

Eötvös Loránd Tudományegyetem, Természettudományi Kar

Diplomamunka

**On the category of unique factorisation
domains**

Készítette: Braun Gábor

Budapest, 2002. január

Ez a diplomamunka a 2001. évi Országos
Tudományos Diákköri Konferencián első díjat nyert
dolgozatom bővített változata.

Chapter 1

Introduction

1.1 Abstract

I would like to generalize two seemingly unconnected groups of results.

First group: categories of rings. In 1973 E. Fried and J. Sichler proved that the category of commutative rings with unit is binding ([4]) and in 1975 they tried to show in a subsequent paper that the category of integral domains is strongly binding ([5]). However, it was discovered in 2000 that their argument only shows that it is moderately binding. Hence the problem whether the category of rings with unit is strongly binding is open again. While the proofs of E. Fried and J. Sichler are complicated, in 1977 J. Kollár gave a simple proof that the category of unique factorisation domains (abbr. UFD) is binding ([7]).

I will improve the method of Kollár to obtain a simple proof for their common generalisation: the category of UFDs is moderately binding (MAIN THEOREM).

Second group: independence theorems of endomorphisms of subgraphs. The problem is the following: given a lattice one wants to represent it as a lattice of some induced subgraphs of a graph. The lattice operations are the set theoretic union and intersection (both on the set of vertices and on the set of edges). Moreover one wants that the endomorphism monoids of the subgraphs can be chosen arbitrarily as abstract monoids.

L. Babai announced in [1] that the above statement holds for all distributive lattice but never published a proof.

J. Sichler and V. Koubek ([9]) proved the theorem for chains (with infinite union and intersection).

A natural generalisation (Theorem 2.2) is that instead of a lattice one chooses an arbitrary collection of sets (say a power set of a set) and one requires that mapping these to the collection of subgraphs every “meaningful” set theoretic operation is preserved (arbitrary union, intersection, subtraction etc.). This will be done in Chapter 2. It will also prove Babai’s theorem.

Combining the two groups. A similar statement on independence of endomorphisms of subUFDs can be proved for UFDs by embedding the category of graphs into the category of

UFDs in a suitable way (Corollary 3.2.3). In fact this is the main principle of the theory of binding categories: using an appropriate embedding reduce your problem to another category where you can solve the problem.

1.2 Introduction to the theory of binding categories

The theory of binding categories arose from the seek of representing groups as automorphism groups of various mathematical objects. As far as I know, representing infinite groups always involves some set theory. Though there are powerful set theoretic tools (e.g. Shelah's Black Box, see [2] for the proof that every infinite group is a Galois group over any field with characteristic zero), the allure of binding categories is that the set theory part is hidden: one need not know set theory for applications.

A detailed discussion of binding categories can be found in the fundamental book [8]. I only recall the basic definitions and facts needed for applications.

Basic facts. A category is *binding* or *algebraically universal* iff every category of universal algebras can be embedded into it. It is easy to see that every monoid appears as an endomorphism monoid in every binding category. Moreover, every small category can be fully embedded into every binding category since every small category can be fully embedded into a category of universal algebras.

The fundamental theorem of the theory of binding categories is that the following categories are binding: $\mathbf{Alg}(1, 1)$, $\mathbf{Alg}(2)$, $\mathbf{Rel}(2)$. Here $\mathbf{Alg}(\Delta)$ resp. $\mathbf{Rel}(\Delta)$ denotes the category of universal resp. relational algebras with type Δ . (Δ is a function from the set of symbols of operations resp. relations to the class of cardinalities. To each symbol R a $\Delta(R)$ -variable operation resp. relation is associated on each algebra. Homomorphisms are maps preserving the operations resp. relations. By preserving a relation we mean that each tuple which is in relation is mapped to a tuple in relation.) Note that $\mathbf{Rel}(2)$ is the category of directed graphs. The category of undirected graphs is also binding.

One usually adds a new category to the list of binding categories by embedding a binding category into it. One usually embeds one of the above mentioned categories so they are particularly important.

Not binding categories. E.g. the category of groups and $\mathbf{Alg}(1)$ are not binding. The reason is that not every group appears as automorphism group. See [6] for a complete description of abelian automorphism groups in $\mathbf{Alg}(1, 1)$.

Outline of the proof of the fundamental theorem I sketch the proof of the main theorem to make the reader familiar with the methods. A detailed proof can be found in [8], which is a fundamental book on the subject. An algebraic category is embedded into $\mathbf{Rel}(2)$ by constructing a chain of embeddings:

$$\mathbf{Alg}(\Delta) \longrightarrow \mathbf{Rel}(\dots) \longrightarrow \mathbf{Rel}(2, \dots, 2) \longrightarrow \mathbf{Rel}(2).$$

So one first replaces operations with relations, then one makes every relation binary (even at the cost of adding new binary relations) and at last one codes all the binary relations with one binary relation. The last embedding is the most difficult. In particular, one has to exclude the image of “homomorphisms” which maps each relation R into a relation S which could be different from R . To do this, one has to put a rigid graph structure (i.e. identity is its only endomorphism) on the set of relation symbols. This was done by Vopěnka, Pultr and Hedrlín ([10]). This is the point where set theory comes in.

This is the outline of proving that $\mathbf{Rel}(2)$ is binding. By constructing a chain of full embeddings

$$\mathbf{Rel}(2) \longrightarrow \mathbf{Alg}(1,1) \longrightarrow \mathbf{Alg}(2)$$

one can show that $\mathbf{Alg}(1,1)$ and $\mathbf{Alg}(2)$ are binding. $\mathbf{Rel}(2)$ can be also embedded into the category of undirected graphs showing that the latter is binding.

Strongly and moderately binding categories. Sometimes one needs information how a functor behaves on the underlying sets (e.g. does it preserve injections or surjections). So let (\mathbf{C}_1, U_1) and (\mathbf{C}_2, U_2) be concrete categories, $\mathbf{F}: \mathbf{C}_1 \longrightarrow \mathbf{C}_2$ be a functor. The best case is when the image of underlying sets resp. morphisms (as maps) depends only on the underlying sets resp. the morphisms as a map between the underlying sets, and not on the particular structure on the underlying sets. The precise definition: \mathbf{F} is called *strong* if there is a faithful functor $\mathbf{H}: \mathbf{Set} \longrightarrow \mathbf{Set}$ such that $U_2 \circ \mathbf{F} = \mathbf{H} \circ U_1$. A category is *strongly binding* if every category of universal algebras can be strongly embedded into it. Only a few examples are known for strongly binding algebraic categories: the category of semigroups and the category of universal algebras with type Δ where $\sum |\Delta| \geq 2$. (This can be seen by a careful analysis of the proof of the fundamental theorem.) It is an open problem whether any category of rings is strongly binding. The strongest result in this direction is the Main Theorem of the present thesis.

In a strongly binding category for every monoid M there are arbitrarily many objects with endomorphism monoid M such that the underlying M -sets are the same. One can even require that there is no morphism between distinct objects.

Chapter 2

Sublattices with arbitrary endomorphism monoids

Roughly, we want to put a graph structure on a set such that its non-empty subsets are subgraphs with prescribed endomorphism monoids. This is obviously not possible because of lack of “space”. So we *expand* the set: replace every point with several points, and even the empty set is replaced by a non-empty set. We do this such that the expansion of the subsets with the induced graph structure have arbitrarily prescribed endomorphism monoids. Precisely:

Definition 2.1. Let X be any set. An *expansion* of X is a subset V together with a partition $\{V_x : x \in X \cup \{0\}\}$. Here 0 is not an element of X . For a subset $H \subseteq X$ the *expansion of H* is $\bigcup\{V_x : x \in H \cup \{0\}\}$.

Theorem 2.2. Let $\{M_H\}_{H \in L}$ be a collection of monoids where L is a collection of non-empty set subsets of a set X . Then there is an undirected graph whose set V of vertices is an expansion of X and for every $H \in L$ the subgraph spanned by the expansion of H has endomorphism monoid M_H . Moreover, for any distinct element x, y of X there is no edge between V_x and V_y .

Note that if L is a complete lattice with the set theoretic operations then the construction gives a complete lattice of subgraphs with the operations the set theoretic ones (both on the set of vertices and on the set of edges).

Corollary 2.3. With the same hypothesis there is also a universal algebra with two unary operations whose underlying set is an expansion of X and for every $H \in L$ the expansion of H is a subalgebra with endomorphism monoid M_H .

Proof. First note that it is enough to find a relational algebra in $\mathbf{Rel}(2, \dots, 2)$ with the properties stated. (The number of relations may depend on the given collection of monoids.) Then one applies to this algebra the embeddings from $\mathbf{Rel}(2, \dots, 2)$ to $\mathbf{Rel}(2)$, from $\mathbf{Rel}(2)$ to $\mathbf{Alg}(1, 1)$ and to the category of symmetric graphs to obtain the required structures in this category. (See [8] for these embeddings.) Note that some of the functors have to be modified because the cartesian square V^2 of the underlying set V is part of the underlying set of the image. Replacing V^2 by $\bigcup\{(V_x \cup V_0)^2 : x \in X\}$ the construction makes sense and we obtain the required algebras.

For each $H \in L$ we construct an algebra $G(H)$ as follows: Choose a graph G_H with endomorphism monoid $M := M_H$ such that the M -set M with the regular left representation is part of the graph. This part will be denoted by M . Let

$$G(H) := G \cup \bigcup_{x \in X} M_x$$

where each M_x is an isomorphic copy of M and the union is disjoint. $G(H)$ is an expansion of X by the partition:

$$G(H)_0 := G_H \cup \{1_x : x \in H\} \tag{2.1}$$

$$G(H)_x := M_x \tag{2.2} \quad (x \in H)$$

$$G(H)_x := M_x \setminus \{1_x\} \tag{2.3} \quad (x \in X \setminus H)$$

The relations of $G(M)$ are

$$R := \{\text{edges of } G\} \cup \{\text{rigid structure on } M_x : x \in X \setminus H\} \tag{2.4}$$

$$R_x := \{(a, a_x) : a \in M\} \quad (x \in X) \tag{2.5}$$

$$R_H := G_H \times G_H \tag{2.6}$$

Thus R_x is the identification of M with M_x .

Finally, the relational algebra G we seek is the disjoint union of the $G(H)$ s:

$$G := \bigcup_{H \in L} G(H).$$

The relations are all the relations introduced for some $G(H)$.

It is easy to see that this G satisfies the requirements. M_H is identified with the endomorphisms of the expansion of H by acting trivially on $G(K)$ for $K \neq H$, and on $G(H)$ by acting on G_H as identified with the endomorphism monoid and on each M_x by left regular representation.

The only non-trivial statement is that the expansion of H has no other endomorphisms. So choose an arbitrary endomorphism φ . It preserves each G_K since it preserves the relation R_K . So it is an endomorphism $m \in M_K$ on G_K . φ can only preserve R_x if it acts on each M_x of $G(K)$ by the left regular representation. If there is an $x \in K \setminus H$ then 1_x is mapped to itself (being the only element of M_x in the graph) so $m = 1$. If there is an $x \in H \setminus K$ then φ is the identity on M_x since it preserves the rigid R on M_x . So again $m = 1$.

Thus φ is trivial on $G(K)$ for $K \neq H$ and is an endomorphism $m \in M_H$ on $G(H)$, hence it is the endomorphism m . \square

Chapter 3

Unique factorisation domains

3.1 Terminology

A class of some objects of a category is *mutually rigid* if the only morphisms between the objects in the class are the identities.

For convenience of the reader, I recall the definition of binding categories and add the definitions needed for the Main Theorem.

Let (\mathbf{C}_1, U_1) and (\mathbf{C}_2, U_2) be concrete categories, $\mathbf{F}: \mathbf{C}_1 \rightarrow \mathbf{C}_2$ be a functor. \mathbf{F} is called *strong* if there is a faithful functor $\mathbf{H}: \mathbf{Set} \rightarrow \mathbf{Set}$ such that $U_2 \circ \mathbf{F} = \mathbf{H} \circ U_1$. \mathbf{F} is *moderate* if there is a faithful functor $\mathbf{H}: (\mathbf{Set}, \text{injective maps}) \rightarrow \mathbf{Set}$ such that $U_2 \circ \mathbf{F} = \mathbf{H} \circ U_1$ when restricted to *injective* morphisms in \mathbf{C}_1 .

Now suppose that U_2 is not only a $\mathbf{C}_2 \rightarrow \mathbf{Set}$ functor but also a faithful $\mathbf{C}_2 \rightarrow \mathbf{Alg}(\mathbf{2})$ functor. Let α be the binary operation in $\mathbf{Alg}(\mathbf{2})$. Define \mathbf{F} to be α -moderate resp. α -strong similarly as above requiring \mathbf{H} to be a $\mathbf{Set} \rightarrow \mathbf{Alg}(\mathbf{2})$ functor.

A category is *binding* if every category of universal algebras can be fully embedded into it. A category is *strongly binding* if every category of universal algebras can be strongly embedded into it. Similarly one can define moderately, α -moderately, α -strongly binding categories.

3.2 Main results

Let \mathbf{UFD} denote the category of UFDs with morphisms the one-preserving ring homomorphisms.

MAIN THEOREM. *The category of UFDs is $+$ -moderately and \bullet -moderately binding.*

CONJECTURE. *The category of UFDs is $+$ -strongly and \bullet -strongly binding.*

The following four section is devoted to the proof of the theorem. Now let us state some interesting consequences.

Corollary 3.2.1. *For every infinite cardinal κ , there are 2^κ non-isomorphic — even mutually rigid — UFD structure over the free abelian group of rank κ as the additive group and with isomorphic multiplicative semigroups.*

Thus the additive as well as the multiplicative structure of a UFD is very far to determine the other.

Remark. E. Fried proved that there are 2^κ mutually rigid integral domains over the κ dimensional rational vector space ([3]).

Corollary 3.2.2. *Let G be a group, $\kappa \geq |G| \cdot \aleph_0$ a cardinal. Then there are 2^κ UFDs over the same κ -rank free abelian group resp. over the same multiplicative semigroup with cardinality κ such that there is no homomorphism between distinct UFDs and all of the UFDs have the same automorphism group (i.e. consisting of the same maps), which is isomorphic to G .*

Corollary 3.2.3. *Let a (complete) lattice be given such that the operations are the set theoretic union and intersection. Assume that a monoid assigned to every element of the lattice. Then the lattice is isomorphic to a (complete) sublattice of a UFD such that the monoids are isomorphic to the endomorphism monoids of the corresponding subUFD.*

The corollaries will be proved in the last section.

3.3 Construction of the embeddings

Let α and β denote the two unary operations in the category $\mathbf{Alg}(1, 1)$. Because this category is strongly binding, it is enough to embed this category into \mathbf{UFD} . Let

$$\mathbf{F}_+(X, \alpha, \beta) := \mathbb{Z} \left[x, \frac{1}{x}, \frac{1}{x+3}, \frac{1}{x^2 + \alpha(x) - 2\beta(x) + 7} : x \in X \right],$$

$$\mathbf{F}_\bullet(X, \alpha, \beta) := \mathbb{Z} \left[x, \frac{1}{x}, \frac{1}{x+3}, \underline{x}, \frac{1}{\underline{x}-x}, \frac{1}{\underline{x}-x+3}, \frac{1}{\underline{x}+x+1}, \frac{x+2\alpha(x)+4\beta(x)+1}{\underline{x}} : x \in X \right],$$

where $\underline{X} := \{\underline{x} : x \in X\}$ is a copy of X . For $x \in X$, x and \underline{x} are considered as indeterminates over \mathbb{Z} . \mathbf{F}_+ and \mathbf{F}_\bullet are defined on the morphisms in the obvious way. We are going to prove that \mathbf{F}_+ is a $+$ -moderate full embedding and \mathbf{F}_\bullet is a \bullet -moderate full embedding if we choose the underlying sets appropriately (to be described in Section 3.5).

3.4 The images are UFDs

In this section we do not distinguish prime elements which only differ by a unit factor.

It is well-known that every polynomial ring over \mathbb{Z} is a UFD and every localization of a UFD is a UFD, in which the primes (up to units) are those primes of the original UFD which have no inverse in the localization. Hence the image of \mathbf{F}_+ is in the category of UFDs.

Lemma 3.4.1. *If R is a UFD, p is a prime of R then $S := R[x, \frac{p}{x}]$ is a UFD with the same units, whose primes are x and f/x^k where $f \in P^k \setminus P^{k+1}$ is a prime of $R[x]$, f is not x , $P := (p, x)$ is a prime ideal of $R[x]$. Especially, the primes of R distinct from p are primes of S .*

Proof. For $f = \sum a_i x^i \in R[x] \setminus \{0\}$, let $a(f) := \max\{k : f \in P^k\}$. The proof consists of six steps.

STEP 1 $a(f) \geq k \Leftrightarrow (\forall i \leq k) p^{k-i} \mid a_i$

Obvious.

STEP 2 $a(fg) = a(f) + a(g)$ if $f, g \in R[x] \setminus \{0\}$

Let $g = \sum b_j x^j, k := a(f), l := a(g)$. It is clear that $fg \in P^{k+l}$. By hypothesis, there are a smallest i and a smallest j such that $p^{k+1-i} \nmid a_i$ and $p^{l+1-j} \nmid b_j$. Then the coefficient of the $i+j$ degree term is $\sum a_t b_{i+j-t}$, which is not divisible by $p^{k+l+1-i-j}$ since exactly one summand is not, namely, $a_i b_j$. Thus $fg \notin P^{k+l+1}$.

STEP 3 $S = \{\frac{f}{x^k} : f \in R[x], k \geq 0, a(f) \geq k\}$

The given elements obviously belong to S and they form a ring including R and containing x and p/x .

STEP 4 *The units of S are the same as the units of R .*

Clear from Step 3.

STEP 5 *The following elements are primes of S : x and f/x^k for $a(f) = k$ and f a prime of $R[x]$ distinct from x .*

Note that $x \mid (g/x^l)$ iff $a(g) > l$. This easily implies that x is prime.

Suppose $f/x^k \mid (g/x^l)(h/x^m)$ in S . Then $f \mid x^N gh$ in $R[x]$ for N large enough. By the assumptions, $f \mid g$ or $f \mid h$ in $R[x]$. In the first case, $g = fq, q \in R[x], g/x^l = (f/x^k)(q/x^{l-k})$. $a(q) = a(g) - a(f) \geq l - k$ thus $q/x^{l-k} \in S$. Similarly, $f/x^k \mid h/x^m$ in the second case.

STEP 6 *Every non-zero element of S is a product of a unit and primes listed in Step 5.*

Let $f \in R[x] \setminus \{0\}, a(f) \geq k$ and let $f = \prod f_i$ be the factorisation of f in $R[x]$. Then $f/x^k = x^{\sum a(f_i)-k} \prod (f_i/x^{a(f_i)})$ is the factorisation of f/x^k in S . \square

Lemma 3.4.2. *Let R be a UFD, $Y \subseteq X$ be sets of indeterminates over R , $\{p_y\}_{y \in Y}$ a family of pairwise distinct primes of R and H a set of primes of $R[X]$ with non-zero constant terms. Let $S = S(Y) := R \left[x, \frac{p_y}{y} : x \in X, y \in Y \right]$. Then S_H is a UFD with the same units as $R[X]_H$, where T_D denotes the localization of the ring T by the set of elements D . There is a natural bijection between the primes of $R[X]_H$ and S_H given by associating each prime p of S_H to its unique multiple $\bar{p} = \bar{p}_Y$ which is a prime in $R[X]_H$. In fact, $\bar{p} = p \prod_{x \in \text{supp } p} \underline{x}^{k_x}$ where $\text{supp } p$ is the set of the variables x such that either x or \underline{x} occurs in p .*

Proof. First let us prove the lemma in the case $H = \emptyset$, when $S_H = S$ and $R[X]_H = R$.

For finite Y , the lemma follows from an easy induction on $|Y|$ using Lemma 3.4.1.

For general Y , note that $S(Y) = \bigcup_{Z \subseteq Y \text{ finite}} S(Z)$. Note also that for every $f \in S$, $\text{supp } f$ is finite and f is prime in S iff it is prime in $S(Z)$ for some $\text{supp } f \subseteq Z \subseteq Y$ iff it is prime in $S(Z)$ for all $\text{supp } f \subseteq Z \subseteq Y$. Moreover, for any prime p of S , \bar{p}_Z is the same for all $\text{supp } f \subseteq Z \subseteq Y$. Define \bar{p} to be this common value. The assertions of the Lemma obviously hold.

For general H , it is clear that $R[X]_H$ and S_H have the same units since R and S have the same units. For every prime p of S , either both of p and \bar{p} are primes in S_H resp. $R[X]_H$, either both of them are units in S_H . In the first case, p does not divide any other prime of $R[X]_H$. Hence the bijection between the primes of $R[X]_H$ and S_H is obtained essentially by restricting the bijection between the primes of R and S . \square

Corollary 3.4.3. *Between the primes of $\mathbb{Z}\left[x, \frac{1}{x}, \frac{1}{x+3}, \underline{x}, \frac{1}{x-x}, \frac{1}{x-x+3}, \frac{1}{x+x+1} : x \in X\right]$ and the primes of $\mathbf{F}_\bullet(X, \alpha, \beta)$ there is a natural bijection given by associating each prime p of the latter ring to its unique multiple \bar{p} which is a prime in the former one. In fact, $\bar{p} = p \prod_{x \in \text{supp } p} \underline{x}^{k_x}$ where $\text{supp } p$ is the set of the variables x such that either x or \underline{x} occurs in p . Moreover, the units of the rings are the same and both of them are UFDs.*

3.5 Moderateness

Let $\mathbf{H}: \mathbf{Set} \rightarrow \mathbf{Semigroups}$, $\mathbf{H}(X) := \mathbb{Z}\left[x, \frac{1}{x}, \frac{1}{x+3}, \underline{x}, \frac{1}{x-x}, \frac{1}{x-x+3}, \frac{1}{x+x+1} : x \in X\right]$ with multiplication as the operation for the semigroup. \mathbf{H} is defined on morphisms the obvious way.

The multiplicative semigroup of a UFD is the direct product of the group of units and the free abelian group with basis the set of primes (up to association). By Corollary 3.4.3, $\mathbf{H}(X)$ and $\mathbf{F}_\bullet(X, \alpha, \beta)$ have the same units and their primes are in bijection, which induces an isomorphism between the multiplicative semigroups. This isomorphism is clearly natural. Hence \mathbf{H} can be extended to a \bullet -moderate functor $\mathbf{Alg}(1, 1) \rightarrow \mathbf{UFD}$ naturally equivalent to \mathbf{F}_\bullet .

In the case of \mathbf{F}_+ , we need the following lemma.

Lemma 3.5.1. *Let $p_x := x(x+3)(x^2 + \alpha(x) - 2\beta(x) + 7)$. Then the additive group of $\mathbf{F}_+(X, \alpha, \beta)$ is a free abelian group with basis $\left\{ \prod x^{i_x} p_x^{j_x} : j_x \in \mathbb{Z}, i_x \in \{0, 1, 2, 3\} \right\}$.*

Proof. First we prove that the given system is a generating system. Obviously, every element can be written as $q \prod p_x^{j_x}$ with q a polynomial. We show by induction on the degree of q that this element is contained in the subgroup generated by the given system. We may assume that q is a monomial. If none of the variables have power at least 4 in q then the element belongs to the given system. If, e.g., $q = y^4 r$ then $q \prod p_x^{j_x} = (y^4 - p_y) r \prod p_x^{j_x} + r(p_y \prod p_x^{j_x})$, which is contained in the subgroup by the inductual hypothesis since r and $(y^4 - p_y)r$ have degree less than q .

Next we show that the system is independent, i.e. no nontrivial linear combination of the system is zero. Take such a linear combination $\sum n_x \prod x^{i_x} p_x^{j_x}$ (finite sum, $n_x \neq 0$). By multiplying with $\prod p_x^{t_x}$ choosing the powers large enough, we can achieve that all of the powers become nonnegative. Multiply out the brackets and consider a greatest degree monomial $\prod p_x^{k_x}$ which occurs in at least one summand. We will show that this monomial appears in exactly one summand hence it has a non-zero coefficient in the linear combination expressed as a polynomial in X , which will prove that the linear combination is not zero. By having the greatest degree, it can occur in a summand $\prod x^{i_x} p_x^{j_x}$ only as the greatest degree term, which is $\prod x^{4j_x + i_x}$. Therefore $k_x = 4j_x + i_x$ must hold for all x , which uniquely determines j_x and i_x . \square

Let $\mathbf{G}: \mathbf{Set} \rightarrow \mathbf{abelian\ groups}$ be the functor where $\mathbf{G}(X)$ is the free abelian group with basis the formal finite products $\prod x^{i_x} p_x^{j_x}$ with j_x any integer and $i_x \in \{0, 1, 2, 3\}$. \mathbf{G} is defined on morphisms the obvious way. Lemma 3.5.1 shows that there is a natural equivalence $\mathbf{F}_+(X, \alpha, \beta) \approx \mathbf{G}(X)$. This defines a UFD structure on $\mathbf{G}(X)$ and hence extends \mathbf{G} to a $+$ -moderate functor $\mathbf{Alg}(1, 1) \rightarrow \mathbf{UFD}$ naturally equivalent to \mathbf{F}_+ .

3.6 The functors are full

The following lemmas are a version of Kollár's lemma in [7].

Lemma 3.6.1. *Let u and $u + 3$ be invertible in $\mathbf{F}_+(X, \alpha, \beta)$ resp. $\mathbf{F}_\bullet(X, \alpha, \beta)$. Then $u \in \{x, -x - 3 : x \in X\}$ resp. $u \in \{x, -x - 3, \underline{x} - x, -\underline{x} + x - 3 : x \in X\}$.*

Proof. First we prove the lemma for \mathbf{F}_+ .

Let $u = f/h, u + 3 = g/h$ where $f, g, h \in \mathbb{Z}[x : x \in X]$ are pairwise relative primes except perhaps a common factor 3 of f and g . Since u and $u + 3$ are invertible, the prime factors of f, g, h must be of the form $x, x + 3$ and $x^2 + \alpha(x) - 2\beta(x) + 7$ (note that $x^2 + 2y - z + 7$ is irreducible for all $x, y, z \in X$). We have the relation

$$g - f = 3h.$$

If none of f, g, h has a factor of the form x then all of them have odd constant terms hence the relation cannot hold. Hence one of them has an x factor. Substitute 0 for x . The other two polynomials remain non-zero and relative primes and will have the same number of prime factors as before since (distinct) prime factors become (distinct) prime factors after the substitution as it can be easily checked. We obtain

$$f = g \text{ or } g = 3h \text{ or } f = -3h \pmod{x}.$$

From now on we consider the original polynomials again. In the first case f and g must equal ± 1 or ± 3 , which is clearly impossible. In the second resp. third case h must be unit. We can assume wlog that $h = 1$. Then $g = x + 3$ resp. $f = -x - 3$, i.e. $u = x$ resp. $u = -x - 3$.

For \mathbf{F}_\bullet , recall that the units of $\mathbf{F}_\bullet(X, \alpha, \beta)$ lie in $\mathbb{Z} \left[x, \frac{1}{x}, \frac{1}{x+3}, \underline{x}, \frac{1}{\underline{x}-x}, \frac{1}{\underline{x}-x+3}, \frac{1}{\underline{x}+x+1} : x \in X \right]$ (Corollary 3.4.3). Hence u and $u + 3$ are contained and are invertible in this ring, in which we are working from now on. Instead of \underline{x} , let us introduce new variables $\widehat{x} := \underline{x} - x$. Then the ring is $\mathbb{Z} \left[x, \frac{1}{x}, \frac{1}{x+3}, \widehat{x}, \frac{1}{\widehat{x}}, \frac{1}{\widehat{x}+3}, \frac{1}{\widehat{x}+2x+1} : x \in X \right]$. With the same argument as above, u and $u+3$ being invertible implies $u = y$ or $u = y + 3$ where $y = x$ or $y = \widehat{x}$ for some $x \in X$. \square

Lemma 3.6.2. *If $u, v, w, u + 3, v + 3, w + 3, u^2 + v - 2w + 7$ are invertible in $\mathbf{F}_+(X, \alpha, \beta)$ then there is an $x \in X$ such that $u = x, v = \alpha(x), w = \beta(x)$.*

Proof. By Lemma 3.6.1, there are $x, y, z \in X$ such that $u \in \{x, -x - 3\}, v \in \{y, -y - 3\}, w \in \{z, -z - 3\}$. Thus the constant term of $u^2 + v - 2w + 7$ is not divisible by 3 hence the polynomial is not divisible by t or $t + 3$ for any $t \in X$. So $u^2 + v - 2w + 7$ can only be invertible if $u^2 + v - 2w + 7 = \pm(t^2 + \alpha(t) - 2\beta(t) + 7)$ for some $t \in X$. Checking the second degree terms gives $t = x$ and the sign of the right-hand side is positive: $u^2 + v - 2w + 7 = x^2 + \alpha(x) - 2\beta(x) + 7$. Checking the constant terms gives $u = x, v = y, w = z$. Hence $y - \alpha(x) = 2(z - \beta(x))$. This can only hold if $y = \alpha(x)$ and $z = \beta(x)$. \square

Lemma 3.6.3. *If $u, u + 3, v, v + 3, u + 2v + 1$ are invertible in $\mathbf{F}_\bullet(X, \alpha, \beta)$ then $u = \underline{x} - x, v = x$ for some $x \in X$.*

Proof. As in Lemma 3.6.1, these elements are already in $\mathbb{Z} \left[x, \frac{1}{x}, \frac{1}{x+3}, \widehat{x}, \frac{1}{\widehat{x}}, \frac{1}{\widehat{x}+3}, \frac{1}{\widehat{x}+2x+1} : x \in X \right]$ and $u \in \{x, -x-3\}, v \in \{y, -y-3\}$ where $x, y \in X \cup \{\widehat{t} : t \in X\}$. Now $u + 2v + 1$ is a linear invertible polynomial. Checking the constant terms of $u + 2v + 1$ and all of the invertible linear polynomials gives $u = x, v = y, u + 2v + 1 = \widehat{t} + 2t + 1$ for some $t \in X$. Hence $u = \widehat{t}, v = t$. \square

Now we are able to prove that the functors are full. Let $f: \mathbf{F}_+(X, \alpha, \beta) \rightarrow \mathbf{F}_+(Y, \alpha, \beta)$ be a ring homomorphism preserving unit. Then it is identical on \mathbb{Z} . By Lemma 3.6.2, there is a unique mapping $g: X \rightarrow Y$ such that $f(x) = g(x), f(\alpha(x)) = \alpha(g(x)), f(\beta(x)) = \beta(g(x))$ for all $x \in X$. Obviously, g preserves α and β and $f = \mathbf{F}_+(g)$.

Let $f: \mathbf{F}_\bullet(X, \alpha, \beta) \rightarrow \mathbf{F}_\bullet(Y, \alpha, \beta)$ be a ring homomorphism preserving unit. Then it is identical on \mathbb{Z} . By Lemma 3.6.3, there is a mapping $g: X \rightarrow Y$ such that $f(x) = g(x), f(\underline{x}) = \underline{g(x)}$ for all $x \in X$. Now $\frac{g(x)+2g(\alpha(x))+4g(\beta(x))+1}{g(x)} = f\left(\frac{x+2\alpha(x)+4\beta(x)+1}{x}\right) \in \mathbf{F}_\bullet(Y, \alpha, \beta)$ implies by Lemma 3.4.3 that $g(x) + 2g(\alpha(x)) + 4g(\beta(x)) + 1 = g(x) + 2\alpha(g(x)) + 4\beta(g(x)) + 1$ and hence $g(\alpha(x)) = \alpha(g(x))$ and $g(\beta(x)) = \beta(g(x))$. Thus g is a homomorphism and clearly $f = \mathbf{F}_\bullet(g)$.

3.7 Proofs of the corollaries of the Main Theorem

Proof of Corollary 3.2.1. It is known (see [8]) that there are 2^κ mutually rigid algebras with κ elements in the category of universal algebras. \mathbf{F}_+ maps these algebras into mutually rigid κ -element UFDs with κ -rank free additive groups (see Lemma 3.5.1), κ primes and isomorphic groups of units (product of a two-element cyclic group and a κ -rank free abelian group). Hence their multiplicative semigroups are isomorphic. \square

Proof of Corollary 3.2.2. It is known (see [8]) that there are 2^κ algebras with two unary operations over a set of cardinality κ such that there is no morphism between distinct algebras and all of them have the *same* automorphism group (i.e. consisting of the same maps), which is isomorphic to G . Applying the functors \mathbf{F}_+ resp. \mathbf{F}_\bullet to this system of algebras, we obtain the required system of UFDs. \square

Proof of Corollary 3.2.3. The statement was proved for the category of $\mathbf{Alg}(1, 1)$ in Corollary 2.3. Applying either the functor \mathbf{F}_+ or \mathbf{F}_\bullet for the construction. Note that both of these functors induce an embedding between the lattice of subalgebras of every algebra and its image. So one gets the required UFD and embedding of lattices. \square

Bibliography

- [1] L. Babai, *Endomorphisms of sub- and factorsemigroups*, Algebraic theory of semigroups (Proc. Sixth Algebraic Conf., Szeged, 1976), North-Holland, Amsterdam, 1979, pp. 43–50.
- [2] Manfred Dugas and Rüdiger Göbel, *All infinite groups are Galois groups over any field*, Trans. Amer. Math. Soc. **304** (1987), no. 1, 355–384.
- [3] E. Fried, *Automorphism group of integral domains fixing a given subring*, Algebra Universalis **7** (1977), no. 3, 373–387.
- [4] E. Fried and J. Sichler, *Homomorphisms of commutative rings with unit element*, Pacific J. Math. **45** (1973), 485–491.
- [5] ———, *Homomorphisms of integral domains of characteristic zero*, Trans. Amer. Math. Soc. **225** (1977), 163–182.
- [6] ———, *On endomorphisms and automorphisms of monounary algebras*, Acta Sci. Math. (Szeged) **64** (1998), no. 1-2, 13–36.
- [7] J. Kollár, *Some subcategories of integral domains*, J. Algebra **54** (1978), no. 2, 329–331.
- [8] Aleš Pultr and Věra Trnková, *Combinatorial, algebraic and topological representations of groups, semigroups and categories*, North-Holland Publishing Co., Amsterdam, 1980.
- [9] J. Sichler and V. Koubek, *Endomorphism monoids of chained graphs*, (not published yet), 2000.
- [10] P. Vopěnka, A. Pultr, and Z. Hedrlín, *A rigid relation exists on any set*, Comment. Math. Univ. Carolinae **6** (1965), 149–155.