The kernel of a monoid morphism

Jean-Éric Pin[1]

[1]LIAFA, CNRS and University Paris Diderot

November 2011, York

Outline

Basic definitions

An element e of a semigroup is idempotent if $e^2 = e$. The set of idempotents of a semigroup S is denoted by $E(S)$.

A semigroup is idempotent if each of its elements is idempotent (that is, if $E(S) = S$). A semilattice is a commutative and idempotent monoid.

A variety of finite monoids is a class of finite monoids closed under taking submonoids, quotient monoids and finite direct products.

Part I

Kernels and extensions

The kernel of a group morphism

Let $\pi : H \to G$ be a surjective group morphism.
The kernel of π is the group

$$T = \mathrm{Ker}(\pi) = \pi^{-1}(1)$$

and H is an extension of G by T.

The synthesis problem in finite group theory consists in constructing H given G and T.

The kernel of a group morphism

Let $\pi : H \to G$ be a surjective group morphism.
The kernel of π is the group

$$T = \mathrm{Ker}(\pi) = \pi^{-1}(1)$$

and H is an extension of G by T.

The synthesis problem in finite group theory consists in constructing H given G and T.

- Is there a similar theory for semigroups?

A specific example

A monoid M is an extension of a group by a semilattice if there is a surjective morphism π from M onto a group G such that $\pi^{-1}(1)$ is a semilattice.

- How to characterize the extensions of a group by a semilattice?
- Is there a synthesis theorem in this case?
- In the finite case, what is the variety generated by the extensions of a group by a semilattice?

The difference between semigroups and groups

Let $\pi : H \to G$ be a surjective group morphism and let $K = \pi^{-1}(1)$. Then $\pi(h_1) = \pi(h_2)$ iff $h_1 h_2^{-1} \in K$.

If $\pi : M \to G$ be a surjective monoid morphism and $K = \pi^{-1}(1)$, there is in general no way to decide whether $\pi(m_1) = \pi(m_2)$, given K.

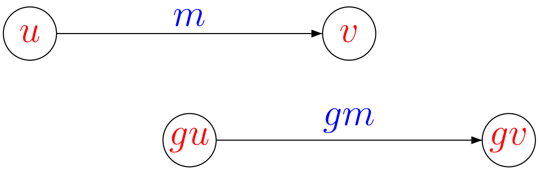
For this reason, the notion of a kernel of a monoid morphism has to be stronger...

The kernel category of a morphism

Let G be a group and let $\pi : M \to G$ be a surjective morphism. The kernel category $Ker(\pi)$ of π has G as its object set and for all $g, h \in G$

$$\mathrm{Mor}(u, v) = \{(u, m, v) \in G \times M \times G \mid u\pi(m) = v\}$$

Note that $\mathrm{Mor}(u, u)$ is a monoid equal to $\pi^{-1}(1)$ and that G acts naturally (on the left) on $Ker(\pi)$:



A first necessary condition

Proposition

Let π be a surjective morphism from a monoid M onto a group G such that $\pi^{-1}(1)$ is a semilattice. Then $\pi^{-1}(1) = E(M)$ and the idempotents of M commute.

Proof. As $\pi^{-1}(1)$ is a semilattice, $\pi^{-1}(1) \subseteq E(M)$. If e is idempotent, then $\pi(e)$ is idempotent and therefore is equal to 1. Thus $E(M) \subseteq \pi^{-1}(1)$. □

A second necessary condition

Let M be a monoid with commuting idempotents.

- It is E-unitary if for all $e, f \in E(M)$ and $x \in M$, one of the conditions $ex = f$ or $xe = f$ implies that x is idempotent.
- It is E-dense if, for each $x \in M$, there are elements x_1 and x_2 in M such that x_1x and xx_2 are idempotent.

Note that any finite monoid is E-dense, since every element has an idempotent power. But $(\mathbb{N}, +)$ is not E-dense since its unique idempotent is 0.

A second necessary condition (2)

Proposition

Let π be a surjective morphism from a monoid M onto a group G such that $\pi^{-1}(1) = E(M)$. Then M is E-unitary dense.

Proof. If $ex = f$ then $\pi(e)\pi(x) = \pi(f)$, that is $\pi(x) = 1$. Thus $x \in E(M)$ and M is E-unitary.

Let $x \in M$ and let $g = \pi(x)$. Let $\bar{x}$ be such that $\pi(\bar{x}) = g^{-1}$. Then $\pi(\bar{x}x) = 1 = \pi(x\bar{x})$. Therefore $\bar{x}x$ and $x\bar{x}$ are idempotent. Thus M is E–dense. □

The fundamental group $\pi_1(M)$

Let $F(M)$ be the free group with basis M. Then there is a natural injection $m \to (m)$ from M into $F(M)$. The fundamental group $\pi_1(M)$ of M is the group with presentation

$$\langle M \mid (m)(n) = (mn) \text{ for all } m, n \in M \rangle$$

Fact. If M is an E-dense monoid with commuting idempotents, then $\pi_1(M)$ is the quotient of M by the congruence $\sim$ defined by $u \sim v$ iff there exists an idempotent e such that $eu = ev$.

Characterization of extensions of groups

Theorem (Margolis-Pin, J. Algebra 1987)

Let M be a monoid whose idempotents form a subsemigroup. TFCAE:

(1) *there is a surjective morphism $\pi : M \to G$ onto a group G such that $\pi^{-1}(1) = E(M)$,*

(2) *the surjective morphism $\pi : M \to \Pi_1(M)$ satisfies $\pi^{-1}(1) = E(M)$,*

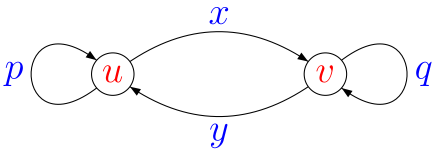
(3) *M is E-unitary dense.*

Part II

The synthesis theorem

Categories

Notation: u and v are objects, x, y, p, q, $p+x$, $p+x+y$ are morphisms, p, q, $x+y$, $y+x$ are loops.



For each object u, there is a loop 0_u based on u such that, for every morphism x from u to v, $0_u + x = x$ and $x + 0_v = x$.

The local monoid at u is the monoid formed by the loops based on u.

Groups acting on a category (1)

An action of a group G on a category C is given by a group morphism from G into the automorphism group of C. We write gx for the result of the action of $g \in G$ on an object or morphism x. Note that for all $g \in G$ and $p, q \in C$:

- $g(p + q) = gp + gq$,
- $g0_u = 0_{gu}$.

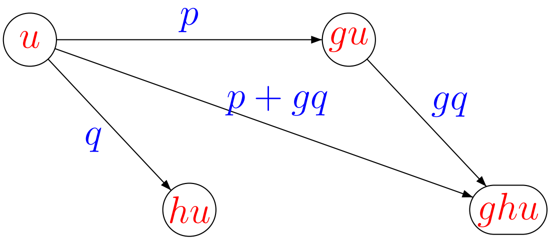
The group G acts freely on C if $gx = x$ implies $g = 1$. It acts transitively if the orbit of any object of C under G is $\mathrm{Obj}(C)$.

The monoid C_u

Let G be a group acting freely and transitively on a category C. Let u be an object of C and let

$$C_u = \{(p, g) \mid g \in G, p \in \mathrm{Mor}(u, gu)\}$$

Then C_u is a monoid under the multiplication defined by $(p, g)(q, h) = (p + gq, gh)$.



A property of he monoid C_u

Proposition

Let G be a group acting freely and transitively on a category. Then for each object u, the monoid C_u is isomorphic to C/G.

The synthesis theorem

Theorem (Margolis-Pin, J. Algebra 1987)

Let M be a monoid. The following conditions are equivalent:

(1) *M is an extension of a group by a semilattice,*

(2) *M is E-unitary dense with commuting idempotents,*

(3) *M is isomorphic to C/G, where G is a group acting freely and transitively on a connected, idempotent and commutative category.*

The covering theorem

Let M and N be monoids with commuting idempotents. A cover is a surjective morphism $\gamma : M \to N$ which induces an isomorphism from $E(M)$ to $E(N)$.

Theorem (Fountain, 1990)

Every E-dense monoid with commuting idempotents has an E-unitary dense cover with commuting idempotents.

Part III

The finite case

Closure properties

Proposition

The class of extensions of groups by semilattices is closed under taking submonoids and direct product.

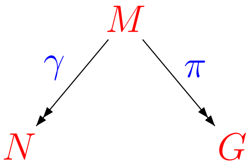
Proof. Let π be a surjective morphism from a monoid M onto a group G such that $\pi^{-1}(1)$ is a semilattice. If N be a submonoid of M, then $\pi(N)$ is a submonoid of G and hence is group H. Thus N is an extension of H and $\pi^{-1}(1) \cap N$ is a semilattice.

Direct products: easy. □

Variety generated by finite extensions

Let **V** be the variety generated by extensions of groups by semilattices.

A monoid belongs to **V** iff it is a quotient of an extension of a group by a semilattice.



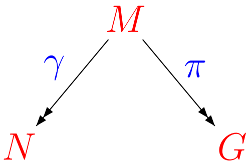
$$\pi^{-1}(1) = E(M)$$

The monoid N belongs to **V**.

Variety generated by finite extensions

Let **V** be the variety generated by extensions of groups by semilattices.

A monoid belongs to **V** iff it is a quotient of an extension of a group by a semilattice.



$$\pi^{-1}(1) = E(M)$$

The monoid N belongs to **V**.

- This diagram is typical of a relational morphism.

Relational morphisms

Let M and N be monoids. A relational morphism from M to N is a map $\tau : M \to \mathcal{P}(N)$ such that:

(1) $\tau(s)$ is nonempty for all $s \in M$,

(2) $\tau(s)\tau(t) \subseteq \tau(st)$ for all $s, t \in M$,

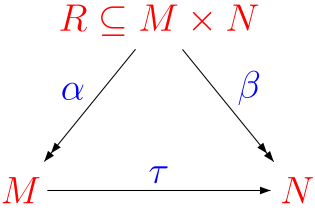
(3) $1 \in \tau(1)$.

Examples of relational morphisms include:

- Morphisms
- Inverses of surjective morphisms
- The composition of two relational morphisms

Graph of a relational morphism

The graph R of τ is a submonoid of $M \times N$. Let $\alpha : R \to M$ and $\beta : R \to N$ be the projections. Then α is surjective and $\tau = \beta \circ \alpha^{-1}$.



$$\alpha(m, n) = m \qquad \tau(m) = \beta(\alpha^{-1}(m))$$
$$\beta(m, n) = n \qquad \tau^{-1}(n) = \alpha(\beta^{-1}(n))$$

An example of relational morphism

Let Q be a finite set. Let $S(Q)$ the symmetric group on Q and let $I(Q)$ be the monoid of all injective partial functions from Q to Q under composition.

Let $\tau : I(Q) \to S(Q)$ be the relational morphism defined by $\tau(f) = \{\text{Bijections extending } f\}$

	1	2	3	4
f	3	-	2	-
h_1	3	1	2	4
h_2	3	4	2	1

$$\tau(f) = \{h_1, h_2\}$$

Relational morphisms

Proposition

Let $\tau : M \to N$ be a relational morphism. If T is a subsemigroup of N, then

$$\tau^{-1}(T) = \{x \in M \mid \tau(x) \cap T \neq \emptyset\}$$

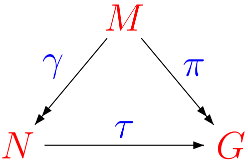
is a subsemigroup of M.

In our example, $\tau^{-1}(1)$ is a semilattice since

$$\begin{aligned}\tau^{-1}(1) &= \{f \in I(Q) \mid \text{the identity extends } f\} \\ &= \{\text{subidentities on } Q\} \equiv (\mathcal{P}(Q), \cap)\end{aligned}$$

Finite extensions and relational morphisms

A monoid belongs to **V** iff it is a quotient of an extension of a group by a semilattice.



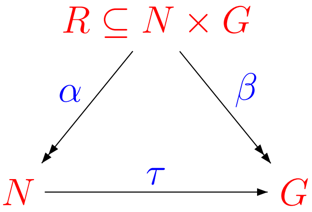
$\pi^{-1}(1)$ semilattice
$\gamma(\pi^{-1}(1))$ semilattice

Proposition

*A monoid N belongs to **V** iff there is a relational morphism τ from N onto a group G such that $\tau^{-1}(1)$ is a semilattice.*

Finite extensions and relational morphisms (2)

Consider the canonical factorization of τ:



Then α induces a isomorphism from $\beta^{-1}(1)$ onto $\tau^{-1}(1)$ since

$$\beta^{-1}(1) = \{(n, 1) \in R \mid 1 \in \tau(n)\}$$
$$\tau^{-1}(1) = \{n \in N \mid 1 \in \tau(n)\}$$

A noneffective characterization

Theorem (Margolis-Pin, J. Algebra 1987)

Let N be a finite monoid. TFCAE

(1) N *belongs to* **V**,

(2) N *is a quotient of an extension of a group by a semilattice,*

(3) N *is covered by an extension of a group by a semilattice,*

(4) *there is a relational morphism* τ *from* N *onto a group* G *such that* $\tau^{-1}(1)$ *is a semilattice.*

The finite covering theorem

Theorem (Ash, 1987)

Every finite monoid with commuting idempotents has a finite E-unitary cover with commuting idempotents.

Corollary

The variety $\mathbf{V}$ *is the variety of finite monoids with commuting idempotents.*

Part IV

Group radical

Group radical of a monoid

Let M be a finite monoid. The group radical of M is the set

$$K(M) = \bigcap_{\tau : M \to G} \tau^{-1}(1)$$

where the intersection runs over the set of all relational morphisms from M into a finite group.

Universal relational morphisms

Proposition

For each finite monoid M, there exists a finite group G and a relational morphism $\tau : M \to G$ such that $K(M) = \tau^{-1}(1)$.

Proof. There are only finitely many subsets of M. Therefore $K(M) = \tau_1^{-1}(1) \cap \cdots \cap \tau_n^{-1}(1)$ where $\tau_1 : M \to G_1, \ldots, \tau_n : M \to G_n$. Let $\tau : M \to G_1 \times \cdots \times G_n$ be the relational morphism defined by $\tau(m) = \tau_1(m) \times \cdots \times \tau_n(m)$. Then $\tau^{-1}(1) = K(M)$. $\square$

Another characterization of **V**

Theorem

Let M be a finite monoid. TFCAE:

(1) M *belongs to* **V**,

(2) $K(M)$ *is a semilattice*,

(3) *The idempotents of* M *commute and* $K(M) = E(M)$.

- Is there an algorithm to compute $K(M)$?

Ash's small theorem

Theorem (Ash 1987)

If M is a finite monoid with commuting idempotents, then $K(M) = E(M)$.

Corollary

The variety $\mathbf{V}$ is the variety of finite monoids with commuting idempotents.

Ash's theorem

Denote by $D(M)$ the least submonoid T of M closed under weak conjugation: if $t \in T$ and $a\bar{a}a = a$, then $at\bar{a} \in T$ and $\bar{a}ta \in T$.

Theorem (Ash 1991)

For each finite monoid M, one has $K(M) = D(M)$.

Corollary

One can effectively compute $K(M)$.

Part V

The topological approach

The pro-group topology

The pro-group topology on A^* [on $FG(A)$] is the least topology such that every morphism from A^* on a finite (discrete) group is continuous.

Proposition

Let L be a subset of A^* and $u \in A^*$. Then $u \in \overline{L}$ iff, for every morphism β from A^* onto a finite group G, $\beta(u) \in \beta(L)$.

A topological characterization of $K(M)$

Theorem (Pin, J. Algebra 1991)

Let $\alpha : A^* \to M$ *be surjective morphism. Then* $m \in K(M)$ *iff* $1 \in \overline{\alpha^{-1}(m)}$.

$$
\begin{aligned}
1 \in \overline{\alpha^{-1}(m)} &\iff \text{for all } \beta : A^* \to G, 1 \in \beta(\alpha^{-1}(m)) \\
&\iff \text{for all } \tau : M \to G, 1 \in \tau(m) \\
&\iff \text{for all } \tau : M \to G, m \in \tau^{-1}(1) \\
&\iff m \in K(M)
\end{aligned}
$$

Finitely generated subgroups of the free group

Theorem (M. Hall 1950)

Every finitely generated subgroup of the free group is closed.

Theorem (Ribes-Zalesskii 1993)

Let $H_1, \ldots, H_n$ be finitely generated subgroups of the free group. Then $H_1 H_2 \cdots H_n$ is closed.

Computation of the closure of a set

Theorem (Pin-Reutenauer, 1991 (mod R.Z.))

There is a simple algorithm to compute the closure of a given rational subset of the free group.

Theorem (Pin, 1991 (mod P.R.))

There is a simple algorithm to compute the closure of a given rational language of the free monoid.

Another proof of Ash's theorem

Theorem (Pin, 1988)

Given the simple algorithm to compute the closure of a rational language, one has $K(M) = D(M)$.

Therefore, Ribes-Zalesskii's theorem gives another proof of Ash's theorem.

Theorem

Given a decidable variety $\mathbf{V}$*, the variety generated by* $\mathbf{V}$*-extensions of groups is decidable.*