RESEARCH ANNOUNCEMENTS

The purpose of this department is to provide early announcement of significant new results, with some indications of proof. Although ordinarily a research announcement should be a brief summary of a paper to be published in full elsewhere, papers giving complete proofs of results of exceptional interest are also solicited. Manuscripts more than eight typewritten double spaced pages long will not be considered as acceptable. All papers to be communicated by a Council member should be sent directly to M. H. Protter, Department of Mathematics, University of California, Berkeley, California 94720.

STRUCTURE OF INCIDENCE ALGEBRAS AND THEIR AUTOMORPHISM GROUPS[1]

BY RICHARD P. STANLEY

Communicated by Gian-Carlo Rota, June 9, 1970

Let P be a locally finite ordered set, i.e., a (partially) ordered set for which every segment $[X, Y]=\{Z \mid X \leqq Z \leqq Y\}$ is finite. The *incidence algebra* $I(P)$ of P over a field K is defined [2] as the algebra of all functions from segments of P into K under the multiplication (convolution)

$$fg(X, Y) = \sum_{Z\in[X,Y]} f(X, Z)g(Z, Y).$$

(We write $f(X, Y)$ for $f([X, Y])$.) Note that the algebra $I(P)$ has an identity element δ given by

$$\begin{aligned} \delta(X, Y) &= 1, \quad \text{if } X = Y, \\ &= 0, \quad \text{if } X \neq Y. \end{aligned}$$

THEOREM 1. *Let P and Q be locally finite ordered sets. If $I(P)$ and $I(Q)$ are isomorphic as K-algebras, then P and Q are isomorphic.*

SKETCH OF PROOF. The idea is to show that the ordered set P can be uniquely recovered from $I(P)$. Let the elements of P be denoted X_α, where α ranges over some index set. Then a maximal set of primitive orthogonal idempotents for $I(P)$ consists of the functions e_α defined by

---

AMS 1969 *subject classifications*. Primary 0620, 1650, 1660; Secondary 0510.

Key words and phrases. Ordered set, partially ordered set, incidence algebra, primitive orthogonal idempotents, outer automorphism group, Hasse diagram.

[1] The research was supported by an NSF Graduate Fellowship and by the Air Force Office of Scientific Research AF 44620-70-C-0079.

$$\begin{aligned} e_\alpha(X_\beta, X_\gamma) &= 1, \quad &&\text{if } \alpha = \beta = \gamma, \\ &= 0, &&\text{otherwise.} \end{aligned}$$

Define an order relation P' on the e_α's by $e_\alpha \leqq e_\beta$ if and only if $e_\alpha I(P) e_\beta \neq 0$. It is easy to see that this order relation is a partial ordering isomorphic to P.

The proof will be complete if we show that given any maximal set of primitive orthogonal idempotents, the order relation defined on this set in analogy to P' is isomorphic to P'. It is easily seen that any maximal set of primitive orthogonal idempotents of $I(P)$ can be labeled as f_α, so that $e_\alpha - f_\alpha \in J$, where J is the two-sided ideal $\{f \mid f(X, X) = 0 \text{ for all } X \in P\}$. We have $\bigcap_{m \geq 1} J^m = 0$. Theorem 1 is now a consequence of the following general ring-theoretic lemma.

LEMMA. *Let R be an associative ring. Suppose e, f, e', f' are idempotents in R such that $e' - e$ and $f' - f$ belong to some two-sided ideal J satisfying $\bigcap_{m \geq 1} J^m = 0$. Then $eRf = 0$ if and only if $e'Rf' = 0$.*

PROOF OF LEMMA. By symmetry it suffices to prove $eRf = 0 \Rightarrow e'Rf' = 0$. Suppose $eRf = 0$. Let $e' = e + x$, $f' = f + y$, where $x, y \in J$. Since e, e', f, f' are idempotent, we have

$$x = ex + xe + x^2, \tag{1}$$

$$y = fy + yf + y^2. \tag{2}$$

Let $a \in R$. Then $e'af' = (e+x)a(f+y) = xaf + eay + xay \in J$, since $eaf = 0$. Substitute for x and y the expressions in (1) and (2). When the resulting expression for $e'af'$ is simplified using $eRf = 0$, we get

$$\begin{aligned} e'af' = {} & x^2af + eay^2 + exay^2 \\ & + xeay^2 + x^2afy + x^2ayf + x^2ay^2 \in J^2. \end{aligned}$$

Again substitute for x and y the expressions in (1) and (2). After simplifying there results $e'af' \in J^4$. Continuing in this way, it is easily proved by induction that after n steps we get $e'af' \in J^{2^n}$. Since $\bigcap_{m \geq 1} J^m = 0$, $e'af' = 0$. This proves the Lemma and with it Theorem 1.

Now let P be a *finite* ordered set, and $\mathcal{A}(I(P))$ be the K-automorphism group of $I(P)$. Let $\mathcal{I}n(I(P))$ be the group of inner automorphisms of $I(P)$, i.e., automorphisms of the form $g \to f^{-1}gf$ for some fixed invertible element $f \in I(P)$. The *outer automorphism* group $\mathcal{O}(I(P))$ is defined to be the quotient group

$$\mathcal{O}(I(P)) = \mathcal{A}(I(P)) / \mathcal{I}n(I(P)).$$

Let $\mathcal{A}(P)$ denote the group of automorphisms of P. If $\sigma \in \mathcal{A}(P)$, then

σ defines an automorphism (also denoted σ) of $I(P)$ by

$$(\sigma f)(X, Y) = f(\sigma X, \sigma Y), \qquad f \in I(P).$$

If f is an invertible element of $I(P)$ and g any element of $I(P)$, then $f^{-1}gf(X, X) = g(X, X)$ for all $X \in P$. It follows that if $\sigma \neq 1$ in $\mathcal{A}(P)$, then the image of σ in $\mathcal{O}(I(P))$ also $\neq 1$. Thus $\mathcal{O}(I(P))$ contains a subgroup naturally isomorphic to $\mathcal{A}(P)$.

Let H denote the Hasse diagram of P, considered as a graph. Thus the vertices of H are the elements of P, and two vertices X and Y are connected by an edge if and only if either X covers Y or Y covers X in P. (We say that X *covers* Y if $X > Y$, and whenever $X \geqq Z > Y$, then $X = Z$.) Let r denote the dimension of the (mod 2) circuit subspace V of H [1, Chapter 7–4], and let t denote the dimension of the subspace of V generated by circuits consisting of two unrefinable chains of P with the same endpoints.

THEOREM 2. *If P is a finite ordered set, then $\mathcal{O}(I(P))$ is isomorphic to a semidirect product of $(K^*)^{r-t}$ by $\mathcal{A}(P)$, where K^* is the multiplicative group of K.*

SKETCH OF PROOF. Let $\mathcal{E}$ be the subgroup of $\mathcal{A}(I(P))$ fixing every e_α, and let $\mathcal{E}' = \mathcal{E} \cap \mathcal{I}n(I(P))$. If $\{f_\alpha\}$ is any maximal set of primitive orthogonal idempotents, labeled so that $e_\alpha - f_\alpha \in J$, then $g = \sum e_\alpha f_\alpha$ is an invertible element of $I(P)$ satisfying $g^{-1}e_\alpha g = f_\alpha$ for all α. From this it follows that $\mathcal{O}(I(P))$ is isomorphic to a semidirect product of $\mathcal{E}/\mathcal{E}'$ by $\mathcal{A}(P)$. It remains to determine $\mathcal{E}/\mathcal{E}'$.

When $X_\alpha \leqq X_\beta$ in P, define $\delta_{\alpha\beta} \in I(P)$ by

$$\begin{aligned} \delta_{\alpha\beta}(X_\gamma, X_\eta) &= 1, \qquad \text{if } \alpha = \gamma \quad \text{and} \quad \beta = \eta, \\ &= 0, \qquad \text{otherwise.} \end{aligned}$$

Thus in particular $\delta_{\alpha\alpha} = e_\alpha$. The functions $\delta_{\alpha\beta}$ form a K-basis for $I(P)$ (when P is finite). If $X_\alpha \leqq X_\beta$, then $e_\alpha I(P) e_\beta$ is a one-dimensional subspace of $I(P)$ spanned by $\delta_{\alpha\beta}$; otherwise $e_\alpha I(P) e_\beta = 0$. Thus any $\sigma \in \mathcal{E}$ satisfies $\sigma(\delta_{\alpha\beta}) = c_{\alpha\beta}\delta_{\alpha\beta}$, where $c_{\alpha\beta} \in K^*$. It is not hard to show that some $q - t$ of the scalars $c_{\alpha\beta}$ can be chosen independently to define a unique $\sigma \in \mathcal{E}$, where q is the number of edges of H. Hence $\mathcal{E} \cong (K^*)^{q-t}$.

One can also show without much difficulty that $\mathcal{E}'$ consists of $p - c$ of the $q - t$ factors of $\mathcal{E}$, where p is the number of vertices and c the number of connected components of H. It follows that $\mathcal{E}/\mathcal{E}' \cong (K^*)^{q-t-(p-c)}$. Since $q - p + c = r$, the proof follows.

To extend this theorem to arbitrary locally finite ordered sets, topological considerations are necessary.

EXAMPLE. Let P be the ordering of W, X, Y, Z defined by $W < Y$,

$W<Z$, $X<Y$, $X<Z$. Then $r=1$ and $t=0$, so $\mathcal{O}(I(P))$ and $\mathcal{A}(P)$ are not isomorphic unless $K=GF(2)$. This provides a specific counterexample to a conjecture made by several persons (unpublished) that $\mathcal{O}(I(P))$ and $\mathcal{A}(P)$ are always isomorphic.

It is easy to see, however, that if P has a unique minimal element 0 or unique maximal element 1, then $r=t$. Thus we get:

COROLLARY. *Let P be a finite ordered set with* 0 *or* 1. *Then* $\mathcal{O}(I(P)) \cong \mathcal{A}(P)$.

REFERENCES

1. C. L. Liu, *Introduction to combinatorial mathematics*, McGraw-Hill, New York, 1968. MR **38** #3154.

2. G. -C. Rota, *On the foundations of combinatorial theory*. I: *Theory of Möbius functions*, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete **2** (1964), 340–368. MR **30** #4688.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MASSACHUSETTS 02139