

ON SCHREIER VARIETIES OF LINEAR ALGEBRAS

BY
JACQUES LEWIN

I. Introduction. A variety \mathfrak{v} of algebraic systems (i.e., a class of algebras defined by identical relations) in which the subalgebras of free algebras are again free is called a Schreier variety. Thus the varieties of groups (Schreier [8]), abelian groups, vector spaces, linear (nonassociative) algebras (Kuroš [5]), Lie algebras (Širšov [9], Witt [12]), commutative algebras, anticommutative algebras (Širšov [10]) are Schreier varieties. Some of the varieties are also what we may call Nielsen varieties, i.e., if g_1, \dots, g_n generate the subalgebra G of the free \mathfrak{v} -algebra F , then there is an effective procedure for obtaining a free set of generators for G . Thus the varieties of abelian groups, vector spaces, groups (Nielsen [7]), Lie algebras (Cohn [2]) are Nielsen varieties. The main purpose of this paper is to show (§III and §IV) that a variety of linear algebras over an infinite field is a Schreier variety if and only if it is a Nielsen variety. The main step of the proof is to show that one can “reduce” the elements g_1, \dots, g_n of a free algebra in a Schreier variety to a free set of generators by applying a sequence of “elementary transformations” i.e., transformations which (a) replace a sequence s_1, \dots, s_n by a linear transform of s_1, \dots, s_n or (b) fix s_1, \dots, s_{n-1} and replace s_n by $s_n + w$, with w in the algebra generated by s_1, \dots, s_{n-1} .

Our main theorem then enables us to find a set of generators for the automorphism group of a finitely generated free algebra in a Schreier variety (see Cohn [2] for the case of Lie algebras) and to solve the generalized word problem for the free algebras in Schreier varieties defined by finitely many multilinear identical relations (§V). Our results apply in particular to the varieties of all linear algebras, commutative algebras, anticommutative algebras, and Lie algebras.

II. Notation and preliminary results.

1. All algebras are not necessarily associative linear algebras with identity 1 over the infinite field ϕ . If S is a subset of an algebra A , $\langle S \rangle$, $\text{Alg}(S)$, $\text{Id}(S)$ denote respectively the subspace, subalgebra, ideal of A generated by S .

Let X be a set. We denote by $F=F(X)$ the free algebra freely generated by X . Thus if $M=M(X)$ is the free groupoid (see e.g., [1, p. 1]) on X , then $M \cup \{1\}$ is a ϕ -basis for F , and the multiplication in F is an extension by linearity of the multiplication in $M \cup \{1\}$. A monomial in F is an element of $M \cup \{1\}$. The degree $d(m)$ of a monomial is defined as usual by setting $d(1)=0$, $d(x)=1$ for $x \in X$ and $d(xm)=d(mx)=d(m)+1$ for $x \in X$ and $m \in M$. Let H^k be the subspace of

Received by the editors April 14, 1967.

F generated by the monomials of degree k . Then F is graded by the H^i i.e., $F = \sum_{i=0}^{\infty} \bigoplus H^i$ and $H^i H^j \subset H^{i+j}$. An element of F is homogeneous if it lies in some H^i .

Let now N be an ideal of F generated by a set of homogeneous elements and let $\eta: F \rightarrow F/N = A$ be the natural epimorphism. Then it is easily verified that the $H^i \eta$ grade A . If m is a monomial in F , we also call $m\eta$ a monomial. It is clear that $H^i \eta$ has a basis consisting of monomials, and thus so does A . We choose a fixed monomial basis B for A . Then, if $0 \neq w \in A$, w can be uniquely written as

$$w = \sum_{i=1}^n \alpha_i m_i, \quad \alpha_i \neq 0, m_i \in B, m_i = m_j \Leftrightarrow i = j.$$

We call n the length of w . Likewise, since the $H^i \eta$ generate their direct sum, w can also be uniquely written as

$$w = \sum_{i=1}^l h_{k_i}, \quad h_{k_i} \neq 0, h_{k_i} \in H^{k_i}, k_1 < k_2 < \dots < k_l.$$

We call the h_{k_i} 's the homogeneous terms of w and we call l the homogeneous length of w . w is homogeneous if it has homogeneous length 1. $d(w) = k_l$ is the degree of w , and $i(w) = k_1$ is the index of w . It is clear that if h_1 and h_2 are homogeneous and $h_1 h_2 \neq 0$, then $d(h_1 h_2) = d(h_1) + d(h_2)$. Also, if w_1 and w_2 are distinct elements of A , then $d(w_1 - w_2) \leq \max(d(w_1), d(w_2))$ and $i(w_1 - w_2) \geq \min(i(w_1), i(w_2))$.

If S is a finite subset of A , the degree (homogeneous length) of A is the sum of the degrees (homogeneous lengths) of the nonzero elements of S .

We will make repeated use of the following (probably well known) fact:

PROPOSITION 1. *Let A be a finitely generated graded algebra as defined above. If θ is an endomorphism of A onto A , then θ is an automorphism.*

Proof. Suppose $w \in \text{Ker } \theta$, with $d(w) = d$. Let $K = \sum_{i=d+1}^{\infty} \bigoplus H^i \eta$. Then K is an ideal of A and $w \notin K$. Since $K\theta \subset K$, θ induces an endomorphism $\bar{\theta}$ of A/K onto A/K , and since A/K is finite dimensional, $\bar{\theta}$ is an automorphism. However, $(w+K)\bar{\theta} = w\theta + K = K$ and hence $w \in K$. This contradiction proves the proposition.

2. Let now X be countably infinite and let V be a subset of $F(X)$. If A is an algebra we define $v(A)$ to be the ideal of A generated by all the elements $v(a_1, \dots, a_k)$ where $v(x_1, \dots, x_k) \in V$, $x_i \in X$ and $a_i \in A$. The variety v is the class of all those algebras A for which $v(A) = 0$. Let Y be a set of cardinal c . The algebra $F(v, Y) = F(Y)/v(F(Y))$ is called the free v -algebra of rank c freely generated by Y . An algebra A is a free v algebra if it is isomorphic to $F(v, Y)$ for some Y . A subset S of an algebra in v is a v -free set if it freely generates a free v -algebra. Thus S is a v -free set if whenever $v(s_1, \dots, s_k) = 0$, with $s_1, \dots, s_k \in S$, then $v(x_1, \dots, x_k) \in v(F(X))$. We note that the above are all standard notions in the theory of universal algebras (see e.g., [3]).

Since ϕ is assumed to be infinite, we may apply a familiar Vandermonde determinant argument (see e.g., [4, Proposition 2, p. 234]) to prove the crucial

PROPOSITION 2. *If Y is any set, and V any subset of X , then $\mathfrak{v}(F(Y))$ is generated by a set of homogeneous elements.*

Thus the notions of §I are applicable to $F(\mathfrak{v}, Y)$.

A variety is a Schreier variety if the subalgebras of free \mathfrak{v} -algebras are again free \mathfrak{v} -algebras.

3. Let now $F(\mathfrak{v}, \{x_1, \dots, x_n\})$ be the free algebra of rank n in some variety \mathfrak{v} . A transformation $\tau: (x_1, \dots, x_n) \rightarrow (y_1, \dots, y_n)$ is an elementary transformation of order n if either

- (i) τ is a nonsingular ϕ -linear transformation, or
- (ii) $y_1 = x_1, \dots, y_{n-1} = x_{n-1}, y_n = x_n + w$ with $w \in \text{Alg}(x_1, \dots, x_{n-1})$.

Let A be any algebra in \mathfrak{v} and (a_1, \dots, a_n) an n -tuple of elements of A . Let also $\varphi: F \rightarrow A$ be the homomorphism for which $x_i \varphi = a_i$. We define $(a_1, \dots, a_n)\tau$ by setting $(a_1, \dots, a_n)\tau = (b_1, \dots, b_n)$ with $b_i = y_i \varphi$.

\mathfrak{v} is a Nielsen variety if whenever a_1, \dots, a_m are elements of a free \mathfrak{v} algebra F of finite rank, then there is a sequence τ_1, \dots, τ_k of elementary transformations of order m such that

$$(\cdots((a_1, \dots, a_m)\tau_1)\cdots)\tau_k = (b_1, \dots, b_m)$$

and the terms of positive degree among b_1, \dots, b_m freely generate the free subalgebra $\text{Alg}(a_1, \dots, a_m)$ of F .

III. Schreier varieties are Nielsen varieties.

1. Let $F = F(\mathfrak{v}, X)$ be the free \mathfrak{v} -algebra of countable rank freely generated by X in some variety \mathfrak{v} . We now drop the \mathfrak{v} from \mathfrak{v} -algebra, \mathfrak{v} -free, etc., whenever the context is clear. A subalgebra R of F is homogeneous if it has a generating set which consists of homogeneous elements. R is homogeneous if, and only if, whenever $w \in R$ then the homogeneous terms of w are also in R .

We first consider homogeneous subalgebras.

LEMMA 1. *Let R be a homogeneous subalgebra of F and suppose R is generated by $Y = \{y_1, \dots, y_n\}$. Let h_i be the homogeneous term of y_i of highest degree. If $H = \{h_1, \dots, h_n\}$ is a free set, then H freely generates R .*

Proof. We proceed by induction on the homogeneous length of Y . If the homogeneous length of Y is n , then either each y_i is homogeneous or some y_i is a constant and there is nothing to prove. Suppose then that the lemma has been proved for sets of generators of homogeneous length s , and that Y has homogeneous length $s+1$.

We reorder the y_i 's if necessary so that $y_1 = h_1, \dots, y_r = h_r$ are homogeneous, and

$$y_{r+i} = l_{r+i} + \bar{y}_{r+i} + h_{r+i}, \quad i = 1, \dots, n-r,$$

with l_{r+i} the homogeneous term of least degree in y_{r+i} . We may further assume that

$d(l_{r+i}) \leq d(l_{r+i+1})$. Since R is homogeneous, $l_{r+1} \in R$ and hence there is an element

$$w(x_1, \dots, x_n) = \sum_{i=1}^k \alpha_i m_i(x_1, \dots, x_n), \quad m_i \in B, \alpha_i \neq 0$$

of F , which we may choose to be of minimal length, for which

$$(1) \quad l_{r+1} = w(y_1, \dots, y_n).$$

It is clear that if m is a monomial, then either $m(h_1, \dots, h_n) = 0$ or $d(m(h_1, \dots, h_n)) = d(m(y_1, \dots, y_n))$. Now, if $m_l(h_1, \dots, h_r) = 0$ for some l , then, since H is a free set, $m_l(y_1, \dots, y_n) = 0$, and hence $l_{r+1} = \sum_{i \neq l} \alpha_i m_i(y_1, \dots, y_n)$, a contradiction to the minimality of the length of w . We may then partition the set $\{1, \dots, k\}$ by declaring that $j \in S_1$, if $m_j(h_1, \dots, h_n) = \max_{1 \leq j \leq r} d(m_j(h_1, \dots, h_n))$ and $j \in S_2$ otherwise. If we put $h = \sum_{i \in S_1} \alpha_i m_i(h_1, \dots, h_n)$, then equating terms of the same degree in (1), we see that $h = 0$ or $h = l_{r+1}$. If $h = 0$, then $\sum_{i \in S_1} \alpha_i m_i(y_1, \dots, y_n) = 0$ and we again contradict the minimality of w . Thus $h = l_{r+1}$. But then, since $d(h_{r+1}) > d(l_{r+1})$, each m_i has degree 0 or is monomial in x_1, \dots, x_r only. Thus $w(y_1, \dots, y_n) \in \text{Alg}(y_1, \dots, y_r)$ and the set $Y' = \{y'_1, \dots, y'_n\}$ defined by

$$y'_1 = y_1, \dots, y'_r = y_r, \quad y'_{r+1} = w(y_1, \dots, y_n), \quad y'_{r+2} = y_{r+2}, \dots, y'_n = y_n$$

is again a set of generators for R . However, Y' has homogeneous length s , and the homogeneous term of y'_1 of highest degree is still h_i . Thus, applying the induction hypothesis, $R = \text{Alg}(H)$ and the lemma is proved.

Let $F^k = \sum_{i=0}^k H^k$. If R is a subalgebra of F , we set, following Witt [11], $R_{-1} = 0$, $R_k = R \cap F^k$ and $R'_k = \text{Alg}(R_{k-1}) \cap F^k$. We can now easily prove

LEMMA 2. *Let $H = \{h_1, \dots, h_n\}$ be a set of homogeneous elements of F . Let $H_k = \{h_i \mid d(h_i) = k\}$ and let $R = \text{Alg}(H)$. Then $\langle H_k \rangle = R_k \text{ mod } R'_k$ and $\text{Alg}(R_k) = \text{Alg}(H_1 \cup \dots \cup H_k)$.*

We can now prove our main theorem for homogeneous subalgebras.

THEOREM 1. *Let \mathfrak{v} be a variety in which finitely generated homogeneous subalgebras of free \mathfrak{v} -algebras are again free \mathfrak{v} -algebras. Let $H = \{h_1, \dots, h_n\}$ be a set of homogeneous elements of F and let $R = \text{Alg}(H)$. Then some subset of H freely generates R .*

Proof. The theorem is obvious if $n = 1$. Suppose then, for an induction, that we have proved the theorem for sets of at most $n - 1$ elements.

Let $L = \{h_1, \dots, h_{n-1}\}$. If L is not free then, by the induction hypothesis some proper subset $L' \subset L$ generates $\text{Alg}(L)$. But then, $R = \text{Alg}(L', h_n)$ is generated by at most $n - 1$ elements and we may again use the induction hypothesis to prove the theorem. Thus we may assume that R has rank at least $n - 1$. However, if R has rank n , then, by Proposition 1, H is a free set and there is nothing to prove. Thus we may assume that R has rank $n - 1$.

Our first task is to show that R has a set of homogeneous free generators. To this effect, let $Y = \{y_1, \dots, y_{n-1}\}$ be a set of free generators of R with homogeneous terms of highest degree z_1, \dots, z_{n-1} such that the degree of Y is minimal. If $Z = \{z_1, \dots, z_{n-1}\}$ is free then Z generates R by Lemma 1 and we are done. Otherwise $\text{Alg}(Z)$ has rank at most $n-2$ and, again by the induction hypothesis, some proper subset Z' of Z freely generates $\text{Alg}(Z)$. Reordering the y_i 's if necessary we find that $z_1 = w(z_2, \dots, z_{n-1})$. Thus the set Y' defined by

$$y'_1 = y_1 - w(y_n, \dots, y_{n-1}), \quad y'_2 = y_2, \dots, y'_{n-1} = y_{n-1}$$

is still a set of generators for R , and has degree smaller than the degree of Y . This contradiction shows that Z is indeed a free set of generators for R .

Let now $H_k = \{h_i \mid d(h_i) = k\}$ and $Z_k = \{z_i \mid d(z_i) = k\}$. By Lemma 3, both H_1 and Z_1 span R_1 mod R_0 . Since Z_1 is free, Z_1 is a basis for R_1 modulo R_0 . Extract a basis H'_1 for R_1 mod R_0 out of H_1 . Then Z_1 and H'_1 generate the same subalgebra and, since they have the same finite cardinal, H'_1 is free by Proposition 1. It then follows that $\{H'_1 \cup \bigcup_{i \geq 2} Z_i\}$ again freely generates R .

Assume then, for an induction that, for $i \leq k$, we have extracted bases H'_i for R_i mod R'_i out of H_i in such a way that $\{\bigcup_{i=1}^k H'_i \cup \bigcup_{i \geq k+1} Y_i\}$ freely generates R . By Lemma 3, Z_{k+1} and H_{k+1} both span R_{k+1} mod R'_{k+1} . Z_{k+1} is actually a basis for R_{k+1} mod R'_{k+1} since, again by Lemma 3, $R'_{k+1} \subset \text{Alg}(R_k) = \text{Alg}(Z_1 \cup \dots \cup Z_k)$ and Z is free. Let $H'_{k+1} \subset H_{k+1}$ be a basis for R_{k+1} mod R'_{k+1} . Thus, if $z \in Z_{k+1}$, then

$$z = \sum \beta_j h_j + u, \quad \beta_j \in \phi, h_j \in H'_{k+1}, u \in R'_{k+1}$$

and, noting that by Lemma 3 $R'_{k+1} \subset \text{Alg}(\bigcup_{i=1}^k H'_i)$, we find that $Z_{k+1} \subset \text{Alg}(\bigcup_{i=1}^{k+1} H'_i)$. It then follows that the set $\{\bigcup_{i=1}^{k+1} H'_i \cup \bigcup_{i \geq k+2} Z_i\}$ generates R . However it must freely generate R since it has the same cardinal as Z .

Since this replacement process eventually replaces Z by a subset of H , the theorem is proved.

2. We now prove our main theorem

THEOREM 2. *Let \mathfrak{v} be a variety in which finitely generated homogeneous subalgebras of free \mathfrak{v} -algebras are again free \mathfrak{v} -algebras. Let $Y = \{y_1, \dots, y_n\}$ be elements of F . Then there is a sequence of degree reducing elementary transformations of order n such that the elements of positive degree in $(\dots(Y\tau_1)\dots)\tau_k$ are a free generating set for $\text{Alg}(Y)$.*

In particular a Schreier variety is a Nielsen variety.

Proof. Clearly we need only show that if Y contains elements of positive degree and these elements are not a free set, then we can reduce the degree of Y by an elementary transformation. We assume, for convenience, that Y consists of elements of positive degree, and we write $y_i = \bar{y}_i + h_i$ with $d(h_i) = d(y_i)$, $\bar{y}_i = 0$ or $d(\bar{y}_i) < d(h_i)$ and h_i homogeneous. Let $H = \{h_1, \dots, h_n\}$. We first show that if H is

free, then so is Y . For let $0 \neq w(x_1, \dots, x_n)$ be an element of minimal length for which $w(y_1, \dots, y_n) = 0$. As in Lemma 2, we write

$$w(x_1, \dots, x_n) = \sum_{i \in S_1} \alpha_i m_i(x_1, \dots, x_n) + \sum_{i \in S_2} \alpha_i m_i(x_1, \dots, x_n); \quad \alpha_i \in \phi, m_i \in B$$

where $m_i(h_1, \dots, h_n) \neq 0$, $i \in S_1$ if $d(m_i(h_1, \dots, h_n)) = \max_i (d(m_i(h_1, \dots, h_n)))$ and $i \in S_2$ otherwise. Thus, since $w(y_1, \dots, y_n) = 0$, we must have $\sum_{i \in S_1} \alpha_i m_i(h_1, \dots, h_n) = 0$ and, since H is free, $\sum_{i \in S_1} \alpha_i m_i(x_1, \dots, x_n) = 0$. Thus, if $S_2 = \emptyset$, then $w(x_1, \dots, x_n) = 0$ and if $S_2 \neq \emptyset$, then

$$0 = w'(y_1, \dots, y_n) = \sum_{i \in S_1} \alpha_i m_i(y_1, \dots, y_n).$$

However, w' is then shorter than w so we have a contradiction in both cases. Thus, if H is free there is nothing to prove.

If H is not free, then, by Theorem 1, some proper subset $K \subset H$ freely generates $\text{Alg}(H)$. Thus, reordering the y_i 's if necessary, we find that $h_1 = w(h_2, \dots, h_n)$ for some $w(x_2, \dots, x_n) \in F$. Define τ by setting $(x_1, \dots, x_n)\tau = (x_1, \dots, x_{n-1}, x_n - w(x_2, \dots, x_n))$. Then $Y\tau$ still generates $\text{Alg}(Y)$, and has smaller degree than Y . This proves Theorem 2.

IV. Nielsen varieties are Schreier varieties. It now follows easily from Theorem 2 that if finitely generated homogeneous subalgebras of free \mathfrak{v} -algebras are free, then all subalgebras of free \mathfrak{v} -algebras are free:

THEOREM 3. *If \mathfrak{v} satisfies the hypotheses of Theorem 2, then \mathfrak{v} is a Schreier variety. Thus a Nielsen variety is a Schreier variety.*

Proof. Let F be a free algebra in \mathfrak{v} , and let R be a subalgebra of F . Let Y_k , for $k \geq 1$, be a basis for $R_k \bmod R'_k$. It is clear that $Y = \bigcup_{i=1}^{\infty} Y_i$ generates R . We show that Y freely generates R . For suppose not. Then there is a finite subset $\bar{Y} = \{y_1, \dots, y_k\}$ of Y which is not free. Since \mathfrak{v} satisfies the hypotheses of Theorem 2, we find, as in the proof of that theorem, that we may reorder \bar{Y} if necessary in such a way that there is an element $w(y_{i_1}, \dots, y_{i_k})$ of F such that

$$(2) \quad d(y_1 - w(y_{i_1}, \dots, y_{i_k})) < d(y_1)$$

with $d(y_{i_j}) \leq d(y_1)$ and $i_j \neq 1$. Thus the terms of degree $d(y_1)$ in the left hand side of (2) must vanish. It is now easy to see that (2) contradicts the fact that the y_i 's of degree $d(y_1)$ are ϕ -independent modulo $R_{d(y_1)}$.

V. Applications.

1. Following the proofs in [6, Theorem 3.2] and [2, Theorem 6.3] it is now an easy matter to obtain

THEOREM 4. *Let $F = F(x_1, \dots, x_n)$ be the free algebra of rank n in a Schreier variety. The group of automorphisms of F is generated by the permutations of x_1, \dots, x_n together with the automorphisms*

$$\alpha_\varphi: x_1 \rightarrow \varphi x_1; \quad x_i \rightarrow x_i, \quad (i \neq 1) \quad (\varphi \in \phi, \varphi \neq 0),$$

$$\tau_w: x_1 \rightarrow x_1 + w(x_2, \dots, x_n), \quad x_i \rightarrow x_i, \quad (i \neq 1).$$

Likewise, following the proof in [6, Theorem 3.3, p. 132] we obtain

THEOREM 5. *Let F be as above, and suppose N is an ideal of F such that F/N is again a free ϕ -algebra. Then there exists a set of generators y_1, \dots, y_n of F such that N is the ideal generated by y_1, \dots, y_k ($k \leq n$).*

2. We now turn our attention to word problems. Specifically, let $F = F(\{x_1, \dots, x_n\})$ be the (absolutely) free algebra freely generated by x_1, \dots, x_n , let N be an ideal of F , and let $A = F/N$. We say that we can solve the word problem in A if, given an element $w \in F$ there is an integer $f(w)$ which depends only on the degree of w such that we can decide in at most $f(w)$ steps whether $w \in N$ or $w \notin N$. It is clear that the word problem is only meaningful if the field ϕ is given in an effective manner, and we will assume this in the remainder of this paper. We shall use the fact that in this case it follows from elementary linear algebra that if E is a $k_1 \times k_2$ system of linear equations over ϕ , then there is an integer $e(k_1, k_2)$ such that, in at most $e(k_1, k_2)$ steps, we can find a solution to E or decide that E has no solution.

Many of the details in the following proofs are easy but cumbersome and will be omitted.

LEMMA 3. *Suppose that N has a set G of homogeneous ideal generators such that, for any k , $G_k = \{g \in G \mid d(g)=k\}$ is finite and can be effectively enumerated. Then we can solve the word problem in A .*

Proof. Define inductively

$$G^0 = G,$$

$$G^i = \{l(gr) \mid l, r \text{ monomials, } g \in G^{i-1}\} \cup \{(lg)r \mid l, r \text{ monomials, } g \in G^{i-1}\}$$

and let $\bar{G} = \bigcup_{i=0}^{\infty} G^i$. Then $\langle \bar{G} \rangle = N$. Further, since F is finitely generated, F has only finitely many monomials of a given degree and hence $\bar{G}_k = \{\bar{g} \in \bar{G} \mid d(\bar{g})=k\}$ is still finite and can be effectively enumerated. In fact we can enumerate \bar{G}_k in $r(k)$ steps, where r is an integer which only depends on ϕ , G , n and k .

Let $w \in F$. Then $w \in N$ if and only if the homogeneous terms of w all lie in N and we may thus assume that w is homogeneous, say of degree k . If $w \in N$, then

$$w = \sum \beta_i \bar{g}_i, \quad \beta_i \in \phi, \bar{g}_i \in \bar{G},$$

and, since each \bar{g}_i is homogeneous, we may assume that

$$(3) \quad w = \sum \beta_i \bar{g}_i, \quad \beta_i \in \phi; \bar{g}_i \in \bar{G}_k.$$

We now write $w = \sum \alpha_s m_s$ and $\bar{g}_i = \sum \alpha_{i,s} m_s$, where m_s ranges over the monomials of degree k . (3) now gives rise to a finite system E of linear equations and $w \in N$ if and only if E has a solution. Thus the proof is complete. We note that if $w \in N$ this method gives an expression for w in terms of the generators G of N .

LEMMA 4. *If N is as in Lemma 3 and $N \neq F$, then we can find a set $B = \{b_0 = 1, b_1, \dots\}$ of monomials of F with the properties:*

- (i) $\{b_i + N\}, i = 0, 1, \dots$, is a ϕ -basis for A .
 - (ii) If $w \in F$ is of degree k , then there is an integer $s(k)$ which depends only on k , G , n and ϕ such that we can find in at most $s(k)$ steps the unique expression
- $$(4) \quad w = \alpha_1 b_{i_1} + \alpha_2 b_{i_2} + \dots + \alpha_r b_{i_r} + t, \quad \alpha_i \in \phi, b_{i_j} \in B, t \in N.$$

Proof. We order the monomials of F lexicographically and declare 1 to be smaller than any other monomial. We define B inductively by setting $B^0 = \{1\}$ and defining $B^t = B^{t-1} \cup \{b_t\}$ if b_t is the least monomial in the order such that $B^t \cup \{b_t\}$ is still linearly independent modulo N or defining $B^t = B^{t-1}$ if there is no such monomial. We then set $B = \bigcup_{i=0}^{\infty} B^i$. It is clear that B has property (i). We now show by induction that we can effectively enumerate B . For suppose we can effectively enumerate B^k , and suppose that the greatest monomial in B^k has degree p . Let $B_p^k = \{b \in B \mid d(b) = p\}$. Let m be a monomial of degree p greater than any monomial in B^k . To test whether $\{m\} \cup B^k$ is still independent, we adjoin B_p^k to G and consider $N' = \text{Id}(G \cup B_p^k)$. By Lemma 3 we can decide if $m \in N'$. If $m \notin N'$, then we can set $B^{k+1} = B^k \cup \{m\}$. If $m \in N'$ then, by Lemma 3, we can effectively express m in terms of $G \cup B_p^k$ and, since $d(m) = p$, this expression is of the form (4). If no monomial of degree p can be adjoined to B^k to define B^{k+1} , and some monomial of degree between p and $2p$ is not in N , then we choose m to be the least such monomial and define $B^{k+1} = B^k \cup \{m\}$. This, again by Lemma 3, can be done effectively. Finally, if all the monomials of degree between p and $2p$ are in N , then every monomial of degree $> p$ is in N and we set $B^{k+1} = B^k$.

It is now clear from the foregoing that property (ii) is satisfied whenever w is a monomial. Since any element of F is a linear combination of finitely many monomials, (ii) is satisfied for any element of F and the proof is complete.

We remind the reader that a variety v is defined via a subset V of the free algebra $F(X)$ of countably infinite rank. If, whenever $v(x_1, \dots, x_r) \in V$ and $w_1, \dots, w_i, w'_i, \dots, w_r \in F(X)$, then

$$v(w_1, \dots, w_i + w'_i, \dots, w_r) = v(w_1, \dots, w_i, \dots, w_r) + v(w_1, \dots, w'_i, \dots, w_r),$$

we say that v is defined by multilinear laws. We note that if ϕ has characteristic $p \neq 2$, then the varieties of Lie algebras, commutative algebras, anticommutative algebras can be defined by multilinear laws.

THEOREM 6. *Let v be a variety defined by finitely many multilinear laws. Then we can solve the word problem in $F(v, \{x_1, \dots, x_n\})$.*

Proof. We first note that, by Proposition 2, we may assume that V consists of finitely many homogeneous multilinear elements. It now follows from the multilinearity that $v(F(x_1, \dots, x_n))$ is generated, qua ideal, by

$$G = \{v(m_1, \dots, m_k) \mid v \in V, m_1, \dots, m_k \text{ monomials}\}.$$

We can then apply Lemma 3 to complete the proof.

3. We apply our last results to Schreier varieties. If \mathfrak{v} is a variety defined by finitely many multilinear laws, then, in view of Theorem 6 and Lemma 4, there exists a monomial basis B for $F = F(\mathfrak{v}, \{x_1, \dots, x_n\})$ such that an expression in the generators of F can be effectively written as a linear combination of the elements of B .

THEOREM 7. *Let \mathfrak{v} be a Schreier variety defined by finitely many multilinear laws. Then the generalized word problem is solvable in $F = F(\mathfrak{v}, \{x_1, \dots, x_n\})$, i.e., given elements z_1, \dots, z_r, z in F , one can decide effectively whether $z \in \text{Alg}(z_1, \dots, z_r)$.*

Proof. We first show that if y_1, \dots, y_r are elements of F with highest homogeneous terms h_1, \dots, h_r , then we can effectively find a set y'_1, \dots, y'_s of elements of F , with homogeneous terms h'_1, \dots, h'_s such that y'_1, \dots, y'_s , freely generate $\text{Alg}(y_1, \dots, y_r)$ and $\{h'_1, \dots, h'_s\}$ is free. For, by Theorem 1, $\{h_1, \dots, h_r\}$ is not free only if, after a suitable reordering of h_1, \dots, h_r , $h_1 \in \text{Alg}(h_2, \dots, h_r)$. If $h_1 \in \text{Alg}(h_2, \dots, h_r)$ then, since h_2, \dots, h_r are homogeneous, h_1 is a linear combination of the products $h_{i_1}h_{i_2}\cdots h_{i_k}$ which have degree $d(h_1)$. By the above remark, we can effectively write each of these products as a linear combination of elements of B , and thus, in order to decide if $h_1 \in \text{Alg}(h_2, \dots, h_r)$, we are led to consider a system of linear equations over ϕ . If there are no solutions, then $h_1 \notin \text{Alg}(h_2, \dots, h_r)$. On the other hand a solution defines an elementary transformation which reduces the degree of $Y = \{y_1, \dots, y_r\}$. Thus, to prove our claim we need only apply the above procedure to every reordering of h_1, \dots, h_r and use induction on the degree of Y .

We may then assume that the highest homogeneous terms h_1, \dots, h_r of z_1, \dots, z_r form a free set. We prove the theorem by induction on the degree of z . If $d(z)=0$, then $z \in \text{Alg}(z_1, \dots, z_r)$ and there is nothing to prove. Suppose then that $d(z)=k$, and that $d(h_1) \leq d(h_2) \leq \dots \leq d(h_s) \leq k$ and $d(h_{s+1}) > k$. Let h be the highest homogeneous term of z . Then, using now familiar arguments, we see that if $\{h_1, \dots, h_s, h\}$ is a free set then $z \notin \text{Alg}(z_1, \dots, z_r)$. Thus, proceeding as in the first part of the proof, we find that $z \notin \text{Alg}(z_1, \dots, z_n)$ or we find an element $w(z_1, \dots, z_s)$ such that $d(z-w(z_1, \dots, z_s)) < k$. However, since $z-w(z_1, \dots, z_s) \in \text{Alg}(z_1, \dots, z_r)$ if and only if $z \in \text{Alg}(z_1, \dots, z_r)$, the proof is complete by induction.

REFERENCES

1. R. H. Bruck, *A survey of binary systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete, N. F., Heft 20, Springer-Verlag, Berlin, 1958.
2. P. M. Cohn, *Subalgebras of free associative algebras*, Proc. London Math. Soc. **56** (1964), 618–632.
3. ———, *Universal algebra*, Harper and Row, New York, 1965.
4. N. Jacobson, *Structure of rings*, rev. ed., Amer. Math. Soc. Colloq. Publ., Vol. 37, Amer. Math. Soc., Providence, R. I., 1964.
5. A. G. Kuroš, *Nonassociative free algebras and free products of algebras*, Mat. Sb. **20** (62) (1947), 239–262. (Russian)

6. W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory*, Interscience, New York, 1966.
7. J. Nielsen, *Die Isomorphismengruppe der freien Gruppen*, Math. Ann. **91** (1924), 169–209.
8. O. Schreier, *Die Untergruppen der freien Gruppen*, Abh. Math. Sem. Univ. Hamburg **5** (1927), 161–183.
9. A. I. Širšov, *On subalgebras of free Lie Algebras*, Mat. Sb. **33** (75) (1953), 441–453. (Russian)
10. ———, *On subalgebras of free commutative and anticommutative algebras*, Mat. Sb. **34** (76) (1954), 81–88. (Russian)
11. E. Witt, *Über freie Ringe und ihre Unterringe*, Math. Z. **58** (1953), 113–114.
12. ———, *Die Unterringe der freien Lieschen Ringe*, **64** (1956), 195–216.

SYRACUSE UNIVERSITY,
SYRACUSE, NEW YORK