Can. J. Math., Vol. XXVII, No. 5, 1975, pp. 1011–1021

CARTAN SUBALGEBRAS OF ZASSENHAUS ALGEBRAS

GORDON BROWN

1. Introduction. Cartan subalgebras play a very important role in the classification of the finite-dimensional simple Lie algebras over an algebraically closed field of characteristic zero. It is well-known [**5**, 273] that any two Cartan subalgebras of such an algebra are conjugate, i.e. images of one another under some automorphism of the algebra. On the other hand, there exist finite-dimensional simple Lie algebras over fields of finite characteristic p possessing non-conjugate Cartan subalgebras [**2**; **3**; **4**]. The simple Lie algebras discovered by Zassenhaus [**6**] also possess non-conjugate Cartan subalgebras, and we shall give a complete classification of Cartan subalgebras of these algebras in this paper.

2. Zassenhaus algebras. Let F be an algebraically closed field of characteristic $p > 2$. Any non-trivial finite subgroup Γ of the additive group of F can be used to index the basis elements D_γ of a simple Lie algebra L over F known as a Zassenhaus algebra. Multiplication in L is determined by $D_\alpha D_\beta = (\alpha - \beta)D_{\alpha+\beta}$. The dimension of L is p^n where n is the dimension of Γ as a vector space over P, the prime field of F.

For the purposes of this paper it will be advantageous to use a different basis for L. First, we define

$$w_k = \sum_{\gamma\in\Gamma} \gamma^{p^n-2-k} D_\gamma$$

for $k = -1, 0, \ldots, p^n - 2$. The elements w_k form a basis for L since the matrix of transition from the given basis is nonsingular Vandermonde. Inasmuch as it will later be shown that all Zassenhaus algebras of dimension p^n are isomorphic, we shall without loss of generality assume that Γ is a field, thus facilitating our computations. For such Γ we have that $\sum_{\gamma\in\Gamma}\gamma^k$ is -1 if k is any positive integral multiple of $p^n - 1$ and is 0 for all other non-negative integers k. Using these relations, one readily computes that

$$w_k w_l = (-1)^{k+1}\left[\binom{p^n-2-l}{k+1} + 2\binom{p^n-2-l}{k}\right] w_{k+l} + 2[\delta_{k,-1}\delta_{l0} - \delta_{k0}\delta_{l,-1}]w_{p^n-2}$$

Received February 13, 1974.

if $\binom{r}{s}$ and w_m are defined to be zero when $s < 0$ or $s > r$ and $m = -2$ or $m > p^n - 2$ respectively.

The basis B which we shall employ consists of the elements v_k for $-1 \leqq k \leqq p^n - 2$, where $v_k = w_k - 2\delta_{k,-1}w_{p^n-2}$. Multiplication of these elements is given by $v_k v_l = N_{k\,l} v_{k+l}$ where

$$N_{k\,l} = (-1)^{k+1}\left[\binom{p^n - 2 - l}{k+1} + 2\binom{p^n - 2 - l}{k}\right]$$

for $k + l > -2$ and v_k is defined to be zero for $k < -1$ and for $k > p^n - 2$. One readily computes that $N_{-1\,l} = 1$ for $l \geqq 0$, $N_{0\,l} = l$, and

$$N_{k\,l} = (-1)^{k+1}\frac{(p^n - l - 2)(p^n - l - 3)\dots(p^n - l - (k+1))}{(k+1)!} \times (p^n - l + k) \quad \text{for } k > 0.$$

It will be helpful to observe some important instances in which $N_{k\,l}$ is zero. Noting that any integer k such that $-1 \leqq k \leqq p^n - 2$ can be expressed uniquely in the form $k = \sum_{i=0}^{n-1} k_i p^i$ where $0 \leqq k_i \leqq p - 1$ for $i > 0$ and $-1 \leqq k_0 \leqq p - 2$, we let $k = \sum_{i=0}^{n-1} k_i p^i$ and $l = \sum_{j=0}^{n-1} l_j p^j$. Then $N_{k\,l} = 0$ if there exists an integer r such that $0 \leqq r < n$ and $\sum_{i=0}^{r} (k_i + l_i)p^i \geqq p^{r+1} - 1$ or if $\sum_{i=0}^{r} k_i p^i = \sum_{i=0}^{r} l_i p^i \neq -1$.

We shall denote the space spanned by all v_k for $k \geqq s$ by $\mathscr{L}_s$ and note that

$$\mathscr{L}_{-1} \supset \mathscr{L}_0 \supset \mathscr{L}_1 \supset \dots \supset \mathscr{L}_{p^n-2}$$

is a filtration of L.

Although L has infinitely many non-conjugate Cartan subalgebras if $n > 1$, we shall show that they all fall into two categories:

(1) those of dimension one, of which the algebra spanned by D_0 is an example, and

(2) those of dimension p^{n-1}, of which the algebra spanned by all v_k for $k \equiv 0 (\mathrm{mod}\ p)$ is an example.

3. Automorphisms. For $l \in L$, let

$$\exp(\operatorname{ad} l) = \sum_{j=0}^{p-1} \frac{1}{j!} (\operatorname{ad} l)^j.$$

It is well-known that if $(\operatorname{ad} l)^{(p+1)/2} = 0$, then $\exp(\operatorname{ad} l)$ is an automorphism of L. For Zassenhaus algebras, this result can be sharpened to establish that if $(\operatorname{ad} v_r)^p = 0$, then $\exp(y \operatorname{ad} v_r)$ is an automorphism of L for every $y \in F$. In particular, we have

THEOREM 1. $\exp(y \operatorname{ad} v_r)$ *is an automorphism of* L *for every* $y \in F$ *and every positive integer* $r \leqq p^n - 2$ *except* $p^i - 1$ *for* $1 \leqq i \leqq n - 1$.

Proof. Let $D = y \operatorname{ad} v_r$. Since $\exp D - 1_L$ is nilpotent on L, $\exp D$ is clearly nonsingular on L.

$$(x(\exp D))(z(\exp D)) - (xz)(\exp D) = \sum_{k=p}^{2p-2} \sum_{\nu=k+1-p}^{p-1} \frac{xD^\nu}{\nu!} \frac{zD^{k-\nu}}{(k-\nu)!}.$$

From the list of instances in which $N_{kl} = 0$ it is clear that if $r > 1$, then $xD^\nu zD^{k-\nu} = 0$ for all $k \geqq p$. If $r = 1$, then also $xD^\nu zD^{k-\nu} = 0$ for all $k > p$, and $v_s D^\nu v_t D^{p-\nu} = 0$ unless $s \equiv t \equiv -1 \pmod p$. Even then $v_s D^\nu v_t D^{p-\nu} = 0$ if $p > 3$ since $v_s D^3 = 0$ if $s \equiv -1 \pmod p$. If $p = 3$ and $s \equiv t \equiv -1 \pmod p$, then

$$\sum_{\nu=1}^{p-1} \frac{v_s D^\nu v_t D^{p-\nu}}{\nu!(p-\nu)!} = 0.$$

Thus in every case $(xz)(\exp D) = (x(\exp D))(y(\exp D))$, and $\exp D$ is an automorphism of L.

4. Some one-dimensional Cartan subalgebras. Barnes [**1**] has shown that every Cartan subalgebra H is a minimal Engel subalgebra, i.e. there exists an element $a \in L$ such that $H = E_L(a) = \{x \in L | x(\operatorname{ad} a)^r = 0$ for some integer $r\}$ and $E_L(b) \subseteq E_L(a)$ only if $E_L(b) = E_L(a)$.

If $a \in \mathscr{L}_1$, then since $\operatorname{ad} a$ is nilpotent, $E_L(a)$ is the entire algebra L, which, of course, is not a Cartan subalgebra. The elements lying outside of $\mathscr{L}_1$ are of two types, namely, those which are members of $\mathscr{L}_0$ and those which are not. The elements not in $\mathscr{L}_0$ will be considered in this section.

LEMMA 1. *Let* $l = \sum_{r=-1}^{p^n-2} \lambda_r v_r$, *where* $\lambda_{-1} \neq 0$. *Then there exists an element*

$$l' = \lambda_{-1} v_{-1} + \sum_{k=1}^{n} \mu_k v_{p^k-2}$$

and an automorphism φ *such that* $l\varphi = l'$.

Proof. Suppose that no such conjugate exists. Then among all conjugates $\sum_{r=-1}^{p^n-2} \lambda_r' v_r$ with $\lambda_{-1}' = \lambda_{-1}$, choose one for which the least integer s such that $\lambda_s' \neq 0$ and $s + 2$ is not a power of p is maximal. Since $N_{-1,s+1} \neq 0$, there exists $y \in F$ such that $\exp(y \operatorname{ad} v_{s+1})$ maps $\sum_{r=-1}^{p^n-2} \lambda_r' v_r$ into an element $\sum_{r=-1}^{p^n-2} \lambda_r'' v_r$ with $\lambda_s'' = 0$ and $\lambda_r'' = \lambda_r'$ for all $r < s$, thus contradicting the maximality of s.

Since for $k \neq 0 \in F$, $E_L(ka) = E_L(a)$, the lemma implies that if $a \notin \mathscr{L}_0$, $E_L(a)$ is conjugate to $E_L(b)$, where b is of the form $v_{-1} + \sum_{k=1}^n \mu_k v_{p^k-2}$. In order to determine whether these Engel subalgebras are Cartan subalgebras we shall first deduce some information concerning $\operatorname{ad}(v_{-1} + \sum_{k=1}^n \mu_k v_{p^k-2})$. We shall denote this mapping by A.

LEMMA 2. *There exist polynomials*

$$f_{kl}(x_1, \ldots, x_l) \in F[x_1, \ldots, x_l] - F[x_1, \ldots, x_{l-1}]$$

for $l = 1, 2, \ldots, k$ *such that*

$$v_{p^n-2}A^{p^k} = \sum_{l=0}^{k} f_{k\,l}(\mu_1, \ldots, \mu_l)v_{p^n-2-p^k-l}$$

for $k = 0, 1, 2, \ldots, n$, *where* $f_{k0} = -1$ *for* $0 \leqq k \leqq n - 1$.

Proof. (Note: We shall usually write $f_{k\,l}$ rather than $f_{k\,l}(\mu_1, \ldots, \mu_l)$, and we shall understand $f_{k\,l}$ to mean zero if l is negative.) The proof is by induction on k. $v_{p^n-2}A = -v_{p^n-3}$, verifying the assertion for $k = 0$. In order to facilitate the proof, it will be useful to establish the formulas given in the following two sublemmas.

Sublemma 1. If Lemma 2 holds for all $k \leqq q$, if $i_0, i_1, \ldots, i_n$ are non-negative integers such that $0 < \sum_{\nu=0}^{n} i_\nu \leqq p - 1$, and if m is the least integer such that $i_m \neq 0$, then

$$(1)\quad v_{p^n-2-\Sigma i_\nu p^\nu}A^{p^q} = \sum_{l=0}^{q} f_{q\,l}v_{p^n-2-\Sigma i_\nu p^\nu-p^q-l} + 2\delta_{i_0,p-2}f_{qq}\mu_1 v_{p^n-2-\Sigma_{\nu>0} i_\nu p^\nu} - \delta_{i_m,p-1}f_{q,q-m}\mu_{m+1}v_{p^n-3}.$$

Proof. If $q \leqq m$ the computation of $v_{p^n-2-\Sigma i_\nu p^\nu}A^{p^q}$ parallels that of $v_{p^n-2}A^{p^q}$, thus establishing (1) for this case. If when $\sum_{\nu=0}^{n} i_\nu = 0$, we interpret $\delta_{i_m,p-1}$ to be zero, (1) holds by hypothesis for $\sum i_\nu p^\nu = 0$, and we may proceed by induction. Suppose that $q > m$ and that (1) holds for $v_{p^n-2-\Sigma j_\nu p^\nu}A^{p^q}$ whenever $\sum j_\nu p^\nu < \sum i_\nu p^\nu$ (and $\sum j_\nu \leqq p - 1$) and also for $v_{p^n-2-\Sigma j_\nu p^\nu}A^{p^k}$ whenever $k < q$ (and $\sum j_\nu \leqq p - 1$). Since

$$v_{p^n-2-\Sigma i_\nu p^\nu+p^m}A^{p^m} = \sum_{l=0}^{m} f_{m\,l}v_{p^n-2-\Sigma i_\nu p^\nu+p^m-p^m-l} - 2\delta_{i_0,p-1}\mu_1 v_{p^n-2},$$

it follows that

$$v_{p^n-2-\Sigma i_\nu p^\nu}A^{p^k} = -v_{p^n-2-\Sigma i_\nu p^\nu+p^m}A^{p^k}A^{p^m} + \sum_{l=1}^{m} f_{m\,l}v_{p^n-2-\Sigma i_\nu p^\nu+p^m-p^m-l}A^{p^k} - 2\delta_{i_0,p-1}\mu_1 v_{p^n-2}A^{p^k}.$$

This expression can be evaluated using (1) since it requires the use of only those cases for which (1) has been assumed valid in the induction hypothesis. The computation completes the proof of the sublemma by induction.

Sublemma 2. If k is an integer for which the formula of Lemma 2 holds, then

$$(2)\quad v_{p^n-2}A^{rp^k} = \sum_{j_0+\ldots+j_k=r} \frac{r!}{j_0!\ldots j_k!}[f_{k0}]^{j_0}\ldots[f_{kk}]^{j_k}v_{p^n-2-\Sigma j_{k-\nu}p^\nu} + 2\delta_{r,p-1}[f_{kk}]^{p-1}\mu_1 v_{p^n-2}.$$

Proof. The proof is by induction on r. If $r = 1$, (2) is the formula of Lemma 2 and holds by hypothesis. Suppose that it holds for r where r is a positive integer less than $p - 1$. Applying A^{p^k} to both sides of the formula and computing by means of (1) shows that (2) holds for $r + 1$ and thus for $r = 1, 2, \ldots, p - 1$.

Continuing the proof of Lemma 2, we assume its validity as a formula for $v_{p^n-2}A^{p^q}$ for all non-negative integers $q \leqq k$. Then, by Sublemma 2,

$$v_{p^n-2}A^{(p-1)p^k} = \sum_{j_0+\ldots+j_k=p-1} \frac{(p-1)!}{j_0! \ldots j_k!}[f_{k0}]^{j_0} \ldots [f_{kk}]^{j_k} v_{p^n-2-\Sigma j_{k-\nu}p^\nu} + 2[f_{kk}]^{p-1}\mu_1 v_{p^n-2}.$$

By Sublemma 1, A^{p^k} maps this element onto

$$\sum_{l=0}^{k} f_{k\,l}{}^p v_{p^n-2-p^{k+1-l}} + 2\mu_1 f_{kk}{}^p - \sum_{l=0}^{k} f_{k\,l}{}^p \mu_{k+1-l\ p^n-3}.$$

Thus

$$v_{p^n-2}A^{p^{k+1}} = \sum_{l=0}^{k+1} f_{k+1,\,l} v_{p^n-2-p^{k+1-l}},$$

where $f_{k+1,\,l} = f_{k\,l}{}^p$ for $0 \leqq l \leqq k$ and

$$f_{k+1,k+1} = 2\mu_1 f_{kk}{}^p - \sum_{l=0}^{k} f_{k\,l}{}^p \mu_{k+1-l}.$$

By induction these functions $f_{k+1,\,l}$ fit the description given in the lemma.

LEMMA 3. *There exist polynomials*

$$g_i(x_1, \ldots, x_i) \in F[x_1, \ldots, x_i] - F[x_1, \ldots, x_{i-1}]$$

for $i = 1, \ldots, m$ *such that* $A^{p^n} + g_1(\mu_1)A^{p^{n-1}} + g_2(\mu_1, \mu_2)A^{p^{n-2}} + \ldots + g_n(\mu_1, \ldots, \mu_n)A = 0.$

Proof. It is a consequence of Lemma 2 that the elements $v_{p^n-2}A^{p^s}$ $(s = 0, 1, \ldots, n)$ are linearly dependent by a dependence relation of the form $v_{p^n-2}f(A) = 0$ where

$$f(A) = A^{p^n} + g_1(\mu_1)A^{p^{n-1}} + g_2(\mu_1, \mu_2)A^{p^{n-2}} + \ldots + g_n(\mu_1, \ldots, \mu_n)A$$

with $g_i(x_1, \ldots, x_i) \in F[x_1, \ldots, x_i] - F[x_1, \ldots, x_{i-1}]$. Since v_{p^n-2} is in the null space of $f(A)$, so are the elements $v_{p^n-2}A^r$ $(r = 0, 1, \ldots, p^n - 1)$. Since these elements span L, it follows that $f(A) = 0$.

Several observations concerning properties of A as a linear transformation are easily made. For example, its eigenspaces are one-dimensional. For, suppose that $\rho \in F$ is an eigenvalue of A and that $\sum_{\nu=-1}^{p^n-2} a_\nu v_\nu$ is a non-zero element such that

$$\left[\sum_{\nu=-1}^{p^n-2} a_\nu v_\nu\right]\left[v_{-1} + \sum_{i=1}^{n} \mu_i v_{p^i-2}\right] = \rho \sum_{\nu=-1}^{p^n-2} a_\nu v_\nu.$$

Let q be the least integer such that $a_q \neq 0$. Comparing coefficients of v_{q-1} on both sides of the equation yields a contradiction if $q > -1$. Consequently $a_{-1} \neq 0$. If there existed as many as two linearly independent solutions, there would be a non-trivial linear combination of them in which the coefficient of v_{-1} would be zero, a contradiction. Thus the eigenspace corresponding to ρ is one-dimensional.

If $g_n \neq 0$, then $h(x) = x^{p^n} + \sum_{i=1}^n g_i x^{p^{n-i}}$ does not have repeated roots, and consequently the minimum polynomial of A does not have repeated roots. Thus if $g_n(\mu_1, \ldots, \mu_n) \neq 0$, then A is diagonable and has one-dimensional eigenspaces, $h(x)$ is both the minimum and the characteristic polynomial of A, and the roots of $h(x)$ are an additive subgroup of F. Also, since $E_L(v_{-1} + \sum_{i=1}^n \mu_i v_{p^i-2}) = H$ is one-dimensional, it is a minimal Engel subalgebra, hence a Cartan subalgebra.

Conversely, one can show that for any additive subgroup Γ of F of order p^n, there exist $\nu_1, \ldots, \nu_n \in F$ such that Γ is the spectrum of

$$\operatorname{ad}\left[v_{-1} + \sum_{i=1}^{n} \nu_i v_{p^i-2}\right].$$

For, $\prod_{\gamma \in \Gamma} (x - \gamma)$ is a p-polynominal, i.e., one in which the coefficient of x^r is zero unless r is a power of p. This follows by induction since $\prod_{i \in P} (x - i\gamma_0) = x^p - \gamma_0^{p-1}x$, and if $\prod_{\gamma \in \Gamma_0} (x - \gamma) = k(x)$ is a p-polynomial, then

$$\prod_{i \in P, \gamma \in \Gamma_0} (x - i\gamma_0 - \gamma) = \prod_{i \in P} k(x - i\gamma_0) = k(x)^p - k(\gamma_0)^{p-1}k(x),$$

which is again a p-polynomial. Since F is algebraically closed and $g_i(x_1, \ldots, x_i) \notin F[x_1, \ldots, x_{i-1}]$, the equations $g_i(x_1, \ldots, x_i) = c_i$ $(i = 1, \ldots, n)$ where $c_i \in F$ have a solution. Thus for any p-polynomial $q(x) = x^{p^n} + \sum_{i=1}^n c_i x^{p^{n-i}}$ there exist $\nu_1, \ldots, \nu_n \in F$ such that $q(x) = x^{p^n} + \sum_{i=1}^n g_i(\nu_1, \ldots, \nu_i) x^{p^{n-i}}$.

Continuing to assume that $g_n(\mu_1, \ldots, \mu_n) \neq 0$, we shall determine the product of elements of the root spaces relative to H. Let Γ be the set of characteristic roots of A. If $\gamma \in \Gamma$, let $u_\gamma = \sum_{\nu=-1}^{p^n-2} a_\nu v_\nu$ be that characteristic vector of A corresponding to the root γ for which $a_{-1} = 1$. Thus $u_\gamma = v_{-1} - \gamma v_0 + \ldots$. Since $u_\rho u_\chi$ must be a multiple of $u_{\rho+\chi}$ and since $u_\rho u_\chi = (\rho - \chi)v_{-1} + \ldots$, we have $u_\rho u_\chi = (\rho - \chi)u_{\rho+\chi}$.

For one-dimensional Cartan subalgebras

$$E_L\left[v_{-1} + \sum_{i=1}^{n} \mu_i v_{p^i-2}\right] = E_L(l) \quad \text{and} \quad E_L\left[v_{-1} + \sum_{i=1}^{n} \mu_i' v_{p^i-2}\right] = E_L(l')$$

to be conjugate, it is necessary that there exist $\lambda \neq 0 \in F$ such that the set Γ' of characteristic roots of ad l' is $\{\lambda\gamma | \gamma \in \Gamma\}$ where Γ is the set of characteristic roots of ad l. This condition is also sufficient since if $v_{\lambda\gamma} = \lambda u_\gamma$, then $v_{\lambda\rho}v_{\lambda\chi} = (\lambda\rho - \lambda\chi)v_{\lambda(\rho+\chi)}$.

We summarize the foregoing discussion in the following theorem.

THEOREM 1. *For each additive subgroup Γ of F containing p^n elements, there exists a one-dimensional Cartan subalgebra H of L such that L has a basis $\{u_\gamma | \gamma \in \Gamma\}$ where $u_\rho u_\chi = (\rho - \chi) u_{\rho+\chi}$ and u_0 spans H. Two such subalgebras H_1 and H_2 associated with groups Γ_1 and Γ_2, respectively, are conjugate if and only if there exists $\lambda \in F$ such that $\Gamma_2 = \{\lambda\gamma | \gamma \in \Gamma_1\}$.*

COROLLARY. *All Zassenhaus algebras of dimension p^n are isomorphic.*

We must still consider the algebra $E_L(v_{-1} + \sum_{i=1}^n \mu_i v_{p^i-2})$ when $g_n(\mu_1, \ldots, \mu_n) = 0$. We shall show that it is not a Cartan subalgebra. The characteristic polynomial of A is a p-polynomial. For, the characteristic polynomial

$$\left| xI - \operatorname{ad}\left(v_{-1} + \sum_{i=1}^{n} \mu_i v_{p^i-2}\right)\right|$$

is of the form

$$x^{p^n} + \sum_{j=0}^{p^n-1} h_j(\mu_1, \ldots, \mu_n) x^j$$

where $h_j(\mu_1, \ldots, \mu_n) \in F[\mu_1, \ldots, \mu_n]$. We have previously shown that if j is not a power of p, then $h_j(\mu_1, \ldots, \mu_n)$ is zero whenever $g_n(\mu_1, \ldots, \mu_n) \neq 0$. Thus $h_j(\mu_1, \ldots, \mu_n) g_n(\mu_1, \ldots, \mu_n)$ is zero for all choices of $\mu_1, \ldots, \mu_n$. Since $F[\mu_1, \ldots, \mu_n]$ is an integral domain, and since $g_n(\mu_1, \ldots, \mu_n)$ is not identically zero, it must be that $h_j(\mu_1, \ldots, \mu_n)$ is identically zero. Similarly, $[h_{p^j}(\mu_1, \ldots, \mu_n) - g_j(\mu_1, \ldots, \mu_j)] g_n(\mu_1, \ldots, \mu_n)$ is identically zero, and $h_{p^j}(\mu_1, \ldots, \mu_n)$ must be identical with $g_j(\mu_1, \ldots, \mu_j)$. Thus $h(x) = x^{p^n} + \sum_{i=1}^n g_i(\mu_1, \ldots, \mu_i) x^{p^{n-i}}$ is the characteristic polynomial of A. Thus if $g_n(\mu_1, \ldots, \mu_n) = 0$, the Fitting null component of A is more than one-dimensional, although, as shown previously, the nullity of A is one. Therefore there must exist $b \in L$ such that $bA^2 = 0$ but $bA \neq 0$. Thus bl must be a non-zero multiple of $l = v_{-1} + \sum_{i=1}^n \mu_i v_{p^i-2}$, and so b is not nilpotent on l. Hence the Fitting null component of A is not a nilpotent algebra, hence not a Cartan subalgebra.

5. The remaining Cartan subalgebras. If l is an element of $\mathscr{L}_0$ not in $\mathscr{L}_1$, then l is conjugate to an element of the form $h + \sum_{i=1}^{n-1} \mu_i v_{p^i-1}$, where $h \in H_0$, the algebra spanned by all v_s for $s \equiv 0 (\bmod p)$, and $h \notin \mathscr{L}_1$. (The automorphism accomplishing this is constructed by analogy with the proof of Lemma 1.) Thus the remaining Cartan subalgebras are to be found among subalgebras conjugate to algebras of the form $E_L(h + \sum_{i=1}^{n-1} \mu_i v_{p^i-1})$. It will be shown that all subalgebras of this form are Cartan.

If $\mu_1 = \mu_2 = \ldots = \mu_{n-1} = 0$, $E_L(h) = H_0$, which is a Cartan subalgebra. The space V_u spanned by all v_s with $s \equiv u (\bmod p)$ is a root space relative to H_0.

We shall be able to make profitable use of the mappings $\exp(t \text{ ad } v_{p^i-1})$ for $t \in F$ even though they are not automorphisms. (If they were automorphisms, the resultant sharpening of Lemma 1 would have diminished the list of characteristic polynomials of ad l for $l \notin \mathscr{L}_0$.) Let us denote $\exp(t \text{ ad } v_{p^i-1})$ by $\psi_i(t)$.

If $h = \sum_{s\equiv 0 (\text{mod } p)} b_s v_s$, and $h \notin \mathscr{L}_1$, i.e., $b_0 \neq 0$, then

$$h\psi_1\left(\frac{-\mu_1}{b_0}\right)\psi_2\left(\frac{-\mu_2}{b_0}\right) \dots \psi_{n-1}\left(\frac{-\mu_{n-1}}{b_0}\right)$$

is an element $\sum_{i=0}^{p^n-2} c_i v_i$ where $c_0 = b_0$ and $c_{p^i-1} = \mu_i$. By applying the automorphism mentioned in the first paragraph of this section, one sees that this element is conjugate to one of the form

$$\sum_{s\equiv 0(\text{mod } p)} a_s v_s + \sum \mu_i v_{p^i-1}$$

where $a_0 = b_0$ and $a_s \in F[b_0, b_p, \dots, b_s] - F[b_0, b_p, \dots, b_{s-p}]$. Therefore, since F is algebraically closed, given any element

$$l = \sum_{s\equiv 0(\text{mod } p)} a_s v_s + \sum_{i=1}^{n-1} \mu_i v_{p^i-1}$$

for which $a_0 \neq 0$, there exist elements $t_1, t_2, \dots, t_{n-1} \in F$ and an element $h \in H_0$ (and $\notin \mathscr{L}_1$) such that $h\psi$ is conjugate to l, where $\psi = \psi_1(t_1)\psi_2(t_2) \dots \psi_{n-1}(t_{n-1})$. It is apparent from its action on the basis $\{v_{-1}, v_0, \dots, v_{p^n-2}\}$ that ψ is a non-singular linear transformation on L.

For the proof of the next theorem it will be convenient to introduce a function which may be viewed as measuring how near a mapping comes to being an endomorphism. In particular, let φ be a mapping of L into itself, and define $\bar{\varphi}$ from $L \times L$ to L by $(x, y)\bar{\varphi} = (x\varphi)(y\varphi) - (xy)\varphi$. Thus $\bar{\varphi}$ is identically zero if and only if φ is an endomorphism of L. It is readily established by induction on r that

$$(3) \quad (x\varphi_1 \dots \varphi_r)(y\varphi_1 \dots \varphi_r) = (xy)\varphi_1 \dots \varphi_r + \sum_{i=1}^{r} (x\varphi_1 \dots \varphi_{i-1}, y\varphi_1 \dots \varphi_{i-1})\bar{\varphi}_i\varphi_{i+1} \dots \varphi_r$$

where $\varphi_1 \dots \varphi_{i-1} = 1$ if $i = 1$. In the case where $\varphi = \psi_j(t)$, we have (cf. [**5**, p. 9])

$$(x, y)\bar{\varphi} = \sum_{n=p}^{2p-2} \left[t^n \sum_{i=1+n-p}^{p-1} \frac{x(\text{ad } v_{p^j-1})^i}{i!} \frac{y(\text{ad } v_{p^j-1})^{n-i}}{(n-i)!} \right].$$

Thus $(v_\nu, v_\mu)\bar{\varphi} = 0$ whenever ν (or μ) is not congruent to $-1, 0, \dots, p - 1 (\text{mod } p^{j+1})$ and also whenever $\nu + \mu$ is not congruent to $-1, 0, \dots, p - 2 (\text{mod } p^{j+1})$. Also $(v_\nu, v_\mu)\bar{\varphi} = 0$ whenever $\nu \equiv \mu \equiv 0 (\text{mod } p^{j+1})$ since $v_\nu(\text{ad } v_{p^j-1})^2 = 0$. If $(v_\nu, v_\mu)\bar{\varphi} \neq 0$, then it is a scalar multiple of $v_{\nu+\mu+p^{j+1}-p}$.

THEOREM 2. *$H_0\psi$ is a Cartan subalgebra of L, where*

$$\psi = \psi_1(t_1)\psi_2(t_2)\ldots\psi_{n-1}(t_{n-1})$$

for $t_i \in F$.

Proof. We shall show that $H_0\psi$ is abelian by showing that the terms $(x\varphi_1\ldots\varphi_{i-1}, y\varphi_1\ldots\varphi_{i-1})\bar{\varphi}_i\varphi_{i+1}\ldots\varphi_{n-1}$ of (3) are zero if $\varphi_i = \psi_i(t_i)$ for $i = 1,\ldots, n-1$, and $x = v_\nu$, $y = v_\mu$ for $\nu \equiv \mu \equiv 0 (\text{mod } p)$. From the list in § 2 of instances in which $N_{kl} = 0$ it is apparent that $x\varphi_1\ldots\varphi_{i-1}$ and $y\varphi_1\ldots\varphi_{i-1}$ cannot contain non-zero terms in v_λ where $\lambda \equiv -1, 0, \ldots, p-1 (\text{mod } p^{i+1})$ when expressed in terms of the basis B except for $\lambda \equiv 0, p-1 (\text{mod } p^{i+1})$. But even then, according to the discussion preceding the statement of the theorem

$$(x\varphi_1\ldots\varphi_{i-1}, y\varphi_1\ldots\varphi_{i-1})\bar{\varphi}_i\varphi_{i+1}\ldots\varphi_{n-1}$$

is zero. Thus $H_0\psi$ is abelian. To show that $H_0\psi$ is its own normalizer we consider products $(v_\nu\psi)(v_\mu\psi)$ where $\mu \equiv 0 (\text{mod } p)$. If $(v_\nu\varphi_1\ldots\varphi_{i-1}, v_\mu\varphi_1\ldots\varphi_{i-1})\bar{\varphi}_i\varphi_{i+1}\ldots\varphi_{n-1}$ is not zero, then it is a scalar multiple of $v_{\nu+\mu+p^{i+1}-p}\varphi_{i+1}\ldots\varphi_{n-1}$, except that if $\nu \equiv -1 (\text{mod } p^{i+1})$ and $\mu \equiv 0 (\text{mod } p^{i+1})$ for $i > 1$, it is a linear combination of $v_{\nu+\mu+p^{i+1}-p}\varphi_{i+1}\ldots\varphi_{n-1}$ and $v_{\nu+\mu+p^{i+1}-1}\varphi_{i+1}\ldots\varphi_{n-1}$. For those values of ν and μ such that $(v_\nu\varphi_1\ldots\varphi_{i-1}, v_\mu\varphi_1\ldots\varphi_{i-1})\bar{\varphi}_i \neq 0$, the space spanned by $v_{\nu+\mu+p^{i+1}-p}$ (or by $v_{\nu+\mu+p^{i+1}-p}$ and $v_{\nu+\mu+p^{i+1}-1}$ if $\nu \equiv -1$ and $\mu \equiv 0 (\text{mod } p^{i+1})$) is invariant under $\varphi_1\ldots\varphi_{i-1}$. Thus, in any case, $(v_\nu\psi)(v_\mu\psi)$ is equal to $v_{\nu+\mu}\psi$ plus a linear combination of elements of the form $v_{\nu+\mu+p^{i+1}-p}\psi$ and $v_{\nu+\mu+p^{i+1}-1}\psi$ for $i = 1, 2, \ldots, n-1$, and, in particular, ad $v_0\psi$ is a nonsingular linear transformation of the space spanned by $\{v_\nu\psi | \nu \not\equiv 0 (\text{mod } p)\}$ onto itself. Hence $H_0\psi$ is its own normalizer, and, since it is abelian, a Cartan subalgebra of L.

What Theorem 2 shows us is that $E_L(h + \sum \mu_i v_{p^i-1})$ is a Cartan subalgebra. For, we previously showed that there exist $h' \in H_0$ (and $\notin \mathscr{L}_1$) and ψ such that $h + \sum \mu_i v_{p^i-1} = h'\psi$, and since ad $h'\psi$ is 0 on $H_0\psi$ and nonsingular on the space spanned by $\{v_\nu\psi | \nu \not\equiv 0 (\text{mod } p)\}$ (since $h' \notin \mathscr{L}_1$), $E_L(h'\psi) = H_0\psi$.

Having examined all the Engel subalgebras of L and having determined which are Cartan subalgebras, we now have a complete list of the Cartan subalgebras of L. It would also be of interest to have some information concerning the conjugacy of Cartan subalgebras of the form $H_0\psi$. To this end we establish the following theorem.

THEOREM 3. *If $n > 2$, then L has infinitely many non-conjugate Cartan subalgebras of dimension p^{n-1}. If $n = 2$, L has exactly two non-conjugate Cartan subalgebras of dimension p.*

Proof. Let V_ψ be the root space relative to $H_0\psi$, where $\psi = \psi_1(t_1)\ldots\psi_{n-1}(t_{n-1})$, consisting of those elements of L annihilated by some power of (ad $v_0\psi - 1$). With the aid of some remarks made in the proof of Theorem 2 it is easily shown

https://doi.org/10.4153/CJM-1975-105-4 Published online by Cambridge University Press

that there exist $N_i \in F$, $i = 1, \ldots, n-1$ such that

$$v_{-1}\psi(\mathrm{ad}\, v_0\psi - 1)^2 = t_1 \sum_{i=1}^{n-1} N_i t_i^p v_{p^{i+1}-2}\psi.$$

Therefore $v_\psi = v_{-1}\psi - t_1 \sum_{i=1}^{n-1} N_i t_i^p v_{p^{i+1}-2}\psi \in V_\psi$. It is readily seen that the nullity of ad v_ψ is one, and we shall show that every element v' of V_ψ such that ad v' has nullity one is a conjugate of a scalar multiple of v_ψ. To see this, we note that

$$\{v_\psi, (v_p\psi)v_\psi, (v_{2p}\psi)v_\psi, \ldots, (v_{p^n-p}\psi)v_\psi\}$$

is a basis for V_ψ for V_ψ since V_ψ is p^{n-1}-dimensional and $(H_0\psi)V_\psi \subset V_\psi$, and that by a proof almost identical to that of Theorem 1 $\exp(y\, ad\, v_s\psi)$ is an automorphism, where $y \in F$ and s is a positive multiple of p. Any element of V_ψ of nullity one is expressible as a linear combination of these basis elements with the coefficient of v_ψ being non-zero. Since ad v_ψ maps $H_0\psi$ onto V_ψ, application of the appropriate composition of automorphisms of the form $\exp(y \,\mathrm{ad}\, v_s\psi)$ yields a scalar multiple of v_ψ. Now suppose that $H_0\psi$ and $H_0\psi^*$ are conjugate, where $\psi^* = \psi_1(t_1^*) \ldots \psi_{n-1}(t_{n-1}^*)$. Then v_ψ must be a conjugate of an element u where u is in a root space relative to $H_0\psi^*$ and ad u has nullity one. Thus v must be a conjugate of some scalar multiple of

$$v_{\psi^*} = v_{-1}\psi^* - t_1^* \sum_{i=1}^{n-1} N_i t_i^{*p} v_{p^{i+1}-2}\psi^*.$$

As in Lemma 1, v_ψ is conjugate to an element of the form $v_{-1} + \sum_{k=1}^n \mu_k v_{p^k-2}$. For $k = 1, \ldots, n-1$, μ_k is t_k plus a polynomial in $t_1, t_2, \ldots, t_{k-1}$. Thus $t_1, t_2, \ldots, t_{n-1}$ (and consequently ψ) can be chosen so as to make $\mu_1, \mu_2, \ldots, \mu_{n-1}$ take on any prescribed $(n-1)$-tuple of values in F, and as in § 4 to make the coefficients $g_1, g_2, \ldots, g_{n-1}$ of the characteristic polynomial $h(x)$ assume any $(n-1)$-tuple of values in F. If $h(x) = x^{p^n} + \sum_{i=1}^n g_i x^{p^{n-i}}$ is the characteristic polynomial of ad v_ψ, then the characteristic polynomial of ad cv_ψ, where $c \in F$, is

$$x^{p^n} + \sum_{i=1}^n c^{p^n - p^{n-i}} g_i x^{p^{n-i}} = c^{p^n} h\left(\frac{x}{c}\right).$$

Let us define two p-polynomials $h_1(x)$ and $h_2(x)$ of degree p^n to be equivalent if there exists $c \in F$ such that $h_2(x) = c^{p^n} h_1(x/c)$. This gives us an equivalence relation defined on the set of p-polynomials of degree p^n. If $H_0\psi$ and $H_0\psi^*$ are conjugate, then the characteristic polynomials of ad v_ψ and ad v_{ψ^*} must be in the same equivalence class. For $n > 2$ the characteristic polynomials of ad v_ψ for all $\psi = \psi_1(t_1) \ldots \psi_{n-1}(t_{n-1})$ lie in infinitely many equivalence classes since g_1 and g_2 may assume any values in F. Thus there are infinitely many non-conjugate Cartan subalgebras of the form $H_0\psi$ when $n > 2$. If $n = 2$, on the other hand, then $H_0\psi_1(t)$ and $H_0\psi_1(u)$ are conjugate if $tu \neq 0$ via the automorphism which maps $v_i\psi_1(t)$ onto $c^i v_i\psi_1(u)$ where $c^{p-1}t = u$. H_0 and $H_0\psi(t)$, where $t \neq 0$, are not conjugate since ad v is nilpotent for every $v \in V_{-1}$, which is not true of the elements of the corresponding root space relative to $H_0\psi(t)$. (This can be seen from the fact that $g_1(\mu_1) = -2\mu_1^p$ and $g_2(\mu_1, \mu_2) = \mu_2$, computations derived from the proof of Lemma 2.) This completes the proof of the theorem.

Our results are summarized in the following theorem:

THEOREM 4. *If Γ is an additive subgroup of F of order p^n, then there exists a basis $\{u_\gamma | \gamma \in \Gamma\}$ of L such that $u_\rho u_\chi = (\rho - \chi)u_{\rho+\chi}$, and u_0 spans a Cartan subalgebra H_Γ of L. If H_0 is the algebra spanned by the elements v_s for all $s \equiv 0 (\mathrm{mod}\ p)$, and*

$$\psi = \prod_{i=1}^{n-1} \exp\,(t_i \operatorname{ad} v_{p^i-1})$$

with $t_i \in F$ for $i = 1, \ldots, n-1$, then $H_0\psi$ is a Cartan subalgebra of L. Every Cartan subalgebra of L is conjugate either to a subalgebra H_Γ or to a subalgebra $H_0\psi$. For $n > 1$, there exist infinitely many non-conjugate Cartan subalgebras H_Γ. For $n > 2$, there exist infinitely many non-congugate Cartan subalgebras $H_0\psi$. For $n = 2$, there exist two non-conjugate Cartan subalgebras $H_0\psi$. For $n = 1$, (and $p > 3$), there exist two non-conjugate Cartan subalgebras, H_0 and H_P.

REFERENCES

1. D. W. Barnes, *On Cartan subalgebras of Lie algebras*, Math. Z. *101* (1967), 350–355.

2. Richard Block, *New simple Lie algebras of prime characteristic*, Trans. Amer. Math. Soc. *89* (1958), 421–449.

3. S. P. Demuškin, *Cartan subalgebras of the simple Lie p-algebras W_n and S_n*, Sibirsk. Mat. Ž *11* (1970), 310–325.

4. ——— *Cartan subalgebras of simple nonclassical Lie p-algebras*, Izv. Akad. Nauk SSSR Ser. Mat. *36*(1972), 915–932.

5. Nathan Jacobson, *Lie Algebras* (Interscience, New York, 1962).

6. Hans Zassenhaus, *Über Liesche Ringe mit Primzahlcharakteristik*, Hamb. Ahb. *13* (1939), 1–100.

University of Colorado,
Boulder, Colorado

https://doi.org/10.4153/CJM-1975-105-4 Published online by Cambridge University Press