IJMMS 26:8 (2001) 467–473
PII. S0161171201005208
http://ijmms.hindawi.com

TWISTED FORMS OF FINITE ÉTALE EXTENSIONS AND SEPARABLE POLYNOMIALS

FRANK DEMEYER

(Received 25 April 2000)

ABSTRACT. Examples of twisted forms of finite étale extensions and separable polynomials are calculated using Mayer-Vietoris sequences for non-abelian cohomology.

2000 Mathematics Subject Classification. 13B05, 13B25, 13B40.

1. Introduction. Let S be a finite étale extension of a commutative Noetherian ring R (a finitely generated projective separable extension of R). A twisted form of S (in the Zariski topology) is a finite étale extension T of R with $R_P \otimes S \cong R_P \otimes T$ as R_P-algebras for each prime ideal P of R. In this case S is locally isomorphic to T. If $Q \subset P$ are prime ideals of R and $R_P \otimes S \cong R_P \otimes T$, then $R_Q \otimes S \cong R_Q \otimes T$ so prime can be replaced by maximal in the definition of the twisted form. In this paper, we study the set of isomorphism classes of twisted forms of S. We especially concentrate on the case where $S \cong R[t]/(p(t))$, where $p(t)$ is a separable polynomial in $R[t]$. Throughout this paper, R denotes a commutative Noetherian ring.

We first observe the well-known facts that if R is an integrally closed domain, then there are no twisted forms of S and in general the twisted forms of S are in bijective correspondence with $H^1(X, \operatorname{Aut}(\mathcal{S}))$, where $\operatorname{Aut}_R(\mathcal{S})$ is the sheaf of automorphisms on $X = \operatorname{Spec}(R)$ associated to $\operatorname{Aut}_R(S)$. We check that $H^1(X, \operatorname{Aut}(\mathcal{S}))$ is unchanged modulo a nilpotent ideal.

With some hypotheses on the sheaf $\operatorname{Aut}_R(\mathcal{S})$, when R is a one-dimensional domain or if R is a reduced one-dimensional ring with connected spectrum, $H^1(X, \operatorname{Aut}(\mathcal{S}))$ fits into a Mayer-Vietoris sequence which makes computations possible. These computations are the point of this article. For infinitely many prime numbers p, q we give a class of examples of integral domains R and separable polynomials $t^p - q \in R[t]$ with the cardinality of the set of isomorphism classes of twisted forms of $S \cong R[t]/(p(t))$ equal to $(p-1)!$. When $p = 3$ these twisted forms T are isomorphic to algebras $T \cong \oplus_{j=0}^{2} I^j t^j$ with $t^3 = q$ and I is a fractional ideal with $I^3 = R$. We give an example of twisted forms that do not have this structure. We also give one-dimensional rings over which finite étale extensions may not have either a primitive element nor a normal basis but which are twisted forms of extensions which do. We also give a separable polynomial which is irreducible over R but factors into linear factors at each localization R_P of R and modulo each maximal ideal of R.

2. Mayer-Vietoris sequences and examples. Let R be a commutative Noetherian ring and S a finite étale R-algebra. Let $X = \operatorname{Spec}(R)$ be the space of prime ideals of R

with the Zariski topology and $\mathbb{O}_X$ the associated sheaf of rings on X, $\mathcal{S}$ the sheaf of $\mathbb{O}_X$-algebras associated to S (see [5, pages 70 and 130]). For each open set $U \subset X$ associate to U the group of R-algebra automorphisms $\mathrm{Aut}_{\mathbb{O}(U)}(\mathcal{S}(U))$, and if $V \subset U$ associate the natural restriction $\mathrm{Aut}_{\mathbb{O}(U)}(\mathcal{S}(U)) \to \mathrm{Aut}_{\mathbb{O}(V)}(\mathcal{S}(V))$. We begin by recording for the readers convenience that $\mathrm{Aut}_R(\mathcal{S})$ forms a sheaf on X and give some of its properties (see also [3]).

Lemma 2.1. *Let S be a finite étale R-algebra.*

(a) *If U is an open set in X and $\{V_i\}$ is an open cover of U, and if $\sigma \in \mathrm{Aut}_{\mathbb{O}(U)}(\mathcal{S}(U))$ satisfies $1 \otimes \sigma = 1$ in $\mathrm{Aut}_{\mathbb{O}(V_i)}(\mathcal{S}(V_i))$ for all i, then $\sigma = 1$ in $\mathrm{Aut}_{\mathbb{O}(U)}(\mathcal{S}(U))$.*

(b) *If U is an open set in X and $\{V_i\}$ is an open cover of U, and if $\sigma_i \in \mathrm{Aut}_{\mathbb{O}(V_i)}(\mathcal{S}(V_i))$ with restrictions $\sigma_i = \sigma_j$ in $\mathrm{Aut}_{\mathbb{O}(V_i \cap V_j)}(\mathcal{S}(V_i \cap V_j))$, then there is an element $\sigma \in \mathrm{Aut}_{\mathbb{O}(U)}(\mathcal{S}(U))$ whose restriction to $\mathrm{Aut}_{\mathbb{O}(V_i)}(\mathcal{S}(V_i))$ is σ_i.*

Lemma 2.2. *Let S, T be finite étale R-algebras and P a prime ideal in R. Let $\sigma : R_P \otimes S \to R_P \otimes T$ be an R_P-algebra homomorphism. Then there is an open set U in X with $P \in U$ and an $\mathbb{O}(U)$-algebra homomorphism $\tau : \mathbb{O}(U) \otimes S \to \mathbb{O}(U) \otimes T$ such that $1 \otimes \tau = \sigma \in \mathrm{Alg}_{R_P}(R_P \otimes S, R_P \otimes T)$. If σ is an isomorphism then U can be chosen so τ is an isomorphism.*

If S, T are finite étale R-algebras and $R_P \otimes S \cong R_P \otimes T$ for all prime ideals P of R we say that S and T are locally isomorphic or that T is a twisted form of S. If T is a twisted form of S then Lemma 2.2 implies there is an open cover $\mathcal{U} = \{U_i\}$ of X and isomorphisms $\sigma_i : \mathbb{O}(U_i) \otimes S \to \mathbb{O}(U_i) \otimes T$ for all i. Define an element $a \in Z^1(\mathcal{U}, \mathrm{Aut}(\mathcal{S}))$ by assigning to the index pair i, j the automorphism $a(i,j) = \sigma_i^{-1}\sigma_j \in \mathrm{Aut}_{\mathbb{O}(U_i \cap U_j)}(\mathbb{O}(U_i \cap U_j) \otimes S)$. Passing to the limit over all covers of X gives an injection from the set of isomorphism classes of twisted forms of S to $H^1(X, \mathrm{Aut}(\mathcal{S}))$. By descent, (see [7, 2.2, page 110] or [8, page 19]), this assignment is onto so $H^1(X, \mathrm{Aut}(\mathcal{S}))$ classifies the twisted forms of S. In the next result we point out that, as with the Brauer group, there are no nontrivial twisted forms in the geometrically irreducible case.

Proposition 2.3. *If R is an integrally closed domain and S is a finite étale R-algebra, then $H^1(X, \mathrm{Aut}(\mathcal{S})) = \{1\}$.*

Proof. We can write $S = S_1 \oplus \cdots \oplus S_k$, where each S_i has a connected spectrum. By [6, Theorem 4.3] or [8, Proposition 3.19, page 28], each S_i is an integrally closed domain. Let K be the quotient field of R. Then $K \otimes S = \oplus_{i=1}^k K \otimes S_i$, where each $K \otimes S_i$ is a finite-dimensional separable field extension of K, and S_i is the integral closure of R in $K \otimes S_i$. Let $\sigma \in \mathrm{Aut}_K(K \otimes S)$, then since the image of an integral element is integral, $\sigma|_S \in \mathrm{Aut}_R(S)$ and $\sigma = 1 \otimes \sigma|_S$. Therefore, the natural map $\mathrm{Aut}_R(S) \to \mathrm{Aut}_K(K \otimes S)$ is a bijection which implies that the sheaf $\mathrm{Aut}(\mathcal{S})$ is constant. Therefore, $H^1(X, \mathrm{Aut}(\mathcal{S})) = \{1\}$. □

Corollary 2.4. *Let R be an integrally closed domain and S, T finite étale R-algebras. If $R_p \otimes S \cong R_P \otimes T$ as R_P-algebras for each $P \in \mathrm{Spec}(R)$, then $S \cong T$ as R-algebras.*

Lemma 2.5. *Let S be a finite étale R-algebra, I an ideal in R, and $\rho : \mathrm{Aut}_R(S) \to \mathrm{Aut}_{R/I}(S/I)$ the natural map.*

(a) *If R has a connected spectrum then ρ is a one-to-one map.*
(b) *If I is nilpotent then ρ is a bijection map.*

Proof. (a) Assume first that S is connected and Galois over R. Then $\mathrm{Aut}_R(S) =$ Galois group of S over R = the Galois group of S/IS over $R/I \subset \mathrm{Aut}_{R/I}(S/IS)$ so ρ is a one-to-one map in this case. If S is connected but not necessarily Galois, imbed S in a connected Galois extension N of R (see [2, Theorem 3.2.9]). Every R-automorphism of S extends to an automorphism of N, and any two such extensions differ by an element of $H = \{\sigma \in \mathrm{Aut}_R(N) \mid \sigma|_S = 1\}$ (see [2, Chapter 3]). By flatness, S/IS is a subalgebra of N/IN and H is the subgroup of the Galois group of N/IN over R/I fixing S/IS. If τ, $\sigma \in \mathrm{Aut}_R(S)$ with extensions $\bar{\tau}, \bar{\sigma}$ to N and with the natural image of $\tau = \sigma$ in $\mathrm{Aut}_{R/I}(S/IS)$, then $\bar{\tau}^{-1}\bar{\sigma} \in H$ so $\tau = \sigma$ on S and ρ is a one-to-one map in this case.

If R is connected then $S = Se_1 \oplus \cdots \oplus S_m$ with $e_ie_j = e_i\delta_{i,j}$, Se_i connected for all i,j. Let $\sigma \in \mathrm{Aut}_R(S)$ and assume σ induces the identity automorphism on S/IS. Then $\sigma(e_i) = e_i$ for all i since $e_i + IS \neq e_j + IS$ for any $i \neq j$. Therefore σ induces $(\sigma_1, \dots, \sigma_m) \in \times_i \mathrm{Aut}_R(Se_i)$. Since σ is the identity on each of these summands, by the previous paragraph σ is the identity on S and ρ is a one-to-one map.

(b) We can write $R = R_1 \oplus \cdots \oplus R_k$, where each R_i has a connected spectrum. Then there are the corresponding decompositions $S = S_1 \oplus \cdots \oplus S_k$ and $I = I_1 \oplus \cdots \oplus I_k$ with I_j a nilpotent ideal of R_j (in particular, no $I_j = R_j$ and $\mathrm{Aut}_R(S) = \times_j \mathrm{Aut}_{R_j}(S_j)$, $\mathrm{Aut}_{R/I}(S/IS) = \times_j \mathrm{Aut}_{R/I_j}(R_j \otimes S/I_j(R_j \otimes S)))$. Thus we can assume R is connected.

If I is nilpotent, then IS is nilpotent and idempotents can be lifted modulo a nilpotent ideal, so R/I has a connected spectrum and if S is connected then S/IS is connected. Assume S is connected and Galois. Then $\mathrm{Aut}_R(S)$ = the Galois group of S over R = the Galois group S/IS over $R/I = \mathrm{Aut}_{R/I}(S/IS)$ so ρ is bijective in this case. If S/R is Galois, then $S = Se_1 \oplus \cdots \oplus Se_m$ with $e_ie_j = e_i\delta_{i,j}$, Se_i connected, $Se_i \cong Se_j$ for all i,j, and each Se_i Galois over R with Galois group of order $n = \mathrm{rank}(Se_i)$. Thus $|\mathrm{Aut}_R(S)| = m!n^m$. Since idempotents can be lifted modulo I, we get the same count for $|\mathrm{Aut}_{R/I}(S/IS)|$, so by part (a), ρ is onto in this case.

If S/R is finite étale, there is a Galois extension N of R containing S constructed in the following way. Write $S = Se_1 \oplus \cdots \oplus Se_m$ as above and let L be a connected Galois extension of R containing all the Se_i. Let $N = Le_1 \oplus \cdots \oplus Le_m$. Let $\bar{\tau} \in \mathrm{Aut}_{R/I}(S/IS)$. Then one can extend $\bar{\tau}$ to $\bar{\gamma} \in \mathrm{Aut}_{R/I}(N/IN)$ which corresponds, by the paragraph above, to $\gamma \in \mathrm{Aut}_R(N)$. Then $(\gamma(S) + IS)/I = S/I$ so $\gamma(S) \subset S$. Therefore $\gamma|_S \in \mathrm{Aut}_R(S)$ and $\rho(\gamma|_S) = \bar{\tau}$. Thus ρ is a bijection in every case. □

Corollary 2.6. *Let $X = \mathrm{Spec}(R)$, I the nil radical of R and $X_{\mathrm{red}} = \mathrm{Spec}(R/I)$. If S is a finite étale R-algebra, then $H^1(X, \mathrm{Aut}(\mathcal{S}))$ and $H^1(X_{\mathrm{red}}, \mathrm{Aut}(\mathcal{S}/\mathcal{I}\mathcal{S}))$ are bijective with one another.*

Proof. By Lemma 2.5, $X = X_{\mathrm{red}}$ and $\mathrm{Aut}(\mathcal{S}) = \mathrm{Aut}(\mathcal{S}/\mathcal{I}\mathcal{S})$. □

Example 2.7. (a) Let $\mathbb{R}$ denote the real numbers and $\mathbb{C}$ the complex numbers. Let $R = \mathbb{R} \oplus \mathbb{R}$ and $S = \mathbb{C} \oplus \mathbb{C}$. Let σ be complex conjugation. Then $(1,1) = (1,\sigma)$ on the first summand but $(1,1) \neq (1,\sigma)$ so the map $\mathrm{Aut}_R(S) \to \mathrm{Aut}_{R/I}(S/IS)$ is not always a one-to-one map.

(b) Let R be the localization of $\mathbb{C}[x]$ at (x) and let $p(t) = t^3 + (x+1) \in R[t]$. Let

$S = R[t]/(p(t))$. Since $p(t)$ is irreducible, $\mathrm{Aut}_R(S) = C_3$ (the cyclic group of order 3) but $R/(x) = \mathbb{C}$ and $S/(x)S = \mathbb{C}\oplus\mathbb{C}\oplus\mathbb{C}$ has $\mathbb{C}$-automorphism group S_3 (the symmetric group on three letters). It is not always the case that $\mathrm{Aut}_R(S) \to \mathrm{Aut}_{R/I}(S/IS)$ is onto.

Mayer-Vietoris I. Let R be a one-dimensional integral domain with module finite integral closure $\bar{R}$ and conductor $c = \{x \in R \mid \bar{R}\cdot x \subset R\}$. Let S be a finite étale R-algebra. Assume the following.

(a) If P is a maximal ideal in R containing c then there is only one maximal ideal Q in $\bar{R}$ lying over P.

(b) If P is a maximal ideal in R containing c then the natural map $\mathrm{Aut}_R(S) \to \mathrm{Aut}_{R/P}(S/PS)$ is surjective.

(c) $\bar{R}\otimes S \cong \bar{R}^{(n)}$, where $n = \mathrm{rank}_R(S)$.

Then there is an exact sequence of pointed sets

$$\begin{aligned} 1 &\longrightarrow \mathrm{Aut}_R(S) \xrightarrow{\alpha} \mathrm{Aut}_{\bar{R}}(\bar{R}\otimes S)\times \mathrm{Aut}_{R/c}(R/c\otimes S) \\ &\xrightarrow{\beta} \mathrm{Aut}_{\bar{R}/c}(\bar{R}/c\otimes S) \xrightarrow{\gamma} H^1(X,\mathrm{Aut}(\mathcal{S})) \longrightarrow 1. \end{aligned} \tag{2.1}$$

Sketch of the proof. We define explicitly the maps in the sequence. Checking exactness at each term is then a straightforward computation.

The map α is given as $\alpha(\sigma) = (1\otimes\sigma, 1\otimes\sigma)$. The map β is given as $\beta(\tau,\rho) = (1\otimes\tau)(1\otimes\rho)^{-1}$.

Let $P_1,\dots,P_k$ be the maximal ideals of R lying over c. Using hypothesis (a), let $Q_1,\dots,Q_k$ be the maximal ideals in $\bar{R}$ lying over c with $Q_i\cap R = P_i$ $(1\le i\le k)$. Then $c = \cap_i P_i^{f_i} = \cap Q_i^{e_i}$ so $R/c = \oplus R/P^{f_i}$ and $\bar{R}/c = \oplus \bar{R}/Q^{e_i}$. Moreover, $\mathrm{Aut}_{R/c}(S/cS) = \times_i \mathrm{Aut}_{R/P^{f_i}}(R/P_i^{f_i}\otimes S)$ and $\mathrm{Aut}_{\bar{R}/c}(\bar{R}/c\otimes S) = \times_i \mathrm{Aut}_{\bar{R}/Q^{e_i}}(\bar{R}/Q^{e_i}\otimes S)$. If $(\dots,\bar{\sigma}_i,\dots) \in \mathrm{Aut}_{\bar{R}/c}(\bar{R}/c\otimes S)$ then by hypothesis (c) and Lemma 2.5, $\mathrm{Aut}_{\bar{R}}(\bar{R}\otimes S) = S_n = \mathrm{Aut}_{\bar{R}/Q_i^{e_i}}(\bar{R}/Q_i^{e_i}\otimes S)$ so there exists $\sigma_i \in \mathrm{Aut}_{\bar{R}}(\bar{R}\otimes S)$ with σ_i a lift of $\bar{\sigma}_i$. Let $\mathcal{U} = \{U_j\}$ be a cover of $X = \mathrm{Spec}(R)$ with $P_i \in U_j$ if and only if $i = j$. Assign to U_j the identity automorphism if no P_i is in U_j. Since $U_i\cap U_j$ does not contain any points lying over c, $\mathrm{Aut}_{\mathbb{O}(U_i\cap U_j)}(\mathcal{S}(U_i\cap U_j)) = S_n$ and therefore contains the element $a(i,j) = \sigma_i^{-1}\sigma_j$. It is now easy to check $a \in Z^1(\mathcal{U},\mathrm{Aut}(\mathcal{S}))$ is a 1-cocycle and a different choice of cover gives an equivalent cocycle modulo coboundaries, so γ is defined by $\gamma(\dots,\bar{\sigma}_i,\dots) = |a| \in H^1(X,\mathrm{Aut}(\mathcal{S}))$.

Mayer-Vietoris II. Let R be a reduced ring with $X = \mathrm{Spec}(R)$ connected. Let $I_1,\dots,I_q$ be the set of minimal prime ideals of R and $\bar{R} = \oplus_{j=1}^q R/I_j$. Assume $\dim R/I_j = 1$ for all j. Identify R with its natural image in $\bar{R}$ and let $c = \{x\in R \mid \bar{R}\cdot x\subset R\}$ be the conductor. Let $Y = \mathrm{Spec}(\bar{R})$. Let S be a finite étale R-algebra.

(a) Assume for each maximal ideal Q in $\bar{R}$ lying over c the natural map $\mathrm{Aut}_R(S) \to \mathrm{Aut}_{\bar{R}/Q}(\bar{R}/Q\otimes S)$ is a surjection.

Then there is an exact sequence of pointed sets

$$\begin{aligned} 1 &\longrightarrow \mathrm{Aut}_R(S) \xrightarrow{\alpha} \mathrm{Aut}_{\bar{R}}(\bar{R}\otimes S)\times \mathrm{Aut}_{R/c}(R/c\otimes S) \\ &\xrightarrow{\beta} \mathrm{Aut}_{\bar{R}/c}(\bar{R}/c\otimes S) \xrightarrow{\gamma} H^1(X,\mathrm{Aut}(\mathcal{S})) \xrightarrow{\delta} H^1(Y,\mathrm{Aut}(\bar{R}\otimes\mathcal{S})). \end{aligned} \tag{2.2}$$

Sketch of the proof. As in Mayer-Vietoris I, we give the maps explicitly, then checking exactness is a straightforward computation. The map α is defined as $\alpha(\sigma) = (1\otimes\sigma, 1\otimes\sigma)$. The map β is $\beta(\tau,\rho) = (1\otimes\tau)(1\otimes\rho)^{-1}$.

Let $P_1,\dots,P_m$ be the maximal ideals in R lying over c and $Q_{i,j}$ the maximal ideals in $\bar{R}$ lying over c where the projection of $Q_{i,j}$ on R/I_j is proper. Write $c = \cap_{k=1}^m P_k^{f_k} = \cap_{i,j} Q_{i,j}^{e_{i,j}}$. Then $\mathrm{Aut}_{\bar{R}}(\bar{R}\otimes S) = \times_{j=1}^q \mathrm{Aut}_{R/I_j}(R/I_j\otimes S)$, $\mathrm{Aut}_{R/c}(R/c\otimes S) = \times_{k=1}^m \mathrm{Aut}_{R/P_k^{f_k}}(R/P_k^{f_k}\otimes S)$, and $\mathrm{Aut}_{\bar{R}/c}(\bar{R}/c\otimes S) = \times_{i,j}\mathrm{Aut}_{\bar{R}/Q_{i,j}^{e_{i,j}}}(\bar{R}/Q_{i,j}^{e_{i,j}}\otimes S)$. Let $(\dots,\bar{\sigma}_{i,j},\dots)\in \mathrm{Aut}_{\bar{R}/c}(\bar{R}/c\otimes S) = \times_{i,j}\mathrm{Aut}_{\bar{R}/Q_{i,j}^{e_{i,j}}}(\bar{R}/Q_{i,j}^{e_{i,j}}\otimes S)$. By hypothesis (a) there is $\sigma_{i,j}\in \mathrm{Aut}_{R/I_i}(R/I_i\otimes S)$ which reduces to $\bar{\sigma}_{i,j}$. For a fixed i, $\{\sigma_{i,j}\}$ determines an element $\sigma_i \in \mathrm{Aut}_{\bar{R}}(\bar{R}\otimes S)$ where we let σ_i be the identity in $\mathrm{Aut}_{R/I_k}(R/I_k\otimes S)$ if k is not any j. Let $\mathcal{U} = \{U_i\}$ be an open cover of $X = \mathrm{Spec}(R)$ where $P_i \in U_j$ if and only if $i = j$. Let $\gamma(\dots,\bar{\sigma}_{i,j},\dots) = |a| \in H^1(X,\mathrm{Aut}(\mathcal{S}))$ where $a \in Z^1(\mathcal{U},\mathrm{Aut}(\mathcal{S}))$ is given by $a(i,k) = \sigma_i^{-1}\sigma_k \in \mathrm{Aut}_{\mathbb{O}(U_i\cap U_k)}(\mathbb{O}(U_i\cap U_k)\otimes S)$. Note, $\sigma_i^{-1}\sigma_k$ is defined since $U_i\cap U_k$ contains no P_j so $\mathbb{O}(U_i\cap U_j)\otimes S = \mathbb{O}(U_i\cap U_j)\otimes_{\bar{R}}\bar{R}\otimes S$. It is clear that the definition of γ is independent of the choice of cover and our assignment gives a well-defined map.

Let $\mathcal{U} = \{U_i\}$ be an open cover of X constructed as above and let $\pi : Y \to X$ be given by restriction. Let $V_i = \pi^{-1}(U_i)$ so $\mathcal{V} = \{V_i\}$ is an open cover of Y. Given $a \in Z^1(\mathcal{U},\mathrm{Aut}(\mathcal{S}))$, let $\delta(a) \in Z^1(\mathcal{V},\mathrm{Aut}(\bar{R}\otimes\mathcal{S}))$ by $\delta(a)(i,j) = a(i,j)$. This assignment is well defined since $\mathbb{O}_X(U_i\cap U_j) = \mathbb{O}_Y(V_i\cap V_j)$.

Note 2.8. If each R/I_j in Mayer-Vietoris II is integrally closed, $H^1(Y,(\bar{R}\otimes\mathcal{S})) = \{1\}$ by Proposition 2.3. This is the case in all the following examples.

Example 2.9. Let $\mathbb{Q}$ denote the rational numbers, let p,q be prime integers, and let ω be a primitive complex pth root of 1. Let $F=\mathbb{Q}(\omega)$ and $R = F[x,y]/(x^p - qy^p(y-1)^p)$. If q is irreducible in $\mathbb{Z}[\omega]$ then by Eisenstein's criterion $x^p - qy^p(y-1)^p$ is irreducible in $F[x,y]$ so R is a one-dimensional Noetherian integral domain. Note that q is irreducible in $\mathbb{Z}[\omega]$ whenever $p \nmid q-1$, $p \neq q$. Let $S = R[t]/(t^p - q)$. Then S is a finite étale R-algebra which is connected since $t^p - q$ is irreducible in $F[t]$ and $R/(x,y) = F$. Identify x,y with their images in R. The integral closure $\bar{R}$ of R is $R(x/y(y-1))$ and since $(x/y(y-1))^p = q$, $t^p - q = \Pi_{i=0}^{p-1}(t-\omega^i(x/(y(y-1)))) \in \bar{R}[t]$ so $\bar{R}\otimes S \cong \bar{R}^{(p)}$. The maximal ideals lying over c in R are (x,y) and $(x,y-1)$ and the only maximal ideal in $\bar{R}$ lying over (x,y) is (y), the only maximal ideal in $\bar{R}$ lying over $(x,y-1)$ is $(y-1)$. Since $R/(x,y) \cong F$, and $R/(x,y-1) \cong F$, and $t^p - q$ is irreducible in $F[t]$, R satisfies the hypothesis of Mayer-Vietoris I. But $\mathrm{Aut}_R(S) = C_p$, the cyclic group of order p. $\mathrm{Aut}_{\bar{R}}(\bar{R}\otimes S) = S_p$, the symmetric group on p-letters. $\mathrm{Aut}_{R/c}(R/c\otimes S) = C_p\times C_p$ and $\mathrm{Aut}_{\bar{R}/c}(\bar{R}/c\otimes S) = S_p\times S_p$ so for this example the Mayer-Vietoris I sequence becomes

$$1 \longrightarrow C_p \longrightarrow S_p\times(C_p\times C_p) \longrightarrow S_p\times S_p \longrightarrow H^1(X,\mathrm{Aut}(\mathcal{S})) \longrightarrow 1. \tag{2.3}$$

Let $K = \{(\tau\rho^{-1},\tau\sigma^{-1}) \mid \tau\in S_p,\ \rho,\sigma\in C_p\}$. Then $H^1(X,\mathrm{Aut}(\mathcal{S}))$ is bijective with the coset space $S_p\times S_p/K$ and has order $(p-1)!$. In particular, when $p=2$ there are no nontrivial twisted forms, when $p=3$ there is exactly one nontrivial twisted form, and so forth.

Example 2.10. (a) Let R be a Noetherian domain with quotient field K, assume R contains a primitive nth root of 1 and I is a fractional R-ideal in K with $I^n = R$. Assume $p(t) = t^n - a \in R[t]$ is a separable polynomial, and $S = R[t]/(p(t))$, $L = K[t]/(p(t))$. Then the subset $T = \oplus_{j=0}^{n-1} I^j t^j$ of L is a twisted form of S.

(b) Let R be a reduced Noetherian ring with minimal prime ideals $I_1, \ldots, I_q$ and assume the dimension of each R/I_j is one. Let $K = \oplus R/I_j$. Assume R contains a primitive nth root of 1 and I is a finitely generated R-submodule of K with $I^n = R$. Assume $p(t) = t^n - a \in R[t]$ is a separable polynomial and $S = R[t]/(p(t))$, $L = K[t]/(p(t))$. Then the subset $T = \oplus_{j=0}^{n-1} I^j t^j$ of L is a twisted form of S.

Note 2.11. In Example 2.9 if $p = 3$ and $q = 2$ then the nontrivial twisted form T is constructed as in Example 2.10 where the ideal $I = (y, y^{-1}x)$, as one can check by showing the associated cocycle in $H^1(X, \mathrm{Aut}(\mathcal{S}))$ is not a coboundary. Notice T is free as an R-module. Let $\mathcal{F}(S)$ be the set of isomorphism classes of twisted forms of S which are free as R-modules and assume S is free as an R-module. Then there is an exact sequence of pointed sets $1 \to \mathcal{F}(S) \to H^1(X, \mathrm{Aut}(\mathcal{S})) \to H^1(X, \mathrm{Gl}(\mathcal{S}))$. The types of examples given in Example 2.10 all lie in $\mathcal{F}(S)$, but we give in Example 2.12 a twisted form of S whose image in $H^1(X, \mathrm{Gl}(\mathcal{S}))$ is not the identity.

Example 2.12. Let $R = \mathbb{R}[x,y]/(y-1)(y-x^2)$ and $\bar{R} = \mathbb{R}[x,y]/(y-1) \oplus \mathbb{R}[x,y]/(y-x^2)$, where $\mathbb{R}$ is the set of the real numbers. Then $R = \{(p(x,y), q(x,y)) \in \bar{R} \mid p(1,1) = q(1,1);\ p(-1,1) = q(-1,1)\}$. Let $I = \{(p(x,y), q(x,y)) \in \bar{R} \mid p(1,1) = q(1,1);\ p(-1,1) = -q(-1,1)\}$. Then I is an R-submodule of $\bar{R}$, $I^2 = R$, and $R_P \otimes I \cong R_P$ for all prime ideals P of R. Let $p(t) = t^2 + 1$, let $S = R[t]/(t^2+1)$, and take $T = R \oplus It$. Then T is a twisted form of S and T is not a free R-module by cancellation [9] so T is a nontrivial twisted form of S. Notice that T is a Galois extension of R with Galois group of order two induced by complex conjugation but since T is not free, T does not have either a normal basis or a primitive element.

Example 2.13. Consider T as constructed in Example 2.12 and let $w^2 + 1 \in T[w]$. Then $q(w) = w^2 + 1$ is irreducible in $T[w]$ but for each prime ideal Q of T, $q(w)$ is reducible in $T_Q[w]$. This gives an example of an irreducible separable polynomial over a connected commutative ring which factors into linear factors over the localization at every prime ideal or modulo each maximal ideal. If $r(w) = w^2 - 1$ then $S_1 = R[w]/(q(w))$ is not isomorphic to $S_2 = R[w]/(r(w))$ since $S_2 \cong R \oplus R$ but S_1 and S_2 are locally isomorphic. This is an example of two separable polynomials that are locally isomorphic but not isomorphic (in the sense of [4]).

Example 2.14. Let $R = \mathbb{Q}[x,y]/(y-1)(y-x^2)$ as in Example 2.12. Let $p(t) = t^3 - 3t + 1$ and $S = R[t]/(p(t))$. Using the Mayer-Vietoris sequence for the Picard group, [1] or [5], one can check the torsion part of the Picard group is C_2. But Mayer-Vietoris II gives $H^1(X, \mathrm{Aut}(\mathcal{S})) = C_3$ so if T is a nontrivial twisted form of S, then T is not isomorphic to $R \oplus It \oplus It^2$ for any fractional ideal of R with $I^3 = R$.

Example 2.15. If R is as in Example 2.14 and $p(t) = t^3 - 2$, then one can check that $p(t)$ is separable and $p(t)$ factors into linear factors modulo each minimal prime ideal of R but $p(t)$ is irreducible in $R[t]$. Hypothesis (a) of Mayer-Vietoris II fails to hold for this example.

Acknowledgement. This article was written while the author was a visitor at the Eidgenossische Technische Hochschule (ETH) in Zurich, Switzerland. I would like to thank Max Knus and Beno Eckmann of the ETH for several stimulating conversations.

References

[1] H. Bass, *Algebraic K-Theory*, Mathematics Lecture Note Series, vol. 15, W. A. Benjamin, New York, 1968. MR 40#2736. Zbl 174.30302.

[2] F. DeMeyer and E. Ingraham, *Separable Algebras over Commutative Rings*, Lecture Notes in Mathematics, vol. 181, Springer-Verlag, New York, 1971. MR 43#6199. Zbl 215.36602.

[3] J. Giraud, *Cohomologie Non Abélienne*, Die Grundlehren der Mathematischen Wissenschaften, vol. 179, Springer-Verlag, Berlin, 1971 (French). MR 49#8992. Zbl 226.14011.

[4] D. K. Harrison and T. McKenzie, *Toward an arithmetic of polynomials*, Aequationes Math. **43** (1992), no. 1, 21–37. MR 92m:13008. Zbl 759.13005.

[5] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, no. 52, Springer-Verlag, New York, 1977. MR 57#3116. Zbl 367.14001.

[6] G. J. Janusz, *Separable algebras over commutative rings*, Trans. Amer. Math. Soc. **122** (1966), 461–479. MR 35#1585. Zbl 141.03402.

[7] M.-A. Knus, *Quadratic and Hermitian Forms over Rings*, Grundlehren der Mathematischen Wissenschaften, vol. 294, Springer-Verlag, Berlin, 1991. MR 92i:11039. Zbl 756.11008.

[8] J. S. Milne, *Étale Cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, New Jersey, 1980. MR 81j:14002. Zbl 433.14012.

[9] J.-P. Serre, *Modules projectifs et espaces fibrés à fibre vectorielle*, Séminaire P. Dubreil, M.-L. Dubreil-Jacotin, et C. Pisot, 1957/58, Algebre Theorie Nombres, no. 23, Secrétariat Mathématique, Paris, 1958 (French). MR 31#1277. Zbl 132.41202.

Frank DeMeyer: Department of Mathematics, Colorado State University, Fort Collins, CO 80523, USA

E-mail address: demeyer@math.colostate.edu