PACIFIC JOURNAL OF MATHEMATICS
Vol. 45, No. 2, 1973

HOMOMORPHISMS OF COMMUTATIVE RINGS WITH UNIT ELEMENT

E. FRIED AND J. SICHLER

Let R be a commutative ring. All its endomorphisms form a monoid $\mathscr{E}(R)$ and a natural question to ask is what monoids appear as full endomorphism monoids of commutative rings. It was shown in [8] that every group is representable as the full automorphism group of a ring without unit element. Much more cannot be expected in this case as the zero mapping is always one of the endomorphisms. The presence of the unit element 1 in the ring changes the picture. We will show here that every monoid is isomorphic to the monoid $\mathscr{E}_1(R)$ of all 1-preserving endomorphisms of a commutative ring R with 1. In fact, a stronger theorem will be proved: the category $\mathscr{R}_1$ of all rings with 1 and all 1-preserving homomorphisms is binding.

DEFINITION. A category $\mathscr{C}$ is *binding* if every category of algebras is isomorphic to a full subcategory of $\mathscr{C}$.

Every monoid is representable as $\mathrm{Hom}_{\mathscr{C}}(C, C)$ for a suitable object C of a binding category $\mathscr{C}$; see e.g. [3]. Many other properties are also shared by binding categories. There is a considerable list of binding categories: categories of directed [5] and undirected graphs [7], the category of semigroups [3], the category of commutative groupoids [9], the category of bounded lattices [1], and other categories of algebras. Next is the list of theorems proved here.

FULL EMBEDDING THEOREM. *$\mathscr{R}_1$ is binding.*

This is the basic theorem. The remaining theorems are consenquences of results proved elsewhere and of the proof of the above theorem.

REPRESENTATION THEOREM. *Let M be a monoid, let σ be a cardinal number, $\sigma \geqq \max(\aleph_0, |M|)$. Then there is a set $(R_\alpha | \alpha \in 2^\sigma)$ of commutative rings R_α with unit such that for all $\alpha, \alpha' \in 2^\sigma$.*

(i) $|R_\alpha| = \sigma$,

(ii) $\mathscr{E}_1(R_\alpha) \cong M$,

(iii) $\mathrm{Hom}_{\mathscr{R}_1}(R_\alpha, R_{\alpha'}) = \emptyset$ *whenever* $\alpha \neq \alpha'$.

In particular, the rings R_α are pairwise nonisomorphic. Note also that the result is the best possible—there are exactly 2^σ pairwise nonisomorphic rings of a cardinality $\sigma \geqq \aleph_0$.

SUBRING INDEPENDENCE THEOREM. *Let M_1 and M_2 be monoids. Then there are commutative rings with unit R_1 and R_2 such that R_1 is a subring of R_2 and $\mathscr{E}_1(R_i) \cong M_i$ for $i = 1, 2$.*

QUOTIENT RING INDEPENDENCE THEOREM. *Let M_1 and M_2 be monoids. Then there are commutative rings with unit R_1 and R_2 such that R_2 is a homomorphic image of R_1 and $\mathscr{E}_1(R_i) \cong M_i$ for $i = 1, 2$.*

EXTENSION PROPERTY. *Let M be a monoid of transformations on the set X. Then there is a commutative ring with unit R such that R contains X and every $m \in M$ extends uniquely to an endomorphism of R. This extension is an isomorphism between M and $\mathscr{E}_1(R)$.*

To prove the first theorem a full embedding Φ of the category $\mathscr{G}$ of undirected graphs into $\mathscr{R}_1$ will be constructed in third section. The necessary definitions follow.

2. Graphs and categories. An *undirected graph* G is a pair $G = \langle X, R\rangle$ where X is a set and R is a set of two-element subsets of X. Let $G' = \langle X', R'\rangle$ be another graph; a mapping $f: X \to X'$ is *compatible* if $\{x_1, x_2\} \in R$ implies $\{f(x_1), f(x_2)\} \in R'$. Let $\mathscr{G}$ be the category whose objects are all undirected graphs and whose morphisms are all compatible mappings. A morphism $f: G \to G'$ is *onto* if f itself is an onto mapping and if $R' = \{\{f(x_1), f(x_2)\} \mid \{x_1, x_2\} \in R\}$.

A *concrete category* is a category $\mathscr{C}$ together with a fixed faithful functor $U: \mathscr{C} \to \mathrm{Set}$ (Set is the category all sets and all mappings). $\mathscr{G}$ is concrete category with $U(\langle X, R\rangle) = X$; for categories of algebras we shall always choose the standard underlying-set functor. Let $\langle \mathscr{C}_1, U_1\rangle$ and $\langle \mathscr{C}_2, U_2\rangle$ be two concrete categories. A functor $\Sigma: \mathscr{C}_1 \to \mathscr{C}_2$ is a *full embedding* if Σ is one-to-one both on objects and on morphisms and if for every $\beta: \Sigma(C) \to \Sigma(C')$ there exists a morphism $\alpha: C \to C'$ in $\mathscr{C}_1$ such that $\Sigma(\alpha) = \beta$. A full embedding Σ is called an *extension* if there is a monotransformation $\mu: U_1 \to U_2 \circ \Sigma$.

The starting point is the following theorem; it can be easily obtained using results of [5] and [7].

THEOREM A. *Let $\mathscr{A}$ be a full category of algebras or a full category of relational systems. Then there is an extension $\Psi_{\mathscr{A}}: \mathscr{A} \to \mathscr{G}$ such that $\Psi_{\mathscr{A}}$ preserves all one-to-one and onto morphisms. If $\mathscr{A}$ is the category of commutative groupoids, then $\Psi_{\mathscr{A}}$ also preserves the cardinalities of those underlying sets that are infinite.*

3. The full embedding. An extension

$$\Phi\colon \mathscr{G} \to \mathscr{R}_1 \tag{1}$$

will be constructed here.

Let $G = \langle X, R\rangle$ be an undirected graph, let Z be the ring of integers. Consider the ideal I generated by the set $\{x^3 - 5.7 \mid x \in X\}$ in the polynomial ring $Z[X]$ and let

$$R(X) = Z[X]/I\ . \tag{2}$$

Obviously, $Z \subseteqq R(X)$ and $R(X)$ contains a copy of the set X as a set of generators. Let $\Phi(G)$ be the subring of $R(X)$ generated by the set

$$Z \cup \{5x \mid x \in X\} \cup \{xy \mid \{x, y\} \in R\}\ . \tag{3}$$

Every compatible mapping $f\colon G \to G' = \langle X', R'\rangle$ extends uniquely to a 1-preserving homomorphism $\bar{f}\colon Z[X] \to Z[X']$ such that $\bar{f}(I) \subseteqq I'$. Hence there is a unique homomorphism $R(f)\colon R(X) \to R(X')$ such that $R(f)(5x) = 5f(x)$ and for each xy in $\Phi(G)$ $R(f)(xy) = f(x)f(y)$. As f is a compatible mapping, $R(f)(\Phi(G)) \subseteqq \Phi(G')$. Let $\Phi(f)$ be the restriction of $R(f)$ to $\Phi(G)$; it is easy to see that Φ is naturally equivalent to a one-to-one functor denoted also as Φ.

The mappings $\mu_G\colon X \to \Phi(G)$ defined by $\mu_G(x) = 5x$ form a natural transformation $\mu\colon U_1 \to U_2 \circ \Phi$, where $U_1\colon \mathscr{G} \to \mathrm{Set}$ and $U_2\colon \mathscr{R}_1 \to \mathrm{Set}$ are the standard underlying-set functors. μ is a monotransformation. To prove that Φ is an extension it is enough to show that for every 1-preserving homomorphism $g\colon \Phi(G) \to \Phi(G')$ there is a compatible mapping $f\colon G \to G'$ such that $g = \Phi(f)$.

First of all, adjoin a third root ρ of the unit to $R(X)$; that is, let $\rho^2 + \rho + 1 = 0$ and let

$$E(X) = (R(X))[\rho]\ .$$

Let $E = Z[\rho]$. Observe that $E(X)$ is a free E-module over the set of all commutative products

$$\pi = x_1^{i_1} \ldots x_n^{i_n} \tag{4}$$

of powers of pairwise different elements of X with $1 \leqq i_j \leqq 2$.

In particular, if

$$e = \sum_{i=1}^{m} e_i \pi_i \qquad (e_i \in E) \tag{5}$$

is an element of $E(X)$ such that the products π_i are pairwise different and if e is divisible by an integer k, then k divides every e_i. No integer is a zero divisor in $E(X)$.

For a product of the form (4) denote

$$u(\pi) = \{x_1, \cdots, x_n\} \tag{6}$$

and

$$(7) \qquad l(\pi) = |u(\pi)| .$$

Note that always $u(\pi_1 \cdot \pi_2) \subseteqq u(\pi_1) \cup u(\pi_2)$; if $u(\pi_1 \cdot \pi_2) \neq u(\pi_1) \cup u(\pi_2)$, then the product $\pi_1 \cdot \pi_2$ is divisible by 5.7.

LEMMA 1. *$\eta^3 = 5^4 \cdot 7$ in $E(X)$ if and only if $\eta = 5\rho^\alpha x$ for some $\alpha \in \{0, 1, 2\}$ and $x \in X$.*

Proof. For each x and α $(5\rho^\alpha x)^3 = 5^3 \cdot 1 \cdot x^3 = 5^4 \cdot 7$. Conversely, let $\eta \in E(X)$ and $\eta^3 = 5^4 \cdot 7$. $\eta = \eta(x_1, \cdots, x_n)$ for a finite set $\{x_1, \cdots, x_n\} \subseteqq X$ so it is enough to prove the lemma for finitely generated rings $E_n = E(\{x_1, \cdots, x_n\})$. We will proceed by induction.

Since E_1 is an integral domain, the polynomial

$$(8) \qquad \eta^3 - 5^4 \cdot 7$$

has at most three roots in E_1. E_1 contains, however, three different roots of (8), namely $5x_1$, $5\rho x_1$ and $5\rho^2 x_1$.

Assume the lemma to be true for n and let $\eta \in E_{n+1}$ be a root of (8),

$$(9) \qquad \eta = a + bx_{n+1} + cx_{n+1}^2$$

for some a, b, c in E_n. It is easy to see that mappings

$$\varphi_i : E_{n+1} \longrightarrow E_{n+1} \qquad (i = 0, 1, 2)$$

defined by

$$\varphi_i(p(x_1, \cdots, x_n, x_{n+1})) = p(x_1, \cdots, x_n, \rho^i x_1)$$

(the coefficients of p are in E) are endomorphisms of E_{n+1} and that $\varphi_i(E_{n+1}) = E_n$ for $i = 0, 1, 2$. Put

$$(10) \qquad \eta_i = \varphi_i(\eta) \qquad (i = 0, 1, 2) .$$

Clearly

$$(11) \qquad \eta_0 = a + bx_1 + cx_1^2 ,$$

$$(12) \qquad \eta_1 = a + b\rho x_1 + c\rho^2 x_1^2 ,$$

$$(13) \qquad \eta_2 = a + b\rho^2 x_1 + c\rho x_1^2 ,$$

and η_0, η_1, η_2 are roots of (8) in E_n. By the induction hypothesis $\eta_0 = 5\rho^\alpha x_i$, $\eta_1 = 5\rho^\beta x_j$, $\eta_2 = 5\rho^\gamma x_k$ for some $\alpha, \beta, \gamma \in \{0, 1, 2\}$ and $i, j, k \in \{1, \cdots, n\}$. Consequently, $3cx_1^2 = \eta_0 + \rho\eta_1 + \rho^2\eta_2 = 5\rho^\alpha x_i + 5\rho^{\beta+1}x_j + 5\rho^{\gamma+2}x_k$. Since the right side of the last equation is divisible by three, $x_i = x_j =$

x_k; so $3cx_1^2 = 5(\rho^\alpha + \rho^{\beta+1} + \rho^{\gamma+2})x_i$. Multiplying both sides by x_1 and dividing by five yields $7(3c) = (\rho^\alpha + \rho^{\beta+1} + \rho^{\gamma+2})x_1x_i$. A sum of three third roots of the unit is divisible by seven if and only if it vanishes, i.e., if either $\alpha \equiv \beta \equiv \gamma (\mathrm{mod}\ 3)$ or $\beta \equiv \alpha + 1 (\mathrm{mod}\ 3)$ and $r \equiv \alpha + 2 (\mathrm{mod}\ 3)$. In both cases $c = 0$.

Let $\alpha \equiv \beta \equiv \gamma (\mathrm{mod}\ 3)$. Note that $3a = \eta_0 + \eta_1 + \eta_2 = 5(\rho^\alpha + \rho^\beta + \rho^\gamma)x_i$; therefore $a = 5\rho^\alpha x_i$ and $b = 0$.

If $\beta \equiv \alpha + 1 (\mathrm{mod}\ 3)$ and $\gamma \equiv \alpha + 2 (\mathrm{mod})$ then $a = 0$. As $c = 0$, (11) implies $bx_1 = 5\rho^\alpha x_i$. If $x_1 \neq x_i$, then $7b = \rho^\alpha x_i x_1^2$—a contradiction. Therefore $x_i = x_1$ and $b = 5\rho^\alpha$.

Since $E(X) = R(X)[\rho]$ the only roots of (8) in $R(X)$ are of the form

$$\eta = 5x \qquad (x \in X) . \tag{14}$$

All of them are contained in $\Phi(G)$.

LEMMA 2. *The only idempotent elements in $\Phi(G)$ are* 0 *and* 1. $s^3 = 0$ *in $\Phi(G)$ if and only if $s = 0$.*

Proof. As $\Phi(G)$ is a subring of $E(X)$, we need only prove the lemma for $E(X)$; in fact the proof for all the rings E_n is sufficient. We can proceed by induction again. E_1 is an integral domain, therefore both assertions hold there. The rest of the proof is similar to the proof of Lemma 1.

LEMMA 3. *Let $G = \langle X, R\rangle$ be a graph. A product xy $(x, y \in X)$ belongs to $\Phi(G)$ if and only if $\{x, y\} \in R$.*

Proof. If $\{x, y\} \in R$, then $xy \in \Phi(G)$ by definition.

Conversely let S be the set of all elements σ of $R(X)$ of the form

$$\sigma = k + \sum_{u(\pi) \in R} k_\pi \cdot \pi + \sum m_\varphi \cdot \varphi \tag{15}$$

where $k, k_\pi \in \{0, \cdots, 4\}$ and for every φ either $l(\varphi) > 2$ or m_φ is divisible by five. All the generators of $\Phi(G)$ are of the form (15) and it is easy to see that S is a ring; $R(X) \supseteq S \supseteq \Phi(G)$. Since $R(X)$ is a free abelian group over the set of all products of the form (4), (15) is determined by σ uniquely. The lemma follows.

To finish the proof of fullness of Φ, let $g: \Phi(G) \to \Phi(G')$ be a 1-preserving homomorphism and let $x \in X$. $(g(5x))^3 = g((5x)^3) = g(5^4 \cdot 7) = 5^4 \cdot 7$, thus, by Lemma 1, $g(5x) = 5f(x)$ for some $f(x) \in X'$ $(f: X \to X'$ is a well-defined mapping). Let $\{x, y\} \in R$. By the definition of $\Phi(G)$,

$xy \in \Phi(G)$ and $25g(xy) = g(5x \cdot 5y) = g(5x) \cdot g(5y) = 25f(x)f(y)$, so $g(xy) = f(x)f(y)$. The product $f(x) \cdot f(y)$ belongs to $\Phi(G')$. By Lemma 3, $\{f(x), f(y)\} \in R'$. $f: \langle X, R\rangle \rightarrow \langle X', R'\rangle$ is a morphism in $\mathscr{G}$ and $\Phi(f) = g$—proving the fullness of Φ.

Now, let $h: \Phi(G) \rightarrow \Phi(G')$ be a homomorphism not preserving the unit element 1. Since 0 is the only other idempotent in $\Phi(G')$, $h(1) = 0$. Thus $h(n) = 0$ for every integer n and, in particular, $(h(5x))^3 = h((5x)^3) = h(5^4 \cdot 7) = 0$ and $(h(xy))^3 = h(x^3y^3) = h(5^2 \cdot 7^2) = 0$. According to Lemma 2, $h(5x) = 0$ a $h(xy) = 0$. All generators of $\Phi(G)$ are mapped to the zero of $\Phi(G')$ so h is the zero homomorphism. The last observation is utilized as follows.

THEOREM. *Let $\mathscr{S}$ be the category of all commutative rings with unit* 1 *and all their* (*not necessarily* 1-*preserving*) *homomorphisms. Let $\mathscr{N}$ be the class of all nonzero homomorphisms of $\mathscr{S}$. Then there is a full subcategory $\mathscr{F}$ of $\mathscr{S}$ such that*

(i) *$\mathscr{F} \cap \mathscr{N}$ is a category*

(ii) *$\mathscr{F} \cap \mathscr{N}$ is binding.*

In particular, for every monoid M there is a commutative ring R with unit such that the set of all its nonzero endomorphisms is closed under composition and isomorphic to M. All the theorems listed in the first section can be similarly reformulated.

4. Concluding remarks. First we shall indicate the proofs of the remaining four theorems.

The Representation Theorem is an immediate consequence of the proof of the Full Embedding Theorem, Theorem A and Theorem 4 of [6].

To prove the Subring Independence and Quotient Ring Independence Theorems, observe that the extension $\Phi: \mathscr{G} \rightarrow \mathscr{R}_1$ preserves all one-to-one and all onto morphisms. Combining this fact with Theorem A and the main results [4] and [2] respectively, we obtain both Independence Theorems.

The proof of the Extension Property is based on the fact that there is an extension $\Phi \circ \Psi_{\mathscr{A}}: \mathscr{A} \rightarrow \mathscr{R}_1$ for every category $\mathscr{A}$ of relational systems (Theorem A and the third section) and on the observation that every monoid M of transformations on the set X is the monoid of all mappings $X \rightarrow X$ compatible with one $|X|$-ary relation.

L. Kučera and Z. Hedrlín have proved recently that any concrete category has an extension to $\mathscr{G}$ provided there are no measurable cardinals. Using this fact one can generalize immediately the Extension Property to the statement saying that any concrete category has an extension to the category of all commutative rings with 1 and all 1-preserving homomorphisms (under the hypothesis of nonexistence of measurable cardinals).

We conclude by mentioning two open problems. Note that all rings $\Phi(G)$ have zero divisors and are infinite. Thus the present results do not apply to the case of finite rings and to the case of integral domains.

REFERENCES

1. G. Grätzer and J. Sichler, *On the endomorphism semigroup (and category) of bounded lattices*. Pacific J. Math., **35** (1970), 639-647.
2. Z. Hedrlín, *On endomorphisms of graphs and their homomorphic images*, Proof Techniques in Graph Theory, Ed. F. Harrary, Academic Press, 1969.
3. Z. Hedrlín and J. Lambek, *How comprehensive is the category of semigroups?* J. Algebra, **11** (1969), 195-212.
4. Z. Hedrlín and E. Mendelsohn, *The category of graphs with given subgraph*, Canad. J. Math., **21** (1969), 1506-1517.
5. Z. Hedrlín and A. Pultr, *On full embeddings of categories of algebras*, Illinois J. Math., **10** (1966), 392-405.
6. Z. Hedrlín and J. Sichler, *Any boundable binding category contains a proper class of mutually disjoint copies of itself*, Algebra Universalis **1**, (1971), 97-103.
7. P. Hell, *Full embeddings into some categories of graphs*, to appear.
8. R. Quackenbush and J. Sichler, *Automorphism groups of commutative rings*, to appear.
9. J. Sichler, *Category of commutative groupoids is binding*, Comment. Math. Univ. Carolinae, **8** (1967), 753-755.

Received June 15, 1971. The authors were supported by grants from National Research Council of Canada.

THE UNIVERSITY OF MANITOBA