TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 327, Number 1, September 1991

AUTOMORPHISMS AND TWISTED FORMS OF GENERALIZED WITT LIE ALGEBRAS

WILLIAM C. WATERHOUSE

ABSTRACT. We prove that the automorphisms of the generalized Witt Lie algebras $W(m, \mathbf{n})$ over arbitrary commutative rings of characteristic $p \geq 3$ all come from automorphisms of the algebras on which they are defined as derivations. By descent theory, this result then implies that if a Lie algebra over a field becomes isomorphic to $W(m, \mathbf{n})$ over the algebraic closure, it is a derivation algebra of the type studied long ago by Ree. Furthermore, all isomorphisms of those derivation algebras are induced by isomorphisms of their underlying associative algebras.

INTRODUCTION

In the middle 1950s, Rimhak Ree [5] introduced a collection of Lie algebras over arbitrary fields of characteristic $p > 0$. He showed that they included (properly, over some fields) the class of generalized Witt Lie algebras; I propose to call them Witt-Ree algebra. Fifteen years later, R. L. Wilson [9] showed that over an algebraically closed field, they each become isomorphic to one or another of a fixed collection of generalized Witt Lie algebras $W(m, \mathbf{n})$. These $W(m, \mathbf{n})$ constitute one of the four known types of nonclassical simple Lie algebras over algebraically closed fields, and there is reason to suppose that no other types exist [10]. Thus determining the twisted forms, i.e. the algebras that become isomorphic to $W(m, \mathbf{n})$ over the algebraic closure, is likely to play a major role in the classification of simple Lie algebras over arbitrary fields. In this paper, I shall prove that the Witt-Ree algebras are in fact (for $p \geq 3$) the only such twisted forms. Furthermore, each Witt-Ree algebra is by definition a Lie algebra of derivations, and I shall show that all isomorphisms among them are induced by isomorphisms of the underlying associative algebras.

Though the results just stated are the attractive ones, they are not in fact where most of the work will be done. The fundamental theorem in the paper is that the automorphisms of the Lie algebras $W(m, \mathbf{n})$ over arbitrary commutative rings all come from automorphisms of the algebras on which they are realized as derivations. To understand why this is fundamental, it may help to review the history of the corresponding results in the case of

Received by the editors August 3, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 17B40, 17B50.
This work was supported in part by the National Science Foundation, Grant No. DMS8701690.

ordinary Witt algebras. These are the full derivation algebras W of $A = R[x_1, \dots, x_n]/(x_1^p, \dots, x_n^p)$. Jacobson, who introduced them over forty years ago [3], showed that A and W have the same automorphisms and derivations over any field. This was not sufficient to determine all the twisted forms, though it allowed him to make the right conjecture. The conjecture was proved about twenty years ago by Allen and Sweedler [1], who used an analysis of divided power sequences in certain Hopf algebras associated with A and W. Thereupon I observed that their work essentially proved that the "formal groups" of automorphisms of A and W were the same. By combining this with Jacobson's result and using some reasoning on affine group schemes, I was able to show [7] that A and W had the same automorphisms over all base rings.

It was clear already then that if the automorphism result could be proved independently, we could use it to derive the analysis of twisted forms by descent theory. This is essentially what I have done here in the more general case. Only a bit of theory will be needed, and I have tried to make this paper comprehensible to algebraists with no previous knowledge of flat descent.

I should perhaps mention that all previous work on these automorphisms has followed Jacobson in restricting p to be at least 5; here we shall also include the case $p = 3$ (with one obvious exception for the algebra of dimension 3). But this merely requires a few extra arguments and is not the main point of interest.

1. Definitions and statement of the theorems

Throughout the paper, all fields and rings will have characteristic $p \geq 3$. A finite-dimensional algebra A over a field k is called *purely inseparable of height one* if it has the form

$$A = k[x_1, \dots, x_n]/(x_1^p - \alpha_1, \dots, x_n^p - \alpha_n)$$

for α_i in k. It is not hard to see that these are precisely the algebras for which $A \otimes_k \overline{k} \cong \overline{k}[y_1, \dots, y_n]/(y_1^p, \dots, y_n^p)$. Looking at the pth roots of the α_i in $\overline{k}$, one can show [3, pp. 116–117] that every such A has the form $E[y_{m+1}, \dots, y_n]/(y_{m+1}^p, \dots, y_n^p)$, where E is an inseparable field extension of k of height one. The field E is uniquely determined (it is A modulo nilpotents), and thus there is one purely inseparable algebra A of height one and dimension p^n for every purely inseparable field extension of height one and dimension $\leq p^n$.

Definition. Let A be purely inseparable of height one over a field k, and let W be a Lie subalgebra of $\mathrm{Der}_k(A)$. Then W is a *Witt-Ree algebra* (on A) if the following hold:

(1) W is a free A-module, where aD is given by $(aD)(x) = a(Dx)$.
(2) Only the constants $k \cdot 1$ inside A are annihilated by all of W.
(3) W is central simple.

Lemma 1.1. *Let k be a field. Let W be a Lie algebra of derivations of an algebra A over k. Let L be an extension field of k. Then W is a Witt-Ree algebra on A if and only ιf $W \otimes_k L$ is a Witt-Ree algebra on $A \otimes_k L$.*

Proof. The fixed behavior over the algebraic closure shows that A is purely inseparable of height one iff $A \otimes_k L$ is. Condition (2) is linear, and hence it is clearly true over k iff it is true over L. Condition (3) is equivalent [4, p. 293] to saying that the mappings $[x, -]$ and $[-, x]$ for x in a basis of W generate the full k-algebra of k-linear endomorphisms of W, and hence it too is linear. Clearly $W \otimes_k L$ is free if W is. Finally, if $W \otimes_k L$ is free over $A \otimes_k L$, then W is projective over A. But it is clear from the explicit description that purely inseparable algebras of height one are local rings, and hence W is free over A. □

Example (cf. [9]). Let m be an integer ≥ 1, and let $\mathbf{n} = \{n(1), \ldots, n(m)\}$ be a sequence of integers ≥ 1. Consider elements x_α, where α is an m-tuple of nonnegative integers with ith entry less than $p^{n(i)}$. We make the k-space with this basis into an algebra $A(m, \mathbf{n})$ by the divided power multiplication $x_\alpha \cdot x_\beta = \binom{\alpha+\beta}{\alpha} x_{\alpha+\beta}$. It is easy to verify that this is purely inseparable of height one, with each $x_\alpha^p = 0$ for $\alpha \neq 0$; its dimension is p^n, where $n = \sum n(i)$. We define $W(m, \mathbf{n})$ to be the algebra of derivations generated over A by $D_1, \ldots, D_m$, where D_i sends each x_α to the corresponding basis element with ith entry in α reduced by one. It is easy to verify that these $W(m, \mathbf{n})$ are Witt-Ree algebras. Their definition still makes sense when k is replaced by any commutative ring of characteristic p.

Ree proved [5, 3.5] that an A-basis $D_1, \ldots, D_m$ of any Witt-Ree algebra can be chosen so that all $[D_i, D_j]$ are 0. He also showed [5, 6.1] that any nonzero common eigenvector of the D_i in $A \otimes_k \overline{k}$ is invertible. Using these two properties, Wilson [9, Lemma 3] proved that every Witt-Ree algebra over an algebraically closed field is isomorphic to exactly one of the algebras $W(m, \mathbf{n})$ (with the same parameter m). More precisely, he established a stronger statement for which we should introduce another definition.

Definition. If W_1 and W_2 are Lie algebras of derivations of algebras A_1 and A_2, a *derivation isomorphism* from W_1 to W_2 is an isomorphism induced by an algebra isomorphism of A_1 to A_2 that carries W_1 isomorphically onto W_2.

Theorem (Wilson). *If W is a Witt-Ree algebra over a field k, then $W \otimes_k \overline{k}$ is derivation-isomorphic to exactly one of the $W(m, \mathbf{n})$.* □

Example. When $p = 3$, the algebra $W(1, \{1\})$ is the classical Lie algebra sl_2. It is easy to see that every Witt-Ree algebra of dimension 3 is isomorphic to it. It has a 3-dimensional family of automorphisms (from conjugation by SL_2), whereas the algebra $k[x]/(x^3)$ has only a two-dimensional family of automorphisms. There are (in general) many different Lie algebras over k that become isomorphic to sl_2 over $\overline{k}$; they are given by the elements of trace zero in quaternion algebras over k, and they do not occur as Witt-Ree algebras. In short, all the theorems to be proved in this paper are false for this case, and it will always be excluded.

We can now state our two main classification results.

Theorem A. *Say* $\operatorname{char}(k) \geq 3$. *If* W *is any Lie algebra over* k *for which* $W \otimes_k \overline{k}$ *is isomorphic to some* $W(M, \mathbf{n})$, *then* W *is isomorphic to some Witt-Ree algebra* (*except when* $\dim(W) = 3$).

Theorem B. *For* $\operatorname{char}(k) \geq 3$, *all isomorphisms between Witt-Ree algebras* (*of dimension* > 3) *are derivation isomorphisms.*

As I said earlier, our main work will actually be concerned with automorphisms of the Lie algebras $W = W(m, \mathbf{n})$ over rings, and we should introduce a few abbreviations. We define the basic algebras $A(m, \mathbf{n})$ and $W(m, \mathbf{n})$ over $\mathbb{F}_p$. For any commutative ring R of characteristic p, we set

$$A(R) = A(m, \mathbf{n}) \otimes_{\mathbb{F}_p} R \quad \text{and} \quad W(R) = W(m, \mathbf{n}) \otimes_{\mathbb{F}_p} R.$$

Here $A(R)$ is still a truncated polynomial algebra, and $W(R)$ is a Lie subalgebra of its R-derivations. We let $\operatorname{Aut}(A)(R)$ denote the R-automorphisms of $A(R)$, and similarly for $\operatorname{Aut}(W)(R)$. Clearly $\operatorname{Aut}(A)$ and $\operatorname{Aut}(W)$ are functors on $\mathbb{F}_p$-algebras R. We let $\operatorname{Aut}(A, W)(R)$ denote the automorphisms of $A(R)$ that preserve $W(R)$; this is again a functor. We can now state the fundamental theorem of the paper.

Theorem C. *The map* $\operatorname{Aut}(A, W)(R) \to \operatorname{Aut}(W)(R)$ *is an isomorphism over every commutative ring* R *having characteristic* $p \geq 3$ (*unless* $\dim W = 3$).

This isomorphism was proved by Ree [5, 12.8] when R is an infinite perfect field with $p \geq 5$. But for descent theory, it will be crucial to have the result over rings with nilpotents (rings like $\overline{k} \otimes_k \overline{k}$ for imperfect fields k). Correspondingly, we shall need two different styles of argument. First will come some computations similar to those in Ree's proof (and in the earlier proof by Jacobson [3] for the Witt algebras); these will be followed by more abstract descent theory. Very little structural information on $W(R)$ will be used. The reason for this is that the automorphisms of $A(R)$ do not have to preserve the ideal generated by the $\{x_\alpha | \alpha \neq 0\}$ when R contains nilpotents, and hence the filtration familiar on W over fields is no longer preserved by all automorphisms.

2. Technical preliminaries

Propositon 2.1. *The only* R*-linear maps* $T\colon A(R) \to A(R)$ *that commute with all elements in* $W(R)$ *are scalars.*

Proof. We have $D_i T(1) = T D_i(1) = 0$ for all i, and hence we have $T(1)$ equal to a constant b in R. More generally, each element in $A(R)$ is determined up to a constant term by the values of the D_i on it. For brevity, let x_1 denote $x_{(1,0,\ldots,0)}$. We have $b\delta_{i1} = T(\delta_{i1}) = T(D_i x_1) = D_i T(x_1)$ for each i, and hence we have $T(x_1)$ equal to bx_1 up to a constant. But then $bx_1 = x_1D_1(Tx_1) = (x_1D_1)T(x_1) = T((x_1D_1)x_1) = T(x_1)$, so indeed $Tx_1 = bx_1$. For every α finally we have

$$T(x_\alpha) = T((x_\alpha D_1)(x_1)) = (x_\alpha D_1)T(x_1) = (x_\alpha D_1)(bx_1) = bx_\alpha. \quad \square$$

Corollary 2.2. *The mapping* $\operatorname{Aut}(A, W)(R) \to \operatorname{Aut}(W)(R)$ *is always one-to-one.*

Proof. Any φ in the kernel commutes with all of $W(R)$, so it is scalar; as it is an algebra automorphism, it is the identity. □

Corollary 2.3. *Let ψ be an automorphism of $W(R)$ and let E be an element of $W(R)$ with some p-power E^{p^i} also lying in $W(R)$. Then $\psi(E^{p^i}) = \psi(E)^{p^i}$. In particular, $\psi(E)^{p^i}$ lies in $W(R)$.*

Proof. Let $\operatorname{ad}(Y)$ denote the map $X \mapsto [Y, X]$ on $\operatorname{Der}_R A(R)$. We have $(\operatorname{ad} E)^{p^i} = \operatorname{ad}(E^{p^i})$, as $\operatorname{Der}_R A(R)$ is a restricted Lie algebra. For all X in $W(R)$, then, we have $(\operatorname{ad}(\psi E))^{p^i}(\psi X) = \operatorname{ad}(\psi(E^{p^i}))(\psi X)$, since ψ preserves the Lie algebra structure on elements in $W(R)$. As ψ is an automorphism, the elements ψX run through all of $W(R)$. But of course $(\operatorname{ad} \psi E)^{p^i} = \operatorname{ad}((\psi E)^{p^i})$, and thus $\operatorname{ad}((\psi E)^{p^i}) - \operatorname{ad}(\psi(E^{p^i}))$ is zero on $W(R)$. Thus $(\psi E)^{p^i} - \psi(E^{p^i})$ is a linear mapping from $A(R)$ to $A(R)$ that commutes with all elements in $W(R)$, and hence by the proposition it is a scalar. As it is also a derivation, it is zero. □

This last result is of course a consequence of Theorem C, but we shall need it in the proof. Specifically, we shall need to know that if $E^{p^i} = E$, then $\psi(E^{p^i}) = \psi(E)$.

Despite the naturalness of the algebras $W(m, \mathbf{n})$, we shall find it easier (following Ree) to do computational arguments on a variant form of them. We fix an algebraically closed field k of characteristic p, and we define objects B and X over k as follows. Take a set of variables x_{is} for $1 \le i \le m$ and $1 \le s \le n(i)$. Set all $(x_{is})^p = 1$, to get a purely inseparable algebra B of height one. Let $q(i) = p^{n(i)}$, and for each i fix elements γ_{is} forming an $\mathbb{F}_p$-basis of $\mathbb{F}_{q(i)}$. Define derivations E_i by setting

$$E_i(x_{js}) = \delta_{ij}\gamma_{is}x_{is}.$$

It is easy to see that these E_i are the basis of a Witt-Ree algebra X.

Lemma 2.4. *The algebra X on B is derivation-isomorphic to* $W(m, \mathbf{n}) \otimes k$.

Proof. Suppose first that $m = 1$. Then by Wilson's theorem (already proved in this case by Ree [5, 8.4]), all we need to do is to check that the dimensions are the same, which is obvious. For larger m, both our X and $W(m, \mathbf{n})$ are constructed as composite actions [5, p. 523] on tensor products of algebras of height one, and thus the isomorphism can be extended inductively. □

We now record some computational results about X.

Lemma 2.5. (1) *$(E_i)^{q(i)} = E_i$ for each i.*

(2) *$[x^\alpha E_i, x^\beta E_j] = x^{\alpha+\beta}\{(\sum_s \beta_{is}\gamma_{is})E_j - (\sum_s \alpha_{js}\gamma_{js})E_i\}$.*

(3) *$\mathrm{ad}_X(E_i)$ is diagonal in the basis $x^\beta E_j$ with eigenvalues $\sum_s \beta_{is}\gamma_{is}$.*

(4) *The mappings $(\mathrm{ad}_X(E_i))^{p^t}$ for $1 \le i \le m$ and $0 \le t < n(i)$ are linearly independent.*

Proof. (1) is obvious since each γ_{is} is in $\mathbb{F}_{q(i)}$. Statement (2) is computed by checking the left side on generators of B, and (3) is an immediate consequence of it. For (4), let $0 = \sum_{i,t} b_{it}(\mathrm{ad}_X(E_i))^{p^t}$. When we apply this map to the element $\prod_s (x_{js})^{\tau(s)} E_j$, we get a multiple of that element, and the multiplier must then be zero; thus for each j and all $\tau(s)$ in $\mathbb{F}_p$ we get $0 = \sum_t b_{jt}(\sum_s \gamma_{js}\tau(s))^{p^t}$ for $0 \le t < n(j)$ and $1 \le s \le n(j)$. As the γ_{js} are a basis of $\mathbb{F}_{q(j)}$ over $\mathbb{F}_p$, this says that the polynomial $\sum_t b_{jt}T^{p^t}$ is identically zero on $\mathbb{F}_{q(j)}$. As its degree is less than $q(j)$, its coefficients must all be zero. □

This last argument has shown that the linear equations imposed on the variables b_{jt} over the field k have only the trivial solution. This automatically remains true over every extension ring, and thus statement (4) of the lemma (like the other parts) will remain true over all k-algebras R.

3. Proof of Theorem C, part one: Making $\psi(E_i) = E_i$

Let R be a local ring containing the field k, with maximal ideal $\mathfrak{M}$. Set $B(R) = B \otimes_k R$ and $X(R) = X \otimes_k R$, and let ψ be a fixed R-isomorphism of $X(R)$. We assume $p \ge 3$ and $\dim(X) > 3$.

Lemma 3.1. *There are elements $u_1, \dots, u_n$ in $B(R)$ such that*

(1) *the monomials u^α are a basis of $B(R)$, and*

(2) *for every family $(\lambda_1, \dots, \lambda_m)$ with $\lambda_i \in \mathbb{F}_{q(i)}$, there is exactly one monomial u^α with $\psi(E_i)u^\alpha = \lambda_i u^\alpha$ for all i.*

Proof. The first step is to observe that we have $(E_i)^{q(i)} = E_i$ for each i, and by Corollary 2.3 the mappings $e_i = \psi(E_i)$ also satisfy $(e_i)^{q(i)} = e_i$ for each i. As $\mathbb{F}_{q(i)}$ is contained in k, the roots of the equation $T^{q(i)} - T = 0$ are in R, and the usual diagonalization argument shows that $B(R)$ is a direct sum of the eigenspaces. As R is local, all the eigenspaces are free. The e_i all commute, since the E_i do, and hence in fact we can write $B(R)$ as a direct sum of free submodules on each of which the e_i are all scalars. Choose a basis (v_λ) of $B(R)$ consisting of common eigenvectors for the e_i. We can choose 1 as one of them, since $R \cdot 1$ is preserved by all of $X(R)$ and is a direct summand of $B(R)$. Let M be the maximal ideal in the algebra $B(R)/\mathfrak{M}B(R)$, and consider the $(R/\mathfrak{M})$-space $(B(R)/\mathfrak{M}B(R))/M^2$. It has dimension $n+1$, and the images $\overline{v}_\lambda$ of the v_λ span it over $R/\mathfrak{M}$. Thus, we can find $\overline{u}_1, \dots, \overline{u}_n$ among the $\overline{v}_\lambda$

which (together with 1) give a basis of the space. It follows [3, p. 108] that the monomials $\bar{u}^{\alpha}$ are a basis of $B(R)/\mathfrak{M}B(R)$, and hence (since R is local) that the monomials u^{α} are a basis of $B(R)$.

We have $e_i(u_r) = c_{ir}u_r$ for some values c_{ir} in $\mathbb{F}_{q(i)}$, and then

$$e_i(u^{\alpha}) = \left(\sum_r c_{ir}\alpha_r\right) u^{\alpha} \quad \text{for all } \alpha = (\alpha_r) \text{ in } \mathbb{F}_p.$$

We have p^n different monomials and $\Pi q(i) = p^n$ families of eigenvalues in (2), so to prove (2) it is enough to show that no two monomials have the same family of eigenvalues. If they do, then (subtracting) we get an $\alpha \neq 0$ with $\sum_r c_{ir}\alpha_r = 0$ for $1 \leq i \leq m$. As the α_r are in $\mathbb{F}_p$, we then have also $\sum_r (c_{ir})^{p^t}\alpha_r = 0$ for $0 \leq t < n(i)$. Thus we have a family of n homogeneous equations in n unknowns with a nontrivial solution. Hence the equations are dependent, and there are constants q_{it} in k, not all zero, with $\sum_{i,t} q_{it}(c_{ir})^{p^t} = 0$ for all r. Let $e = \sum_{i,t} q_{it}(e_i)^{p^t}$, a derivation of $B(R)$. This derivation is identically zero, since it vanishes on all u^{α}. Hence of course $0 = \mathrm{ad}(e) = \sum_{i,t} q_{it}\{\mathrm{ad}(e_i)\}^{p^t}$. It follows that the same equation holds for the restrictions $\mathrm{ad}_{X(R)}(e_i)$. But $e_i = \psi(E_i)$ and ψ is an isomorphism on $X(R)$, so the same equation must hold for the $\mathrm{ad}_{X(R)}(E_i)$. But Lemma 2.5(4) shows that no such dependence exists. □

Observe that the reasoning here implies that the m by n matrix (c_{ir}) has rank m.

Lemma 3.2. *If β is any n-tuple with all entries $\leq p-2$, the elements $u^{\beta}e_j$ are a basis of $\{e \in X(R) | [e_i, e] = (\sum c_{ir}\beta_r)e$ for all $i\}$.*

Proof. We do have $[e_i, u^{\beta}e_j] = (\sum_r c_{ir}\beta_r)u^{\beta}e_j$ for every j. The submodule of $X(R)$ where all $\mathrm{ad}(E_i)$ have specified eigenvalues is free of rank m by Lemma 2.5(3); and as ψ is an isomorphism, the same is true for the $\mathrm{ad}(e_i)$. Thus the m elements $u^{\beta}e_j$ will be a basis if we can show that they are independent modulo $\mathfrak{M}$. But if some $\sum_j h_j u^{\beta}e_j$ reduces to zero modulo $\mathfrak{M}$, then $\sum h_j u^{\beta}e_j(u_r) = \sum h_j c_{jr} u^{\beta}u_r$ reduces to zero in $B(R)/\mathfrak{M}B(R)$ for each r. By the hypothesis on β, the elements $u^{\beta}u_r$ are part of a basis of $X(R)$, so $\sum h_j c_{jr}$ is zero mod $\mathfrak{M}$ for each r. Since (c_{jr}) has rank m, it follows that every h_j reduces to zero mod $\mathfrak{M}$. Thus indeed the reductions of the $u^{\beta}e_j$ are independent. □

Lemma 3.3. *The elements u_r are all invertible.*

Proof. It is enough to prove that the $(u_r)^p$, which lie in R, are all invertible. We first suppose that $p \geq 5$. Consider (say) u_1. Let V_s be the space where each $\mathrm{ad}_{X(R)}(e_i)$ has eigenvalue $s \cdot c_{i1}$. We have just seen that for $s < p-1$, the elements $(u_1)^s e_i$ generate V_s. Every bracket $[u_1^{p-2}e_i, u_1^{p-3}e_j]$ involves a factor of $(u_1)^{2p-5}$, and hence $[V_{p-2}, V_{p-3}]$ is contained in $\mathfrak{M}X(R)$ if $(u_1)^p$ is in the maximal ideal $\mathfrak{M}$. But now let U_s be the space where each $\mathrm{ad}_{X(R)}(E_i)$ has eigenvalue $s \cdot c_{i1}$. As ψ is an isomorphism, it maps U_s isomorphically to V_s, and we must have $[U_{p-2}, U_{p-3}]$ contained in $\mathfrak{M}X(R)$. Let $\beta = (\beta_{it})$ be the family in $\mathbb{F}_p$ such that $\sum_t \gamma_{it}\beta_{it} = c_{i1}$ in $\mathbb{F}_{q(i)}$ for each i. Then the elements $x^{s\beta}E_i$ for fixed s and varying i are a basis of U_s. But $[U_{p-2}, U_{p-3}]$ contains $[x^{(p-2)\beta}E_i, x^{(p-3)\beta}E_i] = x^{(-5\beta)}c_{i1}E_i$ for each i. Since the rank of (c_{ir}) is m, at least one c_{i1} is nonzero in k and hence invertible, so $[U_{p-2}, U_{p-3}]$ is not in $\mathfrak{M}X(R)$. This contradiction shows that $(u_1)^p$ is indeed invertible.

Now we suppose $p = 3$, with (of course) $n > 1$. We still know that $u_1e_1, \dots, u_1e_m$ are a basis of the space V_1 where the $\mathrm{ad}_{X(R)}(e_i)$ have eigenvalues c_{i1}, and Lemma 3.2 also shows that $u_1u_2e_1, \dots, u_1u_2e_m$ are a basis of the space V_{12} with eigenvalues $c_{i1} + c_{i2}$. Simple computation then shows that all elements in $[V_1, [V_1, V_{12}]]$ and $[V_{12}, [V_1, V_{12}]]$ involve a factor of $(u_1)^3$ and hence are contained in $\mathfrak{M}X(R)$ if $(u_1)^3$ is in the maximal ideal $\mathfrak{M}$. Again the spaces U_1 and U_{12}, where the E_i have these eigenvalues, are mapped to V_1 and V_{12} by ψ, and thus it suffices to show that $[U_1, [U_1, U_{12}]]$ and $[U_{12}, [U_1, U_{12}]]$ are not both contained in $\mathfrak{M}X(R)$. Let y be the monomial in x with all $E_i(y) = c_{i1}$, and let z be the one with all $E_i(z) = c_{i1} + c_{i2}$. Then the elements yE_i and zE_i are in U_1 and U_{12}, respectively. Computation gives $[yE_i, zE_i] = c_{i2}yzE_i$, $[yE_i, [yE_i, zE_i]] = c_{i2}(c_{i1} + c_{i2})y^2zE_i$, and $[zE_i, [yE_i, zE_i]] = c_{i2}c_{i1}yz^2E_i$. The elements y and z are invertible. As before, some c_{i2} must be nonzero in k and hence invertible. If c_{i1} for this i is invertible, then $[zE_i, [yE_i, zE_i]]$ is not in $\mathfrak{M}X(R)$; while if c_{i1} is not invertible, then $[yE_i, [yE_i, zE_i]]$ is not in $\mathfrak{M}X(R)$. Thus again the contradiction shows that $(u_1)^p$ is invertible. □

Lemma 3.4. *There is an extension ring S (local and free of finite rank over R) and an automorphism φ of $B(S)$ preserving $X(S)$ such that $\psi \otimes_R (\mathrm{id})_S$ modified by the automorphism induced by φ sends each E_i to itself.*

Proof. Suppose for the moment that we had each $(u_r)^p = (y_r)^p$ for some values y_r in R. The y_r must then all be invertible. Our original choice of the u_r required only that they be basis elements of certain eigenspaces, so we can replace u_r by $(y_r)^{-1}u_r$ and assume $(u_r)^p = 1$ for all r. Lemma 3.1(2) shows us that for $1 \le i \le m$ and $1 \le s \le n(i)$, we can find various $v_{is} = \prod u_r^{b(r,is)}$ with $e_j(v_{is}) = \delta_{ij}\gamma_{is}v_{is}$. The v_{is} all still have pth powers equal to 1. Furthermore, suitable monomials in them obviously give all possible families of eigenvalues, and hence they are again generators of the algebra. There is an automorphism φ of $B(R)$ sending each v_{is} to the corresponding original generator x_{is}, and on derivations this obviously carries each e_i to E_i. Thus φ will induce an automorphism of $X(R)$, and if we modify ψ by this automorphism we will have each E_i sent to itself.

Of course a priori the values $z_r = (u_r)^p$ in R may not be pth powers. This is where the extension enters. We let S be the ring

$$S = R[T_1, \dots, T_n]/(T_1^p - z_1, \dots, T_n^p - z_n).$$

This is obviously a free R-module. Reduced modulo $\mathfrak{M}$ it gives an algebra purely inseparable of height one over $R/\mathfrak{M}$. We know that these algebras are all local, and hence S is also local. The monomials in $u_r \otimes 1$ are still a basis of $B(S)$ and still have all the properties described in the earlier lemmas. But now in S we have also forced each $(u_r)^p$ to be a pth power, and the construction of φ can be carried out over S. □

4. Proof of Theorem C, part two: When ψ fixes the E_i

Lemma 4.1. *With the hypotheses and notation of the previous section, suppose also that $\psi(E_i) = E_i$ for $1 \le i \le m$. Then each $\psi((x_{is})^t E_i)$ is a multiple of $(x_{is})^t E_i$. For each i and s, the multipliers as functions of t are invertible constants $\sigma(t)$ with $\sigma(t+u) = \sigma(t)\sigma(u)$ for $t \ne u$.*

Proof. Fix i and s, and for brevity write x for x_{is} and γ for γ_{is}. Clearly ψ preserves the subspaces of $X(R)$ where the $\operatorname{ad}(E_i)$ have specified values, and thus we have $\psi(x^t E_i) = x^t \sum \sigma(t, j) E_i$ for some constants $\sigma(t, j)$. Applying ψ to the equality $[x^t E_i, x^u E_i] = (u - t)\gamma x^{t+u} E_i$ gives us

$$\sum_j \{u\sigma(t, i)\sigma(u, j) - t\sigma(u, i)\sigma(t, j)\}\gamma x^{t+u} E_j$$
$$= \sum_j (u - t)\sigma(t + u, j)\gamma x^{t+u} E_j.$$

Look first at the coefficients of E_i. We get $\sigma(t+u, i) = \sigma(t, i)\sigma(u, i)$ for all $t \ne u$. We also have $\sigma(0, i) = 1$ since by assumption $\psi(E_i) = E_i$. For $0 \ne t$ we have $t \ne -t$, and thus $\sigma(t, i)\sigma(-t, i) = 1$ and all $\sigma(t, i)$ are invertible.

Now look at the $\sigma(t, j)$ with $j \ne i$. The conditions there are $\sigma(0, j) = 0$ and $(u - t)\sigma(t + u, j) = u\sigma(u, j) - t\sigma(t, j)$. Taking t and u to be 1 and $p - 1$, we get $\sigma(p - 1, j) = (p - 1)\sigma(1, j)$. In general it gives then $u\sigma(u, j) = (u - 1)\sigma(u + 1, j) + \sigma(1, j)$, and downward induction on u shows that $\sigma(u, j) = u\sigma(1, j)$ for all u. Thus

$$\psi(x^t E_i) = x^t \left\{ \sigma(t, i)E_i + t\sum_{k \ne i} \sigma(1, k)E_k \right\}.$$

Consider now any $j \ne i$ and choose any $r \le n(j)$. For brevity again set $y = x_{jr}$ and $\delta = \gamma_{jr}$, so we have $E_j y = \delta y$ and $E_k y = 0$ for $k \ne j$. We know $\psi(yE_j)$ has the form $y(\sum_r b_r E_r)$ for some constants b_r. The coefficient b_j is invertible, by the same argument as for $\sigma(1, i)$. We have $0 = [x^t E_i, yE_j] = [\psi(x^t E_i), \psi(yE_j)]$. When we work this out, we see that the coefficient of the

x^tyE_j-term is $t\sigma(1, j)b_j\delta - b_it^2\gamma\sigma(1, j)$. Since this expression must be zero for $t = 1$ and $t = 2$, it is identically zero. But b_j is invertible, and hence $\sigma(1, j)$ must be zero. But j was an arbitrary element different from i. Writing $\sigma(t)$ for $\sigma(t, i)$, we have our result. □

We now need the following cute little fact.

Lemma 4.2. *Let $\sigma: A \to B$ be a function from one abelian group to another, and suppose $\sigma(t + u) = \sigma(t) + \sigma(u)$ for $t \neq u$. Then σ is a homomorphism so long as A has more than three elements.*

Proof. For fixed t, choose v different from 0, t, and $2t$. We have

$$\sigma(2t + v) = \sigma(2t) + \sigma(v)$$

and also $\sigma(2t + v) = \sigma(t + [t + v]) = \sigma(t) + \sigma(t + v) = \sigma(t) + [\sigma(t) + \sigma(v)] = 2\sigma(t) + \sigma(v)$. Thus additivity holds also when $t = u$. □

Lemma 4.3. *Under the hypotheses of Lemma 4.1, there is an isomorphism of $B(R)$ of the form $\varphi(x_i) = \zeta_i x_i$ (with $(\zeta_i)^p = 1$) such that ψ modified by the automorphism induced by φ preserves all the elements $(x_{is})^tE_i$.*

Proof. Suppose first $p \geq 5$. It follows then from Lemma 4.2 that each $t \mapsto \sigma(t)$ is a homomorphism from $\mathbb{F}_p$ to the multiplicative group of R, and hence $\sigma(t) = \zeta^t$ for some $\zeta = \zeta_{is}$ with $\zeta^p = 1$. We define the automorphism by $\varphi(x_{is}) = (\zeta_{is})^{-1}x_{is}$. This preserves all E_i and thus induces an automorphism of $X(R)$, and we can modify ψ by it. After making that modification, we have every $\psi((x_{is})^tE_i) = (x_{is})^tE_i$.

Now let $p = 3$, and suppose first that $m > 1$, so there is some other $E_j \neq E_i$. Let $\tau(s)$ be the coefficient of x^sE_j in $\psi(x^sE_j)$. We have $[x^tE_i, x^sE_j] = s\gamma x^{s+t}E_j$. Applying ψ to this and looking at the coefficient of $x^{s+t}E_j$, we find that $s\gamma\sigma(t)\tau(s) = s\gamma\tau(s+t)$. We get four different equations from this by taking s and t equal to 1 and 2. As we know $\tau(0) = 1$ and $\sigma(2)\sigma(1) = 1$, they give us $\tau(s) = \sigma(s)$ and $\sigma(2) = \sigma(1)^2$ and then $\sigma(1)^3 = 1$, so again we get $\sigma(t) = \zeta^t$ with $\zeta^3 = 1$.

Finally, suppose $p = 3$ and $m = 1$. We then have $n(i) > 1$. Choose z to be another x_{ir} with $r \neq s$, and set $\lambda = \gamma_{ir}$. We know that ψ maps $x^tz^uE_i$ to a linear combination of various $x^tz^uE_j$. Let $c(t, u)$ be the coefficient of $x^tz^uE_i$ in $\psi(x^tz^uE_i)$. We have $[x^tz^uE_i, x^vz^wE_i] = \{(v - t)\gamma + (w - u)\lambda\}x^{t+v}z^{u+w}E_i$. Applying ψ to this and looking at the E_i-term, we get

$$\{(v - t)\gamma + (w - u)\lambda\}c(t, u)c(v, w) = \{(v - t)\gamma + (w - u)\lambda\}c(t + v, u + w).$$

As γ and λ are linearly independent over $\mathbb{F}_3$, we can conclude that

$$c(t, u)c(v, w) = c(t + v, u + w)$$

for $(t, u) \neq (v, w)$. As $c(0, 0)$ is 1, we again know that all $c(t, u)$ are invertible. Thus Lemma 4.2 shows that c is a homomorphism on $\mathbb{F}_3 \times \mathbb{F}_3$, and again $\sigma(t) = c(t, 0) = \zeta^t$ with $\zeta^3 = 1$. □

Lemma 4.4. *Suppose ψ preserves every $(x_{is})^t E_i$. Then ψ is the identity.*

Proof. This is a simple induction. Suppose first that we have a nontrivial monomial x^α involving only the variables $x_{i1}, \dots, x_{i,s-1}$, and we know already that ψ preserves $x^\alpha E_i$. For $t \neq 0$ we have

$$[x^\alpha E_i, (x_{is})^t E_i] = \left\{ t\gamma_{is} - \sum_{r<s} \alpha_{ir}\gamma_{ir} \right\} x^\alpha (x_{is})^t E_i.$$

As $\gamma_{i1}, \gamma_{i2}, \dots$ are independent over $\mathbb{F}_p$, the coefficient on the right here is nonzero. Since ψ preserves the two entries on the left, it must then preserve $x^\alpha (x_{is})^t E_i$. Thus it preserves $X^\alpha E_i$ whenever x^α involves only the i-variables.

Now suppose inductively that ψ preserves $x^\alpha E_i$ whenever x^α involves only variables x_{ks} with k in a certain subset of $\{1, \dots, m\}$ (containing i). Let j be an index outside that subset, and let x^β be a nontrivial monomial involving only variables of the form x_{js}. We have $E_j x^\beta = \tau x^\beta$ for some nonzero τ in k, and we must have $\psi(x^{\alpha+\beta} E_i) = x^{\alpha+\beta} \sum c_r E_r$ for some constants c_r. We also have $[x^{\alpha+\beta} E_i, x^{-\beta} E_j] = -\tau x^\alpha E_i$, and by induction (and the previous paragraph) we know that ψ fixes $x^\alpha E_i$ and $x^{-\beta} E_j$. Hence we have $[x^{\alpha+\beta} \sum c_r E_r, x^{-\beta} E_j] = -\tau x^\alpha E_i$. That is,

$$x^\alpha c_j(-\tau) E_j - x^\alpha c_j \tau E_j + \sum_{r \neq j} x^\alpha c_r (-\tau) E_r = -\tau x^\alpha E_i.$$

Comparing coefficients, we get $c_i = 1$ and $c_r = 0$ for $r \neq i, j$ and $-2c_j = 0$. Thus we have $\psi(x^{\alpha+\beta} E_i) = x^{\alpha+\beta} E_i$. □

Recall now (Lemma 2.4) that the pair (B, X) is derivation-isomorphic to $(A(k), W(k))$. Thus the results of these last two sections can be summed up as follows:

Proposition 4.5 (Weak Form of the Fundamental Theorem). *Let R be a local ring containing the algebraically closed field k, and let ψ be an element of* $\mathrm{Aut}(W)(R)$. *Then there is an extension ring S (local and free of finite rank over R) and an element φ of* $\mathrm{Aut}(A, W)(S)$ *having the same image as ψ in* $\mathrm{Aut}(W)(S)$. □

5. Proof of Theorem C, part three: Descent

In this section, the style of the argument changes heavily, as we use faithful flatness arguments to deduce Theorem C from the weak form (Proposition 4.5) together with Corollary 2.2. I have tried to give enough detail to make the arguments very nearly self-contained.

Among the invertible linear maps from the algebra $A(R)$ to itself, those that are algebra isomorphisms are precisely those that satisfy certain equations on their matrix entries. As $A(m, \mathbf{n})$ is defined over $\mathbb{F}_p$, the equations have coefficients in $\mathbb{F}_p$. This means that there is an $\mathbb{F}_p$-algebra U_0 (given essentially by imposing those equations on a set of variables) such that the elements of $\operatorname{Aut}(A)(R)$ naturally correspond to the $\mathbb{F}_p$-algebra homomorphisms from U_0 to R. (By definition, this says that $\operatorname{Aut}(A)$ is an affine group scheme [8, p. 5] defined over $\mathbb{F}_p$.) Clearly there is similarly an $\mathbb{F}_p$-algebra U_2 such that $\operatorname{Aut}(W)(R) = \mathbb{F}_p\text{-}\operatorname{Alg Hom}(U_2, R)$ for all $\mathbb{F}_p$-algebras R. Since $W(m, \mathbf{n})$ is a vector subspace of $\operatorname{Der}(A(m, \mathbf{n}))$, it is similarly true that the elements of $\operatorname{Aut}(A, W)$ are determined by equations, so $\operatorname{Aut}(A, W)(R) = \mathbf{F}_p\text{-}\operatorname{Alg Hom}(U_1, R)$ for some $\mathbb{F}_p$-algebra U_1.

We have a natural homomorphism from $\operatorname{Aut}(A, W)$ to $\operatorname{Aut}(W)$. Yoneda's Lemma [8, p. 6] says that this natural mapping is induced by a ring homomorphism from U_2 to U_1, and that the natural mapping is bijective for all R iff that ring homomorphism is an isomorphism.

Lemma 5.1. *The mapping* $\operatorname{Aut}(A, W)(R) \to \operatorname{Aut}(W)(R)$ *is bijective for every local R containing k.*

Proof. Take any ψ in $\operatorname{Aut}(W)(R)$, and construct S and φ as in Proposition 4.5. There are two R-algebra maps $S \to S \otimes_R S$, sending s to $s \otimes 1$ and to $1 \otimes s$. Using an R-basis of S, it is easy to see that only elements of R have the same image under both maps. We rephrase this symbolically as saying that the sequence

$$0 \to R \to S \rightrightarrows S \otimes_R S$$

is exact. It follows that any homomorphism $\varphi \colon U_i \to S$ that gives the same values when composed with the two maps $S \rightrightarrows S \otimes_R S$ must have values lying in R. Thus we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Aut}(A, W)(R) \arrow[r] \arrow[d] & \operatorname{Aut}(A, W)(S) \arrow[r, shift left] \arrow[r, shift right] \arrow[d] & \operatorname{Aut}(A, W)(S \otimes_R S) \arrow[d] \\
0 \arrow[r] & \operatorname{Aut}(W)(R) \arrow[r] & \operatorname{Aut}(W)(S) \arrow[r, shift left] \arrow[r, shift right] & \operatorname{Aut}(W)(S \otimes_R S)
\end{tikzcd}$$

in which the rows are exact. In addition, we know by Corollary 2.2 that the vertical maps are one-to-one. Our ψ in $\operatorname{Aut}(W)(R)$ gives an image ψ_S in $\operatorname{Aut}(W)(S)$ which in turn has the same image under both maps into $\operatorname{Aut}(W)(S \otimes_R S)$. But we know that ψ_S in $\operatorname{Aut}(W)(S)$ comes from some φ in $\operatorname{Aut}(A, W)(S)$. The two images of that φ in $\operatorname{Aut}(A, W)(S \otimes_R S)$ give the two images of ψ_S, and hence the two images of φ must be equal. Hence φ actually comes from some φ_R in the subgroup $\operatorname{Aut}(A, W)(R)$. This φ_R must also give ψ, since it does so after the inclusion into $\operatorname{Aut}(A, W)(S)$. As ψ was arbitrary (though the construction of S depended on ψ), we have shown that $\operatorname{Aut}(A, W)(R) \to \operatorname{Aut}(W)(R)$ is bijective. □

Lemma 5.2. *The mapping* $\operatorname{Aut}(A, W)(R) \to \operatorname{Aut}(W)(R)$ *is bijective for every R containing k.*

Proof. This is a quite similar argument. Given ψ, we take a maximal ideal M of R and form the localization R_M, getting an automorphism ψ_M of

$W(R_M)$. By Lemma 5.1, there is some φ_M in $\operatorname{Aut}(A, W)(R_M)$ giving ψ_M. Now $W(R_M)$ and $A(R_M)$ are finitely generated modules; thus, when we write out φ_M in some basis, only finitely many denominators (all outside M) will be used, and we can find a common denominator outside M. Likewise, the fact that φ_M is an automorphism and yields ψ_M is a statement requiring the equality of finitely many entries in R_M and needs only one suitable denominator. All in all, then, we can find an element $d(M)$ in R outside M such that the single-denominator localization $R_{d(M)}$ gives an element $\varphi_{d(M)}$ in $\operatorname{Aut}(A, W)(R_{d(M)})$ yielding $\psi_{d(M)}$ in $\operatorname{Aut}(W)(R_{d(M)})$. The collection of all these $d(M)$ for various M lies in no maximal ideal, so it generates the unit ideal of R. Consequently, some finite subset $\{d(i)\}$ of these denominators generates the unit ideal. Let S be the R-algebra $\Pi R_{d(i)}$. Then we know that S contains an automorphism $\varphi = (\varphi_{d(i)})$ of $A(S)$ that yields ψ_S in $\operatorname{Aut}(W)(S)$. The exact sequence

$$0 \to R \to S \rightrightarrows S \otimes_R S$$

is valid again in this situation; this follows from the faithful flatness of the S thus constructed (see, e.g., [8, 15.6]) and is also not hard to prove directly. The argument in Lemma 5.1 now works exactly as before to show that ψ is in the image of $\operatorname{Aut}(A, W)(R)$. □

Theorem C. *The map* $\operatorname{Aut}(A, W)(R) \to \operatorname{Aut}(W)(R)$ *is an isomorphism for every* R.

Proof. The natural mapping $\operatorname{Aut}(A, W) \to \operatorname{Aut}(W)$ is induced by a ring homomorphism from U_2 to U_1. It is easy to see [8, p. 11] that the restriction of that mapping to k-algebras corresponds to the base-extended homomorphism $U_2 \otimes_{\mathbb{F}_p} k \to U_1 \otimes_{\mathbb{F}_p} k$. As our natural mapping is bijective for k-algebras, it follows that this k-algebra homomorphism is an isomorphism. But then (just by linear algebra) the ring homomorphism $U_2 \to U_1$ must be an isomorphism, and consequently the natural mapping is bijective for all $\mathbb{F}_p$-algebras (= commutative rings of characteristic p). □

6. Relation to the derivations of W

Derivations are just special kinds of automorphisms, and so it is no surprise that Theorem C quickly yields the following result, which was proved in a quite different manner by Ree [6].

Proposition 6.1. *Let k be any field of characteristic $p \geq 3$. The Lie algebra of derivations of $W(k)$ has dimension* $\dim(W) + (n - m)$, *and it is isomorphic to the smallest restricted Lie subalgebra of* $\operatorname{Der}_k(A(k))$ *containing* $W(k)$.

Proof. Inside $\operatorname{Der}_k(A(k))$, the $n - m$ derivations $(D_i)^{p^s}$ for $1 \leq i \leq m$ and $1 \leq s < n(i)$ are easily seen to be independent modulo $W(k)$. Thus the smallest restricted algebra, $\overline{W}$, has dimension at least $\dim(W) + n - m$. It is a general fact [2, Exercise 1.22] that $[\overline{W}, W]$ is contained in W, and it follows from Proposition 2.1 that $\overline{W}$ then injects into the derivations of W. Hence it will suffice to show that the derivations of W form a space of dimension at most $\dim(W) + n - m$.

The derivations of an algebraic structure over k are precisely the automorphisms over $k[\varepsilon]/\varepsilon^2$ that reduce to the identity when we set $\varepsilon = 0$. Thus by Theorem C the derivations of $W(k)$ are precisely the derivations of $A(k)$ that preserve $W(k)$. The action involved is the adjoint action, so $\mathrm{Der}_k(W(k))$ is isomorphic to the subset of derivations d of $A(k)$ for which $[d, W(k)] \subseteq W(k)$.

To determine the dimension involved, we can pass to the algebraic closure and thus assume $\overline{k} = k$. Just to make the notation a bit easier, we can then replace $(A(k), W(k))$ by $(B(k), X(k))$. It is clear from the definition that an element E in $X(k)$ is determined by the values $E(x_{i1})$ for $1 \leq i \leq m$, and that these values in $B(k)$ can be arbitrarily prescribed. For any derivation d of $B(k)$, we can thus find some E in $W(k)$ agreeing with it on all x_{i1}. If then $\mathrm{ad}(d)$ maps $X(k)$ to itself, the same is true of $\mathrm{ad}(d - E)$, and so we can restrict our attention to the d with $d(x_{i1}) = 0$. But then it is trivial to compute that $[d, E_i](x_{j1}) = 0$ for all i and j; thus $[d, E_i]$, being in $X(k)$, must be zero for all i. Clearly d will be determined by the values $d(x_{is}) = \sum_\alpha c_\alpha(i, s)x^\alpha$ for $s > 1$, and we must have

$$\sum_\alpha c_\alpha(i, s)\left(\sum_t \alpha_{jt}\gamma_{jt}\right)x^\alpha = E_j d(x_{is}) = dE_j(x_{is}) = \delta_{ij}\gamma_{is}\sum_\alpha c_\alpha(i, s)x^\alpha$$

for all j. As the γ_{jt} for fixed j are independent, it is easy to see that each $d(x_{is})$ must be a constant multiple of x_{is}. Thus these d give at most $n - m$ extra dimensions. □

Remark. By yet a different argument, Wilson [9, pp. 196–198] showed that this proposition remains valid for $p = 2$. Thus there is still a close relation between $\mathrm{Aut}(A, W)$ and $\mathrm{Aut}(A)$ in characteristic 2 (specifically, they are affine group schemes with the same Lie algebra). One might hope that, as for $p = 3$, the two may be isomorphic except for certain low-dimensional cases.

7. Proof of Theorems A and B

We consider now an algebraic structure that consists of a pair (A_0, W_0), where A_0 is a commutative algebra and W_0 is a Lie subalgebra of derivations of A_0. The automorphisms of the pair $(A(R), W(R))$ then are exactly the set we have been calling $\mathrm{Aut}(A, W)(R)$. Restating material from §1, we get

Lemma 7.1. *The Witt-Ree algebras, viewed as pairs* (A_0, W_0), *are precisely the twisted forms of the pairs* $(A(m, \mathbf{n}), W(m, \mathbf{n}))$. □

Theorem A. *Say* $\mathrm{char}(k) \geq 3$. *If* W *is any Lie algebra over* k *for which* $W \otimes_k \overline{k}$ *is isomorphic to some* $W(m, \mathbf{n})$, *then* W *is isomorphic to some Witt-Ree algebra* (*except when* $\dim(W) = 3$).

Proof. We continue to use the notations A and W. We need to recall the basic nature (though none of the details) of faithfully flat descent theory [8, §V]. Use the isomorphism to identify W_0 with a subset of $W(\overline{k})$. It is then determined as the set of elements $\sum w_i \otimes c_i$ inside $W(\overline{k}) = W(k) \otimes_k \overline{k}$ satisfying an equation of the form $\varphi(\sum w_i \otimes c_i \otimes 1) = \sum w_i \otimes 1 \otimes c_i$, where φ is in $\mathrm{Aut}(W)(\overline{k} \otimes_k \overline{k})$. This φ satisfies a "cocycle condition", an equation relating its three images in $\mathrm{Aut}(W)(\overline{k} \otimes_k \overline{k} \otimes_k \overline{k})$, and conversely every such cocycle gives a twisted form. Thus we have described the twisted forms in a way that mentions only the automorphisms of W over various rings. But of course we can do the same thing to find the twisted forms of the pair (A, W). Theorem C tells us that the homomorphism $\mathrm{Aut}(A, W) \to \mathrm{Aut}(W)$ is an isomorphism for every ring. Thus every cocycle for W actually comes from a cocycle for (A, W), and hence the twisted forms of W all arise from twisted forms of (A, W). Lemma 7.1 tells us that these are the Witt-Ree algebras. □

Theorem B. *For* $\mathrm{char}(k) \geq 3$, *all isomorphisms between Witt-Ree algebras* (*of dimension* > 3) *are derivation isomorphisms.*

Proof. If two Witt-Ree algebras are isomorphic, they certainly are twisted forms of the same $W(m, \mathbf{n})$. The descent theory tells us that if φ and ψ are cocycles, then the isomorphisms between the corresponding twisted forms (viewed as subsets of $W(\overline{k})$) are given by those $\lambda \in \mathrm{Aut}(W)(\overline{k})$ which in a suitable way intertwine φ and ψ. As in the previous proof, these λ must come from automorphisms of (A, W) satisfying the same condition; that is, they correspond to isomorphisms of the twisted forms of (A, W). □

Corollary 7.2. *Let E be a purely inseparable field extension, and let W_0 and W_1 be two Witt-Ree algebras on E. Then they are not isomorphic unless they coincide.*

Proof. The uniqueness in Wilson's theorem shows that they cannot be isomorphic unless they are twisted forms of the same algebra. They then cannot be isomorphic if they are distinct, since there are no algebra automorphisms of E. □

Theorem B implies in particular that each Witt-Ree algebra uniquely determines the isomorphism type of the algebra A_0 on which it acts. For the original Witt algebras, there is actually a one-to-one correspondence between forms of W and forms of A; this is an immediate consequence of the fact that we have $\mathrm{Aut}(A, W) = \mathrm{Aut}(A)$. But this correspondence no longer holds for more general Witt-Ree algebras, even if we make the obvious restriction that they should be of the same type $(m, \mathbf{n})$. Indeed, on any inseparable field extension E of dimension p^2 it is easy to construct distinct Witt-Ree algebras of type $(1, \{2\})$, and Corollary 7.2 shows that they are not isomorphic.

Corollary 7.3. *Let E be a purely inseparable field extension, and let W_0 be a Witt-Ree algebra on E. Then W_0 has no nontrivial automorphisms.* □

This result was proved by Ree [5, 12.2] for the case $m = 1$.

References

1. H. P. Allen and M. E. Sweedler, *A theory of linear descent based upon Hopf algebraic techniques*, J. Algebra **12** (1969), 242–294.
2. N. Bourbaki, *Groupes et algèbres de Lie*, Chapitre I: *Algèbres de Lie*, Hermann, Paris, 1960.
3. N. Jacobson, *Classes of restricted Lie algebras of characteristic* p. II, Duke Math. J. **10** (1943), 107–121.
4. ——, *Lie algebras*, Dover, New York, 1979. (Reprint of 1962 edition, Interscience, New York.)
5. R. Ree, *On generalized Witt algebras*, Trans. Amer. Math. Soc. **83** (1956), 510–546.
6. ——, *Note on generalized Witt Lie algebras*, Canad. J. Math. **11** (1959), 345–352.
7. W. C. Waterhouse, *Automorphism schemes and forms of Witt Lie algebras*, J. Algebra **17** (1971), 34–40.
8. ——, *Introduction to affine group schemes*, Graduate Texts in Math., vol. 66, Springer-Verlag, New York, 1979.
9. R. L. Wilson, *Classification of generalized Witt algebras over algebraically closed fields*, Trans. Amer. Math. Soc. **153** (1971), 191–210.
10. ——, *Simple Lie algebras over fields of prime characteristic*, Proc. Internat. Congr. Math. (Berkeley), 1986, pp. 407–416.

Department of Mathematics, The Pennsylvania State University, University Park, Pennsylvania 16802