

Deformations and p -adic families of Galois representations.

1. Mazur's deformation functor

Let \mathcal{O} be the ring of p -adic integers of a finite unramified extension of \mathbb{Q}_p and let $k = \mathcal{O}/p\mathcal{O}$ be its residue field. We have $k = \mathbb{F}_q$ for some finite power q of p and we also sometimes write $\mathcal{O} = \mathbb{Z}_q$. We denote by \mathcal{C} the following category:

– An object of \mathcal{C} is a commutative, local, complete, noetherian \mathcal{O} -algebra A whose residue field $k_A := A/m_A$ is isomorphic to k . Here m_A denotes the maximal ideal of A .

– A morphism $f : A \rightarrow B$ in \mathcal{C} is an \mathcal{O} -algebra morphism such that $f(m_A) \subset m_B$ (*continuity property*).

Recall¹ that any object of \mathcal{C} is \mathcal{O} -isomorphic to $\mathcal{O}[[x_1, \dots, x_n]]/I$ for some n and some ideal $I \subset \mathcal{O}[[x_1, \dots, x_n]]$, and conversely. Any such ring A is then complete for its m_A -adic topology : $A \xrightarrow{\sim} \varprojlim_n A/m_A^n$, and will be viewed as a topological ring for this topology. It is even compact as k is finite.

EXAMPLE: For instance \mathcal{O} , $\mathcal{O}/p^2\mathcal{O}$, $k[[T]]$, $(\mathcal{O}/p^7\mathcal{O})[[X, Y]]/(X^2+Y)$ are objects of \mathcal{C} . Any artinian local \mathcal{O} -algebra with residue field k is an object of \mathcal{C} : they are actually the objects of \mathcal{C} which are finite as sets (as k is finite). Note that the respective m_A -adic topologies of these examples are the p -adic topology for \mathcal{O} , the T -adic topology for $k[[T]]$ and the discrete topology in the artinian case.

REMARK: (The augmentation map) The \mathcal{O} -algebra k itself is an object of \mathcal{C} . It turns out that any $A \in \mathcal{C}$ has a unique morphism to k in \mathcal{C} , called the augmentation map. Indeed, the natural map $k = \mathcal{O}/p\mathcal{O} \rightarrow k_A = A/m_A$ is necessarily an isomorphism $k \xrightarrow{\sim} k_A$, so we obtain morphism $A \rightarrow k$ as follows : map A onto k_A and goes back to k by the isomorphism above. The \mathcal{O} -linearity assumption makes this morphism unique. For the same reason, any morphism $A \rightarrow B$ in \mathcal{C} induces then the identity $k_A = k \rightarrow k_B = k$.²

DEFORMATION FUNCTORS: A deformation functor is a covariant functor $F : \mathcal{C} \rightarrow \text{Sets}$. Usually, $F(k)$ will be a singleton “the basic object over k that we want to deform”, and $F(A)$ for any A will be the set of “similar objects over A that lift $F(k)$ to A ”. The kind of objects in question may be quite various. In the beginnings of deformation theory (Kodaira-Spencer, and then Grothendieck), $F(k)$ was typically a fixed algebraic variety X_0 over k and $F(A)$ the set of isomorphism classes of families X_A of varieties parameterized by $\text{Spec}(A)$ such that $X_A \times_A k \simeq X_0$. These considerations are especially useful to study (or even show the existence of) a moduli space in the neighbourhood of a point, and even to show the existence of certain

¹We refer to Matsumura's book *Commutative ring theory* for the basics on complete local noetherian rings.

²Actually, one sometimes defines \mathcal{C} a little differently, by asking that objects of \mathcal{C} are the local complete noetherian rings A equipped with an isomorphism $k_A \xrightarrow{\sim} k$, and that a morphism $f : A \rightarrow B$ between two such objects is a ring homomorphism such that $f(m_A) \subset m_B$ and such that f induces the identity $k_A = k \rightarrow k_B = k$. These are two equivalent ways to define the same category. For instance, Hensel's lemma shows that an object of the latter category is naturally a algebra over the Witt vectors of k , i.e. of \mathcal{O} . In Grothendieck's original approach of deformation theory, one actually restricts in the definition of \mathcal{C} to the full-subcategory of the artinian objects of the category \mathcal{C} defined here.

moduli spaces (it is very useful to read the short Bourbaki seminar of Grothendieck "Géométrie formelle et géométrie algébrique").

We shall be mostly interested in the following example of deformation functor:

MAZUR'S DEFORMATION FUNCTOR : Fix G any profinite group. Fix a continuous group homomorphism

$$\bar{\rho} : G \rightarrow \mathrm{GL}_n(k).$$

Let $F_{\bar{\rho}} : \mathcal{C} \rightarrow \mathrm{Sets}$ be the covariant functor associating to any object A of \mathcal{C} the set of continuous morphisms $\rho_A : G \rightarrow \mathrm{GL}_n(A)$ taken modulo conjugation by $\mathrm{GL}_n(A)$ and such that $\rho_A \otimes_A k \simeq \bar{\rho}$. If $f : A \rightarrow B$ is a morphism in \mathcal{C} , define $F_{\bar{\rho}}(f)(\rho_A)$ as the $\mathrm{GL}_n(B)$ -conjugacy class of $\rho_A \otimes_A B$ (it only depends on the $\mathrm{GL}_n(A)$ -conjugacy class of ρ_A).

Under a weak assumption, Mazur's theorem states (see below) that $F_{\bar{\rho}}$ is representable. If R is an object of \mathcal{C} we denote by $F_R : \mathcal{C} \rightarrow \mathrm{Sets}$ the covariant functor $\mathrm{Hom}_{\mathcal{C}}(R, -)$. Recall that a covariant functor $F : \mathcal{C} \rightarrow \mathrm{Sets}$ is *representable* if there exists an object R of \mathcal{C} and an isomorphism of functors $F \xrightarrow{\sim} F_R$. Equivalently, F is representable if there exists a pair (R, x_R) where R is an object of \mathcal{C} and $x_R \in F(R)$ such that for any object A and any $x_A \in F(A)$, there is a unique morphism $f : R \rightarrow A$ in \mathcal{C} such that $F(f)(x_R) = x_A$. This pair (R, x_R) is unique up to unique isomorphism in \mathcal{C} .

We say that ρ is *absolutely irreducible* if $\rho \otimes_k \bar{k}$ is absolutely irreducible. By a classical result of Wedderburn (see e.g. Lang "Algebra" Chap. XIII), it is equivalent to ask that $k[\rho(G)] = M_n(k)$.

THEOREM 1.1. (*Mazur*) Assume $\bar{\rho}$ absolutely irreducible and that

(*G) for any open subgroup H of G then the continuous group homomorphisms $\mathrm{Hom}(H, \mathbb{F}_p)$ are finite dimensional over \mathbb{F}_p .

Then $F_{\bar{\rho}}$ is representable.

In other words, there is a ring $R(\bar{\rho}) \in \mathrm{Ob}(\mathcal{C})$ and a continuous representation $\rho^u : G \rightarrow \mathrm{GL}_n(R(\bar{\rho}))$ such that for any A in \mathcal{C} and any continuous representation $\rho_A : G \rightarrow \mathrm{GL}_n(A)$, then there is a unique morphism $R(\bar{\rho}) \rightarrow A$ in \mathcal{C} such that $\rho^u \otimes_{R(\bar{\rho})} A \simeq \rho_A$.

The ring $R(\bar{\rho})$ is called the universal deformation ring and ρ^u the universal deformation of $\bar{\rho}$. Our first aim will be to prove this theorem here. We will actually do it under the extra assumption that $p > n$ (and for complete proof mostly when $n = 2$). The original proof of Mazur in his paper "Deforming Galois representations" made use of the so-called Schlessinger representability criterion ("Functors of Artin rings" Invent. Math), which is an improvement of Grothendieck's "tautological" representability criterion : See below for these statements. There have been alternative direct proofs by D.Smit and Lenstra (see the book "Modular forms and Fermat's last theorem").

Mazur's theorem actually extends to the case where $\bar{\rho}$ is not necessarily absolutely irreducible but when we only assume that the centraliser $C(\bar{\rho})$ of $\mathrm{Im}(\bar{\rho}) \in \mathrm{GL}_n(k)$ is reduced to the scalars. We shall give another proof based on the theory of *pseudo-characters*. One draw-back is that it doesn't allow to cover the extension explained above (the assumption $p > n$ might be removed with some more work.

See the author's paper on "Determinants"). There are several advantages however : this proof is somehow more concrete than the approach via Schlessinger's criterion, pseudo-deformations makes sense when $\bar{\rho}$ is any semi-simple representation, and they also quickly lead to the the construction of the *character variety* of G called \mathcal{X} in the introduction. That are our main reasons for using this point of view here.

2. Grothendieck's criterion

Let us say a bit more about necessary conditions for a deformation functor to be representable. Remark that for any three *artinian* objects A, A', A'' in \mathcal{C} and morphisms $f : A' \rightarrow A$ and $g : A'' \rightarrow A$, we may consider their fiber product in \mathcal{C} which is

$$A' \times_A A'' = \{(a', a'') \in A' \times A'', f(a') = g(a'')\}$$

(it is a local ring with maximal ideal $m_{A'} \times_{m_A} m_{A''}$, with residue field k , obviously artinian). It is immediate to check that for any object R of \mathcal{C} , then the functor $F = F_R$ satisfies the following properties:

(G1) $F(k)$ is a singleton,

(G2) (Mayer-Vietoris) For each artinian A, A', A'' as above, the natural map $F(A' \times_A A'') \rightarrow F(A') \times_{F(A)} F(A'')$ is bijective.

(G3) (continuity) The natural map $F(A) \rightarrow \text{projlim}_{n \geq 1} F(A/m_A^n)$ is bijective.

(G4) The tangent space of F is finite dimensional (see below).

We shall go back to (G4) in a minute (it makes sense under (G1) and (G2)). It is not too difficult to see that these conditions are also sufficient for a covariant functor $F : \mathcal{C} \rightarrow \text{Sets}$ to be representable (see §A of Grothendieck "Techniques de descente et théorème d'existence en géométrie algébrique II"). Shlessinger's criterion asserts that we can weaken (G2) to the similar statement where $A \rightarrow A''$ is assumed to be surjective. It is then not too difficult to show that under the assumptions of the statement of Mazur's theorem, then $F_{\bar{\rho}}$ satisfies this criterion, hence is representable (see Mazur's paper). As we already said, we shall proceed differently and not rely on those results. Nevertheless, partial verifications of these axioms will be necessary.

Let us now go back to Mazur's deformation functor. Let G and $\bar{\rho}$ be as above. Following Mazur, define the *strict deformation functor* of $\bar{\rho}$ as follows. It is the functor

$$F'_{\bar{\rho}} : \mathcal{C} \rightarrow \text{Sets}$$

associating to any object A of \mathcal{C} the set of continuous representations $\rho_A : G \rightarrow \text{GL}_n(A)$ such that $\rho_A \bmod m_A = \bar{\rho}$ (note the $=$ rather than $\xrightarrow{\sim}$), modulo conjugation by elements in the kernel of $\text{GL}_n(A) \rightarrow \text{GL}_n(k)$ (*strict equivalence*).

Let $C(\bar{\rho}) \subset \text{GL}_n(k)$ be the subgroup whose elements commute with any element of $\bar{\rho}(G)$.

LEMMA 2.1. *If $C(\bar{\rho}) = k^\times$ is reduced to the scalars (e.g. if $\bar{\rho}$ is absolutely irreducible) then the natural morphism $F'_{\bar{\rho}} \rightarrow F_{\bar{\rho}}$ is an isomorphism. In all cases, $F'_{\bar{\rho}}$ satisfies (G1) and the Mayer-Vietoris property whenever $A = k$.*

Proof — The obvious morphism $F'_{\bar{\rho}} \rightarrow F_{\bar{\rho}}$ is $\rho_A \mapsto \rho_A$ (strict equivalence is weaker than equivalence).

Surjectivity : Let ρ_A be a lift of $\bar{\rho}$ to A , as $\mathrm{GL}_n(A) \rightarrow \mathrm{GL}_n(k)$ is surjective (for any local ring A : lift anyhow the matrix coordinates), an equivalent lift of ρ_A is a strict lift.

Injectivity : If ρ_A and ρ'_A are two strict lifts of $\bar{\rho}$ such that $\rho_A = P\rho'_A P^{-1}$ for some $P \in \mathrm{GL}_n(A)$, then $P \bmod m_A \in C(\bar{\rho})$ hence is a scalar. Let $\lambda \in A^\times$ a lift of that scalar : then $\rho_A = (P\lambda)\rho'_A(P\lambda)^{-1}$ are strictly equivalent.

It is obvious that $F'_\rho(k) = \{\bar{\rho}\}$, so (G1) holds. For the other property, let $\rho_{A'}$ and $\rho_{A''}$ be strict deformations of $\bar{\rho}$. The obvious representation

$$G \rightarrow \mathrm{GL}_n(A' \times A''), g \mapsto (\rho_{A'}(g), \rho_{A''}(g))$$

has coefficients in $A' \times_k A''$ and is a strict lift of $\bar{\rho}$: Mayer-Vietoris map is surjective. Injectivity follows immediately from the formula

$$\mathrm{GL}_n(A') \times_{\mathrm{GL}_n(k)} \mathrm{GL}_n(A'') = \mathrm{GL}_n(A' \times_k A'').$$

□

3. The tangent space of a deformation functor

Let \mathcal{V} be the category of finite-dimensional k -vector spaces and k -linear maps between them. For $V \in \mathcal{V}$ (i.e. an object of \mathcal{V} ...) we denote by

$$k[V]$$

the unique k -algebra whose underlying k -vectorspace structure is $k \oplus V$ and such that $v.v' = 0$ for all $v, v' \in V$. When $V = k$, the map $\lambda \mapsto \lambda\varepsilon$ induces a k -algebra isomorphism $k[V] \xrightarrow{\sim} k[\varepsilon]/(\varepsilon^2)$, this algebra is called the dual numbers and will be simply denoted by $k[\varepsilon]$.

LEMMA 3.1. *The functor $\mathcal{V} \rightarrow \mathcal{C}$ sending V to $k[V]$, and associating to $u \in \mathrm{Hom}_{\mathcal{V}}(V, W)$ the unique k -algebra morphism $k[V] \mapsto k[W]$ that coincides with u on V , is a fully faithful functor whose essential image is exactly the objects A such that $pA = 0$ and $m_A^2 = 0$.*

If $V, W \in \mathcal{V}$, we have a canonical isomorphism

$$k[V] \times_k k[W] = k[V \times W].$$

Proof — This is an immediate consequence of the definitions. □

We say that a covariant functor $F : \mathcal{C} \rightarrow \mathrm{Sets}$ satisfies the *tangent space property* if $F(k)$ is a singleton and if $F|_{\mathcal{V}}$ commutes with finite products : for any $V, W \in \mathcal{V}$ the natural map

$$F(k[V \times W]) \rightarrow F(k[V]) \times F(k[W])$$

is a bijection. In other words, F has to satisfy (G1) and a the very specific case of (G2) for which $A = k$ and A' and A'' are of the form $k[-]$.

PROPOSITION 3.2. *If F satisfies the tangent space property, then for any object V of \mathcal{C} , the k -vectorspace structure on V defines by applying $F(k[-])$ a k -vectorspace structure on $F(k[V])$. In this case, we define the tangent space of F as the k -vector space $F(k[\varepsilon])$.*

Proof — Let $G : \mathcal{V} \rightarrow \text{Sets}$ be any functor commuting with finite products and such that $G(0)$ is a singleton (e.g. $G = F_{|\mathcal{V}}$). For any $V \in \mathcal{V}$, the addition $V \times V \rightarrow V$ is k -linear hence defines an *addition map*

$$G(V) \times G(V) = G(V \times V) \rightarrow G(V).$$

This map is associative as so is the addition on V : consider the commutative diagram associated to the natural two factorization of $V \times V \times V \rightarrow V$, apply the functor G to it (so it remains commutative), and use twice that G commutes with finite fiber products. Using similar arguments one checks at once that this addition is an abelian group law whose 0 element is the image of the trivial morphism $G(0) \rightarrow G(V)$. Similarly, for each $\lambda \in k$, the multiplication by $\lambda : V \rightarrow V$ is k -linear hence induces a linear map $\lambda : G(V) \rightarrow G(V)$. Again, one checks at once that this endows $G(V)$ of a structure of k -vector space. \square

SCHOLIE : *The multiplication by a scalar $\lambda \in k$ on $F(k[\varepsilon])$ is induced by the morphism $k[\varepsilon] \rightarrow k[\varepsilon]$ in \mathcal{C} sending ε to $\lambda\varepsilon$. The addition in $F(k[\varepsilon])$ is induced by the morphism $k[\varepsilon] \times_k k[\varepsilon] \rightarrow k[\varepsilon]$ in \mathcal{C} sending $(\lambda\varepsilon, \lambda'\varepsilon)$ on $(\lambda + \lambda')\varepsilon$.*

Denote by $\text{ad}(\bar{\rho})$ the adjoint representation of $\bar{\rho}$, i.e. the representation on $M_n(k)$ defined by $g.X = \bar{\rho}(g)X\bar{\rho}(g)^{-1}$. The cohomology groups considered in these lectures are continuous cohomology groups.

PROPOSITION 3.3. *The strict deformation functor F'_ρ satisfies the tangent space property and there is a natural isomorphism*

$$F'_\rho(k[\varepsilon]) = H^1(G, \text{ad}(\bar{\rho})).$$

Proof — The first statement has already been proved in lemma 2.1. Fix a map $\rho : G \rightarrow \text{GL}_n(k[\varepsilon])$ whose image in $\text{GL}_n(k)$ is $\bar{\rho}$. Equivalently,

$$\rho(g) = (1 + \varepsilon\delta(g))\bar{\rho}(g)$$

where $\delta(g) \in M_n(k)$. Then ρ is a continuous group homomorphism if, and only if, δ is continuous and

$$\delta(gg') = \delta(g) + \text{ad}(\bar{\rho})(g)\delta(g'),$$

in other words iff δ is a continuous 1-cocycle of G in $\text{ad}(\bar{\rho})$. Moreover, changing ρ to $P\rho P^{-1}$ for $P = 1 + \varepsilon Q \in \text{GL}_n(k[\varepsilon])$ changes δ into $\delta'(g) = \delta(g) + Q - \text{ad}(\bar{\rho})(g)Q$, a coboundary. We have constructed a natural bijection

$$H^1(G, \text{ad}(\bar{\rho})) \rightarrow F'_\rho(k[\varepsilon]).$$

By the scholie above, the map $Z^1(G, \text{ad}(\bar{\rho})) \rightarrow F'_\rho(k[\varepsilon])$ is actually k -linear, it follows that the bijection above is k -linear as well. \square

PROPOSITION 3.4. *If $(*G)$ holds then $H^1(G, \text{ad}(\bar{\rho}))$ is finite dimensional over k .*

Proof — Indeed, let H be the kernel of $\text{ad}(\bar{\rho})$, it is a normal open subgroup of G . The inflation-restriction exact sequence writes

$$0 \rightarrow H^1(G/H, \text{ad}(\bar{\rho})) \rightarrow H^1(G, \text{ad}(\bar{\rho})) \rightarrow H^1(H, \text{ad}(\bar{\rho})) = \text{Hom}(H, \mathbb{F}_p) \otimes_{\mathbb{F}_p} \text{ad}(\bar{\rho}).$$

The left-hand side is finite dimensional as G/H is finite, the right-hand side is finite dimensional by $(*G)$. \square

Let R be a local \mathcal{O} -algebra with residue field $\simeq k$ which is *pro-artinian*. This latter condition means that there is a collection \mathcal{I} of ideals I of R such that :

- R/I is artinian for all $I \in \mathcal{I}$,
- \mathcal{I} is stable by under finite intersections, so is a directed set for the inclusion,
- the natural map $R \rightarrow \text{projlim}_{I \in \mathcal{I}} R/I$ is an isomorphism.

This last identification gives R a natural topology of profinite ring. The objects of \mathcal{C} are examples of pro-artinian rings (where \mathcal{I} is the set of all the ideals), but there are non-noetherian ones (cook some example !) that will naturally occur in the proof below of Mazur's theorem. Nevertheless, for any R as above we may still define the functor $F_R : \mathcal{C} \rightarrow \text{Sets}$ where $F_R(A)$ is the set of \mathcal{O} -algebra morphisms $f : R \rightarrow A$ which are *continuous*, i.e. such that for any $n \geq 0$ there is some $I \in \mathcal{I}$ such that $f(I) \subset m_A^n$. If R is such a ring, an elementary topological argument shows that³ for any ideal $J \subset R$, then $\bar{J} = \bigcap_{I \in \mathcal{I}} (I + J)$. We shall view m_R/\bar{m}_R^2 as a topological (profinite) k -vector space and any $V \in \mathcal{V}$ as a discrete set.

PROPOSITION 3.5. *If R is an pro-artinian local \mathcal{O} -algebra with residue field k , then F_R satisfies (G1), (G2) and (G3).*

In particular, it satisfies the tangent space property and there is a natural isomorphism of k -vector spaces $F_R(k[\varepsilon]) \xrightarrow{\sim} \text{Hom}_{\text{cont}, k\text{-linear}}(m_R/\bar{m}_R^2, k)$.

Furthermore, R is an object of \mathcal{C} if and only if $F_R(k[\varepsilon])$ is finite dimensional over k .

Proof — That F_R satisfies (G1), (G2) and (G3) is obvious from the definitions. Moreover, it follows from the definitions as well that for any $V \in \mathcal{V}$, the restriction $f \mapsto f|_{m_R}$ induces a bijection

$$F_R(k[V]) = \text{Hom}_{\text{cont}, k\text{-linear}}(m_R/\bar{m}_R^2, V).$$

But the structure of k -vector space on the left is by definition induced from the one of V and applying $F(k[-])$, so the natural bijection above (for all V) shows that both k -vector space structures coincides. The first part of the statement follows.

For the second, it is clear that if R is noetherian then m_R^2 is closed and m_R/m_R^2 is a finite dimensional k -vector space. Conversely, let $x_1, \dots, x_n \in m_R$ whose image form a k -basis of m_R/\bar{m}_R^2 and consider the natural \mathcal{O} -algebra morphism

$$\varphi : \mathcal{O}[[X_1, \dots, X_n]] \rightarrow R, \quad \varphi(X_i) = x_i.$$

For $I \in \mathcal{I}$ let φ_I be the composite of φ with $R \rightarrow R/I$. As

$$\varphi : m_R \rightarrow m_{R/I}/m_{R/I}^2 = m_R/(m_R^2 + I)$$

is surjective and factors through m_R/\bar{m}_R^2 , the $\varphi_I(X_i)$ generate $m_{R/I}/m_{R/I}^2$ over k . As $m_{R/I}$ is nilpotent in R/I , one easily checks that the $\varphi_I(X_i)$ generate the whole of R/I as an \mathcal{O} -algebra, so that φ_I is continuous and surjective. It follows that if $J = \text{Ker}(\varphi)$, the natural map

$$\mathcal{O}[[X_1, \dots, X_n]]/J \rightarrow R$$

³Indeed, $j \in \bar{J}$ if and only if a fundamental system of neighbourhood of $j \in R$ meets J . Apply this to the $j + I$ for $I \in \mathcal{I}$.

is continuous, surjective, with dense image. But the left-hand side is a compact topological space as k is finite, so this map is a homeomorphism, hence an isomorphism. \square

4. Digression : characters and pseudo-characters

ASSUMPTIONS AND CONVENTIONS: In this part $n \geq 1$ is an integer, and all the rings we consider are such that $n!$ is invertible. A will usually denote a commutative ring and R an A -algebra (associative, unital, but non necessarily commutative).

We start with an observation. Assume that $2 \in A^\times$ and consider $T : M_2(A) \rightarrow A$ the trace map. Recall the Cayley-Hamilton theorem

$$(4.1) \quad \forall x \in M_2(A), \quad x^2 - T(x)x + \frac{T(x)^2 - T(x^2)}{2} = 0.$$

Applying this identity to $x, y, x + y$ and subtracting we get the *polarized Cayley-Hamilton identity*:

$$(4.2) \quad \forall x, y \in M_2(A), \quad xy + yx - T(x)y - T(y)x + T(x)T(y) - T(xy) = 0.$$

Note that it is a symmetric, A -bilinear, identity of degree 2. As $T(xz) = 0$ for all z if and only if $x = 0$, this identity is also equivalent to

$$(4.3) \quad T(xyz) + T(yxz) - T(x)T(yz) - T(y)T(xz) + T(x)T(y)T(z) - T(xy)T(z) = 0,$$

$\forall x, y, z \in M_2(A)$ (*scalar polarized Cayley-Hamilton identity*).

Let us abstract this notion as follows. Let R be an A -algebra (with the conventions above) and let $T : R \rightarrow A$ be an A -linear map which is *central*, that is such that $T(xy) = T(yx)$ for all $x, y \in R$. For each integer $q \geq 1$, define a map $S_q(T) : R^q \rightarrow A$ by

$$S_q(T)(x) = \sum_{\sigma \in \mathfrak{S}_q} \varepsilon(\sigma) T^\sigma(x),$$

where $T^\sigma : R^q \rightarrow A$ is defined as follows. Let $x = (x_1, \dots, x_q) \in R^q$. If σ is a cycle, say (j_1, \dots, j_m) , then set $T^\sigma(x) = T(x_{j_1} \cdots x_{j_m})$, which is well defined as T is central. In general, we let $T^\sigma(x) = \prod_{i=1}^r T^{\sigma_i}(x)$, where $\sigma = \prod_{i=1}^r \sigma_i$ is the decomposition in cycles with disjoint supports of σ (including the cycles with 1 element).

For instance $S_2(T)(x, y) = T(x)T(y) - T(xy)$ and $S_3(T)(x, y, z)$ is the left-hand side of formula (4.3).

DEFINITION. *If R is an A -algebra, an A -valued pseudo-character of R of dimension n is a central A -linear map $T : R \rightarrow A$ such that $T(1) = n$ and such that $S_{n+1}(T) = 0$ on R^{n+1} .*

If G is a group, an A -valued pseudo-character of G of dimension n is a map $T : G \rightarrow A$ such that $T(1) = n$, $T(gh) = T(hg)$ for all $g, h \in G$, and such that for all $(g_1, \dots, g_{n+1}) \in G^{n+1}$ we have $S_{n+1}(T)(g_1, \dots, g_{n+1}) = 0$.

The restriction $T \mapsto T|_G$ induces a bijection between pseudocharacters of G and of $A[G]$. This definition is due to Taylor (see also Rouquier's paper on pseudo-characters). Even if we are only interested with the group theoretic case, it is often very useful to consider the ring theoretic one.

PROPOSITION 4.1. (*Frobenius, Procesi*) The trace $T : M_n(A) \rightarrow A$ is the unique pseudo-character of dimension n . The relation $S_{n+1}(T) = 0$ is the scalar polarization of the Cayley-Hamilton identity.

In particular, if $\rho : G \rightarrow \mathrm{GL}_n(A)$ is a group representation, then $\mathrm{trace}(\rho)$ is a pseudo-character of G of dimension n (characters are pseudo-characters).

Our policy in this section will be to state theorems for general n and to give complete proofs only in the special case $n = 2$ (the case $n = 1$ will always be trivial). For complete proofs along the lines of the proofs given below, see my book with Bellaïche "Families of Galois representations and Selmer groups" chapter 1.

Proof — Uniqueness: $T(E_{i,j}) = T(E_{i,j}E_{j,j}) = T(E_{j,j}E_{i,j}) = 0$ whenever $i \neq j$. Moreover, $T(E_{1,1}) = T(E_{1,1}E_{1,1}) = T(E_{1,1}E_{1,1}) = T(E_{1,1})$ for all i . So $T(1) = nT(E_{i,i}) = n$ hence $T(E_{i,i}) = 1$ for all i as $n! \in A^\times$.

For $n = 2$, the proposition is exactly the observation made above. For a general n , the fact that the trace of matrices is a pseudo-character was known to Frobenius⁴, the relation to the Cayley-Hamilton identity was found by Procesi (see Procesi "Invariants of $n \times n$ matrices", or Rouquier "Caractères et pseudo-caractères" for another approach). \square

The two main next results of this paragraph will be converse statements to this result. Obviously, pseudo-characters of dimension 1 are A -algebra homomorphisms $R \rightarrow A$ (or morphisms $G \rightarrow A^\times$). For several reasons this is not true when $n \geq 2$. However:

THEOREM 4.2. If $A = k = \bar{k}$ then $\rho \mapsto \mathrm{trace}(\rho)$ is a bijection between isomorphism classes of semi-simple representations $G \rightarrow \mathrm{GL}_n(k)$ and n -dimensional k -valued pseudo-characters on G .

If G is profinite and $k = \overline{\mathbb{F}_p}$ or $\overline{\mathbb{Q}_p}$, this bijection respects continuity on both sides.

This proposition is essentially due to Procesi (see for instance Procesi "A formal inverse to Cayley-Hamilton theorem"). In this language, it is due to Taylor when k has characteristic 0, and to Rouquier when k has characteristic $p > n$. The proof of this proposition needs a little preparation, that we shall need anyway for the other result of this section.

Faithful pseudo-characters. Let $T : R \rightarrow A$ be an n -dimensional pseudo-character. Define a 2-sided ideal of R by the formula

$$\mathrm{Ker}(T) = \{x \in R, T(xy) = 0 \forall y\}.$$

We say that T is *faithful* if $\mathrm{Ker}(T) = 0$. We check at once that an T factors through a linear map $R/\mathrm{Ker}(T) \rightarrow A$, still denoted by T , which is a faithful n -dimensional pseudocharacter of R .

Cayley-Hamilton pseudo-characters. Assume now $n = 2$. For $x \in R$, set $P_x = x^2 - T(x)x + \frac{T(x)^2 - T(x^2)}{2} \in R$. We say that T , or (R, T) , is *Cayley-Hamilton* if $P_x = 0$

⁴(From Rouquier's paper) If $\rho : G \rightarrow \mathrm{GL}_n(A)$ is a representation, then the trace of the element $(g_1 \times g_2 \times \cdots \times g_d)(\sum_{\sigma \in \mathfrak{S}_d} \varepsilon(\sigma))$ on $(A^n)^{\otimes d}$ is exactly $S_d(T)(g_1, \dots, g_n)$ (hint: reduce to the case $A = \mathbb{C}$ and $g_1 = g_2 = \cdots = g_n$ is diagonalisable in ρ). We conclude as $\Lambda_A^{n+1}(A^n) = 0$.

for all $x \in R$. Obviously, we have $P_x = \frac{1}{2}\text{CH}(x, x)$ where

$$\text{CH}(x, y) := P_{x+y} - P_x - P_y = xy + yx - T(x)y - T(y)x + T(x)T(y) - T(xy).$$

In particular, (R, T) is Cayley-Hamilton if and only if $\text{CH}(x, y) = 0$ for all $x, y \in R$. Moreover, $S_3(T)(x, y, z) = T(\text{CH}(x, y)z) = 0$ as T is a pseudo-character. In other words, if we consider the 2-sided ideal of R generated by the P_x :

$$\text{CH}(T) = \sum_{x \in R} R P_x R,$$

then $\text{CH}(T) \subset \text{Ker}(T)$. In particular, if T is faithful then (R, T) is Cayley-Hamilton. Moreover, any T factors through a pseudo-character $R/\text{CH}(T) \rightarrow A$ still denoted by T , and $(R/\text{CH}(T), T)$ is always Cayley-Hamilton.

LEMMA 4.3. *Let $T : R \rightarrow A$ be a Cayley-Hamilton pseudo-character of dimension 2. Assume that $\text{Spec}(A)$ is connected⁵ and let $e \in R$ be an idempotent, i.e. $e^2 = e$, different from 0 or 1. Then:*

- (i) $T(e) = 1$, $eRe = Ae$, and for all $x \in eRe$ we have $x = T(x)e$.
- (ii) If $(x, y, z) \in eR(1-e) \times (1-e)Re \times eR(1-e)$, then $T(xy)z = T(yz)x$.
- (iii) If there exists $x \in eR(1-e)$ and $y \in R$ such that $T(xy) \in A^\times$, then $R \simeq M_2(A)$.

Proof — The relation $S_3(T)(e, e, e) = 0$ combined with $e^2 = e$ writes $2T(e) - 3T(e)^2 + T(e)^3 = 0$, that is

$$T(e)(T(e) - 1)(T(e) - 2) = 0.$$

It is an exercise to check that as $\text{Spec}(A)$ is connected and $2 \in A^\times$ the elements $x \in A$ such that $x(x-1)(x-2) = 0$ are exactly the three distinct elements $\{0, 1, 2\}$ of A . As

$$P_e = e - T(e)e + \frac{1}{2}(T(e)^2 - T(e)) = 0,$$

we see that $T(e) = 0 \Leftrightarrow e = 0$ and $T(e) = 2 \Leftrightarrow e = 1$, so $T(e) = 1$.

Let $x \in eRe$; we have $x(1-e) = (1-e)x = 0$. The relation $\text{CH}(x, 1-e) = 0$ writes $-T(x)(1-e) - x + T(x) = 0$, that is $x = T(x)e$, which ends the proof of (i). Of course, the same statement holds if e is replaced by the idempotent $1-e$. If x, y, z are as in (ii), then $xy = T(xy)e$ and $yz = T(yz)(1-e)$ by (i), so the associativity relation $(xy)z = x(yz)$ in R implies (ii).

Let $x \in eR(1-e)$. For $y \in R$, $T(xy) = T(ex(1-e)y) = T(x(1-e)ye)$ so if (iii) holds we may assume that $y \in (1-e)Re$. Up to replacing y by ay with $a \in A^\times$ we may assume that $T(xy) = 1$. If $z \in eR(1-e)$ then (ii) shows that $z = T(yz)x \in Ax$, so $eR(1-e) = Ax$. Similarly, $(1-e)Re = Ay$. Moreover $xy \in eRe$, so $xy = T(xy)e = e$, and similarly $yx = e$. The Pierce decomposition $R = eRe \oplus (1-e)Re \oplus eR(1-e) \oplus (1-e)R(1-e)$ writes

$$R = Ae \oplus Ax \oplus Ay \oplus A(1-e)$$

as A -module. Each summand of this decomposition is free of rank 1 over A , as $T(e) = T(1-e) = 1$ and $T(xy) = 1$. It follows that the A -linear map $M_2(A) \rightarrow R$ sending $E_{1,1}$ to e , $E_{2,2}$ to $1-e$, $E_{1,2}$ to x and $E_{2,1}$ to y , is an A -algebra isomorphism. \square

⁵Recall that this means that if $f \in A$ is idempotent, then $f = 0$ or $f = 1$.

Let us finally prove Thm. 4.2. We already know that the trace of a representation of dimension n determines its semi-simplification if $n! \in k^\times$ (e.g. by the Brauer-Nesbitt theorem, the next arguments actually contains it somehow). Let k be a separably closed field with $2 \in k^\times$ and $T : G \rightarrow k$ a 2-dimensional pseudo-character. Set $R := k[G]/\text{Ker}(T)$, it is a Cayley-Hamilton k -algebra for the induced pseudo-character T , and we have the tautological group homomorphism

$$\rho : G \rightarrow R^\times$$

such that $T(g) = T(\rho(g))$ for all $g \in G$.

If $R = k.1$, then $\rho(g) = \chi(g).1$ for some character $G \rightarrow k^\times$ and $T(g) = T(\rho(g)) = 2\chi(g)$, and we are done.

Otherwise, for all $x \in R \setminus k$ we have $[k[x] : k] = 2$ by the Cayley-Hamilton identity. As k is separably closed and $2 \in k^\times$, we have either $k[x] \simeq k \times k$ or $k[x] \simeq k[\varepsilon]/(\varepsilon)^2$ for such an x . In the first case, $k[x] \subset R$ contains an idempotent $\neq 0, 1$.

Assume first that R contains an idempotent e different from $0, 1$. By the lemma we have $T(e) = 1$, $eRe = ke$ and $(1 - e)R(1 - e) = k(1 - e)$. If $eR(1 - e) = (1 - e)Re = 0$, then

$$R = eRe \oplus (1 - e)R(1 - e) \simeq k \times k$$

so $\rho(g) = (\chi(g), \chi'(g))$ for two characters $\chi, \chi' : G \rightarrow k^\times$, and $T(g) = \chi(g) + \chi'(g)$ and we are done. If say $eR(e - 1) \neq 0$, then part (iii) of the lemma above applies as T is faithful on R , it ensures that $R \simeq M_2(k)$ (and T is necessarily the trace) and we are done again.

Assume that $R \neq k$ contains no idempotent other than $0, 1$. It follows that any $x \in R$ has the form $\lambda + u$ where $\lambda \in k$ and $u^2 = 0$. For such a u , the relation $P_u = 0 = -T(u)u + T(u)^2/2$ implies that $T(u) = 0$. As a consequence, the trace 0 elements of R are exactly the elements u such that $u^2 = 0$. Fix some $u \neq 0$ in R . As T is faithful on R , we may find $v \in R$ such that $T(uv) = 1$. Replacing v by $v - T(v)/2$ we may assume that $v^2 = T(v) = 0$. But then the element $x = u + v$ satisfies $T(x^2) = 2$ (so $x \neq 0$), $T(x) = 0$ (so $x \notin k$), and $x^2 = 1$ by the Cayley-Hamilton identity, which is absurd as then $k[x] \simeq k \times k$. \square