ISRAEL JOURNAL OF MATHEMATICS **257** (2023), 519–531
DOI: 10.1007/s11856-023-2545-1

A HENSELIAN PREPARATION THEOREM

BY

Laurent Moret-Bailly*

Institut de Recherche Mathématique de Rennes - UMR 6625
Université de Rennes, CNRS, F-35000 Rennes, France
e-mail: laurent.moret-bailly@univ-rennes.fr

Respectfully dedicated to Moshe Jarden

ABSTRACT

We prove an analogue of the Weierstrass preparation theorem for henselian pairs, generalizing the local case recently proved by Bouthier and Česnavičius. As an application, we construct a henselian analogue of the resultant of p-adic series defined by Berger.

1. Introduction

Let R be a ring (commutative, with unit). We denote by $R\{t\}$ the henselization of the polynomial ring $R[t]$ with respect to the ideal (t): this is a subring of the power series ring $R[[t]]$. (For a brief review of henselian pairs and henselization, see Section 2.1.)

* The author was partially supported by the Centre Henri Lebesgue (program ANR-11-LABX-0020-0) and the Geolie project (ANR-15-CE 40-0012).
Received December 22, 2021 and in revised form June 6, 2022

The aim of this work is to prove the following result:

THEOREM 1.1: *Let R be a ring, I an ideal of R. Assume that (R, I) is a henselian pair. Let d be a natural integer and let f be an element of $R\{t\}$ which in $R[[t]]$ has the form $f = \sum_{i\geq 0} a_i t^i$, where $a_d \in R^\times$ and $a_i \in I$ for $i < d$. Then:*

(1) *The images of $1, t, \ldots, t^{d-1}$ form a basis of the R-module $S = R\{t\}/(f)$.*
(2) (Division theorem) *Every element of $R\{t\}$ can be written uniquely in the form $Bf + C$ where $B \in R\{t\}$ and where $C \in R[t]$ is a polynomial of degree $< d$.*
(3) (Preparation theorem) *f can be written uniquely as $f = (t^d + Q)\, v$ where $v \in R\{t\}^\times$ and where $Q \in R[t]$ has degree $< d$ and coefficients in I.*

1.2. RELATED RESULTS. The result (today) most commonly named "Weierstrass preparation theorem" is the analogous statement where $R\{t\}$ is replaced by $R[[t]]$, where R is a complete noetherian local ring with maximal ideal I: see for instance [5, VII, §3, n° 8, prop. 5]. This formal variant was generalized by O'Malley [11, 2.10] to the case where R is I-adically complete and separated (but is no longer assumed local or noetherian).

In the local case, there is a convergent variant, where $R = K\langle x_1, \ldots, x_n\rangle$ is the ring of germs of analytic functions in n variables over some field K complete for an absolute value, and the role of $R\{t\}$ is played by $K\langle x_1, \ldots, x_n, t\rangle$. For $K = \mathbb{C}$, this is in fact the original theorem of Weierstrass. It is generally proved by inspection of the above formal variant (where R is $K[[x_1, \ldots, x_n]]$), checking that the series constructed in the proof remain convergent; see for instance [10, Theorem 45.3].

When R is local henselian with maximal ideal I, Theorem 1.1 was proved by Bouthier and Česnavičius in [6, 3.1.2], which inspired the present paper. The proof we give here is somewhat different and more direct: we do not use reduction to the noetherian case or the classical preparation theorem, but we work directly from the construction of $R\{t\}$ as a filtered colimit of étale $R[t]$-algebras.

Regrettably, there does not seem to be, at the moment, a general result covering all the above-mentioned variants, or at least a common strategy of proof.

1.3. Outline of the paper. In Section 2, we recall some basic facts about henselian pairs and henselization, some elementary results on henselian series rings (i.e., of the form $R\{t_1, \ldots, t_n\}$), and a useful decomposition result for R-schemes, where R is as in Theorem 1.1.

Theorem 1.1 itself is proved in Section 3. The three statements are easily deduced from each other; here we derive (2) and (3) from (1).

Finally, as an easy application, we define in Section 4 a notion of resultant in $R\{t\}$, entirely similar to the resultant constructed by Berger [4] for p-adic formal power series.

Notation and conventions. All rings are commutative with unit; ring homomorphisms respect unit elements. The unit group of a ring R is denoted by $R^\times$, its Jacobson radical by $\mathrm{rad}(R)$.

If x is a point of a scheme, $\kappa(x)$ denotes its residue field.

Let Y be a closed subscheme of a scheme X. We say (X, Y) is a **Zariski pair** if X is the only open subscheme of X containing Y; this condition only depends on the underlying spaces. If $X = \mathrm{Spec}\,(A)$ is affine and $I \subset A$ is the ideal of Y, we say (A, I) is a Zariski pair if (X, Y) is a Zariski pair or, equivalently, if $I \subset \mathrm{rad}(A)$. If (X, Y) is Zariski and $X' \to X$ is a closed morphism, then $(X', Y \times_X X')$ is Zariski.

Acknowledgments. The author is grateful to Henri Lombardi and Herwig Hauser for pointing out references, and to the referee for their remarks.

2. Preliminary results

2.1. Review of henselian pairs. The notion of a henselian pair was defined by Lafon [9], generalizing the local case introduced by Azumaya [3]. Let us first recall the definition:

Definition 2.1.1: Let R be a ring and I an ideal of R. We say that (R, I) is a **henselian pair** if for every étale R-algebra R', every morphism $\overline{\rho} : R' \to R/I$ of R-algebras lifts to a morphism $\rho : R' \to R$.

If (R, I) is a henselian pair, we also say occasionally that $(\mathrm{Spec}\,(R), \mathrm{Spec}\,(R/I))$ is a henselian pair. (There is an obvious generalization to general schemes, but we only need the affine case.) A **henselian local ring** is a local ring R, with maximal ideal I, such that (R, I) is henselian.

A henselian pair is a Zariski pair: if $f \in 1+I$, apply the definition to $R' = R_f$. It follows that, given $\overline{\rho}$ as in the definition, ρ is unique. Another immediate consequence of the henselian property is that the map $R \to R/I$ induces a bijection on idempotents: consider $R' = R[x]/(x(x-1))$.

There are many equivalent definitions of a henselian pair; for this and for more generalities, see for instance [13, Tag 09XD]. One important property that we shall use is that if (R, I) is a henselian pair, so is (R', IR') for every finite (or just integral) R-algebra R'. In particular, idempotents of R'/IR' lift uniquely to idempotents of R'.

2.1.2. *Henselization.* Let R be a ring and $I \subset R$ an ideal. The category of henselian pairs (S, J), where S is an R-algebra and J is an ideal containing IS, has an initial object $(R, I)^{\mathrm{h}} = (R^{\mathrm{h}}, I^{\mathrm{h}})$ called the **henselization** of (R, I) (or the henselization of R at I).[1] We have $I^{\mathrm{h}} = IR^{\mathrm{h}}$ and $R/I \xrightarrow{\sim} R^{\mathrm{h}}/I^{\mathrm{h}}$. We can construct R^{h} as the filtered colimit of étale R-algebras R' such that $R/I \xrightarrow{\sim} R'/IR'$; in particular, R^{h} is flat over R, and faithfully flat if (R, I) is a Zariski pair. If R' is an integral R-algebra (for instance a quotient of R), then

$$(R', IR')^{\mathrm{h}} = (R, I)^{\mathrm{h}} \otimes_R R'.$$

2.2. Structure of henselian series rings. Let R be a ring, $\underline{t} = (t_1, \dots, t_n)$ a finite sequence of indeterminates.[2] We denote by $R\{\underline{t}\}$ the henselization of $R[\underline{t}]$ at the ideal $(t_1, \dots, t_n)$; it is an $R[\underline{t}]$-algebra with an isomorphism $\varepsilon : R\{\underline{t}\}/(\underline{t}) \xrightarrow{\sim} R$, and there is a natural injection $R\{\underline{t}\} \hookrightarrow R[[\underline{t}]]$ making $R[[\underline{t}]]$ the $(\underline{t})$-adic completion of $R\{\underline{t}\}$; the image of $f \in R\{\underline{t}\}$ in $R[[\underline{t}]]$ will be denoted by f_{for}.

As a functor of R, $R\{\underline{t}\}$ is better behaved than $R[[\underline{t}]]$. In particular, it commutes with filtered colimits, and if I is any ideal of R we have

$$R\{\underline{t}\}/IR\{\underline{t}\} \cong (R/I)\{\underline{t}\}.$$

For $f \in R\{\underline{t}\}$ we have the equivalences:

$$f \in R\{\underline{t}\}^\times \Leftrightarrow f_{\mathrm{for}} \in R[[\underline{t}]]^\times \Leftrightarrow \varepsilon(f) \in R^\times.$$

It follows that $\mathrm{rad}(R\{\underline{t}\})$ is generated by $\mathrm{rad}(R)$ and $(\underline{t})$. In particular, if (R, I) is a Zariski pair, so is $(R\{\underline{t}\}, IR\{\underline{t}\} + (\underline{t}))$.

[1] Of course, the notation R^{h} will be used only if there is no doubt about I.

[2] For the preparation theorem we only need the case $n = 1$. The case of an infinite set of indeterminates is left to the reader.

Similarly, if (R, I) is a henselian pair, so is $(R\{\underline{t}\}, IR\{\underline{t}\} + (\underline{t}))$: to see this, view R as the quotient $R\{\underline{t}\}/(\underline{t})$ and apply the transitivity property [13, 0DYD].

Classically, $R\{\underline{t}\}$ can be constructed as the colimit of a filtered family $(A_\lambda)_{\lambda\in L}$ of étale $R[\underline{t}]$-algebras, with compatible isomorphisms $\varepsilon_\lambda : A_\lambda/(\underline{t})A_\lambda \xrightarrow{\sim} R$. In particular, for all $\lambda \in L$ and $N \in \mathbb{N}$, the natural morphism of R-algebras

$$R[\underline{t}]/(\underline{t})^N \to A_\lambda/(\underline{t})^N A_\lambda$$

is an isomorphism.

Each natural morphism $\pi_\lambda : \mathrm{Spec}\,(A_\lambda) \to \mathrm{Spec}\,(R)$ is smooth of relative dimension n, and has a section s_λ deduced from ε_λ.

We say that an R-algebra A is **geometrically irreducible** if the natural morphism $\mathrm{Spec}\,(A) \to \mathrm{Spec}\,(R)$ has geometrically irreducible fibers.

LEMMA 2.2.1: *Let R and $\underline{t} = (t_1, \ldots, t_n)$ be as above. Then one can choose the system $(A_\lambda)_{\lambda\in L}$ such that each A_λ is a geometrically irreducible R-algebra.*

Proof. Starting with an arbitrary family $(A_\lambda)_{\lambda\in L}$, we may assume, by enlarging L, that for all $\lambda \in L$ and $f \in A_\lambda$ such that $\varepsilon_\lambda(f) \in R^\times$, the localized algebra $A_\lambda[1/f]$ is still in the family. It suffices to show that, assuming this, the sub-system formed by the geometrically irreducible A_λ's is cofinal. For each λ, let $U_\lambda \subset \mathrm{Spec}\,(A_\lambda)$ be the union of the connected components of the fibers of π_λ meeting the section s_λ. As π_λ is smooth, U_λ is open in $\mathrm{Spec}\,(A_\lambda)$ [7, (15.6.7)], and its fibers over $\mathrm{Spec}\,(R)$ are smooth and connected, with a rational point, hence geometrically irreducible. Since U_λ is open, there is $f \in A_\lambda$ such that $\mathrm{Im}(s_\lambda) \subset \mathrm{Spec}\,(A_\lambda[1/f]) \subset U_\lambda$ (in an affine scheme, every closed subset has a basis of principal open neighborhoods). The fibers of $\mathrm{Spec}\,(A_\lambda[1/f]) \to \mathrm{Spec}\,(R)$ are nonempty and open in those of $U_\lambda \to \mathrm{Spec}\,(R)$ and therefore geometrically irreducible. This completes the proof. ∎

2.2.2. *Evaluation.* This section will not be used until Section 4.

Let us keep the notation of 2.2 and consider the category $\mathrm{Alg}^{\mathrm{h}}_R$ of henselian pairs (A, J) where A is an R-algebra. Then $(R\{\underline{t}\}, (\underline{t}))$ is an object of $\mathrm{Alg}^{\mathrm{h}}_R$ corepresenting the set-valued functor $(A, J) \mapsto \prod_{i=1}^n J$. In particular, for an object (A, J) of $\mathrm{Alg}^{\mathrm{h}}_R$ and a sequence $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ from J, we have a morphism "evaluation at $\underline{\alpha}$" from $R\{\underline{t}\}$ to A which we denote by $f \mapsto f(\underline{\alpha})$. One may construct it by noting that the morphism $P \mapsto P(\underline{\alpha})$ from $R[\underline{t}]$ to A maps the t_i's into J, hence factors through $R\{\underline{t}\}$ because (A, J) is henselian.

For given $\underline{\alpha}$, the element $f(\underline{\alpha})$ is the sum in A, for the J-adic topology, of the series $f_{\mathrm{for}}(\underline{\alpha})$ obtained by substituting $\underline{\alpha}$ for $\underline{t}$; this property characterizes $f(\underline{\alpha})$ if A is J-adically separated (but not in general).

The reader can check the following nice property, which will not be used here: if I is an ideal of R generated by n elements $a_1, \dots, a_n$, the evaluation morphism $f \mapsto f(\underline{a})$ induces an isomorphism of $R\{\underline{t}\}/(t_i - a_i)_{1 \leq i \leq n}$ with the henselization $(R, I)^{\mathrm{h}}$.

2.3. Schemes over henselian pairs: a decomposition result.

Notation 2.3.1: Let (R, I) be a henselian pair. Put $S = \mathrm{Spec}\,(R)$, $\overline{R} = R/I$, and $\overline{S} = \mathrm{Spec}\,(\overline{R})$; more generally, for each R-algebra A (resp. each R-scheme X) we shall put $\overline{A} = A/IA$ (resp. $\overline{X} = X \times_S \overline{S}$).

The following proposition is a variant of [12, XI, cor. 1 p. 119]:

Proposition 2.3.2: *With notation as above, let Z be a separated R-scheme of finite type. Assume that $\overline{Z}$ is* finite *over $\overline{R}$.*

Then there is a unique open and closed subscheme Z^{f} of Z which is finite over R and satisfies $\overline{Z^{\mathrm{f}}} = \overline{Z}$. Moreover Z^{f} has the following properties:

(1) *The pair $(Z^{\mathrm{f}}, \overline{Z})$ is henselian.*
(2) *Z^{f} is the smallest open subscheme of Z containing $\overline{Z}$.*
(3) *Let T be an R-scheme and $u : T \to Z$ an R-morphism. Assume that $(T, \overline{T})$ is a Zariski pair. Then u factors through Z^{f}.*

Proof. Let us first assume the existence of Z^{f} and prove (1), (2) and (3). First, (1) is clear since (R, I) is henselian and Z^{f} is finite over R. In particular, $(Z^{\mathrm{f}}, \overline{Z})$ is a Zariski pair, and (2) follows because Z^{f} is open in Z. Now take $u : T \to Z$ as in (3): then $u^{-1}(Z^{\mathrm{f}})$ is a neighborhood of $\overline{T}$ in T, hence equal to T, which proves (3).

Observe that (2), for instance, implies the uniqueness of Z^{f}. Now let us prove existence. First, consider the set Z' of points $x \in Z$ isolated in their fiber above $\mathrm{Spec}\,(R)$. Then Z' is open in Z [7, (13.1.4)] and, viewed as an open subscheme, it is quasifinite over $\mathrm{Spec}\,(R)$; in addition, we have $\overline{Z'} = \overline{Z}$. So it is clear that if Z'^{f} exists it is open in Z, and closed since it is finite over R, so we can take $Z^{\mathrm{f}} = Z'^{\mathrm{f}}$. Replacing Z by Z', we can therefore assume Z quasifinite over R.

By Zariski's main theorem [8, (18.12.13)], there is an open immersion $Z \hookrightarrow Z^c$, where Z^c is a finite R-scheme. As $\overline{Z}$ is finite over R, the induced open immersion $\overline{Z} \hookrightarrow \overline{Z^c}$ is closed, so we have $\overline{Z^c} = \overline{Z} \amalg Y$ for an open and closed subscheme Y of $\overline{Z^c}$. Since (R, I) is henselian and Z^c is finite over R, this decomposition is induced (using the idempotent lifting property) by a decomposition $Z^c = Z^{\mathrm{f}} \amalg Z_1^c$ of Z^c, where Z^{f} and Z_1^c are finite over R and $\overline{Z^{\mathrm{f}}} = \overline{Z}$. In particular $(Z^{\mathrm{f}}, \overline{Z^{\mathrm{f}}}) = (Z^{\mathrm{f}}, \overline{Z})$ is a Zariski pair. Since $Z \cap Z^{\mathrm{f}}$ is open in Z^{f} and contains $\overline{Z}$, it is therefore equal to Z^{f} which means that $Z^{\mathrm{f}} \subset Z$ and $Z = Z^{\mathrm{f}} \amalg Z'$ with

$$Z' := Z \cap Z_1^c.$$

Thus, the desired conditions for Z^{f} are satisfied. ∎

Remarks 2.3.3:

(1) Assertions (2) and (3) of 2.3.2 only use the existence of Z^{f} and the Zariski property for (R, I).

(2) We see in particular that Z^{f} is the largest closed subscheme of Z which is finite over S. Moreover, Z^{f} is functorial in Z: if Y is a separated R-scheme of finite type with $\overline{Y}$ finite over $\overline{R}$, every R-morphism $Z \to Y$ sends Z^{f} to Y^{f}.

(3) Using more sophisticated tools, one can generalize 2.3.2 by replacing "finite" by "proper" in the conditions for $\overline{Z}$ and Z^{f}. For the proof, the first step (reduction to the quasifinite case) is of course ignored. One uses Nagata compactification to choose an open immersion $Z \hookrightarrow Z^c$ into a proper S-scheme $p : Z^c \to S$. Then by the properness of Z^c and the henselian property of (R, I), we can apply [13, Tag 0A0C] to the sheaf $(\mathbb{Z}/2\mathbb{Z})_{Z^c}$ to conclude that the idempotent defining $\overline{Z}$ in $\overline{Z^c}$ lifts to a unique idempotent on Z^c, which we take to define Z^{f}.

(4) Assume that R is local henselian and I is its maximal ideal, and let Y be a separated R-scheme of finite type. Let y be an isolated point of $\overline{Y}$. Then $C := \overline{Y} \smallsetminus \{y\}$ is closed in Y, so we can apply 2.3.2 to $Z := Y \smallsetminus C$ since $\overline{Z} = \{y\}$ set-theoretically. It is then easy to see that

$$Z^{\mathrm{f}} = \mathrm{Spec}\,(\mathscr{O}_{Y,y}).$$

In particular, $\mathscr{O}_{Y,y}$ is a finite R-module: this is the Mather division theorem as stated in [1, Theorem 1]. The approach in [1] (and the related paper [2]) is algorithmic, while here we use Zariski's main theorem as a magic wand.

3. The preparation theorem

3.1. Notation and assumptions. We fix a ring R and an indeterminate t. We denote by $\mathrm{Alg}^+_{R[t]}$ the category of pairs (A, x) where A is an $R[t]$-algebra and x is an element of A.

We also fix an element f of $R\{t\}$, and we write

$$f_{\mathrm{for}} = \sum_{i\geq 0} a_i t^i \in R[[t]] \quad (a_i \in R).$$

We assume that the ideal generated by the a_i's $(i > 0)$ is equal to R. Equivalently, for all $\mathfrak{p} \in \mathrm{Spec}\,(R)$, the image of f in $\kappa(\mathfrak{p})[[t]]$, or in $\kappa(\mathfrak{p})\{t\}$, is not a constant.

Finally we denote by S the $R[t]$-algebra $R\{t\}/(f)$.

Proposition 3.2: *With the assumptions of* 3.1, *we also fix an indeterminate* u.

(1) *The object* $(R\{t\}, f)$ *of* $\mathrm{Alg}^+_{R[t]}$ *is the filtered colimit of a system* $(A_\lambda, f_\lambda)_{\lambda\in L}$ *with, for each* $\lambda \in L$, *the following properties:*
   (i) *The* $R[t]$*-algebra* A_λ *is étale and, for all* $n \in \mathbb{N}$, *the canonical morphism* $R[t]/(t^n) \to A_\lambda/t^n A_\lambda$ *is an isomorphism.*
   (ii) *The canonical* R*-morphism* $R[u] \to A_\lambda$ *mapping* u *to* f_λ *is flat and quasifinite.*

   In particular, the canonical R*-morphism* $R[u] \to R\{t\}$ *mapping* u *to* f *is flat, and* f *is a nonzerodivisor in* $R\{t\}$.

(2) *The* $R[t]$*-algebra* S *is the filtered colimit of a system* $(S_\lambda)_{\lambda\in L}$ *with the following properties:*
   (i) *Each* R*-algebra* S_λ *is flat, of finite presentation and quasifinite, and the transition maps* $S_\lambda \to S_\mu$ $(\lambda \leq \mu)$ *are étale. (In particular,* S *is flat over* R.*)*
   (ii) *For all* $n \in \mathbb{N}$ *and* $\lambda \in L$, *the canonical morphism* $R[t]/(t^n) \to S_\lambda/t^n S_\lambda$ *is surjective.*

Proof. Part (1) immediately implies part (2), with $S_\lambda = A_\lambda/(f_\lambda)$ (the transition maps are étale due to the same property for the A_λ's, which are étale over $R[t]$).

To prove (1), write $R\{t\} = \varinjlim_{\lambda\in L} A_\lambda$ as in Lemma 2.2.1, and call $t_\lambda \in A_\lambda$ the canonical image of t. There exists $\lambda_0 \in L$ and $f_{\lambda_0} \in A_{\lambda_0}$ mapping to f; we can restrict L to the indices $\lambda \geq \lambda_0$ and, for each λ, denote by $f_\lambda \in A_\lambda$ the image of f_{λ_0}. Clearly, we have $(R\{t\}, f) = \varinjlim_{\lambda\in L}(A_\lambda, f_\lambda)$. Part (1) (i) is obvious from the choice of $(A_\lambda)_{\lambda\in L}$.

Let us prove (1) (ii). For fixed λ, we can view f_λ as a morphism

$$g_\lambda : X_\lambda := \operatorname{Spec}(A_\lambda) \to \mathbb{A}^1_R = \operatorname{Spec}(R[u])$$

of R-schemes. For $s \in \operatorname{Spec}(R)$, the $\kappa(s)$-morphism $g_{\lambda,s} : X_{\lambda,s} \to \mathbb{A}^1_{\kappa(s)}$ induced on the fibers is deduced from $1 \otimes f_\lambda \in \kappa(s) \otimes_R A_\lambda$, whose image in $\kappa(s) \otimes_R R\{t\}$ is assumed nonconstant. So $g_{\lambda,s}$ is not constant on $X_{\lambda,s}$, which is a smooth geometrically irreducible curve over $\kappa(s)$. It follows that $g_{\lambda,s}$ is flat and quasifinite. Since X_λ and $\mathbb{A}^1_R$ are smooth over $\operatorname{Spec}(R)$, the "fiberwise flatness" criterion [7, (11.3.10)] shows that g_λ is flat. It is also quasifinite since it is affine of finite presentation with finite fibers. This completes the proof. ∎

Definition 3.3: Let R be a ring, I an ideal of R, t an indeterminate.

We say that a formal power series $f = \sum_{i\geq 0} a_i t^i \in R[[t]]$ is **I-normal** if there is $d \in \mathbb{N}$ such that $a_d \in R^\times$ and $a_i \in I$ for $i < d$. The integer d (unique if $I \neq R$) is called the order of f.

We say that f is **I-monic** of order d if it is I-normal of order d and $a_d = 1$.

An element f of $R\{t\}$ is I-normal (I-monic) of order d if $f_{\text{for}} \in R[[t]]$ is.

Proof of Theorem 1.1. As in 1.1, let (R, I) be a henselian pair and let $f \in R\{t\}$ be I-normal of order d, with $f_{\text{for}} = \sum_{i\geq 0} a_i t^i \in R[[t]]$ $(a_i \in R)$. If $d = 0$, everything is trivial, so we assume in addition that $d > 0$; thus, the assumption of 3.1 is satisfied and, in particular, Proposition 3.2 applies to f.

Assume assertion 1.1 (1) is proved, i.e., $S = R\{t\}/(f)$ is a free R-module with the images of $1, t, \ldots, t^{d-1}$ as a basis. This immediately implies the division theorem 1.1 (2), with uniqueness coming from the fact that f is a nonzerodivisor (3.2 (1)).

In turn, the division theorem implies the preparation theorem 1.1 (3). Indeed, the relation in (3) can be rewritten as $t^d = v^{-1} f - Q$, so that uniqueness follows from the uniqueness part of (2); next, applying (2) to t^d, we find that $t^d = Bf - Q$ where Q is a polynomial of degree $< d$. Reducing modulo I and comparing coefficients, we see that Q has coefficients in I and the constant term of B is in $a_d + I$, which gives (3) with $v = B^{-1}$.

It remains to prove 1.1 (1). As in 2.3, we put $\overline{A} = A/IA$ for every R-algebra A.

First we observe that the image $\overline{f}$ of f in $\overline{R\{t\}} \cong \overline{R}\{t\}$ is the product of t^d by a unit, so that

$$\overline{S} \cong \overline{R}\{t\}/(t^d) \cong \overline{R}[t]/(t^d)$$

which is $\overline{R}$-free with basis $(1, t, \ldots, t^{d-1})$.

Let us write S as the colimit of a filtered system $(S_\lambda)_{\lambda\in L}$ of $R[t]$-algebras with the properties of 3.2 (2). We have just seen that t^d vanishes in $\overline{S}$, so by changing the index set L we may assume that t^d vanishes in $\overline{S_\lambda}$ for all λ: thus, $\overline{S_\lambda} = \overline{S_\lambda/t^dS_\lambda}$ hence, by 3.2 (2) (ii), it is a quotient of $\overline{R}[t]/(t^d)$. So we have morphisms of $\overline{R}[t]$-algebras $\overline{R}[t]/(t^d) \to \overline{S_\lambda} \to \overline{S}$ where the first map is surjective and the composition is an isomorphism. We conclude that $\overline{R}[t]/(t^d) \xrightarrow{\sim} \overline{S_\lambda}$ for all λ. In particular, $\overline{S_\lambda}$ is finite over $\overline{R}$. As (R, I) is henselian, we may apply Proposition 2.3.2 and write $S_\lambda = S_\lambda^{\mathrm{f}} \times T_\lambda$, where S_λ^{f} is finite over R and $\overline{S_\lambda^{\mathrm{f}}} = \overline{S_\lambda}$. By functoriality (Remark 2.3.3), the quotients S_λ^{f} of the S_λ's form an inductive system.

Since S is a quotient of $R\{t\}$ and $(R\{t\}, IR\{t\})$ is a Zariski pair, so is (S, IS). Hence, for all λ, the canonical morphism $S_\lambda \to S$ factors through S_λ^{f} by 2.3.2 (3), and finally $S = \varinjlim_{\lambda\in L} S_\lambda^{\mathrm{f}}$.

Since, for each λ, S_λ is a flat R-algebra of finite presentation, so is S_λ^{f}, which is in addition a finite R-module, hence locally free. As $(1, t_\lambda, \dots, t_\lambda^{d-1})$ induces an $\overline{R}$-basis of $\overline{S_\lambda^{\mathrm{f}}}$, and $I \subset \operatorname{rad}(R)$, it follows easily that $(1, t_\lambda, \dots, t_\lambda^{d-1})$ is an R-basis of S_λ^{f} for all λ, and part (1) follows. ∎

4. Application: a henselian resultant

If R is a ring, S a finite locally free R-algebra and x an element of S, we denote by $\mathrm{N}_{S/R}(x) \in R$ the norm of x in R, i.e., the determinant of multiplication by x in the R-module S.

Definition 4.1: Let (R, I) be a henselian pair. Let $f \in R\{t\}$ be I-monic of order d. Denote by S the R-algebra $R\{t\}/(f)$ (which is a free R-module of rank d, by 1.1 (1)).

For $g \in R\{t\}$, the (**henselian**) **resultant** of f and g, denoted by $\mathrm{Res}^{\mathrm{h}}(f, g)$, is the element of R defined by

$$\mathrm{Res}^{\mathrm{h}}(f, g) := \mathrm{N}_{S/R}(g).$$

4.2. Properties of the resultant. We keep the notation and assumptions of 4.1, and we denote by $P = t^d + Q$ the polynomial associated to f by 1.1 (3). The proofs of the following properties are easy and left to the reader.

4.2.1. *Functoriality.* Let $\varphi : (R, I) \to (R', I')$ be a morphism of henselian pairs, f' and g' the images of f and g in $R'\{t\}$. Then

$$\mathrm{Res}^{\mathrm{h}}(f', g') = \varphi(\mathrm{Res}^{\mathrm{h}}(f, g)).$$

4.2.2. By construction, $\mathrm{Res}^{\mathrm{h}}(f, g)$ only depends on f via the R-algebra $R\{t\}/(f)$. In particular,

$$\mathrm{Res}^{\mathrm{h}}(f, g) = \mathrm{Res}^{\mathrm{h}}(P, g).$$

4.2.3. $\mathrm{Res}^{\mathrm{h}}(f, g)$ only depends on g via its class modulo f; in other words, we have

$$\mathrm{Res}^{\mathrm{h}}(f, g + hf) = \mathrm{Res}^{\mathrm{h}}(f, g) \quad \text{for all } h \in R\{t\}.$$

Moreover, $\mathrm{Res}^{\mathrm{h}}(f, g) \in R^\times$ if and only if the ideal $(f, g) \subset R\{t\}$ equals $R\{t\}$. (More generally, see 4.2.8 below.)

4.2.4. *Special cases.* If $\alpha \in R$, we have

$$\mathrm{Res}^{\mathrm{h}}(f, \alpha) = \alpha^d \quad \text{and} \quad \mathrm{Res}^{\mathrm{h}}(f, \alpha - t) = P(\alpha).$$

If $\alpha \in I$, then

$$\mathrm{Res}^{\mathrm{h}}(\alpha - t, g) = g(\alpha)$$

and

$$\mathrm{Res}^{\mathrm{h}}(f, \alpha - t) = (1 + \varepsilon)\, f(\alpha) \quad \text{for some } \varepsilon \in I$$

by the second formula above (recall that f is I-monic).

4.2.5. *Multiplicativities.* If $h \in R\{t\}$, we have

$$\mathrm{Res}^{\mathrm{h}}(f, gh) = \mathrm{Res}^{\mathrm{h}}(f, g)\, \mathrm{Res}^{\mathrm{h}}(f, h);$$

if in addition h is I-monic of order m, then

$$\mathrm{Res}^{\mathrm{h}}(fh, g) = \mathrm{Res}^{\mathrm{h}}(f, g)\, \mathrm{Res}^{\mathrm{h}}(h, g).$$

For the second equality, one may use the exact sequence

$$0 \longrightarrow R\{t\}/(h) \xrightarrow{\times f} R\{t\}/(fh) \longrightarrow R\{t\}/(f) \longrightarrow 0.$$

4.2.6. *Polynomials.* If f and g are in $R[t]$, with f monic of degree d (in the sense of polynomials), then $\mathrm{Res}^{\mathrm{h}}(f, g)$ is the usual resultant. The condition on f is essential: for instance, $\mathrm{Res}^{\mathrm{h}}(1 + \alpha t, g) = 1$ for all $\alpha \in R$ and $g \in R\{t\}$. (In fact, for two possibly non-monic polynomials of respective degrees $\leq d$ and $\leq m$, the definition of the classical resultant depends on the choice of d and m.)

4.2.7. *Weak symmetry.* Assuming that g is I-monic of order m, then

$$\mathrm{Res}^{\mathrm{h}}(g,f) = (-1)^{md}\,(1+\varepsilon)\,\mathrm{Res}^{\mathrm{h}}(f,g) \quad \text{for some } \varepsilon \in I.$$

To see this, reduce to the case of polynomials and apply 4.2.6.

4.2.8. *Elimination.* Let $J \subset R\{t\}$ be the ideal generated by f and g. Then $\mathrm{Res}^{\mathrm{h}}(f,g) \in J$ (thus it belongs to $J \cap R$): indeed, in the free R-module $S = R\{t\}/(f)$, the image of multiplication by g contains $\mathrm{Res}^{\mathrm{h}}(f,g)\,S$.

Conversely, every $\alpha \in J \cap R$ is a multiple of the class of g in S so, taking norms, α^d is a multiple of $\mathrm{Res}^{\mathrm{h}}(f,g)$ in R. In particular, we have in R the inclusions $(\mathrm{Res}^{\mathrm{h}}(f,g)) \subset J \cap R \subset \sqrt{(\mathrm{Res}^{\mathrm{h}}(f,g))}$. Geometrically, the closed subset $V(\mathrm{Res}^{\mathrm{h}}(f,g)) \subset \mathrm{Spec}\,(R)$ is the projection of $V(f,g) \subset \mathrm{Spec}\,(R\{t\})$.

4.2.9. *Roots.* Let $\varphi : R \to R'$ be a ring homomorphism, and let $\alpha \in R'$ be a zero of P in R'. First, I claim that $g(\alpha)$ makes sense in R' and is an element of $R[\alpha] \subset R'$. Indeed, the relation $P(\alpha) = 0$ shows that (due to the form of P) $\alpha^d \in IR[\alpha]$, whence $\alpha \in \sqrt{IR[\alpha]}$. Since $R[\alpha]$ is a finite R-module, the pair $(R[\alpha], \sqrt{IR[\alpha]})$ is henselian, hence the claim.

Now assume that the image of P in $R'[t]$ factors as $\prod_{i=1}^{d}(t-\alpha_i)$, where the α_i's are elements of R'. Then we have in R' the equality

$$\varphi(\mathrm{Res}^{\mathrm{h}}(f,g)) = \prod_{i=1}^{d} g(\alpha_i)$$

as follows from the above remark and properties 4.2.4 and 4.2.5 (applied in the ring $R[\alpha_1,\dots,\alpha_d] \subset R'$).

Note that if we assume for simplicity that $R = R'$ is a domain, then the α_i's are the zeros of f in $\sqrt{I}$.

4.2.10. *Power series.* Assume R is I-adically complete and separated. Then

$$\mathrm{Res}^{\mathrm{h}}(f,g) = \mathrm{Res}(f_{\mathrm{for}}, g_{\mathrm{for}})$$

where Res denotes the resultant defined in [4].

References

[1] M. E. Alonso and H. Lombardi, *Local Bézout theorem*, Journal of Symbolic Computation **45** (2010), 975–985.

[2] M. E. Alonso and H. Lombardi, *Local Bézout theorem for Henselian rings*, Collectanea Mathematica **68** (2017), 419–432.

[3] G. Azumaya, *On maximally central algebras*, Nagoya Mathematical Journal **2** (1951), 119–150.

[4] L. Berger, *The Weierstrass preparation theorem and resultants of p-adic power series*, Münster Journal of Mathematics **14** (2012), 155–163.

[5] N. Bourbaki, *Algèbre commutative, chapitres 5 à 7*, Springer, Berlin–Heidelberg, 2006.

[6] A. Bouthier and K. Česnavičius, *Torsors on loop groups and the Hitchin fibration*, Annales Scientifiques de l'École Normale Supérieure **55** (2022), 791–864.

[7] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III*, Institut des Hautes Études Scientifiques. Publications Mathématiques **28** (1966).

[8] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV*, Institut des Hautes Études Scientifiques. Publications Mathématiques **32** (1967).

[9] J.-P. Lafon, *Anneaux henséliens*, Bulletin de la Société Mathématique de France **91** (1963), 77–107.

[10] M. Nagata, *Local Rings*, Interscience Tracts in Pure and Applied Mathematics, Vol. 13, Interscience, New York–London, 1962.

[11] M. O'Malley, *On the Weierstrass preparation theorem*, Rocky Mountain Journal of Mathematics **2** (1972), 265–273.

[12] M. Raynaud, *Anneaux locaux henséliens*, Lecture Notes in Mathematics, Vol. 169, Springer, Berlin, 1970.

[13] The Stacks project authors, *The Stacks project*, `https://stacks.math.columbia.edu`.