

Ribet's lemma, generalizations, and pseudocharacters

Two lectures at the Clay Mathematical Institute Summer School,
Honolulu, Hawaii, 2009

Prerequisites: The prerequisites for these lectures are elementary:

- (i) Theory of finite-dimensional representations of groups and algebras; definitions and first properties of pseudocharacters (= pseudorepresentations).
- (iii) Very basic group cohomology.

Exercises: There are two kind of exercises, normal and difficult.

Terminology and convention: All rings and algebras have a unity, but are not necessarily commutative. Morphisms of rings and algebra preserve unities. Most often, a subring of a ring will have the same unity as the ring itself, but in a few cases, always explicitly mentioned, the subring shall have a different unity (so the injection map from the subring to the ring will not be a morphism of rings).

In general, A will denote a commutative ring, and R, S shall be non necessarily commutative A -algebra.

If B is a set, and d, d' are integers, then $M_{d,d'}(B)$ is the set of matrices with d columns and d' rows and entries in B . If $d = d'$, we write $M_d(B)$ instead of $M_{d,d}(B)$. If B and C are subsets of a ring A , there is of course a multiplication map $M_{d,d'}(B) \times M_{d',d''}(C) \rightarrow M_{d,d''}(A)$.

From Chris' lectures on Ribet's theorem ^{chHawaii}[S] and my lectures on Bloch-Kato ^{BKHawaii}[B2], you should have seen that constructing (non-trivial) extensions of Galois representations is often important in number theory.

In these lectures, we want to explain the fundamental tool to construct such extensions, *Ribet's lemma* (^F[R]). This is a purely algebraic lemma (with no reference to Galois group), and there will be no Galois group in these lectures. We will also present generalizations of this lemma, due to various authors (mainly Mazur-Wiles ^{MW}[MW], Bellaïche-Grafiéaux ^{BG}[BG] and Bellaïche-Chenevier ^{BC}[BC]). Since those generalizations involve the notion of *pseudo-representations*, that we call for confusion *pseudocharacters*, we also explain the theory of pseudocharacters, proving in particular the fundamental theorems of the theory (Taylor's theorem ^{Tay}[T] and Rouquier-Nyssen's theorem ^{Nys}[Nys] and ^{Rou}[Rou]).

CONTENTS

1. Ribet's Lemma	2
1.1. Reminder on lattices	2
1.2. Ribet's lemma	6
1.3. Exercises	7
1.4. Directions for a more general Ribet's lemma	9
2. Pseudocharacters	9
2.1. Representations and Frobenius' identity	10
2.2. Characteristic polynomial	13
2.3. Pseudocharacters	14
2.4. Taylor's theorem	17
2.5. Proof of Rouquier and Nyssen's theorem	19
2.6. Exercises	20
3. Residually multiplicity-free pseudocharacters	21
3.1. The structure theorem	22
3.2. Total reducibility locus	24
3.3. Generalization of Ribet's lemma: the case $r = 2$	25
3.4. Ribet's generalization: the general case	27
3.5. Exercises	28
References	29

1. RIBET'S LEMMA

In all this section, A is a discrete valuation domain, that is a local principal ideal domain, and K is its field of fraction. Its maximal ideal is therefore of the form πA for some π called a *uniformizer*, and any element of $x \in K^*$ can be written $x = u\pi^n$ with $u \in A^*$ and $n \in \mathbb{Z}$; the integer n is called the *valuation* $v(x)$ of x . We call k the residue field $A/\pi A$ of A .

1.1. Reminder on lattices.

1.1.1. *Definition of a lattice and first properties.* Let V be a vector space over K of dimension d . Since $A \subset K$, V has a structure of A -module.

Lemma and Definition 1.1. Let Λ be an A -submodule of V . The following are equivalent:

- (i) Λ is a finite A -module and $K\Lambda = V$.
- (ii) Λ is a finite A -module and the natural map $\Lambda \otimes_A K \rightarrow V$ (that sends $v \otimes x$ to xv) is an isomorphism.
- (iii) Λ is a free A -module of rank d .

If they hold, we say that Λ is a *lattice* of V .

Proof — The equivalence between (i) and (ii) follows from two simple observations: the map $\Lambda \otimes_A K \rightarrow V$ has image $K\Lambda$ and is injective. Only the second one needs a proof. Let $\sum v_i \otimes x_i$ with $v_i \in \Lambda$, $x_i \in K$ be an element of $\Lambda \otimes K$ that maps to 0 in V , that is such that $\sum_i x_i v_i = 0 \in V$. Let us choose an n such that $\pi^n x_i \in A$ for all i (this is possible since there is a finite number of x_i 's.) Then we have

$$\sum v_i \otimes x_i = \sum v_i \otimes (\pi^{-n} \pi^n x_i) = \left(\sum \pi^n x_i v_i \right) \otimes \pi^{-n} = 0.$$

This proves the desired injectivity.

Now assume that (ii) holds. The A -module Λ is finite, and is torsion-free since it is a sub-module of V which is torsion-free. Since A is a principal ideal domain, Λ is free of some rank d' , and the fact that $\Lambda \otimes_A K \rightarrow V$ is an isomorphism implies that $d' = d$, which proves (iii).

Conversely, assume that (iii) holds. Then Λ is obviously finite, and $\Lambda \otimes_A K$ is a K -vector space of rank d , so the linear map $\Lambda \otimes_A K \rightarrow V$, which we have seen is injective, is also surjective by equality of dimension. This shows (ii). \square

sumlattices

Lemma 1.1. *If $\Lambda \subset \Lambda'$ are two lattices of V and if Λ'' is an A -module such that $\Lambda \subset \Lambda'' \subset \Lambda'$, then Λ'' is also a lattice. If Λ and Λ' are two lattices of V , so is $\Lambda + \Lambda'$. More generally, if (Λ_i) is a non-empty family of sub-lattices of a lattice Λ , then $+_i \Lambda_i$ is a lattice.*

Proof — This is clear using the form (i) of the definition of a lattice. \square

Definition 1.1. We say that two lattices Λ and Λ' are *homothetic* if there exists $x \in K^*$ such that $\Lambda = x\Lambda'$.

Obviously, to be homothetic is an equivalence relation, and x can always be chosen of the form π^n with $n \in \mathbb{Z}$.

1.1.2. *Stable lattices and representations.* Let V be a K -vector space of dimension d .

Definition 1.2. If G is a subgroup of $\mathrm{GL}_K(V)$, we say that a lattice Λ of V is *G -stable* if $G\Lambda = \Lambda$ or equivalently $G\Lambda \subset \Lambda$.

Proposition 1.1. *For G a subgroup of $\mathrm{GL}_K(V)$, the following are equivalent:*

- (a) *There exists a G -stable lattice in V .*
- (b) *The coefficients of the matrices of elements of G in a suitable basis of V are in A .*
- (c) *The subgroup G is bounded in $\mathrm{GL}_d(K)$*

Proof — The implication (a) \Rightarrow (b) \Rightarrow (c) are clear. Let us prove (c) \Rightarrow (a). Let Λ be any lattice in V . Since G is bounded, there exists an $n \in \mathbb{Z}$ ($n \ll 0$) such that $g\Lambda \subset \pi^n \Lambda$ for all $g \in G$. The sum of all $g\Lambda$ is therefore a lattice by Lemma [1.1](#), **sumlattices** and is obviously stable by G . \square

Corollary 1.1. *If G is a compact group, and $\rho : G \rightarrow \mathrm{GL}_K(V)$ is a continuous representation, there exists a lattice stable by ρ (i.e. a lattice Λ such that $\rho(g)\Lambda = \Lambda$ for all $g \in G$.)*

Proof — Apply the proposition to $\rho(G)$, which is compact, hence bounded. \square

If G is a group, and $\rho : G \rightarrow \mathrm{GL}_K(V)$ is a continuous representation, and if Λ is a stable lattice by ρ , then we denote by ρ_Λ the representation $G \rightarrow \mathrm{GL}_A(\Lambda)$ obtained by restriction. This is a continuous "representation" of G (on a free module of rank d) over A . Of course for $n \in \mathbb{N}$, $\pi^n \Lambda$ is also stable by ρ_Λ , so we can define a representation $\rho_{\Lambda,n} : G \rightarrow \mathrm{GL}_{A/\pi^n A}(\Lambda/\pi^n \Lambda)$. If we choose a basis of Λ over A , then it defines a basis of $\Lambda/\pi^n \Lambda$ over $A/\pi^n A$, and in those bases, the matrix of $\rho_{\Lambda,n}(g)$ is just the reduction modulo π^n of $\rho_\Lambda(g)$.

When $n = 1$, $A/\pi A$ is the residue field k , so $\bar{\rho}_{\Lambda,1}$ is a representation of dimension d over the field k . We shall write $\bar{\rho}_\Lambda$ instead of $\rho_{\Lambda,1}$.

There may be various stable lattices Λ for a given ρ . For different stable lattices Λ , the representations $\bar{\rho}_\Lambda$ may be non-isomorphic (we shall see examples below). Of course, if Λ and Λ' are homothetic, then $\bar{\rho}_\Lambda$ and $\bar{\rho}_{\Lambda'}$ are isomorphic, since ρ_Λ and $\rho_{\Lambda'}$ are (the multiplication by x is an isomorphism if $\Lambda' = x\Lambda$.) In general, we have at least

bn **Proposition 1.2.** *If Λ and Λ' are two stable lattices, we have $\bar{\rho}_\Lambda^{\mathrm{ss}} = \bar{\rho}_{\Lambda'}^{\mathrm{ss}}$.*

Here we note ρ^{ss} the semi-simplification of a representation ρ , that is the direct sum of its Jordan-Hölder factors for any Jordan-Hölder sequence.

Proof — Let $g \in G$. The polynomial characteristic of $\bar{\rho}_\Lambda(g)$ is the restriction mod π of the characteristic polynomial of $\bar{\rho}_\Lambda(g)$, which is simply the restriction of the characteristic polynomial of $\rho(g)$ (that we see in passing to be in $A[X]$), so it is the same as the polynomial characteristic of $\rho_{\Lambda'}(g)$. By the Brauer-Nesbitt theorem, this proves that $\bar{\rho}_\Lambda \simeq \bar{\rho}_{\Lambda'}^{\mathrm{ss}}$. \square

Definition 1.3. If ρ is a representation that has a stable lattice, we call $\bar{\rho}^{\mathrm{ss}}$ any of the semi-simplification $\bar{\rho}_\Lambda^{\mathrm{ss}}$ for Λ a stable lattice.

tree

1.1.3. *The tree of $\mathrm{GL}_2(K)$.* Let V be a vector space of dimension d over K . Let X be the set of lattices in V , up to homotheties. If Λ is a lattice, we denote by $[\Lambda] \in X$ its equivalence class up to homotheties. This set has an interesting structure, of which we recall some parts, leaving proofs in exercises.

Definition 1.4. We say that a point x' in X is a *neighbor* of a point $x \in X$ if $x' \neq x$ and there are lattices Λ, Λ' of V such that $x = [\Lambda]$, $x' = [\Lambda']$ and $\pi\Lambda \subset \Lambda' \subset \Lambda$.

neighbors

Lemma 1.2. *Let $x = [\Lambda]$ be a point in X . There exists a natural bijection between the set of neighbors of x and the set of proper non-trivial k -subspaces of the k vector space $\Lambda/\pi\Lambda$.*

The bijection is defined as follows: if x' is a neighbor of X , then the Λ' such that $\pi\Lambda \subset \Lambda' \subset \Lambda$ is unique, Λ being fixed. We attach to x' the subspace $\Lambda'/\pi\Lambda$ of $\Lambda/\pi\Lambda$.

The relation x' is a neighbor of x is symmetric. Therefore the set X with this notions of neighborhood is a undirected graph, and all notions of graph theory applies. For example a *path* from x to x' is a sequence $x = x_0, x_1, \dots, x_n = x'$ of points in X such that for all $i = 0, \dots, n-1$, x_i is a neighbor of x_{i+1} . The integer $n \geq 0$ is the length of the path, and the distance $d(x, x')$ between x and x' is the minimal length of a path from x to x' (if any). A path is said *injective* if we have $x_i \neq x_j$ for all $i, j \in \{0, \dots, n\}$.

proptree

Proposition 1.3. (a) *The graph X is connected, that is, there is a path from any point to any other.*

(b) *If $d = 2$, the graph X is simply connected, that is: for any $x, x' \in X$, $x \neq x'$, there is only one injective path from x to x' .*

A graph X that is connected and simply connected is called a *tree*. From now on, **we assume that** $d = 2$, so X is a tree. If k is finite, the number of neighbors of any point X is $|k| + 1$ (by Lemma ^{neighbors} 1.2), so X is a *homogeneous tree*.

In a tree, we define the *segment* $[x, x']$ as the set $\{x\}$ if $x = x'$, and as the set of points in the unique injective path from x to x' otherwise. A subset C of X is called *convex* if for every $x, x' \in C$, the segment $[x, x']$ is included in C . A *half-line* H in X is a subset of X that is an increasing union of segments of the form $[x, x_n]$ of length n for $n \in \mathbb{N}$. The point x is the *origin* of H .

If $d(x, x') = n$, then we can choose lattices $x = [\Lambda]$ and $x' = [\Lambda']$ such that $\pi^n\Lambda \subset \Lambda' \subset \Lambda$. Once Λ is fixed, Λ' is unique, and the A -modules Λ/Λ' and $\Lambda'/\pi^n\Lambda$ are isomorphic to $A/\pi^n A$. Conversely, such a Λ' define a point at distance n of $[\Lambda]$.

Let $x = [\Lambda]$ be a point in X , and L be a direct summand A sub-module of rank one of Λ . Then if $\Lambda_n := L + \pi^n\Lambda$, $x_n := [\Lambda_n]$ is a point at distance n of x and L define a half-line $H(L, x) = \cup[x, x_n]$ of origin x . Conversely, assume that K is complete. If H is a half-line in X as above, with origin x , there are unique points $x_n = [\Lambda_n]$ in H such that $\pi^n\Lambda \subset \Lambda_n \subset \Lambda$ and $\Lambda/\Lambda_n \simeq A/\pi^n A$. The intersection $L := \cap_{n \in \mathbb{N}} \Lambda_n$ is a free A -submodule of rank one of Λ that is direct summand. It is canonically attached to H and Λ and denoted by $L(H, \Lambda)$.

It is easy to see that a convex C is bounded if and only if it contains no half-line, and that a non empty bounded convex C contains a point that has at most one neighbor.

The group $GL_K(V)$ operates on X (by $g \bullet [\Lambda] := [g\Lambda]$) through its quotient $PGL_k(V)$ and preserves the graph structure. This operation is transitive.

1.2. Ribet's lemma. This is the following statement, that appears (as a "proposition" actually, not a lemma) in [R].

Proposition 1.4. *Assume that K is complete. Let G be a compact group, and $\rho : G \rightarrow \mathrm{GL}_K(V)$ be an irreducible representation of dimension 2. Assume that $\bar{\rho}^{\mathrm{ss}}$ is the sum of two characters $\chi_1, \chi_2 : G \rightarrow k^*$. Then there exists a stable lattice Λ such that $\bar{\rho}_\Lambda$ is a non-trivial extension of χ_1 by χ_2 .*

Remark 1.1. The characters χ_1 and χ_2 play a symmetric part in the hypotheses. Therefore, the Proposition also asserts that there exists a stable lattice Λ' such that $\bar{\rho}_{\Lambda'}$ is a non-trivial extension of χ_2 by χ_1 . In this situation it is clear that $\bar{\rho}_\Lambda$ and $\bar{\rho}_{\Lambda'}$ are not isomorphic.

We shall give a proof, due to Serre, of this result, which, though it is certainly not the shortest, is probably the most illuminating. The proof will occupy the rest of this §.

Let $\rho : G \rightarrow \mathrm{GL}_K(V)$ (with $\dim V = 2$) be any representation **that has a stable lattice**.

Let X be the tree of $\mathrm{GL}_K(V)$ and C be the set of x in X that are fixed by $\rho(G)$ (which operates on X as a subgroup of $\mathrm{GL}_K(V)$). We note that if $x \in C$, and $x = [\Lambda]$, then Λ is a stable lattice for ρ (indeed by definition we have $\rho(g)\Lambda = \pi^k\Lambda$, but since $\rho(G)$ is bounded, k has to be 0). If $x \in C$ and $x = [\Lambda] = [\Lambda']$, then $\bar{\rho}_\Lambda \simeq \bar{\rho}_{\Lambda'}$, therefore there is no ambiguity in calling that representation $\bar{\rho}_x$.

Lemma 1.3. *The subset C of X is non-empty and convex.*

Proof — C is non-empty because it contains $[\Lambda]$ where Λ is stable lattice by ρ . C is convex because, if x, x' are in C , the segment $g \bullet [x, x']$ is a segment of extremities x and x' , so is $[x, x']$ by uniqueness. Therefore $[x, x'] \subset C$. \square

Lemma 1.4. *If x is in C , then we have*

- (a) *x has no neighbor in C if and only if $\bar{\rho}_x$ is irreducible;*
- (b) *x has exactly one neighbor in C if and only if $\bar{\rho}_x$ is reducible but indecomposable;*
- (c) *x has more than one neighbors in C if and only if $\bar{\rho}_x$ is decomposable (that is, the sum of two characters).*

In case (c), the numbers of neighbors in C is 2 if the two characters appearing in $\bar{\rho}_x$ are distinct. If they are equal, every neighbor of x in X is in C .

Proof — It is elementary that a representation of dimension 2 has no (resp. one, resp. 2, resp. all) stable line if and only if it is irreducible (resp. reducible but indecomposable, resp. decomposable in the sum of two distinct characters, resp. decomposable in the sum of two equal characters). This implies the Lemma if we

can identify "Lines stable by $\bar{\rho}_x$ in $\Lambda/\pi\Lambda$ " (where $x = [\Lambda]$) and "neighbors of x in C ". But that identification follows directly from the bijection of Lemma 1.2. \square

Remark 1.2. In particular, $\bar{\rho}^{\text{ss}}$ is irreducible if and only if C is reduced to a point, that is if and only if ρ has only one stable lattice (up to homotheties). This is clear from the lemma, since in a convex set not reduced to a point, every point has a neighbor.

Lemma 1.5. *Assume that K is complete. Then ρ is irreducible if and only if C is bounded.*

Proof — Assume C is not bounded. Then since it is convex it contains a half-line H . Let $x = [\Lambda]$ be the origin of H . Then the free A -submodule of rank one $L = L(H, \Lambda)$ of Λ is by construction stable by $\rho(G)$, so KL is a stable line in V , and ρ is not irreducible.

Assume that ρ is reducible. Then it has a stable K -line V_0 . Let $L = \Lambda \cap V_0$. This is a free A -submodule of rank one, direct summand, of Λ . Let $H = H(L, x)$ be the half-line defined by L in X . By construction $H \subset C$. Therefore C is not bounded. \square

Now let us go back to Ribet's lemma. We assume that ρ is irreducible (so C is bounded), but that $\bar{\rho}^{\text{ss}}$ is not (so that every point of C has at least one neighbor in C). Since C is bounded and convex, it has a point x with at most one, so actually exactly one neighbor in C . Therefore $\bar{\rho}_x$ is reducible but not indecomposable, that is which is a non-trivial extension of χ_1 by χ_2 or of χ_2 by χ_1 .

This simple geometric argument almost proves Ribet's lemma. "Almost", because Ribet's lemma states that we can find an x where we actually get a $\bar{\rho}_x$ that is non-trivial extension of χ_1 by χ_2 , not the other direction. Of course, this only matters when $\chi_1 \neq \chi_2$. So assume that $\chi_1 \neq \chi_2$. Then every point of C has at most two neighbors. Since C is convex and bounded, this easily implies that S is a segment $[x, x']$. It is an easy exercise to see that, up to exchanging x and x' , $\bar{\rho}_x$ is actually a non-trivial extension of χ_1 by χ_2 and $\bar{\rho}_{x'}$ is an extension of χ_1 by χ_2 .

1.3. Exercises.

Exercise 1.1. If $G \subset \text{GL}_K(V)$ has a stable lattice, then $\text{tr}(G) \subset A$. Show that the converse is false, but becomes true if we assume that G is absolutely irreducible.

Exercise 1.2. Prove all the assertions of \S 1.1.^{tree}3. They are all almost trivial, except maybe Proposition 1.3.^{proptree} which may need a little bit of works.

Exercise 1.3. Prove that when $d > 2$, X is not a tree. A *facet* F is a subset of X such that every two distinct elements of F are neighbors. Show that a maximal facet has cardinality d . The set X with the data of all its facets has the structure

of *building* in the sense of Tits (see $\overline{\text{BouI}}$, $\overline{\text{Bourbaki}}$ exercises). It is called the *Bruhat-Tits building* of $\text{PGL}_K(V)$.

Exercise 1.4. Show that when K is not complete, the argument constructing a sub-module L of rank one in Λ attached to a half-line $H \in X$ of origin $[\Lambda]$ may fail. (actually, the sub-module L it constructs may be (0))

Exercise 1.5. Do the exercise that concludes the proof of Ribet's lemma.

In all the following exercises, we keep the notations and assumptions of Ribet's lemma, and we assume moreover that $\chi_1 \neq \chi_2$, and that $\text{char} k \neq 2$. So as we have seen the convex C is a segment.

$\overline{\text{red mod } \pi}$

Exercise 1.6. (difficult) Let l be the length of the segment C . Let $n = n(\rho)$ be the largest integer, if it exists, such that there exists two characters $\psi_1, \psi_2 : G \rightarrow (A/\pi^n A)^*$ such that for all $g \in G$, $\text{tr } \rho(g) \equiv \psi_1(g) + \psi_2(g) \pmod{\pi^n}$

a.– Show first that n exists.

The integer n can be called the *index of reducibility* of ρ : the larger is n , the "more reducible" is ρ residually).

b.– Show that $l = n + 1$. (Hint: choose a $g_0 \in G$ such that $\chi_1(g_0) \neq \chi_2(g_0)$. Show that $\rho(g_0)$ is diagonalizable. In a basis of V where it is diagonal, compare $\rho(g)$ and $\rho(gg_0)$ and their traces for all $g \in G$.)

c.– Show how to construct a representation $G \rightarrow \text{GL}_2(A/\pi^n A)$ which is an extension of ψ_1 by ψ_2 , where reduction modulo π is a non-trivial extension of χ_1 by χ_2 . Show that this extensions generates a sub-module isomorphic to A/π^n in $\text{Ext}_{A[G]}^1(\chi_2, \chi_1)$.

In the following exercise you are allowed to use the exercise $\overline{\text{mod } \pi}$ I.6.

Exercise 1.7. There exists $x \in C$ such that $\bar{\rho}_x$ is $\chi_1 \oplus \chi_2$ if and only if $n(\rho) > 1$.

Exercise 1.8. Let G' be a subgroup of G , and assume that $(\chi_1)|_{G'} \neq (\chi_2)|_{G'}$. Let C' be the subset of X fixed by $\rho(G')$.

a.– Show that C' is either a segment, or a half-line, or a line in X (define yourselves a line in X). Show that $C \subset C'$.

b.– Show that $C = C'$ if and only if for every x such that $\bar{\rho}_x$ is (reducible) indecomposable, then $(\bar{\rho}_x)|_{G'}$ is (reducible) indecomposable.

Exercise 1.9. Let G be the subgroup of $\text{GL}_2(A)$ of matrices whose lower left entry is in πA (this group is called the *Iwahori* subgroup of $\text{GL}_2(K)$). Let $\rho : G \rightarrow \text{GL}_2(K)$ be the representation of G given by inclusion. Show that S has two points in this case, and that for every stable lattice Λ , $\bar{\rho}_\Lambda$ is **not** semi-simple.

Exercise 1.10. Show that up to replace K by any ramified extension, we can always find a stable Λ such that $\bar{\rho}_\Lambda$ is semi-simple.

1.4. Directions for a more general Ribet's lemma. Ribet's Lemma cries for generalizations. First, what happens if ρ is a representation of dimension d , not necessarily 2? When we ask this question, we see that $\bar{\rho}^{\text{ss}}$, if reducible, may be the direct sum of more than 2 irreducible representation, say r irreducible representations $\bar{\rho}_1, \dots, \bar{\rho}_r$ of respective dimensions d_1, \dots, d_r (with of course $d_1 + \dots + d_r = d$, so $r \leq d$). What extensions between the $\bar{\rho}_i$ can we get?

We can go further. We have assumed that A was a complete discrete valuation domain, with fraction field K and residue field k . What if we assume that A is a general local domain, again with fraction field K and residue field k ? The theory of lattices will not be so simple, and it will not be the case that ρ has always a stable free lattice, so we cannot define $\bar{\rho}^{\text{ss}}$ so simply. But if we assume to begin with that ρ is a representation over $A : G \rightarrow \text{GL}_d(A)$ such that $\rho : G \rightarrow \text{GL}_d(K)$ is irreducible, while $\bar{\rho}^{\text{ss}} = \bar{\rho}_1 \oplus \dots \oplus \bar{\rho}_r$ is reducible, then we can ask : can we produce somehow non-trivial extensions of $\bar{\rho}_i$ by $\bar{\rho}_j$?

If A is discrete valuation ring, $\text{Spec } A$ has two points, the closed point $\text{Spec } k$ and the generic point $\text{Spec } K$, and the hypothesis of Ribet's lemma can be rephrased as: ρ is irreducible at the generic point, but reducible at the closed point. When A is a general local domain, the geometry of $\text{Spec } A$ is much richer, and it might be sensible to refine the hypothesis that ρ is irreducible at the generic point. Is there a largest closed subscheme \mathbf{red}_ρ of $\text{Spec } A$ on which ρ is reducible (in some sense, for example some sense inspired by exercise ^{redlocex}1.6)? If so, \mathbf{red}_ρ is a proper subscheme if and only if ρ is irreducible at the generic point, and instead of simply assuming that ρ is irreducible at the generic point, we can make a more precise assumption on \mathbf{red}_ρ , presumably getting better results (that is more non-trivial extensions between the $\bar{\rho}_i$) the smaller \mathbf{red}_ρ is. When we do so, we see that we have no need to speak of the generic point anymore, that is no need to assume that A is a domain: any local ring will do.

To go further, why should we start with a representation $\rho : G \rightarrow \text{GL}_d(A)$? A pseudo-character $T : G \rightarrow A$ of dimension d is more general. When A is a d.v.r., this generality is an illusion, but for general local ring A , it is not as we shall see. So we should work with general pseudocharacters.

In the following sections, we shall give a generalization of Ribet's lemma along the lines explained above. Since Kisin's talk on pseudorepresentations have been sketchy, and since we will need to go in detail, we begin by reviewing them, beginning by giving them their right names.

2. PSEUDOCHARACTERS

This section intends to be a fairly complete and self-contained coverage of the theory of pseudocharacters.

To begin with, pseudocharacters and pseudorepresentations are the same things. *Pseudorepresentations* was the term coined by Wiles, and used thereafter by Taylor,

Nyssen and others. *Pseudocharacters* is the term used by Serre and Rouquier. It is better because pseudocharacters (*false characters* etymologically) look like characters of representations, without always being characters of representations. They don't look at all like representations¹. I will use the term *pseudocharacter*.

Pseudocharacters, in their modern forms, were invented by Taylor in [Tay]. He was inspired both by a variant of this notion, defined under the same name in the special setting of two-dimensional odd representations by Wiles [Wiles], and by Procesi [Pr1], [Pr2], who studied, using Geometric Invariant Theory the closely related notion of trace algebras. Taylor's treatment of the subject, in particular his main theorem that every pseudocharacter over an algebraically closed field comes from a representation relies heavily on Procesi's work, and therefore is limited to characteristic 0. Nyssen ([Nys]) and Rouquier ([Rou]) independently extended Taylor's theorem to the case of residually irreducible pseudocharacters over strictly Henselian local fields. Rouquier's paper, which is the first to use the name pseudocharacters instead of pseudorepresentations, also offers a self-contained and elegant treatment of the subject, as well as an extension in finite characteristic of the theory. This presentation is largely inspired by Rouquier's.

2.1. Representations and Frobenius' identity.

2.1.1. *Definitions and reminder.* Let A be a commutative ring (with unity). If G is a group, a *representation* of G over A of dimension d will be a morphism of groups $\rho : G \rightarrow \mathrm{GL}_d(A)$. If R is an A -algebra (with unity, but non-necessarily commutative), then a *representation* of R over A of dimension d will be a morphism of A -algebras $\rho : R \rightarrow M_d(A)$. Two representations are said *equivalent* if they are conjugate by an element of $\mathrm{GL}_d(A)$. There is a natural and obvious bijection, preserving dimension and equivalence, between representations of a group G over A and representation of its group algebra $A[G]$.

If A' is another commutative ring, which is given an A -algebra structure, and ρ is a representation of a group G (resp. an A -algebra R) over A , we shall denote by $\rho \otimes_A A'$ the representation $\rho : G \rightarrow \mathrm{GL}_d(A) \rightarrow \mathrm{GL}_d(A')$ (resp. $\rho \otimes 1 : R \otimes_A A' \rightarrow M_d(A')$). Of course $\rho \mapsto \rho \otimes_A A'$ preserves equivalence and is compatible with the bijections (over A and A') between representations of a group and its group algebra.

From now on, we shall restrict ourselves to representation of an A -algebra R , since this case is more general.

The *character* of a representation $\rho : R \rightarrow A$ is the application $T : R \rightarrow A$ defined by $T(x) = \mathrm{tr} \rho(x)$. It is well known that if A is a field K of characteristic 0, then two semi-simple representations with the same character are isomorphic. If K has characteristic p , then two semi-simple representations of dimension less than p

¹Actually in the first definition given by Wiles, they looked more like representations. So the terminology was adapted to that notion, but not to Taylor's notion of pseudocharacter.

with the same character are isomorphic, but this obviously fails for representations of dimension p or higher.

frob

2.1.2. *Frobenius identity.* Let $\rho : R \rightarrow M_d(A)$ be a representation, and T its character. Then obviously:

- (i) T is A -linear.
- (ii) We have $T(xy) = T(yx)$ for every x and y in R .
- (iii) $T(1) = d$.

Any application $T : R \rightarrow A$ satisfying (i) and (ii) will be called a *central function*. The precise meaning of (iii) is $T(1_R) = d1_A$.

To give an other, much less obvious, property of T , we introduce some notations. Let $T : R \rightarrow A$ be any central function, and let $k \geq 1$ be an integer. For $\underline{x} = (x_1, \dots, x_k) \in R^k$, and for $\sigma \in S_k$, we define

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

where $\sigma = \prod_{i=1}^n \sigma_i$ is the decomposition of σ into cycles with disjoint supports, and where we have set, if $\sigma = (j_1, \dots, j_r) \in S_k$ is a cycle,

$$T_{[\sigma]}(\underline{x}) = T(x_{j_1} \dots x_{j_r}).$$

Note that a cycle may be written in several ways (j_1, \dots, j_r) , but using (ii) we check at once that $T_{[\sigma]}$ is well defined. Finally, we set

$$S_k(T)(\underline{x}) = \sum_{\sigma \in S_k} \epsilon(\sigma) T_\sigma(\underline{x}).$$

Example 2.1.

$$S_1(T)(x, y) = T(xy) - T(x)T(y).$$

$$S_2(T)(x, y, z) = T(xyz) - T(xy)T(z) - T(xz)T(y) - T(yz)T(x) + T(xy)T(z) + T(xz)T(y) + T(yz)T(x).$$

So $S_k(T)$ is a multilinear form in k variables in R over A . It is easily seen to be symmetric.

thmfrobenius

Theorem 2.1 (Frobenius). *If T is the character of a representation $\rho : R \rightarrow M_d(A)$, then*

$$S_k(T)(\underline{x}) = 0 \text{ for all } k \geq d + 1 \text{ and all } \underline{x} \in R^k.$$

Proof — (This proof is due to Rouquier.) It is obviously enough to prove this identity when $R = M_d(A)$, $\rho = \text{Id}$, that is T is the trace map. It is also enough to prove it for A the ring $A_{\text{univ}} := \mathbb{Z}[(X_{i,j,l})_{i,j \in \{1, \dots, d\}, l \in \{1, \dots, k\}}]$ 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 $A_{\text{univ}} \rightarrow A$ 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 $\underline{x}_{\text{univ}} = ((X_{i,j,1})_{i,j}, \dots, (X_{i,j,k})_{i,j})$ of $M_d(A_{\text{univ}})^k$.

It is then 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 multi-linear and symmetric, it is enough to prove by polarization that $S_k(T)(x, \dots, x) = 0$ for all $x \in M_d(A)$. 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 S_k . Those two operations commute.

We compute the trace of the operator $x\sigma$ on this space. If we denote by (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

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

This contributes to the trace if and only 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 $\sigma_1, \dots, \sigma_n$ (where n is the number of cycles of σ). For $l = 1, \dots, n$, note a_l the common value of 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 $e_{i_1} \otimes \dots \otimes e_{i_k}$ 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

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

Let $P = \sum_{\sigma \in S_k} \epsilon(\sigma) x\sigma$. By the above, we compute easily the trace of P on $V^{\otimes k}$:

$$\text{tr}(P) = \sum_{\sigma \in S_k} \epsilon(\sigma) T(x^{c_1(\sigma)}) \dots T(x^{c_{n(\sigma)}(\sigma)}),$$

where $n(\sigma)$ is the number of cycles in σ and the $c_l(\sigma)$'s are the orders of those cycles. Thus we have

$$\text{tr}(P) = S_k(T)(x, \dots, x).$$

But on the other hand $P = x \sum_{\sigma \in S_k} \epsilon(\sigma) \sigma$ 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 except 0, hence $P = 0$, and $\text{tr} P = 0$. Hence

$$S_k(T)(x, \dots, x) = 0.$$

□

2.2. Characteristic polynomial.

Lemma 2.1 (Newton). *There exist unique polynomials*

$$a_0, \dots, a_{d-1} \in \mathbb{Z}[1/d!][S_1, \dots, S_d]$$

such that for every complex numbers $\alpha_1, \dots, \alpha_d$, if $s_n = \sum_{i=1}^d \alpha_i^n$ for $n = 1, \dots, d$, then the polynomial $X^d + a_{d-1}(s_1, \dots, s_d)X^{d-1} + \dots + a_0(s_1, \dots, s_d)$ has roots $\alpha_1, \dots, \alpha_d$, a root being repeated in this list according to its multiplicity.

The proof is left as an exercise. We use this lemma to define the characteristic polynomial in our context:

Definition 2.1. Let $T : R \rightarrow A$ be a central function such that $T(1) = d$. Assume that $d!$ is invertible in A . If $x \in R$, we set

$$P_{x,T}(X) = X^d + a_{d-1}(T(x), \dots, T(x^d))X^{d-1} + \dots + a_0(T(x), \dots, T(x^d)) \in A[X]$$

and we call this polynomial $P_{x,T}$ the *characteristic polynomial* of x for T .

Indeed, when $T = \text{tr } \rho$ for $\rho : R \rightarrow M_d(A)$, then $P_{x,T}$ is the characteristic polynomial of $\rho(x)$ (easy exercise).

Example 2.2. If $d = 1$, then $P_{x,T}(X) = X - T(x)$. If $d = 2$, then $P_{x,T}(X) = X^2 - T(x)X + \frac{T(x)^2 - T(x^2)}{2}$.

The relation between the characteristic polynomial and the multi-linear function S_k defined in the preceding paragraph is given by:

thmSdq

Theorem 2.2. *Let $T : R \rightarrow A$ be a central function such that $T(1) = d$. Assume that $d!$ is invertible in A . Then for any x and y in R , we have*

SP

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

Proof — Let us have a look to the expressions $S_{d+1}(T)(x, \dots, x, y)$. By definitions, this is a sum of terms, one for each $\sigma \in S_{d+1}$, of the form

$$\epsilon(\sigma)T(x^{c_1})T(x^{c_2}) \dots T(x^{c_{n-1}})T(x^{c_n-1}y)$$

where c_1, \dots, c_n are the order of the cycles of σ , c_n being the order of the cycle having d_1 in its support. Let $Q_{x,T}(X)$ be the sum, over all $\sigma \in S_{d-1}$, of the monomials

$$\epsilon(\sigma)T(x^{c_1})T(x^{c_2}) \dots T(x^{c_{n-1}})X^{c_n-1}.$$

Then by construction, $Q_{x,T}$ is a polynomial in X whose dominant term is $(-1)^d d! X^d$ (every cycle of order $d + 1$ gives one term $(-1)^d X^d$), and which satisfies

Sdq

$$(2) \quad S_{d+1}(T)(x, \dots, x, y) = T(Q_{x,T}(x)y).$$

To prove $\stackrel{\text{SP}}{(\text{I})}$, it just remains to prove that $Q_{x,T} = (-1)^d d! P_{x,T}$. Those are two polynomials of the same degree and same dominant coefficient whose coefficients are given by universal polynomials in the variables $T(1), \dots, T(x^d)$. Therefore,

reasoning as in the proof of Theorem ^{thmfrobenius}2.1, it is enough to prove the result when $A = \mathbb{C}$, $R = M_d(\mathbb{C})$, $T = \text{tr}$, and $x = \text{diag}(\lambda_1, \dots, \lambda_d)$ with the λ_i complex numbers, that we can even assume distinct. By Theorem ^{thmfrobenius}2.1 and equation ^{Sdq}(2), we have $T(Q_{x,T}(x)y) = 0$ for all $y \in M_d(\mathbb{C})$ so $Q_{x,T}(x) = 0$. It follows that the minimal polynomial of x , which is in this case the same as its characteristic polynomial $P_{x,T}(X)$ divides $Q_{x,T}(x)$. Looking at degrees and dominant coefficients, we thus have $Q_{x,T} = (-1)^d d! P_{x,T}$. \square

Remark 2.1. It is also possible, but tedious, to prove that $Q_{x,T} = (-1)^d d! P_{x,T}$ (hence the above theorem) by direct computations, without using Theorem ^{thmfrobenius}2.1. Doing so we indeed get a new proof, perhaps more intuitive, of Theorem ^{thmfrobenius}2.1, since by Cayley-Hamilton's theorem (after reduction to the case $R = M_d(\mathbb{C})$ and $T = \text{tr}$), we have $P_{x,T}(x) = 0$, from which it follows using Theorem ^{thmSdq}2.2 that $S_{d+1}(T)(x, \dots, x, y) = 0$ for all $x, y \in R$, which implies by polarization that $S_{d+1}(T)(\underline{x}) = 0$ for all $\underline{x} \in R^{d+1}$. To conclude that $S_k(T) = 0$ for all $k > d$, one uses the following easy lemma.

lemmaSkk

Lemma 2.2. *For any central function $T : R \rightarrow A$, and k an integer, we have*

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

In particular, if $S_k(T)(\underline{x}) = 0$ for all $\underline{x} \in R^k$, and $k' \geq k$, then $S_{k'}(\underline{x}) = 0$ for all $\underline{x} \in R^{k'}$.

Proof — The equality follows easily by cutting the sum defining $S_{k+1}(T)$ into $(k+1)$ parts, the first one being the sub-sum on the σ 's such that $\sigma(k+1) = k+1$ (which gives the first term in the RHS of the formula) and the k other ones being on the σ such that $\sigma(k+1) = i \neq k+1$ (which gives the i -th term in the sum in the RHS). The second assertion follows by induction on $k' - k$. \square

2.3. Pseudocharacters.

2.3.1. *Definition and first properties.* Let A be a commutative ring, and R an A -algebra

Definition 2.2. A central function $T : R \rightarrow A$ is a *pseudocharacter* if there exists an integer k such that $S_{k+1}(T)(\underline{x}) = 0$ for all $\underline{x} \in R^{k+1}$, and $k!$ is invertible in A . The *dimension* of a pseudocharacter is the smallest d such that $S_{d+1}(T)(\underline{x}) = 0$ for all $\underline{x} \in R^{d+1}$.

Remark 2.2. Using those definitions without the assumption that $k!$ is invertible leads to catastrophes. The correct definitions, if one wants to work with pseudocharacters of dimension greater than the characteristics, have to be quite different: see $\frac{\text{determinants}}{[\mathbb{C}]}$.

Note that a pseudocharacter of dimension d satisfies $S_k(T) = 0$ for all $k \geq d+1$ by Lemma $\frac{\text{lemmaSkk}}{2.2}$. By the Frobenius identity, if $\rho : R \rightarrow M_d(A)$ is a representation, and $d!$ is invertible in A , then $T = \text{tr } \rho$ is a pseudocharacter of dimension at most d . To prove it is of dimension d , we shall need the following important result.

dimT **Proposition 2.1.** *If T is a pseudocharacter of dimension d , and if $A \rightarrow A'$ is any morphism of commutative rings with A' local, then the image of $T(1)$ in A' is d . In particular, if A is itself local, then $T(1) = d$.*

Proof — We use that $S_{d+1}(T)(1, \dots, 1) = 0$. Obviously $T_\sigma(1, \dots, 1) = T^{n(\sigma)}(1)$ where $n(\sigma)$ is the number of cycles in σ . We thus have

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

where $s(d+1, n)$ is the number of $\sigma \in S_{d+1}$ with exactly n numbers. The numbers $s(d+1, n)$ are the so-called *Stirling numbers of the first kind*, and the polynomial $St_{d+1}(X) = \sum_{n=1}^{d+1} s(d+1, n)X^n$ is called the Stirling polynomial. It is proved in any introductory class in combinatorics that $St_{d+1}(X) = X(X-1)\dots(X-d)$. We can get a direct proof of this by observing that $St(X)$ is a monic integral polynomial of degree $d+1$, with 0 as an obvious root, so it is enough to check that $St_{d+1}(d') = 0$ for $d' = 1, \dots, d$. But considering the trace map $\text{tr} : M_{d'}(\mathbb{C}) \rightarrow \mathbb{C}$, for $d' = 1, \dots, d$, which satisfies $S_{d+1}(\text{tr}) = 0$ by Theorem $\frac{\text{thmfrobenius}}{2.1}$, we get by the above considerations that $St_{d+1}(d') = 0$.

We thus have proved $T(1)(T(1) - 1)\dots(T(1) - d) = 0$. Remember that $d!$ is invertible in A hence in A' , so the difference of any two factors in the above product is invertible in A' . It follows that at most one of those factor can be in the maximal ideal m of A' and exactly one is, otherwise their products would be invertible. So $T(1) - d'$, say, is in m . But then, the other factors are not in m , so are invertible, and we thus get $T(1) = d'$ in A' for d' some integer between 0 and d .

To conclude the proof, we use Lemma $\frac{\text{lemmaSkk}}{2.2}$ with $x_{d+1} = 1$, getting $0 = (T(1) - d)S_d(T)(x_1, \dots, x_d)$ for all $(x_1, \dots, x_d) \in R^d$. But since T has dimension d , for some $(x_1, \dots, x_d) \in R^d$ we have $S_d(T)(x_1, \dots, x_d) \neq 0$, so $T(1) - d = d' - d$ is not invertible in A' . The only possibility is $d' = d$, so $T(1) = d$ in A' . \square

Definition 2.3. If $T : R \rightarrow A$ is a linear map, and A' any commutative A -algebra, then we write $T \otimes A'$ for the function $T \otimes 1 : R \otimes_A A' \rightarrow A'$.

Corollary 2.1. *If $T : R \rightarrow A$ is a pseudocharacter of dimension d , then so is $T \otimes_A A'$.*

Proof — It is obvious that $T \otimes A'$ is a central function satisfying $S_{d+1}(T \otimes A') = 0$, and that $d!$ is invertible in A' . Therefore $T \otimes A'$ is a pseudocharacter of dimension d' , with $d' \leq d$. But since $T \otimes A'(1) = T(1) = d$ by the proposition, we have $d' = d$. \square

Theorem 2.3. *If $\rho : R \rightarrow M_d(A)$ is a representation, and $d!$ is invertible in A , then $T = \text{tr } \rho$ is a pseudocharacter of dimension d*

Proof — As we have noted, we know that T is a pseudocharacter of some dimension $d' \leq d$, and we have to prove that $d' = d$. But obviously $T(1) = d$. Choosing a field K with a morphism $A \rightarrow K$ (Krull's lemma), we see by the Proposition that $T(1) = d'$ in K . So $d' = d$ in K and since $d!$ is invertible in K , $d' = d$ as integers. \square

The next subsections will be devoted to the proof of partial converses of this result. We need first some preliminaries.

prel

2.3.2. *Kernel, faithful pseudocharacters, and the Cayley-Hamilton theorem.* Recall that the *kernel* of T is $\ker T = \{x \in R, T(xy) = 0 \forall y \in R\}$. It is a two-sided ideal of A (since $T(xy) = T(yx)$), and T factors through the quotient $R/\ker T$ and define a pseudocharacter $T : R/\ker T \rightarrow A$ which is *faithful*, that is which has trivial kernel.

To get an intuition on the notion of kernel, the following lemma, due to Taylor, may be useful.

kerker

Lemma 2.3. *Let k be a field, R a k -algebra, and $\rho : R \rightarrow M_d(k)$ a representation that is semi-simple. We assume that $\text{char } k > d$, so that $T = \text{tr } \rho$ is a pseudocharacter. Then $\ker T = \ker \rho$.*

We leave the prove as an exercise.

Proposition 2.2. *If T is faithful, then for every $x \in R$, $P_{x,T}(x) = 0$*

Proof — Setting all the variables but one in the definition of a pseudocharacters of dimension d equal to x , and the last one equal to y , we have $T(P_{x,T}(x)y) = 0$. Therefore $P_{x,T}(x) \in \ker T = 0$. \square

We shall refer to this result as "the Cayley-Hamilton's theorem".

2.3.3. *Idempotents and pseudocharacters.* In the following set of lemmas, we assume that A is local (of maximal ideal m), and e is an idempotent of R (that is $e^2 = e$)

Lemma 2.4. *$T(e)$ is an integer between 0 and d .*

The proof is exactly as the first part of the proof of Prop [2.1](#).

Lemma 2.5. *The restriction T_e of T to the A -algebra eRe (with unity e) is a pseudocharacter of dimension $T(e)$.*

Indeed, it is clear that T_e is a pseudocharacter. Its dimension is its value on the unity, hence $T(e)$.

Lemma 2.6. *If T is faithful, and $T(e) = 0$ then $e = 0$.*

Indeed, if $T(e) = 0$, then $T(e^n) = 0$ for all n , so $P_{e,T}(X) = X^d$, and by Cayley-Hamilton, $e^d = 0$, so $e = 0$.

Lemma 2.7. *If T is faithful, 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 2.8. *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, $x = 0$.

2.4. Taylor's theorem.

Theorem 2.4. *If $A = k$ is a separably closed field, and $T : R \rightarrow k$ is a pseudocharacter of dimension d , then $T = \text{tr } \rho$ for a unique semi-simple representation $\rho : R \rightarrow M_d(A)$.*

Actually, this is a theorem of Taylor only if k has characteristic 0. It is due to Rouquier in characteristic p (with $p > d$ of course). The uniqueness of ρ has been proved in Kisin's lecture. Therefore I prove only the existence of ρ . The fundamental idea (of Rouquier's proof) is to investigate the structure of the algebra $R/\ker T$.

Lemma 2.9. *The radical J of $R/\ker T$ is trivial*

Proof — Let $x \in J$. 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 J , so $1+xQ(x)$ is invertible, and we get $x^i = 0$.

The second point is that a nilpotent element x in $R/\ker T$ has $T(x) = 0$. There are many proofs of this fact. Here is one : we may assume by induction that $x^2 = 0$,

and then putting in the definition of a pseudocharacter all the variables equal to x , one gets $T(x)^{d+1} = 0$. But k is a field.

Putting those two points together, we see that every element x of the radical J has $T(x) = 0$. For every $y \in R/\ker T$, xy is also in the radical thus we have $T(xy) = 0$. So $x = 0$. \square

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

Proposition 2.3. *$R/\ker T$ is isomorphic to a product of matrix algebras over k : $M_{d_1}(k) \times \cdots \times M_{d_r}(k)$.*

Note that a classical result states that semi-simple finite-dimensional algebras over k are of this form. 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 implies that there is at most d isomorphism classes of irreducible modules over $R/\ker T$. If V is one of them, then $D := \text{End}_k(V)$ is a division algebra, by Schur's lemma, and the center of D is a separable extension of k . Seeing V as a right- D -vector space, 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 right- D -subspace V' of V of arbitrary high finite dimension. Actually V can not be infinite dimensional because if it was, the image of $R/\ker T$ would contain a matrix algebra $\text{End}_D(V')$ for some V' of D -dimension greater than d , hence elements not killed by any monic polynomial of degree d , a contradiction.

Hence V is finite-dimensional over D and $R \rightarrow \text{End}_D(V)$ is surjective. Since the opposite algebra D^0 of D is isomorphic to a sub-algebra of $\text{End}_D(V)$, we see that every element in D^0 , hence of D , is algebraic over k . Hence D is commutative, that is is a field and is equal to its center, and as we have noted is separable over k . So $D = k$. Hence $\text{End}_D(V) = \text{End}_k(V)$ is a matrix algebra over k .

We see easily, since $R/\ker T$ is semi-simple, that it is isomorphic to the product of $\text{End}_k(V_i)$ where the V_i are the different simple modules over R . \square

Finally we prove Taylor's theorem: we may replace R by $R/\ker T$, 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. Let e_1, \dots, e_r be the idempotents of $R/\ker T$ given by the identity elements of the matrix algebras $M_{d_i}(k)$, so that $e_1 + \cdots + e_r = 1$, and the e_i are orthogonal idempotents. One thus has $T(x) = \sum_{i,j} T(e_i x e_j) = \sum_{i=1}^r T(e_i x e_i)$ since $T(e_i x e_j) = T(e_j e_i x) = 0$ if $i \neq j$. The map

$x \mapsto T(e_i x e_i)$ is a pseudocharacter on $R/\ker T$ that is equal to the restriction T_{e_i} of T on the component $e_i R e_i$ and is 0 elsewhere. Therefore we are reduced to proving that each pseudocharacter T_{e_i} is the trace of a representation of $e_i R e_i \simeq M_d k$, which is done by the following lemma:

Lemma 2.10. *A pseudocharacter $M_d(k) \rightarrow k$ is an integral multiple of the trace, hence is the trace of a sum of copies of the standard representation.*

Indeed, it is an easy exercise to see that a linear form T on $M_{d_i}(k)$ that satisfies $T(xy) = T(yx)$ is a multiple of the trace, say αtr for $\alpha \in k$. Applying this to an idempotent e of trace 1 in $M_{d_i}(k)$, we get $\alpha = T(1)$. But we know that $T(1)$ is an integer.

This concludes the proof of existence in Taylor's theorem. As a corollary of the proof, we get that if T is irreducible (that is not the sum of two pseudo-characters of smaller dimensions), then $R/\ker T \simeq M_d(k)$.

2.5. Proof of Rouquier and Nyssen's theorem.

Theorem 2.5. *Let $T : R \rightarrow A$ be a pseudocharacter of dimension d . Assume that A is local and strictly Henselian², with residue field k . Assume that $\bar{T} := T \otimes 1 : R \otimes_A k \rightarrow k$ is irreducible (not the sum of two non-zero pseudocharacters). Then $R/\ker T \simeq M_d(A)$, and T is the trace of a unique representation, namely $R \rightarrow R/\ker T = M_d(A)$.*

The uniqueness is due to Mazur and Serre and Carayol, the existence of the representation and the result on $R/\ker T$ are due independently to Nyssen and Rouquier.

For the proof, we may as well replace R by $R/\ker(T)$, which simplifies notations and add the hypothesis that T is faithful over R . By the above §, we have that $(R \otimes k)/\ker \bar{T} \simeq M_d(k)$.

As in the case of a field, the starting point is to understand the radical of R .

radical

Lemma 2.11. *If $T : R \rightarrow A$ is faithful, and A, T as above, then the radical J of R is the inverse image of $\ker \bar{T}$ in R . In other words, $R/J = (R \otimes_A k)/\ker \bar{T} \simeq M_d(k)$.*

Proof — Let J' denote the inverse image of $\ker \bar{T}$ in R . It is a two-sided ideal of R . Since $R \otimes k/(\ker \bar{T})$ is a matrix algebra $M_d(k)$, hence is semi-simple, we have $J \subset J'$.

Let $x \in J'$. We will show that $1 + x \in R^*$. We have $T(xy) \in m$, for all 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

²Henselian means that Hensel's lemma is true in A . For example, if A is complete, then it is henselian. Strictly means that the residue field k is separably closed. If not, it is a basic result that we can replace A by an étale extension which is local and strictly henselian

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 $J' \subset J$. \square

After this lemma we are almost done: in $R/J \simeq M_d(k)$ we have the elementary matrices $E_{i,j}$, for $i, j \in \{1, \dots, d\}$. They 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 (this is the basic fact used for example in the theory of Azumaya algebra) that we can lift those elements of R/J into elements of R that we shall still denote $E_{i,j}$ that satisfy the same relations. (This works since J is the radical of R , since R is integral over A , and since A is Henselian. The proof of this "basic fact" is a clever application of Hensel's lemma. cf ^{pourbaki2} [Bou2][Chap. III, §4, exercice 5(c)]).

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 $T(1) = d$, so all the $T(E_{i,i})$ are 1. From this we deduce that the restriction of $T_{E_{i,i}}$ of T to $E_{i,i}RE_{i,i}$ is a faithful pseudocharacter of dimension 1. But clearly this shows that $E_{i,i}RE_{i,i}$ is isomorphic to A as an A -algebra ($T_{E_{i,i}}$ being such an isomorphism). 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 -algebras. This proves the first part of the theorem, from which it is easy to deduce that T is the trace of a representation, as we did in the case of a base field.

2.6. Exercises.

Exercise 2.1. Check formula ^(SP) (II) by direct computations in the cases $d = 1$ and $d = 2$.

Exercise 2.2. Prove Lemma ^{kerker} 2.3. Prove that the hypothesis that ρ is semi-simple cannot be removed.

tb **Exercise 2.3.** If A' is a commutative A -algebra, show that $T \otimes A' : R \otimes A' \rightarrow A'$ is a pseudocharacter of dimension d . Show that if T is faithful and A' is A -flat, then $T \otimes A'$ is faithful. Show that this result may be false when A' is not A -flat.

Exercise 2.4. Let $A = \mathbb{R}$ and \mathbb{H} be the field of quaternions. Show that $T : \mathbb{H} \rightarrow \mathbb{R}$, $T(a + bi + cj + dk) = a$ is a pseudocharacter on \mathbb{H} that does not come from a representation.

Exercise 2.5. Test: Let k be an algebraically closed field, and R a k -algebra. If $T : R \rightarrow k$ is a pseudocharacter of dimension d , and $R/\ker T = M_n(k)$ for some n , is T necessarily irreducible?

Exercise 2.6. Show that Proposition ^{dimT}2.1 remains true if we weaken the assumption that A' is local into *Spec A' is connected*. But show that if $\text{Spec } A'$ is not connected, the result may be false.

Exercise 2.7. If $T : R \rightarrow A$ is a pseudocharacter, we call $\text{CH}(T)$ the two-sided ideal of R generated by the $P_{x,T}(x)$ for $x \in R$. We say that T is *Cayley-Hamilton* if $\text{CH}(T) = 0$.

a.– Show that $\text{CH}(T) \subset \ker T$. Show that faithful implies Cayley-Hamilton.

b.– Deduce that T factors through a pseudocharacter $T : R/\text{CH}(T) \rightarrow A$, which is Cayley-Hamilton.

c.– Show that with the notation of exercise ^{tb}2.3, we have $\text{CH}(T \otimes A') = \text{CH}(T)A'$ (even when A' is not A -flat). In particular, if T is Cayley-Hamilton, then so is $T \otimes A'$.

d.– (**difficult**) If $T : R \rightarrow A$ is Cayley-Hamilton, and $R/\ker T \simeq M_d(A)$, then T is faithful and $R \simeq M_d(A)$.

e.– (**difficult**) Deduce the global form of Rouquier's theorem (with a slightly simpler proof than Rouquier's) : If A is any commutative ring (with $d!$ invertible in A), and $T : R \rightarrow A$ is a pseudocharacter of dimension d such that at every closed point m of $\text{Spec } A$, $T \otimes 1 : R \otimes A/m \rightarrow A/m$ is absolutely irreducible, then $R/\ker T$ is an Azumaya algebra over A (Remark: if you don't know what is an Azumaya algebra, that's not a problem. You only need to know that an algebra over A whose base change to any local ring at closed points of $\text{Spec } A$ is a matrix algebra M_d is an Azumaya algebra)

Exercise 2.8. a.– Let k be a field, and $T : R \rightarrow k$ be a pseudocharacter. Assume that the $T \otimes 1 : R \otimes \bar{k} \rightarrow \bar{k}$ is the trace of a representation ρ that is irreducible. (We say that T is absolutely irreducible). Show that $R/\ker T$ is a central simple algebra. (You might need to use exercise ^{tb}2.3)

b.– By mimicking the proof of Rouquier-Nyssen theorem, show that if A is a local Henselian ring with finite residue field k , and $T : R \rightarrow A$ is a pseudocharacter such that \bar{T} is absolutely irreducible, then T is the trace of a representation. (This statement contains the one used by Mark Kisin (^{KHawaii}[K])).

3. RESIDUALLY MULTIPLICITY-FREE PSEUDOCHARACTERS

(Results from this section are from ^{BC}[BC, Chapter 1].)

We keep the notations of Rouquier and Nyssen's theorem: $T : R \rightarrow A$ be a pseudocharacter of dimension d . the ring A is a local and strictly henselian ring, with

residue field k , maximal ideal m . To simplify the exposition, we shall also assume that A is noetherian and reduced (none of these hypotheses is really necessary), and we call K its total fraction ring: K is a finite product of fields.

Rouquier and Nyssen's theorem is fine, but for the generalizations of Ribet's lemma it is not enough: we need to work without the assumption that $\bar{T} = T \otimes 1 : R \otimes k \rightarrow k$ is irreducible.

If \bar{T} is not irreducible, it is a sum of irreducible characters, each of them being, by Taylor-Rouquier's theorem, the trace of a unique irreducible representation. So we can write

$$T = \text{tr}(\bar{\rho}_1 \oplus \cdots \oplus \bar{\rho}_r).$$

We shall call d_1, \dots, d_r the dimensions of $\bar{\rho}_1, \dots, \bar{\rho}_r$, so that $d_1 + \cdots + d_r = d$.

We will make the following simplifying assumption: for $i \neq j$, $\bar{\rho}_i \not\cong \bar{\rho}_j$. We call a T that satisfies this hypothesis *residually multiplicity free*. Important part of the theory we shall expose below can be done without this hypothesis, that is for general T (see ^{determinants} [C]), but the theory is simpler and more complete in the residually multiplicity free case and this case is sufficient for our purposes.

Our aim is, for T residually multiplicity free as above, to study, as we have done in the more specific cases, the structure of $R/\ker T$ (we shall see this way that such T are not necessarily trace of representations), to define and show how to compute the (total) reducibility locus of T in $\text{Spec } A$ (the maximal closed subscheme on which T is as reducible as it is at the closed point), and to prove the analog of Ribet's lemma (how we can use T to construct non-trivial extensions between the $\bar{\rho}_i$)

structure

3.1. The structure theorem. We shall determine the structure of the A -algebra $R/\ker T$. It will not always be a matrix algebra $M_d(A)$. Instead, it will be a generalized matrix algebra (of type d_1, \dots, d_r) in the following sense:

Lemma and Definition 3.1. Let $A_{i,j}$, $i, j = 1, \dots, r$ be fractional ideals of A (that is finite type A -submodules of K) such that

- (a) $A_{i,i} = A$ for all i
- (b) $A_{i,j}A_{j,k} \subset A_{i,k}$ for all i, j, k .
- (c) $A_{i,j}A_{j,i} \subset m$ for all i, j , $i \neq j$.

Consider elements a of $M_d(K)$ as matrices by blocks of size (d_1, \dots, d_r) : call $a_{i,j} \in M_{d_i, d_j}(K)$ the block (i, j) of the matrix a . Let S be the subset of $M_d(K)$ of elements a such that all the entries of $a_{i,j}$ are in $A_{i,j}$. That is to say:

$$S = \left(\begin{array}{cccc} M_{d_1}(A_{1,1}) & M_{d_1, d_2}(A_{1,2}) & \cdots & M_{d_1, d_r}(A_{1,r}) \\ M_{d_2, d_1}(A_{2,1}) & M_{d_2}(A_{2,2}) & \cdots & M_{d_2, d_r}(A_{2,r}) \\ \vdots & \vdots & \ddots & \vdots \\ M_{d_r, d_1}(A_{r,1}) & M_{d_r, d_2}(A_{r,2}) & \cdots & M_{d_r}(A_{r,r}) \end{array} \right)$$

Then

- (i) S is a A -subalgebra of $M_d(K)$ (with same unity Id).
- (ii) The trace $\text{tr} : M_d(K) \rightarrow K$ induces a map $\mathbf{tr} : S \rightarrow A$ which is a pseudo-character of dimension d .
- (iii) The map $r_i : S \otimes_A k \rightarrow M_{d_i}(k)$ induced by $a \mapsto a_{i,i}$ is an irreducible representation of $S \otimes_A k$, and $r_i \not\cong r_j$ if $i \neq j$. We have $\mathbf{tr} = \text{tr } r_1 + \cdots + \text{tr } r_d$. In particular, the pseudo-character \mathbf{tr} is residually multiplicity free.

The algebra S is called the *generalized matrix algebra* of type (d_1, \dots, d_r) , attached to the families of fractional ideal $(A_{i,j})$.

Proof — It is clear that S is an A -submodule, and properties (b) show that S is stable by multiplication, while (a) shows that S contains Id . This proves (i). Property (a) implies that \mathbf{tr} sends S to A , and it is a pseudocharacter of dimension d since $\text{tr} : M_d(K) \rightarrow K$ is and $\mathbf{tr}(1_S) = d$. This proves (ii). A simple computation using (c) shows that r_i is a morphism of algebras, and since it is clearly surjective, it is an irreducible representation. The rest of (iii) is clear. \square

structurethm

Theorem 3.1. *Let $T : R \rightarrow A$ be a residually multiplicity free pseudocharacters as above. There exists a generalized matrix algebra S of type (d_1, \dots, d_r) attached to a family of fractional ideals $(A_{i,j})$ as above, and an A -isomorphism of algebras $f : R/\ker T \rightarrow S$ such that $\mathbf{tr} \circ f = T$.*

Remark 3.1. The ideals $A_{i,j}$ are not uniquely determined. Actually it is clear that if $(x_i)_{i=1, \dots, r}$ is a families of elements of K^* , then the ideals

trans

$$(3) \quad A'_{i,j} = x_i^{-1} x_j A_{i,j}$$

satisfy the same relations (a), (b), (c), and that the generalized matrix algebra S' attached to the $(A'_{i,j})$ is A -isomorphic to S with an isomorphism compatible with traces. So we can change the $A_{i,j}$ up to a transformation $\overset{\text{trans}}{(3)}$. Actually, it can be shown that the family $(A_{i,j})$ is well-defined, up to a transformation of the type $\overset{\text{trans}}{(3)}$.

We shall use this theorem again and again. For T a residually multiplicity-free pseudocharacter, we shall call $A_{i,j}$ fractional ideals as in the theorem. The fact that the $A_{i,j}$ are well-determined only up to a transformation of type $\overset{\text{trans}}{(3)}$ will not matter, since as the reader can check, all constructions using the $A_{i,j}$ below will actually be invariant by this transformation.

Proof — (Sketch) We can and do assume that T is faithful. We now want to prove that R is a generalized matrix algebra of type (d_1, \dots, d_r) .

Since the character $\bar{T} : R \otimes_A k \rightarrow k$, $\bar{T} = \text{tr } \bar{\rho}_1 \oplus \cdots \oplus \text{tr } \bar{\rho}_r$ is the sum of r non isomorphic representations, we have (see the proof of Taylor's theorem above) $(R \otimes k)/\ker \bar{T} = \bar{\rho}_1(R \otimes k) \times \cdots \times \bar{\rho}_r(R \otimes k) = M_{d_1}(k) \times \cdots \times M_{d_r}(K)$. Let ϵ_i be the identity of $M_{d_i}(K)$ seen as an element of $R/\ker \bar{T}$. Then the ϵ_i 's form an orthogonal family of idempotents of sum 1. Recall that by Lemma $\overset{\text{radical}}{2.11}$, the kernel

of the surjective map $R \rightarrow R \otimes k \rightarrow (R \otimes k)/\ker \bar{T}$ is the radical J of R . Therefore, we can lift the families ϵ_i to a families e_i of orthogonal idempotents of R of sum 1.

Looking at the subalgebra $e_i R e_i$ of R (with unity e_i) and mimicking the proof of Rouquier-Nyssen's theorem, it is not hard to prove that $e_i R e_i \simeq M_{d_i}(A)$ for all $i = 1, \dots, r$ (by considering the elementary matrices $E_{\alpha, \beta} \in M_{d_i}(k)$ seen as elements of $(R \otimes k)/\ker \bar{T}$ and by lifting them to $e_i R e_i$).

Now if $i \neq j$, then $e_i R e_j$ as an obvious structure of left $e_i R e_i \simeq M_{d_i}(A)$ -module and right $e_j R e_j \simeq M_{d_j}(A)$. By Yoneda's theory, $e_i R e_j$ is isomorphic, for its bimodule structure, to $M_{d_i, d_j}(A_{i,j})$ for some A -modules $A_{i,j}$.

Moreover, the multiplication in R induces map $e_i R e_j \otimes e_j R e_k \rightarrow e_i R e_k$. Again by Yoneda's theory, those maps are induced by morphisms of A -modules $\psi_{i,j,k} : A_{i,j} \otimes_A A_{j,k} \rightarrow A_{i,k}$.

So we already can write $R = \oplus_{i,j} e_i R e_j \simeq \oplus_{i,j} M_{d_i, d_j}(A_{i,j})$. Here the \simeq is an isomorphism of algebra, where the right hand side is given an algebra structure using matrix multiplication and the $\psi_{i,j,k}$. To check that the RHS is a generalized matrix algebra, we only have to prove that the A -modules $A_{i,j}$ are finite type and can be embedded in K in such a way that the maps $\psi_{i,j,k} : A_{i,j} \otimes_A A_{j,k} \rightarrow A_{i,k}$ becomes induced by the multiplication of K . We refer to [\[BC\]](#) for that. \square

red

3.2. Total reducibility locus.

Theorem 3.2. *Let $T : R \rightarrow A$ be a residually multiplicity free characters as above. There exists a smallest ideal I of A , such $T \otimes 1 : R \otimes A/I \rightarrow A/I$ is the sum of r non-zero pseudocharacters. We have*

$$I = \sum_{\substack{i,j=1,\dots,r \\ i \neq j}} A_{i,j} A_{j,i},$$

where the fractional ideals $A_{i,j}$ are as in the structure theorem.

For the proof, that relies heavily on the structure theorem, see [\[BC\]](#). We just note that, with the notation of the structure theorem, if

$$\sum_{\substack{i,j=1,\dots,r \\ i \neq j}} A_{i,j} A_{j,i} \subset I,$$

then it is easy to see that $T \otimes 1 : R \otimes A/I \rightarrow A/I$ is the sum of r non-zero pseudocharacters. Indeed, the maps $r_i : R \xrightarrow{f} S \rightarrow M_{d_i}(A/I)$ induced by $a \mapsto a_{i,i} \pmod{I}$ are easily seen to be morphisms of algebras, so their traces $\text{tr } r_i$ define pseudocharacters $R \otimes A/I \rightarrow A/I$ (of dimension d_i) and one has $T \otimes 1 = \sum_{i=1}^r \text{tr } r_i$ in A/I . What is harder is to prove the converse: that is, if for some ideal I , $T \otimes 1 : R \otimes A/I \rightarrow A/I$ is the sum of r characters, then $\sum_{\substack{i,j=1,\dots,r \\ i \neq j}} A_{i,j} A_{j,i} \subset I$.

Definition 3.1. We call I the (total) *reducibility ideal* of T and $\text{Spec } A/I$ the (total) *reducibility locus* of T .

Remark 3.2. (i) We can consider other reducibility conditions. For example, for $1 < s \leq r$, we can ask whether there exists a smallest ideal I such that $T \otimes 1 : R \otimes A/I \rightarrow A/I$ is the sum of s non-zero pseudocharacters. Or, given a partition of $\{1, \dots, r\} = P_1 \amalg P_2 \amalg \dots \amalg P_s$, we can ask whether there exists a smallest ideal I such that $T \otimes 1 : R \otimes A/I \rightarrow A/I$ is the sum of s non-zero pseudocharacters T_1, \dots, T_s such that for $l = 1, \dots, s$, $T_l \otimes 1 : R \otimes k \rightarrow k$ is equal to $\sum_{i \in P_l} \text{tr } \rho_i$. It can be shown that those generalized reducibility ideals always exist. For example, for the one attached to a partition $P_1 \amalg \dots \amalg P_s$, the smallest I is

$$\sum_{i, j \text{ not in the same } P_l} A_{i,j} A_{j,i}.$$

(ii) If we do not assume that T is residually multiplicity free, the reducibility ideal may not exist.

Finally, let J be any proper ideal of A containing the (total) reducibility ideal of T . The pseudocharacter $T \otimes 1 : R \otimes A/J \rightarrow A/J$ is the sum of r pseudocharacters $T_1, \dots, T_r : R \otimes A/J \rightarrow A/J$. Up to renumbering the T_i , we can assume that $\bar{T}_i = T_i \otimes 1 : R \otimes k \rightarrow k$ is $\text{tr } \bar{\rho}_i$. It can be shown that the T_i are unique, that is we do not have another decomposition of $T \otimes 1$ as a sum of r pseudocharacters. By Rouquier and Nyssen's theorem, there exists a unique representation $\rho_i : R \otimes A/J \rightarrow M_{d_i}(A/J)$ of trace T_i . The representation ρ_i is a lift (or a deformation, if you like) of $\bar{\rho}_i$ to A/J .

ribetd2

3.3. Generalization of Ribet's lemma: the case $r = 2$. Before going to the general case, which is combinatorially involved, we dwell a little bit on the case where \bar{T} is the sum of $r = 2$ irreducible pseudocharacters $\text{tr } \bar{\rho}_1$ and $\text{tr } \bar{\rho}_2$. The dimension d of T is still unrestricted, and so is the nature of the local ring A (beside being strictly henselian, Noetherian and reduced, as usual). The ideas in this case mainly come from [MW], though they use a different terminology (Wiles had not invented yet pseudorepresentations), and are in a more restricted situation ($d = 2$, A is finite over a d.v.r, etc.)

In this case the structure theorem takes a very simple form: there are two fractional ideals B and C of A , with $BC \subset m$, and an isomorphism

$$f : R/\ker T \rightarrow S = \begin{pmatrix} M_{d_1}(A) & M_{d_1, d_2}(B) \\ M_{d_2, d_1}(C) & M_{d_2}(A) \end{pmatrix}$$

that is compatible with traces. The proper ideal $I = BC$ of A is the reducibility ideal of A .

ribet2

Proposition 3.1. *Let J be any proper ideal of A that contains I . As we have seen at the end of §3.2, the representations $\bar{\rho}_i$ have canonical lifts $\rho_i : R \otimes A/J \rightarrow M_{d_i}(A/J)$. There exists natural injective maps of A -modules*

$$(4) \quad \iota_B : \text{Hom}_A(B, A/J) \rightarrow \text{Ext}_{R \otimes A/J}^1(\rho_1, \rho_2)$$

$$(5) \quad \iota_C : \mathrm{Hom}_A(C, A/J) \rightarrow \mathrm{Ext}_{R \otimes A/J}^1(\rho_2, \rho_1)$$

Proof — We only treat the first case, the second being symmetric. The proof is by direct computation: for $r \in R$, let us call $f(r)$ its image in S , and $a(r) \in M_{d_1}(A)$, $b(r) \in M_{d_1, d_2}(B)$, $c(r) \in M_{d_2, d_1}(C)$, $d(r) \in M_{d_2}(A)$ be its block constituents. We have the multiplication relations $a(rr') = a(r)a(r') + b(r)c(r')$ in $M_{d_1}(A)$, $b(rr') = a(r)b(r') + b(r)d(r')$ in $M_{d_1, d_2}(B)$, and similarly for the other constituents. Note in particular that $b(r)c(r') \in M_{d_1}(BC) \subset M_{d_1}(J)$ so $a(rr') \equiv a(r)a(r') \pmod{J}$, and similarly for d . Actually, by construction $a(r) \pmod{J} = \rho_1(r)$ in $M_{d_1}(A/J)$ and $d(r) \pmod{J} = \rho_2(r)$.

Now let $l : B \rightarrow A/J$ be a morphism of A -modules. We consider the map $\rho_l : R \otimes A/J \rightarrow M_d(A/J)$ defined by

$$\rho_l(r \otimes 1) = \begin{pmatrix} a(r) & (\text{mod } J) & l(b(r)) \\ & 0 & d(r) & (\text{mod } J) \end{pmatrix},$$

where $l(b(r))$ is the matrix in $M_{d_1, d_2}(A/J)$ obtained from $b(r)$ by applying l to each coefficients.

We claim that ρ_l is a morphism of algebras. Indeed, it obviously respects the addition, and for the multiplication only the upper right corner may be a problem. So we check : the upper right corner of $\rho_l(rr')$ is $l(b(rr')) \in M_{d_1, d_2}(A/J)$. The upper right corner of $\rho_l(r)\rho_l(r')$ is $a(r)l(b(r')) + b(r)l(d(r')) = l(a(r)b(r') + b(r)d(r'))$ since l is A -linear. Now we see that the two upper-tight corners are the same in virtue of the multiplication formula for b given above.

Since ρ_l is a morphism of algebras, it is a representation of $R \otimes A/J$. But clearly it contains $a = \rho_1$ as a sub-representation and $d = \rho_2$ as a quotient. Therefore ρ_l is an extension of ρ_2 by ρ_1 . Hence we have constructed a map $\iota_B : l \mapsto \rho_l$, $\mathrm{Hom}_A(B, A/J) \rightarrow \mathrm{Ext}_{R \otimes A/J}^1(\rho_1, \rho_2)$. This map is clearly linear in view of the definition of ρ_l . It remains to show that it is injective. Assume that the extension ρ_l is trivial. This does not imply that $l(b(r)) = 0$ for all $r \in R$ but this clearly implies that $l(b(r)) = 0$ for r such that $\rho_1(r) = 0$ and $\rho_2(r) = 0$. But f is surjective, so we can find r such that $a(r) = 0$, $d(r) = 0$, and $b(r)$ is arbitrary in $M_{d_1, d_2}(B)$. So we see that l is 0 on B , which proves the injectivity of the map $l \mapsto \rho_l$. \square

The generalization of Ribet's lemma is the combination of this proposition and the fact that BC is the reducibility ideal of T (see §3.2^{red}).

Do you see why it is a generalization of Ribet's lemma? Maybe not. Let me explain... Assume as in the hypotheses of Ribet's lemma that A is discrete valuation domain, of fraction field K , and that $T = \mathrm{tr} \rho$ where ρ is a representation that is irreducible over K , but such that $\bar{\rho}^{\mathrm{ss}} = \bar{\rho}_1 \oplus \bar{\rho}_2$. Since ρ is irreducible over K , the reducibility locus is a proper subscheme of $\mathrm{Spec} A$, that is to say, the reducibility ideal $I = BC$ is not 0. Therefore, neither B nor C is 0. Since they are fractional ideals of A , and A is principal, this does not leave us much choice: both B and C

are as A -modules isomorphic to A (and as fractional ideals, they are of the form $\pi^b B$ and $\pi^c C$ with $b, c \in \mathbb{Z}$, $b + c \geq 1$). Now apply the proposition for $J = m = (\pi)$. Of course $\text{Hom}_A(B, A/m) = k$ and similarly for C , and the proposition tells us that the spaces $\text{Ext}_{R \otimes k}^1(\bar{\rho}_1, \bar{\rho}_2)$ and $\text{Ext}_{R \otimes k}^1(\bar{\rho}_2, \bar{\rho}_1)$ have dimension at least one. This is Ribet's lemma.

Now in the same situation as above, we are not obliged to take $J = m = (\pi)$. We can take any J that contains the reducibility ideal $I = BC$. Say $J = I$. Then the proposition tells us that the module $\text{Ext}_{R \otimes A/I}^1(\rho_1, \rho_2)$ contains a module isomorphic to A/I . Since $I = (\pi^n)$, where n is defined in Exercise I.6, ^{mod pn} we get the result of that Exercise.

But the most interesting aspect of our generalization of Ribet's Lemma is that A can be a much more general local ring than a d.v.r, with dimension greater than one and an rich geometry of its own. To get a sense of what our results says in general, let us focus on the case $J = m$, that is when we only are interested in constructing extensions of $\bar{\rho}_1$ by $\bar{\rho}_2$ over $A/m = k$ (instead of extensions of ρ_1 by ρ_2 over A/J). The A -module $\text{Hom}_A(B, A/m) = \text{Hom}_k(B/mB, k)$ is now the dual vector space of the k -vector space B/mB . By Nakayama's lemma, its dimension is the minimal number of elements of a generating family of B : let's call that $g(B)$. Therefore, the proposition says that

$$\dim_k \text{Ext}_{R \otimes k}^1(\bar{\rho}_1, \bar{\rho}_2) \geq g(B),$$

that is we can construct $g(B)$ independent extensions of $\bar{\rho}_2$ by $\bar{\rho}_1$. Similarly,

$$\dim_k \text{Ext}_{R \otimes k}^1(\bar{\rho}_2, \bar{\rho}_1) \geq g(C).$$

Now what can we say about $g(B)$ and $g(C)$? Well, $BC = I$, the reducibility ideal. It follows immediately that $g(B)g(C) \geq g(I)$. The number $g(I)$ is the minimal number of generators of I . By the hauptidealsatz, it is at least equal to the codimension of $\text{Spec } A/I$ in $\text{Spec } A$, that is the codimension of the irreducibility locus. In other words: the smaller is the reducibility locus, the larger has to be $g(I)$, so the larger has to be $g(B)g(C)$, and the more extensions we construct. This is intuitive.

A special case that we meet in practice is when the irreducibility locus is the smallest possible: the closed point of $\text{Spec } A$, that is $I = m$. In this case, we have $g(B)g(C) \geq g(m)$. But $g(m)$ is by Nakayama's lemma the dimension of m/m^2 , which is the cotangent space of $\text{Spec } A$ at its closed point. If d is the Krull dimension of A , we thus have $g(m) \geq d$, with equality if and only if A is regular ring. In particular $g(B)g(C) \geq d$, and if A happens to be non-regular, $g(B)g(C) > d$. The geometry of A comes into the game.

3.4. Ribet's generalization: the general case.

ribet3

Theorem 3.3. *Let $i, j \in \{1, \dots, r\}$, $i \neq j$. Let J be an ideal containing the reducibility ideal I . Let $A'_{i,j} = \sum_{k \neq i,j} A_{i,k} A_{k,j}$. (We have obviously $A'_{i,j} \subset A_{i,j}$.)*

There exists a natural injective map of A -modules:

$$\iota_{i,j} : \text{Hom}_A(A_{i,j}/A'_{i,j}, A/J) \hookrightarrow \text{Ext}_{R \otimes A/J}^1(\rho_j, \rho_i)$$

where ρ_i and ρ_j are the representations defined at the end of §^{red}3.2.

The construction of $\iota_{i,j}$ and proof of its injectivity is similar to the proof of Proposition ^{ribet2}3.1. See ^{BC}[BC].

One can find that this method of construction of extensions (by hand, by giving explicitly the matrix representation of the extension) is much less elegant than Ribet's method which provides explicitly a free A -module Λ with G -action (a lattice) and see the extension in $\Lambda/m\Lambda$. Esthetic questions aside, it shall be useful in applications to have a construction *a la Ribet* of extensions. We can do that, but we have to give up the freeness assumption of the module.

Theorem 3.4. *Let $i \in \{1, \dots, r\}$. There exists a natural R -module M_i , which is finite torsion-free as an A -module M_i and such that for every $r \in R$, we have $\text{tr}(r|M_i \otimes_A K) = T(r)$. (in particular $M_i \otimes_A K$ has dimension d), and such that*

- (i) *The $R \otimes k$ -module $M_i \otimes k$ has semi-simplification $\bigoplus_{j=1}^r \bar{\rho}_j^{n_j}$ where the n_j are integers ≥ 1 , and $n_i = 1$. Moreover $\bar{\rho}_i$ is a quotient of $M_i \otimes k$.*
- (ii) *For J as in theorem ^{ribet3}3.3, and $j \neq i$, every extension of ρ_i by ρ_j over A/J whose classes lies on the image of $\iota_{i,j}$ appears as a subquotient of M_i .*

Actually one takes M_i the injective hull of $\bar{\rho}_i$ in the category of $R/\ker T$ -modules. We can show that as an A -module, $M_i = \bigoplus_{j=1}^d A_{i,j}^{d_j}$. For the proof, see ^{BC}[BC].

It can be proved (see ^{BC}[BC]) that all extension of ρ_i by ρ_j that appears as a subquotient of an R -module M which is finitely generated and torsion free as an A -module, and whose character of $M \otimes K$ is T appears in the image of $\iota_{i,j}$. In other words, the $\iota_{i,j}$ construction does not miss any extension that it is possible to construct using T .

3.5. Exercises.

Exercise 3.1. Let $A = \mathbb{Z}_p$, and let $R = A[X]$. Let $\rho : R \rightarrow M_2(A)$ be the morphism that sends X to the matrix $\begin{pmatrix} 1 & 1 \\ p^2 & 1 \end{pmatrix}$, and $T = \text{tr } \rho$. Show that $T : R \rightarrow \mathbb{Z}_p$ is a pseudo-character of dimension 2, but that it is not residually multiplicity free. Show that $I = (p^2)$ is the smallest ideal of A such that $T \otimes 1 : R \otimes A/I$ is the sum of two non zero pseudo-characters. Show however that $T \otimes A/I$ is the sum of two pseudo-characters in several different ways.

Exercise 3.2. (difficult) Show by an example, that for a non-residually multiplicity free pseudocharacters, the reducibility ideal may not exist (of course, A has to be not a d.v.r).

Exercise 3.3. Let k be a field and $A = k[[X, Y, X]]/(XY - Z^2)$. Show that A is complete local Noetherian domain with residue field k . Let us call $K = \text{Frac}(A)$. Let $B = XA + ZA \subset A$ and $C = A + (Y/Z)A \subset K$. Show that $R = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$ is a generalized matrix algebra, and that its trace $T = \text{tr}$ is a residually multiplicity free pseudocharacter of dimension 2. Show that T is not the trace of any representation $R \rightarrow M_2(A)$.

Exercise 3.4. (difficult) Assume that A is a unique factorization domain. Show that every residually multiplicity-free pseudocharacter $T : R \rightarrow A$ (for any A -algebra R) of dimension d (any d) is the trace of a representation $R \rightarrow M_d(A)$. (Hint : do first the case $r = 2$, which is simpler).

It can be shown (cf. ^{BC}[BC]) that the converse also holds: if every residually multiplicity-free pseudocharacter $T : R \rightarrow A$ of dimension d is the trace of a representation $R \rightarrow M_d(A)$, then A is a UFD.

Exercise 3.5. Prove theorem ^{ribet3}3.3.

Exercise 3.6. With the notations of ^{ribetd2}§3.3, and assuming that A is a domain (so that K is its fraction field).

a.– show that $T \otimes 1 : R \otimes K \rightarrow K$ is irreducible if and only if $B \neq 0$ and $C \neq 0$.

b.– **(difficult)** Assuming that T is the trace of a representation and that $I = m$, show that $\max(g(B), g(C)) \geq g(I)$.

REFERENCES

bellaïche	[B1] J. Bellaïche, <i>À propos d'un lemme de Ribet</i> , Rendiconti del seminario dell'universita di Padova 109 (2003), 47–62.
BKHawaii	[B2] K. Bellaïche, <i>Introduction to the conjecture of Bloch and Kato</i> , this volume.
BC	[BC] J. Bellaïche & G. Chenevier, <i>p-adic Families of Galois representations</i> , Astérisque, 324, SMF (2009). Also available on arxiv 0602340 (2006).
BG	[BG] J. Bellaïche & P. Graftieaux, <i>Représentations sur un anneau de valuation discrète complet</i> , Math. Annalen.
bourbaki	[Bou1] N. Bourbaki, <i>Éléments de mathématiques. Groupes et algèbres de Lie</i> , Actualités Scientifiques et Industrielles, Hermann, 1961
bourbaki2	[Bou2] N. Bourbaki, <i>Éléments de mathématiques. Algèbre commutative</i> , Actualités Scientifiques et Industrielles, Hermann, 1961
determinants	[C] G. Chenevier, <i>The p-adic analytic space of pseudocharacters of a profinite group, and pseudorepresentations over arbitrary rings</i> , preprint 2008
KHawaii	[K] M. Kisin <i>Lectures on deformations of Galois representation</i> , this volume.
r	[R] K. Ribet, <i>A modular construction of unramified extension of $\mathbb{Q}(\mu_p)$</i> , inventiones math. 1976
MW	[MW] B. Mazur & A. Wiles, <i>The class field of abelian extensions of \mathbb{Q}</i> , Invent. Math. 76 no.2 (1984), 179–330.
Nys	[Nys] L. Nyssen, <i>Pseudo-representations</i> , Math. Annalen 306 (1996), 257–283.
pr1	[P1] C. Procesi <i>The invariant theory of $n \times n$ matrices</i> , Advances in Math. 19 (1976), p. 306–381.
pr2	[P2] C. Procesi, <i>A formal inverse to the Cayley-Hamilton theorem</i> , J. Algebra 107, (1987), p. 63–74.
Rou	[Rou] R. Rouquier, <i>Caractérisation des caractères et pseudo-caractères</i> , J. Algebra 180(2) (1996), 571–586.
chHawaii	[S] C. Skinner, this volume.
Tay	[T] R. Taylor, <i>Galois representations associated to Siegel modular forms of low weight</i> , Duke Math. J. 63 (1991), 281–332.

- wiles [W] A. Wiles *The Iwasawa conjecture for totally real fields*, Ann. of Math. 131 (1990), p. 493–540.

E-mail address: `jbellaic@brandeis.edu`

MATH DEPARTMENT, MS 050, BRANDEIS UNIVERSITY, 415 SOUTH STREET, WALTHAM, MA 02453