Journal of Number Theory 172 (2017) 133–144

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Trace map and regularity of finite extensions of a DVR

Fabio Tonini

Freie Universität Berlin, FB Mathematik und Informatik, Arnimallee 3, Zimmer 112A, 14195 Berlin, Germany

ARTICLE INFO

Article history:
Received 10 May 2016
Received in revised form 20 August 2016
Accepted 22 August 2016
Available online 8 October 2016
Communicated by D. Goss

Keywords:
Regularity
Trace map
Ramification index
Tame

ABSTRACT

We interpret the regularity of a finite and flat extension of a discrete valuation ring in terms of the trace map of the extension.

1. Introduction

Let R be a ring and A be an R-algebra which is projective and finitely generated as R-module. We denote by $\mathrm{tr}_{A/R}\colon A \longrightarrow R$ the trace map and by $\widetilde{\mathrm{tr}}_{A/R}\colon A \longrightarrow A^\vee = \mathrm{Hom}_R(A, R)$ the map $a \longmapsto \mathrm{tr}_{A/R}(a \cdot -)$. It is a well known result of commutative algebra that the étaleness of the extension A/R is entirely encoded in the trace map $\mathrm{tr}_{A/R}$: A/R is étale if and only if the map $\widetilde{\mathrm{tr}}_{A/R}\colon A \longrightarrow A^\vee$ is an isomorphism (see [Gro71, Proposition 4.10]). In this case, if R is a DVR (discrete valuation ring) it follows

E-mail address: tonini@zedat.fu-berlin.de.

http://dx.doi.org/10.1016/j.jnt.2016.08.019
0022-314X/

that A is regular (that is a product of Dedekind domains), while the converse is clearly not true because extensions of Dedekind domains are often ramified.

In this paper we show how to read the regularity of A in terms of the trace map $\operatorname{tr}_{A/R}$. In order to express our result we need some notations and definitions. Let us assume from now on that the ring R is a DVR with residue field k_R. We first extend the notion of tame extensions and ramification index: given a maximal ideal p of A we set

$$e(p, A/R) = \frac{\dim_{k_R}(A_p \otimes_R k_R)}{[k(p) : k_R]}$$

where $k(p) = A/p$, and we call it the *ramification index* of p in the extension A/R. Notice that $e(p, A/R) \in \mathbb{N}$ (see Lemma 2.3). We say that A/R is *tame* (over the maximal ideal of R) if the ramification indexes of all maximal ideals of A are coprime with $\operatorname{char} k_R$. Those definitions agree with the usual ones when A is a Dedekind domain. We also set

$$\mathcal{Q}_{A/R} = \operatorname{Coker}(A \xrightarrow{\widetilde{\operatorname{tr}}_{A/R}} A^\vee), \;\; f^{A/R} = \mathrm{l}(\mathcal{Q}_{A/R})$$

where l denotes the length function. Alternatively $f^{A/R}$ can be seen as the valuation of the discriminant section $\det \widetilde{\operatorname{tr}}_{A/R}$. We also denote by $|\operatorname{Spec}(A \otimes_R \overline{k_R})|$ the number of primes of $A \otimes_R \overline{k_R}$: this number can also be computed as

$$|\operatorname{Spec}(A \otimes_R \overline{k_R})| = \sum_{p \text{ maximal ideals of } A} [F_p : k_R]$$

where F_p denotes the maximal separable extension of k_R inside $k(p) = A/p$ (see Corollary 2.4). Finally we will say that A/R has separable residue fields (over the maximal ideal of R) if for all maximal ideals p of A the finite extension $k(p)/k_R$ is separable. The theorem we are going to prove is the following:

Main theorem. *Let R be a DVR and A be a finite and flat R-algebra. Then we have the inequality*

$$f^{A/R} \geq \operatorname{rk} A - |\operatorname{Spec}(A \otimes_R \overline{k_R})|$$

and the following conditions are equivalent:

1) *the equality holds in the inequality above;*
2) *A is regular and A/R is tame with separable residue fields;*
3) *A/R is tame with separable residue fields and the R-module $\mathcal{Q}_{A/R}$ is defined over k_R, that is $m_R\mathcal{Q}_{A/R} = 0$, where m_R denotes the maximal ideal of R.*

The implication 2) $\implies$ 1) is classical, because it follows directly from the relation between the different and ramification indexes (see [Ser79, III, §6, Proposition 13]). Notice that the étaleness of A/R is equivalent to any of the following conditions: $f^{A/R} = 0$, $\operatorname{rk} A = |\operatorname{Spec}(A \otimes_R \overline{k_R})|$, $\mathcal{Q}_{A/R} = 0$.

The above result has already been proved in my Ph.D. thesis [Ton13, Theorem 4.4.4] under the assumption that a finite solvable group G acts on A in a way that $A^G = R$ and using a completely different strategy: using induction and finding a filtration of R-algebras of $R \subseteq A$ starting from a filtration of normal subgroups of G. Main theorem is an essential ingredient in the proof of [Ton15, Theorem C] which generalizes [Ton13, Theorem 4.4.7].

The paper is organized as follows. In the first section we discuss the notion of tameness and ramification index and recall some basic facts of commutative algebra and, in particular, about the trace map. In the second section we prove the Main theorem.

1.1. Notation

All rings and algebras in this paper are commutative with unity.

Given a ring R and a prime q we denote by $k(q)$ the residue field of R_q. If A is a finite R-algebra we say that A/R has separable residue fields over a prime q of R if for all primes p of A lying over q the finite extension of fields $k(p)/k(q)$ is separable. We say that A/R has separable residue fields if it has this property over all primes of R.

The following conditions are equivalent (see [Gro64, Proposition 1.4.7]): A/R is finite, flat and finitely presented; A is finitely generated and projective as R-module; A is finitely presented as R-module and for all primes q of R the R_q-module A_q is free. In this situation there is a well-defined trace function $\operatorname{Hom}_R(A, A) \longrightarrow R$ which extends the usual trace of matrices and commutes with arbitrary extensions of scalars. The trace map of A/R, denoted by $\operatorname{tr}_{A/R} \colon A \longrightarrow R$ (or simply tr_A), is the composition $A \longrightarrow \operatorname{Hom}_R(A, A) \longrightarrow R$, where the first map is induced by the multiplication in A.

If R is a local ring we denote by m_R its maximal ideal and by k_R its residue field. A DVR is a discrete valuation ring.

If k is a field we denote by $\overline{k}$ an algebraic closure of k and by k^s a separable closure of k.

2. Preliminaries on tameness and trace map

We fix a ring R and a finite, flat and finitely presented R-algebra A over R, that is an R-algebra A which is finitely presented as R-module and such that A_q is a free R_q-module of finite rank for all prime q of R.

Definition 2.1. Given a prime ideal p of A lying above the prime q of R we set

$$e(p, A/R) = \frac{\dim_{k(q)}(A_p \otimes_{R_q} k(q))}{[k(p) : k(q)]}$$

and we call it the *ramification index* of p in the extension A/R. We say that A/R is *tame* in $p \in \operatorname{Spec} A$ if $e(p, A/R)$ is coprime with $\operatorname{char} k(q)$, is *tame* over $q \in \operatorname{Spec} R$ if it is tame over all primes of A over q and, finally, we say that it is *tame* if it is tame over all primes of R (or in all primes of A).

Remark 2.2. The number $e(p, A/R)$ is always a natural number as shown below. Moreover if R and A are Dedekind domains, the notion of ramification index agrees with the usual one.

Lemma 2.3. *Let p be a prime of A lying over the prime q of R and denote by F the maximal separable extension of $k(q)$ inside $k(p)$. Then $e(p, A/R)$ is a natural number and*

$$A_p \otimes_{R_q} \overline{k(q)} \simeq B_1 \times \cdots \times B_s \text{ with } B_i \text{ local, } \dim_{\overline{k(q)}} B_i = e(p, A/R)[k(p) : F]$$
$$\text{and } s = [F : k(q)]$$

Proof. We can assume that $R = k(q) = k$ is a field and that A is local. Set also $L = k(p)$ and write

$$L \otimes_k \overline{k} \simeq C_1 \times \cdots \times C_r, \; A \otimes_k \overline{k} \simeq B_1 \times \cdots \times B_s$$

for the decompositions into local rings. In particular we have that $r = s$ because $A \otimes_k \overline{k} \longrightarrow L \otimes_k \overline{k}$ is surjective with nilpotent kernel. Moreover this map splits as a product of surjective maps $B_i \longrightarrow C_i$. Denote by J_i their kernels and by $\phi\colon A \otimes_k \overline{k} \longrightarrow B_1 \times \cdots \times B_s$ the previous isomorphism of rings. For all $t \in \mathbb{N}$ (including $t = 0$) we have

$$\phi((m_A \otimes_k \overline{k})^t) = J_1^t \times \cdots \times J_s^t$$

In particular for all $t \in \mathbb{N}$ we have

$$\left(\frac{J_1^t}{J_1^{t+1}}\right) \times \cdots \times \left(\frac{J_s^t}{J_s^{t+1}}\right) \simeq \frac{(m_A \otimes_k \overline{k})^t}{(m_A \otimes_k \overline{k})^{t+1}} \simeq \frac{m_A^t}{m_A^{t+1}} \otimes_k \overline{k}$$
$$\simeq (L \otimes_k \overline{k})^{f(t)} \simeq C_1^{f(t)} \times \cdots \times C_s^{f(t)}$$

as $L \otimes_k \overline{k}$-modules, where $f(t) = \dim_L(m_A^t/m_A^{t+1})$. We can conclude that

$$\left(\frac{J_i^t}{J_i^{t+1}}\right) \simeq C_i^{f(t)} \text{ for all } i, t$$

In particular

$$\dim_{\overline{k}} B_i = \sum_{t \in \mathbb{N}} \dim_{\overline{k}} \left(\frac{J_i^t}{J_i^{t+1}}\right) = (\dim_{\overline{k}} C_i) \sum_{t \in \mathbb{N}} f(t)$$

because J_i is nilpotent. Similarly we have

$$\dim_k A = \sum_{t \in N} \dim_k \left(\frac{m_A^t}{m_A^{t+1}} \right) = [L:k] \sum_{t \in \mathbb{N}} f(t)$$

In particular $[L:k] \mid \dim_k A$, so that the ramification index is a natural number. By a direct computation we see that everything follows if we show that $\dim_{\overline{k}} C_i = [L:F]$. Since F/k is separable we know that $F \otimes_k \overline{k} \simeq \overline{k}^{[F:k]}$. Each factor corresponds to an embedding $\sigma\colon F \longrightarrow \overline{k}$ such that $\sigma_{|k} = \mathrm{id}_k$ and

$$L \otimes_k \overline{k} \simeq L \otimes_F (F \otimes_k \overline{k}) \simeq \prod_{\sigma \in \mathrm{Hom}_k(F, \overline{k})} L \otimes_{F,\sigma} \overline{k}$$

This is exactly the decomposition into local rings because, since L/F is purely inseparable, all the rings $L \otimes_{F,\sigma} \overline{k}$ are local. This ends the proof. $\square$

Corollary 2.4. *Let q be a prime of R. Then*

$$|\operatorname{Spec}(A \otimes_R \overline{k(q)})| = \sum_{\substack{p \text{ primes of} \\ A \text{ over } q}} [F_p : k(q)]$$

where F_p denotes the maximal separable extension of $k(q)$ inside $k(p)$.

Proof. It follows from Lemma 2.3 using the fact that $A \otimes_R k(q)$ is the product of the $A_p \otimes_{R_q} k(q)$ for p running through all primes of A over q. $\square$

Definition 2.5. Let p be a prime of A lying over the prime q of R. We denote by $h(p, A/R)$ the common length of the localizations of $A_p \otimes_{R_q} \overline{k(q)}$, that is, following notation from Lemma 2.3, $h(p, A/R) = \dim_k B_i = e(p, A/R)[k(p) : F]$.

Lemma 2.6. *Let p be a prime of A, R' be an R-algebra and p' be a prime of $A' = A \otimes_R R'$ over the prime p. Then*

$$h(p, A/R) = h(p', A'/R')$$

Proof. We can assume that $R = k$ and $R' = k'$ are fields and that A is local. Moreover by definition of the function $h(-)$ we can also assume that k and k' are algebraically closed. In this case $h(p, A/k) = \dim_k A$ and, since $A' = A \otimes_k k'$ is again local, $h(p', A'/k') = \dim_{k'} A' = \dim_k A$. $\square$

Corollary 2.7. *Let p be a prime of A. Then A/R is tame in p and $k(p)/k(q)$ is separable if and only if the number $h(p, A/R)$ is coprime with* $\operatorname{char} k(q)$.

Proof. We can assume that $R = k = k(q)$ is a field and A is local with residue field L. Let also F be the maximal separable extension of k inside L. Thanks to Lemma 2.3, the last condition in the statement is that the number $e(m_A, A/k)[L : F]$ is coprime with $\operatorname{char} k$. Since L/F is purely inseparable, so that $[L : F]$ is either 1 or a power of $\operatorname{char} k$, this is the same as A/k being tame and $L = F$, that is L/k is separable. $\square$

Remark 2.8. Let q be a prime of R, R' be an R-algebra and q' be a prime of R' over R. By Lemma 2.6 and Corollary 2.7 it follows that A/R is tame over q and $A \otimes_R k(q)$ has separable residue fields if and only if the same is true for the extension $(A \otimes_R R')/R'$ with respect to the prime q'. On the other hand tameness alone does not satisfy the same base change property, and, in particular, the function $e(-)$ does not satisfy Lemma 2.6. The counterexample is a finite purely inseparable extension L/k: we have that $e(m_k, L/k) = 1$, so that L/k is tame, while $e(m_{\overline{k}}, L \otimes_k \overline{k}/\overline{k}) = [L : k]$ because $L \otimes_k \overline{k}$ is local, so that $L \otimes_k \overline{k}/k$ is not tame.

Lemma 2.9. *Assume that $R = k$ is a field, that A is local and set $\pi \colon A \longrightarrow k_A$ for the projection. Then*

$$\operatorname{tr}_{A/k} = e(m_A, A/k) \operatorname{tr}_{k_A/k} \circ \pi$$

Proof. Set $P = m_A$, $L = k_A$ and let $x_{1,i}, \dots, x_{r_i,i} \in P^i$ be elements whose projections form an L-basis of P^i/P^{i+1}. We set $x_{1,0} = 1$. Let also $y_1, \dots, y_s \in A$ be elements whose projections form a k-basis of L, where $s = \dim_k L$. It is easy to see that the collection

$$\{x_{\alpha,i} y_\beta\}_{1 \le \alpha \le r_i, 1 \le \beta \le s}$$

is a k-basis of P^i/P^{i+1} for all $i \ge 0$. By an inverse induction starting from the nilpotent index of P, it also follows that

$$\mathcal{B}_n = \{x_{\alpha,i} y_\beta\}_{1 \le \alpha \le r_i, 1 \le \beta \le s, i \ge n}$$

is a k-basis of P^n for all $n \ge 0$. In particular, when $n = 0$ we get a k-basis of $A = P^0$.

We are going to compute the trace map tr_A over the basis $\mathcal{B}_0$. Consider an index $i > 0$. For all possible $\alpha, \beta, \gamma, \delta, j$ we have that

$$z = (x_{\alpha,i} y_\beta)(x_{\gamma,j} y_\delta) \in P^{i+j} \subseteq P^{j+1}$$

Thus z is a linear combination of vectors in $\mathcal{B}_{j+1}$, which does not contain $(x_{\gamma,j} y_\delta)$. It follows that $\operatorname{tr}_A(x_{\alpha,i} y_\beta) = 0$ for all $i > 0$, that is $\operatorname{tr}_A(P) = 0$ which agrees with the formula in the statement. It remains to compute $\operatorname{tr}_A(y_\beta)$. Write

$$y_\beta y_\delta = \sum_q b_{\beta,\delta,q} y_q + u_{\beta,\delta} \text{ with } u_{\beta,\delta} \in P \text{ and } b_{\beta,\delta,q} \in k$$

It follows that

$$\operatorname{tr}_{L/k}(\pi(y_\beta)) = \sum_\delta b_{\beta,\delta,\delta}$$

Let's multiply now y_β with an element $x_{\alpha,i}y_\delta$, obtaining

$$z = y_\beta(x_{\alpha,i}y_\delta) = x_{\alpha,i}u_{\beta,\delta} + \sum_q b_{\beta,\delta,q}x_{\alpha,i}y_q$$

If $i = 0$, so that $\alpha = 1$ and $x_{1,0} = 1$, the coefficient of z with respect to y_δ is $b_{\beta,\delta,\delta}$ because $u_{\beta,\delta} \in P$. If $i > 0$ then the coefficient of z with respect to $(x_{\alpha,i}y_\delta)$ is again $b_{\beta,\delta,\delta}$ because $x_{\alpha,i}u_{\beta,\delta} \in P^{i+1}$ and thus can be written using only the vectors in $\mathcal{B}_{i+1}$. In conclusion we have that

$$\operatorname{tr}_A(y_\beta) = \sum_{i,\alpha,\delta} b_{\beta,\delta,\delta} = (\sum_\delta b_{\beta,\delta,\delta})(\sum_{\alpha,i} 1) = \operatorname{tr}_L(\pi(y_\beta))C \text{ with } C = (\sum_{i,\alpha} 1)$$

Thus $\operatorname{tr}_A = C \operatorname{tr}_L \circ \pi$ and, finally,

$$C = (\sum_{i,\alpha} 1) = \sum_{i \geq 0} \dim_L(\frac{P^i}{P^{i+1}}) = \frac{\dim_k A}{[L:k]} = e(m_A, A/k) \qquad \square$$

Corollary 2.10. *Assume that R and A are local. Then*

1) $\operatorname{tr}_{A/R}(m_A) \subseteq m_R$;
2) if $k_A = k_R$ and $\operatorname{rk} A \in R^*$ then $\operatorname{Ker} \operatorname{tr}_{A/R} \subseteq m_A$.

Proof. Since $\operatorname{tr}_{A/R} \otimes_R k_R = \operatorname{tr}_{(A\otimes_R k_R)/k_R}$ point 1) follows from Lemma 2.9 because $\operatorname{tr}_{(A\otimes_R k_R)/k_R}(m_{A\otimes_R k_R}) = 0$. Assume now the hypothesis of 2) and let $x \in \operatorname{Ker} \operatorname{tr}_A$. If $x \notin m_A$ there exists $\lambda \in R^*$ such that $y = x - \lambda \in m_A$, so that

$$\operatorname{tr}_A(x) = 0 = \operatorname{rk} A\lambda + \operatorname{tr}_A(y) \in R^* + m_R = R^*$$

which is impossible. $\square$

Lemma 2.11. *If R and A are local then*

$$\operatorname{tr}_{A/R} \colon A \longrightarrow R \textit{ is surjective} \iff h(m_A, A/R) \textit{ and } \operatorname{char} k_R \textit{ are coprime}$$

Proof. By Nakayama's lemma $\operatorname{tr}_{A/R} \colon A \longrightarrow R$ is surjective if and only if $\operatorname{tr}_{A/R} \otimes_R k_R = \operatorname{tr}_{A\otimes k_R/k_R} \colon A \otimes k_R \longrightarrow k_R$ is so. Thus we can assume that $R = k$ is a field. By Lemma 2.9 $\operatorname{tr}_{A/k}$ is surjective if and only if $\operatorname{tr}_{k_A/k}$ is surjective, i.e. k_A/k is separable, and $e(m_A, A/k) \in k^*$. The result then follows from Corollary 2.7. $\square$

3. Regularity of finite extensions of DVR

We fix a DVR R and a finite and flat R-algebra A, so that A is free of finite rank $\operatorname{rk} A$ as R-module. We will use the following notation

$$\widetilde{\operatorname{tr}}_{A/R} \colon A \longrightarrow A^\vee,\ a \longmapsto \operatorname{tr}_{A/R}(a \cdot -)$$

$$\mathcal{Q}_{A/R} = \operatorname{Coker}(A \xrightarrow{\widetilde{\operatorname{tr}}_{A/R}} A^\vee),\ f^{A/R} = \operatorname{l}(\mathcal{Q}_{A/R})$$

where l denotes the length function. For simplicity we will replace A/R with A if no confusion can arise.

Remark 3.1. By standard arguments we have that f^A coincides with the valuation over R of $\det(\widetilde{\operatorname{tr}}_A)$. Moreover the following conditions are equivalent:

1) A is generically étale over R;
2) $f^A < \infty$;
3) $\operatorname{tr}_A \colon A \longrightarrow A^\vee$ is injective.

In particular we see that all three conditions in Main theorem implies that A/R is generically étale. This also means that A/R is tame with separable residue fields if and only if $A \otimes_R k_R/k_R$, or $A \otimes_R \overline{k_R}/\overline{k_R}$, is so.

If $\beta = \{x_0, \dots, x_n\}$ is an R-basis of A then the matrix of $\widetilde{\operatorname{tr}}_A \colon A \longrightarrow A^\vee$ with respect to β and its dual is given by $T = (\operatorname{tr}_A(x_i x_j))_{i,j}$. In particular we can conclude that, if $\operatorname{tr}_A \colon A \longrightarrow R$ is not surjective, then $f^A \geq \operatorname{rk} A$, because all entries of T belongs to m_R. If $\operatorname{tr}_A(1) = \operatorname{rk} A \in R^*$ we have a decomposition $A = R1 \oplus \operatorname{Ker} \operatorname{tr}_A$. In particular if $x_0 = 1$ and $x_1, \dots, x_n \in \operatorname{Ker} \operatorname{tr}_A$ (such a basis always exists locally) the matrix T has the form

$$\begin{pmatrix} \operatorname{rk} A & 0 \\ 0 & N \end{pmatrix}$$

and therefore $\mathcal{Q}_A \simeq \operatorname{Coker} N$.

Remark 3.2. Let R^s be the strict Henselization of R and set $A^s = A \otimes_R R^s$. In particular R^s is a discrete valuation ring with residue field the separable closure k_R^s of k_R. Using that the extension $R \longrightarrow R^s$ is faithfully flat and unramified, it is easy to see that

$$f^{A/R} = f^{A^s/R^s},\ |\operatorname{Spec}(A \otimes_R \overline{k_R})| = |\operatorname{Spec}(A^s \otimes_{R^s} \overline{k_{R^s}})|$$

that $\mathcal{Q}_{A/R}$ is defined over k_R if and only if $\mathcal{Q}_{A^s/R^s}$ is defined over k_{R^s} and that A/R is tame with separable residue fields if and only if A^s/R^s is so.

Since R^s is Henselian, we have a decomposition $A^s = A_1 \times \cdots \times A_q$ where the A_j are local rings finite and flat over R^s. Moreover $A_j \otimes_{R^s} \overline{k_{R^s}}$ are still local, so that $q =$

$|\operatorname{Spec}(A \otimes_R \overline{k_R})|$. Since $\widetilde{\operatorname{tr}}_{A^s/R^s} \colon A^s \longrightarrow (A^s)^\vee$ is the direct sum of the $\widetilde{\operatorname{tr}}_{A_j/R^s} \colon A_j \longrightarrow (A_j)^\vee$ we have

$$\mathcal{Q}_{A^s/R^s} \simeq \bigoplus_j \mathcal{Q}_{A_j/R^s} \text{ and } f^{A^s/R^s} = \sum_j f^{A_j/R_s}$$

Finally we have that the following three conditions are equivalent: A is regular; A^s is regular; A_j is regular for all $j = 1, \dots, q$.

Proof. (of Main theorem) By Remark 3.1 and Remark 3.2 we can assume that R is strictly Henselian, that A is local, so that $|\operatorname{Spec}(A \otimes_R \overline{k_R})| = 1$, and that A/R is generically étale. Moreover in this case the following three conditions are equivalent by Corollary 2.7 and Lemma 2.11: A/R is tame with separable residue fields; $k_A = k_R$ and $\operatorname{rk} A \in R^*$; $\operatorname{tr}_{A/R} \colon A \longrightarrow R$ is surjective.

Inequality and 1) $\iff$ 3). By Remark 3.1 we can assume that $\operatorname{tr}_A \colon A \longrightarrow R$ is surjective, so that $k_A = k_R$, $\operatorname{rk} A \in R^*$. By Corollary 2.10 we also have $\operatorname{Ker} \operatorname{tr}_A \subseteq m_A$ and $\operatorname{tr}_A(m_A) \subseteq m_R$. Using Remark 3.1 and its notation, we see that $f^A = v_R(\det N)$. If $i, j \geq 1$ then $x_i x_j \in m_A$ and thus $\operatorname{tr}_A(x_i x_j) \in m_R$, that is all entries of N belongs to m_R. If $\pi \in m_R$ is an uniformizer of R we can write $N = \pi N'$ where N' is a matrix with entries in R. In particular

$$\det N = \pi^{\operatorname{rk} A - 1} \det N'$$

Applying the valuation of R we get $f^A = v_R(\det N) = \operatorname{rk} A - 1 + v_R(\det N')$ and the desired inequality.

If $\mathcal{Q}_A \simeq \operatorname{Coker}(N)$ is defined over k_R we obtain a surjective map $k_R^{\operatorname{rk} A - 1} \longrightarrow \mathcal{Q}_A \otimes k_R \simeq \mathcal{Q}_A$ and therefore that $f^A = \mathrm{l}(\mathcal{Q}_A) \leq \operatorname{rk} A - 1$. Conversely, if $f^A = \operatorname{rk} A - 1$, which means that $N' \colon R^{\operatorname{rk} A - 1} \longrightarrow R^{\operatorname{rk} A - 1}$ is an isomorphism, we have $\mathcal{Q}_A \simeq \operatorname{Coker}(\pi N')$, so that $\mathcal{Q}_A \simeq k_R^{\operatorname{rk} A - 1}$ is defined over k_R as required.

2) $\Longrightarrow$ 1) Let $t \in A$ be a generator of the maximal ideal. The k_R-algebra $A \otimes k_R$ is local, with residue field k_R and its maximal ideal is generated by the projection $\bar{t}$ of t. It is easy to conclude that $A \otimes k_R = k_R[X](X^N)$ where $N = \operatorname{rk} A$ and X corresponds to $\bar{t}$. By Nakayama's lemma it follows that $1, t, \dots, t^{N-1}$ is an R-basis of A and thus that $A \simeq R[Y]/(Y^N - g(Y))$ where Y corresponds to t, $\deg g < N$ and all coefficients of g are in m_R. Since $m_A = \langle t, m_R \rangle_A$, the condition that A is regular tells us that $v_R(g(0)) = 1$. We are going to compute the valuation of the determinant of $\widetilde{\operatorname{tr}_A} \colon A \longrightarrow A^\vee$ writing this map in terms of the basis $1, t, \dots, t^{N-1}$, that is the valuation of the determinant of the matrix $(\operatorname{tr}_A(t^{i+j}))_{0 \leq i,j < N}$ (see Remark 3.1). Set $q_s = \operatorname{tr}_A(t^s)$. By Corollary 2.10 or a direct computation we know that $q_S \in m_R$ for $s > 0$. In particular, since $v_R(g(0)) = 1$, we also have $v_R(q_N) = 1$. Moreover it follows by induction that $v_R(q_s) > 1$ if $s > N$. Set S_N for the group of permutations of the set $\{0, 1, \dots, N-1\}$. We have

$$\det((\operatorname{tr}_A(t^{i+j}))_{0 \leq i,j < N}) = \sum_{\sigma \in S_N} (-1)^{\operatorname{sgn}(\sigma)} z_\sigma \text{ where } z_\sigma = q_{0+\sigma(0)} q_{1+\sigma(1)} \cdots q_{N-1+\sigma(N-1)}$$

We claim that $v_R(z_\sigma) \geq N$ for all $\sigma \in S_n$ but the permutation $\sigma(0) = 0$ and $\sigma(i) = N-i$ for $i \neq 0$, for which $v_R(z_\sigma) = N-1$. This will conclude the proof. Let $\sigma \in S_N$. If $\sigma(0) \neq 0$, then all the N-factors of z_σ are in m_R, which implies that $v_R(z_\sigma) \geq N$. Thus assume that $\sigma(0) = 0$. Since $q_0 = \operatorname{tr}_A(1) = \operatorname{rk} A \in R^*$ we see that z_σ is, up to q_0, the product of $N-1$ elements of m_R. If one of those factors is of the form $q_{i+\sigma(i)}$ with $i+\sigma(i) > N$ then $v_R(z_\sigma) \geq N$ because $v_R(q_s) \geq 2$ if $s > N$. Thus the only case left is when $\sigma(i) \leq N-i$ for all $0 < i < N$ and $\sigma(0) = 0$. But, arguing by induction, this σ is unique and it is given by $\sigma(0) = 0$ and $\sigma(i) = N-i$. In this case we have

$$z_\sigma = \operatorname{rk} A(\operatorname{tr}(t^N))^{N-1}$$

and therefore $v_R(z_\sigma) = N-1$ as required.

1) $\Longrightarrow$ 2) Since 1) $\Longleftrightarrow$ 3), we already know that A/R is tame with separable residue fields. We have to prove that A is regular. Set $k(R)$ for the fraction field of R. Since $A \otimes k(R)$ is etale over $k(R)$, it is a product of fields $L_1, \dots, L_s$ which are separable extensions of $k(R)$. Let B be the integral closure of R inside $A \otimes k(R)$. We have that $A \subseteq B$ and that $B = B_1 \times \cdots \times B_s$ where B_i is the integral closure of R inside L_i. Since R is strictly Henselian and the B_i are domains, it follows that they are local. Moreover since R is a DVR we can also conclude that the B_i are DVR. We are going to prove that $s = 1$ and $A = B$. Notice that $\operatorname{rk} B = \operatorname{rk} A$ and denote by $j\colon A \longrightarrow B$ the inclusion. By computing tr_A and tr_B over $A \otimes k(R) \simeq B \otimes k(R)$ we can conclude that $(\operatorname{tr}_B)_{|A} = \operatorname{tr}_A$. In particular we obtain a commutative diagram of free R-modules

$$\begin{tikzcd} A \arrow[r, "\widetilde{\operatorname{tr}_A}"] \arrow[d, "j"] & A^\vee \\ B \arrow[r, "\widetilde{\operatorname{tr}_B}"] & B^\vee \arrow[u, "j^\vee"'] \end{tikzcd}$$

Notice that $\det j = \det j^\vee$. Thus taking determinants and then valuations we obtain the expression

$$f^A = 2v_R(\det j) + f^B = 2v_R(\det j) + \sum_{i=1}^{s} f^{B_i}$$

Since k is separably closed and thanks to Corollary 2.4 we have that $|\operatorname{Spec}(B_i \otimes_R \overline{k})| = 1$. In particular $f^{B_i} \geq \operatorname{rk} B_i - 1$ by the inequality in the statement. Since $f^A = \operatorname{rk} A - 1$ we get

$$s \geq 1 + 2v_R(\det j)$$

We are going to prove that $v_R(\det j) \geq s-1$. This will end the proof because it implies $s = 1$ and $v_R(\det j) = 0$, that is $B = A$. Since $k_A = k_R$ we have

$$v_R(\det j) = \mathrm{l}(B/A) \geq \dim_{k_R}(B/(A + m_A B))$$

Denote by $e_1, \dots, e_s \in B$ the idempotents corresponding to the decomposition $B = B_1 \times \dots \times B_s$. We will prove that $e_2, \dots, e_s$ are k_R-linearly independent in $B/(A+m_A B)$, that is we prove that if

$$x = x_1 e_1 + \dots + x_s e_s \in A + m_A B \text{ where } x_1 = 0 \text{ and } x_i \in R$$

then all x_i are in the maximal ideal m_R. Notice that, since $k_A = k_R$, 1 and m_A generates A as R-module. In particular $A + m_A B$ is generated by 1 and $m_A B$ as R-module. Moreover since the maps $A \longrightarrow B \longrightarrow B_i$ map m_A inside m_{B_i} it follows that $m_A B \subseteq m_{B_1} \times \dots \times m_{B_s}$. Thus x can be written as

$$x = \alpha + c_1 e_1 + \dots + c_s e_s \text{ with } \alpha \in R \text{ and } c_i \in m_{B_i}$$

inside B. In particular $0 = x_1 = \alpha + c_1$ in B_1, which implies that $\alpha \in m_{B_1} \cap R = m_R$. Thus if $i > 0$ we have

$$x_i = \alpha + c_i \in m_{B_i} \cap R = m_R$$

as required. $\square$

We show via some examples how the conditions of tameness and separability of residue fields in Main theorem cannot be omitted.

Example 3.3. Let $R = \mathbb{Z}_2$ be the ring of 2-adic numbers and consider the R-algebra

$$A = \frac{R[X]}{(X^2 - c)} \text{ with } c \in R$$

We have that $\mathrm{tr}_A(X) = 0$ and $\mathrm{tr}_A(X^2) = 2c$, so that the matrix of $\widetilde{\mathrm{tr}_A} \colon A \longrightarrow A^\vee$ is

$$M = \begin{pmatrix} 2 & 0 \\ 0 & 2c \end{pmatrix}$$

In particular $f^A = v_R(\det M) \geq 2 > \mathrm{rk}\, A - |\operatorname{Spec}(A \otimes_R \overline{k_R})|$ and $\mathcal{Q}_A$ is defined over $\mathbb{F}_2$ if and only if $c \in R^*$.

Assume $c = 2t + d^2$ with $t, d \in R$, so that $A/m_R A \simeq \mathbb{F}_2[Y]/(Y^2)$, A is local with maximal ideal $(m_R, X - d)$, has separable residue fields and it is not tame. We see that $\mathcal{Q}_A$ is defined over $\mathbb{F}_2$ if and only if $d \in R^*$, while A is regular if and only if $t \in R^*$.

Assume $c \in R^*$ and that c is not a square in $\mathbb{F}_2$. In this case A is local with maximal ideal $m_R A$, A/R is tame, its residue field is not separable, it is regular and $\mathcal{Q}_A$ is defined over $\mathbb{F}_2$.

Acknowledgments

I would like to thank Angelo Vistoli and Dajano Tossici for all the useful conversations we had and all the suggestions I received.

References

[Gro64] Alexander Grothendieck, EGA4-1 - Étude locale des schémas et des morphismes de schémas (Première partie) - Éléments de géométrie algébrique (rédigés avec la collaboration de Jean Dieudonné), Publications Mathématiques, vol. 20, Institut des Hautes Études Scientifiques, 1964.

[Gro71] Alexander Grothendieck, Revêtements étales et groupe fondamental, Lecture Notes in Mathematics, vol. 224, Springer-Verlag, jun 1971.

[Ser79] Jean-Pierre Serre, Local Fields, Graduate Texts in Mathematics, vol. 67, Springer, New York, 1979.

[Ton13] Fabio Tonini, Stacks of ramified Galois covers, PhD thesis, July 2013.

[Ton15] Fabio Tonini, Ramified Galois covers via monoidal functors, arXiv:1507.05309, July 2015; Transform. Groups (2016), http://dx.doi.org/10.1007/s00031-016-9395-4, in press.