ELEMENTARY CONSTRUCTIVE THEORY OF HENSELIAN LOCAL RINGS

M. EMILIA ALONSO GARCIA, HENRI LOMBARDI, AND HERVÉ PERDRY

Abstract. We give an elementary theory of Henselian local rings and construct the Henselization of a local ring. All our theorems have an algorithmic content.

1. Introduction

We give an elementary theory of Henselian local rings. The paper is written in the style of Bishop's constructive mathematics, i.e., mathematics with intuitionistic logic (see [2, 3, 8]. In this frame we do not assume any constraint of the kind "explicit means Turing computable". So that, our proofs work as well inside classical mathematics; it is sufficient to assume that "explicit" is a void word. However if the hypotheses are "Turing computable", so are the conclusions. In this sense we claim that our proofs have always an algorithmic content.

Through this paper, when we say: "Let R be a ring ...", this means that:
(1) we know how to construct elements of R (from now on called *canonical elements*), (2) we have given 1_R, 0_R, -1_R, constructed according to (1), (3) we know how to construct $x+y$ and xy according to (1), when the objects x and y are given through the same construction, (4) we know what is the meaning of $x =_R y$ when x and y are elements of R given through the construction (1), and (5) we have constructive proofs showing that the axioms of rings are satisfied by this structure.

Hence, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and all usual rings are rings in the constructive meaning of the word already explained. Notice that (4) does not imply to have given a constructive test of equality for canonical elements. A ring R is said *discrete* when we have, constructively, for any elements x and y of E: $x =_E y$ or $\neg(x =_E y)$. So $\mathbb{R}$ is *not* discrete. If it were the case, this would imply the following so-called *limited principle of omniscience*:

$$(\mathbf{LPO})\quad \forall \alpha \in \{0,1\}^{\mathbb{N}},\ (\exists n,\ \alpha_n = 1) \vee (\forall n,\ \alpha_n = 0)$$

which is considered to be not acceptable in constructive mathematics. For more details, we refer the reader to [3, 8].

Of course, in classical mathematics, all constructive theorems about discrete fields apply to $\mathbb{R}$ because it becomes discrete if we assume (**LPO**).

On the other hand $\mathbb{Z}$ is a discrete ring, even if for "non-canonical"elements of $\mathbb{Z}$ it is impossible to decide the equality (e.g., equality between x and y where $x = 0$ and $y = 0$ if ZF is consistent, and $y = 1$ in the other case).

Many classical definitions have to be rewritten in a suitable form to fit well in our constructive setting. E.g., a *local ring*, will be a ring A such that

$$\forall x \in A,\ x \in A^{\times} \text{ or } (1+x) \in A^{\times}.$$

Precisely, this will means that, for any canonical $x \in A$ we can either construct y such that $xy = 1$, or construct y such that $(1+x)y = 1$, with an explicit meaning for the "or".

Date: May 2006.

Universitad Complutense, Madrid, España. M_Alonso@Mat.UCM.Es.
Univ. de Franche-Comté, 25030 Besançon cedex, France. henri.lombardi@univ-fcomte.fr.
Dip. di Mat. Università di Pisa. Italia. perdry@mail.dm.unipi.it.

This construction is not required to be "extensional": two (canonical) elements x and x' of A which are equal in A, need not give the same branch of the alternative. Typically, $\mathbb{R}$ is a local ring in which there *cannot* exist an extensional way of satisfying the axiom of local rings.

The theory of Henselian rings was developed by Nagata (see [9]). He introduced the notion of Henselization of a local ring based on the case of integrally closed domains. Namely, for an integrally closed domain $(R, \mathfrak{m})$, let R' the separable integral closure of R inside an algebraic closure of its quotient field. Let $\mathfrak{p}'$ a maximal ideal of R' lying over $\mathfrak{m}$, R'' be the splitting ring of $\mathfrak{p}'$ and $\mathfrak{p}'' = R'' \cap \mathfrak{p}'$. The Henselization of R is $R''_{\mathfrak{p}''}$ This "construction" is very abstract, and it seems difficult to be adapted to our constructive setting.

Our approach relies heavily upon more recent expositions, namely the book of Lafon & Marot [5], Chapters 12 & 13. Although this book is not written in a purely constructive way, the authors have made a remarkable effort in order to give simplified proofs of many classical results, so that, it provided us a good basis to develop our constructive theory. In fact, in Lafon&Marot the Henselization of a local ring is constructed as a part of an inductive completion of the ring A. Namely, one consider the inductive limit of the family of sub-rings obtained by taking the completion of local Noetherian sub-rings of A. This is a natural object, but it is difficult to manage it from constructive point of view. Our achievement could be considered as simplifying or making explicit the Lafon&Marot construction.

There are still some problems to be solved in order to have a satisfactory constructive theory of Henselian local rings In particular, to prove the so-called *multi-dimensional Hensel Lemma* whose proof relies on the Zariski Main Theorem, which is highly non constructive. In classical mathematics, the Henselization of a local ring $(A, \mathfrak{m})$ coincides with the limit of the local essentially finitely generated A-algebras $\left(A[X_1, \ldots, X_n]/\langle F_1, \ldots, F_n\rangle\right)_{(\mathfrak{m},x)}$ at a non singular point $(\mathfrak{m}, x)$. This fact allows to represent algebraic functions (locally), and to state algorithms on standard bases in the ring of algebraic formal power series (cf. [1]). This characterization of the Henselization relies on Zariski Main Theorem, which provides a kind of "primitive smooth element" for étale extensions.

Finally, it will be also interesting to compare explicitly our construction to the one, already quoted, given by Nagata in [9].

The plan of the paper is as follows. The first three sections are devoted to study the basic notions that will be useful for our constructive proofs; namely the Boolean algebra of idempotents of a finite A algebra, and the Universal decomposition algebra. Idempotents play a similar role to minimal prime ideals, that are in general non constructable objects.

In 4 & 5 we accomplish the construction of the Henselization of a local ring, and we prove some basic properties of Henselian local rings, including the fact that residual idempotents in a finite algebra over a Henselian ring can be always lifted to idempotents of the algebra. Finally we generalize our approach to the construction of the strict Henselization.

We recall that the constructive theory of Henselian valuation rings has been developed in [6], [10], [11].

2. Rings and Local Rings

In the whole paper, rings are commutative.

2.1. **Radicals.**

The *Jacobson radical* of a ring A is

$$\mathcal{J}_A = \{x \in A \,:\, \forall y \in A,\ 1 + x \cdot y \in A^\times\}.$$

Let A be a ring and $I \subseteq A$ an ideal. The *radical* of I is

$$\sqrt{I} = \{x \in A \,:\, \exists n \in \mathbb{N},\ x^n \in I\}.$$

In classical mathematics, if A is nontrivial $\mathcal{J}_A$ is the intersection of all maximal ideals of A, and $\sqrt{(0)}$ the intersection of all prime ideals of A. Notice that an ideal I is contained in $\mathcal{J}_A$ if and only if $1+I \subseteq A^\times$ and that $x \in A$ is invertible if and only if it is invertible modulo $\mathcal{J}_A$.

The following classical result is true constructively, when we read $x \in A \setminus A^\times$ as "$x \in A$ and $(x \in A^\times \Rightarrow False)$".

Lemma 2.1. *If A is a nontrivial local ring, then $\mathcal{J}_A = A \setminus A^\times$, and it is the unique maximal ideal of A. We denote it by $\mathfrak{m}_A$ or simply by $\mathfrak{m}$.*

The *residue field* of a (nontrivial) local ring A with maximal ideal $\mathfrak{m}$ is $\mathbf{k} = A/\mathfrak{m}$. If $\mathbf{k}$ is discrete, A will be called *residually discrete*.

A nontrivial ring A is local and residually discrete if and only if we have

$$\forall x \in A \quad (x \in A^\times \text{ or } x \in \mathcal{J}_A),$$

with the constructive meaning of the disjunction.

Remark. In constructive mathematics, a Heyting field (or simply a field) is a nontrivial local ring in which "x not invertible implies $x = 0$". This is the same thing as a nontrivial local ring whose Jacobson radical is 0.

The ring A defined by $A = S^{-1}\mathbb{R}[T]$, where S is the set of polynomials g with $g(0) \in \mathbb{R}^\times$, is a local ring: the statement $\forall x \in A,\ x \in A^\times$ or $(1+x) \in A^\times$ holds. The residue field of A is $\mathbb{R}$, and the quotient map $A \longrightarrow \mathbb{R}$ is given by $f/g \mapsto f(0)/g(0)$. This provides an example of a local ring A which is *neither* discrete *nor* residually discrete. The ring of p-adic integers is an example of a local ring which is residually discrete but *not* discrete.

Some results in this paper avoid the hypothesis for a ring to be discrete. We think that when it is possible this greater generality is often usefull, as shown by the previous examples.

2.2. Idempotents and idempotent matrices.

Definition 2.2. *For a commutative ring C we shall denote $\mathbb{B}(C)$ the boolean algebra of idempotents of C. The operations are: $u \wedge v := u \cdot v$, $u \vee v := u+v-u \cdot v$, $u \oplus v := u+v-2 \cdot u \cdot v = (u-v)^2$, the complementary of u is $1-u$, and the partial ordering, $u \preceq v \iff u \wedge v = u \iff u \vee v = v$.*

Note that the partial ordering can be expressed in terms of the homomorphism μ_z of multiplication by z in C: $u \preceq v \iff \ker(\mu_v) \subseteq \ker(\mu_u) \iff \mathrm{Im}(\mu_u) \subseteq \mathrm{Im}(\mu_v)$.

A nonzero idempotent e is said to be *indecomposable* if when it is written as the sum of two orthogonal idempotents e_1 and e_2, then either $e_1 = 0$ or $e_2 = 0$.

A family of idempotent elements $\{r_1, \ldots, r_m\}$ in a commutative ring is a *basic system of orthogonal idempotents* if $\sum_{i=1}^m r_i = 1$ and $r_i \cdot r_j = 0$ for $1 \leq i < j \leq m$.

If B is a finitely generated and discrete boolean algebra, it is possible to construct a basic system of orthogonal indecomposable idempotents $\{r_1, \ldots, r_m\}$ generating B. This shows that B is isomorphic to the boolean algebra $\mathbb{F}_2^m$ (where the field with two elements $\mathbb{F}_2$ is viewed as a boolean algebra).

Lemma 2.3. (idempotents are always isolated)
If e, h are idempotents and $e-h$ is in the Jacobson radical then $e = h$. In other words, the canonical map $\mathbb{B}(A) \to \mathbb{B}(A/\mathcal{J}_A)$ is injective. In particular if $\mathbb{B}(A/\mathcal{J}_A)$ is discrete then so is $\mathbb{B}(A)$.

Proof. First notice that if an idempotent f is in the Jacobson radical then $f = 0$ since $1-f$ is an invertible idempotent. Now two idempotents e, h are equal if and only if $e \oplus h = 0$. But $e \oplus h = (e-h)^2$. So we are done. □

Remark. Lemma 2.3 is a sophisticated rewriting of the identity $(e-h)^3 = (e-h)$ when e and h are idempotents.

Definition 2.4. *A commutative ring A is said to have* the property of idempotents lifting *when the canonical map $\mathbb{B}(A) \to \mathbb{B}(A/\mathcal{J}_A)$ is bijective.*

Lemma 2.5. (idempotents modulo nilpotents can always be lifted)
The canonical map $\mathbb{B}(A) \to \mathbb{B}\left(A/\sqrt{(0)}\right)$ is bijective.

Proof. Injectivity comes from Lemma 2.3. If $e^2 - e = n$ is nilpotent, e.g., $n^{2^k} = 0$, then for $e' = 3e^2 - 2e^3$ we have $e' - e \in nA$ and $(e')^2 - e' \in n^2 A$. So it is sufficient to perform k times the Newton iteration $x \mapsto 3x^2 - 2x^3$. □

Remark. The notion of finite boolean algebra in classical mathematics corresponds to several *nonequivalent*[1] notions in constructive mathematics. A set E is said to be *finite* if there exists a bijection with an initial segment $[1..n]$ of $\mathbb{N}$, *bounded* if we know a bound on the number of pairwise distinct elements, *finitely enumerable* if there exists a surjection from some $[1..n]$ onto E. Finite sets are finitely enumerable discrete sets. Finitely enumerable sets are bounded. The set of the monic divisors of a monic polynomial on a discrete field is discrete and bounded but a priori *not*[2] finitely enumerable. A boolean algebra is finitely enumerable if and only if it is finitely generated.

A *projective module of finite type* over a ring A is a module isomorphic to a direct summand of a free module A^m. Equivalently, M is isomorphic to the image of an idempotent matrix $F \in A^{m\times m}$.

In the following lemma we introduce a polynomial $P_F(T)$ which is the determinant of the multiplication by T in $\mathrm{Im}(F) \otimes_A A[T]$.

Lemma 2.6. *If $F \in A^{m\times m}$ is an idempotent matrix, let*

$$P_F(T) := \det(\mathrm{Id}_m + (T-1)F) = \sum_{i=0}^{m} e_i T^i.$$

Then $\{e_0, \dots, e_m\}$ is a basic system of orthogonal idempotents.

If $P_F(T) = T^r$ the projective module $\mathrm{Im}\, F$ is said to have *constant rank* r.

Proof. A direct computation shows that $P_F(TT') = P_F(T) \cdot P_F(T')$ and $P_F(1) = 1$. □

It can be shown that $\mathrm{Tr}(F) = \sum_{k=0}^{n} k e_k$, so when $\mathbb{Z} \subseteq A$, $\mathrm{Im}\, F$ has constant rank r if and only if $\mathrm{Tr}(F) = r$.

2.3. **Flat and faithfully flat algebras.**

Definition 2.7. *An A-algebra $\varphi : A \to B$ is* flat *if for every linear form*

$$\begin{array}{rccc} \alpha\ : & A^n & \to & A \\ & (x_1, \dots, x_n) & \mapsto & a_1 \cdot x_1 + \cdots + a_n \cdot x_n \end{array}$$

(α is given by the row vector $(a_1, \dots, a_n)$), the kernel of

$$\begin{array}{rccc} \alpha^*\ : & B^n & \to & B \\ & (x_1, \dots, x_n) & \mapsto & \varphi(a_1) \cdot x_1 + \cdots + \varphi(a_n) \cdot x_n \end{array}$$

(α^* is given by the row vector $(\varphi(a_1), \dots, \varphi(a_n))$) is the B-module generated by $\varphi(\ker \alpha)$.

This property is easily extended to kernels of arbitrary matrices. So the intuitive meaning of flatness is that the change of ring from A to B doesn't add "new" solutions to homogeneous linear systems. One says also that B is flat over A, or φ is a flat morphism.

[1] As for "$\mathbb{R}$ is *not* a discrete field", this can be proved by showing that the contrary would imply some principle of omniscience.

[2] Same thing.

Example 2.8. *The composition of two flat morphisms is flat. A localization morphism $A \to S^{-1}A$ is flat. If B is a free A-module it is flat over A.*

Definition 2.9. *A flat algebra is* faithfully flat *if for every linear form $\alpha : A^n \to A$ and every $c \in A$ the linear equation $\alpha(x) = c$ has a solution in A^n if the linear equation $\alpha^*(y) = \varphi(c)$ has a solution in B^n.*

In this case φ is injective, a divides a' in A if $\varphi(a)$ divides $\varphi(a')$ in B, and a is a unit in A if $\varphi(a)$ is a unit in B.

The property in the definition of faithfully flat is easily extended to solutions of arbitrary linear systems. So the intuitive meaning of faithfull flatness is that the change of ring from A to B doesn't add "new" solutions to linear systems.

Definition 2.10. *We say that a ring morphism $\varphi : A \to B$* reflects the units *if for all $a \in A$, $\varphi(a) \in B^\times \Rightarrow a \in A^\times$.*

Lemma 2.11. *A flat morphism $\varphi : A \to B$ is faithfully flat if and only if for every finitely generated ideal $\mathfrak{a}$ of A we have that, $1_B \in \mathfrak{a} \cdot B \Rightarrow 1_A \in \mathfrak{a}$. In case B is local this means that φ reflects the units.*

Proof. The condition is clearly necessary. Let $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle$ and c in A. The equation $\alpha(x) = c$ has a solution in A^n if and only if $\mathfrak{a} : c = \langle 1 \rangle$. Since the morphism is flat $\varphi(\mathfrak{a} : c) \cdot B = (\varphi(\mathfrak{a}) : \varphi(c))$. If $\alpha^*(y) = \varphi(c)$ has a solution in B^n, $1 \in (\varphi(\mathfrak{a}) : \varphi(c))$. So we have a finitely many $x_j \in \mathfrak{a} : c$ such that $1 \in \langle (\varphi(x_j))_{j=1,\ldots,k} \rangle_B$. If the condition holds, $1 \in \langle (x_j)_{j=1,\ldots,k} \rangle_A$, so $1 \in (\mathfrak{a} : c)$: the morphism is faithfully flat. □

Definition 2.12. *A ring morphism φ from a local ring $(A, \mathfrak{m}_A)$ to a local ring $(B, \mathfrak{m}_B)$ is said to be* local *when it reflects the units.*

This implies also that $\varphi(\mathfrak{m}_A) \subseteq \mathfrak{m}_B$. When A and B are residually discrete we have the converse implication: $\varphi(\mathfrak{m}_A) \subseteq \mathfrak{m}_B$. So that the ring morphism is local.

A particular case of lemma 2.11 is the classical following one. It works constructively thanks to the previous "good" definitions in a constructive setting.

Lemma 2.13. *A flat morphism between local rings is local if and only if it is faithfully flat.*

Remark. In classical mathematics, an algebra over a field has always a basis as vector space. In a constructive setting, this property can be in general replaced by the fact that a nontrivial algebra over a discrete field is always faithfully flat.

3. Finite algebras over local rings

An A-algebra B is *finite* if it is finite as A-module.

3.1. **Preliminaries.** When A is a discrete field the classical structure theorem for finite A-algebras, which is a basic tool, has to be rewritten to be constructively valid. This will be done in Corollary 3.5.

Lemma 3.1 (Cayley-Hamilton)**.** *(see [4] Theorem 4.12)*
Let M be a finite module over A. Let $\phi : M \to M$ an homomorphism such that $\phi(M) \subseteq \mathfrak{a} \cdot M$ for some ideal $\mathfrak{a}$ of A. Then we have a polynomial identity of homomorphisms,

$$\phi^n + a_1 \cdot \phi^{n-1} + \ldots + a_n \cdot \mathrm{Id}_M = 0 \qquad (*)$$

where $a_h \in \mathfrak{a}^h$ and n is the cardinality of some system of generators of M.

Corollary 3.2 (Nakayama's lemma)**.** *Let M be a finite module over a ring A, $\mathfrak{m}$ an ideal, and $N \subseteq M$ a submodule. Assume that*

$$M = N + \mathfrak{m} \cdot M$$

Then there exists $m \in \mathfrak{m}$ such that $(1 + m)M \subseteq N$. If moreover $\mathfrak{m} \subseteq \mathcal{J}_A$, then $M = N$.

Applying Lemma 3.1 to the multiplication by an element in a finite algebra, we get the following corollary.

Corollary 3.3. *Let $\varphi : A \to B$ be a finite algebra (B is an A-module generated by n elements), $\mathfrak{a}$ an ideal of A, $A_1 = \varphi(A)$ and $\mathfrak{a}_1 = \varphi(\mathfrak{a})$.*

1. *Every $x \in B$ is integral over A_1. If moreover, $x \in \mathfrak{a}_1 \cdot B$ then $f(x) = 0$ for some $f(X) = X^n + a_1 \cdot X^{n-1} + \cdots + a_n$ where $a_h \in \mathfrak{a}_1^h$.*
2. *If $x \in B^\times$, then there exists $f \in A_1[X]$ such that $f(x) \cdot x = 1_B$ (with $\deg(f) \leq n-1$).*
3. *$A_1 \cap B^\times = A_1^\times$ and $A_1 \cap \mathcal{J}_B = \mathcal{J}_{A_1}$.*
4. *Assume B is nontrivial. If A is local φ reflects the units. If moreover B is local and flat over A then it is faithfully flat.*

Proof. (2) Let y be the inverse of x. If $y^n + a_1 \cdot y^{n-1} + \cdots + a_n = 0$ with $a_i \in A$, multiplying by x^n we get the result.
(3) Let $x \in A_1 \cap B^\times$. Applying (2) we get $v = f(x) \in A_1$ such that $xv = 1_B$.
If x is in $\mathcal{J}_B$, and $y \in \mathbb{A}_1$, then $1 + xy \in A_1 \cap B^\times = A_1^\times$, so $x \in \mathcal{J}_{A_1}$.
If $x \in \mathcal{J}_{A_1}$ and $b \in B$, we have to show that $z = -1 + xb$ is invertible. Write $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$ with a_i's in A_1. So

$$(z+1)^n + a_{n-1}x(z+1)^{n-1} + a_{n-2}x^2(z+1)^{n-2} + \cdots + a_0x^n = 0.$$

The constant coefficient of this polynomial in z is $1 + a_{n-1}x + a_{n-2}x^2 + \cdots + a_0x^n$, so it is invertible, and z is invertible.
(4) Since B is nontrival $\ker \varphi \subseteq \mathcal{J}_A$. If $\varphi(u) \in B^\times$, by (3) we have $v \in A$ such that $uv \in 1+\ker \varphi \subseteq 1+\mathcal{J}_A \subseteq A^\times$. If moreover B is local and flat over A we conclude by Lemma 2.11. □

Definition 3.4. *We say that a ring B is* zero-dimensional *if*

$$\forall x \in B\ \exists y \in B\ \exists k \in \mathbb{N},\ x^k \cdot (1 - x \cdot y) = 0\,.$$

Now we get a constructive version of the classical structure theorem. Notice that it is not assumed that B has a finite basis over $\mathbf{k}$.

Corollary 3.5. (structure theorem for finite algebras over discrete fields).
Let B be a finite algebra over a discrete field $\mathbf{k}$.

1. *B is* zero-dimensional*, more precisely*
$$\forall x \in B\ \exists s \in A[X]\ \exists k \in \mathbb{N},\ x^k \cdot (1 - x \cdot s(x)) = 0\,.$$
2. *$\mathcal{J}_B = \sqrt[B]{\langle 0\rangle}$. So B has the property of idempotents lifting.*
3. *For every $x \in B$, there exists an idempotent $e \in \mathbf{k}[x] \subseteq B$ such that x is invertible in $B[1/e] \cong B\,/\langle 1-e\rangle$ and nilpotent in $B[1/(1-e)] \cong B\,/\langle e\rangle$.*
4. *B is local if and only if every element is nilpotent or invertible, if and only if every idempotent is 0 or 1. Assume B is nontrivial, then it is local if and only if $\mathbb{B}(B) = \mathbb{F}_2$. In this case $B/\mathcal{J}_B$ is a discrete field.*
5. *$\mathbb{B}(B)$ is* bounded*.*
6. *If $\mathbb{B}(B)$ is* finite*, B is the product of a finite number of finite local algebras (in a unique way up to the order of factors).*

3.2. Jacobson radical of a finite algebra over a local ring.

Context. In Sections 3.2 and 3.3 A is a nontrivial residually discrete local ring with maximal ideal $\mathfrak{m}$ and residue field $\mathbf{k}$. We denote by $a \in A \mapsto \overline{a} \in \mathbf{k}$ the quotient map, and extend it to a map $A[X] \longrightarrow \mathbf{k}[X]$ by setting $\overline{\sum_i a_i \cdot X^i} = \sum \overline{a_i} \cdot X^i$.

In the sequel we consider finite algebras $B \supseteq A$. If we had a noninjective homomorphism $\varphi : A \to B$ we could consider $A_1 = \varphi(A) \subseteq B$. If B is non trivial A_1 is a nontrivial residually

discrete local ring with maximal ideal $\mathfrak{m}/\ker\varphi$ and residue field $\mathbf{k}$. So our hypothesis $B \supseteq A$ is not restrictive.

Corollary 3.5 (1) applied to the $\mathbf{k}$-algebra $B/\mathfrak{m}\cdot B$ gives the following lemma.

Lemma 3.6. *Let $B \supseteq A$ be a finite algebra over A. For all $x \in B$, there exist $s \in A[X]$ and $k \in \mathbb{N}$ such that $x^k \cdot (1 - x \cdot s(x)) \in \mathfrak{m} \cdot B$.*

Definition 3.7. *We shall say that a ring B is* pseudo-local *if $B/\mathcal{J}_B$ is zero dimensional, and* semi-local *if moreover $\mathbb{B}(B/\mathcal{J}_B)$ is bounded. If moreover B has the property of idempotent lifting, we say that B is* decomposable.

Notice that our definition of a semi-local ring is equivalent (for nontrivial rings), in classical mathematics, to the usual one.

In classical mathematics, if B is *decomposable*, since $\mathbb{B}(B/\mathcal{J}_B)$ is finite, B is isomorphic to a finite product of local rings, i.e., it is called a *decomposed ring* in Lafon&Marot.

In the following proposition it is not assumed that $B/\mathcal{J}_B$ or $B/\mathfrak{m}\cdot B$ have finite bases over $\mathbf{k}$.

Proposition 3.8. *Let $B \supseteq A$ be a finite algebra over A.*

1. *$\mathcal{J}_B = \sqrt{\mathfrak{m}\cdot B}$. So B has the property of idempotents lifting if and only if one can lift idempotents modulo $\mathfrak{m}\cdot B$.*
2. *B is a semi-local ring.*
3. *B is local if and only if $B/\mathcal{J}_B$ is local, if and only if $B/\mathfrak{m}\cdot B$ is local.*
4. *If B is local then it is residually discrete.*

Proof. (1) Let $x \in \mathfrak{m}\cdot B$. Corollary 3.3 (1) implies that $x^m + a_1x^{n-1} + \ldots + a_n = 0$, with $a_i \in \mathfrak{m}$. By Euclidean division, $x^n + a_1x^{n-1} + \ldots + a_n = 0 = (1-x)q(x) + (1 + a_1 + \cdots + a_n)$ with $1 + a_1 + \cdots + a_n \in A^\times$. So $1 - x \in B^\times$, and we are done.

Let now $x \in \mathcal{J}_B$. Lemma 3.6 implies that $x^k \in \mathfrak{m}\cdot B$.

(2) $B/\mathcal{J}_B$ is a finite $\mathbf{k}$-algebra, so it is zero dimensional and its boolean algebra of idempotents is bounded (see Corollary 3.5).

(3) A quotient of a local ring is always local. Let $C = B/\mathfrak{m}\cdot B$, then $B/\mathcal{J}_B = C/\sqrt[C]{0}$, so B and C are simultaneously local. $B/\mathcal{J}_B$ is a finite $\mathbf{k}$-algebra, so if $B/\mathcal{J}_B$ is local, Corollary 3.5 (2) and (4) shows that every element of B is in $\mathcal{J}_B$ or invertible modulo $\mathcal{J}_B$. This implies that B is a local ring, and if it is nontrivial, it is residually discrete. □

Proposition 3.9. *Let $B \supseteq A$ be a finite algebra over A, and $C \subseteq B$ a subalgebra of B. Then $\mathcal{J}_C = \mathcal{J}_B \cap C$.*

Proof. This is a particular case of Corollary 3.3 (3). □

3.3. **Finite algebras and idempotents.**

Lemma 3.10. *If $g, h \in A[X]$ are monic polynomials such that $\overline{g}$ and $\overline{h}$ are relatively prime, then there exist $u, v \in A[X]$ such that $u \cdot g + v \cdot h = 1$.*

Proof. Let $a = \mathrm{res}(g,h)$, the Sylvester resultant of g and h. Then g and h being monic, $\overline{a} = \mathrm{res}(\overline{g}, \overline{h})$. Then from the hypotheses, we have $\overline{a} \neq 0$, that is $a \in A^\times$. Now a can be written $a = u_0 \cdot g + v_0 \cdot h$, and we get the result. □

The following proposition is a reformulation of Lafon&Marot, 12.20. Our proof follows directly Lafon&Marot. It is a nice generalization of a standard result in the case where A is a discrete field.

Proposition 3.11. *Let $f \in A[X]$ monic. Let B be the finite A-algebra*

$$B = A[X]/\langle f\rangle = A[x].$$

There is a bijection between the idempotents of B, and factorizations $f = g \cdot h$ with g, h monic polynomials and $\gcd(\overline{g}, \overline{h}) = \overline{1} \in \mathbf{k}$. More precisely this bijection associates to the factor $g \in A[X]$ the idempotent $e(x) \in B$ such that $\langle g(x) \rangle = \langle e(x) \rangle$ in B.

Proof. We introduce some notations. The quotient map $A[X] \longrightarrow B = A[x]$ will be denoted by $r(X) \mapsto r(x)$. The quotient $B/\mathfrak{m} \cdot B$ is a finite $\mathbf{k}$-algebra, isomorphic to $\mathbf{k}[X]/\langle \overline{f} \rangle$. We denote by $\overline{x}$ the class of x modulo $\mathfrak{m} \cdot B$. The quotient map from B to $B/\mathfrak{m} \cdot B$ is denoted by $r(x) \mapsto \overline{r(x)} = \overline{r}(\overline{x})$. The canonical map from $\mathbf{k}[X]$ to $B/\mathfrak{m} \cdot B$ is denoted by $\overline{r}(X) \in \mathbf{k}[X] \mapsto \overline{r(x)} = \overline{r}(\overline{x})$.

The situation is summed-up in the following commutative diagram:

$$\begin{array}{ccc} r = r(X) \in A[X] & \longrightarrow & r(x) \in B \\ \downarrow & & \downarrow \\ \overline{r} = \overline{r}(X) \in \mathbf{k}[X] & \longrightarrow & \overline{r}(\overline{x}) \in B/\mathfrak{m} \cdot B \end{array}$$

Let $g, h \in A[X]$ such that $f = g \cdot h$ and $\gcd(\overline{g}, \overline{h}) = \overline{1} \in \mathbf{k}$. Then thanks to Lemma 3.10, we have $u, v \in A[X]$ such that $u \cdot g + v \cdot h = 1$. Let $e = u \cdot g$; then $e - e^2 = e \cdot (1 - e) = u \cdot g \cdot v \cdot h = u \cdot v \cdot f$, and $e(x) - e(x)^2 = u(x) \cdot v(x) \cdot f(x) = 0$; $e(x)$ is an idempotent of B. Note that $g = e \cdot g + v \cdot f$ and $g(x) = e(x) \cdot g(x)$. So $\langle e, f \rangle = \langle g \rangle$ in $A[X]$, $\langle \overline{e}, \overline{f} \rangle = \langle \overline{g} \rangle$ in $\mathbf{k}[X]$ and $\langle g(x) \rangle = \langle e(x) \rangle$ in B.

Now assume that we have $e(X) \in A[X]$, such that $e(x)^2 = e(x)$.

Let g_1 and h_1 be monic polynomials such that $\overline{g_1} = \gcd(\overline{e}, \overline{f})$ and $\overline{h_1} = \gcd(\overline{1 - e}, \overline{f})$. The polynomials $\overline{e}$ and $\overline{1 - e}$ are relatively prime, and $\overline{f}$ divides $\overline{e} \cdot (\overline{1 - e})$, so $\gcd(\overline{g_1}, \overline{h_1}) = \overline{1}$ and $\overline{f} = \overline{g_1} \cdot \overline{h_1}$. Let $\deg g_1 = n$, $\deg h_1 = m$; we have $\deg f = n + m$.

Since $\langle \overline{g_1} \rangle = \langle \overline{e}, \overline{f} \rangle$, we get $\langle \overline{g_1}(\overline{x}) \rangle = \langle \overline{e}(\overline{x}) \rangle$. Similarly $\langle \overline{h_1}(\overline{x}) \rangle = \langle (\overline{1 - e})(\overline{x}) \rangle$.

Now let $g_2 = e \cdot g_1$ and $h_2 = (1 - e) \cdot h_1$. We have $\overline{g_1}(\overline{x}) \in \langle \overline{e}(\overline{x}) \rangle$, and $\overline{e}(\overline{x}) \in B/\mathfrak{m} \cdot B$ is an idempotent, so that $\overline{g_2}(\overline{x}) = \overline{g_1}(\overline{x})$. In the same way, we have $\overline{h_2}(\overline{x}) = \overline{h_1}(\overline{x})$.

Let

$$u_i = X^i \cdot g_2, \quad i = 0, \ldots, m - 1$$

and

$$v_i = X^i \cdot h_2, \quad i = 0, \ldots, n - 1.$$

The determinant of $(\overline{u_0}(\overline{x}), \ldots, \overline{u_{m-1}}(\overline{x}), \overline{v_0}(\overline{x}), \ldots, \overline{v_{n-1}}(\overline{x}))$ w.r.t. the canonical basis $(\overline{1}, \overline{x}, \ldots, \overline{x}^{n+m-1})$ is invertible (the matrix is the Sylvester matrix of $\overline{g_1}(\overline{x})$ and $\overline{h_1}(\overline{x})$). So the determinant of $(u_0(x), \ldots, u_{m-1}(x), v_0(x), \ldots, v_{n-1}(x))$ w.r.t. the canonical basis $(1, x, \ldots, x^{n+m-1})$ is invertible and the family generates B as an A-module.

Let $B_1 = u_0(x) \cdot A + \cdots + u_{m-1}(x) \cdot A$ and $B_2 = v_0(x) \cdot A + \cdots + v_{n-1}(x) \cdot A$. We have $B = B_1 + B_2$. Now $g_2(x) \in \langle e(x) \rangle$, so $B_1 \subseteq \langle e(x) \rangle$, and in the same way $B_2 \subseteq \langle 1 - e(x) \rangle$. We deduce that $B_1 = \langle e(x) \rangle$ and $B_2 = \langle 1 - e(x) \rangle$.

Moreover $B_1 \subseteq \langle g_2(x) \rangle \subseteq \langle e(x) \rangle$, so $B_1 = \langle g_2(x) \rangle = \langle e(x) \rangle$. Similarly $B_2 = \langle h_2(x) \rangle = \langle 1 - e(x) \rangle$

Since $x^m \cdot g_2(x) \in \langle e(x) \rangle = B_1$ there are $a_0, \ldots, a_{m-1} \in A$ such that $x^m \cdot g_2(x) = a_0 \cdot g_2(x) + \cdots + a_{m-1} \cdot x^{m-1} \cdot g_2(x)$. Let $h(X) = X^m - \sum_{i=0}^{m-1} a_i \cdot X^i$. We have $h(x) \cdot g_2(x) = 0$. So $\overline{f} = \overline{g_1} \cdot \overline{h_1}$ divides $\overline{h} \cdot \overline{g_2} = \overline{h} \cdot \overline{g_1}$. Since $\deg(\overline{h}) = \deg(\overline{h_1})$ this implies $\overline{h} = \overline{h_1}$. Moreover, since $\langle g_2(x) \rangle = \langle e(x) \rangle$, we get $h(x) \cdot e(x) = 0$, i.e., $h(x) = (1 - e(x)) \cdot h(x)$.

In the same way we find a monic polynomial $g(X)$ of degree n, such that $g(x) \cdot h_2(x) = 0$, $g(x) = g(x) \cdot e(x)$ and $\overline{g} = \overline{g_1}$.

Then $g(x) \cdot h(x) = g(x) \cdot h(x) \cdot e(x) \cdot (1 - e(x)) = 0$ in B, so that $f(X)$ divides $g(X) \cdot h(X)$. These polynomials are monic with same degree, so $f = g \cdot h$.

Note that $\overline{g} = \overline{g_1} = \gcd(\overline{e}, \overline{f})$, which shows that the two mappings we defined between the set of idempotents and the factors of $\overline{f}$ are each other's inverse. □

Lemma 3.12. *Let $B \supseteq A$ be a finite algebra over A, and $C \subseteq B$ a subalgebra of B. If we have $e \in C$ and $h \in B$ such that $e^2 - e \in \mathfrak{m} \cdot C$, $h - e \in \mathfrak{m} \cdot B$ and $h^2 = h$, then h is in C.*

Proof. Let $C_1 = C + h \cdot C \subseteq B$. We have $h - e \in \mathcal{J}_B \cap C_1 = \mathcal{J}_{C_1}$ by Propositions 3.8 and 3.9. Since h and e are idempotent in $C_1/\mathfrak{m} \cdot C_1$, and since $\mathcal{J}_{C_1/\mathfrak{m} \cdot C_1} = \mathcal{J}_{C_1}/\mathfrak{m} \cdot C_1$, Lemma 2.3 implies that $h = e + z$ for some $z \in \mathfrak{m} \cdot C_1$. Therefore $C_1 = C + \mathfrak{m} \cdot C_1$. Moreover $\mathfrak{m} \subseteq \mathcal{J}_B \cap C = \mathcal{J}_C$ by Propositions 3.8 and 3.9. So by Nakayama's lemma, $C = C_1$. □

Remark. The preceding lemma will be used in the proof of Proposition 5.8, where it works as a substitute of Lafon&Marot, 12.23.

Lafon&Marot 12.23 is the following result: if $C \subset B$, with B integral over C and if B is decomposed (i.e., is a finite product of local rings), then so is C.

Lafon&Marot use freely (being in classical mathematics) the fact that a bounded Boolean algebra is finite. This allows to develop a theory of Henselian local rings based on the notion of decomposed rings. We did not try to develop a completely parallel development based on the notion of decomposable rings.

Since there was no need of a result as general as Lafon&Marot 12.23, we have preferred to give Lemma 3.12 with its short constructive proof.

4. Universal decomposition algebra

In this section A is a ring, not necessarily local. The material presented here will be useful later, in the case of Henselian local rings.

Definition 4.1. *In the ring $A[X_1, \dots, X_n]$, the* elementary symmetric functions *$S_1, \dots, S_n$ are defined to be*

$$S_k = S_k(X_1, \dots, X_n) = \sum_{1 \leq i_1 < \cdots < i_k \leq n} X_{i_1} \cdots X_{i_k}$$

Definition 4.2. *Let $f(T) = T^n + a_1 \cdot T^{n-1} + \cdots + a_{n-1} \cdot T + a_n \in A[T]$ a monic polynomial. The* universal decomposition algebra *of f is $D_A(f)$ defined by*

$$D_A(f) = A[X_1, \dots, X_n] \big/ \langle S_1 + a_1, S_2 - a_2, \dots, S_n + (-1)^{n-1} \cdot a_0 \rangle$$

We shall denote x_i the class of X_i in $D_A(f)$. The following result is standard.

Lemma 4.3. *The universal decomposition algebra $D_A(f)$ of $f \in A[T]$, is a free A module of rank $n!$. A basis of it is given by the power products*

$$\{x_1^{m_1} \cdots x_n^{m_n} : 0 \leq m_j \leq j - 1; j = 1, \dots, n\}$$

Let $\mathfrak{S}_n$ be the n-th permutation group. It acts on $A[X_1, \dots, X_n]$ by setting $\sigma X_i = X_{\sigma(i)}$, so $\sigma f(X_1, \dots, X_n) = f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$. We have clearly $\sigma(f \cdot g) = \sigma f \cdot \sigma g$ and $\sigma(f + g) = \sigma f + \sigma g$; if $\deg f = 0$, $\sigma f = f$.

This group action leaves the ideal $\langle S_1 + a_1, S_2 - a_2, \dots, S_n + (-1)^{n-1} \cdot a_n \rangle$ invariant, so it induces a group action of $\mathfrak{S}_n$ on $D_A(f) = A[x_1, \dots, x_n]$, so that $\sigma f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$.

The so called Theorem of Elementary Symmetric Polynomials is the following lemma.

Lemma 4.4. *If $g \in A[X_1, \dots, X_n]$ is fixed by the action of $\mathfrak{S}_n$, then $g \in A[S_1, \dots, S_n]$ (the subring generated by the elementary symmetric functions).*

In that case, the image of g in the quotient $D_A(f)$ is in A.

However when we consider the induced action in the quotient ring $D_A(f)$, it can happen that some $g \in D_A(f)$ is fixed by this action, but it is not in A, as it is shown with the following example.

Example. Let $A = \mathbb{F}_2(u)$ (here $\mathbb{F}_2$ is the Galois field with two elements), and $f(T) = T^2 - u$. Then $D_A(f) = A[X_1, X_2]/\langle X_1^2 - u, X_2 - X_1\rangle$. Then the whole $D_A(f)$ is fixed by $\mathfrak{S}_2$.

Nevertheless we have the useful following result.

Lemma 4.5. *Assume A has only 0 and 1 as idempotents, then every idempotent $e \in D_A(f)$ invariant by the action of $\mathfrak{S}_n$ belongs to A.*

Proof. Let $E \in A[X_1, \dots, X_n]$, be such that its image in $D_A(f)$ is e. By the elementary symmetric functions theorem $E^* := \prod_{\sigma\in\mathfrak{S}_n} E^\sigma \in A[S_1, \dots, S_n]$. We call e^* the image of E^* in $D_A(f)$, we get $e^* = \prod_{\sigma\in\mathfrak{S}_n} e^\sigma = e^{n!} = e$, and we are done. □

When A is discrete, so are $\mathbb{B}(A)$, $D_A(f)$ and $\mathbb{B}(D_A(f))$. Here is a more subtle result.

Lemma 4.6. *Assume $A \neq 0$ has only 0 and 1 as idempotents. Then $\mathbb{B}(D_A(f))$ is discrete.*

Proof. Let $e \in \mathbb{B}(D_A(f))$. Consider the matrix F representing the multiplication by e. Then $e = 0$ if and only if the projective module $e \cdot D_A(f)$ has constant rank 0, which is equivalent to $P_F(T) = 1$. And we know from Lemma 2.6 that $P_F(T) = T^r$ for some r. □

A similar proof shows more generally that if $\mathbb{B}(A)$ is discrete then $\mathbb{B}(D_A(f))$ is discrete.

Definition 4.7. *An idempotent in $D_A(f)$ is said to be a* Galois idempotent *when its orbit is a basic system of orthogonal idempotents.*

Lemma 4.8. *Assume A has only 0 and 1 as idempotents, and let $e \in D_A(f)$ be an idempotent. Then there exists a Galois idempotent $h \in D_A(f)$ such that e is a sum of conjugates of h.*

Proof. Thanks to Lemma 4.6 the boolean algebra $\mathbb{B}(D_A(f))$ is discrete. Let B be the boolean subalgebra of $\mathbb{B}(D_A(f))$ generated by the orbit of e under $\mathfrak{S}_n$. Since B is discrete and finitely generated we can find an indecomposable element of B. Let h_1 be such a minimal nonzero element of B. For every $g \in B$, we have $g \cdot h_1 = 0$ or h_1. In particular the orbit $h_1, \dots, h_m$ of h_1 is made of orthogonal idempotents. So the sum of this orbit is a nonzero idempotent of A, necessarily equal to 1 by Lemma 4.5. So h_1 is a Galois idempotent and for every $g \in B$, $g = \sum_{i=1}^m g \cdot h_i = \sum_{g\cdot h_i \neq 0} h_i$. □

5. Henselian Local Rings

Definition 5.1. *Let A be a local ring with maximal ideal $\mathfrak{m}$. We say that A is* Henselian *if every monic polynomial $f(X) = X^n + \cdots + a_1 \cdot X + a_0 \in A[X]$ with $a_1 \in A^\times$ and $a_0 \in \mathfrak{m}$ has a root in $\mathfrak{m}$.*

It is easy to show that if $f(X) = X^n + \cdots + a_1 \cdot X + a_0$ with $a_1 \in A^\times$ and $a_0 \in \mathfrak{m}$ has a root in $\mathfrak{m}$, then this root is unique (see Proposition 5.4).

Context. In the whole Section 5 A will be a nontrivial Henselian local ring with maximal ideal $\mathfrak{m}$ and residue field $\mathbf{k}$. We denote by $a \in A \mapsto \overline{a} \in \mathbf{k}$ the quotient map, and extend it to a map $A[X] \longrightarrow \mathbf{k}[X]$ by setting $\overline{\sum_i a_i \cdot X^i} = \sum \overline{a_i} \cdot X^i$.

Note that a nontrivial quotient ring of a Henselian local ring is also a Henselian local ring, with same residue field. So, as noticed at the beginning of Section 3.2, we can restrict our attention to A-algebras containing A.

Definition 5.1 says that it is possible to lift in the local Henselian ring a residual simple root of a monic polynomial. In this section we show that more general liftings are available in a Henselian local ring.

Paragraph 5.1 is devoted to the lifting of any residual simple root of any univariate polynomial.

In Paragraph 5.3 we prove the lifting of coprime factorizations of a monic univariate polynomial and the lifting of idempotents in finite A-algebras.

In Paragraph 5.4 we prove the lifting of coprime factorizations of any univariate polynomial.

5.1. **A first useful generalization.**

Definition 5.2. *We shall denote $A(X)$ the Nagata localization of $A[X]$, i.e., the localization with respect to the monoid of primitive polynomials (a polynomial is primitive when its coefficients generate the ideal $\langle 1\rangle$). It is well known that $A[X] \subseteq A(X)$.*

Lemma 5.3. *Let $f(X) = a_n \cdot X^n + \cdots + a_1 \cdot X + a_0$, with $a_1 \in A^\times$ and $a_0 \in \mathfrak{m}$. There exists a monic polynomial $g(X) \in A[X]$, $g(X) = X^n + \cdots + b_1 \cdot X + b_0$, with $b_1 \in A^\times$ and $b_0 \in \mathfrak{m}$, such that the following equality holds in $A(X)$:*

$$a_0 \cdot g(X) = (X+1)^n \cdot f\left(\frac{-a_0 \cdot a_1^{-1}}{X+1}\right).$$

Proof. We have

$$\begin{aligned} X^n \cdot f\left(\frac{-a_0 \cdot a_1^{-1}}{X}\right) &= a_0 \cdot \left(X^n - X^{n-1} + a_0 \cdot \sum_{j=2}^{n} (-1)^j \cdot a_j a_0^{j-2} a_1^{-j} \cdot X^{n-j}\right) \\ &= a_0 \cdot h(X) \end{aligned}$$

with

$$h(X) = X^n - X^{n-1} + a_0 \cdot \sum_{j=2}^{n} (-1)^j \cdot a_j a_0^{j-2} a_1^{-j} \cdot X^{n-j} = X^n - X^{n-1} + a_0 \cdot \ell(X)$$

We let $g(X) = h(X+1) = X^n + \cdots + b_1 \cdot X + b_0$. It is a monic polynomial, with constant term $b_0 = g(0) = h(1) = a_0 \cdot \ell(1) \in \mathfrak{m}$, and linear term $b_1 = g'(0) = h'(1) = 1 + a_0 \cdot \ell'(1) \in 1 + \mathfrak{m}$. □

Proposition 5.4. *Let $f(X) = a_n \cdot X^n + \cdots + a_1 \cdot X + a_0$, with $a_1 \in A^\times$ and $a_0 \in \mathfrak{m}$. Then f has a unique root in $\mathfrak{m}$.*

Proof. First we prove the uniqueness. Let us write $f(X+Y) = f(X) + Y(f'(X) + Y f_2(X,Y))$. If $f(a) = f(a+\mu)$ with $\mu \in m$ and $f'(\mu) \in A^\times$, we replace X by a and Y by μ and we get $b\mu = 0$ with $b \in A^\times$, so $\mu = 0$.

Let $g(X)$ be the polynomial associated to f by the previous lemma, and $\alpha \in \mathfrak{m}$ its root. Then $(1+\alpha) \in A^\times$; we put $\beta = \frac{-a_0 \cdot a_1^{-1}}{\alpha+1}$, and we have $-a_0 \cdot g(\alpha) = (\alpha+1)^n \cdot f(\beta)$, so that $f(\beta) = 0$. □

Corollary 5.5. *Let $f(X) = a_n \cdot X^n + \cdots + a_0 \in A[X]$ such that $\overline{f}(X) \in \mathbf{k}[X]$ has a simple root $a \in \mathbf{k}$. Then there exists a unique root $\alpha \in A$ of f such that $\overline{\alpha} = a$.*

Proof. Replace X by $X + \gamma$ where $\overline{\gamma} = a$ and use the previous proposition. □

5.2. **Universal decomposition algebra over a Henselian local ring.** Let $f(T) = T^n + \cdots + a_1 \cdot T + a_0 \in A[T]$ be a monic polynomial of degree n, and let $D = D_A(f) = A[x_1, \ldots, x_n]$ be its universal decomposition algebra.

It is easy to check that $D/\mathfrak{m} \cdot D$ is (isomorphic to) $D_{\mathbf{k}}(\overline{f})$. The permutation group $\mathfrak{S}_n$ acts both on D and $D/\mathfrak{m} \cdot D$.

For every $r(\mathbf{X}) = r(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]$ we denote by $r(\mathbf{x}) = r(x_1, \ldots, x_n)$ its image in $A[x_1, \ldots, x_n] = D$, and its image under the quotient map $D \longrightarrow D/\mathfrak{m} \cdot D$ is $\overline{r(\mathbf{x})} = \overline{r}(\overline{\mathbf{x}})$. The canonical map from $\mathbf{k}[\mathbf{X}] = \mathbf{k}[X_1, \ldots, X_n]$ to $D/\mathfrak{m} \cdot D$ is denoted by $\overline{r}(\mathbf{X}) \mapsto \overline{r(\mathbf{x})} = \overline{r}(\overline{\mathbf{x}})$.

The situation is summed-up by the following commutative diagram.

$$\begin{array}{ccc} r = r(\mathbf{X}) \in A[\mathbf{X}] & \longrightarrow & r(\mathbf{x}) \in D \\ \downarrow & & \downarrow \\ \overline{r} = \overline{r}(\mathbf{X}) \in \mathbf{k}[\mathbf{X}] & \longrightarrow & \overline{r(\mathbf{x})} \in D/\mathfrak{m} \cdot D \end{array}$$

In Proposition 5.7 we show that D admits lifting of idempotents modulo $\mathfrak{m} \cdot D$. This has tight connection with Lafon&Marot, 12.27., which settles that D is a finite product of local rings. The result in Lafon&Marot cannot be reached constructively, but Proposition 5.7 implies that D is decomposable, and Proposition 5.13 tells us that if $\mathbb{B}(D)$ is finite (we only know it is bounded) then D is a finite product of local rings. So we see that we will get finally good constructive versions of Lafon&Marot's result, but the general organization of the material is slightly different.

Propositions 5.6 and 5.7 give a useful constructive substitute for Lafon&Marot, 12.27. Their proofs can be seen as extracting the constructive content of the proof of Lafon&Marot.

Proposition 5.6. (lifting a Galois idempotent of $D/\mathfrak{m} \cdot D$)
Let $r(\mathbf{X}) \in A[\mathbf{X}]$ be such that $\overline{r(\mathbf{x})} \in D/\mathfrak{m} \cdot D$ is a Galois idempotent. Then there exists $e(\mathbf{X}) \in A[\mathbf{X}]$ such that $e(\mathbf{x})$ is a Galois idempotent of D with $\overline{e(\mathbf{x})} = \overline{r(\mathbf{x})}$. More precisely, if the orbit of $\overline{r(\mathbf{x})}$ is $[\overline{r(\mathbf{x})}, \sigma_2(\overline{r(\mathbf{x})}), \dots, \sigma_h(\overline{r(\mathbf{x})})]$, then the orbit of $e(\mathbf{x})$ is $[e(\mathbf{x}), \sigma_2(e(\mathbf{x})), \dots, \sigma_h(e(\mathbf{x}))]$.

Proof. By Lemma 4.6 $\mathbb{B}(D_{\mathbf{k}}(\overline{f}))$ is discrete. Let $\overline{r_1(\mathbf{x})} = \overline{r(\mathbf{x})}, \overline{r_2(\mathbf{x})}, \dots, \overline{r_h(\mathbf{x})}$ be the orbit of $\overline{r(\mathbf{x})}$ under the action of $\mathfrak{S}_n$; let $\sigma_2, \dots, \sigma_h \in \mathfrak{S}_n$ such that $\overline{r_i(\mathbf{x})} = \sigma_i \overline{r(\mathbf{x})}$.

Let $G = \mathrm{Stab}_{\mathfrak{S}_n}\left(\overline{r(\mathbf{x})}\right) = \left\{\sigma \in \mathfrak{S}_n \ : \ \sigma\overline{r(\mathbf{x})} = \overline{r(\mathbf{x})}\right\}$.

Let $c_1(\mathbf{X}) = \prod_{\sigma \in G} \sigma r(\mathbf{X})$. Then $\overline{c_1(\mathbf{x})} = \left(\overline{r_1(\mathbf{x})}\right)^{|G|} = \overline{r_1(\mathbf{x})}$.

For $i = 2, \dots, h$, let $c_i(\mathbf{X}) = \sigma_i c_1(\mathbf{X})$. We have $\overline{c_i(\mathbf{x})} = \overline{r_i(\mathbf{x})}$.

Let $P(T) = \prod_{i=1}^{h}(T - c_i(\mathbf{X})) \in A[\mathbf{X}][T]$. The coefficients of $P(T)$ are invariant under the action of $\mathfrak{S}_n$; so $P(T) \in A[S_1, \dots, S_n][T]$. We write $P(T) = R(S_1, \dots, S_n, T)$.

So let $p(T) = R(s_1, \dots, s_n, T)$, where $s_i = S_i(\mathbf{x}) = (-1)^i a_{n-i}$.

We get $p(T) = \prod_i (T - c_i(\mathbf{x})) \in A[T]$ (remember that $f(T) = T^n + \cdots + a_1 \cdot T + a_0$). Modulo $\mathfrak{m}$, we have $\overline{p}(T) = \left(T - \overline{r_1(\mathbf{x})}\right) \cdots \left(T - \overline{r_h(\mathbf{x})}\right) = T^h - T^{h-1} \in \mathbf{k}[T]$.

So $\overline{p}(T) \in \mathbf{k}[T]$ admits $1 \in \mathbf{k}$ has a simple root. We can lift it to a root $\alpha \in A$ of p, such that $\overline{\alpha} = 1$. We have $\overline{p'(\alpha)} = 1$, so that $p'(\alpha) \in A^\times$; let $\lambda \in A$ be its inverse (we have $\overline{\lambda} = 1$).

Let $e_i(\mathbf{x}) = \lambda \cdot \prod_{j \neq i}(\alpha - c_j(\mathbf{x})) \in D$.

We have, for $i \neq k$, $e_i(\mathbf{x}) \cdot e_k(\mathbf{x}) = 0$, and $\sum e_i(\mathbf{x}) = \lambda \cdot p'(\alpha) = 1$; hence $e_i(\mathbf{x})^2 = e_i(\mathbf{x})$. Moreover, $\overline{e_i(\mathbf{x})} = \prod_{j \neq i}(1 - \overline{r_j(\mathbf{x})}) = \overline{r_i(\mathbf{x})}$. □

Proposition 5.7. (lifting an arbitrary idempotent of $D/\mathfrak{m} \cdot D$)
Let $r(\mathbf{X}) \in A[\mathbf{X}]$ be such that $\overline{r(\mathbf{x})} \in D/\mathfrak{m} \cdot D$ is an idempotent. Then there exists $e(\mathbf{X}) \in A[\mathbf{X}]$ such that $e(\mathbf{x})$ is an idempotent of D with $\overline{e(\mathbf{x})} = \overline{r(\mathbf{x})}$.

Proof. Lemma 4.8 says that $\overline{r(\mathbf{x})}$ is a sum of conjugates of a Galois idempotent of $D/\mathfrak{m} \cdot D$. Proposition 5.6 allows us to lift this Galois idempotent. The corresponding sum of conjugates is an idempotent which is a lifting of $\overline{r(\mathbf{x})}$. □

5.3. **Fundamental theorems.**

Context. In Sections 5.3 and 5.4 we assume that A is residually discrete.

Proposition 5.8. *Let $f, g_0, h_0 \in A[T]$ be monic polynomials, such that $\overline{f} = \overline{g}_0 \cdot \overline{h}_0$ in $\mathbf{k}[T]$ and $\gcd(\overline{g}_0, \overline{h}_0) = 1$. Then there exist monic polynomials $g, h \in A[T]$ such that $f = g \cdot h$ and $\overline{g} = \overline{g}_0$, $\overline{h} = \overline{h}_0$. Moreover this factorization is unique.*

Proof. Let $B = A[t] = A[T]/\langle f(T) \rangle$. From Proposition 3.11 we see that it is enough to show that given an idempotent $\overline{e}(t) \in B/\mathfrak{m} \cdot B$, one can lift it to an idempotent $e'(t) \in B$.

Let $D = D_A(f)$. It is an extension ring of B. The situation is the following:

$$\begin{array}{ccccc} A & \longrightarrow & B & \longrightarrow & D \\ \downarrow & & \downarrow & & \downarrow \\ \mathbf{k} & \longrightarrow & B/\mathfrak{m}\cdot B & \longrightarrow & D/\mathfrak{m}\cdot D \end{array}$$

Thanks to Proposition 5.7 there exists an idempotent $e' \in D$ such that $e - e' \in \mathfrak{m} \cdot D$. Then Lemma 3.12 shows that $e' \in B$, and we are done.

The unicity comes from Proposition 3.11, Lemma 2.3 and Proposition 3.8 (1). □

We can now lift idempotents in all finite A-algebras. With Theorem 5.11 this is the main result of the paper.

Theorem 5.9. *Any finite A-algebra $B \supseteq A$ has the property of idempotents lifting. More precisely for any $e \in B$ such that $e^2 - e \in \mathfrak{m} \cdot B$ we can construct an idempotent $e' \in B$ such that $e - e' \in \mathfrak{m} \cdot B$.*

Remark. Since B is semi-local (Proposition 3.8 (2)), it is decomposable.

Proof. We denote by $b \in B \mapsto \overline{b} \in B/\mathfrak{m} \cdot B$ the quotient map. Using finiteness of B, we find a monic polynomial $F(T) \in A[T]$ such that $F(e) = 0$. Its image modulo $\mathfrak{m} \cdot A[T]$ is $\overline{F}(T) \in \mathbf{k}[T]$.

Now $\overline{F}(\overline{e}) = \overline{0}$ in $B/\mathfrak{m} \cdot B$ which is a finite $\mathbf{k}$-algebra, and $\overline{e}^2 = \overline{e}$.

We write $\overline{F}(T) = T^\ell \cdot (T-1)^k \cdot H(T)$ with $k, \ell \geq 0$ and H prime with T and $T-1$. If $\ell = 0$, $\overline{e}$ is invertible, so $\overline{e} = \overline{1}$ is lifted as 1. Similarly, if $k = 0$, $\overline{e} = \overline{0}$ is lifted as 0. If $\ell > 0$, $k > 0$, using Proposition 5.8, we lift the factorization to $F = a \cdot b \cdot h$, with $\overline{a} = T^\ell$, $\overline{b} = (T-1)^k$, $\overline{h} = H$. Since $T(T-1)U + HV = 1$ and $\overline{e}^2 - \overline{e} = \overline{0}$, $\overline{h(e)} = H(\overline{e})$ is invertible, so $h(e)$ is invertible, and $F(e) = 0$ implies $a(e)b(e) = 0$. Moreover $\overline{a(e)} = \overline{e}^\ell = \overline{e}$ and $\overline{b(e)} = \overline{(1-e)}^k = \overline{1} - \overline{e}$ (since $k, \ell > 0$). So $a(e) + b(e) = \mu \in 1 + \mathfrak{m} \cdot B$, which has an inverse $\nu \in 1 + \mathfrak{m} \cdot B$. Finally $\nu \cdot a(e)$ and $\nu \cdot b(e)$ are complementary idempotents with $\overline{\nu \cdot a(e)} = \overline{\nu} \cdot \overline{a(e)} = \overline{e}$. □

We have also an easy converse result (e.g., using Proposition 3.11, but a direct proof is simpler).

Proposition 5.10. *Let B be a nontrivial residually discrete local ring such that every finite B-algebra has the property of idempotents lifting. Then B is Henselian.*

We get now the basic ingredient for the construction of the strict Henselization of a residually discrete local ring.

Theorem 5.11. *Every nontrivial finite local A-algebra B is a Henselian residually discrete local ring.*

Proof. By Proposition 3.8 (4) B is residually discrete. Let C be a finite B algebra; it is a finite A-algebra as well. So by Theorem 5.9 it admits lifting of idempotents modulo $\mathfrak{m} \cdot C = (\mathfrak{m} \cdot B) \cdot C$. Hence by Proposition 5.10 B is Henselian. □

The following corollary gives some precision in a particular case.

Corollary 5.12. *Let $f(X) \in A[X]$ be a monic polynomial such that $\overline{f}(X) \in \mathbf{k}[X]$ is (a power of) an irreducible $h(X) \in \mathbf{k}[X]$. Let B be the quotient algebra $B = A[x] = A[X]/\langle f(X) \rangle$; B is a local Henselian ring with residue field $\mathbf{k}[X]/\langle h(X) \rangle$.*

Proof. By Proposition 3.8 (3) B is local, so apply Theorem 5.11. □

Here we get, within precise constructive hypotheses, the analogue of the characterization of Henselian rings in Lafon&Marot as local rings satisfying "every finite algebra is a finite product of local rings".

Proposition 5.13. *Let B be a finite algebra over A. Assume that $\mathbb{B}(B/\mathfrak{m}\cdot B)$ is finite (a priori, we only know it is bounded). Then B is a finite product of local Henselian rings.*

Proof. By Corollary 3.5 $B/\mathfrak{m}\cdot B$ is a finite product of finite local $\mathbf{k}$-algebras. We lift the idempotents by Theorem 5.9 and we conclude by Proposition 3.8 (3) and Theorem 5.11. □

5.4. **Factorization of non-monic polynomials.**

Now we turn to the case of non-monic polynomials. We want to lift a residual factorization in two coprime polynomials when one residual factor is monic. Since the polynomial we hope to factorize is not monic we cannot apply Proposition 5.8.

Lemma 5.14. *Let $f, g_0, h_0 \in A[X]$ such that $\overline{f} = \overline{g}_0 \cdot \overline{h}_0$ with $\gcd(\overline{g}_0, \overline{h}_0) = 1$ and g_0 is monic. If $f(0) \in A^\times$, then there exist $g, h \in A[X]$ with g monic, such that $f = g\cdot h$, $\overline{g} = \overline{g}_0$ and $\overline{h} = \overline{h}_0$. Moreover this factorization lifting is unique.*

Proof. If $f(X)$ is monic, this is Proposition 5.8.

If $f(X)$ is not monic, then let $d = \deg f$ and $p(X) = f(0)^{-1}\cdot X^d \cdot f(1/X)$. Let $n = \deg g_0$ and $q_0(X) = X^n \cdot g_0(1/X)$. Then $\overline{q}_0$ divides $\overline{p}$, which is monic; if we write $\overline{p} = \overline{q}_0 \cdot \overline{r}_0$, we have $\overline{r}_0(X) = X^{d-n}\overline{h}_0(1/X)$, so that $\gcd(\overline{q}_0, \overline{r}_0) = 1$. By Proposition 5.8, we find $q, r \in A[X]$ such that $p = q\cdot r$ and $\overline{q} = \overline{q}_0$.

Let $g(X) = 1/X^n \cdot q(X)$. Then $g(X)$ divides $f(X)$ and $\overline{g} = \overline{g}_0$. We let $h \in A$ be such that $f = g\cdot h$.

The unicity comes from the unicity in Proposition 5.8. □

We drop the extra-hypothesis "$f(0) \in A^\times$".

Proposition 5.15. *Let $f, g_0, h_0 \in A[X]$ such that $\overline{f} = \overline{g_0}\cdot\overline{h_0}$ with $\gcd(\overline{g_0}, \overline{h_0}) = 1$ and g_0 is monic. There exist $g, h \in A[X]$ with g monic, such that $f = g\cdot h$, $\overline{g} = \overline{g_0}$ and $\overline{h} = \overline{h_0}$. Moreover this factorization lifting is unique.*

Proof. Assume first that the discrete residual field has at least $1 + \deg \overline{f}$ elements. We have some $a \in A$ such that $f(a) \in A^\times$, so we can apply Lemma 5.14 to $f(X + a)$.

In the general case we consider the subfield $\mathbf{k}_0$ generated by the coefficients of $\overline{g_0}$ and $\overline{h_0}$. Since $\mathbf{k}$ is discrete we are able either to find an element $a \in A$ such that $f(a) \in A^\times$ or to assert that $\mathbf{k}_0$ is finite. In this case, we consider the subring A_0 generated by the coefficients of g_0 and h_0, we localize this ring at the prime $\mathfrak{m} \cap A_0$, and we consider the henselian subring $B_0 \subseteq A$ it generates. The morphism $B_0 \to A$ is local and the residue field of B_0 is $\mathbf{k}_0$. We construct two finite extensions $\mathbf{k}_1$ and $\mathbf{k}_2$ of $\mathbf{k}_0$, each one containing an element which is not a root of $\overline{f}$. Moreover $\mathbf{k}_1 \cap \mathbf{k}_2 = \mathbf{k}_0$. Let $p_i \in A_0[T_i]$ $(i = 1, 2)$ be monic polynomials such that $\mathbf{k}_i = \mathbf{k}_0[T_i]/\langle\overline{p_i}(T_i)\rangle$. Let $B_i = B_0[T_i]/\langle p_i(T_i)\rangle$. By Corollary 5.12, B_1 and B_2 are Henselian. By Lemma 5.14 we get a factorization $f(X) = g_i(X)\cdot h_i(X)$ inside each $B_i[X]$. We have

$$B_i \subset B = B_0[T_1, T_2]/\langle p_1(T_1), p_2(T_2)\rangle \simeq B_1 \otimes_{B_0} B_2,$$

which is a free B_0-module of rank $\deg(p_1)\cdot\deg(p_2)$. Inside $B[X]$ we get (by unicity in Lemma 5.14) $g_1 = g_2$ and $h_1 = h_2$, and $g_i(X), h_i(X) \in B_1[X] \cap B_2[X] = B_0[X] \subset A[X]$. □

6. Henselization and strict Henselization of a local ring

Context. In this section, A is a residually discrete local ring with maximal ideal $\mathfrak{m}$ and residual field $\mathbf{k}$.

6.1. **The Henselization.** In this section we construct the Henselization of A as a direct limit of extensions of A that are obtained by adding inductively Hensel roots of monic polynomials.

This kind of construction works for two reasons: the first one is that we are able to make a "simple" extension in a universal way. The second one is that the universal property of simple extensions allows us to give canonical isomorphisms between two "multiple" extensions. In conclusion the system of multiple extensions that we construct is an inductive system and does have a direct limit.

6.1.1. *One step.*

Definition 6.1. *Let $f(X) = X^n + \cdots + a_1 \cdot X + a_0 \in A[X]$ a monic polynomial with $a_1 \in A^\times$ and $a_0 \in \mathfrak{m}$. Then we denote by A_f the ring defined as follows: if $B = A[x] = A[X]/\langle f(X)\rangle$ (where x is the class of X in the quotient ring), let $S \subseteq B$ be the multiplicative part of B defined by*

$$S = \{g(x) \in B \ : \ g(X) \in A[X],\ g(0) \in A^\times\}.$$

Then by definition A_f is B localized in S, that is $A_f = S^{-1} \cdot B$.

We fix a polynomial $f(X) \in A[X]$ such as in the above definition.

Lemma 6.2. *The ring A_f is a residually discrete local ring. Its maximal ideal is $\mathfrak{m} \cdot A_f$. Its residual field is (canonically isomorphic to) $\mathbf{k}$. It is faithfully flat over A. In particular we can identify A with its image in A_f, and write $A \subseteq A_f$.*

Proof. Since A_f is a localization of an algebra which is a free A-module, A_f is flat over A. The elements of A_f can be written formally as fractions $r(x)/s(x)$ with $r, s \in A[X]$, $s(0) \in A^\times$, $r(x), s(x) \in B$. Consider an arbitrary $a = r(x)/s(x) \in A_f$. To prove that A_f is local and residually discrete, we show that $a \in A_f^\times$ or $a \in \mathcal{J}_{A_f}$. If $r(0) \in A^\times$, then $a \in A_f^\times$; if $r(0) \in \mathfrak{m}_A$, then consider an arbitrary $b = q(x)/s'(x) \in A_f$, we have $1 + a \cdot b = (s(x) \cdot s'(x) + r(x) \cdot q(x))/(s(x) \cdot s'(x)) = p(x)/v(x)$ and $p(0) \in A^\times$ so $1 + ab \in A_f^\times$, and we are done.

We have shown that the morphism $A \to A_f$ is local, so A_f is faithfully flat over A (see lemma 2.13) and we consider A as a subring of A_f.

We have also shown that $\mathfrak{m}_{A_f}$ is the set of $r(x)/s(x)$ with $r(0) \in \mathfrak{m}$ (in particular $\mathfrak{m} \subseteq \mathfrak{m}_{A_f}$) and $A_f^\times$ is the set of $r(x)/s(x)$ with $r(0) \in A^\times$. So in order to see that $\mathfrak{m}_{A_f} = \mathfrak{m} \cdot A_f$ it is sufficient to show that $x/1 \in \mathfrak{m} \cdot A_f$. Let

$$y = x^{n-1} + a_{n-1} \cdot x^{n-2} + \cdots + a_2 \cdot x + a_1$$

We have $y \in A_f^\times$, and $y \cdot x = -a_0$, so $x = -a_0 \cdot y^{-1} \in \mathfrak{m} \cdot A_f$.

An equality $r(x)/s(x) = q(x)/u(x) \in A_f$ means an equality

$$v(X) \cdot (s(X) \cdot q(X) - u(X) \cdot r(X)) \in \langle f(X)\rangle$$

in $A[X]$ with $v(0) \in A^\times$ and this implies that $s(0)q(0) - u(0)r(0) \in \mathfrak{m}$. We deduce that the map $A_f \ni r(x)/s(x) \mapsto \overline{r(0)/s(0)} \in \mathbf{k}$ is a well defined ring morphism. As its kernel is $\mathfrak{m}_{A_f}$ we obtain that the residual field of A_f is canonically isomorphic to $\mathbf{k}$. □

In the following, as we did at the end of the proof, we denote x for the element $x/1$ of A_f. It is a zero of f in $\mathfrak{m}_{A_f}$. But we note that $A[x/1]$ as a subring of A_f is a quotient of $B = A[x]$.

Lemma 6.3. *Let $B, \mathfrak{m}_B$ be a local ring and $\phi : A \longrightarrow B$ a local morphism. Let $f(X) = X^n + \cdots + a_1 \cdot X + a_0 \in A[X]$ be a monic polynomial with $a_1 \in A^\times$ and $a_0 \in \mathfrak{m}$.*

If $\phi(f) = X^n + \cdots + \phi(a_1)\cdot X + \phi(a_0) \in B[X]$ has a root ξ in $\mathfrak{m}_B$, then there exists a unique local morphism $\psi : A_f \longrightarrow B$ such that $\psi(x) = \xi$ and the following diagram commutes:

$$\begin{array}{ccc} A, \mathfrak{m} & \xrightarrow{\phi} & B, \mathfrak{m}_B \\ \downarrow & \nearrow_{\psi} & \\ A_f, \mathfrak{m}\cdot A_f & & \end{array}$$

Proof. A_f has been constructed exactly for this purpose. □

6.1.2. *An inductive definition.* We now define an inductive system. Let $\mathcal{S}$ be the smallest family of local rings $(B, \mathfrak{m}\cdot B)$ such that

(1) $(A, \mathfrak{m}) \in \mathcal{S}$;
(2) if $(B, \mathfrak{m}_B) \in \mathcal{S}$, $f(X) = X^n + \cdots + a_1\cdot X + a_0 \in B[X]$ with $a_1 \in B^\times$ and $a_0 \in \mathfrak{m}_B$, then $B_f, \mathfrak{m}_{B_f}$ is in $\mathcal{S}$.

Now we see that $\mathcal{S}$ is an inductive system. The ring A is canonically embedded in each local ring $(B, \mathfrak{m}_B)$ in $\mathcal{S}$, and $\mathfrak{m}_B = \mathfrak{m}\cdot B$. In a similar way, every local ring in $\mathcal{S}$ is canonically embedded in the ones which are constructed from it.

Given two elements $(B, \mathfrak{m}_B)$ and $(C, \mathfrak{m}_C)$ in $\mathcal{S}$, the first one is constructed by adding Hensel roots of successive polynomials $f_1, \ldots, f_k$ in successive extensions, the second one is constructed by adding Hensel roots of successive polynomials $g_1, \ldots, g_\ell$ in successive extensions. Now we can add successively the Hensel roots of polynomials $f_1, \ldots, f_k$ to C and add successively the Hensel roots of polynomials $g_1, \ldots, g_\ell$ to B. It is easy to see that the extension C' of C and the extension B' of B we have constructed are canonically isomorphic. So we have a filtered inductive system all of whose morphisms are injective and the inductive limit is a local ring that "contains" all the elements of $\mathcal{S}$ as subrings.

This kind of machinery always works when we have the property of "unique embedding" described in Lemma 6.3. A similar example is given by the construction of the real closure of an ordered field (see e.g., [7]).

So we can define the *Henselization* of A by

$$A^h = \varinjlim_{B\in\mathcal{S}} B.$$

We have the following theorem.

Theorem 6.4. *The ring A^h is a Henselian local ring with maximal ideal $\mathfrak{m}\cdot A_h$. If $(B, \mathfrak{m}_B)$ is a Henselian local ring and $\phi : A \longrightarrow B$ is a local morphism then there exists a unique local morphism ψ such that the following diagram commutes:*

$$\begin{array}{ccc} A, \mathfrak{m} & \xrightarrow{\phi} & B, \mathfrak{m}_B \\ \downarrow & \nearrow_{\psi} & \\ A^h, \mathfrak{m}\cdot A^h & & \end{array}$$

Proof. Induction on the family $\mathcal{S}$. □

6.2. **The strict Henselization.** A ring is called a *strict Henselian local ring* when it is local Henselian and the residue field is separably closed.

We want to construct a strict Henselian local ring associated to A satisfying a universal property similar to that given in Theorem 6.4.

We give only the sketch of the construction, which is very similar to the Henselization.

Moreover, we will assume that a separable closure of the residual field is given.

We have at the bottom the Henselization A^h of A. We need to construct a natural extension of A^h having as residual field a separable closure of $\mathbf{k}$.

6.2.1. *One step.* Using Corollary 5.12 we can make some "One step" part of the strict Henselization when we know an irreducible separable polynomial $f(T)$ in $\mathbf{k}[T]$. Consider the finite separable extension $\mathbf{k}[t] = \mathbf{k}[T]/\langle f(T)\rangle$ of $\mathbf{k}$.

If $F(U) \in A[U]$ gives $f(U)$ modulo $\mathfrak{m}$ we consider the quotient algebra $A^{(F)} = A^h[u] = A^h[U]/\langle F(U)\rangle$. By Corollary 5.12 we know that it is an Henselian local ring with residue field $\mathbf{k}[t]$. More precisely it is a universal object of this kind, as expressed in the following lemma.

Lemma 6.5. *Let $\varphi : A \to B$ be a local morphism where B is Henselian with residue field $\mathbf{l}$. Assume that $f(T)$ has a root t' in $\mathbf{l}$ through the residual map $\mathbf{k} \to \mathbf{l}$. Then there exists a unique local morphism $A^{(F)} \to B$ which maps residually t on t'.*

If $F_1 \in A[V]$ gives also $f(V)$ modulo $\mathfrak{m}$ let us call v the class of V in $A^{(F_1)}$. Lemma 6.5 implies that $A^{(F)} = A^h[u]$ and $A^{(F_1)} = A^h[v]$ are canonically isomorphic: there is a root u' of F in $A^{(F_1)}$ residually equal to t, and the isomorphism maps u on u'.

In a similar way if $x \in \mathbf{k}[z] \subseteq \mathbf{k}^{sep}$, $x = p(z)$, and $G[T]$ is a polynomial giving modulo $\mathfrak{m}$ the minimal polynomial of z we will have a canonical embedding of $A^{(F)}$ in $A^{(G)}$ if we impose the condition that $P(\zeta) - \xi \in \mathfrak{m}_{A^{(G)}}$ (here ζ is the class of T in $A^{(G)}$, and P is a polynomial giving p modulo $\mathfrak{m}$).

6.2.2. *An inductive definition.* In order to have a construction of the strict Henselization as a usual "static" object we need a *separable closure* of $\mathbf{k}$, i.e., a discrete field $\mathbf{k}^{sep}$ containing $\mathbf{k}$ with the following properties:

(1) Every element $x \in \mathbf{k}^{sep}$ is annihilated by an irreducible separable polynomial in $\mathbf{k}[T]$.
(2) Every separable polynomial in $\mathbf{k}[T]$ decomposes in linear factors over $\mathbf{k}^{sep}$.

In that case we can define the strict Henselization through a new inductive system, which is defined in a natural way from the inductive system of finite subextensions of $\mathbf{k}^{sep}$. We iterate the "one step" construction. The correctness of the glueing of the corresponding extensions of A^h is obtained through Lemma 6.5.

References

[1] M. Emilia Alonso, Teo Mora, Mario Raimondo. *A Computational Model for Algebraic Power Series.* JPAA. **77** (1992) 1–38. 2

[2] Erret Bishop, Douglas Bridges. *Constructive Analysis.* Springer-Verlag (1985). 1

[3] Douglas Bridges, Fred Richman. *Varieties of Constructive Mathematics.* London Math. Soc. LNS 97. Cambridge University Press (1987). 1

[4] David Eisenbud. *Commutative Algebra with a view toward Algebraic Geometry.* Springer Verlag (1995). 5

[5] Jean-Pierre Lafon, Jean Marot. *Algèbre Locale.* Hermann (Paris), (2002). 2

[6] Franz-Viktor Kuhlmann, Henri Lombardi. Construction du hensélisé d'un corps valué. In *Journal of Algebra,* vol. 228 (2000), pages 624–632. 2

[7] Henri Lombardi, Marie-Françoise Roy. Constructive elementary theory of ordered fields, in: *Effective Methods in Algebraic Geometry.* Eds. Mora T., Traverso C.. Birkhaüser (1991). Progress in Math. No 94 (MEGA 90), 249–262. 16

[8] Ray Mines, Fred Richman, Wim Ruitenburg. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, (1988). 1

[9] Masayochi Nagata. *Local rings.* John Wiley & Sons, New York, London (1962). 2

[10] Hervé Perdry. *Aspects constructifs de la théorie des corps valués.* Thèse doctorale. Université de Franche-Comté, Besançon, (2001). 2

[11] Hervé Perdry. *Henselian Valued Fields: A Constructive Point of View.* Mathematical Logic Quarterly. **51**(4), (2005), 400–416. 2

Contents

1. Introduction 1
2. Rings and Local Rings 2
2.1. Radicals 2
2.2. Idempotents and idempotent matrices 3
2.3. Flat and faithfully flat algebras 4
3. Finite algebras over local rings 5
3.1. Preliminaries 5
3.2. Jacobson radical of a finite algebra over a local ring 6
3.3. Finite algebras and idempotents 7
4. Universal decomposition algebra 9
5. Henselian Local Rings 10
5.1. A first useful generalization 11
5.2. Universal decomposition algebra over a Henselian local ring 11
5.3. Fundamental theorems 12
5.4. Factorization of non-monic polynomials 14
6. Henselization and strict Henselization of a local ring 15
6.1. The Henselization 15
6.2. The strict Henselization 16
References 17