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.

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]). So our theorems have all an algorithmic content. In particular if the hypotheses of the theorems are given in an explicit way, our proofs give algorithms and we get the conclusion in an explicit way.

Perhaps it is worthwhile to give some comments about “the Bishop’s style”. In the Bishop’s style, we don’t assume any constraint of the kind “explicit means Turing computable”. So our proofs work as well inside classical mathematics. It is sufficient to assume that “explicit” is a void word.

On the other hand, since we use intuitionistic logic, explicit hypotheses, with the intuitive meaning of the word explicit, give explicit conclusions, in an algorithmic way. In practice, if the hypotheses are “Turing computable”, so are the conclusions.

When we say: “Let $R$ be a ring . . . ” this means that:

1. we know how to construct canonical elements of $R$,
2. we know what is the meaning of $x =_R y$ when $x$ and $y$ are canonical elements of $R$,
3. we have given $1_R$, $0_R$, $-1_R$,
4. we know how to compute $x + y$ and $xy$, and
5. we have constructive proofs showing that the axioms of rings are satisfied by this structure.

So $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and all usual rings are rings in the constructive meaning of the word.

A set $E$ is said discrete when we have, constructively, for any $x$ and $y$ (canonical) elements 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:

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

which is considered to be not acceptable in constructive mathematics. For more details on principles of omniscience and on Brouwerian counter-examples, we refer the reader to [3, 8].

On the other hand $\mathbb{Z}$ is a discrete ring, even if for noncanonical 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 1 in the other case).

Many classical definitions have to be rewritten in a more manageable form in order to fit well in a constructive setting. E.g., a local ring is a ring $A$ such that

$$\forall x \in A, \ x \in A^\times \text{ or } (1 + x) \in A^\times.$$
Precisely, this means that for any \( x \in A \) we can either construct an \( y \) such that \( xy = 1 \), or construct an \( y \) such that \((1 + x)y = 1\), with an explicit meaning for the “or”. 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.

Naturally, if we are in classical mathematics, all constructive theorems about discrete fields apply to \( \mathbb{R} \) since it becomes discrete if we assume (LPO).

The paper heavily relies on the book of Lafon & Marot [5], Chapters 12 & 13, cited as Lafon in the sequel. Even if 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 it was a good basis on which we could construct our “algorithmic” proofs.

We prove some basic properties of Henselian local rings, including the fact that residual idempotents in a finite algebra always can be lifted to idempotents of the algebra. We end by constructions of the Henselization and of the strict Henselization of a local ring.

As algorithmic ones, our main results seem to appear for the first time in the literature.

Reader more interested in the specific case of valuation rings may consult [6], [10], [11].

1. RINGS AND LOCAL RINGS

In the whole paper, rings are commutative.

1.1. 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 \( A \). Remark 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 \( (x \in A^\times \Rightarrow \text{False}) \)”,

**Lemma 1.1.** 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 \( k = A/\mathfrak{m} \).

If \( k \) is discrete, \( A \) will be called residually discrete.

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

\[
\forall x \in A \space (x \in A^\times \text{ or } x \in \mathcal{J}_A),
\]

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 \( A \rightarrow \mathbb{R} \) is given by \( f/g \mapsto f(0)/g(0) \). This provides an example of local ring \( A \) which is neither discrete
For a commutative ring (idempotents modulo nilpotents can always be lifted) is a sophisticated rewriting of the identity (1.3 notations in constructive mathematics. A set

First remark that if an idempotent (idempotents are always isolated) injectivity comes from Lemma 1.3. 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 remark 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 \( e \oplus h \equiv (e - h)^2 \). So we are done. \( \square \)

Remark. Lemma 1.3 is a sophisticated rewriting of the identity \((e - h)^2 = (e - h)\) when \( e \) and \( h \) are idempotents.

Definition 1.4. 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 1.5. (Idempotents modulo nilpotents can always be lifted) The canonical map \( \mathbb{B}(A) \to \mathbb{B}\left(\frac{A}{\sqrt{(0)}}\right) \) is bijective.

Proof. Injectivity comes from Lemma 1.3. 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 \( (e')^2 - e' \in n^2A \). So it is sufficient to perform \( k \) times the Newton iteration \( x \mapsto 3x^2 - 2x^3 \). \( \square \)

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\(^2\)

\(^1\)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.
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 $\text{Im}(F) \otimes_A A[T]$.

**Lemma 1.6.** If $F \in A^{m \times m}$ is an idempotent matrix, let $P_F(T) := \det(\text{Id}_m + (T - 1)F) = \sum_{i=0}^m e_iT^i$. Then $\{e_0, \ldots, e_m\}$ is a basic system of orthogonal idempotents. If $P_F(T) = T^r$ the projective module $\text{Im} F$ 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 $\text{Tr}(F) = \sum_{k=0}^m kc_k$, so when $Z \subseteq A$, $\text{Im} F$ has constant rank $r$ if and only if $\text{Tr}(F) = r$.

### 1.3. Flat and faithfully flat algebras.

**Definition 1.7.** An $A$-algebra $\varphi : A \to B$ is flat if for every linear form $\alpha : A^n \to A$

\[
\alpha : \quad A^n \to A \\
(x_1, \ldots, x_n) \mapsto a_1 \cdot x_1 + \cdots + a_n \cdot x_n
\]

($\alpha$ is given by the row vector $(a_1, \ldots, a_n)$), the kernel of the image $\alpha^*$ of $\alpha$ by $\varphi$:

\[
\alpha^* : \quad B^n \to B \\
(x_1, \ldots, x_n) \mapsto \varphi(a_1) \cdot x_1 + \cdots + \varphi(a_n) \cdot x_n
\]

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

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 $\varphi$ is a flat morphism.

**Example 1.8.** 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 1.9.** 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 $\varphi$ 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 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 faithfully flatness is that the change of ring from $A$ to $B$ doesn’t add “new” solutions to linear systems.

**Definition 1.10.** 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 1.11.** A flat morphism $\varphi : A \to B$ is faithfully flat if and only if for every finitely generated ideal $a$ of $A$ we have that $1_B \in a \cdot B \Rightarrow 1_A \in a$. In case $B$ is local this means that $\varphi$ reflects the units.
Proof. The condition is clearly necessary. Let \( a = (a_1, \ldots, a_n) \) and \( c \in A \). The equation \( \alpha(x) = c \) has a solution in \( A^n \) if and only if \( a : c = \langle 1 \rangle \). Since the morphism is flat \( \varphi(a) : e \cdot B = \langle \varphi(a) : \varphi(c) \rangle \). If \( \alpha^*(y) = \varphi(c) \) has a solution in \( B^n, 1 \in \langle \varphi(a) : \varphi(c) \rangle \). So we have a finitely many \( x_j \in a : c \) such that \( 1 \in \langle (\varphi(x_j))_{j=1,...,k} \rangle_B \). If the condition holds, \( 1 \in \langle (x_j)_{j=1,...,k} \rangle_A \), so \( 1 \in (a : c) \): the morphism is faithfully flat.

Definition 1.12. A ring morphism \( \varphi \) from a local ring \((A, m_A)\) to a local ring \((B, m_B)\) is said to be local when it reflects the units.

This implies by contraposition \( \varphi(m_A) \subseteq m_B \). When \( A \) and \( B \) are residually discrete we have the converse implication: \( \varphi(m_A) \subseteq m_B \) implies that the ring morphism is local.

A particular case of lemma 1.11 is the classical following one. It works constructively thanks to the previous “good” definitions in a constructive setting.

Lemma 1.13. 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.

2. Finite algebras over local rings

An \( A \)-algebra \( B \) is finite if it is finite as \( A \)-module.

2.1. 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 2.5.

Let \( M \) be a finite module over \( A \). Let \( \phi : M \rightarrow M \) an homomorphism such that \( \phi(M) \subseteq a \cdot M \) for some ideal \( a \) of \( A \). Then we have a polynomial identity of homomorphisms,

\[
\phi^n + a_1 \cdot \phi^{n-1} + \cdots + a_n \cdot \text{Id}_M = 0
\]

where \( a_k \in a^h \) and \( n \) is the cardinality of some system of generators of \( M \).

Corollary 2.2 (Nakayama’s lemma). Let \( M \) be a finite module over a ring \( A, m \) an ideal, and \( N \subseteq M \) a submodule. Assume that

\[
M = N + m \cdot M
\]

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

Applying Lemma 2.1 to the multiplication by an element in a finite algebra, we get the following corollary.

Corollary 2.3. Let \( \varphi : A \rightarrow B \) be a finite algebra (\( B \) is an \( A \)-module generated by \( n \) elements), \( a \) an ideal of \( A \), \( A_1 = \varphi(A) \) and \( a_1 = \varphi(a) \).

1. Every \( x \in B \) is integral over \( A_1 \). If moreover, \( x \in a_1 \cdot B \) then \( f(x) = 0 \) for some \( f(X) = X^n + a_1 \cdot X^{n-1} + \cdots + a_n \) where \( a_k \in a_1^h \).

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 \( \varphi \) reflects the units. If moreover \( B \) is local and flat over \( A \) then it is faithfully flat.
We shall say that a ring $A$ is zero-dimensional if
\[ \forall x \in A \exists y \in B \exists k \in \mathbb{N}, x^k \cdot (1 - x \cdot y) = 0. \]

Now we get a constructive version of the classical structure theorem. Remark that our definition of a semi-local ring is equivalent (for nontrivial rings), in classical mathematics, to the usual one.

**Definition 2.4.** We say that a ring $B$ is zero-dimensional if
\[ \forall x \in B \exists y \in B \exists k \in \mathbb{N}, x^k \cdot (1 - x \cdot y) = 0. \]

**Corollary 2.5.** (structure theorem for finite algebras over discrete fields).
Let $B$ be a finite algebra over a discrete field $k$.

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. $J_B = \sqrt{\ker(\varphi)}$. So $B$ has the property of idempotents lifting.

3. For every $x \in B$, there exists an idempotent $e \in k[x] \subseteq B$ such that $x$ is invertible in $B[1/e] \cong B/(1-e)$ and nilpotent in $B[1/(1-e)] \cong B/(e)$.

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 $B(B)$ is nontrivial.

5. $B\langle B \rangle$ is bounded.

6. If $B\langle B \rangle$ is finite, $B$ is the product of a finite number of finite local algebras (in a unique way up to the order of factors).

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

**Context.** In Sections 2.2 and 2.3 $A$ is a nontrivial residually discrete local ring with maximal ideal $m$ and residue field $k$. We denote by $a \in A \mapsto \pi \in k$ the quotient map, and extend it to a map $A[X] \longrightarrow k[X]$ by setting $\sum_{i} a_{i} \cdot X^{i} = \sum_{i} \pi_{i} \cdot X^{i}$.

In the sequel we consider finite algebras $B \supseteq A$. If we had a noninjective homomorphism $\varphi : A \rightarrow B$ 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 $m/\ker \varphi$ and residue field $k$. So our hypothesis $B \supseteq A$ is not restrictive.

Corollary 2.5 (1) applied to the $k$-algebra $B/m \cdot B$ gives the following lemma.

**Lemma 2.6.** 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 $x^k \cdot (1 - x \cdot s(x)) \in m \cdot B$.

**Definition 2.7.** We shall say that a ring $B$ is pseudo-local if $B/J_{B}$ is zero dimensional, semi-local if moreover $B/J_{B}$ is bounded. If moreover $B$ has the property of idempotent liftings, we say that $B$ is decomposable.

Remark 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.

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

**Proposition 2.8.** 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 2.3 (1) implies that $x^m + a_1 x^{n-1} + \ldots + a_n = 0$, with $a_i \in \mathfrak{m}$. By euclidean division, $x^n = a_1 x^{n-1} + \ldots + a_n = 0 = (1 - x)q(x) + (1 + a_1 + \cdots + a_n)$ with $1 + a_1 + \cdots + a_n \in \mathbb{A}^\times$. So $1 - x \in B^\times$, and we are done.

Let now $x \in \mathcal{J}_B$. Lemma 2.6 implies that $x^k \in \mathfrak{m} \cdot B$.

(2) $B/\mathcal{J}_B$ is a finite $k$-algebra, so it is zero dimensional and its boolean algebra of idempotents is bounded (see Corollary 2.5).

(3) A quotient of a local ring is always local. Let $C = B/\mathfrak{m} \cdot B$, then $B/\mathcal{J}_B = C/\sqrt{0}$, so $B$ and $C$ are simultaneously local. $B/\mathcal{J}_B$ is a finite $k$-algebra, so if $B/\mathcal{J}_B$ is local, Corollary 2.5 (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 2.9.** 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 2.3 (3). □

### 2.3. Finite algebras and idempotents.

**Lemma 2.10.** 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 $a = \text{res}(g, h)$, the Sylvester resultant of $f$ and $g$. Then $g$ and $h$ being monic, $\overline{a} = \text{res}(\overline{g}, \overline{h})$. Then from the hypotheses, we have $\overline{a} \neq 0$, that is $a \in \mathbb{A}^\times$. Now $a$ can be written $a = u_0 \cdot f + v_0 \cdot g$, and we get the result. □

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

**Proposition 2.11.** Let $f \in A[X]$ monic. Let $B$ be the finite $A$-algebra

$$B = A[X]/(f) = A[x].$$

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

**Proof.** We introduce some notations. The quotient map $A[X] \twoheadrightarrow B = A[x]$ will be denoted by $r(X) \mapsto r(x)$. The quotient $B/\mathfrak{m} \cdot B$ is a finite $k$-algebra, isomorphic to $k[X]/(\overline{f})$. We denote by $\overline{\pi}$ 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 $k[X]$ to $B/\mathfrak{m} \cdot B$ is denoted by $\overline{\pi}(X) \in k[X] \mapsto \overline{r(x)} = \overline{r(\overline{x})}$.
The situation is summed-up in the following commutative diagram:

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

Let \(g, h \in A[X]\) such that \(f = g \cdot h\) and \(\gcd(\overline{g}, \overline{h}) = \overline{1} \in k\). Then thanks to Lemma 2.10, we have \(u, v \in A[X]\) such that \(u \cdot g + v \cdot h = 1\). Let \(e = u \cdot g\); then \(e^2 - e = e \cdot (e - 1) = u \cdot g \cdot v \cdot h = u \cdot v \cdot f\), and \(e(x)^2 - e(x) = u(x) \cdot v(x) \cdot f(x) = 0\); \(e(x)\) is an idempotent of \(B\). Note that \(g = e \cdot g + v \cdot f\) and \(g(x) = e(x) \cdot g(x)\). So \((e, f) = (g)\) in \(A[X]\), \((\tau, \overline{f}) = (\overline{g})\) in \(k[X]\) and \((g(x)) = (e(x))\) 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 \(\overline{g}_1 = \gcd(\tau, \overline{f})\) and \(\overline{h}_1 = \gcd(1 - \overline{e}, \overline{f})\). The polynomials \(\tau\) and \(1 - e\) are relatively prime, and \(\overline{f}\) divides \((1 - e)\), so \(\gcd(\overline{g}_1, \overline{h}_1) = 1\) and \(\overline{f} = \overline{g}_1 \cdot \overline{h}_1\). Let \(\deg g_1 = n\), \(\deg h_1 = m\); we have \(\deg f = n + m\).

Now let \(g_2 = e \cdot g_1\) and \(h_2 = e \cdot h_1\). We have \(\overline{g}_1(\overline{x}) = (e(\overline{x}))\), and \(\tau(\overline{x}) \in B/m \cdot B\) is an idempotent, so that \(\frac{\overline{g}_2(\overline{x})}{\overline{g}_1(\overline{x})} = \frac{\overline{h}_1(\overline{x})}{\overline{h}_1(\overline{x})}\). In the same way, we have \(\overline{h}_2(\overline{x}) = \overline{h}_1(\overline{x})\).

Let

\[
u_0 = g_2, \nu_1 = X \cdot g_2, \ldots, \nu_{m-1} = X^{m-1} \cdot g_2,
\]

and

\[
u_0 = h_2, \nu_1 = X \cdot h_2, \ldots, \nu_{n-1} = X^{n-1} \cdot h_2.
\]

The family \(\nu_0(\overline{x}), \ldots, \nu_{m-1}(\overline{x}), \nu_0(\overline{x}), \ldots, \nu_{n-1}(\overline{x})\) generates \(B/m \cdot B\) as a \(k\)-vector space. So by Nakayama’s lemma, the family \(u_0(x), \ldots, u_{m-1}(x), v_0(x), \ldots, v_{n-1}(x)\) generates \(B\) as a \(A\)-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 \(g_2(x) \in (e(x))\), so \(B_1 \subseteq (e(x))\), and in the same way \(B_2 \subseteq (1 - e(x))\). We deduce that \(B_1 = (e(x))\) and \(B_2 = (1 - e(x))\).

So \(X^m \cdot g_2(x) \in B_1\); there are \(a_0, \ldots, a_{m-1} \in A\) such that \(X^m \cdot g_2(x) = a_0 \cdot g_2(x) + \cdots + a_{m-1} \cdot g_2(x)\). Let \(h(x) = X^m - \sum_i a_i \cdot X^i\). We have \(h(x) \cdot g_2(x) = 0\).

In the same way we find a monic polynomial \(g(X)\) of degree \(n\), such that \(g(x) \cdot h_2(x) = 0\).

Then \(g(x) \cdot h(x)\) is zero 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 \(\overline{f} = \overline{g}_1 = \gcd(\tau, \overline{f})\), which shows that the two applications we defined between the set of idempotents and the factors of \(\overline{f}\) are each other inverse.

\[\square\]

Lemma 2.12. 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 \(e^2 - e \in m \cdot C\), \(h - e \in m \cdot B\) and \(h^2 = h\), then \(h\) is in \(C\).

Proof. Let \(C_1 = C + h \cdot C \subseteq B\). We have \(h - e \in J_B \cap C_1 = J_{C_1}\) by Propositions 2.8 and 2.9. Since \(h\) and \(e\) are idempotent in \(C_1/m \cdot C_1\), Lemma 1.3 implies that \(h = e + z\) for some \(z \in m \cdot C_1\). Therefore \(C_1 = C + m \cdot C_1\), and by Nakayama’s lemma, \(C = C_1\).

\[\square\]

Remark. The preceding lemma will be used in the proof of Proposition 4.8, where it works as a substitute of Lafon, 12.23.

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

Such a result is not constructive, but it has probably a good constructive substitute in the following form: if \(C \subset B\), with \(B\) integral over \(C\) and if \(B\) is decomposable, then so is \(C\).
Lafon uses freely (becing 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 12.23, we have preferred to give Lemma 2.12 with its short constructive proof.

3. 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 3.1.** In the ring $A[X_1, \ldots, X_n]$, the elementary symmetric functions $S_1, \ldots, S_n$ are defined to be

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

**Definition 3.2.** 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

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

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

**Lemma 3.3.** 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

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

Let $\mathfrak{S}_n$ be the $n$-th permutation group. It acts on $A[X_1, \ldots, X_n]$ by setting $\sigma X_i = X_{\sigma(i)}$, so $\sigma f(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$. 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 $\langle S_1 + a_1, S_2 - a_2, \ldots, S_n + (-1)^{n-1} \cdot a_n \rangle$ invariant, so it induces a group action of $\mathfrak{S}_n$ on $D_A(f) = A[x_1, \ldots, x_n]$, so that $\sigma f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$.

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

**Lemma 3.4.** If $g \in A[X_1, \ldots, X_n]$ is fixed by the action of $\mathfrak{S}_n$, then $g \in A[S_1, \ldots, S_n]$ (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 3.5.** 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 $E \in A[X_1, \ldots, X_n]$, be such that its image in $D_A(f)$ is $e$. By the elementary symmetric functions theorem $E^* := \prod_{\sigma \in \mathfrak{S}_n} E^\sigma \in A[S_1, \ldots, S_n]$. We call $e^*$ the image of $E^*$ in $D_A(f)$, we get $e^* = \prod_{\sigma \in \mathfrak{S}_n} e^\sigma = e^n \cdot e = e$, and we are done. □
When $A$ is discrete, so are $\mathcal{B}(A)$, $D_A(f)$ and $\mathcal{B}(D_A(f))$. Here is a more subtle result.

**Lemma 3.6.** Assume $A \neq 0$ has only 0 and 1 as idempotents. Then $\mathcal{B}(D_A(f))$ is discrete.

**Proof.** Let $e \in \mathcal{B}(D_A(f))$. 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 1.6 that $P_F(T) = T^r$ for some $r$.

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

**Definition 3.7.** An idempotent in $D_A(f)$ is said to be a Galois idempotent when its orbit is a basic system of orthogonal idempotents.

**Lemma 3.8.** 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 3.6 the boolean algebra $\mathcal{B}(D_A(f))$ is discrete. Let $B$ be the boolean subalgebra of $\mathcal{B}(D_A(f))$ 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 $h_1, \ldots, h_m$ 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 3.5. So $h_1$ is a Galois idempotent and for every $g \in B$, $g = \sum_{i=1}^m g \cdot h_1 = \sum_{g \cdot h_i \neq 0} h_i$. □

### 4. Henselian Local Rings

#### 4.1. Definition and first properties.

**Definition 4.1.** Let $A$ be a local ring with maximal ideal $m$. 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 $a_0 \in m$ has a root in $m$.

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 $a_0 \in m$ has a root in $m$, then this root is unique.

**Context.** In the whole Section 4 $A$ will be a nontrivial Henselian local ring with maximal ideal $m$ and residue field $k$. We denote by $a \in A \mapsto \overline{a} \in k$ the quotient map, and extend it to a map $A[X] \longrightarrow k[X]$ by setting $\sum_i a_i \cdot X^i = \sum \overline{a_i} \cdot X^i$.

Note that a nontrivial quotient ring of an Henselian local ring is also an Henselian local ring, with same residue field. So, as remarked at the beginning of Section 2.2, we can restrict our attention to $A$-algebras containing $A$.

**Definition 4.2.** 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 $(1)$). It is well known that $A[X] \subseteq A(X)$.

**Lemma 4.3.** Let $f(X) = a_n \cdot X^n + \cdots + a_1 \cdot X + a_0$, with $a_1 \in A^\times$ and $a_0 \in m$. 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 $b_0 \in m$, such that the following equality holds in $A(X)$:

$$a_0 \cdot g(X) = (X + 1)^n \cdot f \left( \frac{-a_0 \cdot a_1^{-1}}{X + 1} \right).$$
Let give a useful constructive substitute for Lafon, 12.27.

4.6 tells us that if \( f \) implies that

4.7 \( \alpha \)

We have

\[
\text{Let we see that we will get finally good constructive versions of Lafon result, but the finite (we only know it is bounded) then } D
\]

This has tight connection with Lafon, 12.27., which settles that

\[
D
\]

Proposition 4.4. Let \( f(X) = a_n \cdot X^n + \cdots + a_1 \cdot X + a_0 \) with \( a_1 \in A^x \) and \( a_0 \in m \).
Then \( f \) has a unique root in \( m \).

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

Corollary 4.5. Let \( f(X) = a_n \cdot X^n + \cdots + a_0 \in A[X] \) such that \( \overline{f}(X) \in k[X] \) has a simple root \( a \in k \). Then there exists a unique root \( \alpha \in A \) of \( f \) such that \( \overline{\alpha} = a \).

4.2. Universal decomposition algebra over an 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 \( D/m \cdot D \) is (isomorphic to) \( D_k(\overline{f}) \). The permutation group \( S_n \) acts both on \( D \) and \( D/m \cdot D \).

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

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

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

In Proposition 4.7 we show that \( D \) admits lifting of idempotents modulo \( m \cdot D \). This has tight connection with Lafon, 12.27., which settles that \( D \) is a finite product of local rings. The result in Lafon cannot be reached constructively, but Proposition 4.7 implies that \( D \) is decomposable, and Proposition 4.13 tells us that if \( \exists(D) \) 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 result, but the general organization of the material is slightly different.

Propositions 4.6 and 4.7 give a useful constructive substitute for Lafon, 12.27. Their proofs can be seen as extracting the constructive content of the proof of Lafon.

Proposition 4.6. Let \( r(X) \in A[X] \) be such that \( \overline{r(X)} \in D/m \cdot D \) is a Galois idempotent. Then there exists \( e(X) \in A[X] \) such that \( e(X) \) is an idempotent of \( D \) with \( e(X) = r(X) \).
Proof. By Lemma 3.6 \( B(D_h(f)) \) is discrete. Let \( \overline{r_1(x)} = r_1(x), r_2(x), \ldots, r_h(x) \) be the orbit of \( r(x) \) under the action of \( \mathfrak{S}_n \); let \( \sigma_2, \ldots, \sigma_h \in \mathfrak{S}_n \) such that \( r_1(x) = \sigma_1 r(x) \).

Let \( G = \text{Stab}_{\mathfrak{S}_n} (r(x)) = \{ \sigma \in \mathfrak{S}_n : \sigma r(x) = r(x) \} \).

Let \( c_1(X) = \prod_{\sigma \in G} \sigma r(X) \). Then \( c_1(X) = \overline{r_1(X)} = r_1(X) \).

For \( i = 2, \ldots, h \), let \( c_i(X) = \sigma_i c_1(X) \). We have \( c_i(X) = r_i(X) \).

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

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

We get \( p(T) = \prod_{i=1}^h (T - c_i(x)) \in A[T] \) (remember that \( f(T) = T^n + \cdots + a_n T + a_0 \).

Modulo \( m \), we have \( \overline{p(T)} = \overline{T - r_1(x)} \cdots \overline{T - r_h(x)} = T^h - T^{h-1} \in \overline{k(T)} \).

So \( \overline{p(T)} \in k[T] \) admits a root \( \alpha \in A \) of \( p(T) \), such that \( \overline{\alpha} = 1 \). We have \( \overline{p'(\alpha)} = 1 \), so that \( p'(\alpha) \in A^* \); let \( \lambda \in A \) be its inverse (we have \( \overline{\lambda} = 1 \).

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

We have, for \( i \neq k \), \( c_i(x) \cdot c_k(x) = 0 \), and \( \sum c_i(x) = \lambda \cdot p'(\alpha) = 1 \); hence \( c_i(x)^2 = c_i(x) \). Moreover, \( c_i(x) = \prod_{j \neq i} (1 - r_j(x)) = r_i(x) \). \( \square \)

**Proposition 4.7.** Let \( r(X) \in A[X] \) be such that \( \overline{r(X)} \in D/m \cdot D \) is an idempotent. Then there exists \( e(X) \in A[X] \) such that \( e(X) \) is an idempotent of \( D \) with \( e(X) = \overline{r(X)} \).

**Proof.** This is a simple consequence of Lemma 3.8 and Proposition 4.6. \( \square \)

### 4.3. Fundamental theorems

**Context.** In Sections 4.3 and 4.4 we assume that \( A \) is residually discrete.

**Proposition 4.8.** Let \( f, g_0, h_0 \in A[T] \) be monic polynomials, such that \( \overline{f} = \overline{g_0} \cdot \overline{h_0} \) in \( k[T] \) and \( \gcd(\overline{g_0}, \overline{h_0}) = 1 \). Then there exist monic polynomials \( g, h \in A[T] \) such that \( f = g \cdot h \mod \overline{g_0} \cdot \overline{h_0} \). Moreover this factorization is unique.

**Proof.** Let \( B = A[T] / (f(T)) \). From Proposition 2.11 we see that it is enough to show that given an idempotent \( \overline{\tau(t)} \in B/m \cdot B \), one can lift it to an idempotent \( \tau'(t) \in B \).

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

\[
\begin{array}{ccc}
A & \longrightarrow & B & \longrightarrow & D \\
\downarrow & & \downarrow & & \downarrow \\
k & \longrightarrow & B/m \cdot B & \longrightarrow & D/m \cdot D
\end{array}
\]

Thanks to Proposition 4.7 there exists an idempotent \( \epsilon' \in D \) such that \( e - \epsilon' \in m \cdot D \). Then Lemma 2.12 shows that \( \epsilon' \in B \), and we are done.

The unicity comes from Proposition 2.11, Lemma 1.3 and Proposition 2.8 (1). \( \square \)

We can now lift idempotents in all finite \( A \)-algebras. With Theorem 4.11 this is the main result of the paper.

**Theorem 4.9.** Any finite \( A \)-algebra \( B \supseteq A \) has the property of idempotents lifting. More precisely for any \( e \in B \) such that \( e^2 - e \in m \cdot B \) we can construct an idempotent \( \epsilon' \in B \) such that \( e - \epsilon' \in m \cdot B \).

NB: Since \( B \) is semi-local (Proposition 2.8 (2)), it is decomposable.
Proof. We denote by \( b \in B \mapsto \overline{b} \in B/m \cdot B \) 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 \( m \cdot A[T] \) is \( \overline{F}(T) \in k[T] \).

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

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 \( \ell = 0, \overline{\sigma} \) is invertible, so \( \overline{\tau} = \overline{1} \) is lifted as 1. Similarly, if \( k = 0, \overline{\sigma} = \overline{0} \) is lifted as 0. If \( \ell > 0, k > 0 \), using Proposition 4.8, we lift the factorization to \( F = a \cdot b \cdot h \), with \( \overline{\sigma} = T^\ell, \overline{b} = (T - 1)^k, \overline{H} = H(\overline{\tau}) \). Since \( T(T - 1)U + HV = 1 \) and \( \overline{\sigma^2} - \overline{\tau} = \overline{0}, \overline{b}(e) = H(\overline{\tau}) \) is invertible, so \( h(e) \) is invertible, and \( F(e) = 0 \) implies \( a(e)b(e) = 0 \). Moreover \( a(e) = \overline{\sigma^2} = \overline{\tau} \) and \( b(e) = (1 - e)^k = \overline{1} - \overline{\tau} \) (since \( k, \ell > 0 \)). So \( a(e) + b(e) = \mu \in 1 + m \cdot B \), which has an inverse \( \nu \in 1 + m \cdot B \). Finally \( \nu \cdot a(e) \) and \( \nu \cdot b(e) \) are complementary idempotents with \( \nu \cdot a(e) = \nu \cdot \overline{a(\overline{\tau})} = \overline{\sigma} = \overline{\tau} \).

We have also an easy converse result (e.g., using Proposition 2.11, but a direct proof is simpler).

**Proposition 4.10.** 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 stone for the construction of the strict Henselization of a residually discrete local ring.

**Theorem 4.11.** Every nontrivial finite local \( A \)-algebra \( B \) is an Henselian residually discrete local ring.

**Proof.** By Proposition 2.8 (4) \( B \) is residually discrete. Let \( C \) be a finite \( B \)-algebra; it is a finite \( A \)-algebra as well. So by Theorem 4.9 it admits lifting of idempotents modulo \( m \cdot C = (m \cdot B) \cdot C \). Hence by Proposition 4.10 \( B \) is Henselian.

The following corollary gives some precision in a particular case.

**Corollary 4.12.** Let \( f(X) \in A[X] \) be a monic polynomial such that \( \overline{f}(X) \in k[X] \) is (a power of) an irreducible \( h(X) \in k[X] \). Let \( B \) be the quotient algebra \( B = A[x] = A[X]/(f(X)); B \) is a local Henselian ring with residue field \( k[X]/(h(X)) \).

**Proof.** By Proposition 2.8 (3) \( B \) is local, so apply Theorem 4.11.

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

**Proposition 4.13.** Let \( B \) be a finite algebra over \( A \). Assume that \( B(B/m \cdot B) \) is finite (a priori, we only know it is bounded). Then \( B \) is a finite product of local Henselian rings.

**Proof.** By Corollary 2.5 \( B/m \cdot B \) is a finite product of finite local \( k \)-algebras. We lift the idempotents by Theorem 4.9 and we conclude by Proposition 2.8 (3) and Theorem 4.11.

4.4. 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 4.8.

**Lemma 4.14.** Let \( f, g_0, h_0 \in A[X] \) such that \( f = g_0 \cdot h_0 \) with \( \gcd(g_0, h_0) = 1 \) and \( g_0 \) is monic. If \( f(0) \in A^\times \), then there exist \( g, h \in A[X] \) with \( g \) monic, such that \( f = g \cdot h \), \( g = g_0 \) and \( h = h_0 \). Moreover this factorization lifting is unique.
Proof. If \( f(X) \) is not monic, then this is Proposition 4.8.

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 \( g_{0}(X) = X^{n} \cdot g_{0}(1/X) \). Then \( \overline{q}_{0} \) divides \( \overline{p} \), which is monic; if we write \( \overline{p} = \overline{q}_{0} \cdot \overline{r}_{0} \), we have \( \overline{r}_{0}(X) = X^{d-n} \overline{r}_{0}(1/X) \), so that \( \gcd(q_{0}, r_{0}) = 1 \). By Proposition 4.8, we find \( q, r \in A[X] \) such that \( p = q \cdot r \) and \( \overline{q} = \overline{q}_{0} \).

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

The unicity comes from the unicity in Proposition 4.8. \( \square \)

We drop the extra-hypothesis "\( f(0) \in A^{X} \)."

**Proposition 4.15.** 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 \( f(a) \in A^{X} \), so we can apply Lemma 4.14 to \( f(X+a) \).

In the general case we consider the subfield \( k_{0} \) generated by the coefficients of \( \overline{f} \) and \( \overline{h}_{0} \). Since \( k \) is discrete we are able either to find an element \( a \in A \) such that \( f(a) \in A^{X} \) or to assert that \( k_{0} \) 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 \( m \cap A_{0} \), 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 \( k_{0} \). We construct two finite extensions \( k_{1} \) and \( k_{2} \) of \( k_{0} \), each one containing an element which is not a root of \( \overline{f} \). Moreover \( k_{1} \cap k_{2} = k_{0} \). Let \( p_{i} \in A_{0}[T] \) \((i = 1, 2)\) be monic polynomials such that \( k_{i} = k_{0}[T]/(\overline{p}_{i}(T)) \). Let \( B_{i} = B_{0}[T]/(p_{i}(T)) \). By Corollary 4.12, \( B_{1} \) and \( B_{2} \) are Henselian. By Lemma 4.14 we get a factorization \( f(X) = g_{i}(X) \cdot h_{i}(X) \) inside each \( B_{i}[X] \). We have \( B_{1} \subseteq B = B_{0}[T_{1}, T_{2}]/(p_{1}(T_{1}), p_{2}(T_{2})) \simeq B_{1} \otimes_{B_{0}} B_{2} \), 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 4.14) \( g_{1} = g_{2} \) and \( h_{1} = h_{2} \), and \( g_{i}(X), h_{i}(X) \in B_{1}[X] \cap B_{2}[X] = B_{0}[X] \subset A[X] \).

\( \square \)

5. Henselization and strict Henselization of a local ring

**Context.** In this section, \( A \) is a residually discrete local ring with maximal ideal \( m \) and residual field \( k \).

5.1. The Henselization.

5.1.1. One step.

**Definition 5.1.** Let \( f(X) = X^{n} + \cdots + a_{1} \cdot X + a_{0} \in A[X] \) a monic polynomial with \( a_{1} \in A^{X} \) and \( a_{0} \in m \). Then we denote by \( A_{f} \) the ring defined as follows: if \( B = A[x] = A[X]/(f(X)) \) (where \( x \) is the class of \( X \) in the quotient ring), let \( S \subseteq B \) be the multiplicative part of \( B \) defined by \( S = \{ g(x) \in B : g(X) \in A[X], g(0) \in A^{X} \} \).

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 5.2.** The ring \( A_{f} \) is a residually discrete local ring. Its maximal ideal is \( m \cdot A_{f} \). Its residual field is (canonically isomorphic to) \( k \). 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 $a \in J_{A_f}$.

If $r(0) \in A^\times$, then $a \in A_f^\times$; if $r(0) \in m_A$, 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 $A \rightarrow A_f$ is local, so $A_f$ is faithfully flat over $A$ (see lemma 1.13) and we consider $A$ as a subring of $A_f$.

We have also shown that $m_{A_f}$ is the set of $r(x)/s(x)$ with $r(0) \in m$ (in particular $m \subseteq m_{A_f}$) and $A_f^\times$ is the set of $r(x)/s(x)$ with $r(0) \in A^\times$. So in order to see that $m_{A_f} = m \cdot A_f$ it is sufficient to show that $x/1 \in m \cdot A_f$. 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 $x = -a_0 \cdot y^{-1} \in m \cdot A_f$.

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

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

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

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 $m_{A_f}$. But we remark that $A[x/1]$ as a subring of $A_f$ is a quotient of $B = A[x]$.

Lemma 5.3. Let $B, m_B$ be a local ring and $\phi : A \rightarrow B$ 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 $a_0 \in m$.

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

\[
\begin{array}{ccc}
A, m & \xrightarrow{\phi} & B, m_B \\
\downarrow & & \downarrow \\
A_f, m \cdot A_f & \xrightarrow{\psi} & B \\
\end{array}
\]

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

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

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

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

Given two elements $(B, m_B) \in S$ and $(C, m_C) \in S$, 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 $g_1, \ldots, g_l$ 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 $g_1, \ldots, g_l$ 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 whose all morphisms are injective and the inductive limit is a local ring that “contains” all the elements of S as subrings.

This kind of machinery always works when we have the property of “unique embedding” described in Lemma 5.3. 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

\[ A^h = \lim_{\rightarrow \in B \in S} B. \]

We have the following theorem.

**Theorem 5.4.** The ring \( A^h \) is a Henselian local ring with maximal ideal \( m \cdot A^h \).

If \((B, m_B)\) is a Henselian local ring and \( \phi : A \rightarrow B \) is a local morphism then there exists a unique local morphism \( \psi \) such that the following diagram commutes:

\[
\begin{array}{ccc}
A, m & \xrightarrow{\phi} & B, m_B \\
\downarrow & & \downarrow \\
A^h, m \cdot A^h & \xrightarrow{\psi} & B^h, m_B
\end{array}
\]

**Proof.** Induction on the family \( S \). \( \square \)

5.2. **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 universal strict Henselian local ring associated to \( A \) in the same way as in Theorem 5.4.

We have at the bottom the Henselization \( A^h \) of \( A \). We need to construct a natural extensions of \( A^h \) having as residual field a separable closure of \( k \).

5.2.1. **One step.** Using Corollary 4.12 we can make some “One step” part of the strict Henselization when we know an irreducible separable polynomial \( f(T) \) in \( k[T] \). Consider the finite separable extension \( k[t] = k[T]/(f(T)) \) of \( k \).

If \( F(U) \in A[U] \) gives \( f(U) \) modulo \( m \) we consider the quotient algebra \( A^{(F)} = A^h[u] = A^h[U]/(F(U)) \). By Corollary 4.12 we know that it is an Henselian local ring with residue field \( k[t] \). More precisely it is a universal object of this kind, as expressed in the following lemma.

**Lemma 5.5.** Let \( \phi : A \rightarrow B \) be a local morphism where \( B \) is Henselian with residue field \( l \). Assume that \( f(T) \) has a root \( t' \) in \( l \) through the residual map \( k \rightarrow l \). Then there exists a unique local morphism \( A^{(F)} \rightarrow B \) which maps residually \( t \) on \( t' \).

If \( F_1 \in A[V] \) gives also \( f(V) \) modulo \( m \) let us call \( v \) the class of \( V \) in \( A^{(F_1)} \).

Lemma 5.5 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 \( x \in k[z] \subseteq k^{sep} \), \( x = p(z) \), and \( G[T] \) is a polynomial giving modulo \( m \) the minimal polynomial of \( z \) we will have a canonical embedding of \( A^{(F)} \) in \( A^{(G)} \) if we impose the condition that \( P(\zeta) - \xi \in m_{A^{(G)}} \) (here \( \zeta \) is the class of \( T \) in \( A^{(G)} \), and \( P \) is a polynomial giving \( p \) modulo \( m \)).

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

1. Every element \( x \in k^{sep} \) is annihilated by an irreducible separable polynomial in \( k[T] \).
2. Every separable polynomial in \( k[T] \) decomposes in linear factors over \( k^{sep} \).
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 $k^{sep}$. We iterate the “one step” construction. The correctness of the gluing of the corresponding extensions of $A^h$ is obtained through Lemma 5.5.

**Comments and conclusion**

In Lafon, the Henselization is constructed in a very similar way, but as a part of an inductive completion of the ring $A$, which is the inductive limit of the family of rings obtained by taking the completion of Noetherian subrings of $A$. This is a natural object, but it is a bit difficult to control it from the constructive point of view; our construction could be considered as a simplification or an explicitation of Lafon’s one.

It should be also interesting to compare explicitly our construction to the one given by Nagata in the reference book [9].

Lots of work remain to be done to obtain a fully satisfactory constructive theory of Henselian local rings.

In particular, we were not able to prove the so-called multi-dimensional Hensel Lemma whose proof relays in the Zariski Main Theorem, which is highly non constructive. In classical mathematics, and in the geometrical setting the Henselization of a local ring $(A, m)$ coincides with the limit of the local finitely generated $A$-algebras $(A[X_1, \ldots, X_n]/(F_1, \ldots, F_n))_{m,x}$ at a non singular point $(m, x)$; this allows to represent algebraic functions (locally) and to state algorithms on standard bases (cf. [1]). This equality relays again in Zariski Main Theorem, which provides a kind of “primitive smooth element” for etale extensions.

It is also possible to investigate to which conditions the Henselization of a given local ring is discrete; properties, as normality, inherited by the Henselization remain to be investigated.

---

**References**

Contents

Introduction .......................... 1
1. Rings and Local Rings .......... 2
   1.1. Radicals ................... 2
   1.2. Idempotents and idempotent matrices ....... 3
   1.3. Flat and faithfully flat algebras ....... 4
2. Finite algebras over local rings ......... 5
   2.1. Preliminaries ......... 5
   2.2. Jacobson radical of a finite algebra over a local ring ....... 6
   2.3. Finite algebras and idempotents ....... 7
3. Universal decomposition algebra ....... 9
4. Henselian Local Rings .......... 10
   4.1. Definition and first properties ....... 10
   4.2. Universal decomposition algebra over an Henselian local ring ....... 11
   4.3. Fundamental theorems ....... 12
   4.4. Factorization of non-monic polynomials ....... 13
5. Henselization and strict Henselization of a local ring ....... 14
   5.1. The Henselization ....... 14
   5.2. The strict Henselization ....... 16
Comments and conclusion ........... 17
References .......................... 17