in C_S(H)$ to $f \circ \phi \in C_S(H')$. Note that we have $(C(f)\phi)_n = f(\phi)_n$.

Operators on the group of curves

2.9 Following Cartier, we will define three types of operators on $C_S(H), H \in \mathsf{cBialg}_R$. For $a \in \mathbb{N}(S)$ we will define V_a, the a-th *Verschiebung*, and F_a, the a-th *Frobenius operator*, and for $r \in R$ we will define $[r]$, the *Witt operator* or *homothety.*
Since there are some subtilities involved which tend to mess up a clear understanding, we introduce some additional notations.

2.10 Recall that for a generic λ, $\mathcal{A}_\lambda := \mathbb{Z}[\lambda] \otimes \mathcal{A}$ and $\mathcal{A}_{S,\lambda} := \mathbb{Z}[\lambda] \otimes \mathcal{A}_S$ are bialgebras over $\mathbb{Z}[\lambda]$ and $\mathbb{Z}_S[\lambda]$ respectively, obtained by extension of scalars. Also let $\rho_r : \mathbb{Z}[\lambda] \to R$ for $r \in R$, be defined by $\rho_r(\lambda) := r$. We will define $F_a^e, V_a^e \in \mathsf{End}_{\mathsf{cBialg}}(\mathcal{A})$ and $[\lambda]^e \in \mathsf{cBialg}_{\mathbb{Z}}(\mathcal{A}, \mathcal{A}_\lambda)$ and use these to define

$$F_a\phi := \phi \circ F_a^e,\ V_a\phi := \phi \circ V_a^e \text{ and } [r]\phi := (\rho_r \otimes \phi) \circ [\lambda]^e.$$

Especially we have thus defined *generic* operators F_a^g, V_a^g on $C(\mathcal{A})$ and $[\lambda]$ on $C(\mathcal{A}_\lambda)$. We then have, for example, that $F_a^g(\mathsf{Id}_{\mathcal{A}}) = F_a^e$. Therefore defining F_a^e is equivalent to giving the curve $F_a^g(\mathsf{Id}_{\mathcal{A}}) \in C(\mathcal{A})$. The same applies for the other operators.
Notice that the ring generated by all $F_a^e, V_a^e, [\lambda]^e$ is the opposite ring of the ring generated by all $F_a^g, V_a^g, [\lambda]$. Hence we see that in order to prove relations between F_a^e, V_a^e and $[\lambda]^e$ (and thus the "opposite" of these relations hold between F_a, V_a and $[r]$ on $C(H), H \in \mathsf{cBialg}_R$) it suffices to prove the corresponding relations for F_a^g, V_a^g and $[\lambda]$ on $C(\mathcal{A}_\lambda)$. We will say that it suffices to check the relations *generically.*
But as $\mathcal{A}_\lambda$ has no additive torsion we may restrict ourselves to checking the relations we want to prove for the ghost components. This fact will turn out to be a strong tool, for example lemma 2.16 now is reduced to almost a triviality, contrary to [Haz], 16.2.

2.11 We start by defining V_a^e. Under the notations of 1.10, we easily define V_a^e by

$$V_a^e(\mathsf{a}_m) := \mathsf{a}_{m/\!\!/a} \tag{2.11.1}$$

(where $\mathsf{a}_{m/\!\!/a} := \mathsf{a}_{m/a}$ if $a|m$ and $\mathsf{a}_{m/\!\!/a} := 0$ if $a \not| m$), or equivalently,

$$V_a^g(\mathsf{Id}_{\mathcal{A}}) = V_a^g\left(\sum_{n\geq 0} \mathsf{a}_n t^n\right) := \sum_{n\geq 0} \mathsf{a}_n t^{an}, \tag{2.11.2}$$

or equivalently,

$$V_a^g(\mathsf{Id}_{\mathcal{A}}) = V_a^g(exp\left(\sum \frac{\sigma_m}{m} t^m\right)) := exp\left(\sum \frac{\sigma_m}{m} t^{am}\right). \tag{2.11.3}$$

From 2.11.1 or 2.11.2 one immediately has that V_a^e is a $\mathbb{Z}$-algebra endomorphism, while from 2.11.3 one has (using lemma 1.9) that $V_a^g(\mathsf{Id}_{\mathcal{A}})$ is a coalgebra morphism $\mathcal{A} \to \mathbb{Q} \otimes \mathcal{A}$. Thus $V_a^g(\mathsf{Id}_{\mathcal{A}}) \in C(\mathcal{A})$.

2.12 The generic Witt operator $[\lambda]$ is also easily defined by

$$[\lambda]^e(\mathsf{a}_m) := \lambda^m \mathsf{a}_m, \tag{2.12.1}$$

or equivalently,

$$[\lambda](\mathsf{Id}_{\mathcal{A}}) = [\lambda]\left(\sum_{n\geq 0} \mathsf{a}_n t^n\right) := \sum_{n\geq 0} \mathsf{a}_n \lambda^n t^n, \tag{2.12.2}$$

or equivalently,

$$[\lambda](\mathsf{Id}_{\mathcal{A}}) = [\lambda](exp\left(\sum \frac{\sigma_m}{m} t^m\right)) := exp\left(\sum \frac{\sigma_m}{m} \lambda^m t^m\right). \tag{2.12.3}$$

Again: From 2.12.1 or 2.12.2 one immediately has that $[\lambda]^e$ is an $\mathbb{Z}$-algebra morphism $\mathcal{A} \to \mathcal{A}_\lambda$, while from 2.12.3 one has (using lemma 1.9) that $[\lambda](\mathsf{Id}_{\mathcal{A}}) \in C(\mathbb{Q} \otimes \mathcal{A}_\lambda)$. Thus $[\lambda](\mathsf{Id}_{\mathcal{A}}) \in C(\mathcal{A}_\lambda)$.

2.13 For the ghost components we find the following relation

$$r_m\left(V_a^g(\phi)\right) = V_a^g(\phi)(\sigma_m) = \phi(V_a^e(\sigma_m)) = \phi\left(a\sigma_{m/\!/a}\right) = a r_{m/\!/a}(\phi).$$

Analogously we find $r_m([\lambda](\phi)) = \lambda^m r_m(\phi)$.

2.14 The generic Frobenius operator is defined in terms of ghost components as follows

$$r_m\left(F_a^g(\mathsf{Id}_{\mathcal{A}})\right) := \sigma_{am}.$$

So we clearly have that $F_a^g(\mathsf{Id}_{\mathcal{A}}) \in C(\mathbb{Q} \otimes \mathcal{A})$, but we have to check whether $F_a^g(\mathsf{Id}_{\mathcal{A}})$ is still defined over $\mathcal{A}$. For this let ζ_a be a primitive a-th root of unity. From $\sum_{i=1}^a \zeta_a^{im} = a\delta_{a,(m,a)}$ we see that

$$\begin{aligned} V_a^g F_a^g(\mathsf{Id}_{\mathcal{A}}) &= exp\left(\sum \frac{\sigma_{am}}{am} a t^{am}\right) = exp\left(\sum \frac{\sigma_m}{m} (\sum_{i=1}^a \zeta_a^{im}) t^m\right) \\ &= \sum_{i=1}^a [\zeta_a^i]\mathsf{Id}_{\mathcal{A}}. \end{aligned}$$

Since $\sum_{i=1}^a [\zeta_a^i]\mathsf{Id}_{\mathcal{A}}$ is invariant under all $\rho \in \mathsf{Gal}\,(\mathbb{Q}(\zeta)/\mathbb{Q})$, we see that $V_a^g F_a^g(\mathsf{Id}_{\mathcal{A}}) \in C(\mathcal{A})$. Therefore $F_a(\mathsf{Id}_{\mathcal{A}}) \in C(\mathcal{A})$, as V_a^g does not change the ring of definition (2.11.1).

2.15 From the relations for the ghost components we immediately see that all three types of operators may be restricted to S-typical groups of curves. However for $a \notin \mathbb{N}(S)$ we have that F_a and V_a become the trivial operators.

2.16 Lemma. *We have the following relations among the generic Frobenius, the generic Verschiebung and the generic Witt operators on the group* $C(\mathcal{A}_{\lambda,\mu})$

$$V_1^g = F_1^g = [1] = \mathsf{Id}_{\mathcal{A}},$$

$$[\lambda][\mu] = [\lambda\mu],\ V_a^g V_b^g = V_{ab}^g,\ F_a^g F_b^g = F_{ab}^g,$$

$$[\lambda]V_a^g = V_a^g[\lambda^a],\ F_a^g[\lambda] = [\lambda^a]F_a^g,$$

$$F_a^g V_a^g = a,\ F_a^g V_b^g = V_b^g F_a^g \text{ if } (a,b) = 1.$$

□

2.17 Let R have characteristic $p > 0$. We will show that in $C_S(H), H \in \mathsf{cBialg}_R$ the operators F_p and V_p commute. Consider the generic relation

$$(p - V_p^g F_p^g)\mathsf{Id}_{\mathcal{A}} = exp\left(p\sum\nolimits_{m\in\mathbb{N}\setminus p\mathbb{N}} \frac{\sigma_m}{m} t^m\right).$$

We immediately find the right hand side to be a curve in $p\mathbb{Z}_{(p)} \otimes \mathcal{A}$ (but actually it is, of course, a curve in $p\mathcal{A}$ since the left hand side is a curve in $\mathcal{A}$). Therefore after reducing we find that $p = V_p F_p$ as operators of $C_S(H)$, and thus (using lemma 2.16) we have shown $V_p F_p = p = F_p V_p$.

2.18 If $f : H \to H'$ is a homomorphism of bialgebras, then $C(f)$ (see 2.8) commutes with F_a, V_a and $C(f)[r]\phi = [f(r)]C(f)\phi$, as one easily checks.

Topology and convergence

We will show that $C_S(H)$ is a complete separated (or Hausdorff) topological group. (Recall that separated means that any two different curves have non-intersecting neighbourhoods.)

2.19 Lemma. *The group $C_S(H)$ is filtered by $\{V_a C_S(H) \mid a \in \mathbb{N}(S)\}$ and is complete in the following sense: Any sequence $\sum_{a\in\mathbb{N}(S)} V_a\psi_a$ for $\psi_a \in C_S(H)$, converges in $C_S(H)$ (We will say that $C_S(H)$ is V-*complete*).*

proof: Observe that $r_m(V_a\phi) = 0$ for $m < a$. □

It is easy to see that $[\lambda], \lambda \in R$ and $F_a, a \in \mathbb{N}(S)$ are continuous operators with respect to this topology on $C_S(H)$.

2.20 We define $\pi_t : C_S(H) \to P(H)$ by

$$\pi_t\left(\sum_{i\geq 0} \phi_i t^i\right) := \phi_1 = r_1(\phi).$$

Then it is easily seen that π_t is a group homomorphism.
A set of curves $\{\psi_i\}$ ($i \in I$ for some set I) such that $\{\pi_t\psi_i\}$ is a basis for $P(H)$ is called *a fundamental set of curves*

2.21 Let H be the bialgebra $\mathbb{Z}[\sigma]$, for an indeterminate primitive σ. We will prove that $C(H) = \{0\}$, which shows that π_t is in general not surjective.
Suppose $0 \neq \psi \in C(H)$. Without loss of generality we may assume that $\psi_1 \neq 0$, so $\psi_1 = z\sigma$, $z \in \mathbb{Z} - \{0\}$. Write the curve ψ as $exp(\sum m^{-1} r_m(\psi) t^m)$ in $C(H_{\mathbb{Q}})$. Notice that $r_m(\psi) = z_m\sigma$, $z_m \in \mathbb{Z}$. Then we find from the Newton relation that $\psi_i = z^i\sigma^i/i!+$ lower order terms in σ. Thus $\psi_i \notin \mathbb{Z}[\sigma]$ for $i > |z|$.

2.22 Lemma. *Let I be a finite index set and let $\{\psi_i | i \in I, \psi_i \in C_S(H)\}$ be such that $\{\pi_t(\psi_i) | i \in I\}$ is a generating set for $\pi_t(C_S(H))$. Then $\phi \in C_S(H)$ can be written as*

$$\phi = \sum_{a \in \mathbb{N}(S), i \in I} V_a[\lambda_{a,i}]\psi_i, \quad \lambda_{a,i} \in R.$$

If $\{\pi_t(\psi_i) | i \in I\}$ is a basis for $\pi_t(C_S(H))$, then the above expression is unique. So $C_S(H)$ is separated.

proof: Suppose $\phi_m = (\sum_{S, a<n, i\in I} V_a[\lambda_{a,i}]\psi_i)_m$, for $m < n$. Then by observation 2.4 we have that $(\phi - \sum_{S, a<n, i\in I} V_a[\lambda_{a,i}]\psi_i)_n$ is primitive. We therefore may write

$$(\phi - \sum_{\substack{S \\ a<n, i\in I}} V_a[\lambda_{a,i}]\psi_i)_n = \sum_{i\in I} \lambda_{n,i}\pi_t(\psi_i) = \pi_t\left(\sum_{i\in I}[\lambda_{n,i}]\psi_i\right),$$

for some $\lambda_{n,i} \in R$. But then $\phi_m = (\sum_{S, a\leq n, i\in I} V_a[\lambda_{a,i}]\psi_i)_m$, for $m \leq n$. □

2.23 Let H be a DPS-Hopf algebra over R with structural basis $\{\phi_I | I \in \mathsf{MI}(E)\}$. Let ϵ_i ($i \in E$) denote the i-th unit multi-index. Then we define the i^{th} *canonical curve* $\phi_{H,i}$ by

$$\phi_{H,i} := \sum_{n\in\mathbb{N}} \phi_{n\epsilon_i} t^n. \qquad 2.23.1$$

(This is indeed a curve!) Notice that $r_1(\phi_{H,i}) = \phi_{\epsilon_i}$, and that the tempting definition $\psi_i := exp(\phi_{\epsilon_i} t)$ does only give a curve in $C(H)$ if $R \in \mathsf{CUR}_{\mathbb{Q}}$.

2.24 Corollary. *Let $H \in \mathsf{DPS{-}cHopf}_R$ and $\phi \in C(H)$. Then ϕ can be uniquely written as*

$$\phi = \sum_{a\in\mathbb{N}, i\in E} V_a[\lambda_{a,i}]\phi_{H,i} \quad \lambda_{a,i} \in R. \qquad 2.24.2$$

proof: The set $\{\pi_t(\phi_{H,i}) | i \in E\} = \{\phi_{\epsilon_i} | i \in E\}$ is a basis for $\pi_t(C(H)) = P(H)$, so by lemma 2.22 we are done. □

Module structure

2.25 The group $C_S(H)$ is a module over the ring generated by all operators F_a, V_a and $[\lambda]$ $(a \in \mathbb{N}(S), \lambda \in R)$. We will formalize this a little bit. Let $\mathrm{Cart}_S(R)$ be defined as set of formal sums of symbols by

$$\mathrm{Cart}_S(R) := \left\{ \sum\nolimits_{a,b\in\mathbb{N}(S)} V_a[\lambda_{a,b}]F_b \;\middle|\; \lambda_{a,b} \in R,\ \#\{b|\lambda_{a,b} \neq 0\} < \infty \text{ for all } a \right\}.$$

Since $C_S(H)$ is V-complete, we may interpret the elements of $\mathrm{Cart}_S(R)$ as well-defined operators on $C_S(H), H \in \mathsf{cBialg}_R$. As such $\mathrm{Cart}_S(R)$ may be considered as a subset of the ring of operators on $C_S(H)$. From lemmas 2.16 and lemma 2.26 below we see that $\mathrm{Cart}_S(R)$ actually is a subring and that the ring structure is independent of H. Using 2.18 we conclude that $\mathrm{Cart}_S(\bullet)$ may even be considered as a functor $\mathsf{CUR} \to \mathsf{UR}$.

2.26 Lemma. *Let $\mathcal{A}_{S,\mu,\lambda} := \mathbb{Z}[\mu,\lambda] \otimes \mathcal{A}_S$ be the bialgebra over $\mathbb{Z}_S(\mu,\lambda)$ (for generic μ,λ), obtained by extension of scalars. We then have the following relation of generic operators on $C_S(\mathcal{A}_{S,\mu,\lambda})$*

$$[\lambda] + [\mu] = \sum\nolimits_S V_a^g[\nu_a]F_a^g,$$

with unique $\nu_a \in \mathbb{Z}[\lambda,\mu]$.

proof: One easily checks that $r_m(\sum_S V_a^g[\nu_a]F_a^g \mathsf{Id}_{\mathcal{A}_{S,\mu,\lambda}}) = \sum_{d|m} d\nu_d^{m/d}\sigma_m$. So assume that we found $\nu_a \in \mathbb{Z}[\lambda,\mu]$ for $a < n, n \in \mathbb{N}(S)$ such that $r_m([\lambda]\mathsf{Id}_{\mathcal{A}_{S,\mu,\lambda}} + [\mu]\mathsf{Id}_{\mathcal{A}_{S,\mu,\lambda}}) = r_m(\sum_S V_a[\nu_a]F_a \mathsf{Id}_{\mathcal{A}_{S,\mu,\lambda}})$ for $m < n$. Now consider the relation in $C(\mathbb{Q}[\lambda,\mu] \otimes \mathcal{A}) \supset C_S(\mathbb{Q}[\lambda,\mu] \otimes \mathcal{A}_S)$

$$\left([\lambda] + [\mu] - \sum_{a<n}{}_S\, V_a^g[\nu_a]F_a^g\right)\mathsf{Id}_{\mathcal{A}_{S,\mu,\lambda}} = \left(\sum_{a\geq n}{}_S\, V_a^g[\nu_a]F_a^g\right)\mathsf{Id}_{\mathcal{A}_{S,\mu,\lambda}}. \qquad 2.26.1$$

Then we find by comparing the coefficients of t^n in both sides and using observation 2.4, that

$$\frac{\lambda^n + \mu^n - \sum_{d|n,d\neq n} d\nu_d^{n/d}}{n}\sigma_n = \frac{n\nu_n}{n}\sigma_n. \qquad 2.26.2$$

Now, since $C(\mathcal{A}_{\lambda,\mu})$, is a group the left hand side of 2.26.1 is an element of $C(\mathcal{A}_{\lambda,\mu})$, therefore the left hand side of 2.26.2 is an element of $\mathcal{A}_{\lambda,\mu}$. But then there is a unique $\nu_n \in \mathbb{Z}[\lambda,\mu]$ such that $r_n(\sum_S V_a^g[\nu_a]F_a^g \mathsf{Id}_{\mathcal{A}_{S,\mu,\lambda}}) = r_n([\lambda]\mathsf{Id}_{\mathcal{A}_{S,\mu,\lambda}} + [\mu]\mathsf{Id}_{\mathcal{A}_{S,\mu,\lambda}})$. □

We denote the $\mathrm{Cart}_S(R)$-module structure by $\heartsuit$ on places where confusion might arise.

2.27 Remark. – The proof of lemma 2.26 is based on the very small trick: "use the group structure of $C(\mathcal{A})$". We will use this technique several times more, and each time it replaces some (ad hoc) integrality lemma in [Haz] (for instance, the proof of lemma 2.26 replaces [Haz], 16.2.10 and 17.1.3).
– There is a more elegant, but also more involved way of defining $\mathrm{Cart}_S(R)$. That is, we may define $\mathrm{Cart}_S(R)$ as $\mathsf{End}\,(R\otimes\mathcal{A}_S)^{opp}$ (the opposite ring of $\mathsf{End}\,(R\otimes\mathcal{A}_S)$). One then needs the fact that $\mathcal{A}$ is a DPS-Hopf algebra (remark 1.14), so especially $P(R\otimes\mathcal{A}) = R\otimes P(\mathcal{A})$, and the technique of lemma 2.22 to describe $\mathsf{End}\,(R\otimes\mathcal{A}_S)$.

2.28 From lemma 2.26 we immediately see that the subset $\mathcal{W}_S(R)$ of $\mathrm{Cart}_S(R)$ defined by $\mathcal{W}_S(R) := \{\sum_S V_a[\lambda_a]F_a \,|\lambda_a \in R\}$ is a subring. One may check that $\mathcal{W}_S(R)$ is commutative. Thus we may consider $\mathcal{W}_S(\bullet)$ as functor $\mathsf{CUR} \to \mathsf{CUR}$. We will study this functor in the next section.

3 Witt vectors and Hilbert rings

All results of this section for $S = \{p\}$ or $S = \mathcal{P}$ can be found in [Haz, §17 and §27], or in [Laz].

3.1 We define the *ring of S-Witt vectors* or the *S-Witt ring* $W_S(R)$ on $R \in \mathsf{CUR}_{\mathbb{Z}_S}$ as follows. As a set $W_S(R)$ is just $R^{\mathbb{N}(S)}$. If $x \in W_S(R)$, then we write $x = (x_n)_{n\in\mathbb{N}(S)}$. The addition and multiplication on $W_S(R)$ are defined via transport of structure using the isomorphism of sets $\Phi_S(R) : W_S(R) \to \mathcal{W}_S(R)$, $\Phi_S(R)(x) := \sum_S V_a[x_a]F_a$. In the sequel we identify $W_S(R)$ and $\mathcal{W}_S(R)$ via $\Phi_S(R)$.

3.2 Classically $W(R) := W_{\mathcal{P}}(R)$ is defined by means of the *Witt coordinate (polynomials)* $s_n : R^{\mathbb{N}} \to R$ with $s_n(x) := \sum_{d|n} dx_d^{n/d}$. One then proves that there are unique polynomials $g_{\times,i}(x,y), g_{+,i}(x,y) \in \mathbb{Z}[x_1,...,x_i,y_1,...,y_i]$ for $i \in \mathbb{N}$, giving $g_+(x,y), g_\times(x,y) \in W(\mathbb{Z}[x,y])$ such that

$$s_n(x) + s_n(y) = s_n(g_+(x,y)) \text{ and } s_n(x).s_n(y) = s_n(g_\times(x,y)). \qquad 3.2.1$$

3.3 Notice that in order to prove relations in $W_S(R)$ it is sufficient to prove these relations generically (see 2.10), i.e., it suffices to check these relations in $C_S(\mathcal{A}_{S,\nu})$, where ν is any appropriate set of generic variables. Thus we need only to consider the ghost components. But as $r_m(w\phi) = s_m(w)r_m(\phi), w \in W_S(\mathbb{Z}[\nu]), \phi \in C_S(\mathcal{A}_{S,\nu})$ we may even restrict ourselves to comparing the Witt coordinates.
For example we easily prove relations 3.2.1 as follows. Using lemma 2.26 we see that we have unique polynomials $g_{+,i}(x,y) \in \mathbb{Z}[x_1,...,x_i,y_1,...,y_i]$ such that we have the following relation of operators on $C_S(\mathcal{A}_{S,x,y})$

$$\sum_{S,a} V_a^g[x_a]F_a^g + \sum_{S,a} V_a^g[y_a]F_a^g = \sum_{S,a} V_a^g[g_{+,a}(x,y)]F_a^g.$$

Using lemma 2.16 we analogously prove the statement for $g_\times(x,y)$.

3.4 We will define operators $\mathsf{F}_a, \mathsf{V}_a (a \in \mathbb{N}(S))$ and $[\lambda]_W (\lambda \in R)$ on $W_S(R)$. (We use the sans serif font in order to distinguish the operators on $C_S(H)$ from the operators on $W_S(R)$.) Once again V_a and $[\lambda]_W$ are easily defined. For $w \in W_S(R)$ we define

$$(\mathsf{V}_a(w))_n := w_{n/\!/a} \text{ and } ([\lambda]_W(w))_n := \lambda^n w_n, \qquad 3.4.1$$

or equivalently (consider $W_S(R)$ as subring of $\mathrm{Cart}_S(R)$)

$$\mathsf{V}_a(w) := V_a w F_a \text{ and } [\lambda]_W(w) := [\lambda]w \qquad 3.4.2$$

3.5 From the definitions we see that V_a and $[\lambda]_W$ are additive. As will be clear from definition 3.4.2, the operators $[\lambda]_W$ and $[\lambda]$ are closely related. Therefore we will omit the subscript W and just write $[\lambda], \lambda \in R$ for the operator $[\lambda]_W$ on $W_S(R)$. One immediately checks

$$s_m(\mathsf{V}_a w) = a s_{m/\!/a}(w) \text{ and } s_m([\lambda]_W w) = \lambda^m s_m(w)$$

and

$$\mathsf{V}_a w = \sum\nolimits_S{}_m V_m[w_{m/\!/a}]F_m \in V_a \mathrm{Cart}_S(R). \qquad 3.5.1$$

3.6 Define the *Teichmüller map* $\tau_R = \tau : R \to W_S(R)$ by $\tau(r) := (r, 0, 0, ...)$, or equivalently $\tau(r) := [r]$. Then we have $s_m(\tau(r)) = r^m$. We also find that $w \in W_S(R)$ can uniquely be written as:

$$w = \sum\nolimits_S \mathsf{V}_a \tau(w_a).$$

3.7 We define F_a on $W_S(R)$ by the generic relation in $C_S(\mathcal{A}_{S,w})$ for generic $w = (w_n), n \in \mathbb{N}(S)$:

$$(\mathsf{F}_a w) \heartsuit F_a^g \,\mathsf{Id}_{\mathcal{A}_{S,w}} = F_a^g (w \heartsuit \mathsf{Id}_{\mathcal{A}_{S,w}}). \qquad 3.7.1$$

In order to show that F_a is thus well-defined we use the technique of lemma 2.26. Consider in $C_S(\mathbb{Q} \otimes \mathcal{A}_{S,w})$, for generic $w = (w_i), i \in \mathbb{N}(S)$, the relation:

$$\left(\sum\nolimits_S{}_b V_b^g[\mu_b]F_b^g\right) \circ F_a^g \heartsuit \mathsf{Id}_{\mathcal{A}_{S,w}} = F_a^g \circ \left(\sum\nolimits_S{}_b V_b^g[w_b]F_b^g\right) \heartsuit \mathsf{Id}_{\mathcal{A}_{S,w}}.$$

Suppose we have found $\mu_b \in \mathbb{Z}[w]$ for $b < n, n \in \mathbb{N}(S)$ such that the m-th ghost component of the left hand side is the m-th ghost component of the right hand side for $m < n$. Then write:

$$\left(\sum_{\substack{S\\ b\geq n}} V_b^g[\mu_b]F_b^g\right) \circ F_a^g \heartsuit \mathsf{Id}_{\mathcal{A}_{S,w}} =$$

$$F_a^g \circ \left(\sum_{b}{}_S\, V_b^g[w_b]F_b^g\right) \heartsuit \mathsf{Id}_{\mathcal{A}_{S,w}} - \left(\sum_{\substack{S\\ b<n}} V_b^g[\mu_b]F_b^g\right) \circ F_a^g \heartsuit \mathsf{Id}_{\mathcal{A}_{S,w}}.$$

Comparing the coefficients of t^n on both sides (using observation 2.4), we conclude $\mu_n \in \mathbb{Z}[w]$.

3.8 For the Witt coordinates we find $s_m(\mathsf{F}_a w) = s_{am}(w)$, so we may obtain the relations of lemma 2.16 for $\mathsf{F}_a, \mathsf{V}_a$ and $[\lambda]$. One may also check the following relations in $\mathrm{Cart}_S(R)$ for $w \in W_S(R), r \in R$

$$wV_a = V_a(\mathsf{F}_a w) \text{ and } \mathsf{F}_a\tau(r) = \tau(r^a). \qquad 3.8.1$$

If the characteristic of R is $p > 0$, then we find in $\mathrm{Cart}_S(R)$ for $w \in W_S(R)$

$$pw = V_pF_pw = V_p(\mathsf{F}_p w)F_p = \mathsf{V}_p\mathsf{F}_p w.$$

A final remark: From the defining relation for F_a (3.7.1) one immediately finds $\mathsf{F}_a : W(R) \to W(R)$ to be a ring homomorphism.

A special homomorphism

3.9 An *S-Hilbert ring* R is a $\mathbb{Z}_S$-algebra without additive torsion for which there are endomorphisms $\sigma_n, n \in \mathbb{N}(S)$ such that:

$$\sigma_n\sigma_m = \sigma_{nm},$$
$$\sigma_p \equiv (\,)^p \bmod pR,\ p \in S,$$

(so $\sigma_1 = \mathsf{Id}$).

3.10 Warning: The finiteness of human alphabets and convention have led us to a situation that we now have two meanings for the symbol σ_m. On the one hand it may be a distinguished element of $\mathcal{A}_S$, but it may also be an endomorphism of an S-Hilbert ring.

3.11 Remark. The notion of an S-Hilbert ring should be compared with the notion of a p-Hilbert domain in [Dit89], page 83 (p-Hilbert rings R which are p-complete integral domains where pR is a prime ideal) and the notion of a pre-Hilbert domain in [Hov], page 27 (integral domains R in which p is the only non invertible rational prime and which are equipped with an endomorphism σ such that $\sigma(x) \equiv x^p \bmod pR$). Hilbert rings arise in many places in the literature ([Hon], [Haz], [SPM], etc.) but they have never acquired a name.

3.12 Lemma. *Let R be an S-Hilbert ring and $x \in R$. Then there are unique $\lambda_d(x) \in R$, $d \in \mathbb{N}(s)$, such that $\sum_{d|n} d\lambda_d(x)^{n/d} = \sigma_n(x)$ for all $n \in \mathbb{N}(S)$.*

proof: Let $\lambda_d = \lambda_d(x)$ for $d < m$ be given such that $\sum_{d|n} d\lambda_d^{n/d} = \sigma_n(x)$ for $n < m$, $n, m, d \in \mathbb{N}(S)$. Write $m = p^r u$ with $(p, u) = 1$. Then we first notice that:

$$\sum_{d|m} d\lambda_d^{m/d} = p^r \sum_{d|u} d\lambda_{p^r d}^{u/d} + \sum_{d|p^{r-1}u} d\lambda_d^{m/d}.$$

Secondly

$$\sigma_m(x) = \sigma_p(\sigma_{p^{r-1}u}(x)) = \sum_{d|p^{r-1}u} d\sigma_p(\lambda_d)^{p^{r-1}u/d} \equiv \sum_{d|p^{r-1}u} d\lambda_d^{m/d} \bmod p^r R.$$

We conclude that $\lambda_m \in \mathbb{Z}_{(p)} \otimes R$ for all $p|m$, so $\lambda_m \in R$, since R has no additive S-torsion. □

3.13 Actually the proof of lemma 3.12 implies a little bit more, namely the following slightly generalized version of [Haz], lemma 17.6.1: Let R be an S-Hilbert ring and let $\{x_n | n \in \mathbb{N}(S)\}$ be a series of elements of R such that $\sigma_p(x_n) \equiv x_{pn} \bmod p^{\mathrm{ord}_p(n)+1}$ for $p \in S$. Then there is a unique $x \in W_S(R)$ such that $s_n(x) = x_n$.

3.14 We define a homomorphism $\lambda_S : R \to W_S(R)$ for all S-Hilbert rings R by the relation:

$$s_n \circ \lambda_S = \sigma_n.$$

That λ_S is thus well defined follows from lemma 3.12.

3.15 Using Witt coordinates one easily checks the following relation in $W_S(R)$

$$\mathsf{F}_a \lambda_S(r) = \lambda_S(\sigma_a(r)). \qquad 3.15.1$$

3.16 A trivial example of an S-Hilbert ring is $\mathbb{Z}_S$ under the trivial homomorphisms $\sigma_p = \mathsf{Id}\,, p \in S$. If R is an S-Hilbert ring, the free polynomial ring $R[X_i]_{i \in I}$, for some set I has a *canonical S-Hilbert structure* if we extend σ_q by defining $\sigma_q(X_i) := X_i^q$ $(q \in S, i \in I)$.

3.17 An important example of an S-Hilbert ring is $W_S(R)$ for any $\mathbb{Z}_S$-algebra R, under the homomorphisms $\mathsf{F}_a, a \in \mathbb{N}(S)$. In order to check the condition $\mathsf{F}_p w \equiv w^p \bmod pW_S(R)$ consider $\mathbb{Z}_S[x] := \mathbb{Z}_S[x_i]_{i \in \mathbb{N}(S)}$, for generic x_i, with the canonical Hilbert structure. Let $x = (x_i)_{i \in \mathbb{N}(S)} \in W_S(\mathbb{Z}_S[x])$. Define $c_n := p^{-1}(s_n(\mathsf{F}_p x) - s_n(x)^p)$, $n \in \mathbb{N}(S)$. One easily checks that $c_n \in \mathbb{Z}_S[x]$. Some computations show that the set $\{c_n | n \in \mathbb{N}(S)\}$ satisfies the conditions of 3.13 (see [Haz], 17.6.10) and thus we conclude that $\mathsf{F}_p x - x^p \in pW_S(\mathbb{Z}_S[x])$. Using the functoriality of $W_S(\bullet)$ we are done.

3.18 Remark. There is another notion in the literature which is closely related to that of Hilbert rings: Let $\pi : W(A) \to A$ be the projection on the first coordinate. A ring A is called a *λ-ring* if there is a ring homomorphism $\lambda : A \to W(A)$ such that $\pi \circ \lambda = \mathsf{Id}_A$ and

$$\lambda_{W(A)} \circ \lambda = W(\lambda) \circ \lambda,$$

where $\lambda_{W(A)} : W(A) \to W(W(A))$ is the canonical ring homomorphism corresponding to the Hilbert ring $W(A)$, as we have constructed above. One easily checks that Hilbert rings are λ-rings (without additive torsion). Conversely, if A is a λ-ring without additive torsion, A becomes a Hilbert ring if we define $\sigma_n := \pi \circ \mathsf{F}_n \circ \lambda$, $(n \in \mathbb{N})$. Though this can be found in [Bou], exercise 47 in chapter IX, §1, this does not seem to be widely known. For example in the book [FuL] on λ-rings, there is no reference at all to Witt vectors; Even in [Haz] where both concepts are treated, this specific connection is not mentioned.

The following lemma will be used in chapter III, section 2.

3.19 Lemma. *Let $R \in \mathsf{CUR}$. Denote by $\pi : W_S(R) \to R$ the projection on the first coordinate. The following diagrams commute.*

$$\begin{array}{ccc} R & \xrightarrow{\tau} & W_S(R) \\ {\scriptstyle\tau}\downarrow & i & \downarrow{\scriptstyle\tau} \\ W_S(R) & \xrightarrow[\lambda_S]{} & W_S(W_S(R)) \end{array} \qquad \begin{array}{ccc} R & \xrightarrow{\tau} & W_S(R) \\ {\scriptstyle\tau}\downarrow & ii & \downarrow{\scriptstyle\tau} \\ W_S(R) & \xleftarrow[W_S(\pi)]{} & W_S(W_S(R)) \end{array}$$

$$\begin{array}{ccc} R & \xrightarrow{\tau} & W_S(R) \\ {\scriptstyle\tau}\downarrow & iii & \downarrow{\scriptstyle\lambda_S} \\ W_S(R) & \xleftarrow[W_S(\pi)]{} & W_S(W_S(R)) \end{array} \qquad \begin{array}{ccc} R & \xleftarrow{\pi} & W_S(R) \\ {\scriptstyle\pi}\uparrow & iv & \downarrow{\scriptstyle\lambda_S} \\ W_S(R) & \xleftarrow[W_S(\pi)]{} & W_S(W_S(R)) \end{array}$$

proof: In order to prove relation i we need only consider the Witt coordinates $s_\bullet : W_S(W_S(R)) \to W_S(R)$:

$$s_a(\lambda_S(\tau(r))) = F_a(\tau(r)) = \tau(r^a) = \tau(r)^a = s_a(\tau(\tau(r))).$$

Relation *ii* may be directly checked. Combining relations *i* and *ii* we obtain relation *iii*. Relation *iv* follows from:

$$\pi \circ W_S(\pi) \circ \lambda_S(a) = \pi \circ W_S(\pi)(a, ...) = \pi(\pi(a), ...) = \pi(a).$$

□

We end this section with a small lemma. (Compare with [Haz], 17.6.19 or [Laz], IV.4.13 to appreciate its short proof.)

3.20 Lemma. *If the rational prime p is invertible in R, then it is also invertible in $W_S(R), S := \mathcal{P} \setminus \{p\}$.*

proof: Since p is invertible in R we have a ring homomorphism $\imath : \mathbb{Z}_S \to R$ and therefore by functoriality a ring homomorphism $W(\imath) : W(\mathbb{Z}_S) \to W(R)$. Composing with the ring homomorphism $\lambda_S : \mathbb{Z}_S \to W(\mathbb{Z}_S)$ (indeed $\mathbb{Z}_S$ is an S-Hilbert ring) we obtain a ring homomorphism $\mathbb{Z}_S \to W_S(R)$. □

Hilbert operators

3.21 Let R be an S-Hilbert ring, $H \in \mathbf{cBialg}_R$. The homomorphism $\lambda_S : R \to W_S(R)$ as defined in 3.14, induces another set of operators on $C_S(H)$, the *Hilbert operators* $\{r\}$ for $r \in R$

$$\{r\}\phi := \lambda_S(r) \heartsuit \phi. \qquad 3.21.1$$

The group $C_S(H)$ thus becomes an R-module. Notice that $r_m(\{r\}\phi) = r^{\sigma_m} r_m(\phi)$.

3.22 Let $V_S\mathrm{Cart}_S(R)$ be the right ideal in $\mathrm{Cart}_S(R)$ generated by all $V_p, p \in S$. Then from $\{r\} \equiv [r] \bmod V_S\mathrm{Cart}_S(R)$ we find (using 2.22) that any curve $\psi \in C_S(H)$ can uniquely be written as

$$\psi = \sum_{a \in \mathbb{N}(S)} \sum_{i \in I} V_a\{r_{a,i}\}\phi_i, \quad r_{a,i} \in R,$$

where $\{\pi_t(\phi_i) | i \in I\}$ is a basis for $P(H)$.

3.23 Combining (3.8.1) and (3.15.1) we easily check the following relations in $\mathrm{Cart}_S(R)$

$$F_a\{r\} = \{r^{\sigma_a}\}F_a \text{ and } \{r\}V_a = V_a\{r^{\sigma_a}\}.$$

4 The structure of DPS-Hopf algebras

4.1 Let $H \in \mathsf{DPS-cHopf}_R$, $R \in \mathsf{CUR}$ with structural basis $\{\phi_I | I \in \mathsf{MI}(E)\}$. Write $H^* = R[[X_E]]$, where $< X^\pi, \phi_\kappa >= \delta_{\pi,\kappa}$. Let $\phi_{H,i} = \sum_n \phi_{H,i,n} t^n$ be the i-th canonical curve and define

$$\phi_{H,I} := \prod_{i \in E} \phi_{H,i,I_i} \left(= \prod_{i \in E} \phi_{I_i \epsilon_i} \right).$$

4.2 Lemma. *The set* $\phi_H := \{\phi_{H,I} | I \in \mathsf{MI}(E)\}$ *is another structural basis for* H.

proof: Consider the curve $\phi_{H,i} (i \in E)$ as an element of $\mathsf{Alg}_R(H^*, R[[t_i]]) \subset \mathsf{Alg}_R(H^*, R[[t_E]])$. Then under the product structure on $\mathsf{Alg}_R(H^*, R[[t_E]])$ induced by the comultiplication on H^*, the product $\prod_{i \in E} \phi_{H,i} = \sum_\pi \phi_{H,\pi} t^\pi \in H[[t_E]]$ may be considered as an algebra morphism $H^* \to R[[t_E]]$ determined by

$$\left(\prod_{i \in E} \phi_{H,i} \right) (X_j) := \sum_{\pi \in \mathsf{MI}(E)} < \phi_{H,\pi}, X_j > t^\pi,$$

for $j \in E$. Then

$$\left(\prod_{i \in E} \phi_{H,i} \right) (X^\kappa) = \prod_{e \in E} \left(\prod_{i \in E} \phi_{H,i} (X_e) \right)^{\kappa_e} \equiv t^\kappa \bmod R\{t^\pi | \, |\pi| > |\kappa|\}.$$

(Indeed: $(\prod_{i \in E} \phi_{H,i})(X_e) = (1 + \sum_{i \in E} \phi_{H,i} t_i + ...)(X_e) = t_e + ...$) This gives $\phi_{H,\pi}(X^\kappa) = \delta_{\pi,\kappa}$ for $|\pi| \leq |\kappa|$, which means

$$\phi_{H,\pi} = \phi_\pi + \sum_{|\tau| < |\pi|} c_\tau \phi_\tau,$$

for some $c_\tau \in R$. So the set $\{\phi_{H,\pi} | \pi \in \mathsf{MI}(E)\}$ is an R-module basis for H. One easily checks that the basis $\{\phi_{H,\pi} | \pi \in \mathsf{MI}(E)\}$ is structural, i.e., that

$$\Delta \phi_{H,\pi} = \sum_{\tau + \kappa = \pi} \phi_{H,\tau} \otimes \phi_{H,\kappa}.$$

□

4.3 A structural basis $\{\phi_I | I \in \mathsf{MI}(E)\}$ for a DPS-Hopf algebra H will be called *curvilinear* if $\phi_I = \phi_{H,I}$. Thus lemma 4.2 says that every DPS-Hopf algebra admits a curvilinear structural basis.

4.4 Corollary. *The functor* $C(\bullet) : \mathsf{DPS-cHopf}_R \to \mathsf{Mod}_{\mathrm{Cart}(R)}$ *is faithful.*

proof: Let $H \in \mathsf{DPS{-}cHopf}_R$ with curvilinear structural basis $\{\phi_I | I \in \mathsf{MI}(E)\}$. Then $f \in \mathsf{DPS{-}cHopf}_R(H, H')$ is completely determined by the set of all $f(\phi_{m\epsilon_i})$, $m \in \mathbb{N}, i \in E$, or equivalently by $C(f)\phi_{H,i}, i \in E$. □

4.5 Lemma. *Let $\psi = \{\psi_i | i \in E\}$ be any fundamental set of curves for $H \in \mathsf{DPS{-}cHopf}_R$. Then there are $Y_e \in H^*, e \in E$ such that $H^* = R[[Y_E]]$ and $\psi_i(Y_e) = \delta_{i,e}t$.*

proof: Write $\phi_{i,1} = \sum_j M_{i,j}\psi_{i,1}$. Define $Y_{2,i} := \sum_j M_{j,i}X_j$, then one easily computes that $\psi_i(Y_{2,j}) \equiv \delta_{i,j}t \bmod t^2$. So assume we have $Y_{m,i} \in H^*$ such that $\psi_i(Y_{m,j}) \equiv \delta_{i,j}t + c_{i,j}t^m \bmod t^{m+1}$. Define $Y_{m+1,i} := Y_{m,i} - \sum_j c_{j,i}Y_{m,j}^m$. Then one finds that $\psi_i(Y_{m+1,j}) \equiv \delta_{i,j}t \bmod t^{m+1}$. Thus $Y_i := \lim_m Y_{m,i}$ satisfies the conditions of the lemma. □

4.6 Remark. The Y_e in the above lemma are far from unique. Suppose $\{Y_e | e \in E\}$ satisfies the conditions of the lemma. If $Y'_{e_1} := Y_{e_1} + Y_{e_1}Y_{e_2}, Y'_i := Y_i (i \neq e_1)$, then also $\{Y'_e | e \in E\}$ satisfies the conditions of the lemma.
Combining lemmas 4.2 and 4.5 we obtain the following corollary.

4.7 Corollary. *Let $H \in \mathsf{DPS{-}cHopf}_R$ and let $\{\psi_i | i \in E\}$ be a fundamental set of curves. Then H admits a curvilinear structural basis $\{\psi_I | I \in \mathsf{MI}(E)\}$ such that the i-th canonical curve $\psi_{H,i}$ equals ψ_i.* □

The case when R has no additive torsion

4.8 Let $H \in \mathsf{DPS{-}cHopf}_R$, $R \in \mathsf{CUR}$ without additive torsion and assume H has a curvilinear structural basis $\{\phi_I | I \in \mathsf{MI}(E)\}$. Let $\#E = d$. We write $\partial_j := \phi_{H,j,1} = \phi_{\epsilon_j}$ and the i-th canonical curve $\phi_{H,i}$ as

$$\phi_{H,i} = exp\left(\sum_{m=0}^{\infty} \frac{\sum_{j=1}^{d} r_{m,i,j}\partial_j}{m} t^m\right).$$

Write $H^* = R[[X_E]]$, with $< \phi_I, X^\beta >= \delta_{I,\beta}$.

4.9 We will show that the algebra structure of H (or equivalently the coalgebra structure on H^*) is completely determined by the set of all $r_{m,i,j}$.
We proceed as follows: Notice that $\{\partial^\alpha := \prod_i \partial_i^{\alpha_i} | \alpha \in \mathsf{MI}(E)\}$ is a basis for $H_{\mathbb{Q}}$. (Indeed one immediately computes $\phi_\alpha \equiv \partial^\alpha/\alpha! \bmod \mathbb{Q}\{\partial^\beta || \beta| < |\alpha|\}$. Here we have used the curvilinearity.) So we may write

$$\phi_\alpha = \sum_u P_{\alpha,u}\partial^u \text{ and } \partial^u = \sum_\alpha Q_{u,\alpha}\phi_\alpha,$$

where $P_{\alpha,u}, Q_{u,\alpha}$ are rational numbers which depend only on the $r_{m,i,j}$. But then

$$< \phi_\alpha\phi_\beta, X_i >=< \sum_{u,v} P_{\alpha,u}P_{\beta,v}\delta^{u+v}, X_i >= \sum_{u,v} P_{\alpha,u}P_{\beta,v} < \sum_{\gamma} Q_{u+v,\gamma}\phi_\gamma, X_i >=$$

$$= \sum_{u,v} P_{\alpha,u}P_{\beta,v}Q_{u+v,\epsilon_i} =: G_i(\alpha,\beta),$$

or equivalently

$$\Delta X_i = \sum_{\alpha,\beta\in \mathsf{MI}(E)} G_i(\alpha,\beta)X^\alpha \otimes X^\beta.$$

4.10 A curvilinear structural basis $\{\phi_I | I \in \mathsf{MI}(E)\}$ for $H \in \mathsf{DPS{-}cHopf}_R$ ($R \in \mathsf{CUR}$) is called *additive* if

$$\phi_\alpha.\phi_\beta = \binom{\alpha+\beta}{\alpha}\phi_{\alpha+\beta},$$

or equivalently $\Delta X_i = X_i \otimes 1 + 1 \otimes X_i$. (Indeed

$$< \phi_\alpha\phi_\beta, X_\gamma >= \binom{\alpha+\beta}{\alpha}\delta_{\alpha+\beta,\gamma} =< \phi_\alpha \otimes \phi_\beta, \prod_i (X_i \otimes 1 + 1 \otimes X_i)^{\gamma_i} > \quad .)$$

If R has no additive torsion, then the canonical curves corresponding to an additive structural basis can be written as $\phi_{H,i} = exp(\phi_{\epsilon_i}t), i \in E$.

4.11 Proposition. (Q-theorem) *If R is a $\mathbb{Q}$-algebra, then a DPS-Hopf algebra H over R admits an additive curvilinear structural basis.*

proof: The set $\{\psi_i := exp(\partial_i t)\}$ is a fundamental set of curves in $C(H)$ for which we have

$$\psi_\alpha.\psi_\beta = \frac{\partial^\alpha\partial^\beta}{\alpha!\beta!} = \binom{\alpha+\beta}{\alpha}\psi_{\alpha+\beta}.$$

□

4.12 Describing the explicit bialgebra isomorphism of H^* corresponding to the change of structural basis in proposition 4.11 is more involved. We claim that $Y_i = \sum_{m,j} \frac{r_{m,j,i}}{m} X_j^m$ satisfies $\Delta Y_i = Y_i \otimes 1 + 1 \otimes Y_i$.
In order to prove the claim we proceed as follows: One easily sees that $f \in \mathsf{Alg}_R(H^*, R[[t_E, t'_E]])$ can be written as

$$f = \sum_\alpha \phi_\alpha \prod_i f(X_i)^{\alpha_i} = exp\left(\sum_{m\geq 1, i,j\in E} \frac{r_{m,i,j}\partial_j}{m} f(X_i)^m\right). \qquad 4.12.1$$

Let Φ be the R-algebra isomorphism $\Phi : R[[X_E]]\hat{\otimes}R[[X_E]] \cong R[[t_E, t'_E]]$. Consider ϕ_i as an element of $\mathsf{Alg}_R(H^*, R[[t_i]])$. We write ϕ'_i for ϕ_i when considered as an

element of $\mathsf{Alg}_R(H^*, R[[t_i']])$. The set $\mathsf{Alg}_R(H^*, R[[t_E, t_E']])$ has a group structure induced by the comultiplication on H^*, or equivalently by the multiplication on $H[[t_E, t_E']]$. The product $\prod\phi\prod\phi' := \prod_{i\in E}\phi_i\prod_{i\in E}\phi_i' \in \mathsf{Alg}_R(H^*, R[[t_E, t_E']])$ may be written as

$$\prod\phi\prod\phi' = exp\left(\sum_{m,i,j}\left(\frac{r_{m,i,j}\partial_j}{m}t_i^m + \frac{r_{m,i,j}\partial_j}{m}t_i'^m\right)\right).$$

Therefore

$$< \prod\phi\prod\phi', X_l >= exp\left(\sum_{m,i}\left(\frac{r_{m,i,l}}{m}t_i^m + \frac{r_{m,i,l}}{m}t_i'^m\right)\right). \qquad 4.12.2$$

On the other hand

$$< \prod\phi\prod\phi', X_l >= \sum_{\alpha,\beta\in\mathsf{MI}(E)} < \phi_\alpha.\phi_\beta', X_l > t^\alpha t'^\beta = \Phi(\Delta(X_l)).$$

But then, using 4.12.1

$$< \prod\phi\prod\phi', X_l >= exp\left(\sum_{m,i}\frac{r_{m,i,l}}{m}\Phi(\Delta(X_l))^m\right). \qquad 4.12.3$$

Thus comparing (4.12.2) and (4.12.3) we find $\Phi(\Delta(Y_i)) = \Phi(Y_i\otimes 1) + \Phi(1\otimes Y_i)$, which proves the claim.

4.13 Remark. We have just proven that any choice of $r_m = (r_{m,i,j})_{i,j\in E} \in M_d(R), m \in \mathbb{N}$, completely determines a DPS-Hopf algebra H over $\mathbb{Q}\otimes R$, provided R has no additive torsion.

S-typification of DPS-Hopf algebras

4.14 Let $R \in \mathsf{CUR}$ and let S^* be a set of invertible rational primes in R. Let S be the complement of S^* in $\mathcal{P}$. Notice that by lemma 3.20 we have for $p \in S^*$ that $p^{-1} \in \mathrm{Cart}(R)$. So we may define $P_S := \prod_{p\in S^*}(1 - \frac{1}{p}V_pF_p) \in \mathrm{Cart}(R)$.

4.15 A structural basis for a DPS-Hopf algebra is called *S-typical* if the canonical curves are S-typical.

4.16 Proposition. *A DPS-Hopf algebra over R admits an S-typical curvilinear structural basis.*

proof: The set $\{P_S(\phi_{H,i})\}$ is a fundamental set of S-typical curves in $C(H)$. □

4.17 Corollary. *The group of curves $C(H)$, $H \in \mathsf{DPS-cHopf}_R$, $R \in \mathsf{CUR}_{\mathbb{Z}_S}$ can be described as*

$$C(H) \cong C_S(H)^{\mathbb{N}^{(S^*)}}.$$

proof: The isomorphism Φ is given by

$$\Phi(\phi) := (P_S F_n \phi)_{n \in \mathbb{N}(S^*)} \quad \left(\text{and } \Phi^{-1}(\phi_n)_{n \in \mathbb{N}(S^*)} := \sum_{n \in \mathbb{N}(S^*)} n^{-1} V^n \phi_n \right). \qquad \square$$

4.18 Corollary. *Let $R \in \mathsf{CUR}_{\mathbb{Z}_S}$. The functor*

$$C_S(\bullet) : \mathsf{DPS{-}cHopf}_R \to \mathrm{mod}_{\mathrm{Cart}_S(R)}$$

is faithful.

proof: Let $\{\phi_I | I \in \mathsf{MI}(E)\}$ be an S-typical curvilinear structural basis for $H \in \mathsf{DPS{-}cHopf}_R$. Then $f \in \mathsf{DPS{-}cHopf}_R(H, H')$ is fully determined by the S-typical curves $C(f)\phi_{H,i}$ $(i \in E)$. $\square$

Height and jump sequence in positive characteristic

4.19 For the remainder of this section we assume either that R is a perfect field of characteristic $p > 0$, or that R is a p-Hilbert ring on which $\sigma := \sigma_p$ is an automorphism. Let $H \in \mathsf{DPS{-}cHopf}_R$ have dimension d. Everything will be p-typical, thus we denote $W(R) := W_p(R), F := F_p, V := V_p$ and $C(H) := C_p(H)$.

4.20 We define the *height* h of $H \in \mathsf{DPS{-}cHopf}_R$ as follows: If $C(H)$ is not a free $W(R)$-module, then we say that $h := \infty$. If $C(H)$ is a free $W(R)$-module, then we define

$$h := \mathrm{rank}_{W(R)} C(H) = \mathrm{rank}_R C(H) \Big/ (\mathsf{V}W(R))\, C(H) \,.$$

In the special case that $R = k$, a perfect field of characteristic $p > 0$ we may even write $h = \dim_k C(H)/pC(H)$.

4.21 Let M be a finitely generated $W(R)$-module. We denote by $\mathrm{mg}_{W(R)}(M)$ the minimum number of generators of M.

4.22 Define for $i \geq 0$

$$R_i := \mathrm{mg}_{W(R)} C(H) \Big/ V^{i+1} C(H) - \mathrm{mg}_{W(R)} C(H) \Big/ V^i C(H) \,.$$

Thus in particular R_0 is the dimension d of H and $R_i \leq d$ $(i \geq 0)$.

4.23 Lemma. *Let H have finite height. Then F is injective, the operators F and V commute and the sequence $(R_i)_{i \geq 0}$ is decreasing.*

proof: Note that $C(H)$ is a free $W(R)$-module implies that F is injective: $F\psi = 0$ gives that $VF\psi = 0$. Thus we see from $F(VF - FV) = 0$ that $FV = VF$.
One easily checks that $V^{i_0+1}\phi_{j_0} \in W(R)\{V^i\phi_{H,j} \mid i \leq i_0, 1 \leq j \leq d\}$, implies that $V^{i_0+2}\phi_{j_0} \in W(R)\{V^{i_j}\phi_{H,j} \mid i_j \leq i_0 + 1 \text{ for } j \neq j_0, i_{j_0} \leq i_0, 1 \leq j \leq d\}$. Thus with an easy induction we find that the sequence $(R_i)_{i\geq 0}$ is decreasing. □

4.24 We now define the *jump sequence* $(h_i; r_i)_{i\geq 1}$ of $H \in \mathsf{DPS{-}cHopf}_R$, H with finite height as follows: Let h_1 be the smallest number $i \geq 0$ such that $R_{i+1} < R_i$. Write $r_1 := R_{h_1} - R_{h_1+1}$. We inductively define h_j as the smallest number $i > 0$ such that

$$r_j := R_{\sum_{k=1}^{j-1} h_k + i} - R_{\sum_{k=1}^{j-1} h_k + i + 1} > 0.$$

4.25 We give an easy example: Let $H \in \mathsf{DPS{-}cHopf}_R$ be 1-dimensional with curvilinear p-typical structural basis ϕ such that $F\phi_{H,1} = V\phi_{H,1} + V^3\phi_{H,1}$. Then one easily computes that $R_0 = R_1 = 1$, $R_i = 0$ for $i \geq 2$. Thus the jump sequence of H is $(1, 1)$.
We have the following easy lemma connecting the jump sequence with the height.

4.26 Lemma. *Let $H \in \mathsf{DPS{-}cHopf}_R$ with height $h < \infty$. Then H has jump sequence $(h_i; r_i)_{1\leq i\leq \gamma}$ if and only if the $W(R)$-module $C(H)$ has a basis*

$$\left\{ V^{j_l}\phi_{i_l} \;\middle|\; 0 \leq l < \gamma, 0 \leq j_l \leq \sum_{k=1}^{l+1} h_k, \sum_{k=1}^{l} r_k < i_l \leq \sum_{k=1}^{l+1} r_k \right\}.$$

We then also have the relations

$$d = \sum_{i=1}^{\gamma} r_i \quad \text{and } h = \sum_{i=1}^{\gamma} r_i \left(1 + \sum_{j=1}^{i} h_j\right). \qquad \square$$

4.27 Remark. We have the following corollary to chapter III, theorem 2.14 and theorem 5.17:

Corollary. *Let R be a local p-Hilbert domain and $H \in \mathsf{DPS{-}cHopf}_R$. Let F be injective, then the $W(R)$-rank of $C(H)$ is finite, or equivalently, H has finite height.*

The proof can be sketched as follows:
Assume that R is a local p-Hilbert domain and that F is injective on $C(H)$. Denote $T := FV - VF$. Then $FT = 0$, which implies that $T = 0$. We now use chapter III, theorem 2.14 to conclude that F is injective on $C(\pi^*(H))$. Thus the height of $\pi^*(H)$ is finite, and its jump-sequence is well defined. By chapter III, theorem 5.17

however, we know that the jump sequence of H is the jump sequence of $\pi^*(H)$ and thus (using lemma 4.26) we have that the height of H is finite.
The author believes that a direct proof of this corollary may be used together with chapter III, theorem 2.14 to give another (more elegant) proof of our main result, chapter III, theorem 5.17.

5 Commutative formal group laws

In this section we will translate our results obtained in the context of DPS-Hopf algebras into the terminology of the theory of commutative formal group laws. As corollaries we will rediscover some of the classical results of commutative formal group theory.

5.1 A *formal group law* of dimension d defined over a ring R is a d-tuple $G = (G_i), 1 \leq i \leq d$ of formal power series $G_i \in R[[X_1, ..., X_d, Y_1, ..., Y_d]]$ such that

$$G(0, Y) = Y \text{ and } G(X, 0) = X,$$

$$G(X, G(Y, Z)) = G(G(X, Y), Z).$$

A formal group law is called *commutative* if

$$G(X, Y) = G(Y, X).$$

5.2 A homomorphism f between a d-dimensional formal group law G and an n-dimensional formal group law H is by definition an n-tuple of power series $f_i \in R[[X_1, ..., X_d]]$ such that $f(0) = 0$ and

$$f(G(X, Y)) = H(f(X), f(Y)).$$

We denote the category of (d-dimensional) commutative formal group laws defined over R by $\mathsf{CFGL}_R^{(d)}$. An isomorphism f is called a *strong* isomorphism if $f_i \equiv X_i \bmod \deg 2$, otherwise it is called *weak*. The isomorphism f is called *specially weak* if $f_i = \sum_j a_{i,j} X_j$.
The following proposition can be found in [Fro], Chapter I, §3, proposition 1.

5.3 Proposition. *Let G be a d-dimensional commutative formal group law. Then there is a unique d-tuple of power series $I_i \in R[[X_1, ..., X_n]]$ such that $G(I, X) = 0$.*
□

5.4 We associate with $G \in \mathsf{CFGL}_R^d$ a topological Hopf algebra, denoted $\Theta(G)$, and called the *contravariant bialgebra* of G. As topological algebra $\Theta(G)$ is defined as

$R[[X_1, ..., X_d]]$ equipped with the X-adic topology. The comultiplication on $\Theta(G)$ is defined by $\Delta(X_i) := G_i(X \otimes 1, 1 \otimes X)$ and the counit is defined by $\epsilon(X_i) := 0$. Using proposition 5.3 we find that the antipode is given by $\gamma(X_i) = I_i$.
If $f : G \to H$ is a homomorphism of formal group laws, then we denote by $\Theta(f) : \Theta(H) \to \Theta(G)$ the induced homomorphism of Hopf algebras.

5.5 Proposition. *(Dieudonné) The category* CFGL_R *is anti-equivalent to the category* $\mathsf{smooth{-}cHopf}_R$. □

5.6 We now define the *covariant bialgebra*, denoted $U(G)$, of G as the topological dual of $\Theta(G)$. As we have remarked in 1.18, $U(G)$ is a DPS-Hopf algebra over R. We denote the canonical structural basis constructed in proposition 1.17 as $\phi_G = \{\phi_{G,I} | I \in \mathsf{MI}(E)\}$. We then have canonical curves $\phi_{G,i} = 1 + \sum_{n \geq 1} \phi_{G,i,n} t^n$.
If $f : G \to H$ is a homomorphism of formal group laws, then we denote by $U(f) : U(H) \to U(G)$ the induced homomorphism of Hopf algebras.

5.7 Proposition. *The category* CFGL_R *is equivalent to* $\mathsf{DPS{-}cHopf}_R$. *Especially an isomorphism f of commutative formal group laws corresponds to a change of structural basis for $U(G)$. Moreover $f : G \to H$ is a strong isomorphism if and only if $\phi_{G,i,1} = \phi_{G,\epsilon_i} = U(f)(\phi_{H,i,1}), 1 \leq i \leq d$. The isomorphism f is specially weak if $U(f)(\phi_H) = [\Lambda]\phi_G$ for some $\Lambda \in Gl_d(R)$.* □

5.8 If $H \in \mathsf{DPS{-}cHopf}_R$ we denote by G_H the commutative formal group law such that $U(G_H) = H$. We may now prove the second part of remark 1.14: For a DPS-bialgebra H we have that the dual H^* has an antipode, as we already observed, and thus $H = (H^*)^{*c}$ is a DPS-Hopf algebra.
We now give some lemmas which show that the terminology we have defined in the context of DPS-Hopf algebras corresponds to the terminology as used in the theory of commutative formal groups.

5.9 Lemma. *The commutative formal group law G is curvilinear if and only if the covariant bialgebra $U(G)$ is curvilinear.*

proof: For $I, J \in \mathsf{MI}(E)$ denote as IJ the multi-index obtained by entrywise multiplication. Write $G_i(X, Y) = \sum a^{(i)}_{I,J} X^I Y^J$, then the definition of curvilinearity given in [Haz], 12.1 reads as follows: G is curvilinear if $IJ = 0, ||I||, ||J|| \geq 1$ implies $a^{(i)}_{I,J} = 0 (1 \leq i \leq d)$.
Now assume that $U(G)$ has a curvilinear basis $\{\phi_I | I \in \mathsf{MI}(E)\}$, thus $IJ = 0$, $||I||, ||J|| \geq 1$ implies $\phi_{I+J} = \phi_I \phi_J$. Then

$$0 = < \phi_I \phi_J, X_i > = < \phi_I \otimes \phi_J, \Delta X_i > = a^{(i)}_{I,J},$$

thus G is curvilinear. The proof of the converse statement is left to the reader. □

5.10 Lemma. *The commutative formal group law G is S-typical if and only if the covariant bialgebra $U(G)$ is S-typical.*

proof: Corollary 4.17 is exactly definition IV.7.4 of [Laz]. □

5.11 Let k be a perfect field of characteristic $p > 0$. The height of a commutative formal group law over k is defined in [Haz], definition 18.3.8. That this definition is equivalent to ours is proven in [Haz], corollary 28.2.9.

5.12 Define the d-dimensional *additive formal group law* $\hat{G}_a$ by the d-tuple of power series $\hat{G}_a = (\hat{G}_{a,i})$ where

$$\hat{G}_{a,i} := X_i + Y_i \qquad (1 \leq i \leq d).$$

5.13 Lemma. *The commutative formal group law G is additive if and only if the covariant bialgebra $U(G)$ is additive.* □

As corollaries we now may obtain the following classical results.

5.14 Corollary. *(to lemma 4.2) Any commutative formal group law is strongly isomorphic to a curvilinear one.* □

5.15 Corollary. *(to proposition 4.16) Any commutative formal group law defined over a $\mathbb{Z}_S$-algebra is strongly isomorphic to an S-typical one.* □

5.16 Corollary. *(to proposition 4.11) All commutative formal group laws defined over a $\mathbb{Q}$-algebra are isomorphic to an additive formal group law.* □

The isomorphism $\log_G : G \to \hat{G}_a$ of corollary 5.16 is called the *logarithm* of G. From section 4.12 we now find the "first transition theorem" of [Dit90], pg 255.

5.17 Corollary. *Let R have no additive torsion, $G \in \mathsf{CFGL}_R$, G curvilinear. Write the canonical curves as*

$$\phi_{G,i} = exp\left(\sum_{m\geq 1, j\in E} \frac{r_{m,i,j}\partial_j}{m} t^m\right),$$

then $\log_G = \sum_{m\geq 1} m^{-1} r_m^{\mathrm{T}} X^m$, where, as usual, $r_m = (r_{m,i,j})_{i,j}$. □

5.18 We give another standard example. Define the d-dimensional *multiplicative formal group law* $\hat{G}_m$ over $R \in \mathsf{CUR}$ by the d-tuple of power series $\hat{G}_m = (\hat{G}_{m,i})$

$$\hat{G}_{m,i} := X_i + Y_i + X_i Y_i \qquad (1 \leq i \leq d).$$

If R has no additive torsion, then the logarithm of $\hat{G}_m$ is $\sum_m m^{-1}X^m$. Thus by corollary 5.17 we find that the canonical curves are

$$\phi_{\hat{G}_m,i} = exp\left(\sum_{m\geq 1} m^{-1}\partial_i t^m\right).$$

Chapter 2

F-types, universal DPS-Hopf algebras and the Lazard ring

1 Introduction

1.1 In this chapter $d = \#E$ will be a fixed natural number.

1.2 Let $H \in \mathsf{DPS-cHopf}_R, R \in \mathsf{CUR}_{\mathbb{Z}_S}$ with curvilinear structural basis $\{\phi_I | I \in \mathsf{MI}(E)\}, \#E = d$. Then in $C_S(H)$ we may write for $i \in E, a \in \mathbb{N}(S)$

$$F_a\phi_{H,i} = \sum_{l \in \mathbb{N}(S)} V_l \left(\sum_{j \in E} [\lambda_{a,l,i,j}] \phi_{H,j} \right),$$

for some unique $\lambda_{a,l,i,j} \in R$. We will write this as

$$F_a\phi_H = \textstyle\sum_{S,l} V_l[\lambda_{a,l}]\phi_H, \tag{1.2.1}$$

where $\lambda_{a,l} = (\lambda_{a,l,i,j})_{i,j \in E} \in M_d(R)$. We will call this expression the *Witt F_a-type* of H (with respect to ϕ_H).

1.3 Moreover if R is an S-Hilbert ring we analogously define the *Hilbert F_a-type* of H (with respect to ϕ_H) by

$$F_a\phi_H = \textstyle\sum_{S,l} V_l\{\mu_{a,l}\}\phi_H, \tag{1.3.1}$$

for some unique $\mu_{a,l} \in M_d(R)$.

1.4 As an example we will give the F-types of the additive and multiplicative formal group laws. From chapter I, subsection 4.10 we see that $F_a\phi_{\hat{G}_a} = 0$, while from chapter I, subsection 5.18 we see that $F_a\phi_{\hat{G}_m} = \phi_{\hat{G}_m}$.

1.5 We will show (Theorem 4.5) that the F_a-types (Witt or, if they exist, Hilbert) completely determine the algebra structure of H and that this algebra structure

is defined over $\mathbb{Z}[\lambda_{a,l,i,j}](a, l \in \mathbb{N}(S), i, j \in E)$. In the special case that R has no additive torsion and $S = \mathcal{P}$ this statement for Witt F-types is easily seen to be equivalent to [Haz], 27.4.15, the entwined function theorem.

1.6 For any ring R let D_R denote a (small) subcategory of $\mathsf{DPS{-}cHopf}_R$, such that for any homomorphism $f : R \to R'$ and any $H \in \mathsf{D}_R$ the induced $f_*(H) \in \mathsf{D}_{R'}$. We call H^U_{D} defined over the ring L_{D} *universal* (for D) if for any $H \in \mathsf{D}_R$ there is a unique ring homomorphism $\Phi : L_{\mathsf{D}} \to R$ such that $\Phi_*(H^U_{\mathsf{D}}) = H$. (This is equivalent to the statement that the functor $\mathcal{D} : \mathsf{CUR} \to \mathsf{Set}$, sending the ring R to the set D_R, is representable). For background on universal arrows and representability, see for example [MaL], chapter III.

1.7 Let $\mathcal{F} : \mathsf{CUR} \to \mathsf{Set}$ denote the functor which assigns to a ring R the set of all d-dimensional curvilinear commutative formal group laws defined over R. It is a well known result of Lazard that $\mathcal{F}$ is representable by a free polynomial ring L, called the *ring of Lazard* or the *Lazard ring.* Proofs can be found in [Haz], chapter II and in [Laz55]. Lazard's proof is direct but, to quote [Haz], E.1.3, "the proof is exceedingly tough and computational". The proof of Hazewinkel is based on arithmetic properties of the coefficients of the generic logarithm, using his functional equation lemma. We present a third proof here, based on the construction of a universal curvilinear DPS-Hopf algebra H^U.

1.8 In the last three sections we give connections between the F-types of our theory, the theory of Hilbert and Witt functions of Ditters [Dit90], the special elements of Honda [Hon], §§2 and 3 and the theory of Dieudonné as exposed in his book [Dieu]. In the last section we also prove a lemma which enables us to compute the isogeny type for p-typical commutative formal group laws defined over an algebraically closed field of positive characteristic p from the F_p-type.

1.9 As a matter of notation: if $\lambda = (\lambda_{i,j})_{i,j} \in M_d(R)$, then we denote by $\lambda^{(m)}$ the matrix $(\lambda^m_{i,j})_{i,j}$. Analogously if σ is an endomorphism of R, then we denote by λ^σ the matrix $(\lambda^\sigma_{i,j})_{i,j}$. If R is a ring and λ a matrix, then we denote by $R[\lambda]$ the R-algebra generated by the entries of λ. The notions $\mathcal{A}_S$, a_n, E_n and σ_n $(n \in \mathbb{N})$ of chapter I, subsections 1.10 and 1.11, will remain in force.

2 The p-typical case

In this section we will construct $H^U_{d,p}$, the universal d-dimensional p-typical curvilinear DPS-Hopf algebra and its ring of definition $\mathbb{Z}_{(p)}[\Lambda_p]$.

2.1 Lemma. *Let $H \in \mathsf{DPS{-}cHopf}_R, R \in \mathsf{CUR}_{\mathbb{Z}_S}$, R without additive torsion. Let H have Witt F-types as in 1.2.1 or, if R is an S-Hilbert ring, Hilbert F-types as*

in 1.3.1. Then the algebra structure of H is completely determined by the set of all F_p-types with respect to an S-typical curvilinear structural basis for H ($p \in S$). Moreover, write the canonical curves as in chapter I, 4.8

$$\phi_{H,i} = exp\left(\sum_{m\in\mathbb{N}(S)} \frac{\sum_j r_{m,i,j}\partial_j}{m} t^m\right).$$

Then the following formula holds for the matrices of the Witt F-types

$$r_{qm} = \sum_{d|m} d\lambda_{q,d}^{(m/d)} r_{m/d}, \qquad 2.1.1$$

while for the matrices of the Hilbert F-types we have

$$r_{qm} = \sum_{d|m} d\mu_{q,d}^{\sigma_{m/d}} r_{m/d}, \qquad 2.1.2$$

$q, m \in \mathbb{N}(S), q > 1$. If $V \subset \mathbb{N}(S)^2$ is any set such that $f : V \to \mathbb{N}(S)$ defined by $(u,v) \mapsto uv$ is a bijection, then $\mathbb{Q}[r_m]_{m\in\mathbb{N}(S)} = \mathbb{Q}[\lambda_{u,v}]_{(u,v)\in V} = \mathbb{Q}[\mu_{u,v}]_{(u,v)\in V}$

proof: We will only prove the statements for the Witt F-types since the statements for the Hilbert F-types are proven in the same manner.
Let $\{\phi_I | I \in \mathsf{MI}(E)\}$ be an S-typical curvilinear structural basis for H (chapter I, proposition 4.16). We have seen (chapter I, 4.9) that the set of all $r_{m,i,j}, m \in \mathbb{N}(S), i,j \in E$ completely determines the algebra structure of H. Now consider for $i \in E$ and $q \in \mathbb{N}(S)$

$$F_q\phi_{H,i} = exp\left(\sum_{m,S} \frac{\sum_j r_{qm,i,j}\partial_j}{m} t^m\right) = \sum_{l,S} V_l\left(\sum_{j\in E} [\lambda_{q,l,i,j}]\phi_{H,j}\right).$$

Comparing ghost components we find ($i \in E$)

$$\sum_{j,S} r_{qm,i,j}\partial_j = \sum_{d|m, j\in E} \left(d\lambda_{q,d,i,j}^{m/d} \sum_{l\in E} r_{m/d,j,l}\partial_l \right).$$

If we write this in terms of matrices, then we have found formula 2.1.1.
From formula 2.1.1 we inductively find that $\mathbb{Q}[\Lambda_S] = \mathbb{Q}[r_{m,i,j}]_{m\in\mathbb{N}(S),i,j\in E}$ and thus the set of all $\lambda_{q,m}, q, m \in \mathbb{N}(S)$ also completely determines the algebra structure of H. The third statement also follows directly from formula (2.1.1). □

2.2 Notice that the lemma implies that the restriction of the functor $\mathcal{F}$ to the full subcategory $\mathsf{CUR}_{\mathbb{Q}}$ is represented by $\mathbb{Q}[\lambda_{u,v}]_{(u,v)\in V}$ or by $\mathbb{Q}[\mu_{u,v}]_{(u,v)\in V}$, for any V as in the lemma.

2.3 For the remainder of this section we assume that we are in the p-typical context. We will therefore use "logarithmic" notations; indices of the form p^i will be replaced by i. Precise definitions follow, of course.

2.4 Let $\lambda_{a,n,i,j}, a, n \in \mathbb{N}(\{p\}), a > 1, i, j \in E$ be generic variables. Denote by Λ_p the set of all $\lambda_{a,l,i,j}, a, l \in \mathbb{N}(\{p\}), a > 1, i, j \in E$.

2.5 We will define $H_p^U := H_{d,p}^U$ as a curvilinear p-typical DPS-Hopf algebra over $\mathbb{Z}_{(p)}[\Lambda_p]$. As a set H_p^U is defined by

$$H_p^U := \mathbb{Z}_{(p)}[\Lambda_p][\mathsf{a}_{i,m}]_{1 \leq i \leq d, m \geq 0}.$$

The comultiplication is defined by the condition that that $f_i : \mathcal{A}_p \to \mathbb{Z}_{(p)}[\mathsf{a}_{i,m}]_{m \geq 0}$, $f_i(\mathsf{a}_{p^n}) := \mathsf{a}_{i,n}$ is a surjection of bialgebras for all $1 \leq i \leq d$. The algebra structure is then defined by demanding that the F_p-type of H_p^U is given by

$$F_p \phi_{H_p^U} = \sum V_p^i[\lambda_i] \phi_{H_p^U}.$$

Write $E_{i,n} := f_i(E_n)$. Then a structural basis for H_p^U is given by the set $E := \{E_\pi := \prod_i E_{i,\pi_i} | \pi \in \mathsf{MI}(E)\}$. The canonical curves are p-typical by definition, therefore H_p^U is indeed a curvilinear p-typical DPS-Hopf algebra. Since $\mathbb{Z}_{(p)}[\Lambda_p]$ has no additive torsion, we know by lemma 2.1 (and chapter I, remark 4.13) that the F_p-type determines the algebra structure of $\mathbb{Q} \otimes H_p^U$. A priori, the algebra structure is defined over $\mathbb{Q}[\Lambda_p]$, however, the following theorem asserts that H_p^U is indeed defined over $\mathbb{Z}_{(p)}[\Lambda_p]$.

2.6 Theorem. *The DPS-Hopf algebra H_p^U is actually defined over $\mathbb{Z}_{(p)}[\Lambda_p]$ and thus H_p^U is the universal d-dimensional p-typical curvilinear DPS-Hopf algebra.*

proof: In the proof we denote $H := H_p^U$, $\sigma_{j,i} := f_j(\sigma_{p^i})$, and a the set of all $\mathsf{a}_{i,m}, 1 \leq i \leq d, m \in \mathbb{N}$.

We have to show that the algebra structure of H is defined over $\mathbb{Z}_{(p)}[\Lambda_p]$, i.e., that $E_{i,n} E_{i,m} \in \mathbb{Z}_{(p)}[\Lambda_p]\{E_\pi | \pi \in \mathsf{MI}(E)\}$.

We proceed in several steps.

Step 1: First we define a filtration $\mathcal{B} = \{\mathcal{B}_i | i \geq 0\}$ on H. For a monomial $\prod_i \mathsf{a}_{j_i,n_i}^{b_i}$ we define its weight $\| \prod_i \mathsf{a}_{j_i,n_i}^{b_i} \|$ as $\sum_i b_i p^{n_i}$. We extend this to polynomials $P \in \mathbb{Z}_{(p)}[\Lambda_p][\mathsf{a}]$ by defining the weight $\|P\|$ of P to be the maximum of the weight of its terms. A polynomial is called isobaric if the weights of all its terms are equal. Now define

$$\mathcal{B}_i := \{P \in \mathbb{Z}_{(p)}[\Lambda_p][\mathsf{a}] \,\big|\, \|P\| \leq i\}.$$

So, for example, $\mathcal{B}_0 = \mathbb{Z}_{(p)}[\Lambda_p]$ and $\mathcal{B}_1 = \mathbb{Z}_{(p)}[\Lambda_p]\{1, \mathsf{a}_{j,0}\}_j$.

Step 2: As a second step, we will prove

$$\mathsf{a}_{j,i}^p \equiv px\mathsf{a}_{j,i+1} \bmod \mathcal{B}_{p^{i+1}-1}, \qquad 2.6.1$$

for some $x \in \mathbb{Z}_{(p)}$ depending on $\mathsf{a}_{j,i}$.
For this, consider the coefficient of t^{p^i} in $F_p\phi_{H,j}$. This is the coefficient of $t^{p^{i+1}}$ in $V_pF_p\phi_{H,j}$. We have to distinguish two cases: the case $i = 0$ and the case $i \geq 1$.
—*the case* $i = 0$: We have

$$V_pF_p\phi_{H,j} = exp\left(\sum\nolimits_{n\geq 0}\frac{p\sigma_{j,n+1}}{p^{n+1}}t^{p^{n+1}}\right) = 1 + \sigma_{j,1}t^p + \ldots .$$

So the coefficient of t^p is $\sigma_{j,1}$. But then from considering the coefficient of t^p in the relation

$$\sum_n E_{j,n}t^n = exp\left(\sum_n \frac{\sigma_{j,n}}{p^n}t^{p^n}\right),$$

we find

$$E_{j,p} = \mathsf{a}_{j,1} = \frac{\sigma_{j,1}}{p} + \frac{\sigma_{j,0}^p}{p!} \Leftrightarrow \sigma_{j,1} = p\mathsf{a}_{j,1} - \frac{\mathsf{a}_{j,0}^p}{(p-1)!}.$$

Thus we have found that the coefficient of t in $F_p\phi_{H,j}$ is $p\mathsf{a}_{j,1} - (p-1)!^{-1}\mathsf{a}_{j,0}^p$.
—*the case* $i \geq 1$: From the relation for ghost components $r_m(V_pF_p\phi) = pr_m(\phi)$ for $m > 1$, $r_1(V_pF_p\phi) = 0$, we see

$$\begin{aligned} V_pF_p\phi_{H,j} &= p\phi_{H,j} - exp\,(p\mathsf{a}_{j,0}t)\,. \\ &= \left(\sum\nolimits_{n\geq 0}E_{j,n}t^n\right)^p \Big/ \sum\nolimits_{n\geq 0}\frac{(p\mathsf{a}_{j,0}t)^n}{n!}. \end{aligned}$$

(Notice the change from the additive notation for the group structure of curves to the multiplicative notation for multiplication of power series.) Thus the coefficient of t^{p^i} in $F_p\phi_{H,j}$ is

$$\mathsf{a}_{j,i}^p + p\mathsf{a}_{j,i+1} + P(\mathsf{a}_{j,0}, \ldots, \mathsf{a}_{j,i}),$$

where P is a polynomial of weight p^{i+1} in $p\mathbb{Z}_{(p)}[\mathsf{a}_{j,0}, \ldots, \mathsf{a}_{j,i}]$ which does not contain a term $\mathsf{a}_{j,i}^p$. Note that because of weight considerations every monomial of weight p^{i+1} in P contains a p-th power of some $\mathsf{a}_{j,l}$ $(l < i)$. We may thus use induction on i to conclude that the coefficient of t^{p^i} in $F_p\phi_{H,j}$ can be written as

$$(1 + px')\mathsf{a}_{j,i}^p + p\mathsf{a}_{j,i+1} + P'(\mathsf{a}_{j,0}, \ldots, \mathsf{a}_{j,i}),$$

where P' is a polynomial of weight less than p^{i+1} in $p\mathbb{Z}_{(p)}[\mathsf{a}_{j,0}, \ldots, \mathsf{a}_{j,i}]$ and $x' \in \mathbb{Z}_{(p)}$. But on the other hand, from the defining relation $F_p\phi_H = \sum V_p^i[\lambda_i]\phi_H$, we have that the coefficient of t^{p^i} in $F_p\phi_{H,j}$ is an polynomial P'' with $\|P''\| \leq p^i$ in $\mathbb{Z}_{(p)}[\Lambda_p][\mathsf{a}]$, so $P'' \in \mathcal{B}_{p^i}$.
Comparing the two expressions for the coefficients of t^{p^i} in $F_p\phi_{H,j}$ we find the claim (2.6.1).

Step 3: Notice that any isobaric polynomial $P \in \mathbb{Z}_{(p)}[\mathsf{a}_{j,\bullet}]$ of weight n may be uniquely written as follows: Let $n = \sum b_i p^i$ be the p-adic expansion of n and let c be the coefficient of $\prod_i \mathsf{a}_{j,i}^{b_i}$ in P. Then it follows from (2.6.1) that

$$P \equiv (c + px) \prod_i \mathsf{a}_{j,i}^{b_i} \bmod \mathcal{B}_{n-1},$$

for some $x \in \mathbb{Z}_{(p)}$ which depends on P.

Step 4: Let $n \in \mathbb{N}$ have p-adic expansion $n = \sum b_i p^i$. We now will prove

$$E_{j,n} \equiv \left((\prod_i b_i!)^{-1} + px_n \right) \prod \mathsf{a}_{j,i}^{b_i} \bmod \mathcal{B}_{n-1}, \qquad 2.6.2$$

for some $x_n \in \mathbb{Z}_{(p)}$ depending on n. This follows from inspection of the relation $\sum E_{j,n} t^n = exp\left(\sum \sigma_{j,i} p^{-i} t^{p^i}\right)$ in $\mathbb{Q}[\sigma_{j,l}]_{l \geq 1}$:

1^o $\quad E_{j,p^i} = \mathsf{a}_{j,i} \equiv p^{-i} \sigma_{j,i} \bmod \mathbb{Q}[\sigma_{j,l}]_{l<i}$,

2^o $\quad E_{j,n} \equiv (\prod_i b_i!)^{-1} \left(p^{-i} \sigma_{j,i}\right)^{b_i}$ modulo the ideal generated by $\sigma_{j,l}^p, l < n$.

Thus we obtain, using step 3, the claim (2.6.2), indeed $E_{j,n}$ is an isobaric polynomial of weight n in $\mathbb{Z}_{(p)}[\mathsf{a}_{j,\bullet}]$ (chapter I, lemma 1.12).

Step 5: We now easily prove the first part of the theorem. Consider the isobaric polynomial $E_{j,n}E_{j,m} \in \mathbb{Z}_{(p)}[\mathsf{a}_{j,\bullet}]$ and let the p-adic expansion of $n+m$ be $n+m = \sum b_i p^i$. Then using step 3 and (2.6.2) we have

$$E_{j,n}E_{j,m} \equiv x \prod_i \mathsf{a}_{j,i}^{b_i} \equiv x \left((\prod_i b_i!)^{-1} + px_{n+m} \right)^{-1} E_{j,n+m} \bmod \mathcal{B}_{m+n-1},$$

for some $x \in \mathbb{Z}_{(p)}$. Continuing with an easy induction, we have proven the first statement of the theorem.

For the second statement: Let B be any d-dimensional Hopf algebra with curvilinear p-typical structural basis $\{\phi_I | I \in \mathsf{MI}(E)\}$ and write the Witt F_p-type of B as $F_p\phi_B = \sum_{\{p\}} V_p^i[\mu_i]\phi_B$. Then $B = \Phi^*(H)$, where the ring homomorphism Φ is defined by $\Phi(\lambda_{p,p^i,k,l}) := \mu_{i,k,l}$, $a, b \in E$. □

2.7 Notice that if R is an S-Hilbert ring with endomorphisms $\sigma_n, n \in \mathbb{N}(S)$ and $r \in R$ is such that $\sigma_p(r) = r^p, p \in S$, then $\lambda_S(r) = \tau(r) \in W_S(R)$. So if we give $\mathbb{Z}_{(p)}[\Lambda_p]$ the canonical p-Hilbert structure by putting $\sigma_p(\lambda_{p,m,i,j}) := \lambda_{p,m,i,j}^p$, then we find that for H_p^U the Witt F_p-type equals the Hilbert F_p-type.

3 The case R is a $\mathbb{Z}_{(p)}$-algebra

Let p be some fixed but otherwise arbitrary $p \in \mathcal{P}$. In this section we construct $H_d^U(p)$, the universal d-dimensional curvilinear DPS-Hopf algebra for DPS-Hopf algebras over $\mathbb{Z}_{(p)}$-algebras and its ring of definition $L(p)$.

3.1 Define a set $\Lambda(p)$ of generic variables by

$$\Lambda(p) := \{\lambda_{p,p^l,i,j}, \lambda_{n,p^l,i,j} | l \geq 0, n > 1, \gcd(n,p) = 1, i,j \in E\}.$$

Let $L(p)$ be the $\mathbb{Z}_{(p)}$-algebra

$$L(p) := \mathbb{Z}_{(p)}[\Lambda(p)].$$

endowed with the canonical $\mathcal{P}$-Hilbert structure, i.e., $\lambda^{\sigma_q} = \lambda^q$ for $\lambda \in \Lambda(p), q \in \mathcal{P}$ (see chapter I, 3.16).

3.2 For $\lambda_{a,l,i,j} \in \Lambda(p)$, let $\|\lambda_{a,l,i,j}\| := al$ be its weight. Extend this to a weight function on $\mathbb{Z}[\Lambda(p)]$ by putting $\|\lambda\mu\| := \max\{\|\lambda\|, \|\mu\|\}$ and $\|\lambda + \mu\| := \max\{\|\lambda\|, \|\mu\|\}$. We define a filtration $\mathcal{F}il(\Lambda(p)) := \{\mathcal{F}il_i | i \geq 1\}$ on $\mathbb{Z}[\Lambda(p)]$ by

$$\mathcal{F}il_i := \{x \in \mathbb{Z}[\Lambda(p)] | \, \|x\| \leq i\}.$$

(We consider $\mathcal{F}il(\Lambda(p))$ also as an filtration on $M_d(\mathbb{Z}[\Lambda(p)])$ defined entrywise, thus $\mathcal{F}il_i := \{M \in M_d(\mathbb{Z}[\Lambda(p)]) | \, \|M_{k,l}\| \leq i, k,j \in E\}$).

3.3 Let $\lambda_{1,1} := \mathsf{Id}_d$ and $\lambda_{1,n} := 0$ for $n > 1$. Define $\lambda_{a,n,i,j} \in \mathbb{Z}_{(p)}[\Lambda(p)]$ $(a,n \in \mathbb{N}, a > 1, i,j \in E)$ inductively by the (matrix) relations

$$\lambda_{pb,n} = \sum_{d:d|n, d \notin p\mathbb{N}} \lambda_{b,d}^{\sigma_{pn/d}} \lambda_{p,n/d} + p\lambda_{b,pn} \qquad 3.3.1$$

and

$$\lambda_{b,qn} = q^{-1}\lambda_{qb,n} - q^{-1} \sum_{d:d|n, d \notin p\mathbb{N}} \lambda_{b,d}^{\sigma_{qn/d}} \lambda_{q,n/d}, \qquad 3.3.2$$

where $b > 1$ and $q \in \mathcal{P}$ with $\gcd(p,q) = 1$. Notice that these relations imply the following congruences $\lambda_{pb,n} \equiv p\lambda_{b,pn} \bmod \mathcal{F}il_{bpn-1}$ and $\lambda_{b,qn} \equiv q^{-1}\lambda_{qb,n} \bmod \mathcal{F}il_{bqn-1}$, so this is a well-defined inductive process.

3.4 Let a be the set of all $\mathsf{a}_{i,n}, i \in E, n \in \mathbb{N}$. We now define $H^U(p) := H_d^U(p)$ as the curvilinear DPS-Hopf algebra over $\mathbb{Z}_{(p)}[\Lambda(p)]$:

$$H^U(p) := \mathbb{Z}_{(p)}[\Lambda(p)][\mathsf{a}]$$

such that $f_i : \mathcal{A} \to \mathbb{Z}_{(p)}[\mathsf{a}_{i,n}]_{n \geq 0}$, $f_i(\mathsf{a}_n) := \mathsf{a}_{i,n}$ is a homomorphism of bialgebras for all $1 \leq i \leq d$. Then $\{\mathsf{a}_\pi | \pi \in \mathsf{MI}(E)\}$, were $\mathsf{a}_\pi := \prod_i \mathsf{a}_{i,\pi_i}$ is a curvilinear structural basis for $H^U(p)$. We now define the Hilbert F-types of $H^U(p)$ with respect to this structural basis to be

$$F_a \phi_{H^U(p)} = \sum_{n \geq 1} V_n\{\lambda_{a,n}\} \phi_{H^U(p)}, a \in \mathbb{N}.$$

Using lemma 2.1 we know that the F-types completely determine the algebra structure of $\mathbb{Q}\otimes H^U(p)$. We have to check however whether the F-types are well-defined, since the coefficients can not be chosen independently (as was the case in the previous section). But on the one hand relations 3.3.1 and 3.3.2 express the equalities $F_{pb} = F_p \circ F_b$ and $F_{qb} = F_q \circ F_b$ (here we fundamentally use the Hilbert structure). While on the other hand by the third part of lemma 2.1 we have that all $\lambda_{a,n} \in \Lambda(p)$ can be chosen independently (since the $r_m, m \in \mathbb{N}$ can be chosen so).
The following theorem states that the algebra structure which is again a priori defined only over $\mathbb{Q}[\Lambda(p)]$, is actually defined over the ring $\mathbb{Z}_{(p)}[\Lambda(p)]$.

3.5 Theorem. *The curvilinear DPS-Hopf algebra $H^U(p)$ is defined over the ring $\mathbb{Z}_{(p)}[\Lambda(p)]$ and thus $H^U(p)$ is the universal d-dimensional curvilinear DPS-Hopf algebra for DPS-Hopf algebras over $\mathbb{Z}_{(p)}$-algebras.*

proof: Define a new p-typical curvilinear structural basis for $H^U(p)$ by the fundamental set of curves ($i \in E$)

$$\psi_i := \prod_{q\in\mathcal{P}\setminus\{p\}} (1 - q^{-1}V_qF_q)\phi_{H^U(p),i}, \tag{3.5.1}$$

(as in chapter I, proposition 4.16) and let the corresponding F_p-type be

$$F_p\psi = \sum_{i\geq 0} V_p^i\{\mu_i\}\psi. \tag{3.5.2}$$

Then from substituting 3.5.1 in 3.5.2 we find the following relation

$$F_p \prod_{q\in\mathcal{P}\setminus\{p\}} (1 - q^{-1}V_qF_q)\phi_{H^U(p)} = \sum_{i\geq 0} V_p^i\{\mu_i\} \prod_{q\in\mathcal{P}\setminus\{p\}} (1 - q^{-1}V_qF_q)\phi_{H^U(p)}.$$

We therefore see that all $\mu_{i,l,k} \in L(p)$ and thus by theorem 2.6 we conclude that the DPS-Hopf algebra $H^U(p)$ is defined over $\mathbb{Z}_{(p)}[\mu_i]_{i\geq 0} \subset L(p)$.
For the second part of the theorem, let the Witt F-types of $H^U(p)$ be given by

$$F_a\phi_{H^U(p)} = \sum_{n\geq 1} V_n[\nu_{a,n}]\phi_{H^U(p)}.$$

Then from $\{r\} \equiv [r] \bmod V_{\mathcal{P}}\mathrm{Cart}(\mathbb{Z}[r])$ (chapter I, 3.22), we find

$$\nu_{a,n} \equiv \lambda_{a,n} \bmod \mathcal{F}il_{an-1}.$$

Indeed write $[\nu_{a,n}] = \{\nu_{a,n}\} + \sum_{l>1} V_l\{\nu_{a,n,l}\}$, $\nu_{a,n,l} \in M_d(\mathbb{Z}[\nu_{a,n}])$. Then we find from comparing the F_a-types that $\lambda_{a,n} = \nu_{a,n} + \sum_{l|m,l>1} \nu_{a,n/l,l}$. Thus we conclude that $L(p) = \mathbb{Z}_{(p)}[\nu_{a,n,i,j}], a, n \in \mathbb{N}, i, j \in E$. Now for any DPS-Hopf algebra B defined over a $\mathbb{Z}_{(p)}$-algebra R with Witt F-types

$$F_a\phi_B = \sum_{n\geq 0} V_n[\gamma_{a,n}]\phi_B,$$

we have that $B = \Phi_*(H^U(p))$, where the ring homomorphism $\Phi : L(p) \to R$ is defined by $\Phi(\nu_{a,n}) := \gamma_{a,n}$. □

4 The general case; the ring of Lazard

In this section we will construct H_d^U, the universal d-dimensional curvilinear DPS-Hopf algebra and its ring of definition L, the ring of Lazard. This will be done by constructing generators for $L(p)$, $p \in \mathcal{P}$ with the property that they are elements of $\mathbb{Z}[\Lambda]$ and are independent of p. These generators then will turn out to be generators for L.
The notations of the preceding section will remain in force throughout this section.

4.1 Define for $q \in \mathcal{P}, r \in \mathbb{N}$

$$\xi_{q^r} := \lambda_{q,q^{r-1}}.$$

If $n \in \mathbb{N}$ is composite (i.e., n is not a power of a rational prime), let $\text{Decom}\,(n) := \{(u,v)|uv = n, 1 < u\}$. Since n is composite we have that

$$\gcd\{u|(u,v) \in \text{Decom}\,(n)\} = 1,$$

or equivalently there are integers r_u such that

$$\sum_{(u,v)\in\text{Decom}\,(n)} r_u u = 1.$$

Now define

$$\xi_n := \sum_{(u,v)\in\text{Decom}\,(n)} r_u \lambda_{u,v}.$$

4.2 Lemma. *The set of all $\xi_m, m > 1$ is a set of algebraically independent generators for the $\mathbb{Z}_{(p)}$-algebra $L(p)$.*

proof: Fix $p \in \mathcal{P}$ and denote by o_p the p-adic valuation on $\mathbb{N}$. For a natural number $n > 1$ we let the p-adic decomposition of n be $n = p^{o_p(n)}n'$ (so $\gcd(n', p) = 1$). Then we see from the relations 3.3.1 and 3.3.2 that for composite $n \in \mathbb{N}$

$$\begin{aligned}\xi_n &\equiv \sum_{(u,v)\in\text{Decom}\,(n)} r_u p^{o_p(u)} v'^{-1} \lambda_{n',p^{o_p(n)}} \bmod \mathcal{F}il_{n-1} \\ &\equiv \sum_{(u,v)\in\text{Decom}\,(n)} \frac{r_u u p^{o_p(n)}}{n} \lambda_{n',p^{o_p(n)}} \equiv n'^{-1}\lambda_{n',p^{o_p(n)}} \bmod \mathcal{F}il_{n-1}.\end{aligned}$$

If $n = q^r, q \in \mathcal{P}, q \neq p$, then

$$\xi_n = \lambda_{q,q^{r-1}} \equiv q^{1-r}\lambda_{q^r,1} \bmod \mathcal{F}il_{q^r-1},$$

while if $n = p^r$ then, of course, $\xi_n = \lambda_{p,p^{r-1}} \in \Lambda(p)$. So indeed the set of all $\xi_n, n > 1$ is a set of algebraically independent generators for $L(p)$. □

4.3 We may now define L, the ring of Lazard . Let J denote the ideal in $\mathbb{Z}[\Lambda]$ generated by relations 3.3.1 for all $p \in \mathcal{P}$. Denote by J^+ the torsion closure of J, i.e.,

$$J^+ := \{x \in \mathbb{Z}[\Lambda] \mid mx \in J \text{ for some } m \in \mathbb{N}\}.$$

Then let

$$L := \mathbb{Z}[\Lambda] / J^+ .$$

Clearly L has no additive torsion, so we have an imbedding $L \hookrightarrow \mathbb{Z}_{(p)} \otimes L$. We conclude by lemma 4.2 that $L = \cap_p \mathbb{Z}_{(p)} \otimes L = \cap_p \mathbb{Z}_{(p)}[\xi] = \mathbb{Z}[\xi]$. We call L the *ring of Lazard.* The polynomial ring L becomes a $\mathcal{P}$-Hilbert ring under the canonical Hilbert structure.

4.4 Let $\mathsf{a} := \{\mathsf{a}_{i,n} \mid i \leq d, n \in \mathbb{N}\}$. We define $H^U := H^U_d$ as a DPS-Hopf algebra over L by

$$H^U := L[\mathsf{a}],$$

such that $f_i : \mathcal{A} \to H^U$ defined by $f_i(\mathsf{a}_n) := \mathsf{a}_{i,n}$ is a homomorphism of bialgebras. The algebra structure is given by the Hilbert F-types

$$F_a \phi_{H^U} = \sum_{n \geq 1} V_n \{\lambda_{a,n}\} \phi_{H^U}.$$

As in 3.4 we have that H^U will be well-defined provided that we prove the following theorem.

4.5 Theorem. *The curvilinear DPS-Hopf algebra H^U is defined over L and thus H^U is the universal d-dimensional curvilinear DPS-Hopf algebra.*

proof: By theorem 3.5 we have that $\mathbb{Z}_{(p)} \otimes H^U$ is defined over $\mathbb{Z}_{(p)} \otimes L$ for all $p \in \mathcal{P}$ and thus H^U is defined over L.
The second part of the theorem is proven in exactly the same way as the second part of theorem 3.5. □

We may translate these results into the terminology of commutative formal group laws:

4.6 Theorem. *The functor $\mathcal{F}$ is represented by the polynomial ring L. Furthermore every curvilinear commutative formal group law is defined over the ring of coefficients of its F-types (Witt or, if they exist, Hilbert).* □

5 Hilbert functions and Witt functions

In this section we connect the theory of F-types with the the theory of Hilbert functions and Witt functions as presented in [Dit90].

5.1 Let $R \in \mathsf{CUR}_{\mathbb{Z}_S}$ and let $H \in \mathsf{DPS{-}cHopf}_R$ with curvilinear S-typical structural basis $\phi = \{\phi_I | I \in \mathsf{MI}(E)\}, \#E = d$. Write the canonical curves as in lemma 2.1. Then we define a map $gh_H := gh_{H,\phi} : \mathbb{N}(S) \to M_d(R)$ by $gh_H(n) := r_n(\phi_H) = (r_{n,i,j})_{i,j}$. As we have seen, in the case that R has no additive torsion gh_H is closely related to the logarithm of G_H (chapter I, corollary 5.17).

5.2 Let $F_{S,R}$ be the set of all functions $f : \mathbb{N}(S) \to M_d(R)$. We give $F_{S,R}$ the topology induced by the valuation v which is defined as follows: $v(f)$ is the smallest $n \in \mathbb{N}$ such that $f(n) \neq 0$. Define for any function $f \in F_{S,R}$ the following operators:
— V_a by $V_a f(n) := af(n/\!\!/a)$ (where $f(n/\!\!/a) := f(n/a)$ if $a|n$ and 0 otherwise),
— F_a by $F_a f(n) := f(an)$,
— $[\lambda]$, for $\lambda \in M_d(R)$ by $[\lambda]f(n) := \lambda^{(n)} f(n)$.
Moreover if R is an S-Hilbert ring we also define
— $\{\lambda\}$, for $\lambda \in M_d(R)$ by $\{\lambda\}f(n) := \lambda^{\sigma_n} f(n)$.
Thus $F_{S,R}$ becomes a $\mathrm{Cart}_S(R)$-module.

5.3 Now if R has no additive torsion we have by theorem 4.5 that H is completely determined by the expressions ($q \in \mathbb{N}(S)$)

$$F_q gh_H = \sum_S V_a[\lambda_{q,a}] gh_H \qquad 5.3.1$$

($\lambda_{q,a} \in M_d(R)$) since these expressions are equivalent to the expressions

$$F_q \phi_H = \sum_S V_a[\lambda_{q,a}] \phi_H.$$

Indeed since R has no additive torsion, the ghost components completely describe any curve in $C_S(H)$. We also have seen in theorem 4.5 that H is defined over $\mathbb{Z}[\lambda_{q,a,i,j}], q, a \in \mathbb{N}(S), i, j \in E$. If $\psi_H := \sum_S V_a[\lambda_a]\phi_H$, $\lambda_a \in M_d(R), \lambda_1 \in Gl_d(R)$ defines another S-typical curvilinear basis ψ for H, then we find from considering the ghost components the relation

$$gh_{H,\psi} = \sum_S V_a[\lambda_a] gh_{H,\phi}.$$

Moreover if R is an S-Hilbert ring we have analogous statements involving the Hilbert operators $\{\bullet\}$.

5.4 More generally, we call a function $f \in F_{S,R}$ with $f(1) = \mathsf{Id}$ an *S-Witt function* defined over R if

$$F_a f = \sum_S V_d[\lambda_{a,d}] f,$$

where $\lambda_{a,d} \in M_d(R)$. Analogously we define *S-Hilbert functions.* Thus corresponding to any Witt or Hilbert function f there is a DPS-Hopf algebra H_f with structural basis ϕ_f. If we define for an S-Witt function f (respectively an S-Hilbert function g)

$$W_{S,R}(f) := \{\textstyle\sum_S V_a[\lambda_a]f | \lambda_a \in M_d(R)\}$$

(respectively

$$H_{S,R}(g) := \{\textstyle\sum_S V_a\{\lambda_a\}g | \lambda_a \in M_d(R)\})$$

then we rediscover the "theorem of the ghost map" ([Dit90], pg 255) and the corollary in loc. cit. on page 256. We will reformulate them as:

5.5 Proposition. *Let the $\mathbb{Z}_S$-algebra R have no additive torsion. Let $H \in \mathsf{DPS{-}cHopf}_R$ with S-typical curvilinear structural basis $\phi = \{\phi_I | I \in \mathsf{MI}(E)\}$. Then $gh_{H,\phi}$ is an S-Witt function over R and we have an isomorphism of $\mathrm{Cart}_S(R)$-modules $C_S(H) \cong W_{S,R}(gh_{H,\phi})$ by taking ghost components. Let ψ be another S-typical curvilinear structural basis for $\mathbb{Q} \otimes H$. Then ψ is a structural basis for H if and only if $W_{S,R}(gh_{H,\phi}) = W_{S,R}(gh_{H,\psi})$, or equivalently if and only if*

$$gh_{H,\psi}(am) = \sum_{d|m} d\mu_{a,d}^{(m/d)} gh_{H,\phi}(m/d),$$

for unique $\mu_{a,d} \in M_d(R), a, d \in \mathbb{N}(S)$.
If R is an S-Hilbert ring we have an analogous statement. □

The following proposition will be used in chapter IV ("second transition theorem", loc. cit. pg 264).

5.6 Proposition. *Let R be a p-Hilbert ring and let $H \in \mathsf{DPS{-}cHopf}_R$ with p-typical curvilinear basis ϕ. Write the F_p-type of ϕ_H as $F_p gh_{H,\phi} = \sum_{i\geq 0} V_{p^i}\{c_i\}gh_{H,\phi}$. Let ψ be the p-typical curvilinear basis induced by $\psi_H := \sum_{i\geq 0} V_{p^i}\{\lambda_i\}\phi_H$ ($\lambda_i \in M_d(R), \lambda_0 \in Gl_d(R)$). Then for all $m \geq 0$ we have that $g = gh_{H,\psi}$ is a solution of*

$$g(p^{m+1}) - \sum_{j=0}^{m} p^j g(p^{m-j})^{\sigma^{1+j}} c_j = p^{m+1}\lambda_{m+1} \text{ and } g(1) = \lambda_0 \in Gl_d(R). \qquad 5.6.1$$

Conversely if $g : \mathbb{N}(p) \to M_d(R)$ is a solution of the equations 5.6.1 for some $\lambda_i \in M_d(R)$, then $\psi_H := \sum_{i\geq 0} V_{p^i}\{\lambda_i\}\phi_H$ induces another p-typical curvilinear basis ψ for H, for which we have that $gh_{H,\psi} = g$.

proof: A proof using "generic F-type calculation" is given in [Dit90]. We sketch a straightforward proof using induction. One easily checks that $g(1) = \lambda_0$ and $g(p) = p\lambda_1 + \lambda_0 c_0$. Thus equation (5.6.1) holds for $m = 0$.

Assume that $gh_{H,\psi}$ is a solution of 5.6.1 for all $m < n$. Then write

$$p^{n+1}\lambda_{n+1} = gh_{H,\psi}(p^{n+1}) - \sum_{j=0}^{n} p^j \lambda_j^{\sigma^{n+1-j}} gh_{H,\phi}(p^{n+1-j}).$$

Now we may "push this equation down", by using the relations $p^j\lambda_j = gh_{H,\psi}(p^j) - \sum_{l=0}^{j-1} p^l \lambda_l^{\sigma^{j-l}} gh_{H,\phi}(p^{j-l})$ and $gh_{H,\phi}(p^{n-j+1}) = \sum_{i=0}^{n-j} p^i c_i^{\sigma^{n-j-i}} gh_{H,\phi}(p^{n-j-i})$.
Expanding and using the inductive hypothesis we find eventually that $gh_{H,\psi}$ is a solution for 5.6.1 for $m = n$.
Conversely, assume that g is a solution of 5.6.1 for all $m \geq 0$. Then by the first part of the theorem, $gh_{H,\psi}$ is also a solution of 5.6.1. Using induction, one proves that $g = gh_{H,\psi}$. □

6 Connections with the theory of Honda

In this section we discuss a connection between the Hilbert F_p-type of a p-typical curvilinear commutative formal group law defined over a p-Hilbert ring R in which pR is maximal, and Honda's special element for such formal group laws.

6.1 We briefly recall the notations and some of the results of [Hon], §§2 and 3. Let R be a discrete valuation ring having field of fractions K. Let $\wp = (\pi)$ be the maximal ideal of R. Assume the residue field to have characteristic $p > 0$ and also assume that there is an endomorphism σ of K and a power of q of p such that $\sigma(x) \equiv x^q \bmod p$ for $x \in R$. Define $K_\sigma[[T]]$ as the noncommutative power series ring on T with multiplication rule $Tx = x^\sigma T$ $(x \in K)$. We analogously define $R_\sigma[[T]]$. Denote by $A_{m,n}$ the ring of all $m \times n$ matrices over $R_\sigma[[T]]$. Let $X = (X_1, ..., X_n)^{\mathrm{T}}$ and let $K[[X]]_0^m$ be the set of all $f = (f_i)_{1\leq i\leq m}$ with $f_i \in K[[X_i]]_{1\leq i\leq m}$ such that $f_i(0) = 0$ $(1 \leq i \leq m)$. Define an operation $* : A_{m,n} \times K[[X]]_0^n \to K[[X]]_0^m$ by

$$u * f = (\sum_{i\geq 0} C_i T^i) * (f_1, ..., f_n)^{\mathrm{T}} := \sum_{i\geq 0} C_i f^{\sigma^i}(X^{q^i}).$$

An element $u \in A_{n,n}$ is called *special* if $u \equiv \pi \mathsf{Id}_n \bmod \deg 1$. We say that $f \in K[[X]]_0^n$ is *killed by u modulo* $\wp$ if $u * f \in \wp[[X]]_0^n$. If $P \in Gl_n(R)$ and u is special, then $f \in K[[X]]_0^n$ has *type* (P, u) if f is killed by u and $f \equiv PX \bmod \deg 2$.
We then have the following proposition, cf. [Hon], theorem 2 and proposition 3.3.

6.2 Proposition. *If f has type (P, u), then $G_f := f^{-1}(f(X)+f(Y))$ is a commutative formal group law defined over R. Let g be of type (Q, u) (with $Q \in Gl_n(R)$). Then $G_g := g^{-1}(g(X) + g(Y))$ is a commutative formal group law which is weakly isomorphic to G_f. If $P = Q$, then G_g and G_f are strongly isomorphic.*

Moreover in the unramified case, i.e., $\pi = p$, we have that for any commutative formal group law G over R with logarithm $\log_G$ there is a special element u which kills $\log_G$. □

The connection with F_p-types is now given by the following proposition. (Using the notations of section 2.6.)

6.3 Proposition. *Let R be a p-Hilbert ring such that pR is maximal. Let $u = \sum_{i\geq 0} C_i T^i$ be a special element (so $C_0 = p\,\mathsf{Id}$). Write $u^{-1} = \sum_{i\geq 0} B_i T^i$ (so $B_0 = p^{-1}$). Then $\log_G(X) := \sum_{i\geq 0} pB_i X^{(p^i)}$ is the logarithm of a curvilinear commutative formal group law G having F_p-type*

$$F_p\phi_G = \sum_{i\geq 0} V_p^i\{-C_{i+1}^{\mathrm{T}}\}\phi_G.$$

The power series $h = \sum_{i\geq 0} h_i X^{p^i}$ has type (Id, u) if and only if the curvilinear p-typical commutative formal group law H having logarithm h is weakly isomorphic to G, i.e., if and only if the function $gh_H : n \mapsto p^n h_n$ is an element of $H_{\{p\},R}(gh_G)$.

proof: Consider

$$u^{-1}u = 1 \Leftrightarrow \sum_{i=0}^{m} B_{m-i}C_{i+1}^{\sigma^{m-i}} = -pB_{m+1} \quad (m \geq 0)$$

$$\Leftrightarrow p^{m+1}pB_{m+1}^{\mathrm{T}} = -\sum_{i=0}^{m} p^i C_{i+1}^{\mathrm{T}\sigma^{m-i}}(p^{m-i}pB_{m-i}^{\mathrm{T}}) \quad (m \geq 0).$$

Thus from chapter I, corollary 5.17 and formula 2.1.2 we obtain the first part of the proposition. The second part now follows from proposition 5.5. □

7 Connections with the theory of Dieudonné

In this section we describe some connections between the theory we have developed so far and the theory of Dieudonné.

7.1 We briefly recall some of the notations and results of [Dieu], chapter III, §§4 and 5. Let k be a perfect field of characteristic $p > 0$, and let $W := W(k)$. By σ we denote the endomorphism F_p we constructed in chapter I, 3.7.1. Since k is perfect we have that σ is invertible on W. The ring W is a complete valuation ring under the p-adic valuation o_p. We define A, the *Hilbert-Witt ring*, as the W-module of power series $a = \sum_{i\geq 0} a_i T^i$ with multiplication rule $Ta = a^\sigma T$. The ring R will be A localized with respect to T. The automorphism σ is extended to R by defining $\sigma(T) := T$. A right A-module M is called *distinguished* if it is finitely generated

and satisfies the conditions $Mp \subset MT$ and $m \mapsto mT$ is injective on M. The *rank* of a distinguished module is the dimension of the k-vector space M/MT. Then we have [Dieu], chapter III, §4, proposition 7.

7.2 Proposition. *The A-module M is distinguished of rank d if and only if M is isomorphic to a quotient $A^d/u(A^d)$, where u is an endomorphism of A^d whose matrix with respect to the canonical basis of A^d has the form $\mathsf{pId}_d - cT$ ($c \in M_d(A)$).* □

The following easy proposition connects the group of curves of p-typical curvilinear formal group laws and distinguished modules.

7.3 Proposition. *Let $H \in \mathsf{DPS}-\mathsf{cHopf}_k$, with p-typical structural basis $\phi = \{\phi_I | I \in \mathsf{MI}(E)\}$ and F_p-type $F_p\phi_H = \sum_{i\geq 0} V_p^i[\lambda_i]\phi_H$, $\lambda_i \in M_d(k)$. Define $c := \sum_{i\geq 0} \tau(\lambda_i)T^i$. Then the left $W[[V_p]]$-module $C_p(H)$ and the distinguished right $W[[T]]$-module $A^d/(\mathsf{pId}_d - cT)A^d$ are anti-isomorphic.* □

7.4 Now assume k to be algebraically closed. We then have the following proposition, cf. loc. cit. chapter III, theorem 4 (or [Man], chapter III, §5, "the classification theorem").

7.5 Proposition. *Let M be a distinguished A-module. Then the R-module $M_R := R \otimes_A M$ admits a unique direct sum decomposition in simple submodules*

$$M_R \cong \bigoplus_i R\Big/p^{m_i}R \bigoplus_j R\Big/(p^{r_j} - T^{s_j})R\,,$$

where for all j we have $0 < r_j \leq s_j$ and $\gcd(r_j, s_j) = 1$. □

7.6 The decomposition described in the proposition is called the *isogeny type* of M. If G is a commutative formal group law defined over k. Then we define the isogeny type of G as the isogeny type of $C_p(G)$. As in [Man], chapter II, §4 we denote by $G_{m,n-m}$ the commutative formal group law corresponding to the distinguished A-module $A/(p^m - T^n)A$ and by $G_{m,\infty}$ the commutative formal group law corresponding to the A-module A/p^mA. Notice $G_{1,0} = \hat{G}_m$, the 1-dimensional multiplicative formal group law. We then say that M is *isogenous* to $\oplus_i G_{m_i,\infty} \oplus_j G_{r_j,s_j-m_j}$ and denote this equivalence relation by "$\sim$". Manin only defines $G_{n,m}$ for n, m relatively prime but it is well known that $G_{n,m}$ is isogenous to $dG_{n/d,m/d}$, where $d = \gcd(n, m)$. Therefore as in [Hon73], [Hov] or [Yui80] we will often use the notation $G_{n,m}$ even if n and m are not relatively prime.

7.7 In order to be able to compute the isogeny type from the F_p-type, we generalize [Dieu], chapter III, §5, lemma 4. Let $B(k)$ be the field of fractions of $W(k)$. For each natural number e we write $B_e(k)$ for the completely ramified extension of $B(k)$

generated by a root ω of the polynomial $X^e - p$, and W_e for the integral closure of W in $B_e(k)$. The automorphism σ is extended to W_e by defining $\sigma(\omega) := \omega$. We also extend o_p canonically to W_e by $o_p(\omega) := 1/e$. Write A_e for the canonical extension of A, and R_e the canonical extension of R. We define the *costathm* $c(a)$ of $a \in R_e$ by ($c(0) := \infty$)

$$c(a) = c(\sum_{i\geq 0} a_i T^i) = \min\{i \geq 0 | o_p(a_i) = \min\{o_p(a_n) | n \geq 0\}\}.$$

Further, if $a \in A_e$ with $c(a) > 0$ and $\omega \nmid a$, we define the rational number $\gamma(a)$ by

$$\gamma(a) = \gamma(\sum_{i\geq 0} a_i T^i) := \min\left\{\frac{o_p(a_i)}{c(a)-i} \mid 0 \leq i < c(a)\right\},$$

and a natural number $j(a)$ by

$$j(a) := \min\left\{j | \gamma(a) = \frac{o_p(a_j)}{c(a)-j}\right\}.$$

We may now prove the following lemma.

7.8 Lemma. *Let $a \in A_e$ be such that $\gamma(a) = r/s$, $s = c(a) - j(a)$. Then we may write in A_{es}*

$$a = y(p^r - T^s)x,$$

for some $x \in A^*_{es}$. For y we have the following formulae: $c(y) = c(a) - s$ and

$$\gamma(y) := \min\left\{\frac{o_p(a_i) - r}{c(a) - s - i} \mid 0 \leq i < c(a) - s\right\}.$$

proof: Let $a \in A_e$ be such that $\gamma(a) = r/s$, $s = c(a) - j(a)$. By [Man], remark to chapter II, lemma 2.2 we may then write

$$a = y \prod_{i=1}^{s} \left(T - p^{r/s} x_i\right),$$

for some $x_i \in A^*_{es}$. On the other hand, combination of loc. cit. lemma 2.7 and the corollary to lemma 2.5 gives that

$$R_{es} \Big/ \prod_{i=1}^{s} \left(T - p^{r/s} x_i\right) R_{es} \cong R_{es} \Big/ \left(T^s - p^r\right) R_{es}.$$

Thus we find that for some $x \in R^*_{es}$

$$\prod_{i=1}^{s} \left(T - p^{r/s} x_i\right) = \left(T^s - p^r\right) x$$

(and thus $x \in A^*_{es}$). We conclude that $a = y\,(T^s - p^r)\,x$. One now easily computes from this relation that $c(y) = c(a) - s$ and (with induction) that $\gamma(y) = \min_{i<c(a)-s} \{o_p(a_i) - r/c(a) - s - i\}$. □

7.9 Repeated application of the lemma gives that $a \in A$, $p \nmid a$ can be written in A_s, $s = \prod_i s_i$ as

$$a = y \prod_i (p^{r_i} - T^{s_i}) x_i,$$

where $x_i \in A^*_s$, $c(y) = 0$. Thus also $y \in A^*_s$. But then, since R/aR is semisimple ([Dieu], chapter III, theorem 1) and since $R/(p^r - V^s)R$ is simple if $\gcd(r, s) = 1$ (loc.cit. chapter III, theorem 2) we conclude that the isogeny type of A/aA is given by

$$A/aA \sim \bigoplus_i G_{r_i, s_i - r_i}.$$

7.10 The above lemma provides us with a strong tool for computing isogeny types of commutative formal group laws whose F_p-type is given. Just take any canonical curve ϕ_i. Some power of F_p will be an endomorphism of $W(k)[[V]]\{\phi_i\}$. We thus find an $a \in A$ such that $A/aA \hookrightarrow C_p(G)$. We now may use the lemma in order to decompose A/aA. Then, if necessary, we proceed by taking some other ϕ_j. Details of this procedure and examples can be found in chapter IV, sections 2 and 3, where we will compute the isogeny types for 2 and 3-dimensional commutative formal group laws.

Chapter 3

A finiteness theorem

For commutative formal group laws of finite height defined over an algebraically closed field of positive characteristic.

In this chapter it will be proven that any curvilinear commutative formal group law G of finite height defined over an algebraically closed field of positive characteristic is isomorphic to a formal group law G_{typ} having a well characterized finite (Witt) F-type. This has as a corollary that there exists a finite-dimensional catalogue for such formal group laws of bounded height.

This chapter is organized as follows: First an introduction to the problem is given, then two technical sections follow. In these sections some lemmas on reduction of F-types and on a special type of étale extensions are proven. In section 4 a classification result in characteristic zero of Ditters is adapted to our needs. The finite F-type then is constructed in section 5.

In this chapter all formal group laws are commutative and curvilinear.

1 Introduction and statement of the results

1.1 Let k be a ring of characteristic $p > 0$ and G be a d-dimensional p-typical formal group law defined over k. On $C_p(G)$, the (additive) group of p-typical curves of G, we have operators $V := V_p$, $F := F_p$ and $[r]$, $r \in k$. The topological group $C_p(G)$ is V-complete. Passing to the direct sum $C_p(G)^d$, we have seen (chapter II, theorem 4.6) that G is completely determined by its Witt F-type, i.e., the F-type of its canonical curves

$$F\phi_G = \sum_{i=0}^{\infty} V^i[C_i]\phi_G, \qquad 1.1.1$$

where $C_i \in M_d(k)$. (This is an abbreviated form for

$$F\phi_{G,l} = \sum_{i=0}^{\infty} \sum_{j=1}^{n} V^i[C_{i,l,j}]\phi_{G,j},$$

where $C_{i,l,j} \in k$.) Conversely every choice of $C_i \in M_d(k), i \geq 0$ gives rise to a unique formal group law G defined over k, with canonical curves ϕ_G.

1.2 Let the p-typical formal group law G have F-type as in 1.1.1. We will say that the F-type is *finite* and has *length* $n \in \mathbb{N}$ if $C_i = 0$ for $i > n$, $C_n \neq 0$. Notice that G having a finite F-type does not imply that the height of G is finite. (Consider for example $\hat{G}_a$.) A connection between the shape of the C_i and the height of G is given in section 5.

1.3 Moreover we know (chapter I, 5.7), that any formal group law H, isomorphic to G over k, has as a set of canonical curves ϕ_H

$$\phi_H = \sum_{i=0}^{\infty} V^i[\Lambda_i]\phi_G, \tag{1.3.1}$$

where $\Lambda_i \in M_d(k)$ for $i \geq 0$, $\Lambda_0 \in Gl_d(k)$. Let the F-type of H be

$$F\phi_H = \sum_{i=0}^{\infty} V^i[D_i]\phi_H. \tag{1.3.2}$$

1.4 We have the following relation among the C_i, Λ_i, D_i introduced in 1.1 and 1.3 On the one hand we have by (1.3.1) and (1.1.1)

$$F\phi_H = \sum_{i=0}^{\infty} V^i[\Lambda_i^{(p)}]F\phi_G = \sum_{i=0}^{\infty} V^i[\Lambda_i^{(p)}] \left(\sum_{j=0}^{\infty} V^j[C_j]\phi_G \right);$$

while on the other hand we have by (1.3.2) and (1.3.1)

$$F\phi_H = \sum_{i=0}^{\infty} V^i[D_i]\phi_H = \sum_{i=0}^{\infty} V^i[D_i] \left(\sum_{j=0}^{\infty} V^j[\Lambda_j] \right) \phi_G.$$

Therefore we obtain the following identity

$$\sum_{n=0}^{\infty} V^n \left(\sum_{i+j=n} [\Lambda_i^{(p^{j+1})}][C_j] \right) \phi_G = \sum_{n=0}^{\infty} V^n \left(\sum_{i+j=n} [D_i^{(p^j)}][\Lambda_j] \right) \phi_G. \tag{1.4.1}$$

1.5 Recall that the homothety or Witt operator [ ] is not additive, and multiplicative only in dimension one. Therefore working with equation (1.4.1) is very hard.

For example, it suffices, but, it is in general not necessary, that for each $n \geq 0$ the relations

$$\sum_{i+j=n} [D_i^{(p^j)}][\Lambda_j]\phi_G = \sum_{i+j=n} [\Lambda_i^{(p^{j+1})}][C_j]\phi_G, \qquad 1.5.1$$

hold in order to satisfy equation (1.4.1).
As an example we will consider two special cases.

1.6 We take $d = 1$, and $k = \mathbb{F}_p$. Then the equation (1.4.1) reduces to

$$\sum_{n=0}^{\infty} V^n \left(\sum_{i+j=n} [\Lambda_i C_j] \right) \phi_G = \sum_{n=0}^{\infty} V^n \left(\sum_{i+j=n} [D_i \Lambda_j] \right) \phi_G. \qquad 1.6.1$$

Read this equation mod V

$$[\Lambda_0 C_0]\phi_G \equiv [D_0 \Lambda_0]\phi_G \bmod V.$$

As $d = 1$ and $\Lambda_0 \in \mathbb{F}_p^*$ this implies that $C_0 = D_0$. Subtracting the terms $[\Lambda_0 C_0]\phi_G = [D_0\Lambda_0]\phi_G$ and $V[\Lambda_1 C_0]\phi_G = V[D_0\Lambda_1]\phi_G$ from both sides of (1.6.1) we find mod V^2

$$V[\Lambda_0 C_1]\phi_G \equiv V[D_1 \Lambda_0]\phi_G \bmod V^2.$$

This implies by the same reasoning as before that $C_1 = D_1$. Using induction we easily see $D_m = C_m$ for all $m \geq 0$. So we rediscover the following result of Dieudonné ([Dieu], chapter III, §6, no.2, section II, for the translation between the terminology of Dieudonné and ours, see chapter II, section 7).

Theorem. *There is a bijective correspondence between the set of isomorphism classes of 1-dimensional formal group laws over a prime field and the set of all possible F-types (1.1.1).* □

In particular it is not true that over the prime field every 1-dimensional formal group law is isomorphic to a formal group law having a finite F-type.

1.7 Again take $d = 1$, but now assume $k^{\text{ét}}$ to be the étale closure of a field of positive characteristic p. Let G be a 1-dimensional formal group law with F-type (1.1.1). There are two cases to be considered
case 1: All C_i are zero. This is equivalent (chapter II, subsection 1.4) to G being the formal additive group law.
case 2: Not all C_i are zero. Let h be the smallest integer such that C_h is not zero (h is easily seen to the height of G, as defined in chapter I, 4.19). For $n = h$ equation (1.5.1) reads $\Lambda_0^{p^{h+1}} C_h = D_h \Lambda_0$. Since $d = 1$ putting $D_h = 1$ gives an étale equation for which we have an invertible Λ_0 as solution. We may thus assume that $C_h = 1$ and that an $N > h$ is given such that $C_i = 0$ for $h \neq i < N$. Now take

$\Lambda_0 = 1, \Lambda_i = 0$ for every $0 < i < N - h$. We then find $D_i = C_i$ for every $i < N$. At level N, (1.5.1) is now read mod V as

$$\Lambda_{N-h}^{p^{N+1-h}} C_h + C_N = D_N + D_h^{p^{N-h}} \Lambda_{N-h}.$$

Taking $D_N = 0$ we obtain an étale equation in Λ_{N-h}. So by induction we find the following theorem.

Theorem. *Every 1-dimensional formal group law G of finite height h over an étally closed field $k^{\text{ét}}$ of positive characteristic is isomorphic to a formal group law G_{typ} with the F-type*

$$F\phi_{typ} = V^h \phi_{typ}. \qquad \square$$

This theorem gives the well known assertion that the only isomorphism invariant of 1-dimensional formal groups defined over an algebraically closed field of positive characteristic is the height.

1.8 Other published results on the classification up to isomorphism of formal group laws over rings of positive characteristic can be found for the 1-dimensional case in for example [Haz] and [Hon]. An overview is given in [Hill]. The classification for 2-dimensional formal group laws over an algebraically closed field is given by Manin [Man] (contravariant) and Kneppers [Kne] (covariant).

1.9 We will prove in this chapter the following theorem (theorem 5.17).

Theorem. *Let G be a d-dimensional p-typical curvilinear commutative formal group law of finite height, defined over an algebraically closed field k of positive characteristic p. Then G is isomorphic over k to a p-typical curvilinear commutative formal group law G_{typ} having a finite (Witt) F_p-type. Moreover the length λ of the finite F-type is bounded by the height h of G.*

We borrow the definition of a *catalogue* from F. Oort: A catalogue for a small category $\mathcal{C}$ is an algebraic set $\mathcal{S}$ such that there is surjection of sets from $\mathcal{S}$ to the set of isomorphism classes of $\mathcal{C}$. With this notation we obtain as an immediate consequence of the theorem

Corollary. *There is a catalogue of finite dimension over k for all p-typical curvilinear commutative formal group laws G defined over an algebraically closed field k of positive characteristic such that the height of G is bounded by a fixed number.*

1.10 Remark. Let G be defined over an algebraically closed field of positive characteristic p with finite height h. The group $\bar{C}_p$ of p-typical curves of G of course has a canonical $W(k)$-module structure, and as such it has $W(k)$ rank equal

to the height h of G (chapter I, lemma 4.26). However, having a catalogue of finite rank over $W(k)$ does not give any information on finite-dimensionality of a catalogue over k.

2 Reduction of Hilbert F-types

2.1 Let k be an integral domain of characteristic $p > 0$. Let G be a d-dimensional p-typical curvilinear commutative formal group law defined over $R := W_p(k)$ and let $\bar{G}$ denote the reduction of G which is defined over k. Write $C_p = C_p(G)$ and $\bar{C}_p = C_p(\bar{G})$.

2.2 We recall some facts and notations which can be found in chapters I and II. For any formal group law H defined over a $\mathbb{Z}_p$-algebra A, we have the canonical $\mathrm{Cart}_p(A)$-module structure on $C_p(H)$ and also an induced $W_p(A)$-module structure. Thus C_p is a $W_p(R)$-module and $\bar{C}_p$ is an R-module. Let $F := F_p$ and $V := V_p$. As we have seen both G and $\bar{G}$ are determined by their Witt F-types. But since R is a p-Hilbert ring we also know that G is determined by its Hilbert F-type

$$F\phi_G = \sum_{i\geq 0} V^i\{C_i\}\phi_G,$$

for some (unique) $C_i \in M_d(R)$. Contrary to the Witt operators [ ], the Hilbert operators $\{\ \} : R \to \mathrm{End}_{C_p(G)}$ are homomorphisms. Actually, as we have seen, if we denote by $\heartsuit$ the canonical $\mathrm{Cart}_p(R)$-structure on C_p, then

$$[r]\psi = \tau_R(r)\heartsuit\psi, \qquad \{r\}\psi = \lambda_p(r)\heartsuit\psi.$$

2.3 We will treat the following question : For G we can consider its Hilbert F-type and its Witt F-type, while for $\bar{G}$ we can only consider its Witt F-type. What is the relation between the Hilbert F-type of G and the Witt F-type of $\bar{G}$? Or to phrase it differently: what is the fiber of the map π^* from the set of all Hilbert F-types (over R) to the set of all Witt F-types (over k), induced by the canonical projection $\pi : R \mapsto k$ on the first Witt coordinate. (The relation between the Witt F-type of G and the Witt F-type of $\bar{G}$ is, of course, just induced by $[r] \to [\pi(r)]$).

2.4 The first result is the following: From chapter I, lemma 3.19 (iii) we find that G having a Hilbert F-type of the form

$$F\phi_G = \sum_{i\geq 0} V^i\{\tau_k(C_i)\}\phi_G, \qquad C_i \in M_n(k),$$

reduces to $\bar{G}$ having the Witt F-type

$$F\phi_{\bar{G}} = \sum_{i\geq 0} V^i[C_i]\phi_{\bar{G}}, \qquad C_i \in M_n(k).$$

We will proceed to describe the fiber of the reduction map in terms of Hilbert F-types.

2.5 The basic idea is rather simple: in $C_p(\bar{G})$ the operators F and V commute, thus the reduction of $C_p(G)$ to $C_p(\bar{G})$ will factor via $C_p(G)$ modulo the commutation relation of F and V. We will prove that this fact is sufficient to determine $C_p(\bar{G})$.

2.6 We let $T := FV - VF \in \mathrm{Cart}_p(R)$ and define abelian groups C^i $(i \geq 0)$ by

$$C^i = C_p(G) \Big/ \textstyle\sum_{j=0}^{i} V^j T C_p(G) = C^{i-1} \Big/ V^i T C_p(G) \cdot$$

2.7 Some generalities. The operators $F, [\ ], \{\ \}$ stabilize $\sum_{j=0}^{i} V^j T C_p(G)$. So on C^i we have an induced action of F, which we will again denote by F. The same applies to the operators $[\ ]$ and $\{\ \}$. The R-module structure on $C_p(G)$ given by the Hilbert brackets $\{\ \}$ also induces an R-module structure on C^i.
However the operator V does not stabilize $\sum_{j=0}^{i} V^j T C_p(G)$, which means that there is no induced action of V on C^i. Therefore C^i is not an $R[[V]]$-module. (It is a $W_p(R)$-module since F acts trivially on $(FV - VF)C_p(G)$.) The operator V induces a map $C^i \to C^{i+1}$ and thus V induces a well-defined operator on $\varinjlim C^i$.

2.8 We will give an easy example which illustrates some of the features of this construction.
Let G have Hilbert F-type

$$F\phi_G = \{(1+p)\mathsf{Id}\}\phi_G = (1+p)\phi_G.$$

Using 2.4 we see that the following relation holds in $\bar{C}_p$

$$F\phi_{\bar{G}} = (1+p)\phi_{\bar{G}} = (1+VF)\phi_{\bar{G}} = \ldots = \sum_{i \geq 0} V^i \phi_{\bar{G}}.$$

Thus a finite Hilbert F-type may reduce to an infinite Witt F-type. On the other hand we have in $\varinjlim C^i$

$$F\phi_G = (1+p)\phi_G \equiv (1+VF)\phi_G \equiv \ldots \equiv \sum_{i \geq 0} V^i \phi_G.$$

We conclude that in this case the $W_p(k)[[V]]$-modules $\bar{C}_p$ and $\varinjlim C^i$ are isomorphic.

2.9 Every element $\bar{\psi}$ in C^l can be written as

$$\bar{\psi} = cl_l \left\{ \sum_{i,j} V^i \{r_{i,j}\} \phi_{G,j} \right\} \qquad r_{i,j} \in R$$

or as

$$\bar{\psi} = cl_l \left\{ \sum_{i,j} V^i [r_{i,j}] \phi_{G,j} \right\} \qquad r_{i,j} \in R$$

where cl_l denotes the class in C^l. However these expressions are not unique.
In order to obtain a unique representation note that every $r_{i,j} \in R = W_p(k)$ can be written as $(\mathsf{V} := \mathsf{V}_p)$

$$r_{i,j} = \sum_{k \geq 0} \mathsf{V}^k \tau(r_{i,j,k}) \qquad r_{i,j,k} \in k$$

(chapter I, 3.6). We have the following easy but crucial lemma.

2.10 Lemma. *Let $\bar{\psi} = cl_l \{\sum_i V^i \{a_i\} \phi\}$ in C^l and suppose $a_{i_0} = a'_{i_0} + \mathsf{V} r$ for some $i_0 < l$ and $r \in R$, then $\bar{\psi} = cl_l \{\sum_i V^i \{a'_i\} \phi\}$ with $a'_i = a_i$ for $i < i_0$.*

proof: Temporarily working over the perfect closure of the field of fractions of k, we have

$$\begin{aligned} V^{i_0}\{a'_{i_0} + \mathsf{V} r\}\phi &= V^{i_0}\{a'_{i_0}\}\phi + V^{i_0} p\{\mathsf{F}^{-1} r\}\phi \\ &\equiv V^{i_0}\{a'_{i_0}\}\phi + V^{i_0} F\{\mathsf{F}^{-1} r\}\phi \bmod V^{i_0} T C_p(G) \\ &\equiv V^{i_0}\{a'_{i_0}\}\phi + V^{i_0+1}\{r\} F\phi. \end{aligned}$$

Here in the first step we use the commutativity of F and V on $W_p(k)$ (k has characteristic $p > 0$), and the fact that the Hilbert operators induce an R-module structure. In the second step we use $V^{i_0} FV \equiv V^{i_0+1} F \bmod V^{i_0} T$. The third step is the combination of the defining relation of F on $W_p(k)$ (see chapter 1 3.7.1) and chapter I, formula 3.15.1 which describes the action of F on $\lambda_p(r), r \in R$. At the same time this makes clear that the relation is actually defined over k. □

2.11 Proposition. *The class $\bar{\psi}$ in C^l can be written as*

$$\bar{\psi} = cl_l \left\{ \sum_{i=0}^{l} \sum_{j=1}^{d} V^i \{\tau(r_{i,j})\} \phi_{G,j} + \psi' \right\},$$

for some $\psi' \in V^{l+1} C_p(G)$ and unique $r_{i,j} \in k$.

proof: Repeated application of lemma 2.10 yields that $\bar{\psi}$ may be written as claimed.
For the uniqueness, first note that

$$V^n (FV - VF) \sum_{i \geq 0} \sum_{j=1}^{d} V^i \{a_{i,j}\} \phi_{G,j} \equiv \sum_{j=1}^{d} V^n \{p a_{0,j}\} \phi_{G,j} \bmod V^{n+1} C_p(G) \qquad 2.11.1$$

(and $TVC_p(G) = 0$). Assume that $\bar{\psi} \in C^l$ can be written as

$$\bar{\psi} = cl_l \left\{ \sum_{i=0}^{l} \sum_{j=1}^{d} V^i \{\tau(r_{i,j})\} \phi_{G,j} + \psi_r \right\}$$

and also as

$$\bar{\psi} = cl_l \left\{ \sum_{i=0}^{l} \sum_{j=1}^{d} V^i \{\tau(r'_{i,j})\} \phi_{G,j} + \psi'_r \right\}$$

$(\psi_r, \psi'_r \in V^{l+1} C_p(G))$, such that $r_{i,j} = r'_{i,j}$ for $i < i_0 \leq l$. Then we have

$$\sum_{i=i_0}^{l} \sum_{j=1}^{d} V^i \{\tau(r_{i,j}) - \tau(r'_{i,j})\} \phi_{G,j} \in \sum_{k=0}^{l} V^k TC_p(G) + V^{l+1} C_p(G)$$

This together with the first remark (2.11.1) gives that $\tau(r_{i_0,j}) - \tau(r'_{i_0,j}) \in pR$. This in turn implies that $r_{i_0,j} = r'_{i_0,j}$. Thus by induction on i_0 we see that the representation is unique. □

2.12 We conclude from proposition 2.11 that an element $\kappa \in \varinjlim C^i$ can be represented as $\kappa = \sum_{i,j} V^i \{\tau(r_{i,j})\}$ for unique $r_{i,j} \in k$.

2.13 Put $S = W_p(R)[[V]]$. We summarize the different module structures we have so far encountered: C_p is a $W_p(R)$-module via the Cart_p-structure and an R-module by the Hilbert-structure. Therefore C_p is a S-module with $\dim(G)$ generators via the Cart_p-structure and a free $R[[V]]$-module of rank $\dim(G)$ via the Hilbert-structure. The reduced $\bar{C}_p$ is an R-module via the Cart_p-structure, but also an R-module via the reduction of the Hilbert R-module structure on C_p. We also have an S-module structure on $\bar{C}_p$ via reduction of the S-module structure on C_p.
It is clear that the subgroup STC_p $(:= \{sT\phi \mid s \in S, \phi \in C_p(G))$ of C_p is stabilized by $\{\ \}, [\ ], F, V$ (note that $FT = 0$). So we have induced operators on $C_p/STC_p = \varinjlim C^i$, which is therefore also an S-module, and an R-module via $\{\ \}$

2.14 Theorem. *The S-module C_p/STC_p is isomorphic to the S-module $\bar{C}_p$, and the Hilbert R-module structure on C_p reduces to the canonical (Witt) R-module structure on $\bar{C}_p$.*

proof: The isomorphism of the first statement, of course, is given by

$$\Phi : \sum_{i,j} V^i \{\tau(r_{i,j})\} \bar{\phi}_{G,j} \mapsto \sum_{i,j} V^i [r_{i,j}] \phi_{\bar{G},j}.$$

Indeed from proposition 2.11 we find that the map Φ is a bijection. Since we already observed (subsection 2.5) that the reduction factors via $C_p \big/ STC_p$, and

that the induced homomorphism $C_p/STC_p \to \bar{C}_p$ is precisely Φ (subsection 2.4), we are done.
For the second statement, consider for $a \in R$

$$\{a\} = \{\sum_i \tau(a_i^{p^{-i}})\}p^i \equiv \sum_i V^i\{\tau(a_i)\}F^i \bmod ST\mathrm{Cart}_p(R)$$

Since $\{\tau(a_i)\}$ reduces to $[a_i]$ in $\bar{C}_p$ (lemma 3.19) we see that the R-module structure on $\bar{C}_p$ induced by the reduction of the Hilbert R-module structure is exactly the canonical $W_p(k)$-module structure on $\bar{C}_p$. □

We may thus describe the fiber of the reduction map $\mathcal{F}_{W_p(k)} \to \mathcal{F}_k$ in terms of F-types as in the following theorem.

2.15 Theorem. *Let k be an integral domain with positive characteristic p. Let $\bar{G}$ be a d-dimensional curvilinear commutative formal group law defined over k. Assume that $\bar{G}$ has Witt F-type $F\phi_{\bar{G}} = \sum V^i[\bar{C}_i]\phi_{\bar{G}}$ ($\bar{C}_i \in M_d(k)$). Let G be a d-dimensional curvilinear commutative formal group law defined over $W_p(k)$ which reduces to $\bar{G}$, then G has Hilbert F-type*

$$F\phi_G = \sum_{i=0}^{\infty} V^i\{\tau(\bar{C}_i)\}\phi_G + \sum_{i=0}^{\infty} V^i\{B_i\}T\phi_G,$$

where the $B_i \in M_d(W_p(k))$ ($i \geq 0$) may be arbitrarily chosen. □

Reduction of permutation type Hilbert F-types

2.16 Let the p-typical formal group law G defined over $R = W_p(k)$ have Hilbert F-type $F\phi_G = \sum_{i\geq 0} V^i\{C_i\}\phi_G$, $C_i \in M_d(R)$. We say that (the F-type of) G is of *permutation type* if the matrix $\sum_{i\geq 0} C_i t^i$, for some transcendental t, has in every row and column exactly one entry of the form at^m, $a \in R$. All other entries in that row and column are zero.

2.17 Lemma. *Let G have permutation type F-type $F\phi_G = \sum_{l\geq 0} V^l\{C_l\}\phi_G$. Assume that k is algebraically closed. Define $D_l \in M_d(R), l \geq 0$ by:*

$$D_{l,i,j} = p_p^o(C_{l,i,j}),$$

where o_p denotes the p-adic order ($p^\infty := 0$). Then there is a special weak isomorphism $\phi_{G'} = \{\Lambda\}\phi_G$ from G to G' such that the F-type of G' is $F\phi_{G'} = \sum_{l\geq 0} V^l\{D_l\}\phi_{G'}$.

proof: Let $D_l, l \geq 0$ be defined as in the lemma. Then Λ must be an invertible solution of the system of equations

$$\Lambda^{\sigma^l} C_l = D_l\Lambda, \qquad l \geq 0. \tag{2.17.1}$$

We claim that we can find a diagonal matrix Λ (with diagonal entries $\Lambda_i := \Lambda_{i,i}$) which is a solution of 2.17.1. We proceed as follows:
Define the permutation matrix U by $U_{i,j} := 1$ if $C_{l,i,j} \neq 0$ for some l. Define diagonal matrices $\tilde{C}_l, l \geq 0$ by $\tilde{C}_{l,i} := \tilde{C}_{l,i,i} := C_{l,i,j}$ if $C_{l,i,j} \neq 0$ for some j, else $C_{l,i} := 0$. Analogously define diagonal matrices $\tilde{D}_l, l \geq 0$. Then the system of equations 2.17.1 is equivalent to the system of equations

$$\Lambda^{\sigma^l}\tilde{C}_l U = \tilde{D}_l U\Lambda \Leftrightarrow \Lambda^{\sigma^l}\tilde{C}_l = \tilde{D}_l\, U\Lambda U^{-1} \Leftrightarrow$$

$$\Lambda^{\sigma^l}\tilde{C}_l = U\Lambda U^{-1}\,\tilde{D}_l,$$

for $l \geq 0$. Denote $\Lambda_{\pi(i)} := (U\Lambda U^{-1})_{i,i}$ and $f_i := \tilde{C}_{l,i}/\tilde{D}_{l,i}$ if $\tilde{C}_i \neq 0$ for some $l =: l_i \geq 0$ (and thus $\operatorname{ord}_p(f_i) = 0$). Then we find that 2.17.1 is equivalent to

$$\Lambda_i^{\sigma^{l_i}} = f_i\Lambda_{\pi(i)}, \qquad 0 \leq i \leq d.$$

This (étale) system of equations clearly has non-zero solutions in k. □

2.18 Proposition. *Let G be a permutation type formal group law defined over $W_p(k)$, k an algebraically closed field of positive characteristic p. Write the Hilbert F-type of G as $F\phi_G = \sum_{i\geq 0} V^i\{C_i\}\phi_G$. Then the reduction $\bar{G}$ of G is isomorphic to a formal group law $\bar{G}_{typ}$ such that $\bar{G}_{typ}$ has a finite Witt F-type $F\phi_{\bar{G}_{typ}} = \sum_{i\geq 0} V^i[D_i]\phi_{\bar{G}_{typ}}$. Especially, $D_{i,j,l} = 1$ if $C_{i,j,l} \neq 0 \bmod p$, and in every row of $\sum_{i\geq 0} D_i t^i$, for some transcendental t, there is at most one non-zero entry which is a monomial in t with coefficient 1.*

proof: By lemma 2.17 we may assume that the non-zero entries of $C_i, i \geq 0$ are pure powers of p. Thus for $\bar{G}$ we have that $F\phi_{\bar{G},i} = V^{l_i}p^{m_i}\phi_{\bar{G},j_i} = V^{m_i+l_i}F^{m_i}\phi_{\bar{G},j_i}$. Repeated substitution of the action of F on $\phi_{\bar{G},k}$ leaves us with two possibilities: Either after a finite number of steps we have found $F\phi_{\bar{G},i} = V^{l_i}\phi_{\bar{G},a_i}$ or this first possibility does not happen, which means that $F\phi_{\bar{G},i} = 0$. □

3 Two étale lemmas

The first lemma is a lemma in the spirit of [Dieu], chapter III, §5 , lemma 1, which applies to "one dimensional" σ-equations over $W(k)$, where k is an algebraically closed field.

3.1 Lemma. *Let $k^{\text{ét}}$ be an étally closed ring of positive characteristic p. Suppose the matrix equation* Eq *over $W(k^{\text{ét}})$ is defined by*

$$x + \sum_{l=1}^{m} a_l x^{\sigma^l} = c, \qquad a_l, c \in M_n\left(W(k^{\text{ét}})\right) \text{ for } l = 1, ..., m.$$

Let $\varepsilon \in M_n\left(k^{\text{ét}}\right)$ *be a solution of* $\mathsf{Eq} \bmod \mathsf{V}W(k^{\text{ét}})$. *Then* Eq *has a solution* $x \in M_n\left(W(k^{\text{ét}})\right)$ *such that* $x \equiv \tau(\varepsilon) \bmod \mathsf{V}W(k^{\text{ét}})$.

proof: We use induction on powers of V. Suppose we have found a solution $x_i = \sum_{j=0}^{i-1} \mathsf{V}^j \tau(o_j)$ for $\mathsf{Eq} \bmod \mathsf{V}^i$. Define $x_{i+1} = \sum_{j=0}^{i} \mathsf{V}^j \tau(o_j)$, where o_i has yet to be found. Now consider Eq with $x = x_{i+1}$:

$$x_i + \mathsf{V}^i \tau(o_i) + \sum_{l=1}^{m} a_l \left(x_i^{\sigma^l} + \mathsf{V}^i \tau(o_i^{p^l})\right) = c \Leftrightarrow$$

$$\mathsf{V}^i \left(\tau(o_i) + \sum_{l=1}^{m} a_l^{\sigma^i} \tau(o_i^{p^l})\right) = \mathsf{V}^i \tau(r) + \mathsf{V}^{i+1} s,$$

with $r \in M_n\left(k^{\text{ét}}\right), s \in M_n\left(W(k^{\text{ét}})\right)$. Reading this $\bmod \mathsf{V}^{i+1}$, we find:

$$o_i + \sum_{l=1}^{m} \bar{a}_l^{p^i} o_i^{p^l} = r, \qquad (\bar{a} = \pi(a)).$$

Then this equation has by the Jacobi criterion ([Mum], III.5, definition 1) a solution $o_i \in M_n\left(k^{\text{ét}}\right)$. □

The second lemma is on a special type of étale extensions.

3.2 Lemma. *Let* k *be a ring of positive characteristic* p. *Assume that* $k[y_i]_{i=1,\ldots,n}$ *is an étale extension of* $k[y_j^p]_{j=1,\ldots,n}$, *then* $k[y_i]_{i=1,\ldots,n}$ *is an étale extension of* k.

proof: Assume that $k[y_i]_{i=1,\ldots,n}$ is an étale extension of $k[y_j^p]_{j=1,\ldots,n} =: k[y^p]$. This is equivalent by the Jacobi criterion to the y_i being roots of $f_l \in k[y^p][Z_j]_{j=1,\ldots,n} =: k[y^p][Z]$, for $0 \leq l \leq n$, with

$$\det\left(\partial f_i \,/\, \partial Z_j\right)_{i,j}\Big|_{Z=y} \not\equiv 0 \bmod \wp \text{ for } \wp \in \mathsf{Spec}\, k[y].$$

Let $P_l \in k[X_j, Y_j]_{j=1,..,n}$ be polynomials such that $P_l(Z_j, y_j) = f_l$. Define new polynomials $\tilde{f}_l \in k[Z]$ by $P_l(Z_j, Z_j)$. We then obviously have that the y_i are roots of the $\tilde{f}_l$ (for $0 \leq i, l \leq n$) and

$$\det\left(\partial \tilde{f}_i \,/\, \partial Z_j\right)_{i,j}\Big|_{Z=y} = \det\left(\partial f_i \,/\, \partial Z_j\right)_{i,j}\Big|_{Z=y} \not\equiv 0 \bmod \wp \in \mathsf{Spec}\ k[y],$$

because of the relation for monomials ($b > 0, a \in k[Z_i]_{i \neq j}$):

$$\partial a y_j^{pb} Z_j^c \,/\, \partial Z_j\Big|_{Z=y} = a\Big|_{Z=y} c y_j^{pb+c-1} = \partial a Z_j^{pb+c} \,/\, \partial Z_j\Big|_{Z=y}.$$

This establishes that all y_i are étale over k. □

4 A classification result for p-Hilbert domains

In this section we adapt a classification result of Ditters for formal group laws defined over a p-Hilbert domain.

4.1 Theorem. ([Dit89], section 3) *Let R be a p-Hilbert domain. Let G be a d-dimensional formal group law over R, which is not isomorphic to the d-dimensional additive formal group law. Then there exists an element $f \not\equiv 0 \bmod pR$, a positive integer γ and integers $h_i, r_i (1 \leq i \leq \gamma, h_1 \geq 0, h_i \geq 1$ for $i \geq 2, r_i \geq 1)$ and invertible matrices W_1, W_2 in $M_d(R_f)$ such that G is strongly isomorphic over R_f to a formal group law G_{typ} with F-type $F = \sum V^j\{D_j\}$. Here the D_j can be inductively described by the following procedure: Define $g_i = d - \sum_{j=1}^{i-1} r_j$ (so $g_1 = d$), then we have matrices $d_{j,i} \in M_{g_i \times d}(R), j \geq 0, 1 \leq i \leq \gamma + 1$, such that $W_1 D_j W_2 = d_{j,1}$ and*

$$
\begin{aligned}
d_{m,i} &\equiv \begin{pmatrix} * & 0_{g_i} \end{pmatrix} \bmod p, && m < h_i, \\
d_{h_i,i} &\equiv \begin{pmatrix} * & I_{r_i} & 0 \\ * & * & 0_{g_{i+1}} \end{pmatrix} \bmod p, && \\
d_{m,i} &= \begin{pmatrix} 0_{r_i} & 0 \\ d_{m-h_i,i+1} \end{pmatrix}, && m > h_i \\
&\text{and} && \\
d_{m,i} &\equiv \begin{pmatrix} * & 0_{g_{\gamma+1}} \end{pmatrix} \bmod p, && i = \gamma + 1. \qquad \square
\end{aligned}
$$

4.2 In order to help read the inductive formulae of the theorem, notice that $d_{m,1} \equiv 0 \bmod pR$ for $m < h_1$ and that:

$$
d_{h_1,1} = \begin{pmatrix} I_{r_1} & 0 \\ * & 0_{g_2} \end{pmatrix}.
$$

In [Dit89] the set $(h_i; r_i)_{1 \leq i \leq \gamma}$ is called the jump sequence. We will show that this coincides with the notion jump sequence as we defined in chapter I, 4.22. (Thus G has finite height if and only if $\sum_{i=1}^{\gamma} r_i = d$.) The matrices D_m of the normalized F-type are called the *higher Hasse-Witt matrices.*
We will use the following adaption of the above theorem.

4.3 Theorem. *Let G be a d-dimensional formal group law defined over a local p-Hilbert domain R. Then G is isomorphic over R to a formal group law G_{typ}*

described below. In the description we use following data, which we will call the jump data*:*

jd_1*: a number* γ *called* the number of blocks *with* $1 \leq \gamma \leq d$,

jd_2*: numbers* h_i *with* $h_1 \geq 0, h_i > 0$ *for* $2 \leq i \leq \gamma$,

jd_3*: natural numbers* r_i *for* $1 \leq i \leq \gamma$

jd_4*: matrices* $A_i \in Gl_{r_i}(R)$ *for* $1 \leq i \leq \gamma$ (the blocks) *and*

jd_5*: a* $d \times d$ *permutation matrix* U.

The F*-type of* G_{typ} *is related to the jump data as follows: Define* $g_i := d - \sum_{j=1}^{i-1} r_j$ *(so* $g_1 = d$*). The* F*-type* $F = \sum V^j C_j$ *of* G_{typ} *can then be described inductively by matrices* $c_{j,i} \in M_{g_i \times d}(R), j \geq 0, 1 \leq i \leq \gamma + 1$ *such that* $UC_j = c_{j,1}$ *and*

$$\begin{aligned} c_{m,i} &\equiv \begin{pmatrix} * & 0_{g_i} \end{pmatrix} \bmod p, && m < h_i, \\ c_{h_i,i} &\equiv \begin{pmatrix} * & A_i & 0 \\ * & * & 0_{g_{i+1}} \end{pmatrix} \bmod p, && A_i \in Gl_{r_i}(R), \\ c_{m,i} &= \begin{pmatrix} *_{r_i} & 0 \\ c_{m-h_i,i+1} \end{pmatrix}, && m > h_i \end{aligned}$$

and

$$c_{m,i} \equiv \begin{pmatrix} * & 0_{g_{\gamma+1}} \end{pmatrix} \bmod p, \qquad i = \gamma + 1. \qquad \square$$

proof: Let G'_{typ} be isomorphic to G such that the Hilbert F-type $F\phi'_{typ} = \sum V^j D_j \phi'_{typ}$ of G'_{typ} has the properties of theorem 4.1. Apply the special weak isomorphism $\phi_{typ} = W_2^{-1}\phi'_{typ}$ then the F-type of G_{typ} is given by $F\phi_{typ} = \sum V^j C_j \phi_{typ}$, where

$$C_j = W_2^{-\sigma^{j+1}} D_j W_2 = W_2^{-\sigma^{j+1}} W_1^{-1} d_{j,1}.$$

If a column of $d_{j,1}$ is zero then the corresponding column of C_j is also zero, and because the matrix $W_2^{-\sigma^{j+1}} W_1^{-1}$ is invertible we also have that if we got some set of independent columns in $d_{j,1}$ then the set of corresponding columns in C_j is also independent. By multiplying from the left with a permutation matrix U we then may permute rows in order to obtain the $c_{j,1}$ in the form as given by the theorem. $\square$

4.4 Let G have finite height and an F-type in the form of theorem 4.3 then we easily see that the set

$$\left\{ V^{j_l}\phi_{i_l} \;\middle|\; 0 \leq l < \gamma, 0 \leq j_l \leq \sum_{k=1}^{l+1} h_k, \sum_{k=1}^{l} r_k < i_l \leq \sum_{k=1}^{l+1} r_k \right\}$$

is a basis for the $W(R)$-module $C_p(G)$ and thus by chapter I, lemma 4.26 we conclude that the set $(h_i; r_i)_{1 \leq i \leq \gamma}$ is the jump sequence of G as defined in chapter I, 4.22. Lemma 4.26 in chapter I then gives a relation between the height h of G and the jump sequence of G.

4.5 Having any sequence $\mathcal{C} = \{C_i\}_{i \geq 0}$ of $d \times d$ matrices with entries in some local p-Hilbert domain, we define the jump data of $\mathcal{C}$ to be the jump data of the associated formal group law. We denote the jump data as $(\gamma, (h_i; r_i; A_i), U)$.

4.6 We end by noting the following obvious property: Suppose that G has jump data $(\gamma, (h_i; r_i; A_i), U)$ and G' has jump data $(\gamma', (h'_i; r'_i; A'_i), U')$, with $\sum_{i=1}^{\gamma} h_i < h'_1$. Then $G \oplus G'$ has jump data $(\gamma + \gamma', (h^*_i; r^*_i; A^*_i), U^*)$, where $h^*_i := h_i$ if $i \leq \gamma$ and $h^*_i := h'_{i-\gamma}$ if $\gamma < i \leq \gamma'$, the same convention applies for r_i and A^*_i while U^* is the permutation matrix

$$U^* := \begin{pmatrix} U & 0 \\ 0 & U' \end{pmatrix}.$$

5 Constructing the finite F-type

Given a p-typical formal group law G of finite height, determined by its F-type, we construct in this section the finite F-type of a p-typical formal group law G_{typ} which is isomorphic to G.

5.1 Notations, fixed throughout this section. We will denote by k a fixed perfect field of positive characteristic p. For any $\mathbb{Z}_{(p)}$-algebra K we denote as $W(K) := W_p(K)$ the ring of p-typical Witt vectors on K, on which we have injective operators F and V. Also $\pi : W(K) \to K$ will denote the canonical projection to the first coordinate, while $\tau : K \to W(K)$ is the Teichmüller map. On $W(k)$ we have a p-Hilbert structure, i.e., $W(W(k))$ is a $W(k)$-module under the homomorphism $\lambda : W(k) \to W(W(k))$.
All maps are defined entrywise on matrices. For a matrix $A \in M_d(R)$ we will denote by $k[A]$ the subring of R generated by the entries of A.

5.2 We have seen that the problem of classifying d-dimensional formal group laws defined over a ring k of positive characteristic can be formulated in terms of F-types as follows. Find a set of series of matrices $\mathcal{N} \subset M_d(k)^{\mathbb{N} \cup \{0\}}$ with some "nice" properties satisfying the following: Given an arbitrary formal group law $\bar{G}$ defined over k with F-type

$$F\bar{\phi} = \sum_{i=0}^{\infty} V^i[\bar{C}_i]\bar{\phi}, \qquad \bar{C}_i \in M_d(k)$$

there is an isomorphism

$$\bar{\psi} = \sum_{j=0}^{\infty} V^j[\bar{\Lambda}_j]\bar{\phi}, \qquad \bar{\Lambda}_j \in M_d(k)$$

to a formal group law $\bar{G}_N$ over k with the F-type

$$F\bar{\psi} = \sum_{i=0}^{\infty} V^i[\bar{N}_i]\bar{\psi},$$

for some $N = \{\bar{N}_i\}_{i\geq 0} \in \mathcal{N}$. But since $\bar{C}_p(G)$ allows no k-module structure, or equivalently, since the Teichmüller map $\tau : k \to W(k)$ is not additive, we have seen that the computation of such a set $\mathcal{N}$ is not easy.

5.3 The basic idea is to lift everything to $W(k)$. An advantage of doing this is that the group of p-typical curves $C_p(G)$ for a commutative formal group law G over $W(k)$ has a well-behaved $W(k)$-module structure.
First we translate the problem in characteristic zero. From now on we will use only the Hilbert structure, so we may omit the Hilbert parentheses { }, if there is no danger of ambiguity.
So the problem is reduced to the following: Find a set of series of matrices $\mathcal{N} \subset M_d(k)^{\mathbb{N}\cup\{0\}}$ having some "nice" properties, such that the following holds. Given a lifting G over $W(k)$ of a formal group law $\bar{G}$ over k having F-type

$$F\phi_G = \sum_{i=0}^{\infty} V^i C_i \phi_G, \qquad C_i \in M_d\left(W(k)\right),$$

there is an isomorphism

$$\psi = \sum_{j=0}^{\infty} V^j \Lambda_j \phi_G, \qquad \Lambda_j \in M_d\left(W(k)\right)$$

to a formal group law in the fiber above a $\bar{G}_N$ for a suitable $N \in \mathcal{N}$, i.e., by theorem 2.15 to a formal group law $G_{N,B}$ having an F-type of the form ($\psi = \phi_{G_{N,B}}$)

$$F\psi = \sum_{i=0}^{\infty} V^i N_i \psi + \sum_{j=0}^{\infty} V^j B_j T\psi,$$

where $N_i := \tau(\bar{N}_i)$, $B_j \in M_d\left(W(k)\right)$.

5.4 We will rewrite the above formula in a form which will be useful for computations. Write $\phi = \phi_G$. On the one hand we have:

$$\begin{aligned} F\psi &= F\left(\sum_{i=0}^{\infty} V^i \Lambda_i \phi\right) = \Lambda_0^{\sigma} F\phi + p\sum_{i=0}^{\infty} V^i \Lambda_{i+1}\phi \\ &= \sum_{i=0}^{\infty} V^i \left(\Lambda_0^{\sigma^{i+1}} C_i + p\Lambda_{i+1}\right)\phi. \end{aligned}$$

On the other hand we have:

$$\begin{aligned} F\psi &= \left(\sum_i V^i N_i + \sum_i V^i B_i T\right)\psi \\ &= \left(\sum_i V^i N_i + \sum_i V^i B_i T\right)\left(\sum_j V^j \Lambda_j\right)\phi \\ &= \left(\sum_m V^m \left(\sum_{i+j=m} N_i^{\sigma^j}\Lambda_j\right) + \left(\sum_i V^i B_i T\right)\Lambda_0\right)\phi \\ &= \sum_m V^m \left(\sum_{i+j=m}\left(N_i^{\sigma^j}\Lambda_j\right) + pB_m\Lambda_0 - \sum_{i+j=m-1}\left(B_i^{\sigma^{j+1}}\Lambda_0^{\sigma^{j+1}}C_j\right)\right)\phi \end{aligned}$$

Comparing the coefficients of V^m in the above two expressions for $F\psi$, we obtain by unicity the following equation:

$$\Lambda_0^{\sigma^{m+1}}C_m + p\Lambda_{m+1} = \sum_{i+j=m}\left(N_i^{\sigma^j}\Lambda_j\right) + pB_m\Lambda_0 - \sum_{i+j=m-1}\left(B_i^{\sigma^{j+1}}\Lambda_0^{\sigma^{j+1}}C_j\right). \qquad 5.4.1$$

5.5 Thus the problem of classifying d-dimensional commutative formal group laws G over k up to isomorphism boils down to: given an arbitrary commutative formal group law G over $W(k)$, i.e., an arbitrary set

$$C = \{C_i | i \geq 0\}$$

of matrices in $M_d(W(k))$, determine the sets

$$\Lambda = \{\Lambda_i | i \geq 0\}, B = \{B_i | i \geq 0\}$$

of matrices in $M_d(W(k))$ with Λ_0 invertible, such that the set $N = \{N_i | N_i = \tau(\bar{N}_i), i \geq 0\}$, satisfying (5.4.1) is "as nice as possible". The notion "as nice as possible" will be specified in theorem 5.17.

5.6 From now on we will consider only strong isomorphisms, so we take $\Lambda_0 = I_d$. We also assume that G has finite height h.

5.7 We may and will assume that our formal group law G has F-type $F = \sum_i V^i C_i$ where the C_i satisfy the jump data $(\gamma, (h_i; r_i; A_i), U)$ of theorem 4.3.

5.8 Multiplying the system of equations (5.4.1) by U from the left we obtain the system of equations Eq_m:

$$c_m + pU\lambda_{m+1} = \sum_{i+j=m}\left(n_i^{\sigma^j}\lambda_j\right) + pb_m U - \sum_{i+j=m-1}\left(b_i^{\sigma^{j+1}}c_j\right).$$

Here we have put

$$\lambda_j = \Lambda_j, c_j = UC_j, b_j = UB_jU^{-1}, n_j = UN_j.$$

Note first that we have used that U, being a permutation matrix, is invariant under σ, and in the second place that the $c_j = c_{j,1}$ have the properties of theorem 4.3.

5.9 Some more notations. For any matrix $A \in M_d(k)$ we define the following partition:

$$A = \begin{pmatrix} A_{\mathrm{I}} & A_{\mathrm{II}} \\ A_{\mathrm{III}} & A_{\mathrm{IV}} \end{pmatrix}, \qquad A_{\mathrm{I}} \in M_{r_1}(k), \qquad A_{\mathrm{IV}} \in M_{g_2}(k).$$

The matrix relation $AB = C$ then, of course, implies

$$C_{\mathrm{I}} = A_{\mathrm{I}}B_{\mathrm{I}} + A_{\mathrm{II}}\, B_{\mathrm{III}}\,,$$

etc.

5.10 We start by solving (see 5.10.1) the equations $\mathsf{Eq}_m\mathsf{modp}$ over k. Here $\mathsf{Eq}_m\mathsf{modp}$ is defined as:

$$\bar{c}_m = \sum_{i+j=m} \bar{n}_i^{p^j} \bar{\lambda}_j - \sum_{i+j=m-1} \bar{b}_i^{p^{j+1}} \bar{c}_j, \qquad 5.10.0.1$$

with $\bar{c}_j := \pi(c_j) \in k$ and where $\bar{b}_\bullet, \bar{n}_\bullet, \bar{\lambda}_\bullet$ are considered as variables (in which we will later express the $\lambda_\bullet, b_\bullet$ and $n_\bullet$).

5.10.1 Write $h_\Sigma := \sum_{i=2}^{\gamma} h_i$. Solving (5.10.0.1) will mean constructing solutions $\bar{n}_m, \bar{\lambda}_m \in M_d(k[\bar{b}_l^p]_{l<h_\Sigma+m})$ of (5.10.0.1) such that $\bar{n}_m =: \bar{n}_{m,1}$ has the following form (under the notations of theorem 4.3):

$$\begin{aligned} \bar{n}_{m,i} &= \begin{pmatrix} * & 0_{g_i} \end{pmatrix}, && m < h_i, \\ \bar{n}_{h_i,i} &= \begin{pmatrix} * & \bar{A}_i & 0 \\ * & * & 0_{g_{i+1}} \end{pmatrix}, && \bar{A}_i := \pi(A_i), \end{aligned}$$

and

$$\bar{n}_{m,i} = \begin{pmatrix} 0_{r_i} & 0 \\ \bar{n}_{m-h_i,i+1} \end{pmatrix}, \qquad m > h_i.$$

5.10.2 We will prove the existence of such $\bar{n}_m, \bar{\lambda}_m$ by induction on γ, the number of blocks. We will refer to this induction as the *main induction.*

5.10.3 For $\gamma = 1$ the proof is easy:

In fact, $\gamma = 1$ means that $\bar{c}_m = 0$ for $m < h_1$ or $m > h_1$, while $\bar{c}_{h_1} = \bar{A}_1 \in Gl_d(k)$. We therefore find with an easy induction that $\bar{n}_m = \bar{c}_m$ for $m \leq h_1$. For $m > 0$ the equation $\mathsf{Eq}_{h_1+m}\mathsf{modp}$ is read as:

$$\bar{c}_{h_1+m} = \bar{n}_{h_1+m} + \sum_{i+j=m, i,j\neq 0} \bar{n}^{p^j}_{h_1+i}\bar{\lambda}_j + \bar{n}^{p^m}_{h_1}\bar{\lambda}_m - \bar{b}^{p^{h_1+1}}_{m-1}\bar{c}_{h_1}.$$

We conclude that we may choose $\bar{\lambda}_m \in k[\bar{b}^p_l]_{l<m}$ such that $\bar{n}_{h_1+m} = 0$.

5.10.4 So assume that we can solve (5.10.0.1) for all commutative formal group laws having less than γ blocks (for some $\gamma > 1$) and assume next the number of blocks to be γ.

5.10.5 Consider the equations (5.10.0.1). For $m \leq h_1$ we find as in 5.10.3

$$\bar{n}_m = \bar{c}_m = 0, m < h_1 \text{ and } \bar{n}_{h_1} = \bar{c}_{h_1} = \begin{pmatrix} \bar{A}_1 & 0 \\ * & 0 \end{pmatrix}. \qquad 5.10.5.1$$

5.10.6 Now for $m \geq 0$ consider the equation $\mathsf{Eq}_{m+h_1}\mathsf{modp}$. We will use another induction in order to find $\bar{\lambda}_{m\mathrm{I}}$ such that $\bar{n}_{h_1+m\mathrm{I}} = 0$ and also $\bar{\lambda}_{m\mathrm{II}}$ such that $\bar{n}_{h_1+m\mathrm{II}} = 0$. Assume we have proven this up to $h_1 + m$ then by (5.10.5.1):

$$\bar{c}_{h_1+m\mathrm{I}} = \sum_{i+j=m} \left(\bar{n}^{p^j}_{h_1+i\mathrm{I}}\bar{\lambda}_{j\mathrm{I}} + \bar{n}^{p^j}_{h_1+i\mathrm{II}}\bar{\lambda}_{j\mathrm{III}}\right) - \sum_{i+j=m-1} \left(\bar{b}^{p^{h_1+j+1}}_{i\ \mathrm{I}}\bar{c}_{h_1+j\mathrm{I}} + \bar{b}^{p^{h_1+j+1}}_{i\ \mathrm{II}}\bar{c}_{h_1+j\mathrm{III}}\right).$$

Using the inductive hypotheses, the jump data, $\bar{\lambda}_{0\mathrm{I}} = I_{r_1}$, $\bar{\lambda}_{0\mathrm{III}} = 0$ and $\bar{n}_{h_1\mathrm{I}} = \bar{A}_1$ we see:

$$\bar{c}_{h_1+m\mathrm{I}} = \bar{n}_{m+h_1\mathrm{I}} + \bar{A}^{p^m}_1\bar{\lambda}_{m\mathrm{I}} - \bar{b}^{p^{h_1+1}}_{m-1\ \mathrm{I}}\bar{A}_1 - \sum_{i+j=m-1} \bar{b}^{p^{h_1+j+1}}_{i\ \mathrm{II}}\bar{c}_{h_1+j\mathrm{III}}.$$

So we may choose $\bar{\lambda}_{m\mathrm{I}} \in M_{r_1}(k[\bar{b}^p_l]_{l<m})$ such that $\bar{n}_{m+h_1\mathrm{I}} = 0$. Also:

$$\bar{c}_{h_1+m\mathrm{II}} = \sum_{i+j=m} \left(\bar{n}^{p^j}_{h_1+i\mathrm{I}}\bar{\lambda}_{j\mathrm{II}} + \bar{n}^{p^j}_{h_1+i\mathrm{II}}\bar{\lambda}_{j\mathrm{IV}}\right) - \sum_{i+j=m-1} \left(\bar{b}^{p^{h_1+j+1}}_{i\ \mathrm{I}}\bar{c}_{h_1+j\mathrm{II}} + \bar{b}^{p^{h_1+j+1}}_{i\ \mathrm{II}}\bar{c}_{h_1+j\mathrm{IV}}\right).$$

Again using the inductive assumptions and the jump data we find:

$$0 = \bar{A}^{p^m}_1\bar{\lambda}_{m\mathrm{II}} + \bar{n}_{m+h_1\mathrm{II}} - \sum_{i+j=m-1} \bar{b}^{p^{h_1+j+1}}_{i\ \mathrm{II}}\bar{c}_{h_1+j\mathrm{IV}}.$$

So again we may choose $\bar{\lambda}_{m\mathrm{II}} \in M_{r_1\times(n-r_1)}(k[\bar{b}_l^p]_{l<m})$ such that $\bar{n}_{m+h_1\mathrm{II}} = 0$, explicitly ($m \geq 0$):

$$\bar{\lambda}_{m\mathrm{II}} = \bar{A}_1^{-p^m}\left(\sum_{i+j=m-1} \bar{b}_i^{p^{h_1+j+1}}{}_{\mathrm{II}}\, \bar{c}_{h_1+j\mathrm{IV}}\right). \qquad 5.10.6.1$$

5.10.7 From this last relation we even see that for $0 \leq m \leq h_2$ we have $\bar{\lambda}_{m\mathrm{II}} = 0$, since for $0 \leq m < h_2$ the jump data ($c_{m,2} \equiv (*\,0_{g_2}) \bmod p$ for $0 \leq m < h_2$) gives that $\bar{c}_{h_1+m\mathrm{IV}} = 0$. Considering $\mathsf{Eq}_{m+h_1}\mathsf{mod}\mathsf{p}_{\mathrm{IV}}$:

$$\bar{c}_{h_1+m\mathrm{IV}} = \sum_{i+j=m}\left(\bar{n}_{h_1+i\mathrm{III}}^{p^j}\,\bar{\lambda}_{j\mathrm{II}} + \bar{n}_{h_1+i\mathrm{IV}}^{p^j}\,\bar{\lambda}_{j\mathrm{IV}}\right) - \sum_{i+j=m-1}\left(\bar{b}_i^{p^{h_1+j+1}}{}_{\mathrm{III}}\,\bar{c}_{h_1+j\mathrm{II}} + \bar{b}_i^{p^{h_1+j+1}}{}_{\mathrm{IV}}\,\bar{c}_{h_1+j\mathrm{IV}}\right),$$

we now conclude that $\bar{n}_{m+h_1\mathrm{IV}} = 0$, ($0 \leq m < h_2$) and $\bar{n}_{h_1+h_2\mathrm{IV}} = \bar{c}_{h_1+h_2\mathrm{IV}}$ (contrary to what happens in the III-part below, as the reader will see).

5.10.8 Up to this point we have found $\bar{\lambda}_{m\mathrm{I}}, \bar{\lambda}_{m\mathrm{II}}, \bar{n}_{m\mathrm{I}}, \bar{n}_{m\mathrm{II}}$ for all $m \geq 0$, $\bar{n}_{m\mathrm{III}}$ for $0 \leq m < h_1$ and $\bar{n}_{m\mathrm{IV}}$ for $m \leq h_1 + h_2$ satisfying 5.10.1. We will now use the main inductive hypothesis to obtain the remaining parts of $\bar{\lambda}_m$ and $\bar{n}_{m+h_1}$.

5.10.9 Again consider for $m \geq 0$ $\mathsf{Eq}_{m+h_1}\mathsf{mod}\mathsf{p}_{\mathrm{IV}}$:

$$\bar{c}_{h_1+m\mathrm{IV}} = \sum_{i+j=m}\left(\bar{n}_{h_1+i\mathrm{III}}^{p^j}\,\bar{\lambda}_{j\mathrm{II}} + \bar{n}_{h_1+i\mathrm{IV}}^{p^j}\,\bar{\lambda}_{j\mathrm{IV}}\right) - \sum_{i+j=m-1}\left(\bar{b}_i^{p^{h_1+j+1}}{}_{\mathrm{III}}\,\bar{c}_{h_1+j\mathrm{II}} + \bar{b}_i^{p^{h_1+j+1}}{}_{\mathrm{IV}}\,\bar{c}_{h_1+j\mathrm{IV}}\right).$$

Inductively define matrices $c'_m, m \geq 0$ by:

$$c'_m := \bar{c}_{h_1+m\mathrm{IV}} - \sum_{i+j=m}\bar{n}_{h_1+i\mathrm{III}}^{p^j}\,\bar{A}_1^{-p^j}\left(\sum_{k+l=j-1}\bar{b}_k^{p^{l+h_1+1}}{}_{\mathrm{II}}\,\bar{c}_{l+h_1\mathrm{IV}}\right) + \sum_{i+j=m-1}\bar{b}_i^{p^{j+h_1+1}}{}_{\mathrm{IV}}\,\bar{c}_{h_1+j\mathrm{IV}} - \sum_{i+j=m-1}\bar{b}_i^{p^{j+h_1+1}}{}_{\mathrm{IV}}\,c'_j. \qquad 5.10.9.1$$

Let $x \leq d$ be a natural number. We see from (5.10.9.1) that if the last x columns of $\bar{c}_{h_1+l\mathrm{IV}}$ are zero ($l \leq m$) then so are the last x columns of c'_m. Therefore we may even conclude that the jump data of $\{c'_m\}_{m\geq 0}$ are equal to the jump data of $\{c_{h_1+m\mathrm{IV}}\}_{m\geq 0}$. Notice further that the number of blocks of $\{c'_m\}_{m\geq 0}$ is $\gamma - 1$. Using $\bar{c}_{j\mathrm{II}} = 0$ for all $j \geq 0$ and formulae (5.10.9.1) with (5.10.6.1) we rewrite $\mathsf{Eq}_m\mathsf{mod}\mathsf{p}_{\mathrm{IV}}$ as:

$$c'_m = \sum_{i+j=m}\bar{n}_{h_1+i\mathrm{IV}}^{p^j}\,\bar{\lambda}_{j\mathrm{IV}} - \sum_{i+j=m-1}\bar{b}_i^{p^{j+h_1+1}}{}_{\mathrm{IV}}\,c'_j. \qquad 5.10.9.2$$

Comparing $\mathsf{Eq}_m\mathsf{modp}$ with (5.10.9.2) we see that we may use the inductive hypothesis of the main induction in order to solve (5.10.9.2) (in the sense of 5.10.1) as a polynomial function of $\bar{b}_l^p, l \leq h_\Sigma + m$ and $\bar{n}_{l\mathrm{III}}, l < h_1 + m$.

5.10.10 We are left with $\mathsf{Eq}_{m+h_1}\mathsf{modp}_{\mathrm{III}}$:

$$\bar{c}_{h_1+m\mathrm{III}} = \sum_{i+j=m} \left(\bar{n}_{h_1+i\mathrm{III}}^{p^j} \bar{\lambda}_{j\mathrm{I}} + \bar{n}_{h_1+i\mathrm{IV}}^{p^j} \bar{\lambda}_{j\mathrm{III}} \right) - \sum_{i+j=m-1} \left(\bar{b}_i^{p^{h_1+j+1}}{}_{\mathrm{III}} \bar{c}_{h_1+j\mathrm{I}} + \bar{b}_i^{p^{h_1+j+1}}{}_{\mathrm{IV}} \bar{c}_{h_1+j\mathrm{III}} \right).$$

Replacing $\bar{n}_{h_1+i\mathrm{IV}}$ by the polynomial function we obtained in subsubsection 5.10.9 we conclude that $\bar{n}_{h_1+m\mathrm{III}} \in k[\bar{b}_l^p]_{l<h_\Sigma+m}$ and that from the moment we find an invertible subblock along the main diagonal in $\bar{n}_{h_1+i\mathrm{IV}}^{p^j}$ we may choose the corresponding rows in $\bar{\lambda}_{m\mathrm{III}}$ such that those rows are zero in $\bar{n}_{h_1+m+i\mathrm{III}}$.
This concludes the main induction.

5.11 Having found a set of $\bar{n}_m \in M_d(k[\bar{b}_l^p]_{l<h_\Sigma+m})$ solutions of $\mathsf{Eq}_m\mathsf{modp}$ (5.10.0.1), we want to lift these to construct solutions $n_\bullet \in M_d(\tau(k))$ of Eq_m (see 5.8).

5.12 We define

$$n_m := \tau(\bar{n}_m), \lambda_m := \tau(\bar{\lambda}_m) \in M_d(W(k[\bar{b}_l^p]_{l<h_\Sigma+m}))$$

and

$$b_m = \tau(\bar{b}_m) + Vb_m^{\#} \in M_d(W(k[\bar{b}_l]_{l\leq m}^{\text{ét}})),$$

where the $b_m^{\#} \in M_d(W(k[\bar{b}_l]_{l\leq m}^{\text{ét}}))$ are yet to be determined.

5.13 We will first rewrite (5.8). Note that since $\pi(\lambda_\bullet), \pi(n_\bullet), \pi(b_\bullet)$ are solutions of (5.10.0.1) we have:

$$\mathcal{T}_m := c_m - \sum_{i+j=m} n_i^{\sigma^j} \lambda_j + \sum_{i+j=m-1} b_i^{\sigma^{j+1}} c_j \in M_d\left(\mathsf{V}W(k[\bar{b}_i^p]_{i<m})\right).$$

Define x'_m by $\mathsf{V}x'_m = \mathcal{T}_m$. Then Eq_m becomes:

$$\mathsf{VF}b_mU - \mathsf{VF}U\lambda_{m+1} = \mathsf{V}x'_m.$$

Here we have used that the characteristic of $k[\bar{b}_\bullet]$ is p, so $\mathsf{VF} = \mathsf{FV} = p$ on $W(k[\bar{b}_\bullet])$. Since V is injective (on any Witt ring) we find:

$$\mathsf{F}b_mU - \mathsf{F}U\lambda_{m+1} = x'_m.$$

In view of $x'_m \in M_d(W(k[\bar{b}_i^p]_{i<m}))$ and k being perfect we may write $x'_m = \mathsf{F}x_m$. Since F is injective we therefore see:

$$\mathsf{Eq}'_m : \qquad b_mU - U\lambda_{m+1} = x_m \in M_d(W(k[\bar{b}_i]_{i<m})),$$

which defines the equations Eq'_m.

5.14 Now consider $\mathsf{Eq}'_m \bmod \mathsf{V}$:

$$\bar{b}_m U - U\bar{\lambda}_{m+1} = \bar{x}_m,$$

where $\bar{x}_m := \pi(x_m) \in M_d\left(k[\bar{b}_i]_{i<m}\right)$.

5.14.1 For $m = 0$ we have:

$$\bar{b}_0 U = \bar{x}_0 + U\bar{\lambda}_1 \in M_d\left(k[\bar{b}_i^p]_{0\le i\le h_\Sigma}\right),$$

(because $\bar{x}_0 \in M_d(k)$) which gives by the Jacobi criterion (or by lemma 3.2):

$$\bar{b}_0 \in M_d\left(k[\bar{b}_i^p]^{\text{ét}}_{1\le i\le h_\Sigma}\right).$$

By lemma 3.1 we have a solution

$$b_0 \in M_d\left(W(k[\bar{b}_0]^{\text{ét}})\right) \subset M_d\left(W(k[\bar{b}_i^p]^{\text{ét}}_{1\le i\le h_\Sigma})\right)$$

of Eq_0 such that $\pi(b_0) = \bar{b}_0$.

5.14.2 Next assume we have found $\bar{b}_i \in M_d\left(k[\bar{b}_l^p]^{\text{ét}}_{m\le l\le m+h_\Sigma}\right)$ for $i < m$, such that there are solutions $b_i \in M_d\left(W(k[\bar{b}_j]^{\text{ét}}_{j\le i})\right)$ of Eq'_l $(i, l < m)$. Then consider $\mathsf{Eq}'_m \bmod \mathsf{V}$:

$$\bar{b}_m U = \bar{x}_m + U\bar{\lambda}_{m+1} \in M_d\left(k[\bar{b}_i^p]^{\text{ét}}_{m\le i\le m+h_\Sigma}\right),$$

which gives by lemma 3.2

$$\bar{b}_m \in M_d\left(k[\bar{b}_i^p]^{\text{ét}}_{m+1\le i\le m+h_\Sigma}\right).$$

So by lemma 3.1 we have a solution

$$b_m \in M_d\left(W(k[\bar{b}_i]^{\text{ét}}_{i\le m})\right) \subset M_d\left(W(k[\bar{b}_i^p]^{\text{ét}}_{m+1\le i\le m+h_\Sigma})\right)$$

of Eq_m such that $\pi(b_m) = \bar{b}_m$.

5.15 Put $\mathbb{B}_m = k[\bar{b}_i]_{i\le m} \subset k[\bar{b}_i^p]^{\text{ét}}_{m+1\le i\le m+h_\Sigma}$. Then we have found an inductive system:

$$\mathbb{B}_0 \to \mathbb{B}_1 \to \cdots \to \varinjlim \mathbb{B}_n =: \mathbb{B}$$

Since the transcendence degree of all $\mathbb{B}_m \le n^2 h_\Sigma$ we also have that the transcendence degree of $\mathbb{B} \le n^2 h_\Sigma$. Denote the transcendence degree of $\mathbb{B}$ by $tr_{\mathbb{B}}$. We write $\bar{b}_{m,i,j}$ for the image of $\bar{b}_{m,i,j}$ in $\mathbb{B}$.

5.16 From now on we assume that k is algebraically closed. So we have ring homomorphisms $\mathbb{B} \to k$, determined by the choice of the first (in the lexicographic order) $tr_{\mathbb{B}}$ transcendental $\bar{b}_{m,i,j}$. This means that at last we have found solutions $b_m \in M_d(\tau(k))$ for the equations Eq'_m or equivalently for the equations Eq_m. Summarizing, we have proven the following theorem.

5.17 Theorem. *Let $\bar{G}$ be a formal group law of finite height defined over an algebraically closed field k of positive characteristic p. Then $\bar{G}$ is isomorphic to a formal group law $\bar{G}_{typ}$ which has a finite (Witt) F-type.*
More in detail: Let G be a lifting of $\bar{G}$ to $W(k)$. Let the jump data of G be $(\gamma, (h_i; r_i; A_i), U)$ as defined in theorem 4.3. Then $\bar{G}_{typ}$ has an F-type of the form $F = \sum V^i[\bar{N}_i]$, where the $n_{m,1} = U\bar{N}_m$ are described inductively by matrices $n_{m,i} \in M_{g_i \times n}(k)$ as follows:

$$
\begin{aligned}
n_{m,i} &= \begin{pmatrix} * & 0_{g_i} \end{pmatrix} && m < h_i, \\
n_{h_i,i} &= \begin{pmatrix} * & \bar{A}_i & 0 \\ * & * & 0_{g_{i+1}} \end{pmatrix}, && \bar{A}_i \in Gl_{r_i}(k)
\end{aligned}
$$

and

$$
n_{m,i} = \begin{pmatrix} 0_{r_i} & 0 \\ n_{m-h_i,i+1} \end{pmatrix} \qquad m > h_i,
$$

Moreover the jump data is invariant under reduction in the following sense: if G' is any formal group law over $W(k)$ which reduces to $\bar{G}$ and has jump data $(\gamma', (h'_i; r'_i; A'_i), U)$ then $(\gamma', (h'_i; r'_i; \bar{A}'_i), U) = (\gamma, (h_i; r_i; \bar{A}_i), U)$.

5.18 In view of the above theorem we may define the jump data (and jump sequence) of a formal group law $\bar{G}$ defined over a field of positive characteristic in the following obvious way: Let G be any lift of $\bar{G}$, having jump data $(\gamma, (h_i; r_i; A_i), U)$ then the jump data of $\bar{G}$ are defined by $(\gamma, (h_i; r_i; \bar{A}_i), U)$.
Using chapter I, lemma 4.26, which links the height of a formal group law with its jump sequence, we have the following corollary.

5.19 Corollary. *There is a catalogue of finite dimension over k for all formal group laws G defined over an algebraically closed field k of positive characteristic such that the height of G is bounded by a fixed number.*

5.20 Remark. The catalogue given by the above theorem, however, does not give a complete classification.

5.20.1 For example if $\bar{G}$ has jump data $\left(\gamma, (h_i; r_i; \bar{A}_i), U\right)$ such that U is the identity matrix, then $\bar{G}$ is actually isomorphic to a direct sum of 1-dimensional formal

group laws. This is most easily proven as follows: Since U is the identity matrix we have that the stable rank (see [HaW]) of $c_{h_1,1}$ is r_1, but then we may apply [Kne], Theorem 1.10.3 in order to find an isomorphism $G \cong (G_{1,h_1})^{r_1} \oplus G'$. Using property 4.6 we conclude that the jump data of G' must be $(\gamma-1, (h_i'; r_i'; \bar{A}_{i+1}), \mathsf{Id})$, with $h_1' = h_1 + h_2, h_i' = h_{i+1}$ for $i > 1$ and $r_i' = r_{i+1}$ for $i \geq 1$. By an obvious induction we are done.

5.20.2 As another example we may consider the 2-dimensional formal group laws, and compare the catalogue with the complete classification given in chapter IV, section 1. Assume that U is not the identity and $\gamma = 2$. Then we find by theorem 5.17 $\bar{G}_{typ}$ has an F-type of the form

$$F\phi = V^{h_1}\begin{pmatrix} 0 & 0 \\ \alpha_1 & 0 \end{pmatrix} + \sum_{l=d}^{h_2-1} V^{h_1+l}\begin{pmatrix} a_{h_1+l} & 0 \\ 0 & 0 \end{pmatrix} + V^{h_1+h_2}\begin{pmatrix} 0 & \alpha_2 \\ 0 & 0 \end{pmatrix},$$

for some $0 \leq d \leq h_2$, $\alpha_\bullet, a_{h_1+d} \in \tau(k^*)$, and $a_\bullet \in \tau(k)$. While the result of chapter IV, theorem 1.7 is that in this case a classification is given by the F-types

$$F\phi = V^{h_1}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \sum_{l=d}^{\min\{2d,h_2-d\}-1} V^{h_1+l}\begin{pmatrix} a_{h_1+l} & 0 \\ 0 & 0 \end{pmatrix} + V^{h_1+h_2}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

for some $0 < d < h_2$, $a_{h_1+d} \in \tau(k^*)$, and $a_\bullet \in \tau(k)$. Here the $a_\bullet$ still have to be taken modulo the action of some finite group. So clearly there is a lot of redundancy in our catalogue.

5.21 Consider example 2.8. The finite Hilbert F-type of G is in normal form in the sense of theorem 4.1 and has jump data $(1, (0; d; (1+p)\mathsf{Id}), \mathsf{Id})$. Thus the reduction $\bar{G}$ is by theorem 5.17 isomorphic over the algebraic closure $\bar{k}$ of k to $\bar{G}_{typ}$ having jump data $(1, (0; d; \mathsf{Id}), \mathsf{Id})$ and F-type $F\phi_{\bar{G}_{typ}} = \mathsf{Id}\,\phi_{\bar{G}_{typ}}$. This is in accordance with [SPM], proposition 3.7 or [Dit89], theorem 6 —both proofs are not complete, but may be merged to obtain a complete proof— since these propositions imply that over $W(\bar{k})$ the formal group law G is isomorphic to the d-dimensional multiplicative formal group law.

Chapter 4

Some applications

In this chapter we will refer to chapter III, theorem 5.17 as the *finiteness theorem.* As before all formal group laws will be considered to be commutative and curvilinear. In this chapter the following applications will be treated:

Starting with the catalogue in the 2-dimensional case we give a complete classification of all 2-dimensional commutative formal group laws (section 1). Thus we rediscover the classification given for this dimension by Manin ([Man]) and Kneppers ([Kne]).

In the 2 and 3-dimensional case we compute the isogeny types as function of the parameters in our catalogue (sections 2 and 3).

In the 3-dimensional case we will also determine which formal group laws may arise as the completion of an abelian variety (section 3).

The last three sections will be devoted to describing the structure (of the isomorphism classes) of formal Brauer groups of Fermat hypersurfaces defined over an algebraically closed field of positive characteristic. In section 4 the p-adic Gamma function is introduced. The Serre-Witt cohomology of the Fermat hypersurfaces and the connection with the F-types of the formal Brauer groups are presented in section 5. Section 6 then gives the normalized F-types of the formal Brauer groups which represent the isomorphism classes.

In the appendix the decomposition of the formal Brauer group of the Fermat hypersurface corresponding to the affine equation $X^{19} + Y^{19} + Z^{19} = 1$ over $\bar{\mathbb{F}}_5$ is given.

An application which will not be treated here, is another proof for the two finiteness theorems of Manin [Man]. These are corollaries to the finiteness theorem.

1 The classification in dimension 2

We will give a full classification up to isomorphism of 2-dimensional formal group laws of finite height defined over an algebraically closed field k of positive characteristic p. We thus discover the classification for such formal group laws given by Kneppers in [Kne]. We will repeat most of the proof of the finiteness theorem for this special case, and then perform some ad hoc computations to obtain the full classification.

1.1 In this section G will be a 2-dimensional curvilinear p-typical formal group law of finite height defined over an algebraically closed field k of positive characteristic p. Almost all F-types in this section will be Witt F-types; we therefore omit all Witt brackets [ ]. We also omit the canonical curves in the notation for an F-type. A sum of the form $\sum_a^b$ with $a > b$ will be considered zero.

1.2 In the 2-dimensional case we have two possibilities for the 2×2 permutation matrix U appearing in the finiteness theorem. The case $U = \mathsf{Id}$ corresponds to G being a direct sum of two 1-dimensional formal group laws (cf. chapter III, remark 5.20). In this case, as is well known, the only isomorphism invariants are the heights of the 1-dimensional components.

1.3 Thus assume $U \neq \mathsf{Id}$, then by the finiteness theorem G is isomorphic to a formal group law G_{typ} having normalized F-type:

$$F = V^{h_1}\begin{pmatrix} a_{h_1} & 0 \\ \alpha_1 & 0 \end{pmatrix} + \sum_{l=d}^{h_2-1} V^{h_1+l}\begin{pmatrix} a_{h_1+l} & 0 \\ 0 & 0 \end{pmatrix} + V^{h_1+h_2}\begin{pmatrix} a_{h_1+h_2} & \alpha_2 \\ 0 & 0 \end{pmatrix}, \quad 1.3.1$$

where $a_\bullet, \alpha_\bullet \in k$, and $a_{h_1+d}, \alpha_\bullet \neq 0, 0 < d \leq h_2$. Then the height h is given by $h = 2h_1 + h_2 + 2$ (see chapter I, lemma 4.26).

1.4 Lemma. *Let G have normalized F-type*

$$F\phi_G = \sum_{i \geq 0} V^i C_i \phi_G \quad 1.4.2$$

as in (1.3.1). If G is not isomorphic to a direct sum of two lower-dimensional formal group laws (we will say that G is non-split*), then we may moreover assume that*

$$C_{h_1} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ and } C_{h_1+h_2} = \begin{pmatrix} a_{h_1+h_2} & 1 \\ 0 & 0 \end{pmatrix}.$$

proof: By [Kne], theorem 1.10.3 G is split if the stable rank of C_{h_1} is non-zero, thus $a_{h_1} = 0$. Now normalize C_{h_1} à la Hasse and Witt ([HaW], Satz 11). This gives that C_{h_1} has the desired form, but the other non-zero C_j may be changed.

We therefore again apply the finiteness theorem (which does not change the first non-zero matrix). Now let $\lambda_{1,1}, \lambda_{2,2}$ be solutions in k of

$$\lambda_{2,2}^{p^{h_1+1}} = \lambda_{1,1}, \quad \alpha_2' \lambda_{1,1}^{p^{h_1+h_2+1}} = \lambda_{2,2};$$

then $\psi = [\Lambda]\phi_G, \Lambda_{i,j} := \delta_{i,j}\lambda_{i,j}$ is an isomorphism which does not change the shape of the first $h_1 + h_2$ matrices of the F-type but normalizes $C_{h_1+h_2}$. □

We may now prove the following theorem.

1.5 Theorem. *(first version) Any 2-dimensional non-split formal group law G of finite height h defined over an algebraically closed field k of positive characteristic is isomorphic to a p-typical formal group law G_{typ} with F-type:*

$$F = V^{h_1}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \sum_{l=d}^{\min\{2d,h_2\}} V^{h_1+l}\begin{pmatrix} a_{h_1+l} & 0 \\ 0 & 0 \end{pmatrix} + V^{h_1+h_2}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

with $a_\bullet \in k, a_{h_1+d} \neq 0, d > 0$. Furthermore a formal group law G'_{typ} having F-type

$$F = V^{h_1}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \sum_{l=d}^{\min\{2d,h_2\}} V^{h_1+l}\begin{pmatrix} f_{h_1+l} & 0 \\ 0 & 0 \end{pmatrix} + V^{h_1+h_2}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

(with $f_\bullet \in k, f_{h_1+d} \neq 0, d > 0$) is strongly isomorphic to G_{typ} if and only if there are $\beta_i \in \mathbb{F}_{p^h}, 0 < i \leq \min\{d, h_2 - d\}$ such that

$$f_m + \sum_{i=h_1+d} f_i^{p^{m-i}} \beta_{m-i} = a_m + \sum_{i=h_1+d} a_i \beta_{m-i}^{p^{i+1}}$$

for $h_1 + d \leq m \leq h_1 + 2d$. (For the height h we have $h = 2h_1 + h_2 + 2$.)

proof: Assume that G has an F-type as given by lemma 1.4. Denote the F-type of G_{typ} by $F = \sum_{i\geq 0} V^i N_i$. We follow the proof of the finiteness theorem. Thus let $\tilde{G}$ be a lifting of G with Hilbert F-type $F = \sum V^i\{\tau(C_i)\}$. Now we first have to solve the equations $\mathsf{Eq}_m\mathsf{modp}$ in $M_2(k[b_\bullet])$, which in this case are given by:

$$c_m = \sum_{i+j=m} n_i^{p^j} \lambda_j - \sum_{i+j=m-1} b_i^{p^{j+1}} c_j$$

($c_i := UC_i$). Solving here means finding $\lambda_\bullet \in M_2(k[b_\bullet])$ such that all $n_i := UN_i$ have the form as claimed in the theorem. As in the proof of the finiteness theorem we find $n_m = c_m$ for $m \leq h_1$, and $n_m = 0$ for $m > h_1 + h_2$. We will use the convention that λ_i, b_i, c_i and n_i are zero if $i < 0$. Then we may rewrite $\mathsf{Eq}_m\mathsf{modp}$ as:

$$c_m = n_{h_1}^{p^{m-h_1}}\lambda_{m-h_1} + \sum_{i=h_1+1}^{h_1+h_2-1} n_i^{p^{m-i}}\lambda_{m-i} + n_{h_1+h_2}^{p^{m-h_1-h_2}}\lambda_{m-h_1-h_2} - b_{m-1-h_1}^{p^{h_1+1}}c_{h_1} - \sum_{j=h_1+d}^{h_1+h_2-1} b_{m-1-j}^{p^{j+1}}c_j - b_{m-1-h_1-h_2}^{p^{h_1+h_2+1}}c_{h_1+h_2}.$$

One easily checks that the solutions of $\mathsf{Eq}_m\mathsf{modp}$ are as follows (We use roman numerals at the right side of the equation to number the equations, and roman numerals at the left side to indicate which equations we have used.)

$$\lambda_{m,1,1} = b_{m-1,1,1}^{p^{h_1+1}} + \sum_{j=h_1+d}^{h_1+h_2} a_j b_{m+h_1-1-j,1,2}^{p^{j+1}} \qquad \text{I}$$

$$\lambda_{m,1,2} = b_{m-1-h_2,1,2}^{p^{h_1+h_2+1}} \qquad \text{II}$$

$$\lambda_{m,2,1} = -\sum_{i=h_1+1}^{h_1+h_2} f_i^{p^{m+h_1+h_2-i}}\lambda_{m+h_1+h_2-i,1,1} + b_{m+h_2-1,2,1}^{p^{h_1+1}} + \sum_{j=h_1+d}^{h_1+h_2-1} a_j b_{m+h_1+h_2-1-j,2,2}^{p^{j+1}} \qquad \text{III}$$

$$\lambda_{m,2,2} = -\sum_{i=h_1+1}^{h_1+h_2} f_i^{p^{m+h_1+h_2-i,1,2}}\lambda_{m+h_1+h_2-i,1,2} + b_{m-1,2,2}^{p^{h_1+h_2+1}} \qquad \text{IV}$$

and (define $f_m := n_{m,2,1}$ for $m \le h_1 + h_2$)

$$f_m = a_m - \sum_{i=h_1+1}^{m-1} f_i^{p^{m-i}}\lambda_{m-i,1,1} + b_{m-h_1-1,2,1}^{p^{h_1+1}} + \sum_{j=h_1+d}^{h_1+h_2-1} a_j b_{m-1-j,2,2}^{p^{j+1}} \qquad \text{V}$$

1.5.3 We now have to solve the equations $\tilde{b}_m = U\tau(\lambda_{m+1})U^{-1} + \tilde{x}_m U^{-1}$ (for $\tilde{b}_\bullet$'s), where $\tilde{b}_m := \tau(b_m) + Vb_m^{\#}$ for some $b_m^{\#} \in W(k[b_\bullet])$ and where $\tilde{x}_m$ is defined by

$$p\tilde{x}_m = c_m - \sum_{i+j=m} \tau(n_i^{p^j})\tau(\lambda_j) + \sum_{i+j=m-1} \tilde{b}_i^{\sigma^{j+1}}\tau(c_j).$$

But recall that it suffices to solve the equations $b_m = U\lambda_{m+1}U^{-1} + x_m U^{-1}$ (for $b_\bullet$'s and where $x_m := \pi(\tilde{x}_m)$). We then see that in our case

$$x_{m,1,1} = x_{m,1,2} = 0. \qquad \text{VI}$$

1.5.4 Using induction we find:

for $m < h_2$:

XI $\qquad x_{m,2,2} = 0,$ VII

II,VII $b_{m,2,1} = \lambda_{m+1,1,2} + x_{m,2,2} = 0,$ VIII

for $m < d$:

XI $x_{m,2,1} = 0,$ IX

I,IX $b_{m,2,2} = \lambda_{m+1,1,1} + x_{m,2,1} = b_{m,1,1}^{p^{h_1+1}},$ X

V,VIII $f_{m+h_1} = a_{m+h_1} - \sum_{i=1}^{m-1} f_{i+h_1}^{p^{m-i}} \lambda_{m-i,1,1} + b_{m-1,2,1}^{p^{h_1+1}} = 0,$ XI

VI,VIII,XI $b_{m,1,1} = \lambda_{m+1,2,2} + x_{m,1,2} = b_{m,2,2}^{p^{h_1+h_2+1}}.$ XII

1.5.5 From X and XII we conclude that $b_{m,2,2} = b_{m,1,1}^{p^{h_1+1}} \in \mathbb{F}_{p^{2h_1+h_2+2}} = \mathbb{F}_{p^h}$ $(0 \leq m < d)$. Notice that $f_{h_1+d} = a_{h_1+d}$ (V and VIII). The following equation shows that $b_{m,1,2}$ $(0 \leq m < h_2 - 2d)$ can still be chosen freely ($pol(b_{i,j,k})$ denotes a polynomial in $b_{i,j,k}$):

III,VI,XI
$$b_{m,1,2} = \lambda_{m+1,2,1} + x_{m,1,1} = -\sum_{i=h_1+d}^{h_1+h_2} f_i^{p^{m+h_1+h_2+1-i}} \lambda_{m+h_1+h_2+1-i,1,1} + pol(b_{\bullet,2,1}, b_{\bullet,2,2})$$

I
$$= -\sum_{i=d}^{h_2} f_{h_1+i}^{p^{m+h_2+1-i}} \left(b_{m+h_2-i,1,1}^{p^{h_1+1}} + \sum_{j=d}^{h_2} a_{j+h_1} b_{m+h_2-i-j,1,2}^{p^{j+h_1+1}} \right) + pol(b_{\bullet,2,1}, b_{\bullet,2,2})$$

$$= -a_{h_1+d} a_{h_1+d}^{p^{m+h_2+1-d}} b_{m+h_2-2d,1,2}^{p^{h_1+d+1}} + pol(b_{\bullet,1,1}, b_{\bullet,2,1}, b_{\bullet,2,2}, b_{i,1,2})_{i<m+h_2-2d}.$$

For $m \leq h_1 + 2d$ we have:

V,VIII,X $f_m = a_m - \sum_{i=h_1+d}^{m-1} f_i^{p^{m-i}} b_{m-i-1,2,2} + \sum_{j=h_1+d}^{m-1} a_j b_{m-1-j,2,2}^{p^{j+1}}.$ XIII

Notice that if $m \leq h_1 + 2d, h_1 + d \leq i \leq m-1$, then $m - i - 1 \in [0, d\rangle$, so $b_{m,2,2} \in \mathbb{F}_{p^{2h_1+h_2+2}}$. But for $h_1 + 2d < m \leq h_1 + h_2$ we have:

V,VIII $f_m = a_m - \sum_{i=h_1+d}^{m-1} f_i^{p^{m-i}} \lambda_{m-i,1,1} + \sum_{j=h_1+d}^{m-1} a_j b_{m-1-j,2,2}^{p^{j+1}}$

$$\text{I} \qquad = a_m - \sum_{i=h_1+d}^{m-1} f_i^{p^{m-i}} \left(b_{m-i-1,1,1}^{p^{h_1+1}} + \sum_{j=d}^{h_2} a_{j+h_1} b_{m-1-i-j,1,2}^{p^{j+1+h_1}} \right) +$$

$$+ \sum_{j=h_1+d}^{m-1} a_j b_{m-1-j,2,2}^{p^{j+1}}$$

$$= -a_{h_1+d} a_{h_1+d}^{p^{m-1-h_1-d}} b_{m-h_1-2d-1,1,2}^{p^{h_1+d+1}}$$

$$+pol(b_{\bullet,1,1}, b_{\bullet,2,1}, b_{\bullet,2,2}, b_{i,1,2})_{i<m-h_1-2d-1}.$$

So we may choose values for $b_{m-h_1-2d-1,1,2}$ such that $f_m = 0$ $(h_1+2d < m \leq h_1+h_2)$. Therefore we may construct an isomorphism from G to G_{typ}. If G'_{typ} is isomorphic to G_{typ}, then XIII gives the second statement of the theorem. □

Our method gives essentially a classification up to strong isomorphism. (Since we have used as preparation a specially weak isomorphism in lemma 1.4 it isn't a true classification up to strong isomorphism.) In order to give a full classification we have to perform some ad hoc computations which also take all possible weak isomorphisms in effect.

1.6 Lemma. *Let G be a formal group law in the normal form of theorem (1.5). Then there is a (weak) isomorphism $\phi_H = \sum_i V^i[\Lambda_i]\phi_G$ from G to a formal group law H with F-type*

$$F = V^{h_1} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \sum_{l=d}^{\min\{2d,h_2-d\}-1} V^{h_1+l} \begin{pmatrix} \alpha^{p^{h_1+l+1}} \alpha^{-1} a_{h_1+l} & 0 \\ 0 & 0 \end{pmatrix}$$

$$+V^{h_1+h_2} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

where necessarily $\alpha \in \mathbb{F}_{p^h}$.

proof: Use [Kne], chapter II, claim 3.3 for the special case $s = 0, a_{h_1+h_2+h_3} = b_{h_1+h_2} = c_{h_1+h_2+2h_3} = 0$, $d_{h_1+h_2+n} = a_{h_1+\min\{2d,h_2-d\}}$ in order to obtain an isomorphism from G to H' with F-type

$$F = V^{h_1} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \sum_{l=d}^{\min\{2d,h_2-d\}-1} V^{h_1+l} \begin{pmatrix} a_{h_1+l} & 0 \\ 0 & 0 \end{pmatrix}$$

$$+ \sum_{i \geq \min\{2d,h_2-d\}+1} V^i \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} + V^{h_1+h_2} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Using the finiteness theorem we see that we may normalize H' to H'' having the

F-type

$$F = V^{h_1}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \sum_{l=d}^{\min\{2d,h_2-d\}-1} V^{h_1+l}\begin{pmatrix} a_{h_1+l} & 0 \\ 0 & 0 \end{pmatrix} + V^{h_1+h_2}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Any specially weak isomorphism from H'' to H having an F-type of the form

$$F = V^{h_1}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \sum_{l=d}^{\min\{2d,h_2-d\}-1} V^{h_1+l}\begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix} + V^{h_1+h_2}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

necessarily is of the form $\phi_H = \Lambda_0\phi_{H''}$ with

$$\Lambda_0 = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{h_1+h_2+1} \end{pmatrix},$$

with $\alpha \in \mathbb{F}_{p^h}$. Thus H has an F-type of the form as described in the lemma. □

We may now obtain the full classification.

1.7 Theorem. *(final version) Let G be a non-split 2-dimensional formal group law of finite height h defined over an algebraically closed field k of positive characteristic p. Then G is isomorphic to a formal group law G_{typ} with F-type:*

$$F = V^{h_1}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \sum_{l=d}^{\min\{2d,h_2\}-1} V^{h_1+l}\begin{pmatrix} a_{h_1+l} & 0 \\ 0 & 0 \end{pmatrix} + V^{h_1+h_2}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

where $a_\bullet \in k, a_{h_1+d} \neq 0$. Furthermore G_{typ} is isomorphic to a formal group law G'_{typ} with F-type

$$F = V^{h_1}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \sum_{l=d}^{\min\{2d,h_2\}-1} V^{h_1+l}\begin{pmatrix} f_{h_1+l} & 0 \\ 0 & 0 \end{pmatrix} + V^{h_1+h_2}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

($f_\bullet \in k, f_{h_1+d} \neq 0$), if and only if there are $\beta_i \in \mathbb{F}_{p^h} (0 \leq i < \min\{h_2, d\})$, with $\beta_0 \neq 0$ such that

$$\sum_{i=h_1+d} f_i^{p^{m-i}}\beta_{m-i} = \sum_{i=h_1+d} a_i\beta_{m-i}^{p^{i+1}},$$

for $h_1 + d \leq m < h_1 + d + \min\{h_2, d\}$.

proof: Let G and H be in the normal form of lemma 1.6 with parameters $a_\bullet$ and $f_\bullet$. Let $\phi_H = \sum_i V^i\Lambda_i\phi_G$ be an isomorphism from G to H. Then there is an isomorphism $\phi_{H'} = \sum V^i\Lambda'_i\phi_H$ with $\Lambda'_0 = \Lambda_0^{-1}$ such that H' is in the normal form of theorem 1.5 (just take the composition of the special weak isomorphism

$\phi_{H''} = \Lambda_0^{-1}\phi_G$ and the normalization of H'' in the sense of theorem 1.5). Let H' have parameters $f'_\bullet$, then by theorem 1.5 we have:

$$f'_m + \sum_{i=h_1+d} (f'_i)^{p^{m-i}}\beta'_{m-i} = a_m + \sum_{i=h_1+d} a_i(\beta'_{m-i})^{p^{i+1}},$$

for some $\beta'_\bullet \in \mathbb{F}_{p^h}$. Since H is a normalization of H' in the sense of lemma 1.6 we have $f_m = \alpha^{p^{m+1}}\alpha^{-1}f'_m$. Therefore define $\beta_0 = \alpha$ and $\beta_i = \alpha^{p^i}\beta'_i$ for $0 < i < \min\{h_2, d\}$ in order to obtain the assertion. □

1.8 Remark. This classification was already given by Kneppers [Kne], Theorem 2.1.8, who also compared this with the contravariant classification given by Manin ([Man], chapter III, section 8) for the two dimensional case. In order to compare both classifications one should apply the special weak isomorphism $\psi = U\phi$ to our normal form, and our h_1, h_2, d should be replaced by $h_1, h_2 + h_3, h_2$, respectively.

2 Isogeny classes in dimension 2

In [Kne90] Kneppers gives the isogeny classes of 2-dimensional formal group laws defined over an algebraically closed field of positive characteristic and their dependence on the parameters occurring in his normal form (which we discussed in the preceding section).
Using the theory we developed in chapter II, section 7 we will do the same for our normal form. This will turn out to give a substantial reduction in computations. Since the isogeny type does not depend on the "tail" of the F-type, we find the same results,

2.1 Let G be a 2-dimensional formal group law of finite height defined over an algebraically closed field of positive characteristic. Let the jump data of G be $(\gamma, (h_i; r_i; A_i), U)$, and let $\{\phi_1, \phi_2\}$ be a V-basis for $C_p(G)$ such that the F-type of G with respect to this basis has the form as given by the finiteness theorem.

2.2 If G is split, then G is a direct sum of two 1-dimensional formal group laws having height $h_1 + 1$, $h_1 + h_2 + 1$. Thus G has isogeny type $G_{1,h_1} \oplus G_{1,h_1+h_2}$.

2.3 Assume that G is non-split, thus we may assume G has a F-type as described in lemma 1.4. The height h of G then is $2h_1 + h_2 + 2$. Then the following relations hold in $C_p(G)$.

$$\begin{aligned} F\phi_1 &= \sum_{l=d}^{h_2} V^{h_1+l}a_{h_1+l}\phi_1 + V^{h_1+h_2}\phi_2 \\ F\phi_2 &= V^{h_1}\phi_1, \end{aligned}$$

where $a_l \in \tau(k), a_d \neq 0, 0 < d \leq h_2$. This gives

$$F^2\phi_1 = \left(\sum_{l=d}^{h_2-1} pV^{h_1+l-1}a_l + V^{2h_1+h_2} \right) \phi_1.$$

Hence there is a subspace of $C_p(G)$ on which F^2 acts as

$$F^2 = \sum_{l=d}^{h_2} pV^{h_1+l-1}a_l + V^{2h_1+h_2}.$$

Thus after applying V^2 on both sides we find that

$$a := -p^2 + \sum_{l=d}^{h_2-1} pV^{h_1+l+1}a_l + V^{2h_1+h_2+2} = 0$$

on this subspace. Using the notations of chapter II, section 7 we have that $c(a) = h > 0$ and

$$\gamma(a) = \min \left\{ \frac{2}{h}, \frac{1}{h-(h_1+d+1)}, \ldots, \frac{1}{h-(h_1+h_2+1)} \right\}.$$

Notice that $p \nmid a$ and thus we may apply chapter II, lemma 7.8. We conclude that

Case I: If $\gamma(a) = 2/h$, or equivalently if $h_2 - 2d \leq 0$, then G has a 2-dimensional isogeny factor G_{2,h_1+h_2}. Thus G has isogeny type G_{2,h_1+h_2}.

Case II: If $\gamma(a) = 1/(h_1 + h_2 - d + 1)$, or equivalently if $h_2 - 2d > 0$, then G has a 1-dimensional isogeny factor G_{1,h_1+h_2-d}. Since G has dimension 2 and height $2h_1 + h_2 + 2$ the other isogeny factor is necessarily is G_{1,h_1+d}. (But one may also use chapter II, lemma 7.8 to compute $\gamma(y) = 1/(h_1 + d + 1)$, or even compute the action of F^2 on ϕ_2 to find the other 1-dimensional subspace of $C_p(G)_{(V)}$).
We have thus rediscovered [Kne90], summary, pg 313.

2.4 Remark. A (not necessarily commutative) formal group law is called *algebroid* if it arises as the completion of an algebraic group scheme (see [Haz], E4.7 or [Man], chapter I, section 2.2). If a formal group law is algebroid, then any formal group law isogenous to it is also algebroid ([Man], chapter I, proposition 1.6). Algebroid formal group laws arising from connected non-commutative are non-commutative, thus we may restrict ourselves to considering connected commutative algebraic groups. Since any connected commutative algebraic group X over an algebraically closed field (of arbitrary characteristic) contains a connected affine subgroup X_a such that the factor group X/X_a is an abelian variety, it suffices to consider the completions of abelian varieties. (The completion of X_a is isogenous to a direct sum of factors $G_{1,0}$ and $G_{n,\infty}, n \in \mathbb{N}$, all such factors are algebroid.) If the

formal group law G arises from the completion of an abelian variety X, then the height h is equal to $2 \dim X$ Moreover it is a consequence of the Poincaré duality that G is symmetric in the sense that, if G has an isogeny factor $G_{n,m}$, then G also has an isogeny factor $G_{m,n}$. See [Man], chapter IV for details.

Thus in the 2-dimensional case we find that the height h of a (non-split) algebroid formal group law is 4. Then, from $h = 2h_1 + h_2 + 2$ we see that $h_2 = 2, h_1 = 0$. Combining we see that if $d = 0, 1$ we are in case I, the isogeny type is $G_{2,2}$ and thus the formal group is algebroid. If $d \geq 2$, we are in case II, but then the isogeny type is not symmetric and thus the formal group is not algebroid (Actually, $d \geq 2$ is not even possible since $d < h_2 = 2$).

3 The catalogue and isogeny classes for dimension 3

In this section we explicitly describe the catalogue as given by the finiteness theorem in the 3-dimensional case. We derive the isogeny types of all elements in our catalogue and we determine which 3-dimensional formal group laws may arise as the completion of an abelian variety.

3.1 Let G be a 3-dimensional, non-split formal group law of finite height defined over an algebraically closed field k of positive characteristic $p > 0$. As in 1.1 we omit the Witt brackets [ ] and the canonical curves in the notation for an Witt F-type. Then by the finiteness theorem we have the following possibilities for the normalized F-type with respect to a V-basis $\{\phi_1, \phi_2, \phi_3\}$ of $C_p(G)$.

case I:

$$F = V^{h_1}\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} + \sum_{l=h_1+1}^{h_1+h_2} V^l \begin{pmatrix} a_l & b_l & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + V^{h_1+h_2}\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

(define for use in subsection 3.2 $a_{h_1+h_2+1} := b_{h_1+h_2+1} := 1$)

case II:

$$F = V^{h_1}\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \sum_{l=h_1+1}^{h_1+h_2} V^l \begin{pmatrix} a_l & 0 & 0 \\ 0 & 0 & 0 \\ b_l & 0 & 0 \end{pmatrix} + V^{h_1+h_2}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$+ \sum_{l=h_1+h_2+1}^{h_1+h_2+h_3} V^l \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ b_l & c_l & 0 \end{pmatrix} + V^{h_1+h_2+h_3}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

(define for use in subsection 3.2 $a_{h_1+h_2+1} := b_{h_1+h_2+h_3+1} := c_{h_1+h_2+h_3+1} := 1$)

case III:

$$F = V^{h_1}\begin{pmatrix}0&0&0\\1&0&0\\0&0&0\end{pmatrix} + \sum_{l=h_1+1}^{h_1+h_2} V^l \begin{pmatrix}a_l&0&0\\0&0&0\\b_l&0&0\end{pmatrix} + V^{h_1+h_2}\begin{pmatrix}0&0&0\\0&0&0\\0&1&0\end{pmatrix}$$
$$+ \sum_{l=h_1+h_2+1}^{h_1+h_2+h_3} V^l \begin{pmatrix}a_l&c_l&0\\0&0&0\\0&0&0\end{pmatrix} + V^{h_1+h_2+h_3}\begin{pmatrix}0&0&1\\0&0&0\\0&0&0\end{pmatrix},$$

(define for use in subsection 3.2 $b_{h_1+h_2+1} := a_{h_1+h_2+h_3+1} := c_{h_1+h_2+h_3+1} := 1$)

3.2 Define for an F-type as described in one of the cases $d_a \in \mathbb{N}$ by

$$d_a := \min\{l \mid a_l \neq 0\}.$$

We analogously define d_b and d_c. In all three cases we will compute the isogeny type as function of the h_i, d_j.

3.3 Case I: We have that:

$$F^3\phi_1 = \left(\sum_{l=d_a} F^2V^l a_l + \sum_{l=d_b} FV^l b_l^\sigma V^{h_1} + V^{h_1+h_2}V^{h_1}V^{h_1}\right)\phi_1,$$

i.e., there is a subspace of $C_p(G)$ on which

$$a := p^3 - \sum_{l=d_a} p^2V^{l+1}a_l - \sum_{l=d_b} pV^{l+2+h_1}b_l^{\sigma^{h_1+1}} - V^{3h_1+h_2+3} = 0.$$

We will therefore consider $A/aA \hookrightarrow C_p(G)$. It will turn out that R/aR has rank 3 and thus $R/aR \cong C_p(G)_{(V)}$ as $W((V))$-modules.
Using the notations of chapter II, section 7 we have $c(a) := h = 3h_1 + h_2 + 3$ and

$$\gamma(a) = \min\left\{\frac{2}{h-d_a-1}, \frac{1}{h-d_b-2-h_1}, \frac{3}{h}\right\},$$

which leaves us with three subcases:

Case I_a: If $\gamma(a) = 3/h$, or equivalently

$$\begin{aligned} 3h_1 + h_2 - 3d_a &\leq 0,\\ 3h_1 + 2h_2 - 3d_b &\leq 0,\end{aligned}$$

then G has isogeny type $G_{3,h-3}$.

Case I_b: If $\gamma(a) = 2/(h-d_a-1)$, or equivalently

$$\begin{aligned} h_1 + h_2 - 2d_b + d_a &\leq 0,\\ -3h_1 - h_2 + 3d_a &\leq 0,\end{aligned}$$

then G has an isogeny factor $G_{2,h-d_a-3}$ and thus we conclude that G has isogeny type $G_{2,3h_1+h_2-d_a} \ominus G_{1,d_a}$.

Case I_c: If $\gamma(a) = 1/(h - d_b - 2 - h_1)$, or equivalently

$$\begin{aligned} 3h_1 + 2h_2 - 3d_b &\geq 0, \\ h_1 + h_2 + d_a - 2d_b &\geq 0, \end{aligned}$$

then G has an isogeny factor $G_{1,h-d_b-3-h_1}$. With the notations of chapter II, lemma 7.8 we find that

$$\gamma(y) = \min\left\{\frac{2}{d_b + 2 + h_1}, \frac{1}{d_b + 1 + h_1 - d_a}\right\},$$

if $d_b + 1 + h_1 - d_a > 0$, else $\gamma(y) = 2/(d_b + 2 + h_1)$. We end up with the two subsubcases:

Case $\mathrm{I}_{c,1}$: If in addition to the conditions of subcase I_c we have

$$d_b + h_1 - 2d_a \geq 0,$$

then G has isogeny type $G_{1,h-d_b-3-h_1} \oplus G_{1,d_b+h_1-d_a} \oplus G_{1,d_a}$.

Case $\mathrm{I}_{c,2}$: If in addition to the conditions of subcase I_c we have

$$d_b + h_1 - 2d_a < 0,$$

then G has isogeny type $G_{1,h-d_b-3-h_1} \oplus G_{2,d_b+h_1}$.

3.4 Case II: Notice that the height h of G is $3h_1 + 2h_2 + h_3 + 3$. As in Case I we find that $A/aA \hookrightarrow C_p(G)$ where

$$a := p^2 - p\sum_{l=d_a}^{h_1+h_2} V^{l+1}a_l - V^{2h_1+h_2+2}.$$

Then

$$\gamma(a) = \min\left\{\frac{2}{2h_1 + h_2 + 2}, \frac{1}{2h_1 + h_2 + 1 - d_a}\right\},$$

which leaves us with the two subcases

Case II_a: If

$$2h_1 + h_2 - 2d_a \leq 0,$$

then G has an isogeny factor $G_{2,2h_1+h_2}$ and thus we conclude that G has isogeny type $G_{2,2h_1+h_2} \ominus G_{1,h_1+h_2+h_3}$ (since there is an 1-dimensional factor of height $h-c(a)$ left.)

Case II_b: If

$$2h_1 + h_2 - 2d_a \geq 0,$$

then G has isogeny type $G_{1,2h_1+h_2-d_a} \ominus G_{1,d_a} \oplus G_{1,h_1+h_2+h_3}$.

3.5 Case III: Analogously to the preceding cases we find $A/aA \hookrightarrow C_p(G)$ where

$$a := p^3 - \sum_{l=d_a}^{h_1+h_2} p^2 V^{l+1} a_l + \sum_{l=d_c}^{h_1+h_2+h_3} pV^{l+h_1+2} c_l + \sum_{l=d_b}^{h_1+h_2+h_3} pV^{l+h_1+h_2+h_3+2} b_l + V^{3h_1+2h_2+h_3+3}.$$

Then $(h = c(a))$

$$\gamma(a) = \min\left\{\frac{3}{h}, \frac{2}{h-d_a-1}, \frac{1}{h-h_1-d_c-2}, \frac{1}{h-h_1-h_2-h_3-d_b-2}\right\}.$$

We thus have four subcases:

Case III_a: If $\gamma(a) = 3/h$ then G has isogeny type $G_{3,h-3}$.

Case III_b: If $\gamma(a) = 2/(h-d_a-1)$ then G has isogeny type $G_{2,h-d_a-3} \oplus G_{1,d_a}$.

Case III_c: If $\gamma(a) = 1/(h-h_1-d_c-2)$ then G has an isogeny factor $G_{1,h-h_1-d_c-3}$, and with the notations of chapter II, lemma 7.8 we find

$$\gamma(y) = \min\left\{\frac{2}{h_1+d_c+2}, \frac{1}{h_1+d_c-d_a+1}\right\}.$$

Thus we have the two subsubcases

Case $\mathrm{III}_{c,1}$: If $\gamma(y) = 2/(h_1+d_c+2)$ then we conclude that G has the isogeny type $G_{1,2h_1+2h_2+h_3-d_c} \oplus G_{2,h_1+d_c}$.

Case $\mathrm{III}_{c,2}$: If $\gamma(y) = 1/(h_1+d_c-d_a+1)$ then we conclude that G has the isogeny type $G_{1,2h_1+2h_2+h_3-d_c} \oplus G_{1,h_1+d_c-d_a} \oplus G_{1,d_a}$.

Case III_d: If $\gamma(a) = 1/(h-h_1-h_2-h_3-d_b-2)$ then G has an isogeny factor $G_{1,2h_1+h_2-d_b}$, and with the notations of chapter II, lemma 7.8 we find

$$\gamma(y) = \min\left\{\frac{2}{h_1+h_2+h_3+d_b+2}, \frac{1}{h_1+h_2+h_3+d_b-d_a+1}\right\}.$$

Thus we have the two subsubcases

Case $\mathrm{III}_{d,1}$: If $\gamma(y) = 2/(h_1 + h_2 + h_3 + d_b + 2)$ then we conclude that G has the isogeny type $G_{1,2h_1+h_2-d_b} \ominus G_{2,h_1+h_2+h_3+d_b}$.

Case $\mathrm{III}_{d,2}$: If $\gamma(y) = 1/(h_1 + h_2 + h_3 + d_b - d_a + 1)$ then we conclude that G has the isogeny type $G_{1,2h_1+h_2-d_b} \oplus G_{1,h_1+h_2+h_3+d_b-d_a} \oplus G_{1,d_a}$.

3.6 As in the 2-dimensional case we treat de following question: Which 3-dimensional formal group laws are algebroid? By remark 2.4 it suffices to answer the question: Which formal group laws of dimension 3 over k may arise as the completion of an abelian variety, necessarily also of dimension 3?
We first notice that if G arises from the completion of an abelian variety of dimension 3, then it is well-known that the height of G is equal to 6. Moreover, it is a consequence of the Poincaré duality that if G has an isogeny factor $G_{n,m}$ that G then also has an isogeny factor $G_{m,n}$ ($nm \neq 0$) (see [Man], chapter 4, section 3)

3.7 Consider case I. We find that the condition on the height implies that $h_1 = 0, h_2 = 3$. Then we find that the subcases reduce under the symmetry condition to

Case I_a: For $d_a \geq 1, d_b \geq 2$ the isogeny type of G is $G_{3,3}$.

Case I_b: Except for the overlap with case I_a, the isogeny type is not symmetric.

Case I_c: Except for the overlap with case I_a, only the subsubcase $\mathrm{I}_{c,2}$ gives for $d_b = 1, d_a > 0$ the isogeny type $G_{2,1} \oplus G_{1,2}$.

3.8 Consider case II. The condition on the height gives that $h_1 = 0, h_2 = h_3 = 1$. Under the symmetry condition we are left with the case $d_a \geq 0$, then G has isogeny type $G_{2,1} \oplus G_{1,2}$.

3.9 Consider case III. The condition on the height gives that $h_1 = 0, h_2 = h_3 = 1$. Under the symmetry condition we find that the subcases reduce to

Case III_a: The isogeny type is $G_{3,3}$ if $d_a \geq 1, d_c \geq 2, d_b \geq 0$.

Case III_b: Except for the overlap with case III_a, the isogeny type is not symmetric.

Case III_c: Except for the overlap with case III_a, only the subsubcase $\mathrm{III}_{c,1}$ gives for $d_c = 1, d_a \geq 1, d_b \geq 1$ the isogeny type $G_{2,1} \oplus G_{1,2}$.

Case III_d: Except for the overlap with case III_a, the isogeny type is not symmetric.

3.10 We will give some explicit examples using computer packages which have been developed at the Vrije Universiteit in Amsterdam. For several types of curves over $W(k)$ these packages compute the normalized Hilbert F-type of the completion of the Jacobian variety of these curves modulo any chosen power of p (normalized in the sense of chapter III, theorem 4.1).

3.10.1 The curve C defined over $W(\bar{\mathbb{F}}_5)$ given by the (affine) equation $y^2 = 1 + x^7$ has a finite Hilbert-F type of the form

$$F = \{\begin{pmatrix} 0 & 0 & 0 \\ 12 & 0 & 0 \\ 0 & 12 & 0 \end{pmatrix} \bmod 5^2\} + V\{(0) \bmod 5^2\} + V^2\{(0) \bmod 5\}$$
$$+V^3\{\begin{pmatrix} 0 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \bmod 5\}.$$

We may use chapter III, theorem 2.14 which says that the F-type of the reduction $\bar{C}$ of C to $\bar{\mathbb{F}}_5$ can be described by just omitting the Hilbert braces { }. Using $5 = VF$ we conclude that $\bar{C}$ has Witt F-type of the form described in case I, with $d_a, d_b \geq 2$. Thus the isogeny type of $\bar{C}$ is $3G_{1,1}$.

Using the relation between the isogeny type of $\bar{C}$ and the ζ-function we may check this isogeny type by computing the ζ-function (see for example [Man], [Kob] or [Yui78]). One easily computes by counting points that the numerator of the ζ-function of $\bar{C}$ is $1 + 125\lambda^6$. This indeed implies that the isogeny type of $\bar{C}$ is $3G_{1,1}$. This curve is also treated in [Yui78], example 5.4.

3.10.2 We now consider the curve C defined over $W(\bar{\mathbb{F}}_3)$ given by the (affine) equation $y^2 = 1 - x + x^7$. The finite F-type of C has the form

$$F = \{\begin{pmatrix} 0 & 0 & 0 \\ 4 & 3 & 6 \\ 0 & 4 & 3 \end{pmatrix} \bmod 3^2\} + V\{\begin{pmatrix} 8 & 2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \bmod 3^2\}$$
$$+V^2\{\begin{pmatrix} 8 & 7 & 6 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \bmod 3^2\} + V^3\{\begin{pmatrix} 2 & 2 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \bmod 3\}.$$

Then the reduction $\bar{C}$ of C to $\bar{\mathbb{F}}_3$ is seen to have Witt F-type of the form described in case I, with $d_b = 1$. Thus the isogeny type of $\bar{C}$ is $G_{1,2} \oplus G_{2,1}$. This is in accordance with the fact that the numerator of the ζ-function of $\bar{C}$ is $1 + 3\lambda + 6\lambda^2 + 12\lambda^3 + 18\lambda^4 + 27\lambda^5 + 27\lambda^6$, as one easily computes by counting points. This curve is also treated by [Man], chapter IV, section 5, example 1.

3.10.3 Consider now the curve C defined over $W(\bar{\mathbb{F}}_2)$ given by the (affine) equation $y^2 + y = x^7$. The finite F-type of C has the form

$$F = \{\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \bmod 2^3\} + V\{\begin{pmatrix} 6 & 3 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \bmod 2^3\}$$

$$+V^2\{\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 3 \end{pmatrix} \bmod 2^3\}.$$

Then the reduction $\bar{C}$ of C to $\bar{\mathbb{F}}_2$ is seen to have Witt F-type of the form described in case II, with $d_a \geq 1$. Thus the isogeny type of $\bar{C}$ is $G_{1,2} \oplus G_{2,1}$. This is in accordance with the fact that the numerator of the ζ-function of $\bar{C}$ is $1 - 2\lambda^3 + 8\lambda^6$, as one easily computes by counting points.

4 Some lemmas on p-adic Gamma functions

References to this section are the books [Kob80], [Lang], [Sch] and for lemma 4.4 [Hov].

4.1 Let p be a fixed rational prime. Recall the p-adic *Gamma function* Γ_p: It is defined on the natural numbers by

$$\Gamma_p(n) := (-1)^n \prod_{j=1,(p,j)=1}^{n-1} j.$$

One may extend this definition to all of $\mathbb{Z}_p$ using the following well-known lemma.

4.2 Lemma. (Congruence formula) *For any numbers m and n from $\mathbb{Z}_p$ we have*

$$\Gamma_p(m+n) \equiv u_p(n)\Gamma_p(m) \bmod n\mathbb{Z}_p,$$

where the function u_p is defined on $\mathbb{Z}_p$ by

$$u_p(n) := \begin{cases} -1 & \text{if } p = 2 \text{ and } ord_p(n) = 2 \\ 1 & \text{otherwise .} \end{cases}$$

□

4.3 Define the function $\rho : \mathbb{Z} \to \{0,1\}$ by $\rho(z) = 1$ if $z \geq 0$, and 0 otherwise. The following lemma is a slight generalization of [Hov], lemma 1.4.1.

4.4 Lemma. *Let θ, θ' be p-adic integers such that $\theta - p\theta' \in \langle -p, 0] \cap \mathbb{Z}$, let μ, n, α be integers such that $\mu, n > 0$, and $\alpha \in [0, np\rangle$. Then*

$$\frac{\prod_{i=0}^{\alpha+\mu p-1}(\theta+i)}{\prod_{i=0}^{\mu-1}(\theta'+i)} =$$

$$= (-1)^{\alpha+\mu p} p^{\mu} \prod_{u=0}^{n-1} \Big(p(\theta'+\mu+u)\Big)^{\rho(\theta-p\theta'+\alpha-up-1)} \frac{\Gamma_p(\theta+\alpha+\mu p)}{\Gamma_p(\theta)}.$$

We only need the special case $n = 1$, which is exactly Hoving's lemma. We therefore leave the proof of lemma 4.4, which is analogous to the proof of Hoving, to the interested reader.

4.5 Corollary. *We have the following formula*

$$[pc/m]! \,/_{[c/m]!} = (-1)^{[pc/m]+1} p^{[c/m]} \Gamma_p(1 + [pc/m]),$$

where $c, m \in \mathbb{N}$.

proof: Take $n = 1, \mu = [c/m]$, $\alpha = [pc/m] - p[c/m]$ and $\theta = \theta' = 1$ in the previous lemma (note that $\Gamma_p(1) = -1$). □

5 Generalized Witt vector cohomology and F-types

5.1 (For details on this subsection see [SPM] or [Sti].) For any scheme X we may define the sheaf $\mathcal{WO}_X$ of Witt vectors on X. Assume that X is a smooth projective scheme over an affine flat (over $\mathbb{Z}$) scheme $S = \operatorname{Spec} A$, and that $H^m(X, \mathcal{O}_X)$ is a free A-module. Let $\{\omega_1, \ldots, \omega_h\}$ be a basis for $H^m(X, \mathcal{O}_X)$. Denote by $\pi : H^m(X, \mathcal{WO}_X) \to H^m(X, \mathcal{O}_X)$ the map induced by $\pi : \mathcal{WO}_X \to \mathcal{O}_X$, the projection on the first coordinate. Then by [SPM], lemma 2.5 we have that π is surjective. We therefore may choose liftings $\tilde{\omega}_i \in H^m(X, \mathcal{WO}_X)$, i.e., $\pi\tilde{\omega}_i = \omega_i$. We denote by $F_n : H^m(X, \mathcal{WO}_X) \to H^m(X, \mathcal{WO}_X)$ the map induced by $F_n : \mathcal{WO}_X \to \mathcal{WO}_X$, $n \in \mathbb{N}$. For every $n \geq 1$ we define the $h \times h$ matrix $B_n = (b_{n,i,j})$ with entries in A by

$$\pi F_n \tilde{\omega}_i = \sum b_{n,i,j} \omega_j,$$

or, equivalently, in vector notation

$$\pi F_n \underline{\omega} = B_n \underline{\omega}.$$

We then have that $\sum_{n \geq 1} n^{-1} B_n^{\mathrm{T}} T^n$ is the logarithm for the Artin-Mazur formal group with respect to a proper system coordinates (Here we denote by B^{T} the transpose of the matrix B) ([ArM] or [Sti]).

5.2 In general it is not easy to compute the matrices B_n explicitly. In some cases however we can compute them rather easily: Let m be the dimension of X. Assume that $\mathcal{U} = \{U_i\}_{i=0,\ldots,m}$ is an open affine covering of X. Then the Čech cohomology $\check{H}^m(\mathcal{U}, \mathcal{O}_X)$ is isomorphic to $H^m(X, \mathcal{O}_X)$.
A cocycle for the Čech cohomology is just any element f of $\mathcal{O}_X(U_0 \bigcap \ldots \bigcap U_m)$. Denote by $\overline{f}$ the class of f in $\check{H}^m(X, \mathcal{O}_X)$ and by τ the Teichmüller map from $\mathcal{O}_X$

in $W\mathcal{O}_X$. Then as a lifting of $\overline{f}$ in $\check{H}^m(X, W\mathcal{O}_X)$ we may take the class $\overline{\tau(f)}$. The n-th Frobenius map F_n acts rather simply in this case $F_n(\overline{\tau(f)}) = \overline{\tau(f^n)}$. So taking representatives f_i of a basis ω_i of $\check{H}^m(X, \mathcal{O}_X)$, the $B_n = (b_{n,i,j})$ may be computed from

$$\overline{f_i^n} = \sum_j b_{n,i,j} \overline{f_j}.$$

Of course, B_n depends on the choice of liftings.

5.3 If we furthermore assume that A is a p-Hilbert ring with endomorphism $\sigma := \sigma_p$ then we only have to consider the "p-typical matrices" B_{p^n} (chapter I, corollary 4.16). We then find the matrices H_i of the Hilbert F_p-type of the formal group law associated to the $B_\bullet$ recursively from (chapter II, lemma 2.1)

$$B_{p^{n+1}} = \sum_{i=0}^{n} p^i H_i^{\sigma^{n-i}} B_{p^{n-i}}, \tag{5.3.1}$$

i.e., the Hilbert F_p-type of the p-typical formal group law G with logarithm $\sum_{n\geq 0} p^{-n} B_{p^n}^{\mathrm{T}} T^m$ is $F\phi_G = \sum_{i\geq 0} V^i\{H_i\}\phi_G$ ($F := F_p, V := V_p$).

5.4 Let H be a formal group law isomorphic to G with Hilbert F-type $F\phi_H = \sum_{i\geq 0} V^i\{N_i\}\phi_H$. Let $\phi_G = \sum_{i\geq 0} V^i\{\Lambda_i\}\phi_H$. Then we have the following relation

$$B_{p^{m+1}} - \sum_{j=0}^{m} p^j B_{p^{m-j}}^{\sigma^{1+j}} N_j = p^{m+1}\Lambda_{m+1}.$$

Modulo $p^{m+1}A$ this is read as

$$B_{p^{m+1}} \equiv \sum_{j=0}^{m} p^j B_{p^{m-j}}^{\sigma^{1+j}} N_j \bmod p^{m+1}A. \tag{5.4.1}$$

The converse is also true: if we have any solution of (5.4.1) then G is isomorphic to H (chapter II, proposition 5.6).

5.5 So in order to find the higher Hasse-Witt matrices of the normalized F-type of G (in the sense of chapter III, theorem 4.1) we may try to find N_j which have the form as described in chapter III, theorem 4.1 and are solutions of 5.4.1. This is in general hardly possible, but in special cases when the B_j have some regular shape it can be done (see for example [Hov] or [DiH], where these matrix congruences are solved for several types of curves).

6 Higher Hasse-Witt matrices of Fermat Hypersurfaces

6.1 Let $\mathcal{F} = \mathcal{F}_{N,m}$ be the $(N-1)$-dimensional Fermat hypersurface in $\mathbb{P}^N$ corresponding to the (affine) equation

$$X_1^m + \cdots + X_N^m = 1,$$

where $N \geq 2$. Denote $\mathcal{F}_p$ the reduction modulo p of $\mathcal{F}$.

6.2 Choose as open affine covering of $\mathcal{F}_{N,m}$ the set $\mathcal{U} = \{U_i\}_{i=1,\ldots,N}$, the pullback of the affine covering $\{\{x_i \neq 0\}\}_{i=1,\ldots,N}$ of $\mathbb{P}^{N-1}$. Denote $\check{H}^{N-1}(\mathcal{F}) := \check{H}^{N-1}(\mathcal{U}, \mathcal{O}_{\mathcal{F}})$.

6.3 As preparation for the actual computations of the higher Hasse-Witt matrices, for the vector $\underline{a} = (a_1, \ldots, a_N), a_\bullet \in \mathbb{Z}$ we define

$$T^{\underline{a}} = T^{(a_1,\ldots,a_N)} := 1 \Big/ X_1^{a_1} \ldots X_N^{a_N} ,$$

and the length $|\underline{a}|$ of $\underline{a}$ we define by

$$|\underline{a}| := a_1 + \ldots + a_N.$$

We will call $\underline{a}$ an *exponent*. For typographical reasons we will usually write $\sum_v$ instead of $\sum_{v=1}^N$. So for example $|\underline{a}| = \sum_v a_v$. Let e_i be the i-th unit vector. Notice that $T^{\underline{a}}$ is a cocycle in $\check{H}^{N-1}(\mathcal{F})$ if and only if $|\underline{a}| \geq 0$, and that a cocycle $T^{\underline{a}}$ is a coboundary if and only if $a_i \leq 0$ for some i. Obviously for $|\underline{a}| \geq m$ we have in $\check{H}^{N-1}(\mathcal{F})$ the relation

$$T^{\underline{a}} \equiv T^{\underline{a}-me_1} + \ldots + T^{\underline{a}-me_N}, \qquad 6.3.1$$

and if $a_i \leq m$ then $T^{\underline{a}-me_i} \equiv 0$ in $\check{H}^{N-1}(\mathcal{F})$.
We conclude that a basis for $\check{H}^{N-1}(\mathcal{F})$ is given by the classes of $T^{\underline{a}}, a_i > 0, |\underline{a}| < m$ (This gives the well known assertion that

$$\text{rank}_{\text{ base ring}}\ \check{H}^{N-1}(\mathcal{F}) = \binom{m-1}{N}).$$

For details on the computations in the Čech cohomology we refer to [Sti] or [Har].

6.4 We will call an exponent $\underline{a}$ *holomorphic* if the class of $T^{\underline{a}}$ is non-zero. The following easy lemma then gives an arithmetic description of this property.

6.5 Lemma. *$\underline{a}$ is holomorphic if and only if $\sum_v [a_v/m] = [\sum_v a_v/m]$.* □

6.6 Let $a \bmod m := a - [a/m]m$, i.e., $a \bmod m$ is the integer remainder of a modulo m. For a vector $\underline{a}$ we define $\underline{a} \bmod m$ componentwise.

6.7 Lemma. *In $\check{H}^{N-1}(\mathcal{F})$ we have the following relation*

$$T^{\underline{a}} \equiv c_{\underline{a}} T^{\underline{a} \bmod m},$$

where

$$c_{\underline{a}} = \frac{([a_1/m] + \ldots + [a_N/m])!}{([a_1/m])! \ldots ([a_N/m])!}.$$

proof: From 6.3.1 we see that we have $c_{\underline{a}} = \sum_v c_{\underline{a}-me_v}$ for $|\underline{a}| \geq m$ (and obviously $c_{\underline{a}} = 1$ for $|\underline{a}| < m$). We therefore may rewrite the generic power series $\sum_{\underline{a}} c_{\underline{a}} T^{\underline{a}}$ as

$$\begin{aligned} \sum_{\underline{a}} c_{\underline{a}} T^{\underline{a}} &= \sum_{|\underline{a}| \geq m} \left(\sum_v c_{\underline{a}-me_v} \right) T^{\underline{a}} + \sum_{|\underline{a}|<m} c_{\underline{a}} T^{\underline{a}} \\ &= \left(\sum_{\underline{a}} c_{\underline{a}} T^{\underline{a}} \right) \left(\sum_v T^{me_v} \right) + \sum_{|\underline{a}|<m} T^{\underline{a}}. \end{aligned}$$

So

$$\sum_{\underline{a}} c_{\underline{a}} T^{\underline{a}} = \textstyle\sum_{|\underline{a}|<m} T^{\underline{a}} \Big/ 1 - \sum_v T^{me_v} = \displaystyle\sum_{|\underline{a}|<m} T^{\underline{a}} . \sum_{\underline{b}} d_{\underline{b}} T^{m\underline{b}},$$

where

$$d_{\underline{b}} = \binom{b_1 + \ldots + b_N}{b_1} \ldots \binom{b_{N-1} + b_N}{b_{N-1}} = \frac{(b_1 + \ldots + b_N)!}{b_1! \ldots b_N!}.$$

Comparing coefficients we find the assertion. □

6.8 We may now compute the B_n from the relation in $\check{H}^{N-1}(\mathcal{F})$

$$F_n(T^{\underline{a}}) \equiv T^{n\underline{a}} \equiv c_{n,\underline{a}} . T^{n\underline{a} \bmod m}, \tag{6.8.1}$$

where

$$c_{n,\underline{a}} = \frac{([na_1/m] + \ldots + [na_N/m])!}{([na_1/m])! \ldots ([na_N/m])!}$$

and from $T^{n\underline{a} \bmod m} \equiv 0$ if and only if $|n\underline{a} \bmod m| \geq m$.

6.9 Remark. —We observe that $n \equiv 1 \bmod m$ implies that B_n is an invertible (diagonal) matrix. In particular in the case $p \equiv 1 \bmod m$ we see that $\mathcal{F}_p$ is *ordinary*, i.e., $\mathcal{F}_p$ has invertible *Hasse-Witt matrix* $\pi(B_p)$. Conversely, if $p \not\equiv 1 \bmod m$ then put $z := \min\{[(m-1)/N], [(m-1)/(p \bmod m)]\}$. One easily checks that $|p(z, z, \ldots, z) \bmod m| \geq m$ and thus B_p is not invertible.
—The other extreme is the case when $n \equiv -1 \bmod m$. In this case we see that $B_n = 0$ (since $|\underline{a}| < m$ implies in this case $|n\underline{a} \bmod m| = Nm - |a| > m$).

—We note that the B_n (for any $N \geq 2, m \in \mathbb{N}$) are very sparse matrices so one may hope that explicit formula for the normal forms of the higher Hasse-Witt matrices in terms of explicit p-adic limits are obtainable. We will show that this is indeed the case.

6.10 From now on let $N \geq 2, m$ be fixed integers, and p a fixed rational prime such that the gcd $(p, m) = 1$. This condition on p is equivalent ([Kob]) to $\mathcal{F}_p$ being smooth. From now on our discussion will be focussed on p-typical objects. We will simply write B_n instead of B_{p^n}.

6.11 We will consider the p-typical decomposition of $\check{H}^{N-1}(\mathcal{F})$. Take any holomorphic $\underline{a}$. Let $f > 0$ be the smallest integer such that $p^f \underline{a} = \underline{a} \bmod m$ (thus if m is prime then f is the order of p in $(\mathbb{Z}/m\mathbb{Z})^*$). Define the *cycle* $C = C_{\underline{a}}$ as the ordered set $\{\underline{a}, p\underline{a} \bmod m, ..., p^{f-1}\underline{a} \bmod m\}$. Let γ be the number of holomorphic exponents in C and define the function $r_\bullet : \{1, ..., \gamma\} \to C$ by $r_i :=$ "i-th holomorphic exponent in C". The integer $r_{i,j}$ then is the j-th component of r_i. Let $\mathcal{C}$ be a disjoint partition of the set of all exponents in cycles. Also define H_C to be the sub $\mathbb{Z}$-module of $\check{H}^{N-1}(\mathcal{F})$ generated by

$$T^{r_1} (= T^{\underline{a}}), T^{r_2}, \ldots, T^{r_\gamma}.$$

Then obviously $\check{H}^{N-1}(\mathcal{F}) = \oplus_{C \in \mathcal{C}} H_C$ is a direct sum decomposition of $\check{H}^{N-1}(\mathcal{F})$ which is stable under the action of $F = F_p$. Therefore the associated p-typical formal group law G may also be decomposed as $G = \oplus_{C \in \mathcal{C}} G_C$ (Notice that this decomposition is finer than the motivic decomposition as introduced in [Shio]).

6.12 Fix an holomorphic exponent $\underline{a}$. We will restrict our considerations to H_C. Write $B_l := B_{C,l}, l \geq 0$ for the matrices representing the action of F on H_C. Thus

$$b_{n,i,j} = \begin{cases} c_{p^n, r_i} & \text{if } p^n r_i \equiv r_j \bmod m, \\ 0 & \text{otherwise .} \end{cases}$$

6.13 Denote by $N_l := N_{C,l}$ $(l \geq 0)$ the matrices of a finite F-type of G_C. We will see (subsection 6.16) that this finite F-type further is of permutation type (see chapter III, subsection 2.16). In that case the matrix congruences (5.4.1) between the B_n and the N_l boil down to

$$N_{l,k,j} \equiv b_{n+1,i,j} \Big/ p^l b_{n-l,i,k}^{\sigma^{l+1}} \bmod p^{n+1-l-\mathrm{ord}_p(b_{n-l,i,k})}, \qquad 6.13.1$$

where

$$p^{n+1} r_i \equiv r_j \bmod m, p^{n-l} r_i \equiv r_k \bmod m, \qquad 6.13.2$$

and $N_{l,k,j}$ is the possible non-zero entry in the k-th column of $\sum_{l \geq 0} N_l$. Since we are working over $\mathbb{Z}$ we may forget about the endomorphism σ.

6.14 Denote $\underline{\rho} := r_i$, $\rho_j := r_{i,j}$, and consider the quotient

$$b_{n+1,i,j} \Big/ p^l b_{n-l,i,k}^{\sigma^{l+1}} \tag{6.14.1}$$

$$= p^{-l} \cdot \frac{(\sum_v [p^{n+1}\rho_v/m])!}{\prod_v [p^{n+1}\rho_v/m]!} \cdot \frac{\prod_v [p^{n-l}\rho_v/m]!}{(\sum_v [p^{n-l}\rho_v/m])!} =$$

$$p^{-l} \prod_v \frac{[p^{n-l}\rho_v/m]!}{[p^{n+1}\rho_v/m]!} \cdot \frac{(\sum_v [p^{n+1}\rho_v/m])!}{[\sum_v p^{n+1}\rho_v/m]!} \cdot \prod_{u=0}^{l} \frac{[\sum_v p^{n+1-u}\rho_v/m]!}{[\sum_v p^{n-u}\rho_v/m]!} \cdot \frac{[\sum_v p^{n-l}\rho_v/m]!}{(\sum_v [p^{n-l}\rho_v/m])!}.$$

6.15 Using corollary (4.5) we see

$$\frac{[p^{n-l}\rho_v/m]!}{[p^{n+1}\rho_v/m]!} = \prod_{u=0}^{l} \frac{[p^{n-u}\rho_v/m]!}{[p^{n+1-u}\rho_v/m]!} =$$

$$= \prod_{u=0}^{l} (-1)^{[p^{n+1-u}\rho_v/m]+1} p^{-[p^{n-u}\rho_v/m]} \Gamma_p^{-1}(1 + [p^{1+n-u}\rho_v/m]),$$

and also

$$\frac{[\sum_v p^{n+1-u}\rho_v/m]!}{[\sum_v p^{n-u}\rho_v/m]!} =$$

$$= (-1)^{[\sum_v p^{n+1-u}\rho_v/m]+1} p^{[\sum_v p^{n-u}\rho_v/m]} \Gamma_p(1 + [\sum_v p^{n+1-u}\rho_v/m]).$$

We are left with the two odd quotients

$$\frac{(\sum_v [p^{n+1}\rho_v/m])!}{[\sum_v p^{n+1}\rho_v/m]!} = 1 = \frac{[\sum_v p^{n-l}\rho_v/m]!}{(\sum_v [p^{n-l}\rho_v/m])!}.$$

This follows from lemma 6.5 since $p^{n+1}\underline{\rho}$ and $p^{n-l}\underline{\rho}$ are holomorphic (6.13.2).
So we have found for the quotient (6.14.1) that

$$b_{n+1,i,j} \Big/ p^l b_{n-l,i,k}^{\sigma^{l+1}} = (-1)^{Nl}(-p)^{-l+\sum_{u=0}^{l}([\sum_v p^{n-u}\rho_v/m]-\sum_v [p^{n-u}\rho_v/m])} \cdot$$

$$\cdot \prod_{u=0}^{l} \frac{\Gamma_p(1 + [\sum_v p^{n+1-u}\rho_v/m])}{\prod_v \Gamma_p(1 + [p^{n+1-u}\rho_v/m])}. \tag{6.15.1}$$

6.16 We will now choose $l = l_k, j = j_k$ depending on k such that the quotient (6.14.1) has p-adic order greater than or equal to 0. Take $l \geq 0$ to be the minimal integer such that $p^{l+1}r_k$ is holomorphic. Then define j by $r_j = p^{l+1}r_k \bmod m$. So $j = k+1$ if $k < \gamma$, and $j = 1$ if $k = \gamma$. Using lemma 6.5 and (6.13.2) we then have for $u = 0, ..., l-1$

$$[\sum_v p^{n-u}\rho_v/m] - \sum_v [p^{n-u}\rho_v/m] \in \{1, ..., N-1\}. \tag{6.16.1}$$

This implies that the quotient (6.14.1) has positive p-order.
Also notice that a series of matrices $\{N_l\}_{l\geq 0}$ having only non-zero entries at the positions $(N_{l_k})_{j_k,k}$ is of permutation type.

6.17 In order to find the finite F-type we still have to find an expression for (6.14.1) which is independent of n modulo $p^{n+1-l-\mathrm{ord}_p(b_{n-l,i,k})}$. First remark that $[a/m] = a/m - \langle a/m\rangle$ where $\langle a/m\rangle$ denotes the fractional part. Using (6.13.2) we see that

$$\langle p^{n-u}\rho_v/m\rangle = \langle p^{l-u}r_{k,v}/m\rangle. \qquad 6.17.1$$

Then from (6.15.1) we see that the exponent, exp_p of $-p$ in (6.14.1) is given by

$$exp_p = -l + \sum_{u=0}^{l}\left(\sum_v \langle p^u r_{k,v}/m\rangle - \langle(\sum_v p^u r_{k,v})/m\rangle\right). \qquad 6.17.2$$

Using lemma 4.2 and (6.17.1) we find

$$\prod_{u=0}^{l}\frac{\Gamma_p(1+[\sum_v p^{n+1-u}\rho_v/m])}{\prod_v\Gamma_p(1+[p^{n+1-u}\rho_v/m])} \equiv \prod_{u=1}^{l+1}\frac{\Gamma_p(1-\langle(\sum_v p^u r_{k,v})/m\rangle)}{\prod_v\Gamma_p(1-\langle p^u r_{k,v}/m\rangle)} \bmod p^{n+1-l}. \qquad 6.17.3$$

Since $exp_p + n + 1 - l \geq n + 1 - l - \mathrm{ord}_p(b_{n-l,i,k})$ we may conclude from (6.17.2), (6.17.3) and (6.13.1) that

$$N_{l,k,j} = (-1)^{Nl}(-p)^{-l+\sum_{u=0}^{l}(\sum_v\langle p^u r_{k,v}/m\rangle - \langle(\sum_v p^u r_{k,v})/m\rangle)}\cdot\prod_{u=1}^{l+1}\frac{\Gamma_p(1-\langle(\sum_v p^u r_{k,v})/m\rangle)}{\prod_v\Gamma_p(1-\langle p^u r_{k,v}/m\rangle)}.$$

6.18 We have found that the associated formal group law G to $\mathcal{F}$ is isomorphic over $\mathbb{Z}_p$ to $\oplus_{C\in\mathcal{C}} G_{C,typ}$ where the F-type of $G_{C,typ}$ is

$$F\phi_{G_{C,typ}} = \sum_{l\geq 0} V^l N_{C,l}\phi_{G_{C,typ}}.$$

6.19 Using chapter III, lemma 2.17 we conclude that $G_{\mathcal{F}}$ is isomorphic over $W_p(\bar{\mathbb{F}}_p)$ to $\oplus_{C\in\mathcal{C}} G'_{C,typ}$, where the F-type of $G'_{C,typ}$ is

$$F\phi_{G'_{C,typ}} = \sum_{l\geq 0} V^l N'_{C,l}\phi_{G'_{C,typ}},$$

and where $N'_{C,l,i,j} := p^o$ if the p-adic order $o_p(N_{C,l,i,j}) = o$ ($p^\infty := 0$).

6.20 We now apply chapter III, proposition 2.18: the associated formal group law $\bar{G}$ to $\mathcal{F}_p$ is isomorphic over the algebraic closure $\bar{\mathbb{F}}_p$ of $\mathbb{F}_p$ to $\oplus_{C\in\mathcal{C}}\bar{G}_{C,typ}$, where $\bar{G}_{C,typ}$ has a finite Witt F-type

$$F\phi_{\bar{G}_{C,typ}} = \sum V^l[D_{C,l}]\phi_{\bar{G}_{typ}}.$$

Moreover we know that if $N_{C,l,i,j} \not\equiv 0 \bmod p$ that then $D_{C,l,i,j} = 1$.
We have some easy corollaries

6.21 Corollary. *The formal group law $\bar{G}$ associated to the reduction of the Fermat Hypersurface $\mathcal{F}_p$*

i: is ordinary (i.e., has invertible Hasse-Witt matrix) if and only if $p \equiv 1 \bmod m$,

ii: (Koblitz [Kob], pg 198) has Hasse-Witt matrix zero if and only if for all holomorphic $\underline{a}$ we have that $p\underline{a}$ is not holomorphic.

iii: has finite height if $N = 2$,

iv: has an additive direct summand if and only if there exists a holomorphic $\underline{a}$ for which the following holds: For all r with $p^r\underline{a}$ holomorphic there is a u (with $0 \leq u < f_r$) such that $[\sum_v p^u a_v/m] - \sum_v [p^u a_v/m] > 1$ (or equivalently $\sum_v \langle p^u a_v/m\rangle - \langle(\sum_v p^u a_v)/m\rangle > 1$), where $f_r > 0$ is the smallest integer such that $p^{r+f_r}\underline{a}$ is holomorphic,

v: is additive if $N > 2$ and $p \equiv -1 \bmod m$,

vi: can not be additive if $m > Np$,

proof: *i*: This we already observed in remark 6.9.
ii: Let $\bar{N}_{l,j,k}$ be a non zero entry of the finite F-type. Let k correspond to the holomorphic exponent $\underline{a}$. Then $l \geq 0$ is the smallest integer such that $p^{l+1}\underline{a}$ is holomorphic.
iii: From formulae 6.16.1 and 6.17.2 we conclude that all non-zero entries in the normal form of the Hilbert F-type are 1 (cf. for example [Yui80]).
iv: In order for G_C to be additive all entries of the finite F-type need to be zero modulo p.
v: If $p \equiv -1 \bmod m$, then we have for any holomorphic $\underline{a}$ that $\sum_v \langle pa_v/m\rangle - \langle(\sum_v pa_v)/m\rangle = N - 1$. So for $N > 2$ we everywhere have positive p-powers in the finite F-type, i.e., the formal group law is additive.
vi: If $m > Np$ we see that both $(1, 1, ..., 1)$ and $(p, p, ..., p)$ are holomorphic, so the Hasse-Witt matrix is non-zero and therefore the formal group law is not additive.
□

6.22 We start with two easy examples which one can handle using only (5.3.1) and (6.8.1). Consider the case $N = 3$ and $m = 4$. Then $T^{(1,1,1)}$ is a basis for $\check{H}^{N-1}(\mathcal{F})$. Take $p = 2$, we then see that all B_{2^n} are zero, and therefore by 5.3.1 that all higher Hasse-Witt matrices are zero: the associated 2-typical formal group law is the additive one.

Take $p = 3$, we then see that $B_{3^n} = 0$ if n is odd, and that B_{3^n} is divisible by 3^n if n is even. We conclude, using 5.3.1, that all higher Hasse-Witt matrices are divisible by 3: the associated formal group law is again just the additive one.

6.23 The author has written a small Maple program which computes the normal form as described in subsubsection 6.19. Using this program the following 3 examples have been computed.

6.23.1 As an example, consider the case $N = 3$, $m = 9$ and $p = 5$. We then obtain that the associated formal group law $G_{\mathcal{F}}$ to the Fermat hypersurface $\mathcal{F} = \mathcal{F}_{N,m}$ is isomorphic over $W_p(\bar{\mathbb{F}}_p)$ to (we denote a formal group law by its Hilbert F_p-type)

$$G_{\mathcal{F}} \cong \left(F = \left\{ \begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix} \right\} + V^4 \left\{ \begin{matrix} 0 & 0 \\ p^2 & 0 \end{matrix} \right\}\right)^{16} \oplus \left(F = V^5\{p\}\right)^{24}.$$

Thus the associated formal group law $G_{\mathcal{F}_5}$ to the reduction $\mathcal{F}_p$ is by subsection 6.20 isomorphic over $\bar{\mathbb{F}}_p$ to (here we denote the formal group laws by their Witt F_p-type)

$$G_{\mathcal{F}_p} \cong \hat{G}_a^{24} \oplus \left(F = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right)^{16}.$$

6.23.2 As another example consider $N = 3, m = 9$, and $p = 7$. Then we obtain that

$$G_{\mathcal{F}} \cong \left(F = V^2\{p\}\right)^{32} \oplus \left(F = V^2\{1\}\right)^{24}.$$

Thus we conclude that

$$G_{\mathcal{F}_p} \cong \hat{G}_a^{32} \oplus \left(F = V^2\right)^{24}.$$

6.23.3 As last example consider the case $N = 3, m = 19$ and $p = 5$. This example is treated in the appendix.

6.24 Remark. In [Eke] Ekedahl introduces the notion of varieties of CM-type. He then uses crystalline cohomology in order to describe the formal Brauer group of surfaces which are Mazur-Ogus (Fermat surfaces and their quotients) and of CM-type in degree 2 (i.e., their formal Brauer group is a direct sum of 2-dimensional subgroups). His results agree with ours.

7 Appendix

In this appendix the decomposition of the associated formal group law to the Fermat hypersurface $\mathcal{F}_{3,19}$ over $W_5(\bar{\mathbb{F}}_5)$, the corresponding decomposition of the

reduction $\mathcal{F}_{3,19,5}$ over $\bar{\mathbb{F}}_5$ and the isogeny type are given. We refer to section 6 for (computational) details.

A1 The associated formal group law $G_{\mathcal{F}}$ of dimension 816 to the fermat hypersurface $\mathcal{F}_{3,19}$ can be decomposed over $W_5(\bar{\mathbb{F}}_5)$ as follows:

1. The following component of dimension 1 appears 24 times, the F-type of this component is

$$F = V^8 \left[\begin{array}{c} 1 \end{array} \right]$$

2. The following component of dimension 1 appears 48 times, the F-type of this component is

$$F = V^8 \left[\begin{array}{c} p^1 \end{array} \right]$$

3. The following component of dimension 1 appears 84 times, the F-type of this component is

$$F = V^8 \left[\begin{array}{c} p^2 \end{array} \right]$$

4. The following component of dimension 1 appears 12 times, the F-type of this component is

$$F = V^8 \left[\begin{array}{c} p^3 \end{array} \right]$$

5. The following component of dimension 2 appears 24 times, the F-type of this component is

$$F = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + V^7 \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

6. The following component of dimension 2 appears 36 times, the F-type of this component is

$$F = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + V^7 \begin{bmatrix} 0 & 0 \\ p^1 & 0 \end{bmatrix}$$

7. The following component of dimension 2 appears 60 times, the F-type of this component is

$$F = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + V^7 \begin{bmatrix} 0 & p^2 \\ 0 & 0 \end{bmatrix}$$

8. The following component of dimension 2 appears 12 times, the F-type of this component is

$$F = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + V^7 \begin{bmatrix} 0 & 0 \\ p^3 & 0 \end{bmatrix}$$

9. The following component of dimension 2 appears 48 times, the F-type of this component is

$$F = V^2 \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + V^5 \begin{bmatrix} 0 & 0 \\ p^1 & 0 \end{bmatrix}$$

10. The following component of dimension 2 appears 12 times, the F-type of this component is

$$F = V^2 \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + V^5 \begin{bmatrix} 0 & 0 \\ p^2 & 0 \end{bmatrix}$$

11. The following component of dimension 2 appears 24 times, the F-type of this component is

$$F = V^2 \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + V^5 \begin{bmatrix} 0 & 0 \\ p^3 & 0 \end{bmatrix}$$

12. The following component of dimension 2 appears 4 times, the F-type of this component is

$$F = V^2 \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + V^5 \begin{bmatrix} 0 & p^4 \\ 0 & 0 \end{bmatrix}$$

13. The following component of dimension 2 appears 24 times, the F-type of this component is

$$F = V^2 \begin{bmatrix} 0 & p^1 \\ 0 & 0 \end{bmatrix} + V^5 \begin{bmatrix} 0 & 0 \\ p^1 & 0 \end{bmatrix}$$

14. The following component of dimension 3 appears 24 times, the F-type of this component is

$$F = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} + V^6 \begin{bmatrix} 0 & p^2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

15. The following component of dimension 3 appears 12 times, the F-type of this component is

$$F = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} + V \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} + V^5 \begin{bmatrix} 0 & p^1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

16. The following component of dimension 3 appears 12 times, the F-type of this component is

$$F = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} + V \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} + V^5 \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & p^2 \\ 0 & 0 & 0 \end{bmatrix}$$

17. The following component of dimension 4 appears 4 times, the F-type of this component is

$$F = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} + V^5 \begin{bmatrix} 0 & p^2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

A2 We thus observe that the formal group law $\bar{G}_{\mathcal{F}}$ associated to the reduction $\mathcal{F}_{3,19,5}$ of $\mathcal{F}_{3,19}$ modulo 5 can be decomposed over $\bar{\mathbb{F}}_5$ in the following way:

The components 1 reduce to 24 times the following component of dimension 1 with F-type

$$F = V^8 \begin{bmatrix} 1 \end{bmatrix}$$

The components 2, 3, 4, 13 reduce to 192 times $\hat{G}_a$
The components 5 reduce to 24 times the following component of dimension 2 with F-type

$$F = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + V^7 \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

The components 6 reduce to 36 times the following component of dimension 2 with F-type

$$F = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + V^8 \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

The components 7 and 8 reduce to 72 times the following component of dimension 2 with F-type

$$F = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

The components 9 reduce to 48 times the following component of dimension 2 with F-type

$$F = V^2 \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + V^8 \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

The components 10,11 and 12 reduce to 40 times the following component of dimension 2 with F-type

$$F = V^2 \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

The components 14 reduce to 24 times the following component of dimension 3 with F-type

$$F = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} + V^8 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

The components 15 reduce to 12 times the following component of dimension 3 with F-type

$$F = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} + V \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} + V^7 \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

The components 16 reduce to 12 times the following component of dimension 3 with F-type

$$F = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} + V \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} + V^8 \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

The components 17 reduce to 4 times the following component of dimension 4 with F-type

$$F = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} + V^7 \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

A3 The isogeny type of $\bar{G}_{\mathcal{F}}$ can now easily be computed:

$$\bar{G}_{\mathcal{F}} \sim \hat{G}_a^{288} \oplus G_{2,\infty}^{152} \oplus G_{1,8}^{144} \oplus G_{2,7}^{40}.$$

Bibliography

[Abe] Abe,E. *Hopf algebras*, Cambridge Univ. Press, **1077**, 1977.

[ArM] Artin, M. and Mazur, B. *Formal groups arising from algebraic varieties*, Ann. Scient. Éc. Norm. Sup., 4^e serie, t. 10, 87-132, 1977.

[Bou] Bourbaki, N. *Algèbre commutative*, chapitre 9, Masson, Paris, 1983.

[Dieu] Dieudonné, J. *Introduction to the theory of formal groups*, Marcel Dekker Inc., New York, 1973.

[Dieu52] Dieudonné, J.A. *Sur les groupes de Lie algébriques sur un corps de caractéristique* $p > 0$, Rend. Circ. Mat. Palermo (2), I 380 - 402, 1952.

[DiH] Ditters, E.J., Hoving, S.J. *On the connected part of the covariant Tate p - divisible group and the ζ - function of the family of hyperelliptic curves* $y^2 = 1 + \mu x^N$ *modulo various primes*, Math. Z., **200**, 245 - 264, 1989.

[Dit89] Ditters, E.J. *On the Classification of Commutative Formal Group Laws over p-Hilbert domains*, Math. Z., **202**, 83-109, 1989.

[Dit90] Ditters, E.J. *Hilbert functions and Witt functions. An identity for congruences of Atkin and of Swinnerton - Dyer type*, Math. Z., **205**, 247-278, 1990.

[Eke] Ekedahl, T. *Varieties of CM-type*, preliminary note communicated by the author, 1994.

[Fro] Fröhlich, A. *Formal Groups*, Lec. Notes Math., **74**, Springer-Verlag, Berlin, 1968.

[FuL] Fulton, W. and Lang, S. *Riemann-Roch algebra*, Grundl. der Math. Wiss., **277**, Springer-Verlag, Berlin, 1985.

[Har] Hartshorne, R. *Algebraic Geometry*, Grad. Texts Math. **52**, Springer-Verlag, Berlin, 1977.

[HaW] Hasse, H. und Witt, E. *Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Charakteristik p*, Monat. für die Math. und Phy., 477-492, 1936.

[Haz] Hazewinkel.M. *Formal groups and applications*, Academic Press, New York, 1978.

[Hill] Hill, W.L. *Formal groups and Zeta-functions of elliptic curves*, Inventiones Math., **12**, 321-336, 1971.

[Hon] Honda, T. *On the theory of commutative formal groups*, J. Math. Soc. Japan, **22**, no.2, 213-246, 1970.

[Hov] Hoving, S.J. *W(k)[F,V]-Modules and Zeta Functions of several Types of Curves*, Thesis, Vrije Universiteit, 1990.

[Kne] Kneppers, H.A.W.M. *The covariant classification of two-dimensional smooth commutative formal groups over an algebraically closed field of positive characteristic*, Math. Centre Tracts, **157**, Math. Centre, Amsterdam, 1983.

[Kne90] Kneppers, H.A.W.M. *Two-dimensional Formal groups, form isomorphism to isogeny*, Math. Z., **205**, 309-313, 1990.

[Kob] Koblitz, N. *p-adic variation of the zeta-function*, Comp. Math., **31**, 119-218, 1975.

[Kob80] Koblitz, N. *p-adic Analysis: a short course on recent work*, Lond. Math. Soc. Lect. Note Ser., **46**, Cambrigde University Press, Cambridge, 1980.

[Lang] Lang, S. Cyclotomic Fields II, Grad. Texts Math., **69**, Springer-Verlag, Berlin, 1980.

[Laz] Lazard, M. *Commutative Formal Groups*, Lect. Notes Math., **443**, Springer-Verlag, Berlin, 1975.

[Laz55] Lazard, M. *Lois de groupes et analyseurs*, Ann. Ecole Norm. Sup. , **72**, 299-400, 1955.

[MaL] Mac Lane, S. *Categories for the working mathematician*, GTM, **5**, Springer-Verlag, Berlin, 1971.

[Man] Manin, Yu.I. The theory of commutative formal groups over fields of finite characteristic, Russ. Math. Survey, **18**, 1-83, 1963.

[Mum] Mumford, D. *The Red Book of Varieties and Schemes*, Lect. Notes Math., **1358**, Springer-Verlag, Berlin, 1988.

[Sch] Schikhof, W.H. *Ultrametric Calculus*, Camb. Stud. Adv. Math., **4**, Cambridge University Press, Cambridge, 1984.

[Scho] Scholtens, A.C.J. *On the graded dual of the non-commutative universal Leibniz Hopf algebra Z*, rapport, **WS-419**, Vrije Universiteit, Amsterdam, 1994.

[Shio] Shioda, T. *Some observations on Jacobi sums*, Adv. Stud. Pure Math., **12**, 119-135, 1987.

[SPM] Stienstra, J., Van der Put, M., Van der Marel, B. *On p-adic monodromy*, Math. Z., **208**, 309-325, 1991.

[Sti] Stienstra, J. *Formal Group Laws Arising from Algebraic Varieties*, Am. Jour. of Math., **109**, 907-925, 1986.

[Yan] Yanagihara, H. *Theory of Hopf Algebras Attached to Group Schemes*, Lect. Notes. Math., **614**, Springer-Verlag, Berlin, 1977.

[Yui78] Yui, N. *On the Jacobian Varieties of Hyperelliptic Curves over Fields of Characteristic p>2*, J. of Alg., **52**, 378-410, 1978.

[Yui80] Yui, N. *On the Jacobian Variety of the Fermat Curve*, J. of Alg., **65**, 1-35, 1980.

List of Symbols

Index

CWI TRACTS

1 D.H.J. Epema. *Surfaces with canonical hyperplane sections.* 1984.

2 J.J. Dijkstra. *Fake topological Hilbert spaces and characterizations of dimension in terms of negligibility.* 1984.

3 A.J. van der Schaft. *System theoretic descriptions of physical systems.* 1984.

4 J. Koene. *Minimal cost flow in processing networks, a primal approach.* 1984.

5 B. Hoogenboom. *Intertwining functions on compact Lie groups.* 1984.

6 A.P.W. Böhm. *Dataflow computation.* 1984.

7 A. Blokhuis. *Few-distance sets.* 1984.

8 M.H. van Hoorn. *Algorithms and approximations for queueing systems.* 1984.

9 C.P.J. Koymans. *Models of the lambda calculus.* 1984.

10 C.G. van der Laan, N.M. Temme. *Calculation of special functions: the gamma function, the exponential integrals and error-like functions.* 1984.

11 N.M. van Dijk. *Controlled Markov processes; time-discretization.* 1984.

12 W.H. Hundsdorfer. *The numerical solution of nonlinear stiff initial value problems: an analysis of one step methods.* 1985.

13 D. Grune. *On the design of ALEPH.* 1985.

14 J.G.F. Thiemann. *Analytic spaces and dynamic programming: a measure theoretic approach.* 1985.

15 F.J. van der Linden. *Euclidean rings with two infinite primes.* 1985.

16 R.J.P. Groothuizen. *Mixed elliptic-hyperbolic partial differential operators: a case-study in Fourier integral operators.* 1985.

17 H.M.M. ten Eikelder. *Symmetries for dynamical and Hamiltonian systems.* 1985.

18 A.D.M. Kester. *Some large deviation results in statistics.* 1985.

19 T.M.V. Janssen. *Foundations and applications of Montague grammar, part 1: Philosophy, framework, computer science.* 1986.

20 B.F. Schriever. *Order dependence.* 1986.

21 D.P. van der Vecht. *Inequalities for stopped Brownian motion.* 1986.

22 J.C.S.P. van der Woude. *Topological dynamix.* 1986.

23 A.F. Monna. *Methods, concepts and ideas in mathematics: aspects of an evolution.* 1986.

24 J.C.M. Baeten. *Filters and ultrafilters over definable subsets of admissible ordinals.* 1986.

25 A.W.J. Kolen. *Tree network and planar rectilinear location theory.* 1986.

26 A.H. Veen. *The misconstrued semicolon: Reconciling imperative languages and dataflow machines.* 1986.

27 A.J.M. van Engelen. *Homogeneous zero-dimensional absolute Borel sets.* 1986.

28 T.M.V. Janssen. *Foundations and applications of Montague grammar, part 2: Applications to natural language.* 1986.

29 H.L. Trentelman. *Almost invariant subspaces and high gain feedback.* 1986.

30 A.G. de Kok. *Production-inventory control models: approximations and algorithms.* 1987.

31 E.E.M. van Berkum. *Optimal paired comparison designs for factorial experiments.* 1987.

32 J.H.J. Einmahl. *Multivariate empirical processes.* 1987.

33 O.J. Vrieze. *Stochastic games with finite state and action spaces.* 1987.

34 P.H.M. Kersten. *Infinitesimal symmetries: a computational approach.* 1987.

35 M.L. Eaton. *Lectures on topics in probability inequalities.* 1987.

36 A.H.P. van der Burgh, R.M.M. Mattheij (eds.). *Proceedings of the first international conference on industrial and applied mathematics (ICIAM 87).* 1987.

37 L. Stougie. *Design and analysis of algorithms for stochastic integer programming.* 1987.

38 J.B.G. Frenk. *On Banach algebras, renewal measures and regenerative processes.* 1987.

39 H.J.M. Peters, O.J. Vrieze (eds.). *Surveys in game theory and related topics.* 1987.

40 J.L. Geluk, L. de Haan. *Regular variation, extensions and Tauberian theorems.* 1987.

41 Sape J. Mullender (ed.). *The Amoeba distributed operating system: Selected papers 1984-1987.* 1987.

42 P.R.J. Asveld, A. Nijholt (eds.). *Essays on concepts, formalisms, and tools.* 1987.

43 H.L. Bodlaender. *Distributed computing: structure and complexity.* 1987.

44 A.W. van der Vaart. *Statistical estimation in large parameter spaces.* 1988.

45 S.A. van de Geer. *Regression analysis and empirical processes.* 1988.

46 S.P. Spekreijse. *Multigrid solution of the steady Euler equations.* 1988.

47 J.B. Dijkstra. *Analysis of means in some non-standard situations.* 1988.

48 F.C. Drost. *Asymptotics for generalized chi-square goodness-of-fit tests.* 1988.

49 F.W. Wubs. *Numerical solution of the shallow-water equations.* 1988.

50 F. de Kerf. *Asymptotic analysis of a class of perturbed Korteweg-de Vries initial value problems.* 1988.

51 P.J.M. van Laarhoven. *Theoretical and computational aspects of simulated annealing.* 1988.

52 P.M. van Loon. *Continuous decoupling transformations for linear boundary value problems.* 1988.

53 K.C.P. Machielsen. *Numerical solution of optimal control problems with state constraints by sequential quadratic programming in function space.* 1988.

54 L.C.R.J. Willenborg. *Computational aspects of survey data processing.* 1988.

55 G.J. van der Steen. *A program generator for recognition, parsing and transduction with syntactic patterns.* 1988.

56 J.C. Ebergen. *Translating programs into delay-insensitive circuits.* 1989.

57 S.M. Verduyn Lunel. *Exponential type calculus for linear delay equations.* 1989.

58 M.C.M. de Gunst. *A random model for plant cell population growth.* 1989.

59 D. van Dulst. *Characterizations of Banach spaces not containing l^1.* 1989.

60 H.E. de Swart. *Vacillation and predictability properties of low-order atmospheric spectral models.* 1989.

61 P. de Jong. *Central limit theorems for generalized multilinear forms.* 1989.

62 V.J. de Jong. *A specification system for statistical software.* 1989.

63 B. Hanzon. *Identifiability, recursive identification and spaces of linear dynamical systems, part I.* 1989.

64 B. Hanzon. *Identifiability, recursive identification and spaces of linear dynamical systems, part II.* 1989.

65 B.M.M. de Weger. *Algorithms for diophantine equations.* 1989.

66 A. Jung. *Cartesian closed categories of domains.* 1989.

67 J.W. Polderman. *Adaptive control & identification: Conflict or conflux?.* 1989.

68 H.J. Woerdeman. *Matrix and operator extensions.* 1989.

69 B.G. Hansen. *Monotonicity properties of infinitely divisible distributions.* 1989.

70 J.K. Lenstra, H.C. Tijms, A. Volgenant (eds.). *Twenty-five years of operations research in the Netherlands: Papers dedicated to Gijs de Leve.* 1990.

71 P.J.C. Spreij. *Counting process systems. Identification and stochastic realization.* 1990.

72 J.F. Kaashoek. *Modeling one dimensional pattern formation by anti-diffusion.* 1990.

73 A.M.H. Gerards. *Graphs and polyhedra. Binary spaces and cutting planes.* 1990.

74 B. Koren. *Multigrid and defect correction for the steady Navier-Stokes equations. Application to aerodynamics.* 1991.

75 M.W.P. Savelsbergh. *Computer aided routing.* 1992.

76 O.E. Flippo. *Stability, duality and decomposition in general mathematical programming.* 1991.

77 A.J. van Es. *Aspects of nonparametric density estimation.* 1991.

78 G.A.P. Kindervater. *Exercises in parallel combinatorial computing.* 1992.

79 J.J. Lodder. *Towards a symmetrical theory of generalized functions.* 1991.

80 S.A. Smulders. *Control of freeway traffic flow.* 1993.

81 P.H.M. America, J.J.M.M. Rutten. *A parallel object-oriented language: design and semantic foundations.* 1992.

82 F. Thuijsman. *Optimality and equilibria in stochastic games.* 1992.

83 R.J. Kooman. *Convergence properties of recurrence sequences.* 1992.

84 A.M. Cohen (ed.). *Computational aspects of Lie group representations and related topics. Proceedings of the 1990 Computational Algebra Seminar at CWI, Amsterdam.* 1991.

85 V. de Valk. *One-dependent processes.* 1994.

86 J.A. Baars, J.A.M. de Groot. *On topological and linear equivalence of certain function spaces.* 1992.

87 A.F. Monna. *The way of mathematics and mathematicians.* 1992.

88 E.D. de Goede. *Numerical methods for the three-dimensional shallow water equations.* 1993.

89 M. Zwaan. *Moment problems in Hilbert space with applications to magnetic resonance imaging.* 1993.

90 C. Vuik. *The solution of a one-dimensional Stefan problem.* 1993.

91 E.R. Verheul. *Multimedians in metric and normed spaces.* 1993.

92 J.L.M. Maubach. *Iterative methods for non-linear partial differential equations.* 1994.

93 A.W. Ambergen. *Statistical uncertainties in posterior probabilities.* 1993.

94 P.A. Zegeling. *Moving-grid methods for time-dependent partial differential equations.* 1993.

95 M.J.C. van Pul. *Statistical analysis of software reliability models.* 1993.

96 J.K. Scholma. *A Lie algebraic study of some integrable systems associated with root systems.* 1993.

97 J.L. van den Berg. *Sojourn times in feedback and processor sharing queues.* 1993.

98 A.J. Koning. *Stochastic integrals and goodness-of-fit tests.* 1993.

99 B.P. Sommeijer. *Parallelism in the numerical integration of initial value problems.* 1993.

100 J. Molenaar. *Multigrid methods for semiconductor device simulation.* 1993.

101 H.J.C. Huijberts. *Dynamic feedback in nonlinear synthesis problems.* 1994.

102 J.A.M. van der Weide. *Stochastic processes and point processes of excursions.* 1994.

103 P.W. Hemker, P. Wesseling (eds.). *Contributions to multigrid.* 1994.

104 I.J.B.F. Adan. *A compensation approach for queueing problems.* 1994.

105 O.J. Boxma, G.M. Koole (eds.). *Performance evaluation of parallel and distributed systems - solution methods. Part 1.* 1994.

106 O.J. Boxma, G.M. Koole (eds.). *Performance evaluation of parallel and distributed systems - solution methods. Part 2.* 1994.

107 R.A. Trompert. *Local uniform grid refinement for time-dependent partial differential equations.* 1995.

108 M.N.M. van Lieshout. *Stochastic geometry models in image analysis and spatial statistics.* 1995.

109 R.J. van Glabbeek. *Comparative concurrency semantics and refinement of actions.* 1995.

110 W. Vervaat (ed.). *Probability and lattices.* 1995.

111 I. Helsloot. *Covariant formal group theory and some applications.* 1995.

112 R.N. Bol. *Loop checking in logic programming.* 1995.

113 G.J.M. Koole. *Stochastic scheduling and dynamic programming.* 1995.

MATHEMATICAL CENTRE TRACTS

1 T. van der Walt. *Fixed and almost fixed points.* 1963.

2 A.R. Bloemena. *Sampling from a graph.* 1964.

3 G. de Leve. *Generalized Markovian decision processes, part I: model and method.* 1964.

4 G. de Leve. *Generalized Markovian decision processes, part II: probabilistic background.* 1964.

5 G. de Leve, H.C. Tijms, P.J. Weeda. *Generalized Markovian decision processes, applications.* 1970.

6 M.A. Maurice. *Compact ordered spaces.* 1964.

7 W.R. van Zwet. *Convex transformations of random variables.* 1964.

8 J.A. Zonneveld. *Automatic numerical integration.* 1964.

9 P.C. Baayen. *Universal morphisms.* 1964.

10 E.M. de Jager. *Applications of distributions in mathematical physics.* 1964.

11 A.B. Paalman-de Miranda. *Topological semigroups.* 1964.

12 J.A.Th.M. van Berckel, H. Brandt Corstius, R.J. Mokken, A. van Wijngaarden. *Formal properties of newspaper Dutch.* 1965.

13 H.A. Lauwerier. *Asymptotic expansions.* 1966, out of print: replaced by MCT 54.

14 H.A. Lauwerier. *Calculus of variations in mathematical physics.* 1966.

15 R. Doornbos. *Slippage tests.* 1966.

16 J.W. de Bakker. *Formal definition of programming languages with an application to the definition of ALGOL 60.* 1967.

17 R.P. van de Riet. *Formula manipulation in ALGOL 60, part 1.* 1968.

18 R.P. van de Riet. *Formula manipulation in ALGOL 60, part 2.* 1968.

19 J. van der Slot. *Some properties related to compactness.* 1968.

20 P.J. van der Houwen. *Finite difference methods for solving partial differential equations.* 1968.

21 E. Wattel. *The compactness operator in set theory and topology.* 1968.

22 T.J. Dekker. *ALGOL 60 procedures in numerical algebra, part 1.* 1968.

23 T.J. Dekker, W. Hoffmann. *ALGOL 60 procedures in numerical algebra, part 2.* 1968.

24 J.W. de Bakker. *Recursive procedures.* 1971.

25 E.R. Paërl. *Representations of the Lorentz group and projective geometry.* 1969.

26 European Meeting 1968. *Selected statistical papers, part I.* 1968.

27 European Meeting 1968. *Selected statistical papers, part II.* 1968.

28 J. Oosterhoff. *Combination of one-sided statistical tests.* 1969.

29 J. Verhoeff. *Error detecting decimal codes.* 1969.

30 H. Brandt Corstius. *Exercises in computational linguistics.* 1970.

31 W. Molenaar. *Approximations to the Poisson, binomial and hypergeometric distribution functions.* 1970.

32 L. de Haan. *On regular variation and its application to the weak convergence of sample extremes.* 1970.

33 F.W. Steutel. *Preservations of infinite divisibility under mixing and related topics.* 1970.

34 I. Juhász, A. Verbeek, N.S. Kroonenberg. *Cardinal functions in topology.* 1971.

35 M.H. van Emden. *An analysis of complexity.* 1971.

36 J. Grasman. *On the birth of boundary layers.* 1971.

37 J.W. de Bakker, G.A. Blaauw, A.J.W. Duijvestijn, E.W. Dijkstra, P.J. van der Houwen, G.A.M. Kamsteeg-Kemper, F.E.J. Kruseman Aretz, W.L. van der Poel, J.P. Schaap-Kruseman, M.V. Wilkes, G. Zoutendijk. *MC-25 Informatica Symposium.* 1971.

38 W.A. Verloren van Themaat. *Automatic analysis of Dutch compound words.* 1972.

39 H. Bavinck. *Jacobi series and approximation.* 1972.

40 H.C. Tijms. *Analysis of (s,S) inventory models.* 1972.

41 A. Verbeek. *Superextensions of topological spaces.* 1972.

42 W. Vervaat. *Success epochs in Bernoulli trials (with applications in number theory).* 1972.

43 F.H. Ruymgaart. *Asymptotic theory of rank tests for independence.* 1973.

44 H. Bart. *Meromorphic operator valued functions.* 1973.

45 A.A. Balkema. *Monotone transformations and limit laws.* 1973.

46 R.P. van de Riet. *ABC ALGOL, a portable language for formula manipulation systems, part 1: the language.* 1973.

47 R.P. van de Riet. *ABC ALGOL, a portable language for formula manipulation systems, part 2: the compiler.* 1973.

48 F.E.J. Kruseman Aretz, P.J.W. ten Hagen, H.L. Oudshoorn. *An ALGOL 60 compiler in ALGOL 60, text of the MC-compiler for the EL-X8.* 1973.

49 H. Kok. *Connected orderable spaces.* 1974.

50 A. van Wijngaarden, B.J. Mailloux, J.E.L. Peck, C.H.A. Koster, M. Sintzoff, C.H. Lindsey, L.G.L.T. Meertens, R.G. Fisker (eds.). *Revised report on the algorithmic language ALGOL 68.* 1976.

51 A. Hordijk. *Dynamic programming and Markov potential theory.* 1974.

52 P.C. Baayen (ed.). *Topological structures.* 1974.

53 M.J. Faber. *Metrizability in generalized ordered spaces.* 1974.

54 H.A. Lauwerier. *Asymptotic analysis, part 1.* 1974.

55 M. Hall, Jr., J.H. van Lint (eds.). *Combinatorics, part 1: theory of designs, finite geometry and coding theory.* 1974.

56 M. Hall, Jr., J.H. van Lint (eds.). *Combinatorics, part 2: graph theory, foundations, partitions and combinatorial geometry.* 1974.

57 M. Hall, Jr., J.H. van Lint (eds.). *Combinatorics, part 3: combinatorial group theory.* 1974.

58 W. Albers. *Asymptotic expansions and the deficiency concept in statistics.* 1975.

59 J.L. Mijnheer. *Sample path properties of stable processes.* 1975.

60 F. Göbel. *Queueing models involving buffers.* 1975.

63 J.W. de Bakker (ed.). *Foundations of computer science.* 1975.

64 W.J. de Schipper. *Symmetric closed categories.* 1975.

65 J. de Vries. *Topological transformation groups, 1: a categorical approach.* 1975.

66 H.G.J. Pijls. *Logically convex algebras in spectral theory and eigenfunction expansions.* 1976.

68 P.P.N. de Groen. *Singularly perturbed differential operators of second order.* 1976.

69 J.K. Lenstra. *Sequencing by enumerative methods.* 1977.

70 W.P. de Roever, Jr. *Recursive program schemes: semantics and proof theory.* 1976.

71 J.A.E.E. van Nunen. *Contracting Markov decision processes.* 1976.

72 J.K.M. Jansen. *Simple periodic and non-periodic Lamé functions and their applications in the theory of conical waveguides.* 1977.

73 D.M.R. Leivant. *Absoluteness of intuitionistic logic.* 1979.

74 H.J.J. te Riele. *A theoretical and computational study of generalized aliquot sequences.* 1976.

75 A.E. Brouwer. *Treelike spaces and related connected topological spaces.* 1977.

76 M. Rem. *Associons and the closure statements.* 1976.

77 W.C.M. Kallenberg. *Asymptotic optimality of likelihood ratio tests in exponential families.* 1978.

78 E. de Jonge, A.C.M. van Rooij. *Introduction to Riesz spaces.* 1977.

79 M.C.A. van Zuijlen. *Empirical distributions and rank statistics.* 1977.

80 P.W. Hemker. *A numerical study of stiff two-point boundary problems.* 1977.

81 K.R. Apt, J.W. de Bakker (eds.). *Foundations of computer science II, part 1.* 1976.

82 K.R. Apt, J.W. de Bakker (eds.). *Foundations of computer science II, part 2.* 1976.

83 L.S. van Benthem Jutting. *Checking Landau's "Grundlagen" in the AUTOMATH system.* 1979.

84 H.L.L. Busard. *The translation of the elements of Euclid from the Arabic into Latin by Hermann of Carinthia (?), books vii-xii.* 1977.

85 J. van Mill. *Supercompactness and Wallmann spaces.* 1977.

86 S.G. van der Meulen, M. Veldhorst. *Torrix I, a programming system for operations on vectors and matrices over arbitrary fields and of variable size.* 1978.

88 A. Schrijver. *Matroids and linking systems.* 1977.

89 J.W. de Roever. *Complex Fourier transformation and analytic functionals with unbounded carriers.* 1978.

90 L.P.J. Groenewegen. *Characterization of optimal strategies in dynamic games.* 1981.

91 J.M. Geysel. *Transcendence in fields of positive characteristic.* 1979.

92 P.J. Weeda. *Finite generalized Markov programming.* 1979.

93 H.C. Tijms, J. Wessels (eds.). *Markov decision theory.* 1977.

94 A. Bijlsma. *Simultaneous approximations in transcendental number theory.* 1978.

95 K.M. van Hee. *Bayesian control of Markov chains.* 1978.

96 P.M.B. Vitányi. *Lindenmayer systems: structure, languages, and growth functions.* 1980.

97 A. Federgruen. *Markovian control problems; functional equations and algorithms.* 1984.

98 R. Geel. *Singular perturbations of hyperbolic type.* 1978.

99 J.K. Lenstra, A.H.G. Rinnooy Kan, P. van Emde Boas (eds.). *Interfaces between computer science and operations research.* 1978.

100 P.C. Baayen, D. van Dulst, J. Oosterhoff (eds.). *Proceedings bicentennial congress of the Wiskundig Genootschap, part 1.* 1979.

101 P.C. Baayen, D. van Dulst, J. Oosterhoff (eds.). *Proceedings bicentennial congress of the Wiskundig Genootschap, part 2.* 1979.

102 D. van Dulst. *Reflexive and superreflexive Banach spaces.* 1978.

103 K. van Harn. *Classifying infinitely divisible distributions by functional equations.* 1978.

104 J.M. van Wouwe. *GO-spaces and generalizations of metrizability.* 1979.

105 R. Helmers. *Edgeworth expansions for linear combinations of order statistics.* 1982.

106 A. Schrijver (ed.). *Packing and covering in combinatorics.* 1979.

107 C. den Heijer. *The numerical solution of nonlinear operator equations by imbedding methods.* 1979.

108 J.W. de Bakker, J. van Leeuwen (eds.). *Foundations of computer science III, part 1.* 1979.

109 J.W. de Bakker, J. van Leeuwen (eds.). *Foundations of computer science III, part 2.* 1979.

110 J.C. van Vliet. *ALGOL 68 transput, part I: historical review and discussion of the implementation model.* 1979.

111 J.C. van Vliet. *ALGOL 68 transput, part II: an implementation model.* 1979.

112 H.C.P. Berbee. *Random walks with stationary increments and renewal theory.* 1979.

113 T.A.B. Snijders. *Asymptotic optimality theory for testing problems with restricted alternatives.* 1979.

114 A.J.E.M. Janssen. *Application of the Wigner distribution to harmonic analysis of generalized stochastic processes.* 1979.

115 P.C. Baayen, J. van Mill (eds.). *Topological structures II, part 1.* 1979.

116 P.C. Baayen, J. van Mill (eds.). *Topological structures II, part 2.* 1979.

117 P.J.M. Kallenberg. *Branching processes with continuous state space.* 1979.

118 P. Groeneboom. *Large deviations and asymptotic efficiencies.* 1980.

119 F.J. Peters. *Sparse matrices and substructures, with a novel implementation of finite element algorithms.* 1980.

120 W.P.M. de Ruyter. *On the asymptotic analysis of large-scale ocean circulation.* 1980.

121 W.H. Haemers. *Eigenvalue techniques in design and graph theory.* 1980.

122 J.C.P. Bus. *Numerical solution of systems of nonlinear equations.* 1980.

123 I. Yuhász. *Cardinal functions in topology - ten years later.* 1980.

124 R.D. Gill. *Censoring and stochastic integrals.* 1980.

125 R. Eising. *2-D systems, an algebraic approach.* 1980.

126 G. van der Hoek. *Reduction methods in nonlinear programming.* 1980.

127 J.W. Klop. *Combinatory reduction systems.* 1980.

128 A.J.J. Talman. *Variable dimension fixed point algorithms and triangulations.* 1980.

129 G. van der Laan. *Simplicial fixed point algorithms.* 1980.

130 P.J.W. ten Hagen, T. Hagen, P. Klint, H. Noot, H.J. Sint, A.H. Veen. *ILP: intermediate language for pictures.* 1980.

131 R.J.R. Back. *Correctness preserving program refinements: proof theory and applications.* 1980.

132 H.M. Mulder. *The interval function of a graph.* 1980.

133 C.A.J. Klaassen. *Statistical performance of location estimators.* 1981.

134 J.C. van Vliet, H. Wupper (eds.). *Proceedings international conference on ALGOL 68.* 1981.

135 J.A.G. Groenendijk, T.M.V. Janssen, M.J.B. Stokhof (eds.). *Formal methods in the study of language, part I.* 1981.

136 J.A.G. Groenendijk, T.M.V. Janssen, M.J.B. Stokhof (eds.). *Formal methods in the study of language, part II.* 1981.

137 J. Telgen. *Redundancy and linear programs.* 1981.

138 H.A. Lauwerier. *Mathematical models of epidemics.* 1981.

139 J. van der Wal. *Stochastic dynamic programming, successive approximations and nearly optimal strategies for Markov decision processes and Markov games.* 1981.

140 J.H. van Geldrop. *A mathematical theory of pure exchange economies without the no-critical-point hypothesis.* 1981.

141 G.E. Welters. *Abel-Jacobi isogenies for certain types of Fano threefolds.* 1981.

142 H.R. Bennett, D.J. Lutzer (eds.). *Topology and order structures, part 1.* 1981.

143 J.M. Schumacher. *Dynamic feedback in finite- and infinite-dimensional linear systems.* 1981.

144 P. Eijgenraam. *The solution of initial value problems using interval arithmetic; formulation and analysis of an algorithm.* 1981.

145 A.J. Brentjes. *Multi-dimensional continued fraction algorithms.* 1981.

146 C.V.M. van der Mee. *Semigroup and factorization methods in transport theory.* 1981.

147 H.H. Tigelaar. *Identification and informative sample size.* 1982.

148 L.C.M. Kallenberg. *Linear programming and finite Markovian control problems.* 1983.

149 C.B. Huijsmans, M.A. Kaashoek, W.A.J. Luxemburg, W.K. Vietsch (eds.). *From A to Z, proceedings of a symposium in honour of A.C. Zaanen.* 1982.

150 M. Veldhorst. *An analysis of sparse matrix storage schemes.* 1982.

151 R.J.M.M. Does. *Higher order asymptotics for simple linear rank statistics.* 1982.

152 G.F. van der Hoeven. *Projections of lawless sequencies.* 1982.

153 J.P.C. Blanc. *Application of the theory of boundary value problems in the analysis of a queueing model with paired services.* 1982.

154 H.W. Lenstra, Jr., R. Tijdeman (eds.). *Computational methods in number theory, part I.* 1982.

155 H.W. Lenstra, Jr., R. Tijdeman (eds.). *Computational methods in number theory, part II.* 1982.

156 P.M.G. Apers. *Query processing and data allocation in distributed database systems.* 1983.

157 H.A.W.M. Kneppers. *The covariant classification of two-dimensional smooth commutative formal groups over an algebraically closed field of positive characteristic.* 1983.

158 J.W. de Bakker, J. van Leeuwen (eds.). *Foundations of computer science IV, distributed systems, part 1.* 1983.

159 J.W. de Bakker, J. van Leeuwen (eds.). *Foundations of computer science IV, distributed systems, part 2.* 1983.

160 A. Rezus. *Abstract AUTOMATH.* 1983.

161 G.F. Helminck. *Eisenstein series on the metaplectic group, an algebraic approach.* 1983.

162 J.J. Dik. *Tests for preference.* 1983.

163 H. Schippers. *Multiple grid methods for equations of the second kind with applications in fluid mechanics.* 1983.

164 F.A. van der Duyn Schouten. *Markov decision processes with continuous time parameter.* 1983.

165 P.C.T. van der Hoeven. *On point processes.* 1983.

166 H.B.M. Jonkers. *Abstraction, specification and implementation techniques, with an application to garbage collection.* 1983.

167 W.H.M. Zijm. *Nonnegative matrices in dynamic programming.* 1983.

168 J.H. Evertse. *Upper bounds for the numbers of solutions of diophantine equations.* 1983.

169 H.R. Bennett, D.J. Lutzer (eds.). *Topology and order structures, part 2.* 1983.