COMPOSITA, EQUATIONS, AND FREELY GENERATED ALGEBRAS[1]

BY

A. NERODE

1. **Introduction and examples.** This paper is intended as an exposition of the theory and applications of a new class of algebraic structures, composita. Composita arise naturally both in the context of algebra and in the context of logic. In algebra, they arise from an attempt to establish on a firm foundation the theory of an abstract algebra free on a generating set. In logic, they arise as algebraic counterparts to the calculus of identities (equations) of Birkhoff [2]. One application of composita is to freely generated algebras; this brings unity and simplicity to proofs. A byproduct (Corollary 4.10) appears to be a solution to Problem 68 of Birkhoff [4, p. 146].

A *V-compositum* T consists of a set T containing at least two elements, a nonempty subset V of T, and a set S of maps on T to T such that:

(1.1) S contains the identity map and is closed under composition,

(1.2) every map on V to T has a unique extension in S.

One example is a vector space T with basis V, and with the set of all linear transformations on T in the role of S. Further examples of this sort are obtained from a free group T (or a free group modulo a proper fully invariant subgroup, or a free ring, or a free ring modulo a proper T-ideal in the sense of Amitsur [1], or a free boolean algebra, or a free distributive lattice) with free generating set V, and with the set of all endomorphisms in the role of S. For still another example, let T be a semigroup with unit e, let V consist of e alone, and let S consist of all left multiplications of T. All of these examples are special cases of the following one.

Let T be an algebra (throughout this paper we assume the definitions concerning algebras of Birkhoff [4, pp. VII–IX], except that we require in the definition of algebra that it contain at least two elements), let V be a generating set for T, and let S be the set of all endomorphisms of T. We shall say that the structure consisting of the algebra T together with the generating set V is *free* (or, briefly, T is *free* on V) if every map on V to T has an extension in S. Then T is a V-compositum. This was suggested as a possible definition of the concept of freely generated algebra in Birkhoff [3]. Warning: if a group T is free on V, T is not necessarily a free group; T may be a free group modulo a fully invariant subgroup.

An illuminating special case which we shall utilize in connection with identities arises as follows. Let V, F be disjoint nonempty sets. Suppose that

Presented to the Society August 30, 1957; received by the editors June 17, 1957.

(1) Revised version of part of a Ph.D. dissertation submitted to The University of Chicago.

to each element f of F there corresponds a positive integer n, called the *degree* of f. Let T be the smallest class of finite sequences of elements of $V \cup F$ which contains all 1-term sequences whose only member is in V and which is such that: whenever $f \in F$ is of degree n and $t_1, \cdots, t_n \in T$, then $ft_1 \cdots t_n \in T$. Let S consist of all maps $s: T \to T$ such that for any $f \in F$ of degree n and any $t_1, \cdots, t_n \in T$, $s(ft_1 \cdots t_n) = f(st_1) \cdots (st_n)$. There are words from logic to describe this compositum: V consists of *individual variables*, T of *terms*, and S of *substitutions*. Finally, F consists of *function symbols*.

Let R consist of at least two elements, let T denote the set of all functions on $R \times R$ to R, and let V consist of the two projections $v_1, v_2 \in T$ given by $v_1(r_1, r_2) = r_1$, $v_2(r_1, r_2) = r_2$ for $r_1, r_2 \in R$. Let S consist of all $s: T \to T$ such that for $t \in T$, $r_1, r_2 \in R$, $(st)(r_1, r_2) = t((sv_1)(r_1, r_2), (sv_2)(r_1, r_2))$. It is not hard to see that T is a V-compositum. Our last example generalizes this one.

Let R, V be nonempty sets. Denote by X the set of all functions on V to R, by R^X the set of all functions on X to R. Let $-: V \to R^X$ be defined by $\bar{v}(x) = x(v)$ for $x \in X$, $v \in V$. Every map $s: R^X \to R^X$ induces a map $s^\sharp: X \to X$ given by $(s^\sharp x)(v) = (s\bar{v})(x)$ for $x \in X$, $v \in V$. Let S consist of all maps $s: R^X \to R^X$ such that

$$(1.3) \qquad (st)(x) = t(s^\sharp x) \text{ for all } x \in X,\ t \in R^X.$$

Suppose that R contains at least two elements. Then a tedious but easy argument shows that R^X is a $\overline{V}$-compositum. Composita so arising from a pair of sets V, R we call *concrete* composita.

2. **Representations of composita.** Suppose that T is a V-compositum with set S of maps and that T' is a V'-compositum with set S' of maps. Any $H: T \to T'$ which maps V 1-1 onto V' induces a map $\tilde{H}: S \to S'$ defined by the requirement that $(\tilde{H}s)(Hv) = H(sv)$ for $s \in S$, $v \in V$. $\tilde{H}$ is well-defined due to (1.2).

A map $H: T \to T'$ is a *compositum homomorphism* if

(2.1) H extends a 1-1 map from V onto V',

(2.2) for $s \in S$, $t \in T$, $H(st) = (\tilde{H}s)(Ht)$.

Moreover, H is an *epimorphism*, *monomorphism*, or *isomorphism* as H is onto, 1-1, or 1-1 onto. If $V = V'$, $T = T'$, $S = S'$, then H is an *endomorphism*.

(2.3) If H is a homomorphism and $s_1, s_2 \in S$, then $(\tilde{H}s_1)(\tilde{H}s_2) = \tilde{H}(s_1 s_2)$.

(2.4) Suppose that $H: T \to T'$ is a homomorphism. Let t be an element of T and W a nonempty subset of V such that if $s_1, s_2 \in S$ agree on W, then $s_1 t = s_2 t$. It follows that if $s_1', s_2' \in S'$ agree on $H(W)$, then $s_1'(Ht) = s_2'(Ht)$.

To prove (2.4), select an $s \in S$ such that s coincides with the identity map $u: T \to T$ on W and such that $s(V) = W$. Since s and u coincide on W, $st = t$; so by (2.2), $(\tilde{H}s)(Ht) = Ht$. Then (1.2) implies that it suffices to prove the equality of $s_1'(\tilde{H}s)(Hv)$, $s_2'(\tilde{H}s)(Hv)$ for $v \in V$. But s_1', s_2' agree on $H(W) = H(s(V))$, so $s_1' H(sv) = s_2' H(sv)$.

A subset T' of a V-compositum T is a *subcompositum* of T provided that:

V is a subset of T'; $st \in T'$ whenever $s \in S$, $t \in T'$, $s(V) \subset T'$. A subset G of a V-compositum T is a *generating set* if the only subcompositum of T containing G is T itself.

By generalizing the construction of the composita of terms described in §1, one obtains what deserve to be called free composita.

THEOREM 2.1. *Let V, G be nonempty sets. Then there exists a V-compositum T, unique up to isomorphisms preserving G, such that: G generates T; if T' is a V-compositum with generating set G' and $e: G \to G'$ is onto, then there exists a unique epimorphism $E: T \to T'$ extending e.*

Let T be a V-compositum. Then a *congruence relation* on T is an equivalence relation C on T such that: C does not identify distinct elements of V; if $s_1, s_2 \in S$, $t_1, t_2 \in T$, $(s_1 v, s_2 v) \in C$ for $v \in V$, $(t_1, t_2) \in C$, then $(s_1 t_1, s_2 t_2) \in C$. Moreover, C is *proper* if C is distinct from $T \times T$. The *kernel* C of a map $H: T \to T'$ is the equivalence relation C on T such that $(t_1, t_2) \in C$ if and only if $Ht_1 = Ht_2$. Then the following two theorems can be obtained using (2.3).

THEOREM 2.2. *Suppose $E_2: T \to T_2$ is an epimorphism. Let $H_3: T \to T_3$ be a homomorphism such that the kernel of H_3 contains the kernel of E_2. Then there exists a unique homomorphism $H_1: T_2 \to T_3$ such that $H_1 E_2 = H_3$.*

THEOREM 2.3. *The kernel of a compositum homomorphism is a congruence relation. Conversely, suppose that C is a proper congruence relation on T. Then there exists a V'-compositum T' and an epimorphism $E: T \to T'$ with kernel C. Moreover, T' is determined up to isomorphism by T and C. We denote T' as T/C.*

A subset T' of a V-compositum T is *full* if T' contains at least two elements and whenever $s \in S$, $s(V) \subset T'$, then $s(T) \subset T'$. To obtain examples, let W be a subset of V, and let T_W consist of all t in T such that for any s_1, s_2 in S which agree on W, $s_1 t = s_2 t$. If T_W contains at least two elements, then T_W is full. In case W is null, elements of T_W are called *constants*.

If $k: V \to T$, denote by $k^*: T \to T$ the extension of k in S.

LEMMA 2.4. *Let R be a full subset of a V-compositum T, and let $j: R \to T$ be the inclusion map. Let $X = R^V$, and define $H: T \to R^X$ by*

$$(Ht)(x) = (jx)^* t, \qquad t \in T, x \in X. \tag{2.5}$$

Then H is a homomorphism on the V-compositum T to the concrete $\overline{V}$-compositum R^X.

Proof. To verify (2.1), note that for $x \in X$, $v \in V$, $(Hv)x = x(v)$. As for (2.2), note first that

$$(j(\tilde{H}s)^\sharp x)^* = (jx)^* s, \qquad s \in S, x \in X, \tag{2.6}$$

since consecutive applications of the definitions of $\sharp$, $\bar{v}$, $\tilde{H}$, and H yield

$$((\tilde{H}s)\#x)v = ((\tilde{H}s)\bar{v})(x) = ((\tilde{H}s)(Hv))(x)$$
$$= (H(sv))(x) = (jx)^*(sv) = ((jx)^*s)(v).$$

Consequently, applying (1.3), (2.5), (2.6), and finally (2.5) again,

$$((\tilde{H}s)(Ht))(x) = (Ht)((\tilde{H}s)\#x) = (j(\tilde{H}s)\#x)^*t$$
$$= ((jx)^*s)(t) = (jx)^*(st) = (H(st))(x).$$

THEOREM 2.5 (*The regular representation*). *Suppose that T is a V-compositum. Let $X = T^V$. Then the map $M: T \to T^X$ given by*

$$(Mt)(x) = x^*t, \qquad x \in X, t \in T, \tag{2.7}$$

is a monomorphism on the V-compositum T to the concrete $\overline{V}$-compositum T^X.

Proof. Lemma 2.4 applied to the full subset T of T shows that M is a homomorphism. To see that M is 1-1, suppose $Mt_1 = Mt_2$. If $u: V \to T$ is the inclusion map, $u^*: T \to T$ is the identity, and

$$t_1 = u^*t_1 = (Mt_1)(u) = (Mt_2)(u) = u^*t_2 = t_2.$$

THEOREM 2.6. *A V-compositum T is isomorphic to a concrete compositum if and only if T contains at least two constants and* (i) *below holds.* (i) *Let I be the set of constants of T, let $j: I \to T$ be the inclusion map, and let $X = I^V$. Then the map $H: T \to I^X$ given by*

$$(Ht)(x) = (jx)^*t, \qquad x \in X, t \in T,$$

is an isomorphism.

Proof. If H is an isomorphism, then T is isomorphic to the concrete compositum I^X. In proving the converse, it suffices to consider concrete composita; for if the H associated by (i) with a given compositum T is an isomorphism, so is the H associated with any compositum isomorphic to T. Suppose that T is a concrete $\overline{V}$-compositum, $T = R^Y$, $Y = R^V$. Define $q: R \to R^Y$ by $(qr)(y) = r$ for all y in Y; then $I = q(R)$. In the obvious way the 1-1 maps $-: V \to R^Y$, $q: R \to R^Y$ induce a 1-1 onto map on $Y = R^V$ to $X = I^{\overline{V}}$, and hence induce a 1-1 onto map $H': R^Y \to I^X$. It is easy to see that $H = H'$, so H is 1-1 onto. Lemma 2.4 applied to the full set of constants implies that H is a homomorphism.

Let T be a V-compositum, let n be the ordinal number of a well-ordering of V. Let T^n denote the set of well-ordered transfinite sequences $(t_1, t_2, \cdots)$ of elements of T of length n. Using the well-ordering of V, we may identify functions on T^n to T with elements of T^X, where $X = T^V$. The definition of an algebra T which we have adopted from Birkhoff [4, p. VII] allows only functions on T^n to T with n finite. For the next theorem only, we allow n to be infinite so as to be able to consider a structure consisting of the set T together with certain functions in T^X as defining an algebra T.

THEOREM 2.7. *Let T be a V-compositum. Suppose that $M: T \to T^X$ is the regular representation, where $X = T^V$. Construe the structure consisting of the set T together with the set of functions $M(T)$ as an algebra. Then T is free on V, and S is the set of all endomorphisms of T.*

Proof. Suppose that T' is a subset of T containing V and closed under all members of $M(T)$. Let $u: V \to T$ be the inclusion map, so that $u^*: T \to T$ is the identity. Then if $t \in T$, $t = u^*t = (Mt)(u) \in T'$, hence $T = T'$. Thus V generates T.

Suppose that $e: T \to T$ is an endomorphism. Applying successively (2.7), the fact that e is an endomorphism, and (2.7) again, we see that for $t \in T$,

$$et = e(u^*t) = e((Mt)(u)) = (Mt)(eu) = (eu)^*t,$$

so $e = (eu)^*$. Consequently every endomorphism is in S. Conversely, suppose $s \in S$; then for $x \in X$, $sx^* = (sx)^*$. Thus for $t \in T$,

$$s((Mt)(x)) = s(x^*t) = (sx^*)t = (sx)^*t = (Mt)(sx),$$

or s is an endomorphism.

COROLLARY 2.8. *Let C be a proper congruence relation on a V-compositum T. Then there exists a homomorphism on T to a concrete compositum with kernel C.*

Proof. Let $E: T \to T/C$ be the epimorphism given by Theorem 2.3. Let $M: T/C \to R^X$ be the regular representation of theorem 2.5. Then $ME: T \to R^X$ is satisfactory.

This corollary is a generalization to composita of the semantic completeness of the calculus of identities of Birkhoff [2, §10]. We now turn to this subject.

3. **The calculus of identities.** From now on, let V be the fixed countably infinite set consisting of $v_1, v_2, \cdots$. Furthermore, let F be a fixed set of function symbols, and denote by T the set of terms built out of V and F (see §1). In logical language, an ordered pair (t_1, t_2) from $T \times T$ is called an *identity* and written $(t_1 = t_2)$. A set of identities is called *deductively closed* if the set is a congruence relation for the compositum T. With every set A of identities is correlated its *deductive closure* C, the congruence relation generated by A. Furthermore, A is *nontrivial* if C is proper.

It is not hard to see that a set C of identities is deductively closed if and only if C satisfies (i), (ii), (iii) below.

(i) $(t = t) \in C$ for $t \in T$; $(t_1 = t_2) \in C$ implies $(t_2 = t_1) \in C$; $(t_1 = t_2)$, $(t_2 = t_3) \in C$ implies $(t_1 = t_3) \in C$.

(ii) If $(t_1 = t_2) \in C$ and $s: T \to T$ is a substitution, then $(st_1 = st_2) \in C$.

(iii) If $f \in F$ is of degree n and $(t_1 = t_1'), \cdots, (t_n = t_n') \in C$, then

$$(ft_1 \cdots t_n = ft_1' \cdots t_n') \in C.$$

An *F-algebra* consists of a set R containing at least two elements together

with a function d with domain F assigning to each $f\in F$ of degree n a function $df\colon R^n\to R$.

THEOREM 3.1. *Every F-algebra R induces a compositum homomorphism $D\colon T\to R^X$ $(X=R^V)$ such that: $Dv=\bar{v}$ for $v\in V$; if $f\in F$ is of degree n and $t_1, \cdots, t_n\in T$, then for $x\in X$,*

$$(Dft_1 \cdots t_n)(x) = df((Dt_1)(x), \cdots, (Dt_n)(x)).$$

Conversely, every compositum homomorphism $D\colon T\to R^X$ such that $Dv=\bar{v}$ for $v\in V$ is so induced by precisely one F-algebra.

Proof. We prove the first assertion by verifying (2.2) for fixed s by a recursion on the definition of T. Note that for $v\in V$, $(\tilde{D}s)(\bar{v})=D(sv)$, so the conclusion holds for v in V; also note that whenever $f\in F$ is of degree n and the conclusion holds for $t_1, \cdots, t_n$ (that is, $(\tilde{D}s)(Dt_i)=D(st_i)$, $i=1, \cdots, n$) we may conclude that for all $x\in X$,

$$((\tilde{D}s)(Dft_1 \cdots t_n))(x) = (Df(st_1) \cdots (st_n))(x).$$

In fact, to obtain the right term from the left, apply (1.3), the definition of D, (1.3) again, the assumption $D(st_i)=(\tilde{D}s)(Dt_i)$, and finally the definition of D again. Consequently, D is a homomorphism.

As for the second assertion, for $f\in F$ of degree n we must define $df(r_1, \cdots, r_n)$ for $r_1, \cdots, r_n\in R$. Choose any $s\colon R^X\to R^X$ in S such that $s\bar{v}_i\colon X\to R$ has constant value r_i, $i=1, \cdots, n$. Then put $df(r_1, \cdots, r_n)$ equal to $(sDfv_1 \cdots v_n)(x)$ for any $x\in X$. By (2.4) this is independent of the choice of s, and is trivially independent of x. It is easy to verify that $df(r_1, \cdots, r_n)=(Dfv_1 \cdots v_n)(x)$ for any $x\in X$ such that $x(v_i)=r_i$, $i=1, \cdots, n$. This implies that the homomorphism induced by the F-algebra coincides with D on V and on terms of the form $fv_1 \cdots v_n$. Since such terms generate the compositum T, the F-algebra induces D. We omit the proof of uniqueness.

Combining Theorem 2.2 with Theorem 3.1 one obtains

COROLLARY 3.2. *Suppose that R_2 and R_3 are F-algebras inducing homomorphisms D_2, D_3. Then $D_2(T)$, $D_3(T)$ are $\overline{V}$-composita. Further,*

(i) *an epimorphism $E\colon R_2\to R_3$ induces an epimorphism on $D_2(T)$ to $D_3(T)$ given by $D_2t\to D_3t$ for $t\in T$,*

(ii) *a monomorphism $M\colon R_2\to R_3$ induces an epimorphism on $D_3(T)$ to $D_2(T)$ given by $D_3t\to D_2t$ for $t\in T$.*

We call an identity $(t_1=t_2)$ *true* in an F-algebra R if $Dt_1=Dt_2$ for the compositum homomorphism D induced by R. To see that this definition has the proper effect, suppose that F contains a function symbol f of degree 2. Consider the commutative law $(fv_1v_2=fv_2v_1)$. According to the definition just given, this identity is true in an F-algebra R if and only if

$$df(x(v_1), x(v_2)) = df(x(v_2), x(v_1))$$

for all x: $V \to R$; that is, if and only if for all $r_1, r_2 \in R$, $df(r_1, r_2) = df(r_2, r_1)$.

Combining Theorem 3.1 with Corollary 2.8 we obtain

COROLLARY 3.3. *Let A be a nontrivial deductively closed set of identities. Then $(t_1 = t_2) \in A$ if and only if $(t_1 = t_2)$ is true in all F-algebras in which each member of A is true.*

4. Identities and freely generated algebras.

THEOREM 4.1. *Suppose that R is an F-algebra with generating set G. Then each of the following conditions is necessary and sufficient that R be free on G.*

(4.1) *If an identity $(t_1 = t_2)$ is satisfied by some assignment of distinct elements of G to distinct variables occurring in $(t_1 = t_2)$, then $(t_1 = t_2)$ is true in R.*

(4.2) *Suppose that R' is an F-algebra with the following property: if k is the number of elements in G, and $(t_1 = t_2)$ is an identity true in R containing no more than k distinct variables, then $(t_1 = t_2)$ is true in R'. Then any map h: $G \to R'$ can be extended to a homomorphism H: $R \to R'$.*

(4.3) *Suppose that R' is an F-algebra such that every identity true in R is true in R'. Suppose that e: $G \to R'$ maps G onto a generating set. Then e can be extended to an epimorphism E: $R \to R'$.*

Proof. The origin of condition (4.1) was a perusal of Tarski [8]. The essential steps are contained in Lemmas 4.3 and 4.4. Lemma 4.2 can be proven by recursion on the definition of T. Further, we note that (4.1) has the following technical expression.

(4.4) Let $X = R^V$ and let D: $T \to R^X$ be the compositum homomorphism induced by the F-algebra R. Suppose there exists an $x \in X$ which maps the set of variables occurring in an identity $(t_1 = t_2)$ 1-1 into G, and in addition satisfies $(Dt_1)(x) = (Dt_2)(x)$; then $Dt_1 = Dt_2$.

LEMMA 4.2. *Let R_1, R_2 be F-algebras, let $X_1 = R_1^V$, $X_2 = R_2^V$, and let*

$$D_1\colon\ T \to R_1^{X_1}, \qquad D_2\colon\ T \to R_2^{X_2}$$

be the induced compositum homomorphisms. Then for any homomorphism H: $R_1 \to R_2$ and any $x \in X_1$, $H((D_1 t)(x)) = (D_2 t)(Hx)$.

LEMMA 4.3. *R is free on G implies that* (4.4) *holds.*

Proof. Let W be the subset of V consisting of all variables which occur in $(t_1 = t_2)$. It suffices to show that $(Dt_1)(y) = (Dt_2)(y)$ for $y \in X$. There exists a homomorphism H: $R \to R$ such that $H(x(v)) = y(v)$ for $v \in W$. Thus $(Dt_i)(y) = (Dt_i)(Hx)$, so Lemma 4.2 yields $(Dt_i)(y) = H((Dt_i)(x))$, $i = 1, 2$. Since $(Dt_1)(x) = (Dt_2)(x)$, $(Dt_1)(y) = (Dt_2)(y)$.

LEMMA 4.4. (4.4) *implies* (4.2).

Proof. It will be convenient to introduce the set Q of terms built out of G as set of individual variables and F as set of function symbols Let $X = R^G$,

$X' = (R')^G$, and let $D: Q \to R^X$, $D': Q \to (R')^{X'}$ be the homomorphisms induced by the F-algebras R and R' in accordance with Theorem 3.1, where we let G play the role of V. A recursion on the definition of Q shows that

(4.5) if $j: G \to R$ is the inclusion map, and $r \in R$, then there exists a $q \in Q$ with $(Dq)(j) = r$.

The definition of truth for identities shows that (4.4) and (4.2) are respectively equivalent to (4.6) and (4.7) below.

(4.6) If $q_1, q_2 \in Q$, and $(Dq_1)(j) = (Dq_2)(j)$, then $Dq_1 = Dq_2$.

(4.7) Suppose that R' is an F-algebra with the following property: if $q_1, q_2 \in Q$, $Dq_1 = Dq_2$, then $D'q_1 = D'q_2$. Then any map $h: G \to R'$ can be extended to a homomorphism $H: R \to R'$.

We derive (4.7) from (4.6). Apply (4.5) to define the $H: R \to R'$ required for (4.7) by the requirement that for $r \in R$, $Hr = (D'q)(h)$. This is independent of the choice of q. For if $r = (Dq_1)(j) = (Dq_2)(j)$, then by (4.6), $Dq_1 = Dq_2$; consequently (4.7) implies $D'q_1 = D'q_2$, so $(D'q_1)(h) = (D'q_2)(h)$. Moreover, H extends h since $Hg = (D'g)(h) = hg$.

Finally, we show that H is a homomorphism. If $f \in F$, denote by df the function f denotes in the F-algebra R, and by $d'f$ the function f denotes in the F-algebra R'. If n is the degree of f, and $q_1, \cdots, q_n \in Q$, it suffices by (4.5) to show that

$$H(df((Dq_1)(j), \cdots, (Dq_n)(j))) = d'f(H((Dq_1)(j)), \cdots, H((Dq_n)(j))).$$

To obtain the right term from the left, apply the definitions of D, H, D', H in that order.

COROLLARY 4.5. *Let R be an F-algebra free on G. Let G' be a nonempty subset of G, and let R' be the subalgebra generated by G'. Then R' is free on G'. Moreover, if $R' = R$, then $G' = G$.*

We say that an F-algebra R free on G is *characterized* by a set A of identities provided that every member of A is true in R and

(4.8) whenever the number of distinct variables occurring in an identity $(t_1 = t_2)$ true in R does not exceed the cardinality of G, then $(t_1 = t_2)$ is in the deductive closure of A.

For an example, suppose that F consists of a function symbol f of degree 2 and a function symbol g of degree 1. Let A be a set of identities true in an F-algebra if and only if f is the product and g the inverse operation for a group. Given a nonempty set G, there exist many nonisomorphic groups R free on G; in particular, the free group, the free abelian group, or free groups modulo fully invariant subgroups. However, only the free group generated by G is characterized by A.

THEOREM 4.6. *Let A be a nontrivial set of identities, and let G be a nonempty set. Then there exists an F-algebra R_G free on G characterized by A. Moreover, R_G is unique up to isomorphisms preserving G.*

Proof. To demonstrate uniqueness, suppose that R and R' are free on G and characterized by A. By (4.2) the identity map on G can be extended to epimorphisms $E: R \to R'$, $E': R' \to R$. E and E' are inverses and isomorphisms. As for existence, apply Corollary 2.8 to find a homomorphism $D: T \to R^X$ $(X = R^V)$ with kernel the deductive closure of A. According to Theorem 3.1, D induces an F-algebra R such that the deductive closure of A coincides with the set of true identities of R. Theorem 4.7 below implies the existence of an F-algebra R_G free on $\overline{G}$ characterized by A. Identifying G with $\overline{G}$ under $g \to \bar{g}$, R_G free on G is as desired.

For clarity in the next theorem, if $f \in F$, let $d_R f$ denote the function which f refers to in an F-algebra R.

THEOREM 4.7. *Let R be an F-algebra, let G be a nonempty set, and denote by P the set of all functions on R^G to R. Construe P as an F-algebra by requiring that for $f \in F$ of degree n and $p_1, \cdots, p_n \in P$,*

$$(d_P f(p_1, \cdots, p_n))(z) = d_R f(p_1(z), \cdots, p_n(z)), \qquad z \in R^G.$$

(4.9) *R and P have the same true identities.*

(4.10) *Let $-: G \to P$ be given by $\bar{g}(z) = z(g)$ for $g \in G$. Then the subalgebra R_G of P generated by $\overline{G}$ is free on $\overline{G}$ and characterized by the set of all identities true in R.*

LEMMA 4.8. *Suppose that R contains at least two elements, and that V, G are nonempty. Denote by P the set of all functions on R^G to R. Then each $y \in P^V$ induces a map $y': R^G \to R^V$ such that whenever $z \in R^G$, $(y'z)(v) = (y(v))(z)$ for all $v \in V$. Let $X = R^V$, $Y = P^V$, and define $M: R^X \to P^Y$ by requiring that for $t \in R^X$,*

$$((Mt)(y))(z) = t(y'z), \qquad y \in Y, z \in R^G. \tag{4.11}$$

Then M is a monomorphism on the concrete compositum R^X to the concrete compositum P^Y.

Proof. First, M is 1-1; that is, if $t_1, t_2 \in R^X$ and $Mt_1 = Mt_2$, then $t_1(x) = t_2(x)$ for all $x \in X$. For if we define $y \in Y$ by requiring that $y(v) \in P$ is that function on R^G to R with constant value $x(v)$, then $y'z = x$ for all $z \in R^G$: hence $((Mt_i)(y))(z) = t_i(x)$ for $i = 1, 2$.

For M, (2.1) is obvious. As for (2.2), note that for $s: R^X \to R^X$ in S, $y \in Y$,

$$((\tilde{M}s)\#y)'(z) = s\#(y'z) \qquad \text{for all } z \in R^G. \tag{4.12}$$

This follows from the fact that successive applications of the definitions of $'$, $\#$, $\tilde{M}$, M, and $\#$ again yield

$$(((\tilde{M}s)\#y)'z)(v) = ((M(s\bar{v}))(y))(z) = (s\bar{v})(y'z) = (s\#(y'z))(v).$$

Hence for $t \in R^X$, $(((\tilde{M}s)(Mt))(y))(z) = ((Mst)(y))(z)$, since the right-hand term can be obtained from the left by successive applications of (1.3), (4.11), (4.12), and finally (1.3), (4.11) again. For, note that

$$((\tilde{M}sMt)(y))(z) = ((Mt)((\tilde{M}s)^{\#}(y)))(z) = t(((\tilde{M}s)^{\#}y)'(z))$$
$$= t(s^{\#}(y'z)) = (st)(y'z) = ((Mst)(y))(z).$$

LEMMA 4.9. *Lemma* 4.8 *implies Theorem* 4.7.

Proof. Assume the notation of Lemma 4.8, and let $D: T \to R^X$ be the homomorphism induced by the F-algebra R in accordance with Theorem 3.1. Then $MD: T \to P^Y$ is a homomorphism inducing the F-algebra P defined in Theorem 4.7. Since M is 1-1, (4.9) follows. We employ (4.4) to prove (4.10). Let $k: V \to R_G$ map the set W of variables which occur in an identity $(t_1 = t_2)$ 1-1 into $\overline{G}$. Suppose further that

$$(D't_1)(k) = (D't_2)(k), \tag{4.13}$$

where D' is the homomorphism induced by the F-algebra R_G. It is sufficient to prove that

$$(Dt_1)(x) = (Dt_2)(x), \qquad x \in X. \tag{4.14}$$

For then $(t_1 = t_2)$ is true in R, hence by (4.9) also in P, hence in the subalgebra R_G of P; so by (4.4), it follows that R_G is free on $\overline{G}$. Further, since then the identity $(t_1 = t_2)$ is true in R, R_G is characterized by the set of all identities true in R.

To prove (4.14), let $z \in R^G$ be such that $(kv)(z) = x(v)$ for $v \in W$. Let $j: R_G \to P$ be the inclusion map. Since MD induces the F-algebra P and the inclusion map on R_G to P is a monomorphism, (ii) of Corollary 3.2 implies that $((D't_i)(k))(z) = ((MDt_i)(jk))(z)$ for $i = 1, 2$. Then (4.11) implies that for $i = 1, 2$, $((D't_i)(k))(z) = (Dt_i)(x)$. This and (4.13) imply (4.14).

COROLLARY 4.10. *Let G be a nonempty set. Let $P(G)$ be the collection of all subsets of G. Let $P(P(G))$ be the collection of all subsets of $P(G)$. If $g \in G$, denote by W_g the collection of all subsets of G containing g. Denote by W the set of all W_g for $g \in G$. Then the distributive sublattice of $P(P(G))$ generated by W is free on W.*

Proof. We remark that a similar result holds for boolean algebras, Post algebras, and many other algebraic systems. Let the set F of function symbols consist of $\cup$, $\cap$ each of degree 2. As a consequence of either the representation theorem for distributive lattices, or a direct combinatory argument,

(4.15) An F-algebra is a distributive lattice if and only if its set of true identities coincides with the set of true identities of the two element distributive lattice R consisting of 0 and 1.

If R_G is given by Theorem 4.7, then (4.15) implies that R_G must be the free distributive lattice with generating set $\overline{G}$, due to the uniqueness assertion of Theorem 4.6. The vital remaining assertion is that there exists a natural isomorphism between the distributive lattice P given by Theorem 4.7 and the distributive lattice $P(P(G))$ under which each $\bar{g}$ corresponds to W_g, $\overline{G}$ to

W, and R_G to the sublattice of $P(P(G))$ generated by W. This isomorphism is given by characteristic functions in the obvious way.

For the last two theorems we assume as known the notions of congruence relation and direct product (union) for algebras from Birkhoff [4, pp. VII–VIII]; we also employ the analogues of Theorems 2.2, 2.3 for algebras.

Let R be an F-algebra free on G. Then a proper congruence relation for the algebra R is called *fully invariant* if also a congruence relation for the G-compositum R. An algebra homomorphism $H: R \to R'$ is *fully invariant* if H is 1-1 on G, R' is free on $H(G)$, and H is a compositum homomorphism on the G-compositum R to the $H(G)$-compositum R'. R free on G is *irreducible* if whenever $\{E_C: R \to R_C\}_{C \in K}$ is an indexed collection of fully invariant epimorphisms and the map $M: R \to \prod_{C \in K} R_C$ given for $r \in R$ by $(Mr)_C = E_C r$ is a monomorphism, then for some $C \in K$, E_C is an isomorphism.

For an example, let R be a free boolean algebra free on generating set G. Note that if C is a fully invariant congruence relation on R, then the equivalence class containing 0 is a boolean ideal closed under all endomorphisms of R; the only such ideals are the unit ideal and the zero ideal.

For another example, let R_1 be a free abelian group free on generating set G_1. Let p be a prime, let $a \geqq 1$ be an integer, and let $p^a R_1$ be the subgroup of p^a-powers in R_1. If G is the image of G_1 in $R = R_1/p^a R_1$, then R is free on G and irreducible.

For a last example, let A be a maximal nontrivial set of identities (any such set is complete in the sense of Kalicki and Scott [6]), and let R free on G be characterized by A.

By imitating the argument of Birkhoff [4, p. 92], letting fully invariant congruence relations play the role that congruence relations fill in the argument of Birkhoff, we obtain

THEOREM 4.11. *Let R be free on G but not irreducible. Then there exists a collection $\{E_C: R \to R_C\}_{C \in K}$ of fully invariant epimorphisms, none of which is a monomorphism, such that: R_C is irreducible for all $C \in K$; the map*

$$M: R \to \prod_{C \in K} R_C$$

given by $(Mr)_C = E_C r$ is a monomorphism.

Resuming the notation of the second of the group of examples preceding, we obtain a monomorphism $M: R_1 \to \prod_{p^a} R_1/p^a R_1$ of the given type by setting $(Mr_1)_{p^a} = r_1 + p^a R_1$ for $r_1 \in R_1$. (The product extends over all primes p and all $a \geqq 1$.)

The next and last theorem is closely related to [2, Theorem 10], but differs from the latter in that it refers to the internal structure of a single arbitrary freely generated algebra.

THEOREM 4.12. *Let R be an F-algebra free on G. Let K be a nonempty col-*

lection of proper congruence relations on R. Then the following conditions are equivalent.

(i) *There exists a nontrivial set A of identities such that if C is the kernel of an epimorphism $E: R \to R'$, then $C \in K$ if and only if every member of A is true in R'.*

(ii) (a) *If K' is a nonempty subset of K, and C is a proper congruence relation containing the intersection of all members of K', then $C \in K$.*

(b) *Suppose that C is the kernel of an epimorphism $E: R \to R'$ and that C_H is proper and the kernel of a homomorphism $H: R \to R'$. Then if $C \in K$, it follows that $C_H \in K$.*

Proof. It is routine to verify that (i) implies (ii). We verify the converse. Let $E_2: R \to R_2$ be an epimorphism with kernel the intersection C_2 of all members of K. Let A be the set of all identities true in R_2. We show that A will do.

One part is easy. If $E_3: R \to R_3$ is an epimorphism with kernel $C_3 \in K$, then A is true of R_3; for then C_3 contains C_2, hence by the analogue of Theorem 2.2 for algebras, there is an epimorphism $E_1: R_2 \to R_3$.

We conclude by showing that if $E_3: R \to R_3$ has kernel C_3 and every member of A is true in R_3, then $C_3 \in K$. This we derive from (4.16) below. Since every identity true in R_2 is true in R_3, (4.16) and (4.3) imply that there exists an epimorphism $E_1: R_2 \to R_3$ with $E_1E_2g = E_3g$ for $g \in G$. Since E_1E_2, E_3 agree on a generating set, $E_1E_2 = E_3$. Hence C_3 contains C_2. Then (ii)(a) yields that $C_3 \in K$.

(4.16) The map $g \in G \to E_2g \in E_2G$ maps G 1-1 onto E_2G. Moreover, R_2 is free on E_2G.

Suppose that $g_1, g_2 \in G$, $g_1 \neq g_2$. Since every identity true in R is also true in R_2, and since R_2 contains at least two elements, (4.2) implies that there exists a homomorphism $H: R \to R_2$ with $Hg_1 \neq Hg_2$. Then (ii)(b) implies that K contains the kernel C_H of H, and hence also C_H contains C_2. Consequently, (g_1, g_2) is not in C_2, or g_1, g_2 have distinct images under E_2.

Finally, we must extend any $h: E_2G \to R_2$ to an endomorphism $H: R_2 \to R_2$. Since R is free on G, there exists an endomorphism $e: R \to R$ with $E_2eg = hE_2g$ for $g \in G$. Hence by (ii)(b), the kernel C of $E_2e: R \to R_2$ is in K if proper. Thus C contains C_2, so the analogue of Theorem 2.2 for algebras implies that there exists a homomorphism $H: R_2 \to R_2$ such that $E_2e = HE_2$. Moreover, H extends h.

References

1. S. A. Amitsur, *The T-ideals of the free ring*, J. London Math. Soc. vol. 30 (1955) pp. 470–475.

2. G. Birkhoff, *On the structure of abstract algebras*, Proc. Cambridge Philos. Soc. vol. 31 (1935) pp. 433–454.

3. ———, *Universal algebra*, Proceedings of the Canadian Mathematical Congress, vol. 1, 1945, pp. 310–326.

4. ———, *Lattice theory*, Amer. Math. Soc. Colloquium Publications, vol. 25, rev. ed., New York, 1948.

5. A. L. Foster, *The identities of—and unique subdirect factorization within—classes of universal algebras*, Math. Z. vol. 62 (1955) pp. 171–188.

6. J. Kalicki and D. Scott, *Equational completeness of abstract algebras*, Nederl. Akad. Wetensch. Proc. Ser. A. vol. 58 (1955) pp. 650–659.

7. H. F. J. Lowig, *Gesetzrelationen uber frei erzeugten Algebren*, J. Reine Angew. Math. vol. 193 (1954) pp. 129–142.

8. A. Tarski, *A remark on functionally free algebras*, Ann. of Math. vol. 47 (1946) pp. 163–165.

9. ———, *Contributions to the theory of models* III, Nederl. Akad. Wetensch. Proc. Ser. A. vol. 58 (1955) pp. 56–63.

INSTITUTE FOR ADVANCED STUDY,
PRINCETON, N. J.
UNIVERSITY OF CHICAGO,
CHICAGO, ILL.