PSEUDO-CHARACTERS
(AN EXTENDED DISCUSSION OF §7 IN MAZUR'S PAPER)

VLADIMIR DOTSENKO

While preparing these notes I used many sources, but the primary one is [1]. Some of the proofs there were a bit confusing, so I came up with their alternatives and/or modifications; I take full responsibility for possible mistakes this note contains as a result. The key statements reproduced here were first obtained by Taylor [5] (theorem 4) and Nyssen [3] and Rouqier [4] (theorem 5).

Below A denotes a local commutative ring (more restrictions on A will be introduced when needed), and R an algebra over A. No assumptions on R are really needed, though of course, our main candidate is $R = A[[\Pi]]$ for a profinite group Π. This assumption, according to previous sections of Mazur's paper, will guarantee the uniqueness in Theorem 5 in some cases, while we only claim existence (since traces determine representations uniquely under the assumption that the reduction is absolutely irreducible). Whenever we work with pseudo-characters of degree d, we assume that $d!$ is invertible in A.

1. Introduction to pseudo-characters

Let f be a central function on R, that is an A-linear map $R \to A$ such that $f(xy) = f(yx)$ for all $x, y \in R$.

Definition 1. We shall now define mappings $S_k(f)\colon R^{\otimes k} \to A$. Let $x_1 \otimes \cdots \otimes x_k \in R^{\otimes k}$. For a permutation $\sigma \in \Sigma_k$, let $\sigma = c_1 \cdots c_l$ be its decomposition into disjoint cycles, let $f_{c_i} = f(x_{a_{i1}} x_{a_{i2}} \cdots x_{a_{in_i}})$, where a_{i1}, …, a_{in_i} are the numbers permuted by c_i in the induced cyclic order (since f is central, it is well defined on products that are defined up to a cyclic permutation of factors), and finally let $f_\sigma = f_{c_1} f_{c_2} \cdots f_{c_l}$. We put

$$S_k(f)(x_1, \ldots, x_k) = \sum_{\sigma \in \Sigma_k} (-1)^\sigma f_\sigma.$$

This formula is useful, but for some statements it'd be nice to have an alternative definition that allows for nice inductive proofs.

Proposition 1. *Mappings $S_k(f)\colon R^{\otimes k} \to A$ can be defined recursively as $S_1(f) = f$, and*

$$S_{k+1}(f)(x_1, \ldots, x_{k+1} = f(x_{k+1}) S_k(f)(x_1, \ldots, x_k) - \sum_{i=1}^{k} S_k(f)(x_1, \ldots, x_{i-1}, x_i x_{k+1}, x_{i+1}, \ldots, x_k).$$

Proof. In the formula for $S_{k+1}(f)$ as a sum over all permutations, let us, for each m, the summands corresponding to permutations where $k+1$ belongs to the cycle of length m. For $m = 1$, these summands together give $f(x_{k+1}) S_k(f)(x_1, \ldots, x_k)$. For larger m, we can "glue" x_{k+1} to its preimage, recovering $S_k(f)(x_1, \ldots, x_{i-1}, x_i x_{k+1}, x_{i+1}, \ldots, x_k)$ as the contribution of all the terms with $\sigma^{-1}(k+1) = i$. □

The following result, first noticed by Frobenius, will be motivational for us. The proof below is due to Rouquier.

Theorem 1. *If f is a character of some d-dimensional representation $\rho\colon R \to \mathrm{Mat}_d(A)$, then $S_k(f) = 0$ for $k > d$.*

Proof. First, it is enough to prove our result for $R = \mathrm{Mat}_d(A)$, $f = \mathrm{tr}$ (looking at the image, and noticing that if we prove our result for the matrix algebra, it surely remains true after a restriction to its subalgebra). Second, it is enough to consider the case $A = \mathbb{Z}[x_{ij}^{(l)}, 1 \le i, j \le d, 1 \le l \le k+1]$,

because this means that our polynomial identity will hold for matrices with generic coefficients. Finally, the field of fractions of a finitely generated ring $\mathbb{Z}[x_{ij}^{(l)}, 1 \leq i,j \leq d, 1 \leq l \leq k+1]$ can be embedded in $\mathbb{C}$, so it is enough to prove our result for $A = \mathbb{C}$. Moreover, since $S_k(f)$ is multilinear and symmetric, it is enough to prove that $S_k(f)(x,x,\ldots,x) = 0$ (indeed, it follows from the polarisation trick: to go back to non-equal arguments, set $x = c_1x_1 + \ldots + c_kx_k$, and look at the coefficient of $c_1 \cdots c_k$ there). Finally, since $S_k(f)$ is invariant under conjugation and continuous, we may assume that x can be diagonalised.

Let us look at the space $W = (\mathbb{C}^d)^{\otimes k}$. On this space, there is the diagonal action of $\mathrm{Mat}_d(\mathbb{C})$ and the action of σ_k permuting the factors. Our idea is to use the fact that

$$S_k(f)(x,x,\ldots,x) = \mathrm{tr}_W\left(\sum_{\sigma \in \Sigma_k} (-1)^\sigma x\sigma\right).$$

How does one see that this formula holds? To compute the trace of $x\sigma$, we note that in the basis of eigenvectors $e_1 \ldots, e_d$ of x, the tensor $e_{i_1} \otimes \cdots \otimes e_{i_k}$ contributes to the trace if and only if it is fixed by σ, which happens if and only if the function $j \mapsto i_j$ is constant on each cycle of σ. If we denote by a_p the value of this function on the cycle c_p, then the eigenvalue of this eigenvector is $\lambda_{a_1}^{|c_1|} \cdots \lambda_{a_l}^{|c_l|}$, where λ_i are eigenvalues of x on $\mathbb{C}^d$. Adding this up over all eigenvectors, we obtain $\mathrm{tr}(x\sigma) = \mathrm{tr}(x^{|c_1|}) \cdots \mathrm{tr}(x^{|c_l|})$. Finally, alternating this over $\sigma \in \Sigma_k$ indeed gives the formula for $S_k(f)$ we expect. It remains to notice that $\sum\limits_{\sigma \in \Sigma_k} (-1)^\sigma x\sigma = x \sum\limits_{\sigma \in \Sigma_k} (-1)^\sigma \sigma$, and $\sum\limits_{\sigma \in \Sigma_k} (-1)^\sigma \sigma$ projects onto the alternating elements in $(\mathbb{C}^d)^{\otimes k}$, but there are no such elements for $k > d$, so the operator is equal to zero, and as a consequence its trace is equal to zero. □

Remark 1. Before we move further on towards understanding functions determined by vanishing conditions for $S_{d+1}(f)$, let us make a historical remark. For Frobenuis, the previous theorem was not the end of the story either, but his direction of work was about using the expressions $S_k(f)$ to factorise group determinants. For a finite group G, the group determinant D_G is the determinant of the matrix M_G over the ring A of polynomials in variables x_g, $g \in G$, whose rows and columns are indexed by elements of G, and the element at the intersection of the row g and the column h is $x_{gh^{-1}}$. Essentially, it is the "determinant of the Cayley table of G". Dedekind noticed that for small groups the prime factor decomposition of the polynomial D_G (over an algebraically closed ground field) was somewhat remarkable, and, after several attempts of understand that decomposition in general, introduced Frobenius to this question (in two letters written in the spring of 1896). This led Frobenius to the discovery of the theory of characters of finite non-Abelian groups. His main result may be stated as follows. Let $a = \sum_{g \in G} x_g g \in A[G]$. Then

$$D_G = \prod_{i \in \widehat{G}} S_{n_i}(\chi_i)(a,a,\ldots,a)^{n_i},$$

where the product is over all isomorphism classes of representations of G, n_i is the dimension of the corresponding representation, and χ_i is its character. Moreover, each polynomial $S_{n_i}(\chi_i)(a,a,\ldots,a)$ is irreducible.

Definition 2. A central function f is said to be a pseudo-character of degree d if $S_{d+1}(f) = 0$, but $S_d(f)$ is not identically zero. (Clearly, the recursive formula of Lemma 1 implies that in this case $S_k(f) = 0$ for all $k > d$.)

Proposition 2. *The trace of a d-dimensional representation $R \to \mathrm{Mat}_d(A)$ is a pseudo-character of degree d. (As always, whenever we mention pseudo-characters, we assume that $d!$ is invertible in A.)*

Proof. We already know that tr is a pseudo-character of degree at most d. Clearly, $\mathrm{tr}(1) = d$. Suppose that tr is a pseudo-character of degree $d' < d$. Applying the recursive formula of Lemma 1 to compute $S_{d'+1}(\mathrm{tr})(x_1,\ldots,x_{d'},1)$, we get

$$0 = (\mathrm{tr}(1) - d')S_{d'}(\mathrm{tr})(x_1,\ldots,x_{d'}) = (d-d')S_{d'}(\mathrm{tr})(x_1,\ldots,x_{d'}),$$

but since $d!$ is invertible this would imply $S_{d'}(\mathrm{tr})(x_1,\ldots,x_{d'}) = 0$ identically, a contradiction. □

The following basic property of pseudo-characters is proved in a similar way, and will be used many times in this note.

Proposition 3. *If $f\colon R \to A$ is a pseudo-character of degree d, then $f(1) = d$.*

Proof. Applying the recursive formula of Lemma 1 to compute $S_{d+1}(f)(x_1, \dots, x_d, 1)$, we see that

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

and by induction

$$S_{d+1}(f)(1, \dots, 1) = f(1)(f(1) - 1) \cdots (f(1) - d),$$

so

$$f(1)(f(1) - 1) \cdots (f(1) - d) = 0,$$

Since $d!$ is invertible, the difference of every two factors $f(1) - d'$ and $f(1) - d''$, that is $d'' - d'$, is invertible, so at most one of them belongs to the maximal ideal of A, and the others are invertible, so $f(1)$ is an integer between 0 and d. If $f(1) = d' < d$, we have

$$0 = S_{d+1}(f)(x_1, \dots, x_d, 1) = (d' - d)S_d(f)(x_1, \dots, x_d),$$

but $d' - d$ is invertible in A, so $S_d(f)(x_1, \dots, x_d)$, a contradiction. □

If $f_1, \dots, f_n$ are pseudo-characters of degree 1, that is homomorphisms $R \to A$, then $f_1 + f_2 + \cdots + f_d$ is a pseudo-character of degree d, since it is the trace of the d-dimensional representation $f_1 \oplus \cdots \oplus f_d$. The next proposition shows that the most naïve generalisation of this result holds.

Proposition 4. *The sum of a pseudo-character of degree n and a pseudo-character of degree m is a pseudo-character of degree $m + n$.*

Proof. The following proof works over rationals; it is easy to show that in fact it is only necessary to assume that $(m + n)!$ is invertible (which we need to assume since we are dealing with a pseudo-character of that degree). Note that

$$S_k(f)(x, x, \dots, x) = (k - 1)! \sum_{l=1}^{k} (-1)^{l+1} f(x^l) \frac{S_{k-l}(f)(x, x, \dots, x)}{(k - l)!}$$

(we break the sum over permutations according to the length of the cycle containing k). This easily yields a differential equation for the formal power series

$$H_f(t) = 1 + \sum_{k \geq 1} S_k(f) \frac{t^k}{k!},$$

namely

$$H'_f(t) = \left(\sum_{l \geq 1} (-1)^{l+1} f(x^l) t^l \right) H_f(t),$$

and solving that equation, we obtain

$$H_f(t) = \exp \left(\sum_{l \geq 1} (-1)^{l+1} f(x^l) \frac{t^l}{l} \right).$$

Therefore,

$$H_{f+g}(t) = H_f(t) H_g(t),$$

from which our statement is almost immediate. □

To show even larger similarity between pseudo-characters of degree d and traces of d-dimensional representations, let us define a general construction associated to a given pseudo-character f: the characteristic polynomial with respect to f; those coincide with the usual characteristic polynomials in the case of traces, and share key properties with them in general. First, we recall the following basic fact about symmetric functions.

Proposition 5 (Newton's formulae)**.** *There exists unique polynomials $a_0, \ldots, a_{d-1}$ in the ring $\mathbb{Z}\left[\frac{1}{d!}\right][s_1, \ldots, s_d]$ such that for the specialisation at the point $s_k = \alpha_1^k + \ldots + \alpha_d^k$, where $1 \leq k \leq d$, and α_1, …, α_d are some complex numbers the following identity holds:*

$$t^d + a_{d-1}(s_1, \ldots, s_d)t^{d-1} + \cdots + a_1(s_1, \ldots, s_d)t + a_0(s_1, \ldots, s_d) = (t - \alpha_1) \cdots (t - \alpha_d).$$

Definition 3. Let A be a ring where $d!$ is invertible. We define the characteristic polynomial $P_{x,f}(t) \in A[t]$ of an element $x \in R$ with respect to a function $f\colon R \to A$ as the specialisation of the polynomial $t^d + a_{d-1}(s_1, \ldots, s_d)t^{d-1} + \cdots + a_1(s_1, \ldots, s_d)t + a_0(s_1, \ldots, s_d)$ at the point $s_k = f(x^k)$, $1 \leq k \leq d$.

Theorem 2. *For a ring A as above, and a central function $f\colon R \to A$ with $f(1) = d$, we have*

$$S_{d+1}(f)(x, x, \ldots, x, y) = (-1)^d d! f(P_{x,f}(x)y).$$

Proof. The formula for $S_{d+1}(f)(x, x, \ldots, x, y)$ as a sum over permutations shows that the polynomial $Q_{x,f}(t)$ defined by the formula

$$Q_{x,f}(t) = \sum_{\sigma \in \Sigma_{d+1}} (-1)^\sigma f(x^{|c_1|}) \cdots f(x^{|c_{l-1}|}) t^{|c_l - 1|}$$

satisfies the property

$$S_{d+1}(f)(x, x, \ldots, x, y) = f(Q_{x,f}(x)y),$$

is of degree d, and its leading coefficient is $(-1)^d d!$ (each of the $d!$ cycles of length $d+1$ contributes $(-1)^d$). It remains to prove that $Q_{x,f} = (-1)^d d! P_{x,f}$. Similar to Theorem 1, it is enough to prove that for $A = \mathbb{C}$, $R = \mathrm{Mat}_d(\mathbb{C})$, $f = \mathrm{tr}$, and x a diagonal matrix, which we can assume to have distinct eigenvalues. By Theorem 1, $S_{d+1}(f)(x, x, \ldots, x, y) = 0$ for all y, so $Q_{x,f}(x) = 0$. This means that $Q_{x,f}(t)$ is divisible by the minimal polynomial of x, which in our case coincides with $P_{x,f}(t)$, so since these polynomials are of the same degree and with the same leading coefficient, the theorem follows. □

Corollary 1 (Weak Cayley–Hamilton theorem)**.** *For a pseudo-character f of degree d, we have*

$$f(P_{x,f}(x)y) = 0$$

identically in x, y.

To make the above result imply the usual Cayley–Hamilton theorem, we need to make an assumption that our character is "non-degenerate".

Definition 4. The kernel $\mathrm{Ker}(f)$ of a central function $f\colon R \to A$ consists of all elements $x \in R$ for which $f(xy) = 0$ identically in y.

Because f is central, $\mathrm{Ker}(f)$ is a two-sided ideal. One can prove that for a semisimple representation, the kernel of its character is equal to the kernel of this representation in the usual sense.

Definition 5. A pseudo-character is said to be faithful if its kernel is trivial.

Our definitions make the following statement obvious.

Theorem 3 (Cayley–Hamilton theorem)**.** *If f is a faithful pseudo-character of degree d, then for every $x \in R$ we have*

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

2. Pseudo-characters over a field

Theorem 4. *Let k be a separably closed field, $f\colon R \to k$ a pseudo-character of degree d. Then f is the trace of a semisimple representation $\rho\colon R \to \mathrm{Mat}_d(k)$.*

Proof. The proof consists of several steps. Note that we may replace R by $R/\mathrm{Ker}(f)$ and assume that f is faithful.

Lemma 4.1. *Our algebra is semisimple:* $\mathrm{Rad}(R) = 0$.

Proof. Let us first show that all elements $x \in \mathrm{Rad}(R)$ are nilpotent. That is fairly easy: if we denote by t^k is the first power of t that appears in the characteristic polynomial of x, we see that

$$0 = P_{x,f}(x) = ax^l(1 + xQ(x)),$$

where $a \in k^\times$, and Q is some polynomial. Since $xQ(x)$ belongs to the radical, $1 + xQ(x)$ is invertible, and we conclude that $x^l = 0$.

Next, let us show that $f(x) = 0$ for $x \in \mathrm{Rad}(R)$. If $x^2 = 0$ then we note that $0 = S_{d+1}(f)(x, x, \dots, x) = f(x)^{d+1}$ (all other terms are equal to zero) so $f(x) = 0$ since we are working over a field. If $x^2 \neq 0$ but $x^4 = 0$, our argument shows that $f(x^d) = 0$ for $d \geq 2$, so again $0 = S_{d+1}(f)(x, x, \dots, x) = f(x)^{d+1}$, and so on. Since we already know that all elements of the radical are nilpotent, this iterated squaring will do the job.

Finally, since for $x \in \mathrm{Rad}(R)$ and $y \in R$ we have $xy \in \mathrm{Rad}(R)$, we conclude that $f(xy) = 0$ for all $x \in \mathrm{Rad}(R), y \in R$, so for each $x \in \mathrm{Rad}(R)$ we have $x = 0$ because f is faithul. □

If we knew in addition that R is a finite-dimensional algebra, then we would conclude that is is a product of matrix algebras over division rings (in fact, over k, since k is separably closed, $d!$ is invertible, and by Cayley–Hamilton every element is annihilated by a polynomial of degree d). We would like to make that conclusion now, but for that we shall have to work a bit more.

Lemma 4.2. *For a nonzero idempotent e in R, the value $f(e)$ is an integer between 1 and d.*

Proof. We shall use the property $S_{d+1}(f)(e, e, \dots, e) = 0$. Using the fact that $e^2 = e$, and the recursive formula of Lemma 1, we conclude that

$$f(e)(f(e) - 1) \cdots (f(e) - d) = 0,$$

so $f(e) = d'$ for some $0 \leq d' \leq d$, since we work over a field. Finally, if $f(e) = 0$, then by Cayley–Hamilton $e^d = 0$, but $e^d = e$, so $e = 0$. □

In fact, in this lemma we don't need to assume that k is a field, it would be enough to work over a local ring A, arguing as in the proof of Proposition 3. We shall be using it later on.

The previous lemma guarantees that R cannot have more than d pairwise orthogonal idempotents (and as a consequence it has at most d isomorphism classes of simple modules). Indeed, if $e_1, \dots, e_k$ are orthogonal idempotents, the element $e_1 + e_2 + \cdots + e_k$ is also an idempotent, and

$$d \geq f(e_1 + e_2 + \cdots + e_k) = f(e_1) + f(e_2) + \cdots + f(e_k) \geq k.$$

We are ready to prove

Lemma 4.3.

$$R \simeq \mathrm{Mat}_{d_1}(k) \oplus \ldots \oplus \mathrm{Mat}_{d_r}(k).$$

Proof. Let $V_1, \dots, V_r$ represent the classes of isomorphisms of simple R-modules. For each simple module V, the algebra $D = \mathrm{End}_R(V)$ is a division algebra. We regard V as a right module over D, so there is a natural morphism from R to $\mathrm{End}_{D^{op}}(V)$. By Jacobson Density Theorem, this morphism is surjective if V is finite-dimensional, and contains $\mathrm{End}_{D^{op}}(V')$ for $V' \subset V$ of arbitrary large dimension over D in its image otherwise. (Sketch of a proof: for an n-tuple of elements $x_1, \dots, x_n \in V$ that are linearly independent over D, we can consider the R-submodule $R \cdot (x_1, \dots, x_n) \subset V^n$. Since it is a submodule, we can find an R-equivaiant projection $\pi \colon V^n \to R \cdot (x_1, \dots, x_n)$, so that $\pi \in \mathrm{End}_R(V^n) = \mathrm{Mat}_n(D)$. For $T \in \mathrm{End}_{D^{op}}(V)$, we have $\pi(Tx_1, \dots, Tx_n) = (Tx_1, \dots, Tx_n)$; on the other hand, by the definition of π, there exists $r \in R$ such that $\pi(Tx_1, \dots, Tx_n) = (rx_1, \dots, rx_n)$.) This immediately means that V cannon be infinitely dimensional, since elements of the matrix algebra Mat_n for $n > d$ are not generally annihilated by polynomials of degree d, which is the case for R by Cayley–Hamilton. We conclude that the morphism $R \to \mathrm{End}_{D^{op}}(V)$ is surjective, therefore every element of D^{op} (and hence of D) is annihilated by a polynomial of degree d with coefficients in k. Since $d!$ is invertible and k is separably closed, this implies that $D = k$. Finally, the kernel of the map $R \to \mathrm{End}_k(V_1) \oplus \ldots \oplus \mathrm{End}_k(V_r)$ coincides with the radical, so that map is an isomorphism. □

Let us conclude the proof of our theorem. Let $e_1, \ldots, e_r$ be the idempotents of the respective matrix algebras; these are pairwise orthogonal idempotents that add up to 1. We see that for every $x \in R$

$$f(x) = \sum_{i,j} f(e_i x e_j) = \sum_i f(e_i x e_i),$$

since for $i \neq j$ we obtain $f(e_i x e_j) = f(e_j e_i x) = 0$. The map $x \mapsto f(e_i x e_i)$ is a pseudocharacter of R which is only nonzero on the matrix algebra $e_i R e_i$, so it is sufficient to classify pseudo-characters of matrix algebras. Note that a central function on a matrix algebra is proportional to the trace. (Indeed, since for $i \neq j$ we have $E_{ij} = E_{ii}E_{ij} - E_{ij}E_{ii}$, a central function vanishes on non-diagonal matrix units, and since $E_{ii} - E_{jj} = E_{ij}E_{ji} - E_{ji}E_{ij}$, all values on diagonal matrix units are equal.) But if $f(x) = c\,\mathrm{tr}(x)$, we see that $f(E_{11}) = c$ is an integer between 1 and d by Lemma 4.2. Therefore f is the sum of c copies of the standard representation. □

Examining this proof, it is easy to obtain the following

Corollary 2. *If f is a pseudo-character of degree d which is faithful and irreducible (that is not a sum of two pseudo-characters of smaller degrees), then $R \simeq \mathrm{Mat}_d(k)$.*

Remark 2. Buchstaber and Rees [2] showed that if A us a finitely generated commutative algebra over $\mathbb{C}$, and $f\colon A \to \mathbb{C}$ is a pseudo-character of degree d, then there exist ring homomorphisms $f_1, \ldots, f_d\colon A \to \mathbb{C}$ such that $f = f_1 + \cdots + f_d$. (An important corollary of that is the fact that if we let $\Phi_d(A) = \{f\colon A \to \mathbb{C} \mid S_{d+1}(f) = 0, f(1) = d\}$ then, as affine varieties,

$$\mathrm{Sym}^d(\Phi_1(A)) \simeq \Phi_d(A),$$

which, for example, gives an elegant and economic system of equations for the symmetric power $\mathrm{Sym}^d(\mathbb{C}^n)$.) This result in fact follows from Theorem 4, since a semisimple representation of a commutative algebra is a direct sum of one-dimensional representations.

3. Pseudo-characters over a local ring

From now on we assume that A is a Henselian local ring, and that the residue field $k = A/\mathfrak{m}$ is separably closed.

Theorem 5. *Suppose that $f\colon R \to A$ is a pseudo-character of degree d for which the reduction $\overline{f}\colon R \to A/\mathfrak{m}$ to the residue field is irreducible, that is not a sum of two pseudo-characters of smaller degrees. Then $R/\operatorname{Ker}(f) \simeq \mathrm{Mat}_d(A)$ and f is the trace of the representation $R \to R/\operatorname{Ker}(f) \simeq \mathrm{Mat}_d(A)$.*

Proof. First of all, we can factor out the kernel of f right away and assume that f is faithful.

Lemma 5.1. *The radical $\mathrm{Rad}(R)$ coincides with preimage of the kernel of $\overline{f}$ under the canonical projection $R \to R/\mathfrak{m}R$.*

Proof. Let us denote by J the preimage of the kernel of $\overline{f}$ under the canonical projection. Then, first,

$$R/J \simeq (R/\mathfrak{m}R)/\operatorname{Ker}(\overline{f}) \simeq \mathrm{Mat}_d(A/\mathfrak{m})$$

(the latter isomorphism holds because of our previous results, and irreducibility of $\overline{f}$), so R/J is semisimple, and therefore $\mathrm{Rad}(R) \subset (J)$. Also, if $x \in J$, then $f(x) \in \mathfrak{m}$, and moreover $f(xy) \in \mathfrak{m}$ for all $y \in R$. In particular, $f(x^i) \in \mathfrak{m}$ for all $i > 0$, so by Cayley–Hamilton $x^d \in \mathfrak{m} \cdot A[x]$. This means that for the ring $B = A[x]$ which is of finite dimension over A, the ring $B/\mathfrak{m}B$ is local, hence B itself is local with the maximal ideal $(\mathfrak{m}, x)$. Consequently, $1 + x$ is invertible in B, hence is invertible in R, so $1 + J$ consists of invertible elements. We conclude that $J \subset R$. Altogether, this means that $J = R$. □

In other words, this lemma can be formulated as

$$R/\operatorname{Rad}(R) \simeq (R/\mathfrak{m}R)/\operatorname{Ker}(\overline{f}) \simeq \mathrm{Mat}_d(A/\mathfrak{m}).$$

This formulation brings us very close to what we want to prove.

Lemma 5.2. *Let u and v be two orthogonal idempotents in $R/\operatorname{Rad}(R)$. Then there exist two orthogonal idempotents e and f in R which project into u and v.*

Proof. First, let us remark that by Cayley–Hamilton, every one-generated A-subalgebra of R is finite-dimensional over A, so is Henselian once A is. Let us take some r that projects into u; in the commutative subalgebra $A[r] \subset R$, we can lift u to an idempotent e. Let us take some element b that projects into v. The element $a = (1-e)b(1-e)$ also projects into v, and $ea = ae = 0$. Let us put $z = a^2 - a$. Clearly, $ze = ez = 0$. If $z = 0$ we are done, so we may assume $z \neq 0$. However, since a projects into an idempotent, $z \in \operatorname{Rad}(R)$. We observe that $(2a-1)^2 = 4z+1 \in 1+\operatorname{Rad}(R)$, so $2a-1$ is invertible. In R, we can solve the equation $w^2 + w + \frac{z}{(2a-1)^2} = 0$; moreover, we may lift the solution $w = 0$ that exists in $R/\operatorname{Rad}(R)$, so $w \in \operatorname{Rad}(R)$, and w commutes with e (we can work inside the commutative subalgebra generated by $\frac{z}{(2a-1)^2}$, each element of which commutes with e). Let $x = (1-e)w$. Then $x^2 + x + + \frac{z}{(2a-1)^2} = 0$, $ex = xe = 0$. Let $f = a + x(2a-1)$. Then $f^2 = f$, $ef = fe = 0$, and f projects into v because $x(2a-1)$ is in $\operatorname{Rad}(R)$. □

Note that we proved more: for every lifting e of u there is a lifting of v. We shall use it later.

Lemma 5.3. *Let u and v be two orthogonal idempotents in $R/\operatorname{Rad}(R)$ which are* related*: there exist elements $p \in u[R/\operatorname{Rad}(R)]v$ and $q \in v[R/\operatorname{Rad}(R)]u$ in such that $pq = u$, $qp = v$. Then the orthogonal idempotents e and f lifting u and v in R are related as well: there exist $x \in eRf$ and $y \in fRe$ such that $xy = e$, $yx = f$.*

Proof. Let $x_0 \in eRf$ and $y_0 \in fRe$ be some lifts of p and q. Since $x_0y_0 - e \in eRe$ projects to zero, we see that x_0y_0 is invertible in eRe (note that e is the unit of eRe). Let eze be its inverse: $x_0y_0eze = e$; the element eze projects into u in $u[R/\operatorname{Rad}(R)]u$. Let us put $x = x_0$, $y = y_0eze$. Then we already have $xy = e$, and we still have $x \in eRf$ and $y \in fRe$, and y still projects into q. What about yx? The element $g = yx - f$ satisfies

$$g^2 = yxyx - yxf - fyx + f = yex - yxf - fyx + f = yx - f = g$$

because $x \in eRf$ and $y \in fRe$. So, g is an idempotent that projects into 0 in $R/\operatorname{Rad}(R)$, so belongs to the radical. But a nonzero idempotent cannot belong to the radical, so $yx = f$. □

Lemma 5.4. *Suppose that the elements $e_{ij} \in R/\operatorname{Rad}(R)$, $1 \leq i, j \leq d$, are such that $e_{ij}e_{kl} = \delta_{jk}e_{il}$. Then there exist elements $E_{ij} \in R$ lifting those for which $E_{ij}E_{kl} = \delta_{jk}E_{il}$.*

Proof. By Lemma 5.2, the orthogonal idempotents e_{11}, …, e_{nn} can be lifted into orthogonal idempotents E_{11}, …, E_{nn}. (Induction: if we already lifted e_{11}, …, e_{kk}, we apply the lemma to the two orthogonal idempotents $e_{11} + \cdots + e_{kk}$ and $e_{k+1,k+1}$.) Also, the pair E_{11}, E_{kk} is related by the elements $E_{1k} \in E_{11}RE_{kk}$ and $E_{k1} \in E_{kk}RE_{11}$. It remains to put $E_{ij} = E_{i1}E_{1j}$; clearly, the required relations are satisfied. □

We are almost ready to conclude the proof of Theorem 5. Since by Lemma 5.1 the quotient $R/\operatorname{Rad}(R)$ is isomorphic to the matrix algebra, we can find elements E_{ij}, $1 \leq i, j \leq d$ that generate a subalgebra $\operatorname{Mat}_d(A)$ in R. It remains to prove that there is no other elements in R. First of all, we note that $E_{11} + \ldots + E_{dd} = 1$, because $1 - E_{11} - \cdots - E_{dd}$ is an idempotent in the radical of R. Recall that each $f(E_{ii})$ is a *positive* integer (since our representation is faithful), and $f(1) = d$, so we conclude that $f(E_{ii}) = 1$ for every i. Therefore the restriction of f on $E_{ii}RE_{ii}$ is a pseudo-character of degree 1. Being a pseudo-character of degree 1 means that $f\colon E_{ii}RE_{ii} \to A$ is a homomorphism of algebras; since it is faithful, it is an isomorphism. Let us now take $x \in E_{ii}RE_{jj}$ for $i \neq j$. Then $E_{ji}x \in E_{jj}RE_{jj}$, so by what we just proved we have $E_{ji}x = f(E_{ji}x)E_{jj}$. Consequently,

$$x = E_{ij}E_{ji}x = f(E_{ji}x)E_{ij}E_{jj} = f(E_{ji}x)E_{ij},$$

so $E_{ii}RE_{jj} = AE_{ij}$. This means that R is isomorphic to $\operatorname{Mat}_d(A)$. Also, since for $i \neq j$ we have $f(E_{ij}) = 0$ since $E_{ij} = E_{ii}E_{ij} - E_{ij}E_{ii}$. Recalling that $f(E_{ii}) = 1$, we conclude that f is the matrix trace. □

References

[1] Joël Bellaïche, *Ribet's lemma, generalizations, and pseudocharacters*, online lecture notes available at http://people.brandeis.edu/~jbellaic/RibetHawaii3.pdf.

[2] Victor Buchstaber and Elmer Rees, *The Gelfand map and symmetric products*, Sel. Math., New ser. **8** (2002), 523–535.

[3] Louise Nyssen, *Pseudo-représentations*, Math. Ann. **306** (1996), no. 2, 257–283.

[4] Raphaël Rouquier, *Caractérisation des caractères et pseudo-caractères*, J. Algebra **180** (1996), no. 2, 571–586.

[5] Richard Taylor, *Galois representations associated to Siegel modular forms of low weight*, Duke Math. J. **63** (1991), no. 2, 281–332.