The Perils of Taking Shortcuts: Embedding Semigroups in the 1930s

Christopher Hollings

Mathematical Institute, University of Oxford

NBSAN, Manchester, 30th August 2011

The problem

Let S be a cancellative semigroup. We seek to embed (or immerse) S in some group G, i.e., to find an isomorphic copy of S inside G.

Alternatively, we seek to extend S to a group through the adjunction of additional elements.

Seek (necessary and/or sufficient) conditions for a cancellative semigroup to be embeddable in a group.

Important fact: even a cancellative semigroup may not, in general, be embedded in a group.

Timeline

1910: some ingredients provided by Steinitz.

1930: van der Waerden poses a related problem.

1931: Ore finds a sufficient condition.

1935: Sushkevich goes awry.

1937: Maltsev shows that it's not quite so simple...

1939: Maltsev gives necessary and sufficient conditions.

1940: Maltsev's follow-up.

1940s: sufficient conditions studied by Dubreil and others.

1949: Pták's group-theoretic approach.

1951: Lambek's geometrical approach.

Steinitz

Ernst Steinitz (1871–1928)

Algebraische Theorie der Körper (1910).

Defined field of fractions of integral domain.

Field of fractions

Any integral domain may be embedded in a field (namely, its field of fractions).

Easily adapted to show that any commutative cancellative semigroup may be embedded in a group.

van der Waerden

B. L. van der Waerden (1903–1996)

Moderne Algebra (1930).

Notes that any integral domain may be embedded in a field, but indicates that the problem is unsolved in the non-commutative case: can a non-commutative ring without zero divisors be embedded in a skew field? (‘van der Waerden’s problem’)

Sushkevich

Anton Kazimirovich Sushkevich (1889–1961)

On the extension of a semigroup to a whole group (1935).

‘Proved’ that any cancellative semigroup can be embedded in a group.

Group and principal parts

Über Semigruppen (1934).

Decompose cancellative semigroup $\mathfrak{S}$ as:

$$\mathfrak{S} = \mathfrak{G} \cup \mathfrak{H},$$

where

$\mathfrak{G}$ is the group part (group of units), and

$\mathfrak{H}$ is the principal part (two-sided ideal of non-invertible elements).

$$\mathfrak{G} \neq \emptyset \iff \mathfrak{S} \text{ has an identity.}$$

Extension of $\mathfrak{S}$ in the $\mathfrak{G} = \emptyset$ case

$\mathfrak{S} = \mathfrak{H}$

For each $X \in \mathfrak{H}$, introduce new element $\overline{X}$; denote collection of all such by $\overline{\mathfrak{H}}$; $\overline{Q}\,\overline{P} = \overline{R}$ whenever $PQ = R$.

Introduce new element E, defined to be a two-sided identity for both $\mathfrak{H}$ and $\overline{\mathfrak{H}}$; also: $X\overline{X} = \overline{X}X = E$.

Form products: $P\overline{Q}$, $\overline{P}Q$, $P\overline{Q}R$, $\overline{P}Q\overline{R}$, $P\overline{Q}R\overline{S}$, $\overline{P}Q\overline{R}S, \ldots$

Then (Sushkevich claims)

$$\mathfrak{H}_1 = \{\text{products}\} \cup \mathfrak{H} \cup \overline{\mathfrak{H}} \cup \{E\}$$

is a group...

Extension of $\mathfrak{S}$ in the $\mathfrak{G} \neq \emptyset$ case

$\mathfrak{S} = \mathfrak{G} \cup \mathfrak{H}$

Apply previous construction to $\mathfrak{H}$ to obtain 'group' $\mathfrak{H}_1$.

Set out to combine $\mathfrak{H}_1$ and $\mathfrak{G}$: try to form group from their union.

Must identify identities of $\mathfrak{H}_1$ and $\mathfrak{G}$.

Need to determine products of elements from $\mathfrak{G}$ with those from $\overline{\mathfrak{H}}$.

Extension of $\mathfrak{S}$ in the $\mathfrak{G} \neq \emptyset$ case

Take $A \in \mathfrak{G}$ and $P, Q, R \in \mathfrak{H}$:

$$A\overline{P} = \overline{Q}, \text{ if } PA^{-1} = Q$$

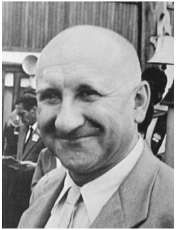
$$\overline{P}A = \overline{R}, \text{ if } A^{-1}P = R$$

It follows that $A = \overline{Q}P = P\overline{R} \in \mathfrak{H}_1$.

Given any $A \in \mathfrak{G}$ and any $P \in \mathfrak{H}$, can always find appropriate $Q, R \in \mathfrak{H}$. Thus $\mathfrak{G} \subseteq \mathfrak{H}_1$.

$\mathfrak{S} = \mathfrak{G} \cup \mathfrak{H}$ is therefore extended to $\mathfrak{H}_1$ in this case also.

Kurosh



Aleksandr Gannadievich Kurosh (1908–1971)

Wrote review of Sushkevich's paper for
Zentralblatt für Mathematik und ihre Grenzgebiete

Notes that Sushkevich does not prove adequately that the multiplication in $\mathfrak{H}_1$ is associative and well-defined — "certainly not trivial".

Extension of $\mathfrak{S}$ in the $\mathfrak{G} = \emptyset$ case

$\mathfrak{S} = \mathfrak{H}$

For each $X \in \mathfrak{H}$, introduce new element $\overline{X}$; denote collection of all such by $\overline{\mathfrak{H}}$; $\overline{Q}\,\overline{P} = \overline{R}$ whenever $PQ = R$.

Introduce new element E, defined to be a two-sided identity for both $\mathfrak{H}$ and $\overline{\mathfrak{H}}$; also: $X\overline{X} = \overline{X}X = E$.

Form products: $P\overline{Q},\ \overline{P}Q,\ P\overline{Q}R,\ \overline{P}Q\overline{R},\ P\overline{Q}R\overline{S},\ \overline{P}Q\overline{R}S, \ldots$

Then (Sushkevich claims)

$$\mathfrak{H}_1 = \{\text{products}\} \cup \mathfrak{H} \cup \overline{\mathfrak{H}} \cup \{E\}$$

is a group...

What did Sushkevich say about this?

Concerning associativity and well-definedness in $\mathfrak{H}_1$:

“This argument does not present any difficulties.”

Maltsev

Anatoly Ivanovich Maltsev (1909–1967)

On the immersion of an algebraic ring into a field (1937).

Provides negative solution to van der Waerden's problem, first dealing with the semigroup case, then building on this to obtain the ring case.

Condition Z

Maltsev writes down a necessary condition for a cancellative semigroup to be embedded in a group.

Condition Z:

$$(AX = BY,\ CX = DY,\ AU = BV) \Longrightarrow CU = DV.$$

(Suppose that a cancellative semigroup S may be embedded in a group G. Then

$$B^{-1}A = YX^{-1},\ D^{-1}C = YX^{-1},\ B^{-1}A = VU^{-1},$$

whence $D^{-1}C = VU^{-1}$, or $CU = DV$.)

A semigroup not satisfying condition Z

Take $S = \{a, b, c, d, x, y, u, v\}^+$ and identify the following pairs of words:

$$ax \leftrightarrow by, \quad cx \leftrightarrow dy, \quad au \leftrightarrow bv.$$

'Elementary transformation': replace pair of letters in given word by corresponding pair.

Call words α, β equivalent ($\alpha \sim \beta$) if can get from α to β via a finite sequence of elementary transformations.

$\sim$ is in fact a congruence. Put $\mathfrak{H} = S/{\sim}$.

A semigroup not satisfying condition Z

$\mathfrak{H}$ is a cancellative semigroup which does not satisfy condition Z:

$(a)(x) = (b)(y), (c)(x) = (d)(y)$ and $(a)(u) = (b)(v)$, but $(c)(u) \neq (d)(v)$.

Thus $\mathfrak{H}$ may not be embedded in a group.

Finally constructs ring $\mathfrak{R}$ with $\mathfrak{H}$ as multiplicative semigroup:

$$\mathfrak{R} = \left\{ \sum_i k_i X_i : X_i \in \mathfrak{H},\ k_i \in \mathbb{Q},\ \text{only finite number of } k_i \neq 0 \right\}.$$

Thus $\mathfrak{R}$ may not be embedded in a skew field, thereby giving a negative solution to van der Waerden's problem.

Necessary and sufficient conditions

“We have also found the necessary and sufficient conditions for the possibility of immersion of a semigroup into a group. However these are too complicated to be included in this paper.”

Appeared later, in paper of 1939.

See: Clifford and Preston, volume II, §12.6.

Or: George Clark Bush, *On embedding a semigroup in a group*, PhD thesis, Queen’s University, Kingston, Ontario, 1961.

(Necessary and sufficient conditions are countably infinite in number (1939), and no finite subset will suffice (1940).)

Back to Sushkevich

Reproduced much of his earlier material in 1937 monograph *Theory of generalised groups*, including ‘proof’ of well-definedness.

Acknowledges Maltsev’s counterexample, and yet still tries to obtain embedding in $\mathfrak{G} \neq \emptyset$ case...

May eventually have acknowledged his mistake because tried to disown (?) his 1935 paper — missing from publications lists.

Moscow, 1939

All-Union Conference on Algebra, Moscow, 13th–17th November 1939.

Afternoon session of 16th November:

- A. K. Sushkevich, *On a type of generalised group*.
- A. I. Maltsev, *On extensions of associative systems*.

The End