Group conjugation has non-trivial LD-identities

Aleš Drápal, Tomáš Kepka, Michal Musílek

Abstract. We show that group conjugation generates a proper subvariety of left distributive idempotent groupoids. This subvariety coincides with the variety generated by all cancellative left distributive groupoids.

Keywords: left distributivity, free group

Classification: 20N02, 20A99

Given a group G, define an operation $*$ on G by $x * y = xyx^{-1}$. $G(*)$ is an idempotent left distributive groupoid (i.e. $x * x = x$ and $x * (y * z) = (x * y) * (x * z)$ for any $x, y, z \in G$). It has been an open question, whether a non-trivial free idempotent groupoid occurs as a subgroupoid of $G(*)$ for some group G, particularly for G free. One easily verifies that

$$((x * y) * y) * x = (x * y) * ((y * x) * x) \tag{†}$$

holds in any group G.

We present here two left distributive idempotent groupoids on four elements which do not satisfy (†):

$*$	1	2	3	4
1	1	2	4	3
2	1	2	4	3
3	4	4	3	1
4	3	3	1	4

$*$	1	2	3	4
1	1	2	3	4
2	2	2	4	4
3	1	1	3	3
4	1	2	3	4

To see that the identity (†) does not hold, put $x = 2$ and $y = 3$, in both cases.

Note that our result contrasts with an older result of Pierce [4], by which free left distributive idempotent groupoids satisfying $x * (x * y) = y$ can be obtained as subgroupoids of $G(*)$, if the group G is freely generated by involutions.

The presented groupoids have been found by a brute-force computer search. Each of these groupoids has just one non-trivial automorphism, and hence on the set $\{1, 2, 3, 4\}$ there exist 24 groupoids isomorphic to one of them. There are 2183 different idempotent left distributive groupoids on a four-element set, and these groupoids fall into 141 isomorphism classes. The above examples represent the only classes, in which the identity (†) does not hold.

A groupoid $A(*)$ is said to be left (right) cancellative, if $a*b = a*c$ ($b*a = c*a$) implies $b = c$ for any $a, b, c \in A$. If a groupoid is both left and right cancellative, it is called cancellative.

In every idempotent left distributive groupoid $A(*)$ the elastic law $x*(y*x) = (x*y)*x$ holds and we have

$$
\begin{aligned}
&(((x*y)*y)*(x*y))*(((x*y)*y)*x) = \\
&\qquad ((x*y)*y)*((x*y)*x) = (x*y)*(y*x) = \\
&\qquad (x*y)*((y*x)*(y*x)) = (x*y)*(((y*x)*y)*((y*x)*x)) = \\
&\qquad ((x*y)*(y*(x*y)))*((x*y)*((y*x)*x)) = \\
&(((x*y)*y)*(x*y))*((x*y)*((y*x)*x))
\end{aligned}
$$

for any $x, y \in A$.

Denote by $W(X)$ the absolutely free groupoid of terms with a base X and by $\sim$ the congruence of $W(X)$ induced by the left distributive and idempotent laws. Then $W(X)/\!\sim$ is a free left distributive idempotent groupoid. We have proved:

Proposition 1. *If* $\operatorname{card}(X) \geq 2$, *then* $W(X)/\!\sim$ *is not left cancellative.*

For terms $t_1, t_2, \dots, t_k \in W(X)$ write $t_1 t_2 \dots t_k$ in place of $t_1(t_2(\dots t_k))$ and define a relation $\approx$ on $W(X)$ by

$$s \approx t \quad \Longleftrightarrow \quad a_1 a_2 \dots a_k s \sim a_1 a_2 \dots a_k t$$

for some $a_1, a_2, \dots, a_k \in W(X)$.

Proposition 2. *The relation* $\approx$ *is a congruence of* $W(X)$ *and* $W(X)/\!\approx$ *is left cancellative. Moreover,* $W(X)/\!\approx$ *is free in the variety generated by all left cancellative left distributive idempotent groupoids.*

Proof: Note that we have $b_1 \dots b_r a_1 \dots a_k t \sim (b_1 \dots b_r a_1) \dots (b_1 \dots b_r a_k)$ $(b_1 \dots b_k t)$ for any $b_1, \dots, b_r, a_1, \dots, a_k, t \in W(X)$. Therefore if $a_1 \dots a_k r \sim a_1 \dots a_k s$ and $b_1 \dots b_m s \sim b_1 \dots b_m t$ hold, then $b_1 \dots b_m a_1 \dots a_k r \sim b_1 \dots b_m a_1 \dots a_k s \sim (b_1 \dots b_m a_1) \dots (b_1 \dots b_m a_k)(b_1 \dots b_m s) \sim (b_1 \dots b_m a_1) \dots (b_1 \dots b_m a_k)$ $(b_1 \dots b_m t) \sim b_1 \dots b_m a_1 \dots a_k t$ holds as well. This proves that $\approx$ is an equivalence. To prove it is a congruence, one proceeds in a similar manner.

$W(X)/\!\approx$ is thus idempotent, left distributive and left cancellative. If $A = A(\cdot)$ is another left cancellative idempotent left distributive groupoid and $\varphi : W(X) \to A$ is a homomorphism, then $a_1 \dots a_k s \sim a_1 \dots a_k t$ implies $\varphi(a_1) \dots \varphi(a_k)\varphi(s) = \varphi(a_1) \dots \varphi(a_k)\varphi(t)$. As A is left cancellative, we obtain $\varphi(s) = \varphi(t)$, and we see that $\ker \varphi$ contains $\approx$. □

Let V_g be the variety generated by all groupoids $G(*)$ for G a group and $*$ the conjugation. Further, let V_c denote the variety generated by all cancellative left distributive groupoids. From $x*(x*x) = (x*x)*(x*x)$ it follows that every right cancellative groupoid is idempotent, and hence V_c contains only idempotent groupoids.

It is not complicated to prove that V_g and V_c coincide. However, first we shall describe a generator of V_g.

For a free group $F = F(X)$ with a base X, denote $F_0 = F_0(X)$ the subgroupoid of $F(*)$ generated by X.

Proposition 3. *Let $F = F(x, y)$ be the free group with two generators. Then the groupoid $F_0(*)$ generates the variety V_g.*

Proof: The set of all $y^i x y^{-i}$, $i \geq 0$, is a free base of a subgroup it generates, and belongs to F_0. Hence it suffices to prove that $F_0(X)$ generates V_g for a countable infinite set $X = \{x_1, x_2, \dots\}$. We shall show that if a $*$-identity $t(y_1, \dots, y_k) = s(y_1, \dots, y_k)$ is not satisfied in a group G, it does not hold also in $F_0(X)$. Let $g_1, \dots, g_k \in G$ be such that $t(g_1, \dots, g_k) \neq s(g_1, \dots, g_k)$ and consider a group homomorphism $\varphi : F(X) \to G$ with $\varphi(x_i) = g_i$ for $1 \leq i \leq k$. Then $\psi = \varphi \restriction F_0(X)$ is a homomorphism of $F_0(X)$ into $G(*)$ and hence $t(x_1, \dots, x_k) \neq s(x_1, \dots, x_k)$. □

From the proof of the above proposition we also obtain:

Corollary. *$F_0(X)$ is free in V_g for any nonempty base X.*

Proposition 4. *$F_0(X)$ is a right cancellative groupoid for any nonempty set X.*

Proof: Every $a \in F_0(X)$ is a conjugate of some $x \in X$. Hence a cannot be a non-trivial positive power of any $u \in F(X)$. If $a, b, c \in F_0(X)$ are such that $b * a = c * a$, then $c^{-1}b$ and a commute in $F(X)$. Hence $c^{-1}b$ and a are powers of some element $v \in F(X)$. But then $a = v^{\pm 1}$, and we can assume $a = v$. As the sum of all exponents is zero in $c^{-1}b$ and it is i in a^i, we see that $c = b$. □

Proposition 5. *The varieties V_g and V_c coincide.*

Proof: $V_g \subseteq V_c$ by Propositions 3 and 4. Let $A(*) \in V_c$ and suppose first that the left translations of A (i.e. the mappings $L_a : b \to a * b$) are permutations — such groupoids are often called left quasigroups. By a well known and easy construction, the mapping $a \to L_a$ is a homomorphism of $A(*)$ into $G(*)$, where G is the group generated by $\{L_a; a \in A\}$. Now, every left cancellative idempotent LD-groupoid can be embedded into a left distributive idempotent left quasigroup [2, Proposition 2.10]. If A is cancellative, then for $a \in A$ the mapping $a \to L_a$ is faithful, and hence A is in V_g. □

Denote by V the variety of all idempotent LD-groupoids and by V_l (V_r) its subvariety generated by all left (right) cancellative groupoids. We have $V_g \subseteq V_l \subsetneq V$ and $V_g \subseteq V_r \subseteq V$. It seems to be an open problem which of the indicated inclusions are proper ones. We conjecture that V_g equals V_l and V_r coincides with V.

The free non-idempotent groupoids have received a lot of interest recently (for example, see [1] and [3]). We hope that this short contribution will help to focus interest also to the idempotent case.

The authors were recently informed that the identity (†), the respective four-element groupoids and the Propositions 1 and 2 were found out independently by Larue [5], [6]. Note also that the congruence $\approx$ appears already in [2].

References

[1] Dehornoy P., *Braid groups and left distributive structures*, Transactions AMS, to appear.
[2] Kepka T., *Notes on left distributive groupoids*, Acta Univ. Carolinae - Math. et Ph. **22** (1981), 23–37.
[3] Laver R., *The left distributive law and the freeness of an algebra of elementary embeddings*, Advances in Mathematics **91** (1992), 209–231.
[4] Pierce R.S., *Symmetric groupoids*, Osaka J. Math. **15** (1978), 51–76.
[5] Larue D.M., Unpublished notes, 1992.
[6] ———, Ph. D. Thesis, University of Colorado, 1994.

Aleš Drápal and Tomáš Kepka
Faculty of Mathematics and Physics, Charles University, Sokolovská 83,
186 00 Praha 8, Czech Republic

Michal Musílek
U plovárny 1415, 504 01 Nový Bydžov, Czech Republic

(*Received* November 15, 1993)