

## HOMOMORPHISMS OF INTEGRAL DOMAINS OF CHARACTERISTIC ZERO

BY

E. FRIED AND J. SICHLER<sup>(1)</sup>

**ABSTRACT.** Every category of universal algebras is isomorphic to a full subcategory of the category of all integral domains of characteristic zero and all their 1-preserving homomorphisms. Consequently, every monoid is isomorphic to the monoid of all 1-preserving endomorphisms of an integral domain of characteristic zero.

**1. Introduction.** An *integral domain* is, as usual, a commutative ring with no zero divisors. Let  $\mathbf{I}$  denote the category of all integral domains and all their homomorphisms, let  $\mathbf{I}_k$  denote the category of all integral domains with 1 and of characteristic  $k$  ( $k$  is zero or a prime) and all their 1-preserving homomorphisms. Finally, let  $\mathbf{J}_0$  stand for the category of all integral domains of characteristic zero with no units and all their homomorphisms. Note that every nonzero homomorphism of integral domains with 1 must be 1-preserving.

To state the principal results we need to recall some categorical concepts.

All functors are covariant unless specified otherwise. A functor  $\mathbf{F}: \mathbf{A} \rightarrow \mathbf{B}$  which is one-to-one on every  $\text{Hom}_{\mathbf{A}}(a, a')$  is called *faithful*; if, in addition,  $\mathbf{F}$  is also one-to-one on the class of all objects of  $\mathbf{A}$  we call it an *embedding*.  $\mathbf{F}$  is *full* if every morphism  $d: \mathbf{F}(a) \rightarrow \mathbf{F}(a')$  of  $\mathbf{B}$  has the form  $d = \mathbf{F}(c)$  for some morphism  $c: a \rightarrow a'$  from  $\mathbf{A}$ . A *full embedding* thus defines an isomorphism between  $\mathbf{A}$  and a *full subcategory* of  $\mathbf{B}$ . A *concrete category* is a category  $\mathbf{A}$  together with a fixed faithful functor  $\mathbf{U}: \mathbf{A} \rightarrow \mathbf{Set}$  into the category  $\mathbf{Set}$  of all sets and all mappings. A category  $\mathbf{A}$  of universal algebras will always be considered as a concrete category whose faithful functor  $\mathbf{U}: \mathbf{A} \rightarrow \mathbf{Set}$  is the usual underlying-set functor.

Let  $\mathbf{A}_1, \mathbf{A}_2$  be concrete categories and let  $\mathbf{U}_i: \mathbf{A}_i \rightarrow \mathbf{Set}$  be their corresponding functors. A full embedding  $\mathbf{F}: \mathbf{A}_1 \rightarrow \mathbf{A}_2$  is called an *extension* if there is a monotransformation  $\mathbf{m}: \mathbf{U}_1 \rightarrow \mathbf{U}_2 \circ \mathbf{F}$  (i.e., a natural transformation whose components  $\mathbf{m}_a: \mathbf{U}_1(a) \rightarrow \mathbf{U}_2(\mathbf{F}(a))$  are one-to-one mappings).  $\mathbf{F}$  is a *strong*

---

Received by the editors August 19, 1975.

*AMS (MOS) subject classifications* (1970). Primary 13G05, 18B15; Secondary 08A25, 13B10.

*Key words and phrases.* Integral domain, universal algebra, homomorphism, concrete category, full embedding, binding category.

<sup>(1)</sup> The work of both authors was supported by the National Research Council of Canada.

© American Mathematical Society 1977

*embedding* if  $H \circ U_1 = U_2 \circ F$  for some faithful functor  $H: \mathbf{Set} \rightarrow \mathbf{Set}$ ;  $H$  is called the *carrier of F*. It is easy to see that a functor  $H: \mathbf{Set} \rightarrow \mathbf{Set}$  is faithful if and only if there is a monotransformation of the identity functor on  $\mathbf{Set}$  into  $H$ ; thus every strong embedding is also an extension.

DEFINITION 1. A category  $C$  is *binding* (or *universal*) if every category  $A$  of universal algebras has a full embedding into  $C$ . If  $C$  is concrete with  $V: C \rightarrow \mathbf{Set}$ , then  $C$  is called *strongly binding* (or *strongly universal*) if every category of universal algebras can be strongly embedded into  $C$ .

Note that every strongly universal category has to be also universal. [6] contains a basic list of simple universal categories: the category  $\mathbf{R}$  of directed graphs and all their compatible mappings, the category  $A(2)$  of all groupoids and all their homomorphisms, and the category  $2A$  of all algebras with two unary operations and all their homomorphisms. The list of binding categories of algebras has later been extended by the category of semigroups [4], the category of bounded lattices and all their  $(0, 1)$ -preserving homomorphisms [2], and the category of commutative rings with 1 and all their 1-preserving homomorphisms [1]—to name only a few. Since binding categories of algebras can be fully embedded into each other, an addition  $C$  to the list of binding categories can be obtained simply by a construction of a full embedding into  $C$  of any category from the list above. It was shown in [9] that  $2A$  is a strongly universal category; to prove strong universality of a concrete category  $C$  it is therefore enough to construct a strong embedding of  $2A$  into  $C$ .

Since every monoid  $M$  is isomorphic to the full endomorphism monoid of an algebra with unary operations (e.g., to the endomorphism monoid of the dual of the Cayley representation of  $M$ ), it is clear that a universal category will contain an object whose endomorphism monoid is isomorphic to  $M$ .

Another important property of a binding category  $C$  is that it contains a proper class of pairwise nonisomorphic rigid objects ( $c$  is *rigid* if  $\text{Hom}_C(c, c) = \{1_c\}$ )—see, for instance, [7]. Since the zero mapping is always one of the endomorphisms of a ring, there are no nontrivial rigid integral domains. Similarly, the mapping  $x \mapsto x^p$  is always one of the 1-preserving endomorphisms of an integral domain  $I$  of a prime characteristic  $p$ ; this mapping is trivial only if  $I$  is one of the finite primefields. Hence the following negative result.

PROPOSITION 1. *None of the categories  $\mathbf{I}$ ,  $\mathbf{J}_0$ ,  $\mathbf{I}_p$  ( $p$  prime) is universal.*

It will be seen later that removal of the zero morphisms from  $\mathbf{I}$  ( $\mathbf{J}_0$ , respectively) will give rise to a class  $\mathbf{I}^*$  ( $\mathbf{J}_0^*$ , respectively) containing a strongly binding category as a full subcategory.

Throughout the paper we are working within the framework of the Gödel-Bernays set theory including the axiom of choice for sets.

Following is the list of results proved here.

**THEOREM 1.** *There is a strong embedding  $F: 2A \rightarrow I_0$  carried by a functor  $H: \text{Set} \rightarrow \text{Set}$  such that  $H(X)$  is countably infinite for every finite set  $X$  and  $\text{card}(H(X)) = \text{card}(X)$  if  $X$  is infinite. Consequently,  $I_0$  is strongly universal.*

Since an extension cannot decrease cardinalities of underlying sets and since  $I_0$  has no finite objects the strong embedding  $F$  above is the smallest possible in terms of cardinalities of underlying sets. Theorem 1 is the main result that is subsequently used in conjunction with results found elsewhere to obtain Theorems 2–6.

**DEFINITION 2.** A *transformation monoid* is a pair  $(X, N)$  in which  $X$  is a set and  $N \subseteq X^X$  includes the identity transformation  $1_X$  and is closed under composition of mappings.

The next theorem determines the number of nonisomorphic objects of  $I_0$  with isomorphic endomorphism monoids.

**THEOREM 2.** *Let  $M$  be a monoid and let  $c \geq \text{card}(M) + \aleph_0$  be a cardinal number. Then there is a transformation monoid  $(X, M^*) \cong M$  on a set  $X$  of cardinality  $c$  and a system  $(I_a: a \in 2^c)$  of integral domains of characteristic zero such that:*

(i) *every  $I_a$  is defined on  $X$  and the monoid of all 1-preserving endomorphisms of each  $I_a$  equals to  $(X, M^*)$ ;*

(ii) *if  $f: I_a \rightarrow I_{a'}$  is a 1-preserving homomorphism, then  $a = a'$ .*

This, in a way, is a negative result: not even a complete description of the endomorphisms would single out a particular object of  $I_0$ . Since  $c$  has no upper bound we see that there is a proper class of pairwise nonisomorphic objects of  $I_0$  with endomorphism monoids isomorphic to a given monoid  $M$ . There are exactly  $2^c$  pairwise nonisomorphic integral domains of cardinality  $c$  and in this sense Theorem 2 is the best possible as it gives the same (maximal) number of nonisomorphic domains representing a given monoid  $M$ .

**THEOREM 3.** *For every monoid  $M$  there is an integral domain  $I$  of characteristic zero such that:*

(i) *the monoid of all 1-preserving endomorphisms of  $I$  is isomorphic to  $M$ ;*

(ii) *the category of all objects of  $I_0$  containing  $I$  as a subring is binding.*

**THEOREM 4.** *For every monoid  $M$  there is an integral domain  $I$  of characteristic zero such that:*

(i) *the monoid of all 1-preserving endomorphisms of  $I$  is isomorphic to  $M$ ;*

(ii) *the category of all objects of  $I_0$  that have  $I$  as a quotient object is binding.*

Thus, in particular, the endomorphism monoids of pairs object-subobject (object-quotient object, respectively) in  $I_0$  are independent and can be chosen arbitrarily.

**THEOREM 5.** *For every transformation monoid  $(X, M)$  there is an integral*

domain  $I$  in  $I_0$  such that:

- (i)  $I$  contains  $X$ ;
- (ii) every mapping  $m \in M$  extends uniquely to an endomorphism of  $I$ ;
- (iii) this extension is an isomorphism between  $M$  and the endomorphism monoid of  $I$ .

For a given  $(X, M)$  there is a proper class of pairwise nonisomorphic objects  $I$  of  $I_0$  satisfying (i), (ii), (iii).

In another words, every one-object concrete category can be extended into  $I_0$ . This suggests another question: what concrete categories can be extended into  $I_0$ ? A powerful (unpublished) theorem of L. Kučera and Z. Hedrlín states that under the set-theoretical assumption:

(M) there is a cardinal number  $c$  such that every  $c$ -complete ultrafilter is principal,

every concrete category has an extension into  $2A$ . Since any strong embedding is an extension and since composites of extensions are extensions again, Theorem 1 implies that under (M) every concrete category can be extended into  $I_0$ . On the other hand, the dual  $\mathbf{Set}^{\text{opp}}$  of the category  $\mathbf{Set}$  can be fully embedded into a category of algebras only if (M) holds [8]. Since there are covariant faithful functors  $\mathbf{Set}^{\text{opp}} \rightarrow \mathbf{Set}$  the following generalization of Theorem 5 holds.

**THEOREM 6.** *The following three statements are equivalent:*

- (i)  $\mathbf{Set}^{\text{opp}}$  can be fully embedded into  $I_0$ ,
- (ii) every concrete category has an extension into  $I_0$ ,
- (iii) there is a cardinal number  $c$  such that every  $c$ -complete ultrafilter is principal.

The strong embedding  $F: 2A \rightarrow I_0$  is described in the next section; §3 contains ring-theoretic results needed for the proof of fulness of  $F$ . Proofs of Theorems 2–5 are included in the last part of the paper.

**2. Construction of the strong embedding  $F$ .** Let  $X$  be a set and let  $\bar{X}$  denote another copy of  $X$  such that  $X \cap \bar{X} = \emptyset$ . Fix once and for all a bijection  $x \mapsto \bar{x}$  of  $X$  onto  $\bar{X}$ . Denote by  $P(X)$  the ring of all polynomials over  $X \cup \bar{X}$  with integer coefficients, i.e.,  $P(X) = Z[X \cup \bar{X}]$  and let  $K(X)$  be the ideal of  $P(X)$  generated by the set  $\{x^3 + \bar{x}^3 - 5: x \in X\}$ . Set  $D(X) = P(X)/K(X)$  and let  $\varphi_X: P(X) \rightarrow D(X)$  be the natural homomorphism whose kernel is  $K(X)$ . For an element  $p = p(x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n)$  of  $P(X)$  denote by  $d(p)$  its total degree, by  $d_y(p)$  the degree of  $p$  in an indeterminate  $y \in X \cup \bar{X}$ . Let  $c(p)$  denote the codegree of  $p$ , that is, the smallest degree of a nonzero monomial term of  $p$ . Define

$$T(X) = \{p \in P(X): c(p) > 3\}, \quad J(X) = 5D(X) + \varphi_X(T(X)),$$

and note that  $J(X)$  is an ideal of  $D(X)$ . Given a mapping  $f: X_0 \rightarrow X_1$  define an extension  $f_1: X_0 \cup \bar{X}_0 \rightarrow X_1 \cup \bar{X}_1$  of  $f$  by  $f_1(x) = f(x)$ ,  $f_1(\bar{x}) = \overline{f(x)}$ . The mapping  $f_1$  extends uniquely to a 1-preserving homomorphism  $P(f): P(X_0) \rightarrow P(X_1)$  which maps  $K(K_0)$  into  $K(X_1)$ . Hence there is a unique 1-preserving homomorphism  $D(f): D(X_0) \rightarrow D(X_1)$  such that  $\varphi_{X_1} \circ P(f) = D(f) \circ \varphi_{X_0}$ ; note that  $D(f)$  maps  $J(X_0)$  into  $J(X_1)$ .

Given an algebra  $(X; \alpha, \beta)$  in  $2A$ , define  $F(X; \alpha, \beta)$  as the subring of  $D(X)$  generated by the set

$$Y = Z \cup \{ \varphi_X(x^2 \cdot \overline{\alpha(x)}) : x \in X \} \cup \{ \varphi_X(x \cdot \overline{\beta(x)}) : x \in X \} \cup J(X).$$

If  $f: (X; \alpha, \beta) \rightarrow (X'; \alpha', \beta')$  is a homomorphism of the two unary algebras, then  $D(f)$  maps the group  $Z + J(X)$  into  $Z + J(X')$ , and

$$\begin{aligned} D(f)(\varphi_X(x^2 \cdot \overline{\alpha(x)})) &= \varphi_{X'}(P(f)(x^2 \cdot \overline{\alpha(x)})) = \varphi_{X'}(f(x)^2 \cdot f_1(\overline{\alpha(x)})) \\ &= \varphi_{X'}(f(x)^2 \cdot \overline{f(\alpha(x))}) = \varphi_{X'}(f(x)^2 \cdot \overline{\alpha'(f(x))}); \end{aligned}$$

similarly

$$D(f)(\varphi_X(x \cdot \overline{\beta(x)})) = \varphi_{X'}(f(x) \cdot \overline{\beta'(f(x))})$$

for all  $x \in X$ . Thus  $D(f)$  maps  $F(X; \alpha, \beta)$  into  $F(X'; \alpha', \beta')$  and this enables us to define  $F(f)$  as the restriction of  $D(f)$  to  $F(X; \alpha, \beta)$ . It is easy to see that  $1 \in D(X)$  and that  $D(X)$  is an integral domain of characteristic zero. Hence  $F(X; \alpha, \beta)$  is an object in  $I_0$  for every  $(X; \alpha, \beta)$  from  $2A$ ;  $F$  is a covariant functor from  $2A$  into  $I_0$ .

We need the lemma below to prove that  $F$  is carried by a faithful functor **H: Set**  $\rightarrow$  **Set**.

**LEMMA 1.** *For every  $d \in D(X)$  there are uniquely determined  $j \in J(X)$  and  $p_0 \in P(X)$  such that:*

- (a) *the coefficients of  $p_0$  are elements of the set  $\{0, 1, 2, 3, 4\}$ ;*
- (b)  *$d(p_0) \leq 3$ ;*
- (c)  *$d_{\bar{x}}(p_0) < 3$  for every  $\bar{x} \in \bar{X}$ ,*

*and  $d = \varphi_X(p_0) + j$ .*

**PROOF.** Since  $\varphi_X$  is onto,  $d = \varphi_X(q)$  for some  $q \in P(X)$ ; write  $q = q_0 + q_1$ , where  $d(q_0) \leq 3$  and  $c(q_1) > 3$ . Replace every occurrence of  $\bar{x}^3$  in  $q_0$  by  $5 - x^3$  to obtain a polynomial  $r_0$  satisfying (b) and (c) and such that  $\varphi_X(r_0) = \varphi_X(q_0)$ .  $r_0 = p_0 + 5p_1$  where  $p_0$  satisfies (a). It is clear that (b) and (c) also hold for  $p_0$ ;

$$\begin{aligned} d &= \varphi_X(q) = \varphi_X(q_0) + \varphi_X(q_1) \\ &= \varphi_X(r_0) + \varphi_X(q_1) = \varphi_X(p_0) + \varphi_X(5p_1 + q_1), \end{aligned}$$

where the second term belongs to  $J(X)$ .

We will prove the uniqueness of the representation now. Let  $\rho$  be a third

root of 1 (i.e.,  $\rho^2 + \rho + 1 = 0$ ) and set  $G(X) = Z_5[\rho][X]$ . Let  $S$  denote the set of all homomorphisms  $s: P(X) \rightarrow G(X)$  such that  $s(x) = x$  and  $s(\bar{x}) = -\rho^i x$  ( $i$  depends on  $x$ ) for all  $x \in X$ .  $s(x^3 + \bar{x}^3 - 5) = 0$  and, hence,  $\text{Ker}(s) \supseteq K(X) = \text{Ker}(\varphi_X)$  for all  $s \in S$ ; let  $s^*: D(X) \rightarrow G(X)$  denote the unique homomorphism for which  $s = s^* \circ \varphi_X$ . If  $0 = \varphi_X(p_0) + j$ , then  $0 = s^*(\varphi_X(p_0) + j) = s(p_0) + s(t)$ , where  $t = 0$  or  $c(t) > 3$ . Since for every monomial  $m \in P(X)$  either  $s(m) = 0$  or  $d(s(m)) = d(m)$ , we get  $d(s(p_0)) < d(p_0) < 3 < c(t) < c(s(t))$  which, in turn, implies  $s(p_0) = 0$  and  $s(t) = 0$  for every  $s \in S$ . We will show that  $s(p_0) = 0$  for every  $s \in S$  and  $p_0$  satisfying (a), (b), (c) holds only if  $p_0 = 0$  (by induction on the number of pairs  $\{x, \bar{x}\}$  of indeterminates of  $p_0$ ). If  $p_0$  is a constant, then it must be zero because any  $s \in S$  is one-to-one on  $\{0, \dots, 4\}$ ; let  $p_0 = p_0(x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n)$  and let the claim be valid for all  $q_0(x_1, \dots, x_{n-1}, \bar{x}_1, \dots, \bar{x}_{n-1})$  satisfying (a)–(c).  $p_0$  can be written in the form

$$(1) \quad p_0 = A_0(x_n) + A_1(x_n) \cdot \bar{x}_n + A_2(x_n) \cdot \bar{x}_n^2,$$

where all  $A_i(x_n)$  satisfy (a)–(c) and do not depend on  $\bar{x}_n$ . Let  $s \in S$  be arbitrary and let us define new homomorphisms  $s_0, s_1, s_2 \in S$  by  $s_i(z) = s(z)$  for all  $z \in X \cup \bar{X}$ ,  $z \neq \bar{x}_n$ , and by  $s_i(\bar{x}_n) = -\rho^i x_n$ . Since  $s_j(A_i) = s(A_i)$  for all  $i, j$ , an application of  $s_0, s_1, s_2$  to (1) will yield, respectively,

$$(2) \quad 0 = s(A_0) - s(A_1)x_n + s(A_2)x_n^2,$$

$$(3) \quad 0 = s(A_0) - s(A_1)x_n\rho + s(A_2)x_n^2\rho^2,$$

$$(4) \quad 0 = s(A_0) - s(A_1)x_n\rho^2 + s(A_2)x_n^2\rho.$$

Adding (2)–(4) gives  $3s(A_0) = 0$  and because  $3 \neq 0$  in the integral domain  $G(X)$ ,  $s(A_0) = 0$ . Taking linear combinations of (2), (3), (4) whose coefficients are suitable powers of  $\rho$  we similarly obtain  $s(A_1) = s(A_2) = 0$ . Each  $A_i$  can now be written as

$$(5) \quad A_i(x_n) = B_{i0} + B_{i1} \cdot x_n + B_{i2} \cdot x_n^2 + B_{i3} \cdot x_n^3,$$

where the coefficients  $B_{ij}$  do not depend on  $x_n$  and satisfy (a)–(c). Apply  $s$  to (5) to get the following equality in  $G(X)$ :

$$(6) \quad 0 = s(B_{i0}) + s(B_{i1}) \cdot x_n + s(B_{i2}) \cdot x_n^2 + s(B_{i3}) \cdot x_n^3.$$

Since  $s(B_{ij})$  are independent of  $x_n$  we conclude that all of them must vanish. By the induction hypothesis,  $B_{ij} = 0$  for all  $i, j$  so that  $p_0 = 0$  as desired. The uniqueness follows immediately.

*Notation.* The previous lemma implies that  $\varphi_X$  is one-to-one on the set of all polynomials  $p_0$  for which (a)–(c) hold. Hence there is no danger of confusion in writing  $p_0$  instead of  $\varphi_X(p_0)$ . Similar comment applies to the set of all  $5z$  with  $z \in X \cup \bar{X}$ .

LEMMA 2. *There is a functor  $\mathbf{H}: \mathbf{Set} \rightarrow \mathbf{Set}$  that carries  $\mathbf{F}$ .*

PROOF. Denote  $X_\alpha = \{x^2 \cdot \overline{\alpha(x)}: x \in X\}$ ,  $X_\beta = \{x \cdot \overline{\beta(x)}: x \in X\}$  and recall that the underlying set of  $\mathbf{F}(X; \alpha, \beta)$  is the subring of  $D(X)$  generated by  $X_\alpha \cup X_\beta \cup \{1\} \cup J(X)$ . Observe that the product of any pair of elements of  $X_\alpha \cup X_\beta$  lies in the ideal  $J(X)$  so that every element  $w \in \mathbf{F}(X; \alpha, \beta)$  has a representation

$$w = c + \sum c_i y_i + j,$$

where  $y_i \in X_\alpha \cup X_\beta$ ,  $j \in J(X)$ ,  $c, c_i \in Z_s$ , and only finitely many coefficients  $c_i$  do not vanish; Lemma 1 implies the uniqueness of this representation. Therefore the underlying set of  $\mathbf{F}(X; \alpha, \beta)$  equals the underlying set of the direct sum  $W_s(X_\alpha \cup X_\beta \cup \{1\}) \oplus J(X)$  of the group freely generated in the class  $5z = 0$  by the disjoint union of  $X_\alpha$ ,  $X_\beta$ , and  $\{1\}$  with the additive group of  $J(X)$ . Furthermore, both  $X_\alpha$  and  $X_\beta$  are naturally bijective to  $X$  through the mappings  $x \mapsto x^2 \cdot \overline{\alpha(x)}$ ,  $x \mapsto x \cdot \overline{\beta(x)}$ , respectively. The underlying set of  $\mathbf{F}(X; \alpha, \beta)$  is thus naturally isomorphic to the underlying set  $\mathbf{H}(X)$  of the group  $W(X) = W_s(X \times \{\alpha, \beta\} \cup \{1\}) \oplus J(X)$  and hence it may be identified with  $\mathbf{H}(X)$ . If  $f: X \rightarrow X'$  is an arbitrary mapping, define  $\mathbf{H}(f)$  as the underlying mapping of the group homomorphism

$$(7) \quad W(f) = W_s(f) \oplus D_1(f),$$

where  $D_1(f)$  is the restriction of  $D(f)$  to  $J(X)$  and  $W_s(f)$  is the unique extension of the mapping that sends 1 to 1,  $(x, \alpha)$  to  $(f(x), \alpha)$ , and  $(x, \beta)$  to  $(f(x), \beta)$ . Since  $D(f)$  maps  $J(X)$  into  $J(X')$ ,  $\mathbf{H}(f)$  is well defined and it is also easy to see that the functor  $\mathbf{H}$  thus defined is faithful: each  $\mathbf{H}(X)$  contains a copy of  $X$  ( $X \times \{\alpha\}$ , for instance) on which the mapping  $\mathbf{H}(f)$  behaves exactly like the original  $f$ .

If  $f: (X; \alpha, \beta) \rightarrow (X'; \alpha', \beta')$  is a morphism in  $2\mathbf{A}$ , then  $\mathbf{F}(f)(j) = D(f)(j) = W(f)(j)$  for all  $j \in J(X)$  and  $\mathbf{F}(f)(1) = 1 = W(f)(1)$ . Since  $\mathbf{F}(f)$  is a restriction  $D(f)$ , we get

$$\begin{aligned} \mathbf{F}(f)(x, \alpha) &= \mathbf{F}(f)(x^2 \cdot \overline{\alpha(x)}) = (\mathbf{F}(f)(x))^2 \cdot \mathbf{F}(f)(\overline{\alpha(x)}) \\ &= f(x)^2 \cdot \overline{f(\alpha(x))} = f(x)^2 \cdot \overline{\alpha'(f(x))} \end{aligned}$$

where the last equality holds because  $f$  is a morphism in  $2\mathbf{A}$ . Simultaneously,

$$W(f)(x, \alpha) = (f(x), \alpha) = f(x)^2 \cdot \overline{\alpha'(f(x))};$$

analogously one shows that  $\mathbf{F}(f)(x, \beta) = W(f)(x, \beta)$ . It is easy to see that  $\mathbf{F}(f)$  is also a homomorphism of  $W(X)$  into  $W(X')$ ; since it coincides with  $W(f)$  on the set of generators of  $W(X)$ ,  $\mathbf{F}(f) = W(f)$ , and this means that  $\mathbf{H}(f)$  is the underlying mapping of  $\mathbf{F}(f)$ .

The lemma below will be used in the proof of fulness of  $\mathbf{F}$ .

LEMMA 3. *Let  $u, v \in X \cup \bar{X}$ . Then  $u^2v \in \mathbf{F}(X; \alpha, \beta)$  if and only if  $u \in X$*

and  $v = \overline{\alpha(x)}$ . Similarly, if  $r, s \in X$ , then  $r\bar{s} \in F(X; \alpha, \beta)$  if and only if  $s = \beta(r)$ .

PROOF. Immediate from Lemma 1.

Another property of  $D(X)$  needed for the proof of fulness of  $F$  is described by the following theorem which is a corollary of the main result of §3.

**THEOREM 7.** *Let  $a, b \in D(X)$ . Then  $a^3 + b^3 = 5^4$  if and only if  $\{a, b\} = \{5x, 5\bar{x}\}$  for some  $x \in X$ .*

The remainder of this section will be devoted to the proof of fulness of  $F$  based on Lemma 3 and Theorem 7; we will also modify  $F$  to obtain a functor that is one-to-one also on objects. The second task is simple: once we have a full faithful functor  $F: 2A \rightarrow I_0$ , we define  $F^*(A) = F(A) \times \{A\}$ . Then  $F^*$  is naturally equivalent to  $F$  and it is obviously one-to-one on the class of objects of  $2A$ . There is no reason to use a different notation and we may just as well assume that  $F$  defined above is an embedding.

To show that  $F$  is a full functor, let  $h: F(X; \alpha, \beta) \rightarrow F(X'; \alpha', \beta')$  be a 1-preserving homomorphism of the two rings and let  $x \in X$ . Then  $(5x)^3 + (5\bar{x})^3 = 5^4$  and since this equality must be preserved by  $h$ , we conclude from Theorem 7 that there is a uniquely determined  $y \in X'$  such that  $\{h(5x), h(5\bar{x})\} = \{5y, 5\bar{y}\}$ . Thus there is a well-defined mapping  $f: X \rightarrow X'$  characterized by  $\{h(5x), h(5\bar{x})\} = \{5f(x), 5\bar{f}(x)\}$ .

$$5^3 h(x^2 \cdot \overline{\alpha(x)}) = h(5x)^2 \cdot h(5\overline{\alpha(x)}) = (5u)^2 \cdot 5v,$$

where  $u \in \{f(x), \overline{f(x)}\}$  and  $v \in \{f(\alpha(x)), \overline{f(\alpha(x))}\}$ . Hence

$$u^2 v = h(x^2 \cdot \overline{\alpha(x)}) \in F(X'; \alpha', \beta')$$

and, by Lemma 3, this happens only if  $u \in X'$  and  $v = \overline{\alpha'(u)}$ . Therefore  $u = f(x)$  and  $\alpha'(f(x)) = \overline{\alpha'(u)} = v = \overline{f(\alpha(x))}$ ; this implies that  $h(5x) = 5f(x)$  for every  $x \in X$  (and, consequently—using Theorem 7 again— $h(5\bar{x}) = 5\bar{f}(x)$  for all  $x \in X$ ), and that  $f(\alpha(x)) = \alpha'(f(x))$  for every  $x \in X$ . An analogous use of the second part of Lemma 3 allows us to conclude that  $f$  is a morphism in  $2A$ . It is clear that  $h$  is a restriction of  $D(f)$  to  $F(X; \alpha, \beta)$ —therefore  $h = F(f)$  as required.

REMARK. It is obvious that the only homomorphism

$$F(A) \rightarrow F(A')$$

that does not preserve 1 is the zero homomorphism. One may wish to ask whether the presence of units is essential here; it can be easily seen that this is not the case. We can modify our construction in the following way: define  $F_0(X; \alpha, \beta)$  as the subring of  $D(X)$  generated by  $X_\alpha \cup X_\beta \cup J(X)$  only. Lemma 3 and Theorem 7 will apply in the present case as well and the set-functor  $H_0$  obtained as the restriction of  $H$  to the underlying set of



$$W_5(X \times \{\alpha, \beta\}) \oplus J(X)$$

will carry  $F_0$ . Each  $F_0(f)$  is therefore just a restriction of  $F(f)$  to  $F_0(X; \alpha, \beta)$ —which has no units. A simple argument shows that every nonzero homomorphism is in the image of  $2A$  under  $F_0$ : since  $5^2 = 5 + 5 + 5 + 5 + 5$  in each  $F_0(X; \alpha, \beta)$ , every homomorphism  $h$  satisfies  $h(5)^2 = 5h(5)$ , i.e.,  $0 = h(5)(h(5) - 5)$ . Either  $h(5) = 5$  and  $h = F_0(f)$  for some homomorphism  $f$  of unary algebras, or  $h(5) = 0$ . In the latter case  $5h(w) = h(5w) = 0$  for all  $w$ ; thus  $h$  is the zero homomorphism. We can formulate our findings as follows.

**THEOREM 8.** *The class  $I^*$  ( $J_0^*$ , respectively) of all nonzero morphisms from  $I$  ( $J_0$ , resp.) contains a full subcategory which is strongly universal.*

It is clear that Theorems 2–6 can now be appropriately reformulated for  $I^*$  and  $J_0^*$ . We leave this to the reader, pointing out only one of the consequences: every monoid  $M$  appears as the monoid of all nonzero endomorphisms of an integral domain of characteristic zero with (or without) units. This includes the claim that the nonzero homomorphisms cannot compose into a zero homomorphism for any of these rings.

### 3. Proof of Theorem 7.

**LEMMA 4.** *The equation  $a^3 + b^3 = 5^4$  has no solution in the ring  $Z$  of integers.*

**PROOF.** If  $5^4 = (a + b)(a^2 - ab + b^2)$  for some  $a, b \in Z$ , then  $0 \neq a \neq b \neq 0$ ; without loss of generality we may assume  $a > b$ . Since  $a^2 - ab + b^2 > 0$  for all nonzero values of  $a$  and  $b$ ,  $a + b = 5^k$  and  $a^2 - ab + b^2 = 5^{4-k}$  for some  $k \in \{0, \dots, 4\}$ . Furthermore,

$$5^k = a + b \leq a(a - b) + b \leq a(a - b) + b^2 = 5^{4-k}$$

and this implies  $k \leq 2$ . If  $k = 2$ , then  $a = b + 1$  and  $b^2 = b$ , that is,  $b = 1$  and  $a = 2$ —a contradiction. Substituting  $b = 5^k - a$  into  $a^2 - ab + b^2 = 5^{4-k}$  one finds easily that the discriminant of the resulting quadratic equation is not a square of an integer if  $k = 0$  or  $k = 1$ .

Theorem 7 is a consequence of Theorem 9 below.

**THEOREM 9.** *Let  $R$  be an integral domain of characteristic zero and let  $a \neq 0$  be an arbitrary element of  $R$ . Set  $R^* = R[x, y]/J$  where  $J$  is the ideal generated by  $x^3 + y^3 - a$ . Then  $\xi^3 + \eta^3 = a^4$  in  $R^*$  if and only if either both  $\xi$  and  $\eta$  are in  $R$  or  $\{\xi, \eta\} = \{arx, asy\}$  for some third roots  $r, s$  of 1.*

**REMARK.** It is easy to prove Theorem 7 from Theorem 9: every solution pair of the cubic equation in question belongs to some subring  $B_n$  of  $D(X)$  generated by finitely many variables  $x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n$ . If  $a = 5$  and  $R$  is taken to be  $B_n$ , then  $R^* = B_{n+1}$ . Since the only third root of 1 in  $D(X)$  is

the element 1 itself, a simple induction yields Theorem 7 immediately once Lemma 4 is taken into account.

Note that  $R^*$  is a cubic extension of the polynomial ring  $R[x]$ ; the difficulties involved in handling cubic extensions are the main reason why, instead of showing Theorem 9 directly, we will extend  $R^*$  to a ring  $E$  that will be only a quadratic extension of the relatively uncomplicated ring  $R[t, t^{-1}]$  with  $t$  which is transcendental over  $R$ .

DEFINITIONS AND NOTATION. Since every integral domain of characteristic zero can be extended to an integral domain  $R$  containing the field  $C$  of complex numbers it is enough to prove Theorem 9 for these  $R$  only. From now on we will assume that  $C \subseteq R$  and make no further references to this assumption.

Let  $R, R^*$  be as in Theorem 9 and let  $C \subseteq R$ . Denote  $x + y = t, t^4 - 4at = \Delta$  and observe that

$$\begin{aligned}\Delta &= t(t^3 - 4a) = (x + y)((x + y)^3 - a - 3(x + y)(x^2 - xy + y^2)) \\ &= -3(x + y)^2(x - y)^2.\end{aligned}$$

Choose  $a = (-3)^{-1/2}$  and denote

$$\Gamma = \Delta^{1/2} = (-3)^{1/2}(x + y)(x - y).$$

The ring  $E = R[t, t^{-1}][\Gamma]$  contains  $R^*$  since both  $x$  and  $y$  are in  $E$ . If  $t$  was algebraic over  $R$ , then the algebraic extension  $E$  of  $R[t, t^{-1}]$  would be also algebraic over  $R$ ; this would imply that both  $x$  and  $y$  are algebraic over  $R$ —a contradiction. Hence  $t$  is transcendental over  $R$  and every element  $w$  of  $R[t, t^{-1}]$  can be uniquely written in the form

$$w = \sum r_i t^i$$

where all  $i$  are integers and only finitely many coefficients  $r_i \in R$  are different from zero. Let  $d(w)$  denote the degree of a nonzero  $w \in R[t, t^{-1}]$  and let  $c(w)$  stand for its codegree (i.e.,  $c(w)$  is the least  $i$  with  $r_i \neq 0$ ). Since  $t$  is transcendental  $R[t, t^{-1}]$  is an integral domain and  $c(w) \leq d(w)$  for all nonzero  $w$  in  $R[t, t^{-1}]$ ;  $c(w) = d(w)$  if and only if  $w$  is a monomial. Note also that  $c(w_1 \cdot w_2) = c(w_1) + c(w_2)$  and  $d(w_1 \cdot w_2) = d(w_1) + d(w_2)$  for all nonzero  $w_1, w_2$  in  $R[t, t^{-1}]$ .

$E$  is a proper extension of  $R[t, t^{-1}]$ —for if  $\Gamma \in R[t, t^{-1}]$ , then  $t^4 - 4at$  would be a square of a nonzero element  $w$  of  $R[t, t^{-1}]$  and  $2c(w) = c(w^2) = c(t^4 - 4at) = 1$ —a contradiction. Therefore every  $e \in E$  has the form  $e = A + B\Gamma$ , where  $A, B \in R[t, t^{-1}]$  are uniquely determined by  $e$ .  $e \in R[t, t^{-1}]$  if and only if  $B = 0$ .

For every  $e = A + B\Gamma$  let  $e^* = A - B\Gamma$  denote its conjugate and let  $N(e) = e \cdot e^*$  be called the *norm* of  $e$ .  $N(e) = A^2 - B^2\Delta \in R[t, t^{-1}]$ ; if  $e_1 \cdot e_2 = 0$  then  $0 = N(e_1 \cdot e_2) = N(e_1) \cdot N(e_2)$  and at least one of the factors

in the last equation must vanish. If  $A_i^2 - B_i^2\Delta = 0$ , then the codegrees of the two additive terms are  $2c(A_i)$  and  $2c(B_i) + 1$ ; thus  $B_i = 0$  and, consequently,  $A_i = 0$ . We conclude that  $E$  is an integral domain.

Let  $0 \neq a \in R$  and let  $f, g \in E$  be such that  $f^3 + g^3 = a^4$ ; denote  $X_i = f + g\rho^i$  for  $i = 0, 1, 2$  and a  $\rho$  satisfying  $\rho^2 + \rho + 1 = 0$ . Hence  $X_i$  belong all to  $E$  and

$$(8) \quad X_0 \cdot X_1 \cdot X_2 = a^4,$$

$$(9) \quad X_0 + \rho X_1 + \rho^2 X_2 = 0.$$

To prove Theorem 9 we have to find all the joint solutions of (8) and (9) in  $E$ . We will deal with equation (8) first.

The automorphism of  $E$  determined by  $\Gamma \rightarrow -\Gamma$  leaves  $R[t, t^{-1}]$  fixed elementwise and transforms (8) into

$$(10) \quad X_0^* \cdot X_1^* \cdot X_2^* = a^4.$$

Multiply (10) by (8) to obtain

$$(11) \quad N(X_0) \cdot N(X_1) \cdot N(X_2) = a^8,$$

and write  $X_i = A_i + B_i\Gamma$ . (11) now becomes

$$(12) \quad (A_0^2 - B_0^2\Delta)(A_1^2 - B_1^2\Delta)(A_2^2 - B_2^2\Delta) = a^8.$$

Thus the sum of the degrees of the three factors on the left-hand side of (12) must be zero and the same is true for the sum of their codegrees. Therefore

$$(13) \quad c(A_i^2 - B_i^2\Delta) = d(A_i^2 - B_i^2\Delta), \quad i = 0, 1, 2,$$

in other words, each  $A_i^2 - B_i^2\Delta$  is a monomial.

There are, however, infinitely many elements of  $E$  whose norm is a monomial in  $R[t, t^{-1}]$ . If  $e$  is a monomial itself, then  $N(e) = e^2$  is a monomial again. Similarly, if  $G_1 = t^2$ ,  $H_1 = 1$ , then

$$N(G_1 \pm H_1\Gamma) = t^4 - (t^4 - 4at) = 4at.$$

Since a product of monomials is a monomial again, every element of  $E$  that has the form

$$(14) \quad st^k(G_1 \pm H_1\Gamma)^n, \quad \text{where } s \neq 0, n \geq 0, k \in \mathbb{Z},$$

will satisfy (13).

Next we will show that all elements of  $E$  that satisfy (13) are of the form (14). The proof depends on the three lemmas below.

Note first that  $N(A + B\Gamma) = rt^k$  for  $0 \neq r \in R$  implies  $A \neq 0$ : if  $A = 0$ , then  $B^2\Delta = rt^k$ —but  $B^2\Delta$  is not a monomial.

LEMMA 5. Let  $0 \neq r \in R$  and let  $A, B \in R[t, t^{-1}]$ ,  $B \neq 0$  be such that

$$(15) \quad A^2 - B^2\Delta = rt^k$$

for some  $k \in \mathbb{Z}$ . If  $c = \min(c(A), c(B))$ , then  $At^{-c} = P$ ,  $Bt^{-c} = Q$  are

elements of  $R[t]$  such that  $\min(c(P), c(Q)) = 0$  and

$$(16) \quad P^2 - Q^2\Delta = rt^e, \quad e \in \{0, 1\}.$$

PROOF. Clearly  $c(P) = c(A) - c > 0$  and  $c(Q) > 0$ ;  $\min(c(P), c(Q)) = 0$  and  $P, Q$  are polynomials of  $t$  only. Substitute  $A = Pt^c, B = Qt^c$  into (15) to see that  $P^2 - Q^2\Delta = rt^e$ . If  $c(P) = 0$ , then  $e = 0$  since  $c(Q^2\Delta) > 1$ ; if  $c(P) > 0$ , then  $c(Q) = \min(c(P), c(Q)) = 0$  so that  $c(Q^2\Delta) = 1 < 2 < c(P^2)$  which means that  $e = c(P^2 - Q^2\Delta) = 1$ .

Let  $\lambda(A)$  denote the leading coefficient of a nonzero  $A$  in  $R[t, t^{-1}]$ , that is, the coefficient of the highest degree monomial term of  $A$ .

LEMMA 6. If  $A, B$  are as in Lemma 5, then  $d(A) = d(B) + 2$  and  $\lambda(A) = \pm\lambda(B)$ .

PROOF. Let  $A = Pt^c, B = Qt^c$  as in Lemma 5. The degrees of the three additive terms of (16) are, respectively,  $2d(P), 2d(Q) + 4$ , and  $e$ . For (16) to hold it is therefore necessary to have  $2d(P) = 2d(Q) + 4$  and  $\lambda(P^2) = \lambda(Q^2\Delta)$ . As  $\lambda(\Delta) = 1$  the second equality gives  $\lambda(P) = \pm\lambda(Q)$ .  $d(A) = c + d(P) = c + d(Q) + 2 = d(B) + 2$  and  $\lambda(A) = \lambda(P) = \pm\lambda(Q) = \pm\lambda(B)$  as was to be shown.

LEMMA 7. Let  $P, Q$  be polynomials satisfying (16), let  $Q \neq 0$  and  $\lambda(P) = \delta\lambda(Q)$  for a  $\delta \in \{-1, +1\}$ . Then

- (a) if  $d(Q) = 0$ , then  $P + Q\Gamma = q(G_1 + \delta H_1\Gamma)$  for some  $q$  in  $R$ ,
- (b) if  $d(Q) > 0$ , then the norm of  $(P_1 + Q_1\Gamma) = (P + Q\Gamma) \cdot (G_1 - \delta H_1\Gamma)$  is a monomial,  $Q_1 \neq 0$  and  $P_1$  are polynomials of  $t$ , and  $d(Q_1) = d(Q) - 1$ .

PROOF. Recall that  $G_1 = t^2, H_1 = 1$  so that  $P_1 = t^2P - \Delta Q\delta$  and  $Q_1 = t^2Q - \delta P$  are polynomials again. Note that

$$\begin{aligned} rt^e &= P^2 - Q^2\Delta = P^2 - (t^4 - 4at)Q^2 \\ &= (\delta P - Qt^2) \cdot (\delta P + Qt^2) + 4atQ^2, \end{aligned}$$

that is,

$$(17) \quad rt^e = -Q_1(\delta P + Qt^2) + 4atQ^2.$$

Since  $Q \neq 0$ , Lemma 6 gives  $d(P) = d(Q) + 2$ . Moreover,  $\lambda(Q) = \lambda(Qt^2)$  and since  $\lambda(P) = \delta\lambda(Q)$  is assumed we conclude that  $d(\delta P + Qt^2) = d(Q) + 2$ .

Let us consider the case of  $d(Q) = 0$  first. If  $Q_1 \neq 0$ , then

$$d(-Q_1(\delta P + Qt^2)) = d(Q_1) + d(Q) + 2 > 2$$

while  $d(rt^e) = e < 1$  and  $d(4atQ^2) = 1$ , which contradicts (17). Hence  $Q_1 = 0$ , that is,  $P = \delta Qt^2$ . Since  $\delta Q = q \in R$  we see that

$$P + Q\Gamma = q(G_1 + \delta H_1\Gamma).$$

This proves (a).

If  $d(Q) > 0$ , then  $d(4atQ^2) = 2d(Q) + 1 > 1 \geq e$ ; hence  $Q_1 \neq 0$  and  $2d(Q) + 1 = d(Q_1) + d(Q) + 2$  because of (17). The last equality shows that  $d(Q_1) = d(Q) - 1$ .

LEMMA 8. *Let  $A, B \in R[t, t^{-1}]$ . Then  $N(A + B\Gamma)$  is a nonzero monomial if and only if there is a monomial  $T$ ,  $\delta \in \{-1, +1\}$ , and  $n \geq 0$  such that  $A + B\Gamma = T(G_1 + \delta H_1\Gamma)^n$ .*

PROOF. We have already shown that all the elements of the form (14) have a monomial norm. Using the three lemmas above we will show the converse.

If  $B = 0$ , then  $N(A + B\Gamma) = A^2$  is a monomial only if  $A$  is a monomial itself.

If  $B \neq 0$ , let  $P$  and  $Q \neq 0$  be polynomials obtained as in Lemma 5. If  $d(Q) = 0$ , then Lemma 7 yields  $P + Q\Gamma = q(G_1 + \delta H_1\Gamma)$  and we see that  $A + B\Gamma$  has the required form. Finally, let  $d(Q) > 0$ ,  $\lambda(P) = \delta\lambda(Q)$ . Part (b) of Lemma 7 can now be applied to provide polynomials  $P_1, Q_1 \neq 0$  such that  $P + Q\Gamma = M_1(G_1 + \delta H_1\Gamma)(P_1 + Q_1\Gamma)$  for some monomial  $M_1$ . Now we use Lemma 5 to obtain polynomials  $P_2, Q_2 \neq 0$  such that  $N(P_2 + Q_2\Gamma)$  is a monomial of degree 0 or 1 and  $(P_2 + Q_2\Gamma)M_2 = P_1 + Q_1\Gamma$  for a monomial  $M_2$  of a nonnegative degree. Note that  $d(Q_2) \leq d(Q_1) < d(Q)$ ; we are able to apply Lemmas 6 and 7 again, this time to  $P_2 + Q_2\Gamma$ . After finitely many steps we arrive at a first  $k$  such that  $Q_{2k} \neq 0$  has degree zero. Applying Lemma 6 and the first clause of Lemma 7 once more we can conclude from the induction outlined above that  $P + Q\Gamma = M'(G_1 + H_1\Gamma)^l \cdot (G_1 - H_1\Gamma)^m$  for some monomial  $M'$  and nonnegative integers  $l, m$ . Thus  $P + Q\Gamma = M(G_1 + \delta H_1\Gamma)^n$ , where  $M$  is a monomial,  $n = |l - m|$  and  $l - m = \delta n$ . Since  $A + B\Gamma$  is a product of a monomial and  $P + Q\Gamma$  this finishes the proof.

NOTATION. If  $k \geq 0$ , define  $G_k + H_k\Gamma = (G_1 + H_1\Gamma)^k$ .

LEMMA 9.  $d(G_k) = 2k$ ,  $d(H_k) = 2k - 2$ , and  $\lambda(G_k) = 2^{k-1} = \lambda(H_k)$  for every  $k \geq 1$ . Consequently,  $(G_1 + H_1\Gamma)^k$  belongs to  $R[t, t^{-1}]$  if and only if  $k = 0$ .

PROOF. The lemma will be proved by induction on  $k$ . It is clearly true for  $k = 1$ . Since  $G_{k+1} + H_{k+1}\Gamma = (G_k + H_k\Gamma) \cdot (G_1 + H_1\Gamma)$ ,  $G_{k+1}$  and  $H_{k+1}$  are given by equations

$$G_{k+1} = t^2G_k + \Delta H_k, \quad H_{k+1} = t^2H_k + G_k.$$

As

$$d(G_k) = 2 + d(H_k) = d(t^2H_k) \quad \text{and} \quad \lambda(G_k) = \lambda(H_k) = \lambda(t^2H_k),$$

the second equation gives

$$d(H_{k+1}) = d(G_k) = 2k, \quad \lambda(H_{k+1}) = 2\lambda(G_k) = 2^k.$$

Consider the first equation now and note that

$$d(t^2 G_k) = 2k + 2 = d(\Delta H_k).$$

Since  $\lambda(\Delta) = 1$  we also have

$$\lambda(t^2 G_k) = \lambda(G_k) = \lambda(H_k) = \lambda(\Delta H_k)$$

and, consequently,

$$d(G_{k+1}) = 2k + 2 \quad \text{and} \quad \lambda(G_{k+1}) = 2\lambda(G_k) = 2^k.$$

This finishes the proof.

To conclude the proof of Theorem 9 we have to find all joint solutions of (8) and (9). Lemma 8 says that each  $X_i$  must have the form

$$(18) \quad X_i = T_i(G_1 + \delta_i H_1 \Gamma)^{m_i}, \quad i = 0, 1, 2,$$

for some monomial  $T_i$ ,  $\delta_i \in \{-1, +1\}$ , and  $m_i \geq 0$ . Since the product

$$(19) \quad \prod_{i=0}^2 (G_1 + \delta_i H_1 \Gamma)^{m_i}$$

must be a monomial—see (8), Lemma 9 implies that

$$(20) \quad \delta_0 m_0 + \delta_1 m_1 + \delta_2 m_2 = 0,$$

and we may assume that  $0 \leq m_0 \leq m_1 \leq m_2$ .  $\delta_0 = +1$  may also be assumed (if  $\delta_0 = -1$  we may solve (8) and (9) for the conjugates  $X_i^*$  instead).

If  $\delta_0 = 1$  and  $\delta_1 = -1$ , then (20) implies  $\delta_2 = 1$  and  $m_2 \leq m_0 + m_2 = m_1 \leq m_2$ . Thus  $m_0 = 0$ ,  $m_1 = m_2$ . If  $\delta_1 = 1$ , then  $\delta_2 = -1$  and in either case we can set  $m_0 = m$ ,  $m_1 = m + k$ ,  $m_2 = 2m + k$  for some nonnegative integers  $m, k$ . The equations (8) and (9) now become, respectively,

$$(21) \quad \begin{aligned} &T_0 T_1 T_2 (4at)^{2m+k} = a^4, \\ &0 = T_0(G_m + H_m \Gamma) + \rho T_1(G_{m+k} + H_{m+k} \Gamma) \end{aligned}$$

$$(22) \quad + \rho^2 T_2(G_{2m+k} - H_{2m+k} \Gamma).$$

Multiplying (22) by  $(G_m - H_m \Gamma)$  and by a suitable power of  $t$  will yield

$$(23) \quad 0 \neq r = M_1(G_k + H_k \Gamma) + M_2(G_{3m+k} - H_{3m+k} \Gamma),$$

where  $r \in R$  and  $M_1, M_2$  are monomials.

Let  $k = 0$  first. Then  $H_k = 0$  and (23) implies that  $H_{3m} = 0$  as well, that is,  $m = 0$ . As  $t$  is transcendental over  $R$  we conclude from (22) that  $d(T_0) = d(T_1) = d(T_2)$ ; (21) yields  $d(T_0) + d(T_1) + d(T_2) = 0$ . Hence  $d(T_i) = 0$  for  $i = 0, 1, 2$  and this means that all  $X_i$  belong to  $R$ . Since  $3f = X_0 + X_1 + X_2$ ,  $f$  and  $g$  are in  $R$  as well. This proves the first clause of Theorem 9.

From now on we will assume  $k > 0$ .

Lemma 9 implies that  $H_k \neq 0 \neq H_{3m+k}$  in this case; (23) gives  $M_1 H_k =$

$M_2H_{3m+k}$  and this, in turn, implies

$$d(M_1) + d(H_k) = d(M_2) + d(H_{3m+k}),$$

$$\lambda(M_1) \cdot \lambda(H_k) = \lambda(M_2) \cdot \lambda(H_{3m+k}).$$

From here and from Lemma 9 we have

$$\begin{aligned} d(M_1G_k) &= d(M_1) + d(H_k) + 2 \\ &= d(M_2) + d(H_{3m+k}) + 2 = d(M_2G_{3m+k}), \\ \lambda(M_1G_k) &= \lambda(M_1) \cdot \lambda(G_k) = \lambda(M_1) \cdot \lambda(H_k) \\ &= \lambda(M_2) \cdot \lambda(H_{3m+k}) = \lambda(M_2G_{3m+k}). \end{aligned}$$

Therefore

$$d(M_1G_k + M_2G_{3m+k}) = d(M_1G_k) = d(M_2G_{3m+k})$$

and (23) can hold only if  $d(M_1G_k) = 0$ . Rewrite (23) as

$$(r - M_1G_k) - M_1H_k\Gamma = M_2(G_{3m+k} - H_{3m+k}\Gamma)$$

and compare the norms of the two sides:

$$(24) \quad r(r - 2M_1G_k) + M_1^2(4at)^k = M_2^2(4at)^{3m+k}.$$

The three additive terms of (24) are monomials;  $d(r(r - 2M_1G_k)) = 0$  if it exists—because  $d(M_1G_k) = 0$ . Since  $d(G_k) = 2k$  we also have  $d(M_1^2(4at)^k) = -3k$  and  $d(M_2^2(4at)^{3m+k}) = -9m - 3k$ . As  $k > 0$ , (24) can be valid only if  $r = 2M_1G_k$  and  $m = 0$ .  $G_k$  is, therefore, a monomial and Lemma 9 gives  $G_k = 2^{k-1}t^{2k}$ .

Next we will show that  $k = 1$ . Note that

$$(4at)^k = N(G_k + H_k\Gamma) = 4^{k-1}t^{4k} - (t^4 - 4at)H_k^2$$

implies the equation

$$(25) \quad 4^{k-1}t^k(t^{3k} - 4a^k) = (t^3 - 4a)tH_k^2,$$

which says, in particular, that the left-hand side is a multiple of  $t^3 - 4a$ . On the other hand, however,  $4^{k-1}t^k(t^{3k} - (4a)^k)$  is a multiple of  $t^3 - 4a$  as well, so that the difference of the two polynomials is a multiple of  $t^3 - 4a$  again. The difference is equal to the monomial  $4^{k-1}t^ka^k(4^k - 4)$ . Since  $a \neq 0$  we conclude that  $4^k = 4$ ; this is possible only if  $k = 1$  as the characteristic of  $R$  is zero.

Therefore the only possible solutions of (8) and (9) in the case  $k > 0$  are triples  $T_0, T_1(t^2 - \Gamma), T_2(t^2 + \Gamma)$ , where  $T_0, T_1, T_2$  are monomials. If a suitable third root  $\rho$  of 1 is chosen, we may specify  $X_0 = T_0, X_1 = T_1(t^2 - \Gamma), X_2 = T_2(t^2 + \Gamma)$  and write (9) as the following pair of equations:

$$(26) \quad -\rho T_1 + \rho^2 T_2 = 0,$$

$$(27) \quad T_0 + \rho T_1 t^2 + \rho^2 T_2 t^2 = 0.$$

(26) yields  $T_1 = \rho T_2$  and from (27) we will then obtain  $T_0 = -2\rho^2 t^2 T_2$ .

Substitute for  $X_i$  into (8) to get  $a^4 = -a(2tT_2)^3$ , that is,

$$(2T_2t + a)(2T_2t + a\rho)(2T_2t + a\rho^2) = 0.$$

Thus  $T_2 = -\frac{1}{2}\rho^{c+1}at^{-1}$  for some integer  $c$ ,  $T_1 = -\frac{1}{2}\rho^{c+2}at^{-1}$ , and  $T_0 = \rho^cat$ .

As  $(\rho^{-b} - \rho^b)^2 = -3$  for any integer  $b \notin 3\mathbb{Z}$ ,

$$\Gamma = (\rho^{-b} - \rho^b)(x + y)(x - y)$$

for a suitable choice of  $b$ . Note also that  $(\rho^2 - \rho)(\rho^{-b} - \rho^b) = (-1)^b 3$  and recall that  $t = x + y$ . Consequently,

$$\begin{aligned} 3f &= X_0 + X_1 + X_2 = T_0 + T_1(t^2 - \Gamma) + T_2(t^2 + \Gamma) \\ &= \rho^cat\left(t - \frac{1}{2}t(\rho^2 + \rho)\right) + \frac{1}{2}\rho^cat^{-1}(\rho^2 - \rho)(\rho^{-b} - \rho^b)(x + y)(x - y) \\ &= 3\rho^ca\left(\frac{1}{2}(x + y) + \frac{1}{2}(-1)^b(x - y)\right), \end{aligned}$$

that is,  $f = \rho^cax$  or  $f = \rho^cay$  depending on whether  $b$  is even or odd.  $g = X_0 - f$  and this enables us to conclude that  $\{f, g\} = \{\rho^cax, \rho^cay\}$ . This finishes the proof of Theorem 9; the other solution pairs  $\{f, g\}$  are obtained by choosing the values of  $\rho$  and of  $(-3)^{1/2}$  in other combinations than those used in the above argument.

#### 4. Proofs of Theorems 2–5.

**PROOF OF THEOREM 2.** Theorem 2 was formulated and proved for the category **C** of commutative groupoids in [7]. There is a strong embedding  $\mathbf{G}: \mathbf{C} \rightarrow 2\mathbf{A}$  preserving cardinalities of infinite underlying sets and mapping finite groupoids to finite unary algebras in  $2\mathbf{A}$  ([6] or [10]). The strong embedding constructed in the present paper also preserves cardinalities of infinite algebras and assigns countable integral domains to finite algebras from  $2\mathbf{A}$ . The composite full embedding  $\mathbf{F} \circ \mathbf{G}: \mathbf{C} \rightarrow \mathbf{I}_0$  is strong and preserves the cardinalities of infinite sets. The proof of Theorem 2 is concluded by the following simple observation: a strong embedding that preserves infinite cardinalities must also translate everything Theorem 2 describes.

Theorems 3 and 4 can be proved as consequences of [3] and [4], respectively, using composites of some of the full embeddings included in [6] and in [10]. To minimize the number of needed references we prove a stronger result instead.

**THEOREM 10.** *For every monoid  $M$  there is an integral domain  $I$  of characteristic zero such that:*

- (i) *the monoid of all 1-preserving endomorphisms of  $I$  is isomorphic to  $M$ ;*
- (ii) *the category of all objects  $J$  of  $\mathbf{I}_0$  such that  $I \subseteq J$  is strongly binding;*
- (iii) *the category of all objects  $K$  of  $\mathbf{I}_0$  that have  $I$  as a quotient ring is strongly binding.*



This generalizes Theorems 3 and 4 in two ways: first, the object  $I$  can be chosen the same for both claims; secondly, the two categories claimed are not only universal but strongly universal as well.

To prove Theorem 10 for  $I_0$  we will first prove its version in a more suitable category of universal algebras and then use the strong universality of  $I_0$  together with the fact that "to be an onto homomorphism" and "to be a one-to-one homomorphism" are properties that are clearly preserved by any strong embedding from one category of algebras into another. The category we chose is  $4A$ —the category of all algebras  $(X; a_0, a_1, a_2, a_3)$  with four unary operations  $a_i$  and all their homomorphisms.

We proceed as follows.

Let  $A = (X; m_0, m_1)$  be an arbitrary nonempty algebra in  $2A$  whose endomorphism monoid is isomorphic to  $M$ . Define an expansion  $B$  of  $A$  in the category  $4A$  by

$$B = (X \cup \{0, 1\}; b_0, b_1, b_2, b_3),$$

where the union is disjoint and

$$b_0(x) = m_0(x), \quad b_1(x) = m_1(x), \quad b_2(x) = b_3(x) = 1$$

for all  $x \in X$ ;

$$b_0(i) = b_1(i) = b_3(i) = i, \quad b_2(i) = 1 - i$$

for  $i = 0, 1$ . It is easy to see that every endomorphism  $f$  of  $A$  extends to an endomorphism  $f^*$  of  $B$  such that  $f^*(i) = i$  for  $i = 0, 1$ . Conversely, note that  $b_2(w) = b_3(w)$  in  $B$  holds if and only if  $w \in X$  and hence every endomorphism  $g$  of  $B$  has to preserve  $X$ . Denote by  $f$  the restriction of  $g$  to  $X$ ; since  $b_0, b_1$  coincide with  $m_0, m_1$  on  $X$ ,  $f$  is an endomorphism of  $A$ . Furthermore,  $g(1) = g(b_2(x)) = b_2(g(x)) = b_2(f(x)) = 1$ , and  $g(0) = g(b_2(1)) = b_2(1) = 0$ . This shows that  $g = f^*$  and, consequently, the endomorphism monoid of  $B$  is also isomorphic to  $M$ .

Now we will construct strong embeddings  $G, H: 2A \rightarrow 4A$  such that  $G(C)$  will have  $B$  as a homomorphic image and  $B$  will be a subalgebra of  $H(C)$  for every  $C$  in  $2A$ .

Recall that the underlying set of  $A$  is  $X$  and choose an arbitrary rigid algebra  $(X; r_0, r_1)$  in  $2A$ . Such an algebra always exists—cf. [10].  $(X; r_0, r_1)$  will be used as an element of both constructions.

Let us define  $H$  first. For an arbitrary algebra  $C = (Z; \alpha_0, \alpha_1)$  in  $2A$  set

$$H(C) = (X \times \{0, 1\} \cup Z \cup \{0, 1\}; c_0, c_1, c_2, c_3)$$

where the union is again disjoint and the operations  $c_i$  are defined by

$$\begin{aligned} c_0(x, 0) &= (m_0(x), 0), & c_1(x, 0) &= (m_1(x), 0), \\ c_0(x, 1) &= (r_0(x), 1), & c_1(x, 1) &= (r_1(x), 1) \quad \text{for all } x \in X; \end{aligned}$$

$$\begin{aligned}
c_0(z) &= \alpha_0(z), c_1(z) = \alpha_1(z) \text{ for all } z \in Z; \\
c_0(i) &= c_1(i) = i \text{ for } i = 0, 1; \\
c_2(z) &= z \text{ for all } z \in Z; \\
c_2(x, 1) &= c_2(1) = 0, c_2(x, 0) = c_2(0) = 1 \text{ for all } x \in X; \\
c_3(z) &= 0 \text{ for } z \in Z; \\
c_3(x, 1) &= (x, 0), c_3(x, 0) = 1 \text{ for all } x \in X; \\
c_3(0) &= 0, c_3(1) = 1.
\end{aligned}$$

If  $f: (Z; \alpha_0, \alpha_1) \rightarrow (Z'; \alpha'_0, \alpha'_1)$  is a morphism in  $2A$ , define  $H(f)(z) = f(z)$  for  $z \in Z$  and  $H(f)(w) = w$  if  $w \in W = X \times \{0, 1\} \cup \{0, 1\}$ . It is clear that  $H$  is carried by a functor  $\text{Set} \rightarrow \text{Set}$ ; a routine computation shows that  $H(f)$  is a homomorphism in  $4A$ . To prove the fulness of  $H$ , observe that  $c_2(v) = v$  in  $H(Z; \alpha_0, \alpha_1)$  if and only if  $v \in Z$ . Therefore any homomorphism

$$g: H(Z; \alpha_0, \alpha_1) \rightarrow H(Z'; \alpha'_0, \alpha'_1)$$

maps  $Z$  into  $Z'$ ; let  $f$  denote the restriction of  $g$  to  $Z$ . Since  $c_0, c_1$  coincide with  $\alpha_0, \alpha_1$ , respectively, on  $Z$ ,  $f$  is a morphism in  $2A$ . Furthermore,  $g(0) = g(c_3(z)) = c'_3(g(z)) = c'_3(f(z)) = 0$  and, similarly,  $g(1) = 1$ .  $c_2(v) = c_3(v)$  if and only if  $v \in X \times \{0\}$  and thus  $g(x, 0) = (h(x), 0)$  for some  $h: X \rightarrow X$ .  $(h(x), 0) = g(c_3(x, 1)) = c'_3(g(x, 1))$  implies  $g(x, 1) = (h(x), 1)$ , hence

$$(r_i(h(x)), 1) = c'_i(g(x, 1)) = g(c_i(x, 1)) = g(r_i(x), 1) = (h(r_i(x)), 1)$$

for  $i = 0, 1$ . But the identity mapping  $id_X$  is the only endomorphism of  $(X; r_0, r_1)$  so that  $h(x) = x$  for  $x \in X$ . Thus  $g(x, i) = (x, i)$  and this concludes the proof of the equality  $g = H(f)$ . The functor  $H$  is a strong embedding.

The functor  $G: 2A \rightarrow 4A$  is defined as follows.

$$G(Z; \alpha_0, \alpha_1) = (X \times \{0, 1\} \cup Z \cup \{0, 1, 2, 3\}; a_0, a_1, a_2, a_3),$$

where the union is disjoint and

$$\begin{aligned}
a_0(x, 0) &= (m_0(x), 0), & a_1(x, 0) &= (m_1(x), 0), \\
a_0(x, 1) &= (r_0(x), 1), & a_1(x, 1) &= (r_1(x), 1) \text{ for all } x \in X;
\end{aligned}$$

$$\begin{aligned}
a_0(z) &= \alpha_0(z), a_1(z) = \alpha_1(z) \text{ for all } z \in Z; \\
a_0(i) &= a_1(i) = i \text{ for } i = 0, 1, 2, 3; \\
a_2(x, 0) &= (x, 1), a_2(x, 1) = 2 \text{ for all } x \in X; \\
a_2(z) &= a_2(2) = 3 \text{ for all } z \in Z; \\
a_2(0) &= 1, a_2(1) = a_2(3) = 0; \\
a_3(x, 0) &= a_3(x, 1) = 3 \text{ for all } x \in X; \\
a_3(z) &= a_3(0) = 2 \text{ for all } z \in Z; \\
a_3(1) &= a_3(3) = 1, a_3(2) = 0.
\end{aligned}$$

If  $f: (Z; \alpha_0, \alpha_1) \rightarrow (Z'; \alpha'_0, \alpha'_1)$  is a morphism in  $2A$ , set  $G(f)(z) = f(z)$  for  $z \in Z$ ,  $G(f)(v) = v$  for all  $v \in V = X \times \{0, 1\} \cup \{0, 1, 2, 3\}$ ; it is easy to verify that  $G(f)$  is a morphism in  $4A$  and that  $G$  is carried by a set-functor. Let  $g: G(Z; \alpha_0, \alpha_1) \rightarrow G(Z'; \alpha'_0, \alpha'_1)$  be a homomorphism of the two algebras.

Since 1 is the only element fixed by  $a_3$ , we have  $g(1) = 1$  and using  $a_2, a_3$  we get also  $g(0) = 0$ ,  $g(2) = 2$ ,  $g(3) = 3$ , in that order. Note that  $a_2(w) = 2$  exactly when  $w \in X \times \{1\}$ . The operations  $a_0, a_1$  coincide on  $X \times \{1\}$  with the operations of the rigid algebra  $(X; r_0, r_1)$  and hence  $g(x, 1) = (x, 1)$  for all  $x \in X$ .  $a'_2(g(x, 0)) = g(a_2(x, 0)) = g(x, 1) = (x, 1)$  implies  $g(x, 0) = (x, 0)$  for all  $x \in X$ .  $Z$  is the set of all elements  $u$  of  $G(Z; \alpha_0, \alpha_1)$  for which  $a_3(u) = 2$  and  $a_2(u) = 3$ ; therefore  $g$  maps  $Z$  into  $Z'$  and compatibility of  $g$  with  $a_0, a_1$  on  $Z$  implies that the restriction  $f$  of  $g$  to  $Z$  is a morphism in 2A. Thus  $G$  is a strong embedding.

It is straightforward to verify that the mapping  $k_C: G(C) \rightarrow B$  defined by  $k_C(z) = k_C(0) = k_C(2) = 0$  for all  $z \in Z$ ,  $k_C(x, 0) = x$  and  $k_C(x, 1) = k_C(1) = k_C(3) = 1$  for all  $x \in X$  is an onto homomorphism for every  $C = (Z; \alpha_0, \alpha_1)$  in 2A. Similarly, the subalgebra of each  $H(Z; \alpha_0, \alpha_1)$  based on  $X \times \{0\} \cup \{0, 1\}$  is isomorphic to  $B$ .

This proves the claim of Theorem 10 for the category 4A; using the strong universality of  $I_0$  we get Theorem 10 as stated above.

PROOF OF THEOREM 5. Every transformation monoid  $(X, M)$  is the full endomorphism monoid of one  $\text{card}(X)$ -ary relation on  $X$ . Since every category of relational systems can be extended into 2A [6], Theorem 1 implies the existence of an integral domain  $I$  in  $I_0$  satisfying (i)–(iii). The remainder of Theorem 5 follows immediately from [7] where the main result says that for every strongly universal category of algebras  $C$  there is a proper class of strong embeddings  $S_i: C \rightarrow C$  such that  $S_i(c) \cong S_j(d)$  only if  $i = j$  and  $c \cong d$  ( $c, d$  objects of  $C$ ).

REMARK. Since every concrete category  $K$  with only a set of objects (*small* concrete category) is a full subcategory of some category of relational systems (where we include one  $\text{card}(X)$ -ary relation  $R_k$  for each object  $k$  of  $K$  whose underlying set is  $X$ ), we have an immediate generalization of Theorem 5 for small categories in an arbitrary concrete representation. Theorem 6 is even more general: it extends the claim of Theorem 5 to categories that have a proper class of objects. It is clear that the method outlined here would not be adequate for the proof of Theorem 6.

There are other consequences of the strong universality of  $I_0$  too numerous to mention. Theorems 2–5, for instance, can be further generalized and combined in various ways; there are other results utilizing the special properties of the strong embedding  $F$  from Theorem 1. It is hoped, however, that the spectrum of results presented here is wide enough to convey some of the flavor of the field and to indicate possible usefulness of the concept of universality.

## REFERENCES

1. E. Fried and J. Sichler, *Homomorphisms of commutative rings with unit element*, Pacific J. Math. **45** (1973), 485–491. MR **49** #270.

2. G. Grätzer and J. Sichler, *On the endomorphism semigroup (and category) of bounded lattices*, Pacific J. Math. **35** (1970), 639–647. MR **43** #3175.
3. Z. Hedrlín, *On endomorphisms of graphs and their homomorphic images*, Proof Techniques in Graph Theory (Proc. 2nd Ann Arbor Graph Theory Conf., 1968), Academic Press, New York, 1969, pp. 73–85. MR **41** #1568.
4. Z. Hedrlín and J. Lambek, *How comprehensive is the category of semigroups?*, J. Algebra **11** (1969), 195–212. MR **38** #5892.
5. Z. Hedrlín and E. Mendelsohn, *The category of graphs with a given subgraph—with applications to topology and algebra*, Canad. J. Math. **21** (1969), 1506–1517. MR **41** #5232.
6. Z. Hedrlín and A. Pultr, *On full embeddings of categories of algebras*, Illinois J. Math. **10** (1966), 392–406. MR **33** #85.
7. Z. Hedrlín and J. Sichler, *Any boundable binding category contains a proper class of mutually disjoint copies of itself*, Algebra Universalis **1** (1971), no. 1, 97–103. MR **44** #2798.
8. L. Kučera and A. Pultr, *Non-algebraic concrete categories*, J. Pure Appl. Algebra **3** (1972), 95–102. MR **49** #375.
9. A. Pultr, *Eine Bemerkung über volle Einbettungen von Kategorien von Algebren*, Math. Ann. **178** (1968), 78–82. MR **37** #6352.
10. J. Sichler, *Testing categories and strong universality*, Canad. J. Math. **25** (1973), 370–385. MR **47** #6805.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MANITOBA, WINNIPEG, MANITOBA, CANADA R3T 2N2 (Current address of J. Sichler)

*Current address* (E. Fried): B.E.L.T., Algebra és Számelmélet Tanszék, 1088 Budapest, Múzeum-Körút 6–8, Hungary