AUTOMORPHISMS OF GENERALIZED WITT ALGEBRAS HAVE FIXED POINTS

DAVID LISSNER[1]

Generalized Witt algebras are defined as follows: Let F be a field of characteristic p, $F[x_1, \cdots, x_n]$ the ring of polynomials in n commutative indeterminants over F, $\xi_i \in F$ for $i=1, \cdots, n$, and $(x_1^p-\xi_1, \cdots, x_n^p-\xi_n)$ the ideal generated by the indicated elements. Form the residue class algebra

$$\mathfrak{A} = \frac{F[x_1, \cdots, x_n]}{(x_1^p - \xi_1, \cdots, x_n^p - \xi_n)},$$

and let $\mathfrak{L}$ be the algebra of derivations of $\mathfrak{A}$, considered as a restricted Lie algebra. The generalized Witt algebras are precisely all algebras of this form; they were defined by Jacobson in [2], and the name results from the fact that the specialization $n=1$ and $\xi_1=1$ yields the usual Witt algebras. The purpose of this paper is to prove that for $p \geqq 5$ all automorphisms of these algebras have nontrivial fixed points; actually, we show that the fixed point set of any such automorphism is a vector space of dimension $\geqq n$. As pointed out by Jacobson in [2], it follows from the fact that $\mathfrak{L}$ is simple (as an ordinary Lie algebra) that all automorphisms of the Lie structure of $\mathfrak{L}$ preserve the restricted structure as well; thus the automorphisms of $\mathfrak{L}$ as a Lie algebra and the automorphisms of $\mathfrak{L}$ as a restricted Lie algebra are the same, and we need not distinguish between them.

Let K be the algebraic closure of F and extend $\mathfrak{A}$ to $\mathfrak{A}_K = \mathfrak{A} \otimes_F K$ and $\mathfrak{L}$ to $\mathfrak{L}_K = \mathfrak{L} \otimes_F K$ in the usual way. We will identify $\mathfrak{L}_K$ with the algebra of derivations of $\mathfrak{A}_K$ as indicated by Jacobson in [1, p. 213]. An automorphism σ of $\mathfrak{L}$ extends to an automorphism σ_K of $\mathfrak{L}_K$ in the obvious way. The fixed points of σ are the zeroes of the linear transformation $I-\sigma$; hence they form a subspace of $\mathfrak{L}$ whose dimension is equal to the dimension of the set of zeroes of the extended linear transformation $(I-\sigma)_K = I-\sigma_K$, which in turn is the set of fixed points of σ_K. Hence it will be sufficient to consider the dimension of the fixed point set of σ_K, i.e., we may restrict ourselves to the case in which the base field is algebraically closed.

Thus from now on we will assume that F is algebraically closed; then we have $\xi_i^{1/p} \in F$ for all i.

Let $y_i = x_i - \xi_i^{1/p}$ for each i; then the y_i's also generate $\mathfrak{A}$, and $y_i^p = 0$ for all i. It follows from this and a dimension argument that $\mathfrak{A}$ can

Received by the editors November 30, 1961.

[1] This work was supported in part by NSF grant NSF G-18916.

be represented as

$$\mathfrak{A} = \frac{F[y_1, \cdots, y_n]}{(y_1^p, \cdots, y_n^p)},$$

so it will now be sufficient to consider the one case where $\xi_i = 0$ for all i.

If G is an automorphism of the associative algebra $\mathfrak{A}$, and $D \in \mathfrak{L}$, then $G^{-1}DG \in \mathfrak{L}$ also. The mapping $\sigma_G: \mathfrak{L} \to \mathfrak{L}$ defined by $D\sigma_G = G^{-1}DG$ for all $D \in \mathfrak{L}$ is clearly an automorphism, and Jacobson shows in [2, Theorem 9] that if $p \geqq 5$ these are all the automorphisms of $\mathfrak{L}$. Therefore what we must show is: For every automorphism G of $\mathfrak{A}$ there are at least n linearly independent derivations D of $\mathfrak{A}$ such that $D = G^{-1}DG$, i.e., such that D commutes with G.

Let $\mathfrak{N}$ be the subalgebra of $\mathfrak{A}$ generated by the elements $x_1, \cdots, x_n$; this is easily seen to be the radical of $\mathfrak{A}$, and $\mathfrak{A}$ is the algebra generated by $\mathfrak{N}$ and 1. It is convenient to consider only those derivations which map $\mathfrak{A}$ into $\mathfrak{N}$. Thus what we propose to show is that for any automorphism G of $\mathfrak{A}$, the set of all derivations of $\mathfrak{A}$ into $\mathfrak{N}$ which commute with G is a vector space of dimension $\geqq n$. That this is a vector space is clear; we must estimate its dimension.

If D is any derivation of $\mathfrak{A}$ into $\mathfrak{N}$ then D restricted to $\mathfrak{N}$ is a derivation of $\mathfrak{N}$; call this D'. Similarly if G is any automorphism of $\mathfrak{A}$ then G maps $\mathfrak{N}$ into $\mathfrak{N}$, so that G restricted to $\mathfrak{N}$ is an automorphism of $\mathfrak{N}$; call this G'. If $xDG = xGD$ and $yDG = yGD$ then it follows that $(xy)DG = (xy)GD$ and $(\alpha x + \beta y)DG = (\alpha x + \beta y)GD$ for all $\alpha, \beta \in F$; hence to show that D commutes G it suffices to show that $xDG = xGD$ for all x in a set of generators for $\mathfrak{A}$. The elements $1, x_1, \cdots, x_n$ form such a set, and we have $1GD = 1D = 0 = 1DG$ in any case, so D will commute with G if and only if $x_iDG = x_iGD$ for all i, i.e., if and only if D' commutes with G'. Clearly any derivation D' of $\mathfrak{N}$ can be extended to a derivation D of $\mathfrak{A}$ into $\mathfrak{N}$ by defining $1D = 0$, and D will commute with G if and only if D' commutes with G', so it will now be sufficient to show that if G' is any automorphism of $\mathfrak{N}$ then the set of all derivations of $\mathfrak{N}$ which commute with G' is a vector space of dimension $\geqq n$.

Let I be the finite set $\{0, 1, \cdots, p-1\}$. We will use $(i) = (i_1, \cdots, i_n)$ to denote an element of I^n, (0) for the particular element $(0, \cdots, 0)$, and $X^{(i)}$ for the element $x_1^{i_1}x_2^{i_2} \cdots x_n^{i_n}$ of $\mathfrak{A}$. Then $\{X^{(i)} \mid (i) \in I^n\}$ is a basis for $\mathfrak{A}$, and $\{X^{(i)} \mid (i) \in I^n, (i) \neq (0)\}$ is a basis for $\mathfrak{N}$. Thus each $a \in \mathfrak{A}$ can be written uniquely as

$$a = \sum_{(i) \in I^n} a_{(i)}X^{(i)}, \quad a_{(i)} \in F \quad \text{for all } (i) \in I^n,$$

and $a \in \mathfrak{N}$ if and only if $a_{(0)} = 0$.

Let G be any automorphism of $\mathfrak{N}$, D any derivation of $\mathfrak{N}$, and let

$$x_j G = g_j = \sum g^j_{(i)} X^{(i)}$$

and

$$x_j D = d_j = \sum d^j_{(i)} X^{(i)}$$

for each $j = 1, \cdots, n$. Then $g^j_{(0)} = d^j_{(0)} = 0$ for all j, and for any $a = a(x_1, \cdots, x_n) \in N$ we have $aG = a(g_1, \cdots, g_n)$ since G is an automorphism and

$$aD = \sum_{j=1}^{n} \frac{\partial a}{\partial x_j} d_j$$

since D is a derivation. In particular $x_k DG = d_k G = d_k(g_1, \cdots, g_n)$ and

$$x_k GD = g_k D = \sum_{j=1}^{n} \frac{\partial g_k}{\partial x_j} d_j,$$

so D commutes with G if and only if

$$d_k(g_1, \cdots, g_n) = \sum_{j=1}^{n} \frac{\partial g_k}{\partial x_j} d_j$$

for all $k = 1, \cdots, n$. That is, D commutes with G if and only if

$$(1) \qquad \sum_{(i) \in I^n} d^k_{(i)} g_1^{i_1} \cdots g_n^{i_n} = \sum_{j=1}^{n} \frac{\partial g_k}{\partial x_j} \left[\sum_{(i) \in I^n} d^j_{(i)} X^{(i)} \right]$$

for all $k = 1, \cdots, n$. Note that aside from the condition $d^j_{(0)} = 0$ the d_j's may be perfectly arbitrary, for since $x_j^p = 0$ are the only relations satisfied by the x_j's, the only relations which the d_j's must satisfy are

$$x_j^p D = p x_j^{p-1} d_j = 0,$$

which hold in any case because F has characteristic p. Thus any set of $d^j_{(i)}$'s for which $d^j_{(0)} = 0$ will define a derivation of $\mathfrak{N}$, and this will be the zero derivation only if all the $d^j_{(i)}$'s are 0. It follows that distinct sets of $d^j_{(i)}$'s define distinct derivations, and that a given collection of derivations is linearly independent if and only if the corresponding sets of $d^j_{(i)}$'s are linearly independent.

Now consider G to be fixed. If we substitute $\sum g^s_{(t)} X^{(t)}$ for each g_s in equation (1) and then equate the coefficients of $X^{(i)}$ for all $(i) \neq (0)$ we get a system of $n(p^n - 1)$ *homogeneous* linear equations in the

$n(p^n-1)$ unknowns $d^k_{(i)}$ $((i)\neq(0))$, which will be satisfied if and only if D commutes with G. Thus the number of linearly independent derivations D commuting with G is precisely the number of linearly independent solutions of these equations, and we are in effect trying to show that the rank of this system of equations is $\leqq n(p^n-1)-n$.

Define the degree of $(i)=(i_1, \cdots, i_n)$ to be $i_1+\cdots+i_n$, and let $\mathfrak{N}^h$ denote, as usual, the ideal in $\mathfrak{N}$ generated by all h-fold products $n_1n_2\cdots n_h$; $\mathfrak{N}^h$ is clearly the subspace of $\mathfrak{N}$ spanned by $\{X^{(i)} \mid \deg\ (i)\geqq h\}$. Now consider a fixed (i_0) with $\deg\ (i_0)<h$; we claim that only those $d^j_{(i)}$'s for which $\deg\ (i)<h$ actually occur in the coefficients of $X^{(i_0)}$ in equation (1).

PROOF. The left hand side of equation (1) is

$$d_kG=[\sum d^k_{(i)}X^{(i)}]G=\sum (d^k_{(i)}X^{(i)}G),$$

and G maps $\mathfrak{N}^h$ into $\mathfrak{N}^h$ since G is an automorphism of $\mathfrak{N}$. Thus $\deg\ (i)\geqq h$ implies $d^k_{(i)}X^{(i)}G\in\mathfrak{N}^h$, so that $d^k_{(i)}$ does not occur in the coefficient of $X^{(i_0)}$ in this expression. The right-hand side is

$$\sum\left(\frac{\partial g_k}{\partial x_j}\right)(d^j_{(i)}X^{(i)}),$$

and $\partial g_k/\partial x_j\in\mathfrak{A}$ in any case, so $\deg\ (i)\geqq h$ implies

$$\left(\frac{\partial g_k}{\partial x_j}\right)(d^j_{(i)}X^{(i)})\in\mathfrak{N}^h,$$

and it again follows that $d^j_{(i)}$ does not occur in the coefficient of $X^{(i_0)}$.

Now let I^n_h be the set of all $(i)\in I^n$ such that $(i)\neq(0)$ and $\deg\ (i)<h$, and let l be the number of elements in I^n_h. When we equate the coefficients of $X^{(i)}$ in equation (1) for all $(i)\in I^n_h$ and all $k=1, \cdots, n$ we get nl homogeneous linear equations in the nl unknowns $d^k_{(i)}((i)\in I^n_h)$; we will refer to this system of equations as (*). To show that the entire system of equations has rank $\leqq n(p^n-1)-n$ it will now be sufficient to show that (*) has rank $\leqq nl-n$, i.e., that (*) has at least n linearly independent solutions.

The equations (*) can be interpreted as follows. Let $\overline{\mathfrak{N}}^h$ be the subspace of $\mathfrak{N}$ spanned by $\{X^{(i)} \mid (i)\in I^n_h\}$, and $n\to\bar{n}$ be the natural map of $\mathfrak{N}$ onto $\mathfrak{N}/\mathfrak{N}^h$. Clearly $\mathfrak{N}=\overline{\mathfrak{N}}^h\oplus\mathfrak{N}^h$, so this map induces a vector space isomorphism of $\overline{\mathfrak{N}}^h$ with $\mathfrak{N}/\mathfrak{N}^h$. Thus $\{\overline{X}^{(i)} \mid (i)\in I^n_h\}$ is a basis for $\mathfrak{N}/\mathfrak{N}^h$ and the elements $\bar{x}_1, \cdots, \bar{x}_n$ generate $\mathfrak{N}/\mathfrak{N}^h$. Since G maps $\mathfrak{N}^h$ into $\mathfrak{N}^h$ G defines an induced automorphism $\overline{G}$ of $\mathfrak{N}/\mathfrak{N}^h$ for which

$$\bar{x}_j\overline{G}=[(x_jG)]^-=\bar{g}_j=\sum_{(i)\in I^n_h} g^j_{(i)}\overline{X}^{(i)}$$

for all j. Similarly, it follows from the derivative rule for products that D also maps $\mathfrak{N}^h$ into $\mathfrak{N}^h$, and so defines an induced derivation $\overline{D}$ of $\mathfrak{N}/\mathfrak{N}^h$ for which

$$\bar{x}_j \overline{D} = [(x_j D)]^- = \bar{d}_j = \sum_{(i)\in I_h^n} d_{(i)}^j \overline{X}^{(i)}$$

for all j. Since the $\bar{x}_j$'s generate $\mathfrak{N}/\mathfrak{N}^h$ we have as before that $\overline{D}$ commutes with $\overline{G}$ if and only if $\bar{x}_k \overline{D}\,\overline{G} = \bar{x}_k \overline{G}\,\overline{D}$ for all k. But $\bar{x}_k \overline{D}\,\overline{G} = [(x_k D)G = (x_k DG)]^-$ by the definition of induced maps, and similarly $\bar{x}_k \overline{G}\overline{D} = [(x_k GD)]^-$, so $\overline{D}$ commutes with $\overline{G}$ if and only if $[(x_k DG) = (x_k GD)]^-$ for all k. Now $x_k DG$ and $x_k GD$ are the left- and right-hand sides, respectively, of equation (1), so our condition is that equation (1) should hold modulo $\mathfrak{N}^h$. Since $\overline{X}^{(i)} = 0$ if $(i) \notin I_h^n$ and $\{\overline{X}^{(i)} \mid (i) \in I_h^n\}$ is a basis for $\mathfrak{N}/\mathfrak{N}^h$ this will be the case if and only if the equations obtained by equating the coefficients of $X^{(i)}$ for all $(i) \in I_h^n$ are satisfied. Thus the equations (*) give a necessary and sufficient condition for $\overline{D}$ to commute with $\overline{G}$.

Now let D' be any derivation of $\mathfrak{N}/\mathfrak{N}^h$, and let $\bar{x}_j D' = \sum_{(i)\in I_h^n} f_{(i)}^j \overline{X}^{(i)}$ for each $j = 1, \cdots, n$. If we define a derivation D of $\mathfrak{N}$ by $x_j D = \sum_{(i)\in I_h^n} f_{(i)}^j X^{(i)}$ for all j then we clearly have $\overline{D} = D'$. This shows two things: first, that in the definition of D' the $f_{(i)}^j$'s may be perfectly arbitrary, for any set of $f_{(i)}^j$'s will define a derivation of $\mathfrak{N}$ and hence an induced derivation of $\mathfrak{N}/\mathfrak{N}^h$; and second, that every derivation of $\mathfrak{N}/\mathfrak{N}^h$ is induced by some derivation of $\mathfrak{N}$.

If the $f_{(i)}^j$'s are not all 0 then D' is not 0. It follows as before that a given collection of derivations of $\mathfrak{N}/\mathfrak{N}^h$ is linearly independent if and only if the corresponding sets of $f_{(i)}^j$'s are linearly independent. Hence the number of linearly independent solutions of (*) is the number of linearly independent induced derivations of $\mathfrak{N}/\mathfrak{N}^h$ which commute with $\overline{G}$, which in turn is equal to the total number of linearly independent derivations of $\mathfrak{N}/\mathfrak{N}^h$ which commute with $\overline{G}$. Thus it will now be sufficient to show that for any automorphism $\overline{G}$ of $\mathfrak{N}/\mathfrak{N}^h$ there are at least n linearly independent derivations of $\mathfrak{N}/\mathfrak{N}^h$ which commute with $\overline{G}$.

If we take $h = 2$ this last statement is almost trivial. For then the dimension of $\mathfrak{N}/\mathfrak{N}^2$ is n, and $\mathfrak{N}/\mathfrak{N}^2$ is a ring with trivial multiplication, so every linear transformation is a derivation and every nonsingular linear transformation is an automorphism. Thus we are reduced to showing that if $\overline{G}$ is any nonsingular linear transformation of an n-dimensional vector space then the set of all linear transformations commuting with $\overline{G}$ has dimension $\geqq n$. In fact this is true without the condition that $\overline{G}$ be nonsingular and is, of course, well known. We

include a proof for completeness.

The requirement that a matrix A commute with a given matrix B amounts to a system of homogeneous linear equations for the entries of A, so the dimension of the solution space is invariant under extension of the base field, and we may assume the base field to be algebraically closed. Of course in the current context we have that anyway, but the theorem does not depend on this. Then we may suppose B to be in Jordan canonical form, and it follows that it will be sufficient to prove the statement for $n \times n$ matrices of the form

$$\begin{pmatrix} \lambda & & & \\ 1 & \cdot & & 0 \\ & \cdot & \cdot & \\ & & \cdot & \cdot \\ & 0 & & 1 \quad \lambda \end{pmatrix} = \lambda I + N.$$

A commutes with this matrix if and only if it commutes with N, so we are reduced to showing that there are n linearly independent matrices commuting with N. But the minimum polynomial of N is x^n, so the cyclic subalgebra generated by N has dimension n, and all the matrices of this algebra certainly commute with N.

We have now proved:

THEOREM. *Let F be a field of characteristic p, $\xi_1, \cdots, \xi_n \in F$,*

$$\mathfrak{A} = \frac{F[x_1, \cdots, x_n]}{(x_1^p - \xi_1, \cdots, x_n^p - \xi_n)},$$

and G any automorphism of $\mathfrak{A}$. Then the set of all derivations of $\mathfrak{A}$ which commute with G is a vector space of dimension $\geqq n$.

This, together with the theorem of Jacobson mentioned earlier, gives:

COROLLARY. *With the same hypothesis as in the theorem, suppose that $p \geqq 5$, let $\mathfrak{W}$ be the algebra of derivations of $\mathfrak{A}$, and let σ be any automorphism of $\mathfrak{W}$, considered either as a Lie algebra or as a restricted Lie algebra. Then the set of fixed points of σ is a vector space of dimension $\geqq n$.*

BIBLIOGRAPHY

1. N. Jacobson, *Abstract derivation and Lie algebras*, Trans. Amer. Math. Soc. **42** (1937), 206–224.

2. ———, *Classes of restricted Lie algebras of characteristic p.* II, Duke Math. J. **10** (1943), 107–121.

YALE UNIVERSITY