

PSEUDOCHARACTERS
LECTURES AT THE CLAY INSTITUTE, MAY 10, 12

JOËL BELLAÏCHE

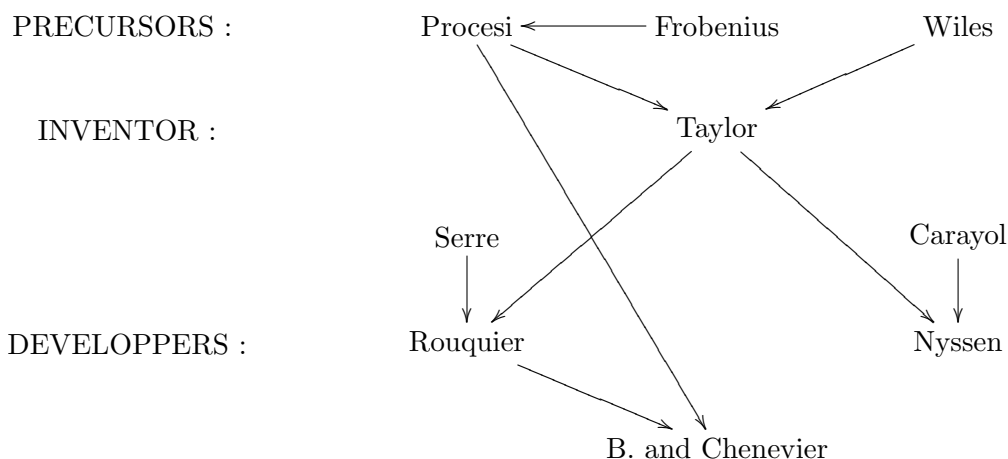
This talk is based on a joint work with Gaëtan Chenevier.

1. INTRODUCTION AND SHORT HISTORY

In all this talk, "representation" will mean a *finite dimensional* representation of a group G over a commutative ring (with unit, always) $A : \rho : G \rightarrow \mathrm{GL}_d(A)$; or, more generally, a representation of an A -algebra R (non necessarily commutative, but with unit), that is a morphism of A -algebras $\rho : R \rightarrow M_d(A)$. As it is well known, the *character* of ρ is the function $\mathrm{tr} \rho : R \rightarrow A$; when A is a field of characteristic greater than d , the character determines the semi-simplification of ρ , up to isomorphism.

A *pseudocharacter* is a function $T : R \rightarrow A$ that *looks like* the character of a representation. For the precise definition, wait and see. Pseudocharacters provide a natural generalization of the notion of representations that is easier to deal with (they are easier to glue hence they avoid rationality questions). They also provide more general notion of families/deformations of representations. As it will become clear, the usual notions are fine as long as we deal only with irreducible representations.

The aim of this talk is to review from scratch, with complete proofs, the theory of pseudocharacters and to explain in details our (that is Chenevier's and my) results on this subject. The main contributors to this theory are :



Roughly speaking, Frobenius describes what a character *looks like*. Wiles defined a (slightly less general) notion of pseudocharacter in dimension 2 case. Procesi did a lot of work on the related notion of *trace algebras*. Taylor defined pseudocharacters (he called them *pseudorepresentations* and proved that over an algebraically closed

field over, every pseudocharacter is the character of a (unique if semi-simple) representation. Rouquier and Nyssen proved the same result (independently) over a strict henselian local ring, assuming (this is very important) that the residual pseudocharacter is irreducible. The uniqueness part of their result was proved earlier by Serre and Carayol. We extend the study to reducible cases.

2. THE FORMULA OF FROBENIUS

Let $\rho : R \rightarrow M_d(A)$ be a representation and set $T = \text{tr } \rho$ its character. Obviously $T : R \rightarrow A$ satisfies

- (0) T is A -linear.
- (i) $T(1_R) = d$
- (ii) $T(xy) = T(yx)$ for all x and y in R .

Is that all ? No : Frobenius proved a remarkable identity that we now explain.

Let k be an integer. For $\underline{x} = (x_1, \dots, x_k) \in R^k$, and $\sigma \in \mathcal{G}_k$ (the permutations group on $\{1, \dots, k\}$) define $T_\sigma(\underline{x}) = T(x_{j_1} \dots x_{j_r})$ if $\sigma = (j_1, \dots, j_r)$ is a cycle of order $r \leq k$ (note that we use (ii) to see that T_σ only depends of the cycle σ) and

$$T_\sigma(\underline{x}) = \prod_{i=1}^n T_{\sigma_i}(\underline{x})$$

in general, where $\sigma = \prod_{i=1}^n \sigma_i$ is the decomposition of σ into a product of cycles with disjoint supports. Then set

$$S_k(T)(\underline{x}) := \sum_{\sigma \in S_k} \varepsilon(\sigma) T_\sigma(\underline{x})$$

Example 1.

$$S_2(T)(x, y) = T(xy) - T(x)T(y)$$

$$S_3(T)(x, y, z) = T(x)T(y)T(x) - T(x)T(yz) - T(y)T(zx) - T(z)T(xy) + T(xyz) + T(xzy)$$

Theorem 2 (Frobenius). *For any $k \geq d + 1$, we have $S_k(T) = 0$.*

Proof — (This proof is due to Rouquier.) It is obviously enough to prove this identity when $R = M_d(A)$, $\rho = \text{Id}$. It is also enough to prove it for A the universal ring of $A_{UNIV} = \mathbb{Z}[(X_{i,j,l})_{i,j \in \{1 \dots d\}, l \in \{1, \dots, k\}}]$ because if we want to prove the identity for a particular $\underline{x} = (x_1, \dots, x_k)$ in $M_d(A)^k$ for a particular ring A , then we may consider the morphism of rings $A_{univ} \rightarrow A$ that sends $X_{i,j,l}$ on the (i, j) -coefficient of the matrix x_l , and then it is clear that the identity to prove is the image by this morphism of the same identity on A_{univ} applied to the "universal" element \underline{x} of $M_d(A_{univ})^k$. Now it is enough to prove the identity in the fraction ring of A_{univ} which is a field of characteristic zero that can be embedded in \mathbb{C} , so clearly it is enough to prove the result for $A = \mathbb{C}$.

Moreover, since $S_k(T)$ is linear in each of the x_l and, symmetric, it is enough to prove by polarization that $S_k(\text{tr})(x, \dots, x) = 0$ for all $x \in M_d(\mathbb{C})$. Since this function of x is invariant by conjugation and continuous, it is enough to prove the formula for x a diagonal matrix, say $x = \text{diag}(\lambda_1, \dots, \lambda_d)$.

After those reduction steps, we set $V = \mathbb{C}^d$ and we consider the space $V^{\otimes k}$. It has a diagonal action of R (coming from the action on \mathbb{C}^d) and a permutation action of \mathcal{G}_k . Those two operations commute.

We compute the trace of the operator $x\sigma$ on this space. If we denote (e_1, \dots, e_d) the canonical basis of $V = \mathbb{C}^d$, then the $e_{i_1} \otimes \dots \otimes e_{i_k}$'s, for $i_1, \dots, i_k \in \{1, \dots, d\}$ form a basis of $V^{\otimes k}$. The image by $x\sigma$ of such an element is

$$x\sigma(e_{i_1} \otimes \dots \otimes e_{i_k}) = \prod_{j=1}^k \lambda_{i_j} e_{i_{\sigma(1)}} \otimes \dots \otimes e_{i_{\sigma(k)}}.$$

This contributes to the trace if $i_j = i_{\sigma(j)}$ for all $j = 1, \dots, k$. In other words, $j \mapsto i_j$ has to be constant on the orbits of σ , that is, on the support of the cycles $\sigma_1, \dots, \sigma_n$. For $l = 1, \dots, n$ (the number of cycle in σ) note a_l the value of any i_j for j in the support of the cycle σ_l and note c_l the order of the cycle σ_l . Then the contribution of the diagonal term corresponding to $e_{i_{\sigma(1)}} \otimes \dots \otimes e_{i_{\sigma(k)}}$ is

$$\lambda_{a_1}^{c_1} \dots \lambda_{a_n}^{c_n}.$$

The trace of $x\sigma$ is the sum of all such terms, hence :

$$\begin{aligned} \text{tr}(x\sigma) &= \sum_{a_1, \dots, a_n \in \{1, \dots, d\}} \lambda_{a_1}^{c_1} \dots \lambda_{a_n}^{c_n} \\ &= T(x^{c_1}) \dots T(x^{c_n}) \end{aligned}$$

Finally, we compute the trace of $P = \sum_{\sigma \in \mathcal{G}_k} \varepsilon(\sigma) x\sigma$. This is

$$\sum_{\sigma \in \mathcal{G}_k} \varepsilon(\sigma) T(x^{c_1(\sigma)}) \dots T(x^{c_{n(\sigma)}(\sigma)})$$

where $c_1(\sigma), \dots, c_{n(\sigma)}(\sigma)$ are the order of the cycles of σ . But this is exactly $S_k(T)(x, \dots, x)$

But clearly $P = x(\sum_{\sigma \in S_k} \varepsilon(\sigma)\sigma)$ and the right factor is the projection on the alternate elements in $V^{\otimes k}$. If $k \geq d + 1$, there is no such elements but 0, hence $P = 0$, and so is its trace of P . Hence $S_k(T)(x, \dots, x)$ \square

The proof above may not be very inspiring. Here is a sketch of a second one. Let's consider the characteristic polynomial of the matrix x . Its coefficients may be computed using universal formulas (known as Newton's formula) in terms of the values $T(1) = d, T(x), T(x^2), \dots, T(x^{d-1})$ as long as $d!$ is invertible. so we denote it $P_{x,T}(X)$. The Cayley-Hamilton theorem states that

$$P_{x,T}(x) = 0.$$

This is an equality between two matrices. If we want an equality between scalars, we may take the trace. but doing so we loose a lot of information. Instead we can multiply by a matrix y and then take the trace, getting

$$T(P_{x,T}(x)y) = 0.$$

This a scalar identity, involving traces of powers of x and of y , which is linear in y but of degree d in x . If we expand all the formulas involved, we discover that

$$S_{d+1}(T)(x, \dots, x, y) = T(P_{x,T}(x)y).$$

Hence Frobenius' formula, in the case $k = d + 1$ (the case higher k follows easily) may be seen (and proved) as the polarized form of the above relation, whose content is exactly the Cayley-Hamilton theorem.

3. DEFINITION OF PSEUDOCHARACTERS

We now assume that $d!$ is invertible in A , and that $\text{Spec } A$ is connected.

Definition 3. A *pseudocharacter* (after Rouquier) of dimension d is a function $T : R \rightarrow A$ satisfying

- (0) T is A -linear.
- (i) $T(xy) = T(yx)$ for all x and y in R .
- (ii) The number d is the smallest integer such that $S_{d+1}(T) = 0$ identically

The reader may have notice that we do not assume $T(1_R) = d$. Indeed, we will prove it

Proposition 4. For T as above, we have $T(1) = d$

Proof — We use $S_{d+1}(1, \dots, 1) = 0$. We see easily that this may be written

$$\boxed{\text{eq1}} \quad (1) \quad \sum_{n=1}^{d+1} (-1)^{d+1-n} s(d+1, n) T(1)^n = 0$$

when $s(d+1, i)$ is the number of permutations in \mathcal{G}_{d+1} with exactly n cycles.

Now you may know, especially if you already taught (or followed) a undergraduate combinatorics course that the numbers $(-1)^{d+1-n} s(d+1, n)$ are called the *Stirling number of the first kind* and that their generating polynomial satisfy

$$\sum_{n=1}^{d+1} (-1)^{d+1-n} s(d+1, n) X^n = X(X-1)(X-2) \dots (X-d)$$

If not, you may prove it easily from the recursive formula $s(d+1, k) = s(d, k-1) + (d+1)s(d, k)$ which in turns follows from elementary reasoning (count the number of permutations with k cycles where $d+1$ is a cycle on its own - they are $s(d, k-1)$ - or not) Another way to prove this is to apply $\boxed{\text{eq1}}$ to the character of the unique representation of dimension i , $i = 0, \dots, d$ of the trivial algebra $R = A$. We thus get that the polynomial above has $0, 1, 2, \dots, d$ as roots.

Anyway, we get

$$T(1)(T(1) - 1) \dots (T(1) - d),$$

so since $d!$ is invertible in A , and $\text{Spec } A$ connected, we see that $T(1)$ is constant and equal to an integer between 0 and d . Now which one is it ?

Using again the definition of $S_{d+1}(T)$, we see easily that

$$S_{d+1}(T)(x_1, \dots, x_d, 1) = (T(1) - d) S_d(T)(x_1, \dots, x_d).$$

If $T(1) \neq d$, $T(1) - d$ would be an invertible integer and $S_d(T)$ would be identically zero, which is not. So

$$T(1) = d.$$

□

Hence a T satisfying (0) and (i) of the definition, plus $S_k(T) = 0$ for some k will be a pseudocharacter, and its dimension d is the integer $T(1)$. it will satisfy $S_{d+1}(T) = 0$. This was the definition of Taylor, and we see that it is equivalent to the one of Rouquier.

A pseudocharacter of a group is a function $T : G \rightarrow A$ that satisfy (i) and (ii) of the definition above. It is obvious that such a pseudocharacter defines by linearity a pseudocharacter $T : A[G] \rightarrow A$. As Taylor remarks, If $T : G \rightarrow A$ is a pseudocharacter, and $T(G) \subset A'$, where A' is a subring of A , then obviously $T : G \rightarrow A'$ is a pseudocharacter with the same dimension. Hence, we have no descent problem for pseudocharacters !

The sum of two pseudocharacters of dimension d_1 and d_2 can be seen as being a pseudocharacter with dimension $d = d_1 + d_2$ (as long as $d!$ is invertible in A).

We may extend the scalars : If $T : R \rightarrow A$ is a pseudocharacter, and A' is a commutative A -algebra, then so is $T \otimes 1 : R \otimes A' \rightarrow A'$ defined by linearity. we shall denote it by $T \otimes A'$

4. FAITHFULL AND CAYLEY-HAMILTON PSEUDOCHARACTERS

Definition 5 (Taylor,Rouquier). The *kernel* of T is the set $\text{Ker } T$ of all $x \in R$ such that $T(xy) = 0$ for all $y \in R$. We say that T is *faithful* if $\text{Ker } T = (0)$.

By (i) of the definition, $\text{Ker } T$ is a two-sided ideal. If I is a two-sided ideal such that $I \subset \text{Ker } T$, then $T : R \rightarrow A$ factors by a linear map $R/I \rightarrow \text{Ker } T$ which is easily seen to be a pseudocharacter of kernel $\text{Ker } T/I$. We denote this pseudocharacter by T again. In particular $T : R/\text{Ker } T \rightarrow A$ is faithful.

A (serious) problem with the notion of faithfulness is that it is not stable by base change, that is $T \otimes A'$ may not be faithful if T is. (This does not happen for A' , say, finite flat over A , but this typically happen when A' is a quotient of A).

So we (we = Gaetan and me, inspired by Procesi) introduce a slightly weaker, more stable notion :

If $T : R \rightarrow A$ is a linear map satisfying $T(1) = d$, $T(xy) = T(yx)$, we can consider the polynomial $P_{x,T}(X)$, which is the unitary polynomial of degree d "whose roots are such that the sum of their i -power is $T(x^i)$, for $i = 0, \dots, d-1$ ". This does not make sense in general, but at least it does when $A = \mathbb{C}$, and actually the formula giving the coefficient of $P_{x,T}(X)$ in this cases are actually seen to be polynomial with coefficient in $Z[1/d!]$ in terms of the $T(x^i)$, allowing to define $P_{x,T}(X)$ in any case. As we saw earlier, we have the remarkable identity

$$S_{d+1}(T)(x, \dots, x, y) = T(P_{x,T}(x)y)$$

and of course both members are zero if T is a pseudocharacter of dimension d

So we see that

Proposition 6. *If T is a faithful pseudocharacter of dimension d , then $P_{x,T}(x) = 0$ for all x*

Definition 7. A pseudocharacter of dimension d is Cayley-Hamilton if $P_{x,T}(x) = 0$ for all x in R .

If $T : R \rightarrow A$ is a pseudocharacter of dimension d , we note $CH(T)$ the two-sided ideal generated by the $P_{x,T}(x)$, $x \in R$. By the above $CH(T) \subset \text{Ker } T$ and obviously,

$T : R/CH(T) \rightarrow A$ is Cayley-Hamilton. It is even the "biggest" Cayley-Hamilton quotient by which T factors (to be precise, the initial object of the category of quotient of R by which T factors as a Cayley-Hamilton pseudocharacter), whereas $R/\text{Ker } T$ is the smallest such quotient (to be precise, the final object of the same category).

The nice although obvious fact is that to be Cayley-Hamilton is stable by arbitrary base change $A \rightarrow A'$. Even more, the formation of the quotient $S/CH(T)$ is compatible with any base change. This will turn out to be crucial when defining problems of pseudodeformations.

To understand better the above notion, consider the case of a representation $\rho : R \rightarrow M_d(A)$, and set $T = \text{tr } \rho$. Then if ρ is injective ("faithful" in the language of representation theory) then T is Cayley-Hamilton (but not necessarily faithful : consider the case where R is the algebra of upper triangular matrix). If A is a field, and ρ semi-simple, $\text{Ker } T = \text{Ker } \rho$, so if ρ is injective in this case, T is faithful. In any case, if T is faithful, then ρ is injective.

5. PSEUDOCHARACTER AND IDEMPOTENTS

A simple technical tool for all what follow is the following set of results, where T is a pseudocharacter of dimension d and e an idempotent in A .

Lemma 8. *$T(e)$ is an integer between 0 and d*

Indeed if we compute $S_{d+1}(T)(e, \dots, e) = 0$ we get

$$\sum (-1)^{d+1-n} s(d+1, n) T(e)^n = 0,$$

that is $T(e)(T(e) - 1) \dots (T(e) - d) = 0$ and we conclude as for $T(1)$

Lemma 9. *The restriction T_e of T to the sub-algebra eRe (with unit e) is a pseudocharacter of dimension $T(e)$.*

Indeed, it is clear that T_e is linear and central (properties (0) and (i) of the definition) and $S_{d+1}(T_e) = 0$ obviously, so T_e is a pseudocharacter. Its dimension is its value on the unit, hence $T(e)$.

Lemma 10. *If T is Cayley-Hamilton, and $T(e) = 0$, then $e = 0$.*

Indeed, if $T(e) = 0$, then $T(e^i) = T(e) = 0$ for all i in the characteristic polynomial of e , $P_{e,T}(X)$ is X^d . Since T is Cayley-Hamilton, $e^d = 0$, but this implies $e = 0$.

Lemma 11. *There cannot be in R a family of more than d nonzero orthogonal idempotents.*

Indeed, the sum of all those idempotents e_1, \dots, e_k would be an idempotent e such that $T(e) = T(e_1) + \dots + T(e_k) \geq 1 + \dots + 1 = k > d$

Lemma 12. *If T is faithful, then so is T_e*

Indeed, if $x \in eRe$, is such that $T_e(xy) = 0$ for each y in eRe , then take $z \in R$. We have $T(xz) = T(xze) + T(xz(1-e))$ but $T(xz(1-e)) = T((1-e)xz) = 0$ so $T(xz) = T(xze) = T(xeze) = T_e(xeze) = 0$. Since T is faithful, $x = 0$.

Lemma 13. *If T is Cayley-Hamilton, so is T_e*

Here, as Buzzard saw, there is a little something to prove :

Clearly $P_{exe, T_e} P_{(1-e)x(1-e), T_{1-e}} = P_{x, T}$. If $x \in eRe$, the the second polynomial is simply $X^{d-T(e)}$, and we get $P_{e, T_e}(x) X^{d-T(e)} = 0$.

We now want to get rid of the $X^{d-T(e)}$ factor. We can do this because we have the above equality for all x in R . Indeed we may polarize the above equality, getting a multilinear symmetric forms in d variables, and then set the first $T(e)$ variables equal to x last $d - T(e)$ variables equal to 1 : we are done.

6. THE THEOREM OF TAYLOR

Theorem 14 (Taylor, Rouquier). *If A is an separably closed field k , then every pseudocharacter of dimension $d : T : R \rightarrow A$ is the trace of a representation $\rho : R \rightarrow M_d(k)$*

The method (not the one of Taylor) is to understand the structure of the algebra $R/\text{Ker } T$. For this we use a lemma :

Lemma 15. *The radical $\text{rad}(R/\text{Ker } T)$ of $R/\text{Ker } T$ is trivial.*

Proof — Let x be in the radical of $R/\text{Ker } T$. We first prove that x is nilpotent. Indeed write $P_{x, T}(X)$ as $aX^i(1 + XQ(X))$ with $a \in k^*$, $i \geq 0$. Then by Cayley-Hamilton, $ax^i(1 + xQ(x)) = 0$. But $xQ(x)$ is in the radical, so $1 + xQ(x)$ is invertible, and we get $x^i = 0$.

The second point is that a nilpotent element x in $R/\text{Ker } T$ has $T(x) = 0$. There are zillions of proofs of this fact. Here is one : we may assume by induction that $x^2 = 0$, and then the formula $S_{d+1}(T)(x, \dots, x)$ says exactly that $T(x)^{d+1} = 0$.

Putting those two points together, we see that every element x of the radical has $T(x) = 0$. For every $y \in R/\text{Ker } T$, xy is also in the radical thus we have $T(xy) = 0$. Since T is faithful, $x = 0$. \square

This lemma says that $R/\text{Ker } T$ is semi-simple. Moreover it is integral over A (since it is Cayley-Hamilton) and which is more every element in R is killed by a monic polynomial of degree d . And finally there are no family of more than d orthogonal non-zero idempotents. Those three properties implies :

Proposition 16. *$R/\text{Ker } T$ is isomorphic to a product of matrix algebras over k $M_{d_1}(k) \times \dots \times M_{d_r}(k)$.*

Note that the classical result state that semi-simple finite-dimensional algebra over k . Here we see that we can weaken the finite dimensionality, replacing it by two finiteness conditions, one on idempotents, the other on degree.

Proof — The conditions on idempotents prove that there is at most d isomorphism classes of irreducible modules over $R/\text{Ker } T$. If V is one of them, then $D := \text{End}_K(V)$ is a division algebra. There is a natural morphism $R \rightarrow \text{End}_D(V)$. The Jacobson density theorem states that this morphism is surjective if V is finite dimensional, and at least of dense image in the general case, in the sense that the image contains $\text{End}_D(V')$ for D -subspace V' of V of arbitrary high finite dimension. But V can not be infinite dimensional because this would imply that the image of

$R/\text{Ker } T$, hence $R/\text{Ker } T$ itself, would contain elements not killed by a unitary degree d -polynomial. Hence $R \rightarrow \text{End}_D(V)$ is surjective. Since $D \subset \text{End}_D(V)$, we see that every element in D is algebraic over k . Hence D is commutative, and a subfield of \bar{k} . Finally we use the classical result that the center of D is separable over k to conclude $D = k$. Hence $\text{End}_D(V)$ is a matrix algebra over k . We see easily, since $R/\text{Ker } T$ is semi-simple, that it is isomorphic to the product of $\text{End}_k(V_i)$ where V_i are the different simple modules over R . \square

Finally we have Taylor's theorem : we may replace R by $R/\text{Ker } T$, which is a product of matrix algebras, and we want to show that the pseudocharacter T on it is the trace of a semi-simple representation. Using idempotents e_1, \dots, e_r of $R/\text{Ker } T$ given by the identity elements of the matrix algebras $M_{d_i}(k)$, and results above on idempotents, we may assume that $R/\text{Ker } T$ is a matrix algebra $M_{d_i}(k)$.

We are reduced to prove the following lemma

Lemma 17. *A pseudocharacter on $M_d(k)$ is an integral multiple of the trace, hence the trace of a copies of multiple of the standard representation.*

Indeed, it is a trivial exercise to see that a central linear form T on $M_{d_i}(k)$ is a multiple of the trace, say αtr . Applying this to an idempotent ε of trace 1 in $M_{d_i}(k)$, we get $\alpha = T(\varepsilon)$ so α is an integer.

Note that on the case where T is irreducible, then obviously we have only one d_i which is d (hence $R/\text{Ker } T \simeq M_d(A)$) and the integer in the lemma above is 1.

7. THE IRREDUCIBLE CASE : THE RESULTS OF ROUQUIER AND NYSSSEN

Theorem 18. *Let $T : R \rightarrow A$ be a pseudocharacter of dimension d . Assume that A is local and strictly henselian, with residue field k . Assume that $\bar{T} := T \otimes k : R \otimes k \rightarrow k$ is irreducible (not the sum of two non-zero pseudocharacters). Then $R/\text{CH}(T) = R/\text{Ker } T \simeq M_d(A)$, and T is the trace of a (unique) representation, namely $R \rightarrow R/\text{Ker } T \simeq M_d(A)$.*

The uniqueness is due to Serre and Carayol, the existence of the representation and the result on $R/\text{Ker } T$ are due independently to Nyssen and Rouquier. The slightly stronger result on $R/\text{CH}(T)$ is ours.

Note that $\bar{T} : R \otimes k \rightarrow k$ is an irreducible pseudocharacter over a separably closed field, hence $(R \otimes k)/\text{Ker } \bar{T}$ is isomorphic to $M_d(k)$ by the above result.

For the proof, we may as well replace R by $R/\text{CH}(T)$, which simplifies notation and add the hypothesis that T is Cayley-Hamilton on R . As in the case of a field, the starting point is to understand the radical of R

Lemma 19. *If $T : R \rightarrow A$ is Cayley-Hamilton, and A, T has above, then $\text{rad } R$ is the inverse image of $\text{Ker } \bar{T}$ in R . In other words, $R/\text{rad } R = (R \otimes k)/\text{Ker } \bar{T} \simeq M_d(k)$.*

Proof — Let J denote the inverse image of $\text{Ker } \bar{T}$, it is a two-sided ideal of R . $\bar{R}/(\text{Ker } \bar{T})$ is a matrix algebra, hence is semi-simple, hence $\text{rad}(R) \subset J$.

Let $x \in J$; we will show that $1 + x \in R^*$. We have $T(xy) \in m, \forall y \in R$, hence $T(x^i) \in m$ for all i , so that by the Cayley-Hamilton identity $x^d \in m(A[x])$. Let us consider the commutative finite A -algebra $B := A[x]$. Then B is local with maximal

ideal (m, x) , as B/mB is. As a consequence, $1 + x$ is invertible in B , hence in R . As J is a two-sided ideal of R such that $1 + J \subset R^*$, we have $J \subset \text{rad}(R)$. \square

After this lemma we are almost done : on $R/\text{rad}R$ we have the elementary matrices $E_{i,j}$, for $i, j \in \{1, \dots, d\}$ that satisfy

$$E_{i,j}E_{k,l} = \delta_{j,k}E_{i,l}, \quad \sum_{i=1}^d E_{i,i} = 1.$$

It is well known (see Bourbaki - this is the basic fact used for example in the theory of Azumaya algebra) that we can lift those elements to R into elements, that we still denote $E_{i,j}$, that satisfy the same relations (note that we may lift the $E_{i,j}$ from the quotient by the radical, it would not work for an arbitrary two-sided ideal).

The $E_{i,i}$ are idempotents, hence each $T(E_{i,i})$ is an integer, which is not zero since $E_{i,i} \neq 0$. their sum has to be d , so all the $T(E_{i,i})$ are 1. From this we deduce that the restriction of T to $E_{i,i}RE_{i,i}$ is a Cayley-Hamilton pseudocharacter of dimension 1. But clearly this shows that $E_{i,i}RE_{i,i} = AE_{i,i}$ and is isomorphic to A as an A -module (T is a). As for $E_{i,i}RE_{j,j}$ take x in this set. Then $E_{j,i}x$ is in $E_{j,j}RE_{j,j}$ so by the above $E_{j,i}x = T(E_{j,i}x)E_{j,j}$. Then $x = E_{i,j}E_{j,i}x = T(E_{j,i}x)E_{i,j}$. This proves that $E_{i,i}RE_{j,j} = AE_{i,j}$. From those results it is easy to see that the linear map from R to $M_d(A)$ that sends $E_{i,j}$ to the (i, j) -elementary matrix is an isomorphism of A -algebra.

This proves the isomorphism, from which it is trivial to deduce that T is the trace of a representation as we did in the case of a base field.

Remark 20. An example of pseudocharacter that is not the trace of representations, was I asked after my first talk ? Well, since pseudocharacter descends (or glue, since the invention of Grothendieck's topology we know that it is the same) but not always representations, it is not hard to find in a non-local (for the étale topology, say) situation : for example take $A = k = \mathbb{R}$, $G = \mathcal{G}_3$ and ρ its natural complex 2 dimensional representation. Since it is the only representation of dimension 2 it is self-dual, so its trace T has value in \mathbb{R} , hence is a pseudocharacter $T : G \rightarrow \mathbb{R}$. But it is not the trace of the representation over \mathbb{R} . Note that in this case $A[G]/\text{Ker} T$ is the field of quaternions.

What is more serious is to find counter-example in a local situation, say over a strictly henselian local ring. We will construct a lot of them soon.

We can easily globalize this result : we release the hypothesis that A is local and henselian.

Corollary 21 (Rouquier). *Assume that $T : R \rightarrow A$ is a pseudocharacter such that for all $x \in \text{spec}(A)$, the pseudocharacter $T \otimes_{\bar{k}(x)}$ is irreducible ($\bar{k}(x)$ denote the separable closure of the residue field $k(x)$ of A at x). Then there is an Azumaya algebra \mathcal{A} on A and a morphism of algebras $\rho : R \rightarrow \mathcal{A}$ whose reduced trace is ρ .*

Indeed, take $\mathcal{A} = R/CH(T)$. Then since the formation of this algebra commutes to arbitrary base change, we see that (\mathcal{A}) is a matrix algebra $M_d(A)$ after every base change to a strictly henselian local ring. But this exactly one of the standard characterizations of (\mathcal{A}) being an Azumaya algebra. (At least when A is noetherian

- see "Le Groupe de Brauer" by Grothendieck - but this also works without the noetherian hypothesis - believe me)

Rouquier, who works with $R/\text{Ker } T$ has much more trouble proving this corollary,

8. RESIDUALLY MULTIPLICITY FREE PSEUDOCHARACTERS : FIRST STRUCTURE RESULTS

What follows is our work. We aim to understand, at least locally (for the etale topology, that is on a strictly henselian local ring), without the irreducibility hypothesis. Let A be a strictly local henselian ring, m is the maximal ideal of A , and $k := A/m$. Let R be an A -algebra and $T : R \rightarrow A$ be a pseudocharacter of dimension d . Let $\bar{R} := R \otimes_A k$ and $\bar{T} := T \otimes_A k : \bar{R} \rightarrow k$ be the reductions mod m of R and T .

By Taylor's result, there are (unique) representations $\bar{\rho}_i : R \rightarrow M_{d_i}(k)$, $i = 1, \dots, r$, which are irreducible such that $\bar{T} = \sum_{i=1}^r \text{tr } \bar{\rho}_i$.

Definition 22. We say that T is residually multiplicity free if the $\bar{\rho}_i : R \rightarrow M_{d_i}(k)$, $i = 1, \dots, r$, are pairwise non isomorphic.

In this case we have $\sum_{i=1}^r d_i = d$.

Once again, our objective is to describe a Cayley-Hamilton quotient of (R, T) . So we replace R by any Cayley-Hamilton quotient of (R, T) , for example $R/\text{Ker } T$ or the bigger $R/CH(T)$ or anything between. In other words, we assume that T is Cayley-Hamilton.

As we have seen earlier $R/\text{rad}R$ is isomorphic to $\bar{R}/\text{Ker } \bar{T} \simeq \prod_{i=1}^r M_{d_i}(k)$ and this isomorphism is compatible with T and the trace. Note ε_i , $i = 1, \dots, r$ the identity elements of $M_{d_i}(k)$ seen as idempotents of $R/\text{rad}R$. The ε_i are orthogonal and their sum is 1.

We may lift the ε_i into a family of orthogonal idempotents e_i of R . The idempotent $1 - \sum_{i=1}^r e_i$ is in $\text{rad}R$, so it is zero :

$$\sum_{i=1}^r e_i = 1.$$

Moreover, $T(e_i)$ is an integer between 1 and d that reduces to d_i modulo the maximal ideal of A . Hence $T(e_i) = d_i$.

Consider the restriction T_{e_i} of T to $e_i R e_i$. As we know, this is a Cayley-Hamilton pseudocharacter of dimension d_i , and we see easily that its residual pseudocharacter is $\text{tr } \bar{\rho}_i$ hence irreducible. By the theorem of the above section, we have an isomorphism

$$\psi_i : e_i R e_i \simeq M_{d_i}(A)$$

whose trace is T_{e_i} .

To complete our understanding of the structure of R , we need a description of the $e_i R e_j$ as well, when $i \neq j$. But $e_i R e_j$ is a left $e_i R e_i$ -module, that is a left $M_{d_i}(A)$ -module, and also a right $e_j R e_j$, that is $M_{d_j}(A)$ -module. By the very first result of Morita's equivalence theory, or by elementary reasoning using elementary matrices, we see that

$$e_i R e_j \simeq M_{d_i, d_j}(A_{i, j})$$

for a certain A -module $A_{i,j}$. This is to understand as the fact that $e_i R e_j$ is isomorphic, as an A -module, to the module of rectangular $d_i \times d_j$ matrices with coefficients in $A_{i,j}$ (that is $d_i d_j$ copies of $A_{i,j}$), and that the structure of left and right module under $M_{d_i}(A)$ and $M_{d_j}(A)$ are given by the usual multiplication formula, using the structure of A -modules on $A_{i,j}$ to multiply coefficients.

Finally, the multiplication of R restricts to maps $(e_i R e_j) \times (e_j R e_k) \rightarrow e_i R e_k$. Using the identification above, Morita's theory say that those maps come from bilinear maps

$$\phi_{i,j,k} : A_{i,j} \times A_{j,k} \rightarrow A_{i,k}$$

where we have set $A_{i,i} = A$.

The $\phi_{i,j,k}$ satisfy the symmetry condition

$$\phi_{i,j,i}(x, y) = \phi_{j,i,j}(y, x), \quad \forall x \in A_{i,j}, y \in A_{j,i}$$

since $T(xy) = T(yx)$.

To summarize, we have constructed an isomorphism of A algebra

$$R \simeq \begin{pmatrix} M_{d_1}(A_{1,1}) & M_{d_1,d_2}(A_{1,2}) & \dots & M_{d_1,d_r}(A_{1,r}) \\ M_{d_2,d_1}(A_{2,1}) & M_{d_2}(A_{2,2}) & \dots & M_{d_2,d_r}(A_{2,r}) \\ \vdots & \vdots & \ddots & \vdots \\ M_{d_r,d_1}(A_{r,1}) & M_{d_r,d_2}(A_{r,2}) & \dots & M_{d_r}(A_{r,r}) \end{pmatrix}$$

where the right hand side has the following meaning : it is an a A -algebra, the structure of A -modules is obvious, and the multiplication is given by the usual rule of multiplications of matrices using the $\phi_{i,j,k}$ when we need to multiply a coefficient in $A_{i,j}$ by a coefficient in $A_{j,k}$. Furthermore, all the $A_{i,i}$ are equal to A and the trace function of the right hand side (that is the sum of the diagonal element) corresponds to the T function on the left hand side.

We also note that

$$\phi_{i,j,i}(A_{i,j} \times A_{j,i}) \subset m$$

This follows from the fact that $T(e_i x e_j y e_i) \in m$ for all x and y in R which itself follows from the fact $e_i x e_j y e_i = 0$ for all $x \in R/\text{rad}R$.

As Gaetan explained, the modules $A_{i,j}$ together with the structural morphisms $\phi_{i,j,k}$ encode in a simple way a lot of significant information about the pseudocharacter T : for example, the extension we can construct from T between the $\bar{\rho}_i$, or the reducibility loci of T . I will say a little more on this in subsequent talks, but I refer to Gaetan's talk or to our preprint for the whole story.

9. GENERALIZED MATRIX ALGEBRAS AND MANY EXAMPLES OF PSEUDOCHARACTERS

No we reverse the process. We suppose given a family of A -modules, $A_{i,j}$ for $i, j \in \{1, \dots, r\}$, with $A_{i,i} = A$. (Here A may be a local henselian ring as before, or any commutative ring with unit if you wish). We also suppose given bilinear morphisms $\phi_{i,j,k} : A_{i,j} \times A_{j,k} \rightarrow A_{i,k}$ satisfying the symmetry condition

$$\phi_{i,j,i}(x, y) = \phi_{j,i,j}(y, x)$$

whenever this makes sense. From this, and integers d_1, \dots, d_r we can define an A -module

$$R \simeq \begin{pmatrix} M_{d_1}(A_{1,1}) & M_{d_1,d_2}(A_{1,2}) & \dots & M_{d_1,d_r}(A_{1,r}) \\ M_{d_2,d_1}(A_{2,1}) & M_{d_2}(A_{2,2}) & \dots & M_{d_2,d_r}(A_{2,r}) \\ \vdots & \vdots & \ddots & \vdots \\ M_{d_r,d_1}(A_{r,1}) & M_{d_r,d_2}(A_{r,2}) & \dots & M_{d_r}(A_{r,r}) \end{pmatrix}$$

and put a multiplication on it using the rule of matrix multiplication and the $\phi_{i,j}$. If R together with this multiplication turn out to be an associative algebra over A with unit the diagonal element made of 1 (this involves some explicit conditions on the $\phi_{i,j,k}$ we could but will not write down), then we say that R is a *Generalized matrix algebra* or *GMA*.

If R is a GMA, we can define the trace function $T : R \rightarrow A$ as the sum of the diagonal elements. We have $T(1) = d := d_1 + \dots + d_r$, and also $T(xy) = T(yx)$ for all $x, y \in R$.

By the preceding question we know that Cayley-Hamilton pseudocharacters that are residually multiplicity free (over a local strictly henselian ring) define GMA. But conversely :

- (1) On a GMA, is T always a pseudocharacter of dimension d ?
- (2) Does a GMA satisfy the Cayley-Hamilton theorem, in other words do we have $P_{x,T}(x) = 0$ for all $x \in R$?

A positive answer to (1) would prove a lot of non-trivial example of pseudocharacters. A positive answer to (2) would imply a positive answer to (1) since we know that $S_{d+1}(T)(x, \dots, x, y) = T(P_{x,T}(x)y)$

Remark 23. If we think about question (2) we see that this is a natural question about the domain of validity of the Cayley-Hamilton theorem. Indeed this theorem is nothing but a set of remarkable polynomial identities, true in any commutative ring, involving d^2 variables $X_{i,j}$ (the coefficients of a "generic" matrix). A little thinkig indicates that those indentities only involves products of the variable of the form $X_{i,j}X_{j,k}$, never $X_{i,j}X_{k,l}$ for $j \neq k$. Using a little bit of terminology of logic, It amouns to say that the theorem of Cayley Hamilton makes sense not only in the theory of commutative rings, but in a similar theory where variables have types (i, j) and only product of compatibles types $((i, j)$ with $(j, k))$ are allowed (which something of type (i, k)), with natural axiomms of commutativity and associativity. But the fact that the Cayley-Hamilton makes sense in this theory does not imply a priori that it is true in this theory (does it ?). The fact that it is, is precisely the content of question (2).

An even stronger question is

- (3) Is there a commutative ring B containing A and an *injective* morphism of A -algebra $\rho : R \hookrightarrow M_d(B)$ compatible with the trace functions ?

Indeed, if there was one, even with a huge and ugly B , the Cayley-Hamilton theorem for $M_d(B)$ would imply a positive answer to question (2)

Questions of the type of (3), namely question of embedding an algebra in a matrix algebras have been the subject of much interest since the sixties. A result of Procesi say that if A is a \mathbb{Q} -algebra, and if (2) has a positive answer then so has (3).

His method uses invariant theory and do not extend to the positive characteristic case.

- (4) Is there a commutative ring B containing A , and injections of A -modules of all the $A_{i,j}$ in the same ring B such that the morphisms $\phi_{i,j,k}$ become restriction of the multiplication of B ?

If (4) has a positive answer, then putting together the injection defines an injective representation as in (3).

Of course for example

Theorem 24. *Question (4) (hence questions (3), (2) and (1)) has a positive answer.*

For the proof, we refer the reader to \mathbb{BC} .

10. WHEN DO PSEUDOCHARACTERS COME FROM A REPRESENTATION

Let A be a local strictly henselian ring. Let $d \geq 2$ be an integer

Theorem 25. *The following assertion hold if and only if A is a unique factorization domain : for every A -algebra R and every pseudocharacter $T : R \rightarrow A$ of dimension d that is residually multiplicity free, there is a representation $\rho : R \rightarrow M_d(A)$ of trace T*

For the proof, we refer the reader to \mathbb{BC} .

We know almost nothing on the geometry of eigenvarieties. We don't know in general that they are smooth or locally UFD. So the natural Galois pseudocharacter on them has no reason to come from a true representation, near reducible points.

11. RIBET'S LEMMA FOR PSEUDOCHARACTERS, OR WHAT WE NEED TO CONSTRUCT SEVERAL INDEPENDANT EXTENSIONS (IN A RESIDUALLY MULTIPLICITY FREE CONTEXT)

Ribet's lemma asserts that if a representation ρ over a complete discrete valuation ring A is *generically irreducible* but residually, after semi-simplification, the sum of two characters, then there exists a non-trivial extension between those two pseudocharacters.

Ribet's lemma has been generalized by Mazur-Wiles for pseudocharacters of dimension 2 over more general local ring A - even if they don't say it this way - with the same multiplicity free condition hidden as an oddness assumption, and orthogonally by Bellaïche-Grafiëaux in the case of an arbitrary dimension and an arbitrary number of residual factors, but still over a complete d.v.r. Ribet's lemma and its generalization has been and is widely used in applications of automorphic forms theory to Selmer groups.

Now I want to present a generalization englobing all the preceeding ones in our context of a residually multiplicity character $T : R \rightarrow A$. we assume R Cayley-Hamilton, and we use the same notations as above. All the modules $A_{i,j}$, $i, j \in \{1 \dots r\}$ are supposed to be embedded in a ring B , so we can multiply them without mentioning the $\phi_{i,j,k}$.

Our first take is to generalize the *generic irreducibility* hypothesis in our setting.

Proposition 26. *There is a smallest ideal I in A such that $T \otimes A/I$ is the sum of r A/I -valued pseudocharacter. We have $I = \sum_{i \neq j} A_{i,j} A_{j,i}$. I is called the total reducibility ideal.*

In the case of Ribet, the generic irreducibility assumption simply says $I = 0$. Intuitively, the smaller is I , the more generically irreducible is T , and the more extensions we will be able to construct. To be complete we should also consider partial reducibility ideals I' such that $T \otimes A/J$

The proof of the proposition is not very hard, see [BC]. Let's just say that the existence of a smallest such ideal would not hold if the residual pseudocharacter was not multiplicity free,

By definition, we have $T \otimes A/I = \sum_{i=1}^r T_i$. Each of the characters T_i reduce to a character $\text{tr } \bar{\rho}_i$ module the maximal ideal. Hence by Rouquier and Nyssen's result each of the pseudocharacters $T_i : R/IR \rightarrow A/I$ is the trace of a true representation $\rho_i : R/IR \rightarrow M_{d_i}(A/I)$ that lifts $\bar{\rho}_i$.

We can now state the generalization of Ribet's lemma.

Theorem 27. *Let J be any ideal containing I (for the example I , or the maximal ideal m). Let i, j be two integers between 1 and r . Then there is a natural injection of A/J -modules*

$$\text{Hom}(A_{i,j} / (\sum_{k \neq i,j} A_{i,k} A_{k,j}), A/J) \hookrightarrow \text{Ext}_{R \otimes A/J}(\rho_j, \rho_i).$$

Moreover this result is optimal in the sense that this map is also surjective : we don't miss any extension "that T can see" this way

Once again, I refer to [BC] for the proof.

Let's try to understand what the theorem says. Consider the case $k = 2$. Then there is no k different from both i and j and we get

$$\text{Hom}(A_{i,j}, A/J) \hookrightarrow \text{Ext}_{R \otimes A/J}(\rho_j, \rho_i).$$

In this case, the reducibility ideal is simply $I = A_{1,2} A_{2,1}$.

This result is essentially due to Mazur-Wiles. With their notations, which are also the notations of Skinner's talk, we have $B = A_{1,2}$ and $C = A_{2,1}$. Their irreducibility ideal $I = BC$ is related to the Eisenstein ideal, hence to the p -adic L -function. Having some control on BC , they use the theory of the fitting ideal to get some control (lower bound) on $\text{Hom}(B, A/I)$ and construct enough extension.

One point to notice is that by this method they do not know if they construct, say, several independent extensions over k , or one big extension over A/J , or anything between. I mean, they only control the length of a module of extensions, not its structure. This is enough for the proof of the Main Conjecture. The questions about the structure of the constructed modules of extensions, are, in this context, related to the still-open Vandiver conjecture.

What would be needed to construct several "independent" extensions over k ? Take $J = m$ in the above injection : we get

$$\text{Hom}(A_{i,j}, k) \hookrightarrow \text{Ext}_{R \otimes k}(\bar{\rho}_j, \bar{\rho}_i)$$

The dimension of the right hand side is, by Nakayama, the minimal number of generators of the module $A_{i,j}$: that's the number of independent extension we can

construct. We thus see in particular that on a discrete valuation ring, we can only construct one independant extension.

In general, we do not control the $A_{i,j}$'s but the reducibility locus $I = A_{1,2}A_{2,1}$. We get easily

Corollary 28. *Assuem $r = 2$. The product of the dimension of $\text{Ext}(\bar{\rho}_1, \bar{\rho}_2)$ and $\text{Ext}(\bar{\rho}_2, \bar{\rho}_1)$ is greater than the minimal number of generator of the reducibility ideal I*

An interesting special case is when I is the maximal ideal of A (we are able to prove that this happens in many cases near reducible points in eigenvarieties). Then we see that the product of the dimension in the corollary is at least the Krull dimension of A , and even more if A is not regular. The geometry of A come into the game.

To be continued...

12. MODULES OVAR A GMA

13. PROLONGATION OF CRYSTALLINE PERIOD FOR A PSEUDOCHARACTER

14. GALOIS PSEUDEDEFORMATION AND $R = \mathbb{T}$ IN REDUCIBLE CASES

REFERENCES

- BC [BC] J. Bellaïche & G. Chenevier, *p-adic families of Galois representations and Selmer groups*, book in preparation (available on www.dma.ens.fr/~chenevie)
- Bki [Bki1] N. Bourbaki, *Éléments de mathématiques*, Algèbre, Actualités Scientifiques et Industrielles, Hermann, Paris, 1961.
- BouAc [Bki2] N. Bourbaki, *Éléments de mathématiques*, Algèbre commutative, Actualités Scientifiques et Industrielles, Hermann, Paris, 1961.
- Nys [Nys] L. Nyssen, *Pseudo-representations*, Math. Annalen 306 (1996), 257-283.
- Proc1 [Pr1] C. Procesi, *The invariant theory of $n \times n$ matrices*, Advances in math 19 (1976), 306–381.
- Proc2 [Pr2] C. Procesi, *A formal inverse to the Cayley-Hamilton theorem*, Journal of algebra 107 (1987), 63–74.
- Rou [Rou] R. Rouquier, *Caractérisation des caractères et pseudo-caractères*, J. Algebra 180(2) (1996), 571–586.
- Tay [T] R. Taylor, *Galois representations associated to Siegel modular forms of low weight*, Duke Math. J. 63 (1991), 281–332.