Geometric quadratic chabauty and other topics in number theory

Lido, G.M.

Chapter 2

Formal biextensions and quadratic Chabauty

The proof of Theorem 1.4.10 in the previous chapter uses the formal logarithm of the two formal group laws associated to the biextension $P^{\times,\rho-1} \to J \times J^{\vee,\rho-1}$. Hence it uses that both laws are trivializable, that is they are both isomorphic to the additive law (over different bases).

In this chapter we study formal biextension laws and the main result implies that it is possible to trivialize both group laws of $P^{\times,\rho-1}$ simultaneously. We also prove that the power series defining the trivialization converge on the residue disk of the neutral element of $P^{\times,\rho-1}(\mathbb{Z}_p)$ if $p > 2$. This leads to another proof of Theorem 1.4.10. Notice that the triviality of commutative formal biextensions in characteristic zero was already treated in Section 1.9.2, but here we give a different proof, working directly with rings of power series.

2.1 Recap on formal group laws

Given a ring R, a *formal group law* of dimension d over R is a system $F = (F_1, \dots F_d)$ of power series in $2d$ indeterminates $x' = \{x'_1, \dots, x'_d\}$, $x'' = \{x''_1, \dots, x''_d\}$ such that

(I) $F(x', 0) = x'$ and $F(0, x'') = x''$;

(II) $F(x', F(x'', x''')) = F(F(x', x''), x''')$.

The first property implies that

$$F_i \equiv x'_i + x''_i \text{ mod terms of degree} \geq 2\,, \tag{2.1.1}$$

hence the substitution in the second property makes sense.

Let us rephrase this definition. Given a system of indeterminates $t = \{t_1, \dots, t_n\}$, the ring of formal power series $R[\![t]\!] = R[\![t_1, \dots, t_n]\!]$ is complete and separated with respect to the $(t_1, \dots, t_n)$-adic topology. Denoting $\hat{\otimes}_R$ the completed tensor product of linearly topologized R-modules (we give R the discrete topology), we have a unique continuous isomorphism of R-algebras

$$R[\![x'_1, \dots, x'_d, x''_1, \dots x''_d]\!] = R[\![x_1, \dots, x_d]\!] \hat{\otimes}_R R[\![x_1, \dots, x_d]\!] \tag{2.1.2}$$

sending x'_i to $x_i \otimes 1$ and x''_i to $1 \otimes x_i$. Hence, the choice of elements $F_1, \dots, F_d$ in the ring $R[\![x_1, \dots, x'_d, x''_1, \dots, x''_d]\!]$ is equivalent to the choice of a morphism of R-algebras $R[x_1, \dots, x_d] \to R[\![x_1, \dots, x_d]\!] \hat{\otimes}_R R[\![x_1, \dots, x_d]\!]$. Such a map extends to a continuous morphism of R-algebras

$$A \colon R[\![x_1, \dots, x_d]\!] \longrightarrow R[\![x_1, \dots, x_d]\!] \hat{\otimes}_R R[\![x_1, \dots, x_d]\!]$$

if and only if for each i we have $F_i(0, 0) = 0$, which is the case for formal group laws. We can also reformulate properties (I) and (II) in terms of A: denoting x the system of indeterminates $\{x_1, \dots, x_d\}$ and $e \colon R[\![x]\!] \to R$ the homomorphism evaluating power series at $x_1 = \dots = x_d = 0$, they are equivalent to the commutation of the following diagrams (2.1.3)

$$\begin{array}{ccc} R[\![x]\!] & \xrightarrow{A} & R[\![x]\!] \hat{\otimes}_R R[\![x]\!] \\ \downarrow{\scriptstyle A} & \searrow^{\mathrm{id}} & \downarrow{\scriptstyle \mathrm{id} \hat{\otimes}_R e} \\ R[\![x]\!] \hat{\otimes}_R R[\![x]\!] & \xrightarrow{e \hat{\otimes}_R \mathrm{id}} & R[\![x]\!] \end{array} \qquad \begin{array}{ccc} R[\![x]\!] & \xrightarrow{A} & R[\![x]\!] \hat{\otimes}_R R[\![x]\!] \\ \downarrow{\scriptstyle A} & & \downarrow{\scriptstyle \mathrm{id} \hat{\otimes}_R A} \\ R[\![x]\!] \hat{\otimes}_R R[\![x]\!] & \xrightarrow{A \hat{\otimes}_R \mathrm{id}} & R[\![x]\!] \hat{\otimes}_R R[\![x]\!] \hat{\otimes}_R R[\![x]\!] \end{array} .$$

Hence, by formal group law of dimension d, we also mean a continuous homomorphism of R-algebras $A \colon R[\![x_1, \dots, x_d]\!] \to R[\![x_1, \dots, x_d]\!] \hat{\otimes}_R R[\![x_1, \dots, x_d]\!]$ such that the above diagrams commute. Given two formal group laws A, B of dimensions a, b, a homomorphism between A and B is a continuous homomorphism $\phi \colon R[\![x_1, \dots, x_a]\!] \to R[\![x_1, \dots, x_b]\!]$ such that $(\phi \hat{\otimes}_R \phi) \circ A = B \circ \phi$.

We notice that the above diagrams say that $\mathrm{Spf}(R[\![x]\!])$, with multiplication given by $\mathrm{Spf}(A)$ and neutral element $\mathrm{Spf}(e)$, is a formal group scheme over R (the existence of the "inverse" morphism $\mathrm{Spf}(R[\![x]\!]) \to \mathrm{Spf}(R[\![x]\!])$ is proven in [45, P3, Proposition 1]).

Let $S \colon R[\![x]\!] \hat{\otimes}_R R[\![x]\!] \to R[\![x]\!] \hat{\otimes}_R R[\![x]\!]$ be the "symmetry" homomorphism. We say that a formal group law A is *commutative* if $S \circ A = A$. Equivalently a formal group law $F = (F_1, \dots, F_d)$ is commutative if $F(x', x'') = F(x'', x')$. An example of commutative formal group law is the *additive formal group law AD* of dimension d, defined by

$$AD(x_i) = x_i \hat{\otimes} 1 + 1 \hat{\otimes} x_i = x'_i + x''_i \, .$$

As proved in [54, Theorem 1], when $\mathbb{Q} \subset R$ the additive formal group law is the fundamental example of commutative formal group law: given a commutative formal group law

A of dimension d over a $\mathbb{Q}$-algebra R, there exists an isomorphism $\log_A\colon R[\![x]\!] \to R[\![x]\!]$ between the additive formal group law of dimension d and A. Moreover by [54, Proposition 1.6], such an isomorphism is unique when we require that it reduces to the identity modulo the ideal $(x_1, \dots, x_d)^2 \subset R[\![x]\!]$ and we refer to it as *formal logarithm of A*.

Given an R-algebra R', considered with the discrete topology, and a formal group law $A\colon R[\![x]\!] \to R[\![x]\!] \hat{\otimes}_R R[\![x]\!]$ over R, we denote $A_{R'}$ the formal group law over R' defined as $R' \hat{\otimes}_R A\colon R'[\![x]\!] \to R'[\![x]\!] \hat{\otimes}_{R'} R'[\![x]\!]$.

Finally, we recall that, given a formal group $A\colon R[\![x]\!] \to R[\![x]\!] \hat{\otimes}_R R[\![x]\!]$ of dimension a, we can talk about "points on A". Given an adic R-algebra S, namely an R-algebra which is also a separated and complete topological ring whose topology is induced by some ideal $I \subset S$, we define the set of S-valued points of A to be

$$A(S) := \mathrm{Hom}_{\mathrm{cont}}(R[\![x]\!], S) = (\mathfrak{N}_S)^a\,,$$

where $\mathfrak{N}_S$ denotes the ideal of topologically nilpotent elements in S. Since

$$\mathrm{Hom}_{\mathrm{cont}}(R[\![x]\!], S) \times \mathrm{Hom}_{\mathrm{cont}}(R[\![x]\!], S) = \mathrm{Hom}_{\mathrm{cont}}(R[\![x]\!] \hat{\otimes}_R R[\![x]\!], S)\,,$$

the formal group law A defines a group structure on $A(S)$ with neutral element $(0, \dots, 0)$. Hence A defines a covariant functor from the category of topological R-algebras to the category of groups. Vice versa suppose that A is a covariant functor from the category of adic R-algebras to the category of groups and suppose that there exists a positive integer a such that, functorially in S, we have a bijection $A(S) = (\mathfrak{N}_S)^a$ sending the neutral element to $(0, \dots, 0)$; then, by Yoneda's lemma, A is the functor of points of a formal group law. We call *formal groups* such functors.

We notice that a formal group law A is commutative if and only if for every S the group $A(S)$ is commutative. Moreover, given two formal group laws A and B, Yoneda's lemma tells us that giving a morphism between A and B is the same as giving a natural transformation between their functors of points, but going in the opposite direction.

Remark 2.1.4. One could give a more general notion of formal group by substituting $R[\![x]\!]$ with any *admissible* ring, (see Definition 7.1.2 in [41]), so that the relative tangent space of the formal group is not forced to be free. Anyway, we do not need this generality for our purposes.

2.2 Commutative formal biextension laws

One way to define a formal biextensions is by using the functorial point of view, as done in [80]. Given three formal groups

$$A, B, C\colon \text{Adic } R\text{-Algebras} \longrightarrow \text{Groups}$$

a biextension of A and B by C is a functor

$$D\colon \text{Adic } R\text{-Algebras} \longrightarrow \text{Sets}$$

such that functorially in S, the set $D(S)$ is a biextension of $A(S) \times B(S)$ by $C(S)$, in the sense of Section 1.2. Given three other formal groups F, G, H and a bi-extension K of F, G by H, a morphism between D and K is a triple of natural transformations $(A{\to}F, B{\to}G, D{\to}K)$ that commute with the (partial) group laws and with the natural transformations $D \to A \times B$ and $K \to F \times G$.

We can also give a "dual" definition, using rings of power series, which is more cumbersome, but useful in our proof of Theorem 2.2.3. Suppose we are given a ring R and three formal group laws

$$A\colon R[\![x]\!] \to R[\![x]\!] \hat{\otimes}_R R[\![x]\!]\,, \quad B\colon R[\![y]\!] \to R[\![y]\!] \hat{\otimes}_R R[\![y]\!]\,, \quad C\colon R[\![z]\!] \to R[\![z]\!] \hat{\otimes}_R R[\![z]\!]\,,$$

with $x = \{x_1, \ldots, x_a\}$, $y = \{y_1, \ldots, y_b\}$, $z = \{z_1, \ldots, z_c\}$ being system of indeterminates. A biextension of A and B by C is a pair of formal group laws

$$\begin{aligned} \mathcal{A}\colon R[\![x,y,z]\!] &\longrightarrow R[\![x,y,z]\!] \hat{\otimes}_{R[\![y]\!]} R[\![x,y,z]\!] = R[\![x',x'',y,z',z'']\!] \qquad \text{over } R[\![y]\!]\,,\\ \mathcal{B}\colon R[\![x,y,z]\!] &\longrightarrow R[\![x,y,z]\!] \hat{\otimes}_{R[\![x]\!]} R[\![x,y,z]\!] = R[\![x,y',y'',z',z'']\!] \qquad \text{over } R[\![x]\!]\,, \end{aligned}$$

such that $\mathcal{A}$ is an extension of $A\hat{\otimes}_R R[\![y]\!]$ by $C\hat{\otimes}_R R[\![y]\!]$, $\mathcal{B}$ is an extension of $B\hat{\otimes}_R R[\![x]\!]$ by $C\hat{\otimes}_R R[\![x]\!]$, and moreover $\mathcal{A}$ and $\mathcal{B}$ are compatible in the "dual sense" of (1.2.5). More explicitly we require that:

(i) the inclusion $R[\![x,y]\!] \to R[\![x,y,z]\!]$ is both a homomorphism between $A_{R[\![y]\!]}$ and $\mathcal{A}$ and also an homomorphism between $B_{R[\![x]\!]}$ and $\mathcal{B}$;

(ii) the continuous homomorphism of R-algebras $R[\![x,y,z]\!] \to R[\![y,z]\!]$ evaluating power series at $x_1{=}\ldots{=}x_a{=}0$ is a homomorphism between $\mathcal{A}$ and $C_{R[\![y]\!]}$ and the continuous homomorphism of R-algebras $R[\![x,y,z]\!] \to R[\![x,z]\!]$ evaluating power series at $y_1{=}\ldots{=}y_b{=}0$ is a homomorphism between $\mathcal{B}$ and $C_{R[\![x]\!]}$;

(iii) using the isomorphism (2.1.2), the following diagram commutes

$$\begin{array}{ccc} R[\![x,y,z]\!] & \xrightarrow{\quad\mathcal{A}\quad} & R[\![x',x',y,z',z'']\!] \\ \big\downarrow{\scriptstyle\mathcal{B}} & & \big\downarrow{\scriptstyle\mathcal{B}\hat{\otimes}\mathcal{B}} \\ R[\![x,y',y'',z',z'']\!] & \xrightarrow{\mathcal{A}\hat{\otimes}\mathcal{A}} & R[\![x',x',y',y'',z',z''z''',z^{(iv)}]\!]\,, \end{array} \tag{2.2.1}$$

where both the $(R[\![x,y,z]\!] \hat{\otimes}_{R[\![x]\!]} R[\![x,y,z]\!]) \hat{\otimes}_{R[\![y]\!]\,\hat{\otimes}_R\, R[\![y]\!]} (R[\![x,y,z]\!] \hat{\otimes}_{R[\![x]\!]} R[\![x,y,z]\!])$ and $(R[\![x,y,z]\!] \hat{\otimes}_{R[\![y]\!]} R[\![x,y,z]\!]) \hat{\otimes}_{R[\![x]\!]\,\hat{\otimes}_R\, R[\![x]\!]} (R[\![x,y,z]\!] \hat{\otimes}_{R[\![y]\!]} R[\![x,y,z]\!])$ are identified with $R[\![x',x',y',y'',z',z''z''',z^{(iv)}]\!]$, in the first case with $(z{\otimes}1){\otimes}(1{\otimes}1) \leftrightarrow z'$,

$(1\otimes z)\otimes(1\otimes 1) \leftrightarrow z''$, $(1\otimes 1)\otimes(z\otimes 1) \leftrightarrow z'''$, $(1\otimes 1)\otimes(1\otimes z) \leftrightarrow z^{(iv)}$ and in the second case with $(z\otimes 1)\otimes(1\otimes 1) \leftrightarrow z'$, $(1\otimes z)\otimes(1\otimes 1) \leftrightarrow z'''$, $(1\otimes 1)\otimes(z\otimes 1) \leftrightarrow z''$, $(1\otimes 1)\otimes(1\otimes z) \leftrightarrow z^{(iv)}$.

We call such an object $(\mathcal{A},\mathcal{B})$ a *formal biextension law*. Now suppose we are given three other formal group laws

$$H\colon R[\![u]\!] \to R[\![u]\!]\,\hat{\otimes}_R R[\![u]\!]\,, \quad J\colon R[\![v]\!] \to R[\![v]\!]\,\hat{\otimes}_R R[\![v]\!]\,, \quad K\colon R[\![w]\!] \to R[\![w]\!]\,\hat{\otimes}_R R[\![w]\!]\,,$$

and a biextension $(\mathcal{H},\mathcal{J})$ of H and J by K. Then a morphism between $(\mathcal{A},\mathcal{B})$ and $(\mathcal{H},\mathcal{J})$ is a morphism $\phi\colon R[\![x,y,z]\!] \to R[\![u,v,w]\!]$ such that

- ϕ restricts to maps $\phi^x\colon R[\![x]\!] \to R[\![u]\!]$ and $\phi^y\colon R[\![y]\!] \to R[\![v]\!]$ such that ϕ^x is a morphism between A and H and ϕ^y is a morphism between B and J;
- the following diagrams are commutative

$$\begin{array}{ccc} R[\![x,y,z]\!] & \xrightarrow{\mathcal{A}} & R[\![x,y,z]\!]\hat{\otimes}_{R[\![y]\!]}R[\![x,y,z]\!] \\ \downarrow{\scriptstyle\phi} & & \downarrow{\scriptstyle\phi\,\hat{\otimes}_{\phi^y}\,\phi} \\ R[\![u,v,w]\!] & \xrightarrow{\mathcal{H}} & R[\![u,v,w]\!]\hat{\otimes}_{R[\![v]\!]}R[\![u,v,w]\!] \end{array} \qquad \begin{array}{ccc} R[\![x,y,z]\!] & \xrightarrow{\mathcal{B}} & R[\![x,y,z]\!]\hat{\otimes}_{R[\![x]\!]}R[\![x,y,z]\!] \\ \downarrow{\scriptstyle\phi} & & \downarrow{\scriptstyle\phi\,\hat{\otimes}_{\phi^x}\,\phi} \\ R[\![u,v,w]\!] & \xrightarrow{\mathcal{J}} & R[\![u,v,w]\!]\hat{\otimes}_{R[\![u]\!]}R[\![u,v,w]\!] \end{array}$$

In this setting the functor $D{=}(\mathcal{A},\mathcal{B})$ going from topological R-algebras to sets defined as

$$(\mathcal{A},\mathcal{B})(S) = \mathrm{Hom}_{\mathrm{cont}}(R[\![x,y,z]\!],S) = \mathfrak{N}_S^{a+b+c}$$

has two partial group laws induced by $\mathcal{A}$ and $\mathcal{B}$ that make D a biextension of the functors of groups A and B by C. Vice versa if D is a biextension of the functors of groups A and B by C, then one can show that D is representable by $R[\![x,y,z]\!]$ in such a way that the natural transformation $D \to A\times B$ is induced by the inclusion $R[\![x,y]\!] \to R[\![x,y,z]\!]$ and the natural transformations $A\times C, B\times C \to D$ describing the kernels of $D \to A\times B$ are induced by the maps $R[\![x,y,z]\!] \to R[\![x,z]\!], R[\![y,z]\!]$ sending y or x to zero. This is enough to prove that every formal biextension is induced by a formal biextension law.

We say that a formal biextension law $(\mathcal{A},\mathcal{B})$ is commutative if both $\mathcal{A}$ and $\mathcal{B}$ are commutative group laws. Given additive formal group laws AD_1, AD_2, AD_3 of dimensions d_1,d_2,d_3, the additive formal biextension law of dimensions (d_1,d_2,d_3) is the commutative formal biextension law $(\mathcal{AD}_1,\mathcal{AD}_2)$ of AD_1 and AD_2 by AD_3 given by

$$\begin{aligned} &\mathcal{AD}_1(x_i) = x_i\otimes 1 + 1\otimes x_i = x_i' + x_i''\,, \quad \mathcal{AD}_2(y_i) = y_i\otimes 1 + 1\otimes y_i = y_i' + y_i''\,, \\ &\mathcal{AD}_1(z_i) = z_i\otimes 1 + 1\otimes z_i = z_i' + z_i''\,, \quad \mathcal{AD}_2(z_i) = z_i\otimes 1 + 1\otimes z_i = z_i' + z_i''\,. \end{aligned} \tag{2.2.2}$$

In the next theorem we prove that every commutative biextension over R is isomorphic to an additive biextension, if $\mathbb{Q}\subset R$.

Theorem 2.2.3. *Let R be a $\mathbb{Q}$-algebra, let $x = \{x_1, \dots, x_a\}$, $y = \{y_1, \dots, y_b\}$ and $z = \{z_1, \dots, z_c\}$ be systems of indeterminates, let*

$$A\colon R[\![x]\!] \to R[\![x]\!] \hat{\otimes}_R R[\![x]\!], \quad B\colon R[\![y]\!] \to R[\![y]\!] \hat{\otimes}_R R[\![y]\!], \quad C\colon R[\![z]\!] \to R[\![z]\!] \hat{\otimes}_R R[\![z]\!],$$

be three formal group laws over R and let $(\mathcal{A}, \mathcal{B})$ be a commutative formal biextension of A, B by C. Let $\mathcal{I} \subset R[\![x, y, z]\!]$ be the ideal $(x_1, \dots, x_a, z_1, \dots, z_c)^2 + (y_1, \dots, y_b, z_1, \dots, z_c)^2$.

Then there is a unique isomorphism $\psi\colon R[\![x, y, z]\!] \to R[\![x, y, z]\!]$ between the additive formal biextension law of dimensions (a, b, c) and $(\mathcal{A}, \mathcal{B})$ such that ψ reduces to the identity modulo $\mathcal{I}$. Moreover such a ψ restricts to $\psi|_{R[\![x]\!]} = \log_A\colon R[\![x]\!] \to R[\![x]\!]$ and $\psi|_{R[\![y]\!]} = \log_B\colon R[\![y]\!] \to R[\![y]\!]$.

Proof. We first prove the uniqueness. Since two isomorphisms between the additive formal biextension $(\mathcal{AD}_1, \mathcal{AD}_2)$ of dimensions (a, b, c) and $(\mathcal{A}, \mathcal{B})$ differ by automorphisms of $(\mathcal{AD}_1, \mathcal{AD}_2)$, it is enough to prove uniqueness in the case $(\mathcal{A}, \mathcal{B}) = (\mathcal{AD}_1, \mathcal{AD}_2)$. Let ψ be an automorphism of $(\mathcal{AD}_1, \mathcal{AD}_2)$ reducing to the identity modulo $\mathcal{I}$. By definition of homomorphism of formal biextension laws, ψ restricts to an automorphism $\psi^x\colon R[\![x]\!] \to R[\![x]\!]$ of the additive formal group law A and, by the hypothesis on ψ mod $\mathcal{I}$, ψ^x reduces to the identity modulo $(x_1, \dots, x_a)^2$. Then, by uniqueness of the formal logarithm,

$$\psi^x = \mathrm{id}_{R[\![x]\!]},$$

hence $\psi\colon R[\![x]\!][\![y, z]\!] \to R[\![x]\!][\![y, z]\!]$ is a morphism of $R[\![x]\!]$-algebras. This, together with the definition of homomorphism of formal biextension, implies that ψ is an automorphism of the additive biextension law $\mathcal{AD}_2$. Symmetrically $\psi^y := \psi|_{R[\![y]\!]} = \mathrm{id}_{R[\![y]\!]}$ and ψ is an automorphism of the additive biextension law $\mathcal{AD}_1$. Since all the homomorphisms of additive groups are linear, there exist power series $\lambda_{i,j}, \mu_{i,k} \in R[\![x]\!]$ and $\sigma_{i,j}, \tau_{i,l} \in R[\![y]\!]$ such that

$$\psi(z_i) = z_i + \sum_{j=1}^{c} \lambda_{i,j}(x) z_j + \sum_{k=1}^{b} \mu_{i,k}(x) y_k = z_i + \sum_{j=1}^{c} \sigma_{i,j}(y) z_j + \sum_{l=1}^{a} \tau_{i,l}(y) x_l.$$

We deduce that $\lambda_{i,j}(x) = \sigma_{i,j}(y)$ is constant, and since $\psi(z_i) \equiv z_i$ modulo I, we deduce that $\lambda_{i,j}(x) = \sigma_{i,j}(y) = 0$. The above equation also implies that power series $\mu_{i,j}(x)$ are linear polynomials in the x_l's. Hence $\psi(z_i) - z_i$ is a linear combination of the monomials $y_k x_l$ and, since it belongs to I, we deduce that $\psi(z_i) - z_i = 0$.

We have proved that ψ and the identity agree when evaluated on all the x_l's, y_k's and z_j's, hence, by continuity, ψ is the identity, which proves the uniqueness.

For the existence of ψ we proceed in four steps, that is we define automorphisms $\psi_1, \psi_2, \psi_3, \psi_4$ of $R[\![x, y, z]\!]$ whose composition $\psi_4 \circ \psi_3 \circ \psi_2 \circ \psi_1$ is the ψ we are looking for.

Let ψ_1 be the formal logarithm of $\mathcal{B}$. By definition we have $\psi_1^x := \psi_1|_{R[\![x]\!]} = \mathrm{id}_{R[\![x]\!]}$ and, by the explicit formulas for the formal logarithm in [54, Proposition 1.1 and Theorem 1] and the fact that $\mathcal{B}|_{R[\![y]\!]} = B$, the map $\psi_1^y := \psi_1|_{R[\![y]\!]}$ is equal to the formal logarithm of B. In particular ψ_1 restricts to an automorphism of both $R[\![x]\!]$ and $R[\![y]\!]$, hence it makes sense to define the "pullback" $(\mathcal{A}_1, \mathcal{B}_1)$ of $(\mathcal{A}, \mathcal{B})$ by ψ_1: we define $\mathcal{A}_1$ and $\mathcal{B}_1$ to be the unique maps making the following diagrams commute

(2.2.3.1)

$$\begin{array}{ccc} R[\![x,y,z]\!] & \xrightarrow{\mathcal{A}_1} & R[\![x',x'',y,z',z'']\!] \\ \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_1 \hat{\otimes}_{\psi_1^y} \psi_1} \\ R[\![x,y,z]\!] & \xrightarrow{\mathcal{A}} & R[\![x',x'',y,z',z'']\!] \end{array} \qquad \begin{array}{ccc} R[\![x,y,z]\!] & \xrightarrow{\mathcal{B}_1} & R[\![x,y',y'',z',z'']\!] \\ \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_1 \hat{\otimes}_{\psi_1^x} \psi_1} \\ R[\![x,y,z]\!] & \xrightarrow{\mathcal{B}} & R[\![x,y',y'',z',z'']\!] \end{array} .$$

Then $(\mathcal{A}_1, \mathcal{B}_1)$ is a biextension of certain formal group laws A_1, B_1 by C_1: indeed we define $A_1 := \mathcal{A}_1|_{R[\![x]\!]}$, $B_1 := \mathcal{A}_1|_{R[\![y]\!]}$ and we define C_1 functorially by imposing that, for every adic R-algebra S, $C_1(S)$ is the set of points in $\mathfrak{N}_S^{a+b+c}$ that project to $(0,0) \in (A_1 \times B_1)(S)$ with the group law given by $\mathcal{A}_1$; it is easy to check, sometimes using the functorial point of view and sometimes using the ring theoretic point of view, that $\mathcal{A}_1$ and $\mathcal{B}_1$ are formal groups, that they are compatible in the sense of (2.2.1), that $\mathcal{A}_1$ is an extension of $(A_1)_{R[\![y]\!]}$ by $(C_1)_{R[\![y]\!]}$ and that $\mathcal{B}_1$ is an extension of $(B_1)_{R[\![x]\!]}$ by $(C_1)_{R[\![x]\!]}$.

The definition of ψ_1 as formal logarithm implies that $\mathcal{B}_1 = \mathcal{A}\mathcal{D}_2$ as in (2.2.2) and consequently both B_1 and C_1 are additive. Since $\psi_1^x = \mathrm{id}_{R[\![x]\!]}$, then $A_1 = A$.

Now we define $\psi_2 \colon R[\![x,y,z]\!] \to R[\![x,y,z]\!]$ to be the unique continuous morphism being equal to the identity when restricted to $R[\![y,z]\!]$ and equal to the formal logarithm of $A_1 = A$ when restricted to $R[\![x]\!]$. Since ψ_2 restricts to automorphisms ψ_2^x, ψ_2^y of $R[\![x]\!], R[\![y]\!]$, we can define the pullback $(\mathcal{A}_2, \mathcal{B}_2)$ of $(\mathcal{A}_1, \mathcal{B}_1)$ by the map ψ_2, in the same way we defined the pullback $(\mathcal{A}_1, \mathcal{B}_1)$ of $(\mathcal{A}, \mathcal{B})$. Again $(\mathcal{A}_2, \mathcal{B}_2)$ is a biextension of certain formal group laws A_2, B_2 by C_2.

Since ψ_2 acts as the identity on $R[\![y,z]\!]$ we check that $\mathcal{B}_1 = \mathcal{A}\mathcal{D}_2 = \mathcal{B}_2$, hence both B_2 and C_2 are additive. The map $\psi_2^x = \log_A$ is an isomorphism between A_2 and A_1, hence A_2 is an additive formal group law. For each $i = 1, \ldots, c$ let us now look at the power series

$$\mathcal{A}_2(z_i) = \sum_{I',I'',J,K',K''} \lambda_{I',I'',J,K',K''} (x')^{I'} (x'')^{I''} y^J (z')^{K'} (z'')^{K''}.$$

The compatibility (2.2.1) between $\mathcal{B}_2 = \mathcal{A}\mathcal{D}_2$ and $\mathcal{A}_2$ implies that

$$\mathcal{A}_2(z_i)(x', x'', y'+y'', z'+z'', z'''+z^{(iv)}) = \mathcal{A}_2(z_i)(x', x'', y', z', z''') + \mathcal{A}_2(z_i)(x', x'', y'', z'', z^{(iv)}).$$

Since in the R.H.S of this equation there is no monomial multiple of $y_i' y_j''$, by expanding the series on the L.H.S we see that $\lambda_{I',I'',J,K',K''} = 0$ if $|J| \geq 2$. Analogously by looking

at monomials multiple of $z'_i z''$ or multiple of $z'_i z_j^{(iv)}$ or multiple of $z_i''' z_j^{(iv)}$, we infer that $\lambda_{I',I'',J,K',K''} = 0$ if $|K' + K''| \geq 2$. By looking at monomials multiple of $z'_i y''_j$ or multiple of $z''_i y'_j$ we infer that $\lambda_{I',I'',J,K',K''} = 0$ if $|J+K''+K'| \geq 2$. The term $(x')^{I'}(x'')^{I''}$ appears with coefficient $\lambda_{I',I'',0,0,0}$ on the left and with coefficient $2\lambda_{I',I'',0,0,0}$ the right, thus we must have $\lambda_{I',I'',0,0,0} = 0$. We have proved that the only coefficients $\lambda_{I',I'',J,K',K''} \neq 0$ are the ones with $|J + K' + K''| = 1$, hence

$$\mathcal{A}_2(z_i) = \sum_{j=1}^{b} d_{i,j}(x', x'')y_j + \sum_{j=1}^{c} f_{i,j}(x', x'')z'_j + \sum_{j=1}^{c} e_{i,j}(x', x'')z''_j. \tag{2.2.3.2}$$

with appropriate $d_{i,j} f_{i,j}, e_{i,j} \in R[\![x]\!]$. By the commutativity of $\mathcal{A}_2$, for each $j \in \{1, \ldots, c\}$ we have $f_{i,j}(x', x'') = e_{i,j}(x'', x')$. Let $f(x', x'')$ be the matrix with (i, j)-entry equal to $f_{i,j}$, let $d(x', x'')$ be the matrix with (i, j)-entry equal to $d_{i,j}$ and let $\mathcal{A}_2(z)$ be the column vector $(\mathcal{A}_2(z_1), \ldots, \mathcal{A}_2(z_d))^t$. Looking at x, y, z, z', z'' as column vectors, we can rewrite equation (2.2.3.2) as

$$\mathcal{A}_2(z) = d(x', x'') \cdot y + f(x', x'') \cdot z' + f(x'', x') \cdot z'' \,. \tag{2.2.3.3}$$

The property (2.1.1) of formal group laws implies that f is congruent to the identity matrix modulo the ideal $(x'_1, x''_1, \ldots, x'_a, x''_a)$.In particular the determinant of f is invertible in $R[\![x', x'']\!]$, hence f has an inverse with coefficients in $R[\![x', x'']\!]$. Writing down the associativity of $\mathcal{A}_2$ (the right diagram in Equation (2.1.3)), we find the identity

$$f(x', x'' + x''') = f(x' + x'', x''') \cdot f(x', x'').$$

If we plug in the values $x' \leftarrow 0$, $x'' \leftarrow x'$ and $x''' \leftarrow x''$ we immediately see that

$$f(x', x'') = g(x' + x'') \cdot g(x')^{-1} \tag{2.2.3.4}$$

where $g(x) := f(0, x) \in R[\![x]\!]^{c \times c}$, which is invertible because f is invertible. We now define the continuous automorphism

$$\psi_3 \colon R[\![x, y, z]\!] \longrightarrow R[\![x, y, z]\!] \,, \quad x \longmapsto x \,, y \longmapsto y \,, z \longmapsto g(x) \cdot z \,.$$

Again let $(\mathcal{A}_3, \mathcal{B}_3)$ be the formal biextension law obtained pulling back $(\mathcal{A}_2, \mathcal{B}_2)$ by ψ_3. We now prove that $\mathcal{B}_3 = \mathcal{AD}_2$ and that $\mathcal{A}_3$ is "almost equal" to $\mathcal{AD}_1$. Using that ψ_3 acts as the identity on $R[\![x, y]\!]$, we check that $\mathcal{B}_3(y_i) = \mathcal{AD}_2(y_i)$ and that $\mathcal{A}_3(x_i) = \mathcal{AD}_1(x_i)$.

Using the isomorphism (2.1.2) and Equation (2.2.3.4) we get

$$\begin{aligned}
\mathcal{B}_3(z) &= (\psi_3 \hat{\otimes}_{R[\![x]\!]} \psi_3) \circ \mathcal{B}_2 \circ \psi_3^{-1}(z) = (\psi_3 \hat{\otimes}_{R[\![x]\!]} \psi_3) \circ \mathcal{B}_2(g(x)^{-1} \cdot z) \\
&= (\psi_3 \hat{\otimes}_{R[\![x]\!]} \psi_3)\big(g(x)^{-1} \cdot (z' + z'')\big) = g(x)^{-1} \cdot \big(g(x) \cdot z' + g(x) \cdot z''\big) \\
&= z' + z'' = \mathcal{AD}_2(z). \\
\mathcal{A}_3(z) &= (\psi_3 \hat{\otimes}_{R[\![x]\!]} \psi_3) \circ \mathcal{A}_2 \circ \psi_3^{-1}(z) = (\psi_3 \hat{\otimes}_{R[\![x]\!]} \psi_3) \circ \mathcal{A}_2(g(x)^{-1} \cdot z) \\
&= (\psi_3 \hat{\otimes}_{R[\![x]\!]} \psi_3)\big(g(x' + x'')^{-1} \cdot \big(d(x', x'') \cdot y + f(x', x'') \cdot z' + f(x'', x') \cdot z''\big)\big) \\
&= g(x' + x'')^{-1} \cdot \big(d(x', x'') \cdot y + f(x', x'') \cdot g(x') \cdot z' + f(x'', x') \cdot g(x'') \cdot z''\big) \\
&= z' + z'' + g(x' + x'')^{-1} \cdot d(x', x'') \cdot y = \mathcal{AD}_1(z) + g(x' + x'')^{-1} \cdot d(x', x'') y.
\end{aligned}$$

By the associativity and commutativity of $\mathcal{A}_3$ we can prove the following claim.

Claim 2.2.4. *There exists a unique matrix of power series $h(x) \in R[\![x]\!]^{c \times b}$ such that*

$$g(x' + x'')^{-1} \cdot d(x', x'') = h(x' + x'') - h(x') - h(x'') \quad \textit{and} \tag{2.2.4.1}$$

$$h(0) \equiv 0 \pmod{(x_1, \ldots, x_a)^2}. \tag{2.2.4.2}$$

Proof. We define $m(x', x'') := g(x' + x'')^{-1} d(x', x'')$. When proving the claim, we can work separately on each entry $m_{i,j}$ and $h_{i,j}$, hence we can consider m as an element in $R[\![x', x'']\!]$ and h as an element in $R[\![x]\!]$, instead of considering them as matrices on the same rings.

Notice that two solutions of (2.2.4.1) differ by a (matrix of) linear polynomial(s) in the x_i's, hence the congruence (2.2.4.2) ensures uniqueness. We now prove existence.

We know that a power series $S \in R[\![x', x'']\!] = R[\![x'']\!][\![x']\!]$ is zero if and only if $S(0, x'') = 0$ and $\partial S / \partial x_i' = 0$ for each $i \in \{0, \ldots, a\}$: applying this principle to our claim we get that, for any h, Equation (2.2.4.1) holds if and only if

$$m(0, x'') = -h(0) \qquad \text{and} \tag{2.2.4.3}$$

$$\frac{\partial m}{\partial x_i'}(x', x'') = \frac{\partial h}{\partial x_i}(x' + x'') - \frac{\partial h}{\partial x_i}(x') \qquad \forall i = 1, \ldots, a. \tag{2.2.4.4}$$

Equation (2.2.4.3) is equivalent to $h(0) = 0$: indeed $m(0, x'') = 0$ because the evaluation of $\mathcal{A}_3(z)$ at $x' = z' = 0$ is equal to z'', as implied by the first property in the definition of formal group laws (the one saying that "the point 0" is the neutral element). Moreover if $h(0) = 0$, then, up to adding a (matrix of) linear polynomial(s) in the x_i's, we can suppose that h is congruent to 0 modulo $(x_1, \ldots, x_a)^2$. Hence proving our claim is equivalent solving Equation (2.2.4.4) and $h(0) = 0$, which is in turn equivalent to finding

$n_1, \dots, n_a$ being (matrices with coefficients) in $R[\![x]\!]$ such that

$$n := \sum_{i=1}^{a} n_i(x)dx_i \quad \text{is a closed form} \qquad \text{and} \tag{2.2.4.5}$$

$$\frac{\partial m}{\partial x_i'}(x', x'') = n_i(x' + x'') - n_i(x') \qquad \forall i = 1, \dots, a. \tag{2.2.4.6}$$

Indeed, given h as in Equations (2.2.4.3), (2.2.4.4) we can take $n_i = \partial h/\partial x_i$ and given $n_1, \dots, n_a$ as above, since all closed forms in $R[\![x]\!]$ are exact, there exists a unique $h \in R[\![x]\!]$ such that $h(0) = 0$ and $\partial h/\partial x_i = n_i$. We now look for such n_i's.

Associativity of the formal group law $\mathcal{A}_3$ tells us that

$$m(x' + x'', x''') + m(x', x'') = m(x', x'' + x''') + m(x'', x''').$$

Taking the partial derivative with respect to x_i', we get

$$\frac{\partial m}{\partial x_i'}(x' + x'', x''') + \frac{\partial m}{\partial x_i'}(x', x'') = \frac{\partial m}{\partial x_i'}(x', x'' + x'''). \tag{2.2.4.7}$$

Plugging the values $x' \leftarrow 0$, $x'' \leftarrow x'$ and $x''' \leftarrow x''$ in the above equation we see that

$$n_i(x) := \frac{\partial m}{\partial x_i'}(0, x)\,,$$

automatically satisfy Equation (2.2.4.6). It remains to show that, with the above definition of the n_i's, Equation (2.2.4.5) is also satisfied. Taking the derivative of Equation (2.2.4.7) with respect to x_j''' we find

$$\frac{\partial^2 m}{\partial x_j'' \partial x_i'}(x' + x'', x''') = \frac{\partial^2 m}{\partial x_j'' \partial x_i'}(x', x'' + x'''). \tag{2.2.4.8}$$

The commutativity of $\mathcal{A}_3$ implies $m(x', x'') = m(x'', x')$, and taking two derivatives we get

$$\frac{\partial^2 m}{\partial x_i'' \partial x_j'}(x', x'') = \frac{\partial^2 m}{\partial x_j'' \partial x_i'}(x'', x'). \tag{2.2.4.9}$$

Deriving the definition of n_i and specializing Equations (2.2.4.8) and (2.2.4.9) in $x' \leftarrow 0$, $x'' \leftarrow x$, $x''' \leftarrow 0$, we find that for every $i, j = 1, \dots, a$

$$\frac{\partial n_i}{\partial x_j} = \frac{\partial^2 m}{\partial x_j'' \partial x_i'}(0, x) = \frac{\partial^2 m}{\partial x_j'' \partial x_i'}(x, 0) = \frac{\partial^2 m}{\partial x_i'' \partial x_j'}(0, x) = \frac{\partial n_j}{\partial x_i},$$

proving that the form n in Equation (2.2.4.5) is closed. □

Taking h as in the claim we define the continuous automorphism

$$\psi_4 \colon R[\![x,y,z]\!] \longrightarrow R[\![x,y,z]\!]\,, \quad x \longmapsto x\,, y \longmapsto y\,, z \longmapsto z + h(x)\cdot y\,,$$

and we define $(\mathcal{A}_4, \mathcal{B}_4)$ to be the pullback of the formal biextension law $(\mathcal{A}_4, \mathcal{B}_4)$ by ψ_4. We easily check that $\mathcal{B}_4 = \mathcal{AD}_2$ and $\mathcal{A}_4(y_i) = \mathcal{AD}_1(y_i)$. Moreover, using the definition of $\mathcal{A}_4$, the formula for $\mathcal{A}_3(z)$ we previously found and the definition of h, we get

$$\begin{aligned}
\mathcal{A}_4(z) &= (\psi_4 \hat{\otimes}_{R[\![x]\!]} \psi_4) \circ \mathcal{A}_3 \circ \psi_4^{-1}(z) = (\psi_4 \hat{\otimes}_{R[\![x]\!]} \psi_4) \circ \mathcal{A}_3\big(z - h(x)\cdot y\big) \\
&= (\psi_4 \hat{\otimes}_{R[\![x]\!]} \psi_4)\big(z' + z'' + g(x'+x'')^{-1}\cdot d(x', x'')\cdot y - h(x'+x'')\cdot y\big) \\
&= (\psi_4 \hat{\otimes}_{R[\![x]\!]} \psi_4)\big(z' + z'' - h(x')\cdot y - h(x'')\cdot y\big) \\
&= z' + h(x')\cdot y + z'' + h(x'')\cdot y - h(x')\cdot y - h(x'') \\
&= z' + z'' = \mathcal{AD}_1(z)\,.
\end{aligned}$$

Hence $\mathcal{A}_4 = \mathcal{AD}_1$ and $(\mathcal{A}_4, \mathcal{B}_4)$ is the additive formal biextension law of dimensions (a, b, c).

For each $i = 1, 2, 3, 4$ we have defined $(\mathcal{A}_i, \mathcal{B}_i)$ as the pullback of $(\mathcal{A}_{i-1}, \mathcal{B}_{i-1})$ by ψ_i (here $(\mathcal{A}_0, \mathcal{B}_0) = (\mathcal{A}, \mathcal{B})$) hence, by the definition of pullback in (2.2.3.1), the map ψ_i is an isomorphism between $(\mathcal{A}_i, \mathcal{B}_i)$ and $(\mathcal{A}_{i-1}, \mathcal{B}_{i-1})$. Consequently $\psi := \psi_4 \circ \psi_3 \circ \psi_2 \circ \psi_1$ is an isomorphism between $(\mathcal{A}_4, \mathcal{B}_4) = (\mathcal{AD}_1, \mathcal{AD}_2)$ and $(\mathcal{A}_0, \mathcal{B}_0) = (\mathcal{A}, \mathcal{B})$. Moreover ψ is the identity when reduced modulo $\mathcal{I}$ since the same is true for $\psi_1, \psi_2, \psi_3, \psi_4$: for ψ_1 and ψ_2 it is true by the definition of formal logarithms, for ψ_3 it is true because $g(x) = f(0, x)$ is congruent to the identity matrix modulo the ideal $(x_1, \ldots, x_a)$ and for ψ_4 it is true because h is congruent to the zero matrix modulo the ideal $(x_1, \ldots, x_a)^2$. Finally we notice that the subrings $R[\![x]\!], R[\![y]\!] \subset R[\![x,y,z]\!]$ are stable under $\psi_1, \psi_2, \psi_3, \psi_4$ so they are also stable under ϕ, that restricts to isomorphisms

$$\begin{aligned}
\psi^x &:= \psi|_{R[\![x]\!]} = \psi_4^x \circ \psi_3^x \circ \psi_2^x \circ \psi_1^x = \mathrm{id}_{R[\![x]\!]} \circ \mathrm{id}_{R[\![x]\!]} \circ \log_A \circ \mathrm{id}_{R[\![x]\!]} = \log_A\,, \\
\psi^y &:= \psi|_{R[\![y]\!]} = \psi_4^y \circ \psi_3^y \circ \psi_2^y \circ \psi_1^y = \mathrm{id}_{R[\![y]\!]} \circ \mathrm{id}_{R[\![y]\!]} \circ \mathrm{id}_{R[\![y]\!]} \circ \log_B = \log_B\,.
\end{aligned}$$

□

2.3 Biextensions over the p-adics and convergence

Given a commutative algebraic group $G/\mathbb{Z}_p$, the formal logarithm is useful to describe the group $G(\mathbb{Z}_p)$ in a neighbourhood of its neutral element. Analogously we want to use the map ψ of Theorem 2.2.3 to describe biextensions over $\mathbb{Z}_p$, hence we are interested in the convergence and integrality of the power series determining ψ.

Let R be a $\mathbb{Z}_{(p)}$-algebra of characteristic zero equipped with a positive discrete valuation v extending the p-adic valuation on $\mathbb{Z}_{(p)}$ and such that the ideal $\{r \in R : v(r) > 0\}$ is generated by an element π. Examples of such rings are $R = \mathbb{Z}_{(p)}[\![x_1, \dots, x_d]\!]$ equipped with the p-adic valuations or the discrete valuation rings contained in finite extensions of $\mathbb{Q}_p$.

For any formal group $A\colon R[\![x]\!] \to R[\![x]\!]\hat{\otimes}R[\![x]\!]$ of dimension a we have

$$A(R) = \mathrm{Hom}_{\mathrm{cont}}(R[\![x]\!], R) = (\pi R)^a\,,$$

where $R[\![x]\!]$ is endowed with the $(x_1, \dots, x_a)$-adic topology and R with the v-adic topology. Then the elements $\tilde{x}_i := \frac{x_i}{\pi} \in (R \otimes \mathbb{Q})[\![x]\!]$ define a bijection

$$\tilde{x} = (\tilde{x}_1, \dots, \tilde{x}_a)\colon A(R) \longrightarrow R^a\,, \tag{2.3.1}$$

that suggests the definition of the following ring of "integral converging power series"

$$R\langle\tilde{x}\rangle = R\langle\tilde{x}_1, \dots, \tilde{x}_a\rangle := \left\{ \sum_{I\in\mathbb{N}^a} \lambda_I \tilde{x}^I \in R[\![\tilde{x}]\!] : \forall n \geq 0,\ \ {}^{\mathrm{almost}}\forall I,\ v(\lambda_I) \geq n \right\} \subset (R\otimes\mathbb{Q})[\![x]\!]$$

This ring resembles the one in Equation (1.3.2) and, when R is complete with respect to v, each element of $R\langle\tilde{x}\rangle$ defines a continuous function $A(R) \to R$.

If A is commutative, the formal logarithm $\log_A := \log_{A_{R\otimes\mathbb{Q}}}\colon (R\otimes\mathbb{Q})[\![x]\!] \to (R\otimes\mathbb{Q})[\![x]\!]$ helps us understanding the group $A(R)$: if π^{p-2} is a multiple of p (when R is the discrete valuation ring contained in finite extensions of $\mathbb{Q}_p$ this is equivalent to the ramification being strictly smaller than $p-1$), then for each $i \in \{1, \dots, a\}$ we have

$$\log_A(\tilde{x}_i) \in R\langle\tilde{x}\rangle\,, \quad \log_A(\tilde{x}_i) \equiv x_i \bmod \pi\,. \tag{2.3.2}$$

Hence, if R is v-adically complete, we get an isomorphism of groups

$$(\log_A(\tilde{x}_1), \dots, \log_A(\tilde{x}_a))\colon A(R) \longrightarrow (R^a, +)\,, \tag{2.3.3}$$

that is given by integral converging power series and that, using the isomorphism (2.3.1), reduces to the identity modulo v. This fact can be proven with the same arguments in the proof of Lemma 1.5.1.1, replacing $\mathcal{O}_{S,s}$ with R.

We give an analogous statement for biextensions. In such context the biextension analogous to the additive group is the biextension $(R^a \times R^b \times R^c, +_1, +_2)$ of the additive groups $(R^a, +)$, $(R^b, +)$ by $(R^c, +)$, with partial group operations

$$\begin{aligned} (r'_A, r_B, r'_C) +_1 (r''_A, r_B, r''_C) &= (r'_A + r''_A, r_B, r'_C + r''_C), \\ (r_A, r'_B, r'_C) +_2 (r_A, r''_B, r''_C) &= (r_A, r'_B + r''_B, r'_C + r''_C). \end{aligned} \tag{2.3.4}$$

Proposition 2.3.5. *Let R be a $\mathbb{Z}_{(p)}$-algebra of characteristic zero equipped with a positive discrete valuation v extending the p-adic valuation on $\mathbb{Z}_{(p)}$. Suppose that the ideal $\{r \in R : v(r) > 0\}$ is generated by an element π such that π^{p-2} is a multiple of p. Let*

$$A\colon R[\![x]\!] \to R[\![x]\!] \hat{\otimes}_R R[\![x]\!]\,, \quad B\colon R[\![y]\!] \to R[\![y]\!] \hat{\otimes}_R R[\![y]\!]\,, \quad C\colon R[\![z]\!] \to R[\![z]\!] \hat{\otimes}_R R[\![z]\!]\,,$$

be formal group laws of dimensions a, b, c, let $(\mathcal{A}, \mathcal{B})$ be a commutative formal biextension of A, B by C and let $\psi\colon (R\otimes\mathbb{Q})[\![x,y,z]\!] \to (R\otimes\mathbb{Q})[\![x,y,z]\!]$ be the map in Theorem 2.2.3.

Using the definitions $\tilde{x}_i := x_i/\pi$, $\tilde{y}_j := y_j/\pi$, $\tilde{z}_k := z_k/\pi$, we have

$$\psi(\tilde{x}_i)\,, \psi(\tilde{y}_j)\,, \psi(\tilde{z}_k)\,, \psi^{-1}(\tilde{x}_i)\,, \psi^{-1}(\tilde{y}_j)\,, \psi^{-1}(\tilde{z}_k) \in R\langle \tilde{x}, \tilde{y}, \tilde{z}\rangle \quad \textit{and}$$
$$\psi(\tilde{x}_i) \equiv \psi^{-1}(\tilde{x}_i) \equiv \tilde{x}_i\,, \quad \psi(\tilde{y}_i) \equiv \psi^{-1}(\tilde{y}_j) \equiv \tilde{y}_j\,, \quad \psi(\tilde{z}_k) \equiv \psi^{-1}(\tilde{z}_k) \equiv \tilde{z}_k \quad \textit{modulo } \pi\,.$$

Moreover, if R is v-adically complete, the power series $\psi(\tilde{x}_i), \psi(\tilde{y}_j), \psi(\tilde{z}_k)$ give an isomorphism of biextensions

$$(\mathcal{A}, \mathcal{B})(R) \longrightarrow (R^a \times R^b \times R^c, +_1, +_2)\,,$$

where $(R^a \times R^b \times R^c, +_1, +_2)$ is the additive biextension given by (2.3.4).

Proof. For an additive formal biextension law $(\mathcal{AD}_1, \mathcal{AD}_2)$ of dimensions (a, b, c), the set of R-points $(\mathcal{AD}_1, \mathcal{AD}_2)(R)$ is exactly $(R^a \times R^b \times R^c, +_1, +_2)$, hence it is enough to prove that the power series $\psi(\tilde{x}_i)$, $\psi(\tilde{y}_j)$, $\psi(\tilde{z}_k)$, $\psi^{-1}(\tilde{x}_i)$, $\psi^{-1}(\tilde{y}_j)$, $\psi^{-1}(\tilde{z}_k)$ are contained in $R\langle \tilde{x}, \tilde{y}, \tilde{z}\rangle$ and proving the congruences. This is equivalent to proving that ψ and ψ^{-1} restrict to maps $R\langle \tilde{x}, \tilde{y}, \tilde{z}\rangle \to R\langle \tilde{x}, \tilde{y}, \tilde{z}\rangle$ that modulo π reduce to the identity of $(R/\pi)[\tilde{x}, \tilde{y}, \tilde{z}]$. Moreover once it is proven for ψ it is automatically true for ψ^{-1}.

We can write $\psi = \psi_4 \circ \psi_3 \circ \psi_2 \circ \psi_1$, where the ψ_i's are the ones defined in the proof of Theorem 2.2.3, hence it is enough to prove that both ψ_1 and $\psi_4 \circ \psi_3 \circ \psi_2$ restrict to maps $R\langle \tilde{x}, \tilde{y}, \tilde{z}\rangle \to R\langle \tilde{x}, \tilde{y}, \tilde{z}\rangle$ that modulo π reduce to the identity of $(R/\pi)[\tilde{x}, \tilde{y}, \tilde{z}]$. In other words it is enough to prove that the power series $\psi_1(\tilde{x}_i)$, $\psi_4 \circ \psi_3 \circ \psi_2(\tilde{x}_i)$, $\psi_1(\tilde{y}_j)$, $\psi_4 \circ \psi_3 \circ \psi_2(\tilde{y}_j)$, $\psi_1(\tilde{z}_k)$ and $\psi_4 \circ \psi_3 \circ \psi_2(\tilde{z}_k)$ lie in $R\langle \tilde{x}, \tilde{y}, \tilde{z}\rangle$ and that they are congruent respectively to $\tilde{x}_i$, $\tilde{x}_i$, $\tilde{y}_j$, $\tilde{y}_j$, $\tilde{z}_k$ and $\tilde{z}_k$ modulo π. We know that $\psi_1 = \log_{\mathcal{B}}$, hence, using Equation (2.3.2),

$$\psi_1(\tilde{x}_i) = \tilde{x}_i\,, \psi_1(\tilde{y}_j)\,, \psi_1(\tilde{z}_k) \in R[\![x]\!]\langle \tilde{y}, \tilde{z}\rangle \subset R\langle \tilde{x}, \tilde{y}, \tilde{z}\rangle \quad \text{and}$$
$$\psi_1(\tilde{x}_i) \equiv \tilde{x}_i (\mathrm{mod}\pi)\,, \quad \psi_1(\tilde{y}_i) \equiv \tilde{y}_i (\mathrm{mod}\pi)\,, \quad \psi_1(\tilde{y}_i) \equiv \tilde{y}_i (\mathrm{mod}\pi)\,,$$

where $R[\![x]\!]\langle \tilde{y}, \tilde{z}\rangle$ is defined with respect to the π-adic valuation on $R[\![x]\!]$. We notice that $\psi_2 \circ \psi_3 \circ \psi_4$ is the identity when restricted to $R[\![y]\!]$, hence $\psi_2 \circ \psi_3 \circ \psi_4\colon R[\![y]\!][\![x,z]\!] \to R[\![y]\!][\![x,z]\!]$ is an isomorphism between the additive formal group law of dimension $a+c$ over $R[\![y]\!]$ and the formal group law $\mathcal{A}_1$ which is defined in the proof of Theorem 2.2.3; moreover

$\psi_2\circ\psi_3\circ\psi_4$ reduces to the identity modulo $(x_1,\dots,x_a,z_1,\dots,x_c)^2$. By the uniqueness of the formal logarithm, $\psi_2\circ\psi_3\circ\psi_4=\log_{\mathcal{A}_1}$, hence, using Equation (2.3.2),

$$\psi_2\circ\psi_3\circ\psi_4(\tilde{x}_i)=\tilde{x}_i\,,\psi_2\circ\psi_3\circ\psi_4(\tilde{y}_j)\,,\psi_2\circ\psi_3\circ\psi_4(\tilde{z}_k)\in R[\![y]\!]\langle\tilde{x},\tilde{z}\rangle\subset R\langle\tilde{x},\tilde{y},\tilde{z}\rangle\quad\text{and}$$
$$\psi_2\circ\psi_3\circ\psi_4(\tilde{x}_i)\equiv\tilde{x}_i(\mathrm{mod}\pi)\,,\quad\psi_2\circ\psi_3\circ\psi_4(\tilde{y}_i)\equiv\tilde{y}_i(\mathrm{mod}\pi)\,,\quad\psi_2\circ\psi_3\circ\psi_4(\tilde{y}_i)\equiv\tilde{y}_i(\mathrm{mod}\pi)\,,$$

where $R[\![y]\!]\langle\tilde{x},\tilde{z}\rangle$ is defined with respect to the π-adic valuation on $R[\![y]\!]$. □

2.4 Another proof of Theorem 1.4.10

We now use Theorem 2.2.3 and Proposition 2.3.5 to give another proof of Theorem 1.4.10. Our strategy is constructing a chart $\Phi\colon\mathbb{Z}_p^{\rho g+\rho-1}\to P^{\times,\rho-1}(\mathbb{Z}_p)_t$, such that the map $\Phi^{-1}\circ\kappa$ is given by linear and quadratic polynomials. In order to construct Φ we first establish coordinates to define a formal biextension law associated to $P^{\times,\rho-1}$, then we use the map of Theorem 2.2.3 to describe more easily the partial group operations of $P^{\times,\rho-1}(\mathbb{Z}_p)$ in a neighbourhood of the neutral element, then we make translations to work in the residue disk of t.

Let $J,(J^{\vee 0})^{\rho-1},P^{\times,\rho-1}$ and T be as in Section 1.2 and let π_J and $\pi_{(J^{\vee 0})^{\rho-1}}$ be the two projections $P^{\times,\rho-1}\to J$ and $P^{\times,\rho-1}\to(J^{\vee 0})^{\rho-1}$. Letting $0,\overline{0}$ be the neutral elements of $J(\mathbb{Z}_p),J(\mathbb{F}_p)$, we choose $y_1,\dots,y_g\in\mathcal{O}_{J,\overline{0}}$ that vanish on 0 and that, together with p, generate the maximal ideal $\mathfrak{m}\subset\mathcal{O}_{J,\overline{0}}$. The embedding $\mathbb{Z}[y_1,\dots,y_g]\to\mathcal{O}_{J,\overline{0}}$ induces an isomorphism

$$\mathbb{Z}_p[\![y]\!]=\mathbb{Z}_p[\![y_1,\dots,y_g]\!]\xrightarrow{\sim}\mathcal{O}_{J,\overline{0}}^{\wedge_{\mathfrak{m}}}\,.$$

The group operation $M_J\colon J\times J\to J$ induces a morphism of rings $\mathcal{O}_{J,\overline{0}}\to\mathcal{O}_{J,\overline{0}}\otimes\mathcal{O}_{J,\overline{0}}$ and taking completions we get a formal group law over $\mathbb{Z}_p$

$$M_J^*\colon\mathbb{Z}_p[\![y]\!]=\mathcal{O}_{J,\overline{0}}^{\wedge_{\mathfrak{m}}}\longrightarrow(\mathcal{O}_{J,\overline{0}}\otimes\mathcal{O}_{J,\overline{0}})^{\wedge_{\mathfrak{m}\otimes\mathcal{O}_{J,\overline{0}}+\mathcal{O}_{J,\overline{0}}\otimes\mathfrak{m}}}=\mathbb{Z}_p[\![y]\!]\hat{\otimes}_{\mathbb{Z}_p}\mathbb{Z}_p[\![y]\!]\,.$$

Then we have an isomorphism of groups given by the composition

$$J(\mathbb{Z}_p)_{\overline{0}}=\mathrm{Hom}_{\mathrm{loc}}(\mathcal{O}_{J,\overline{0}},\mathbb{Z}_p)=\mathrm{Hom}_{\mathrm{cont}}(\mathcal{O}_{J,\overline{0}}^{\wedge_{\mathfrak{m}}},\mathbb{Z}_p)=\mathrm{Hom}_{\mathrm{cont}}(\mathbb{Z}_p[\![y]\!],\mathbb{Z}_p)=M_J^*(\mathbb{Z}_p)\,.$$

Analogously we choose $z_1,\dots,z_{\rho g-g}\in\mathcal{O}_{(J^{\vee 0})^{\rho-1},\overline{0}}$ that vanish on 0 and that, together with p, generate the maximal ideal of $\mathcal{O}_{(J^{\vee 0})^{\rho-1},\overline{0}}$. The group operation on $(J^{\vee 0})^{\rho-1}$ induces a formal group law

$$M_{(J^{\vee 0})^{\rho-1}}^*\colon\mathbb{Z}_p[\![z_1,\dots,z_{\rho g-g}]\!]=\mathbb{Z}_p[\![z]\!]\longrightarrow\mathbb{Z}_p[\![z]\!]\hat{\otimes}_{\mathbb{Z}_p}\mathbb{Z}_p[\![z]\!]\,,$$

that describes the group $(J^{\vee 0})^{\rho-1}(\mathbb{Z}_p)_{\overline{0}}$.

The rigidification of $P^{\times,\rho-1}$ along $J \times \{0\}$ gives an element $1 \in P^{\times,\rho-1}(0,0)(\mathbb{Z}_p)$ that is the neutral element of both the groups $\pi_J^{-1}(0)(\mathbb{Z}_p)$ and $\pi_{J^{\vee 0},\rho-1}^{-1}(0)(\mathbb{Z}_p)$. We call such an element the neutral element of $P^{\times,\rho-1}(\mathbb{Z}_p)$ and we denote by $\overline{1}$ its image in $P^{\times,\rho-1}(\mathbb{F}_p)$. We choose $w_1, \dots, w_{\rho-1} \in \mathcal{O}_{P^{\times,\rho-1},\overline{1}}$ that vanish on 1 and that, together with $x_1, \dots, x_g, z_1, \dots, z_{\rho g-g}$ and p generate the maximal ideal $\mathfrak{m} \subset \mathcal{O}_{P^{\times,\rho-1},\overline{1}}$. As before we have an isomorphism

$$\mathbb{Z}_p[\![y,z,w]\!] = \mathbb{Z}_p[\![y_1,\dots,y_g,z_1,\dots,z_{\rho g-g},w_1,\dots,w_{\rho-1}]\!] \xrightarrow{\sim} \mathcal{O}^{\wedge_{\mathfrak{m}}}_{P^{\times,\rho-1},\overline{1}}$$

and the two partial group laws

$$+_1 \colon P^{\times,\rho-1} \times_{(J^{\vee 0})^{\rho-1}} P^{\times,\rho-1} \longrightarrow P^{\times,\rho-1}, \quad +_2 \colon P^{\times,\rho-1} \times_J P^{\times,\rho-1} \longrightarrow P^{\times,\rho-1},$$

and induce a biextension

$$\begin{aligned} \mathcal{M}_J^* &\colon \mathbb{Z}_p[\![y,z,w]\!] \longrightarrow \mathbb{Z}_p[\![y,z,w]\!] \hat{\otimes}_{\mathbb{Z}_p[\![z]\!]} \mathbb{Z}_p[\![y,z,w]\!], \\ \mathcal{M}_{J^{\vee 0},\rho-1}^* &\colon \mathbb{Z}_p[\![y,z,w]\!] \longrightarrow \mathbb{Z}_p[\![y,z,w]\!] \hat{\otimes}_{\mathbb{Z}_p[\![y]\!]} \mathbb{Z}_p[\![y,z,w]\!], \end{aligned}$$

of the formal group laws M_J^* and $M_{J^{\vee 0},\rho-1}^*$ by the formal group law induced by the algebraic group $\mathbb{G}_{\mathrm{m}}^{\rho-1}$. In particular $P^{\times,\rho-1}(\mathbb{Z}_p)_{\overline{1}}$ is a biextension of $J(\mathbb{Z}_p)_{\overline{0}}$ and $(J^{\vee 0})^{\rho-1}(\mathbb{Z}_p)_{\overline{0}}$ by $\mathbb{G}_{\mathrm{m}}^{\rho-1}(\mathbb{Z}_p)_{\overline{1}}$, and it is isomorphic to $(\mathcal{M}_J, \mathcal{M}_{J^{0\vee},\rho-1})(\mathbb{Z}_p)$. Applying Theorem 2.2.3 and Proposition 2.3.5 we get an isomorphism of biextensions

$$\Psi \colon (P^{\times,\rho-1}(\mathbb{Z}_p)_{\overline{1}}, +_1, +_2) \longrightarrow (\mathbb{Z}_p^g \times \mathbb{Z}_p^{\rho g-g} \times \mathbb{Z}_p^{\rho-1}, +_1, +_2),$$

given by power series in $\mathcal{O}(\widetilde{(P^{\times,\rho-1})^p_x})^{\wedge_p}$, that modulo p give a linear map between the tangent space of $P^{\times,\rho-1}$ at $\overline{1}$ and $\mathbb{F}_p^{\rho g+\rho-1}$.

We now take care of translating Ψ. Let f and m be as in Section 1.2 and let $x_{\widetilde{t}} \in J(\mathbb{Z})$, $\widetilde{t} \in T(\mathbb{Z}) \subset P^{\times,\rho-1}(\mathbb{Z})$ be as in Section 1.4. By Equations (2.3.2) and (2.3.3), the formal logarithms of (the formal group laws associated to) the algebraic groups $\pi_{(J^{\vee 0})^{\rho-1}}^{-1}(m\cdot \circ \mathrm{tr}_c \circ f(x_{\widetilde{t}}))$ and $\pi_J^{-1}(x_{\widetilde{t}})$ give isomorphisms of groups

$$\begin{aligned} \Psi_1 &\colon \left(\pi_{J^{\vee 0},\rho-1}^{-1}(m\cdot \circ \mathrm{tr}_c \circ f(x_{\widetilde{t}}))(\mathbb{Z}_p)_{\overline{1}}, +_1\right) \longrightarrow (\mathbb{Z}_p^g \times \mathbb{Z}_p^{\rho-1}, +), \\ \Psi_2 &\colon \left(\pi_J^{-1}(x_{\widetilde{t}})(\mathbb{Z}_p)_{\overline{1}}, +_2\right) \longrightarrow (\mathbb{Z}_p^{\rho g-g} \times \mathbb{Z}_p^{\rho-1}, +), \end{aligned}$$

where we denote by $\overline{1}$ the reduction modulo p of the neutral elements of the respective groups. Since $\pi_J^{-1}(x_{\widetilde{t}})$ is an extension of $(J^{\vee 0})^{\rho-1}$, the first $\rho g-g$ coordinates of Ψ_2 are given by the composition of the projection $\pi_J^{-1}(x_{\widetilde{t}})(\mathbb{Z}_p)_{\overline{1}} \to (J^{\vee 0})^{\rho-1}(\mathbb{Z}_p)_{\overline{0}}$ with the formal logarithm of $(J^{\vee 0})^{\rho-1}$. Analogously the first g coordinates of Ψ_1 are given by the composition of $\pi_{(J^{\vee 0})^{\rho-1}}^{-1}(m\cdot \circ \mathrm{tr}_c \circ f(x_{\widetilde{t}}))(\mathbb{Z}_p)_{\overline{1}} \to J(\mathbb{Z}_p)_{\overline{0}}$ with the formal

logarithm of J. By Theorem 2.2.3, analogous statements are true for the first g coordinates of Ψ and the subsequent $\rho g-g$ coordinates of Ψ. This implies that for every $(\alpha,\beta,\gamma)\in\mathbb{Z}_p^g\times\mathbb{Z}_p^{\rho g-g}\times\mathbb{Z}_p^{\rho-1}$ we have

$$\begin{aligned}\pi_J\left(\Psi^{-1}(\alpha,\beta,\gamma)\right)&=\pi_J\left(\Psi_1^{-1}(\alpha,\gamma)\right)=\pi_J\left(\Psi_1^{-1}(\alpha,0)\right),\\ \pi_{(J^{\vee 0})^{\rho-1}}\left(\Psi^{-1}(\alpha,\beta,\gamma)\right)&=\pi_{(J^{\vee 0})^{\rho-1}}\left(\Psi_2^{-1}(\beta,\gamma)\right)=\pi_{(J^{\vee 0})^{\rho-1}}\left(\Psi_2^{-1}(\beta,0)\right).\end{aligned}\tag{2.4.1}$$

Moreover, using the $\mathbb{G}_{\mathrm{m}}^{\rho-1}$-structure of $P^{\times,\rho-1}$ and the fact that both the groups $\pi_J^{-1}(0)$ and $\pi_{J^{\vee 0},\rho-1}^{-1}(0)$ are base changes of $\mathbb{G}_{\mathrm{m}}^{\rho-1}$, for every $(\alpha,\beta,\gamma)\in\mathbb{Z}_p^g\times\mathbb{Z}_p^{\rho g-g}\times\mathbb{Z}_p^{\rho-1}$ we have

$$\begin{aligned}\Psi^{-1}(\alpha,\beta,\gamma)&=\Psi^{-1}(0,\beta,\gamma)+_1\Psi^{-1}(\alpha,\beta,0)=\exp^{\rho-1}(\gamma)\cdot\Psi^{-1}(\alpha,\beta,0),\\ \Psi_1^{-1}(\alpha,\gamma)&=\Psi_1^{-1}(0,\gamma)+_1\Psi_1^{-1}(\alpha,0)=\exp^{\rho-1}(\gamma)\cdot\Psi_1^{-1}(\alpha,0),\\ \Psi_2^{-1}(\beta,\gamma)&=\Psi_2^{-1}(\beta,\gamma)+_2\Psi_2^{-1}(\beta,0)=\exp^{\rho-1}(\gamma)\cdot\Psi_2^{-1}(\beta,0),\end{aligned}$$

where $\exp^{\rho-1}\colon\mathbb{Z}_p^{\rho-1}\to\mathbb{Z}_p^{\times,\rho-1}$ is obtained taking the $(\rho-1)$-th power of

$$\exp\colon\mathbb{Z}_p\longrightarrow\mathbb{G}_{\mathrm{m}}(\mathbb{Z}_p)_{\overline{1}}=1+p\mathbb{Z}_p,$$

which is the inverse of the map (2.3.3) induced by the formal logarithm of $\mathbb{G}_{\mathrm{m}}$. By (2.4.1), we can "translate" the map Ψ by Ψ_1 and Ψ_2, obtaining the following map

$$\begin{aligned}\Phi\colon\mathbb{Z}_p^g\times\mathbb{Z}_p^{\rho g-g}\times\mathbb{Z}_p^{\rho-1}&\longrightarrow P^{\times,\rho-1}(\mathbb{Z}_p)_t\\ (\alpha,\beta,\gamma)&\longmapsto\left(\Psi^{-1}(\alpha,\beta,\gamma)+_2\Psi_1^{-1}(\alpha,0)\right)+_1\left(\Psi_2^{-1}(\beta,0)+_2\widetilde{t}\right)\\ &=\exp^{\rho-1}(\gamma)\cdot\left(\left(\Psi^{-1}(\alpha,\beta,0)+_2\Psi_1^{-1}(\alpha,0)\right)+_1\left(\Psi_2^{-1}(\beta,0)+_2\widetilde{t}\right)\right).\end{aligned}$$

Let us fix coordinates to study Φ. Let $u_1,\dots,u_{\rho g-g}$ be elements of $\mathcal{O}_{(J^{\vee 0})^{\rho-1},m\cdot\mathrm{otr}_c\circ f(j_b(u))}$ such that together with p they form a system of parameters of $\mathcal{O}_{(J^{\vee 0})^{\rho-1},m\cdot\mathrm{otr}_c\circ f(j_b(u))}$, and let us lift $v_1,\dots,v_{\rho-1}$ to elements in $\mathcal{O}_{P^{\times,\rho-1},t}$. Then $u_1,\dots,u_{\rho g-g}$, $v_1,\dots,v_{\rho-1}$ and p, together with $x_1,\dots,x_g$ defined in the statement of Theorem 1.4.10, form a a system of parameters of $\mathcal{O}_{P^{\times,\rho-1},t}$. The functions $\widetilde{x}_i:=\frac{x_i}{p}$, $\widetilde{u}_i:=\frac{u_i}{p}$ and $\widetilde{v}_i:=\frac{v_i}{p}$ give bijections with powers of $\mathbb{Z}_p$ that make the following diagram commute

$$\begin{array}{ccc}P^{\times,\rho-1}(\mathbb{Z}_p)_t & \xrightarrow{(\widetilde{x},\widetilde{u},\widetilde{v})=(\widetilde{x}_1,\dots,\widetilde{x}_g,\widetilde{u}_1,\dots,\widetilde{u}_{\rho g-g},\widetilde{v}_1,\dots,\widetilde{v}_{\rho-1})} & \mathbb{Z}_p^g\times\mathbb{Z}_p^{\rho g-g}\times\mathbb{Z}_p^{\rho-1}\\ \uparrow & & \downarrow\\ T(\mathbb{Z}_p)_t & \xrightarrow{(\widetilde{x}_1,\dots,\widetilde{x}_g,\widetilde{v}_1,\dots,\widetilde{v}_{\rho-1})} & \mathbb{Z}_p^g\times\mathbb{Z}_p^{\rho g-g}\times\mathbb{Z}_p^{\rho-1}\end{array}.$$

The biextension structure on $P^{\times,\rho-1}$ implies that Φ is a bijection and, since it is defined composing maps given by integral power series that reduce to linear polynomials

modulo p, then $(\widetilde{x},\widetilde{u},\widetilde{v})\circ\Phi$ is given by power series that reduce to linear polynomials modulo p. Hence the same is true for the inverse of $(\widetilde{x},\widetilde{u},\widetilde{v})\circ\Phi$. This and the commutativity of the above diagram imply that, in order to prove Theorem 1.4.10, it is enough to prove that the map $\Phi^{-1}\circ\kappa_{\mathbb{Z}}$ is given by $g+(\rho g-g)$ linear polynomials and $\rho-1$ quadratic polynomials in the n_i and also proving that $\Phi^{-1}(\overline{T(\mathbb{Z})_t})$ is the image of such a polynomial map. To do so we give names to the coordinates of the relevant points: for each $i,j\in\{1,\dots,r\}$ let $P_{i,j},R_{i,\widetilde{t}},S_{\widetilde{t},j}\in P^{\times,\rho-1}(\mathbb{Z})$ be as in Equation (1.4.1) and let $\alpha_i\in\mathbb{Z}_p^g$, $\beta_j\in\mathbb{Z}_p^{\rho g-g}$, $\gamma_{i,j},\gamma_{i,\widetilde{t}},\gamma_{\widetilde{t},j}\in\mathbb{Z}_p^{\rho-1}$ and $\xi_{i,j},\xi_{i,\widetilde{t}},\xi_{\widetilde{t},j}\in\mathbb{F}_p^{\times,\rho-1}\subset\mathbb{Z}_p^{\times,\rho-1}$ be such that

$$P_{i,j}=\xi_{i,j}\cdot\Psi^{-1}(\alpha_i,\beta_j,\gamma_{i,j})\,,\quad R_{i,\widetilde{t}}=\xi_{i,\widetilde{t}}\cdot\Psi_1^{-1}(\alpha_i,\gamma_{i,\widetilde{t}})\,,\quad S_{\widetilde{t},j}=\xi_{\widetilde{t},j}\cdot\Psi_2^{-1}(\beta_j,\gamma_{\widetilde{t},j})\,.$$

The maps Ψ,Ψ_1 and Ψ_2 are formal logarithms, hence they allow us to write very easily the two partial group laws, and in particular we can describe the maps A,B,C,D in Equations (1.4.2), (1.4.3) and (1.4.4) as follows

$$\begin{aligned}
A_{\widetilde{t}}(n)&=\sum_{j=1}^{r}{}_2\, n_j\cdot_2 S_{\widetilde{t},j}=\left(\prod_{j=1}^{r}\xi_{\widetilde{t},j}^{n_j}\right)\cdot\Psi_2^{-1}\left(\sum_{j=1}^{r}n_j\beta_j\,,\sum_{j=1}^{r}n_j\gamma_{\widetilde{t},j}\right)\,,\\
B_{\widetilde{t}}(n)&=\sum_{i=1}^{r}{}_1\, n_i\cdot_1 R_{i,\widetilde{t}}=\left(\prod_{i=1}^{r}\xi_{i,\widetilde{t}}^{n_i}\right)\cdot\Psi_1^{-1}\left(\sum_{i=1}^{r}n_i\alpha_i\,,\sum_{i=1}^{r}n_i\gamma_{i,\widetilde{t}}\right)\,,\\
C(n)&=\sum_{i=1}^{r}{}_1\, n_i\cdot_1\Big(\sum_{j=1}^{r}{}_2\, n_j\cdot_2 P_{i,j}\Big)\\
&=\left(\prod_{i,j=1}^{r}\xi_{i,j}^{n_in_j}\right)\cdot\Psi^{-1}\left(\sum_{i=1}^{r}n_i\alpha_i\,,\sum_{j=1}^{r}n_j\beta_j\,,\sum_{i,j=1}^{r}n_in_j\gamma_{i,j}\right)\,,\\
D_{\widetilde{t}}(n)&=\big(C(n)+_2 B_{\widetilde{t}}(n)\big)+_1\big(A_{\widetilde{t}}(n)+_2\widetilde{t}\big)\\
&=\xi(n)\cdot\Phi\left(\sum_{i=1}^{r}n_i\alpha_i\,,\sum_{j=1}^{r}n_j\beta_j\,,\sum_{i,j=1}^{r}n_in_j\gamma_{i,j}+\sum_{j=1}^{r}n_j\gamma_{\widetilde{t},j}+\sum_{i=1}^{r}n_i\gamma_{i,\widetilde{t}}\right)\,,\\
&\text{with }\xi(n):=\prod_{i,j=1}^{r}\xi_{i,j}^{n_in_j}\cdot\prod_{i=1}^{r}\xi_{i,\widetilde{t}}^{n_i}\cdot\prod_{j=1}^{r}\xi_{\widetilde{t},j}^{n_j}\in\mathbb{F}_p^{\times,\rho-1}\,.
\end{aligned}$$

For any $n\in\mathbb{Z}^r$ we have $\xi((p-1)n)=1$, hence

$$\begin{aligned}
\Phi^{-1}\circ\kappa_{\mathbb{Z}}(n)&=\Phi^{-1}(D_{\widetilde{t}}((p-1)n))\\
&=\left((p-1)\sum_{i=1}^{r}n_i\alpha_i\,,(p-1)\sum_{j=1}^{r}n_j\beta_j\,,(p-1)^2\sum_{i,j=1}^{r}n_in_j\gamma_{i,j}+(p-1)\sum_{i=1}^{r}n_i(\gamma_{i,\widetilde{t}}+\gamma_{\widetilde{t},i})\right)
\end{aligned}$$

is described by linear and quadratic polynomial in n_i and extends continuously to

$$\Phi^{-1}\circ\kappa\colon\mathbb{Z}_p^r\longrightarrow\mathbb{Z}_p^g\times\mathbb{Z}_p^{\rho g-g}\times\mathbb{Z}_p^{\rho-1}\,.$$

Finally,

$$\kappa(\mathbb{Z}^r) \subset T(\mathbb{Z})_t \subset \left(\mathbb{F}_p^{\times,\rho-1} \cdot D_{\widetilde{t}}(\mathbb{Z}^r)\right) \cap P^{\times,\rho-1}(\mathbb{Z}_p)_t = \kappa\left(\tfrac{1}{p-1}\mathbb{Z}^r\right),$$

hence

$$\kappa(\mathbb{Z}_p^r) \subset \overline{T(\mathbb{Z})_t} \subset \kappa(\mathbb{Z}_p^r).$$