Prace Naukowe Wyższej Szkoły Pedagogicznej w Częstochowie

Matematyka VIII, Częstochowa 2000 - 2001

Left Distributive Groupoids, Large Cardinals, and Laver Tables

Petr Němec

1. Introduction

Non-associative, or more particularly selfdistributive structures can arise quite naturally in many different settings. Recall that a groupoid $G(*)$ (i. e., a non-empty set G equipped with one binary operation $*$) is said to be *left distributive* if it satisfies the identity

$$x*(y*z)=(x*y)(x*z).$$

Similarly, $G(*)$ is *right distributive* if it satisfies the identity $(x*y)*z=(x*z)*(y*z)$.

Natural examples of left distributive groupoids are weighted mean of real numbers defined by $x*y=\alpha x+(1-\alpha y)$, where $0<\alpha<1$ (this groupoid is also right distributive), or conjugation in a group defined by $x*y=xyx^{-1}$. Both these examples are also *idempotent*, i. e., satisfy the identity $x*x=x$.

It is natural to ask whether there are left distributive groupoids which are (in a certain sense) "far from idempotence". Rather surprisingly, there is an intimate connection with Set Theory, namely with axioms concerning large cardinals. More precisely, under the assumption of their existence, the set of all non-projective elementary embeddings of a limit ordinal can be equipped with a left distributive operation having the required property.

The structure of left distributive groupoids is very complicated. Namely, already among left distributive groupoids generated by one element we can find extremely complicated combinatorial structures, so called *Laver tables* L_n, which are multiplication tables of left distributive groupoids on the set $\{1,2,\ldots,2^n\}$ with the first column prescribed by the rule

$$a*1\equiv(a+1)\bmod 2^n.$$

In this paper, we shall try to present a short survey of the topics and interconnections mentioned above. The first explicit allusion to selfdistributivity seems to appear in [13]. Looking at the pages 33 and 34 of the cited article, we can read the following comment on selfdistributivity: *"These are other cases of the distributive principle. ... These formulae, which have hitherto escaped notice, are not without interest."* Another early work which is worth mentioning is [15]. We can already see there (p. 249) a particular example of a non-associative (left and right) distributive groupoid G:

G	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

Of course, G is idempotent and commutative and, in fact, it is the smallest non-trivial Kirkman – Steiner triple system. It seems that the first article fully devoted to selfdistributivity is [1]. This paper deals with (left and right) distributive quasigroups. One-sided selfdistributive structures (namely left distributive quasigroups) appeared a bit later in [16]. Two-sided (generally non-idempotent) distributive groupoids were studied in [14] and, finally, non-idempotent left distributive groupoids in [8].

Idempotent (either one-sided or two-sided) selfdistributive groupoids are known to appear in many algebraic, geometrical, topological and combinatorial contexts and the theory of (two-sided) distributive groupoids is easily transferred to the idempotent case (see e.g. [7]).

On the other hand, the theory of non-idempotent left distributive groupoids (even of those possessing no idempotent elements) has its own flavour and some of these groupoids are of special interest because of their connections to more popular and fashionable objects like large cardinal numbers and braid groups.

The rôle of selfdistributivity in the Set Theory was more or less known for a long time (first results in this direction are due to P. Dehornoy) and the most important theorems were proved by R. Laver (see e.g. [10]). The relations to the braid groups were studied mainly by P. Dehornoy (see e.g. [2], [3] and [12]). An excellent detailed account of these connections is given in [4]. A survey of purely algebraic aspects of the theory of left distributive groupoids is presented in [6] and [9].

2. Large cardinals

Recall that a mapping $j : S \longrightarrow T$, S and T being sets with operations and relations of the same type, is said to be an *elementary embedding* if (somewhat roughly speaking) for any formula $F(x_1, \ldots)$ in the language of S and all $x_1, \ldots \in S$, $F(a_1, \ldots)$ is true in S iff $F(j(a_1), \ldots)$ is true in T. This obviously implies that j is an injective homomorphism for all operations and relations definable in S. Further, for any ordinal α, define inductively the set R_α by $R_0 = \emptyset$, $R_{\alpha+1} = P(R_\alpha)$ (the set of all subsets of R_α) and $R_\alpha = \cup_{\beta<\alpha} R_\beta$ for α limit. Further, denote by E_α the set of all non-projective elementary embeddings of R_α (with the relation $\in$) into itself (of course, the identity mapping on R_α is a projective elementary imbedding). If E_α is non-empty for some ordinal α then also E_λ is non-empty for the limit ordinal $\lambda = \text{card}(\alpha)$.

Suppose now that λ is a limit ordinal, $j \in E_\lambda$ is a non-projective elementary imbedding of R_α into itself and $\alpha = \text{crit}(j)$ is the least ordinal such that $j(\alpha) \neq \alpha$, so called *critical ordinal* of the elementary imbedding j. Let us remark here that the assumption of the existence of a non-projective elementary imbedding is a very strong "infinity" axiom, since in this case α is the α-th measurable cardinal.

2.1 Lemma. *Suppose that λ is a limit ordinal and E_λ is non-empty. Define*

$$j_1 * j_2 = \cup_{\gamma<\lambda} j_1(j_2 \mid R_\gamma)$$

for all $j_1, j_2 \in E_\lambda$. Then the operation $*$ is correctly defined and $E_\lambda(*)$ is a left distributive groupoid.

In [11], the following important result(so called Laver-Steel theorem) is proved:

2.2 Theorem. *In the situation of the preceding Lemma, if $j_1, j_2, \ldots \in E_\lambda$ are such that for every n there is x_n with $j_{n+1} = j_n * x_n$ then $\sup(\text{crit}(j_n)) = \lambda$.*

2.3 Corollary. *In E_λ, the following formula is true:*

$$(\forall x)\,(\forall n \geq 1)\,(\forall y_1, y_2, \ldots, y_n)\; x \neq (((x * y_1) * y_2) * \ldots) * y_n\,.$$

This means that the groupoid E_λ is as far from idempotency as possible. The Laver-Steel theorem was the first example of a left distributive groupoid with this "torsionfree" property, however this result used very strong set axioms. Later, it was shown (see e.g. [4]) that free left distributive groupoids have this property (moreover, a monogenic, i.e. generated by one element, left distributive groupoid is free iff it has this property). This was shown by a careful and complicated geometrical analysis of the extended braid group, already without any set axioms. Now, a relatively simple direct construction is possible (see e.g. [9]):

2.4 Lemma. *Let G be a group and $f \in \mathrm{End}(G)$, $a \in G$ be such that $af(a)a = f(a)af(a)$ and $af^2(x) = f^2(x)a$ for all $x \in G$. Define $x * y = xf(y)af(x)^{-1}$ for all $x, y \in G$. Then $G(*)$ is a left distributive groupoid.*

2.5 Theorem. *Let G be a group defined by generators and relations as*

$$G = \langle s_i, i \geq 1 \mid s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}, s_i s_j = s_j s_i \text{ for } |i - j| \neq 1 \rangle,$$

$a = s_1$ and $f(s_i) = s_{i+1}$ for all $i \geq 1$. Then $G(*)$, where $*$ is an operation defined in the preceding Lemma, satisfies the formula from 2.3.

3. Laver tables

Let us define a partial operation on the set $\{1, 2, \ldots, n\}$ by the following table:

S_n	1	2	. . .	n
1	2			
2	3			
.	.			
a	a+1			
.	.			
n-1	n			
n	1			

This means that the first column is prescribed by the rule

(1) $$a{*}1 \equiv (a{+}1) \bmod n\,.$$

3.1 Lemma. *For every $n \geq 1$, there is a unique operation on the set $\{1, 2, \ldots, n\}$ satisfying (1) and $a * (b * 1) = (a * b) * (a * 1)$ for all a, b. This groupoid will be denoted by S_n. Moreover, for all $a, b \in S_n$ we have the following properties: $n{*}b = b$, $a{*}b = 1$ for $a{*}(b{-}1) = n$ and $a{*}b > a{*}(b{-}1)$ otherwise, $(n-1) * b = n$, $(n-2) * b = n - 1$ for b odd and $(n-2) * b = n$ for b even.*

3.2 Theorem. *A left distributive groupoid $G(*)$ with the underlying set $\{1, 2, \ldots, n\}$ satisfying (1) exists iff $n = 2^k$ for some k. In this case, $G(*) \cong S_n$.*

These (uniquely defined) left distributive groupoids $L_n = S_{2^n}$ are called *Laver tables.* A good account of this topic can be found e.g. in [4]. Although the groupoids L_n are monogenic (every element is of the form

$((1*1)*\ldots$, i.e., the groupoid L_n is generated by the element 1) their combinatorial structure (of course, except the last three rows which are completely described in 3.1) is extremely complicated.

All rows of L_n are periodic and the period of the row corresponding to $a \in L_n$, which is (with respect to 3.1) equal to the number of different values in the row and also to the number $\min\{\, b \mid a * b = 2^n \,\}$, is a power of 2. Thus, for all positive integers $a \le n$, we can define the number $o_n(a)$ in such a way that $2^{o_n(a)}$ is the period of the row corresponding to a in the groupoid L_n. It is interesting that these finite objects have intimate connection to extremely large infinite cardinals.

All groupoids L_n are factors of E_λ (under the assumption $E_\lambda \neq \emptyset$). This correspondence may be used in both directions, e.g. it is possible to calculate critical ordinals of the iterations of an elementary imbedding j by means of groupoids L_n. In the other direction, we have e.g. the following result (see [4]):

3.3 Theorem. *If $E_\lambda \neq \emptyset$ then, for every positive integer a,*

$$\lim_{n\to\infty} o_n(a) = \infty\,.$$

However, it is an open problem whether, without the assumption of the existence of non-projective elementary imbedding, $o_n(1)$ tends to infinity. If so, this convergence must be extremely slow, which is indicated by the following result which does not require any set theoretic assumptions (see e.g. [5]):

3.4 Theorem. *If the period of 1 in L_n is 32 then $n \ge f_9(f_8(f_8(254)))$, where f_k are the Ackermann functions defined inductively by $f_0(n) = n+1$, $f_{k+1}(0) = f_k(1)$ and $f_{k+1}(n) = f_k(f_{k+1}(n-1))$ for all non-negative integers n, k.*

The rate of growth of Ackermann functions is extremely high, since the function $f_\omega(n) = f_n(n)$ grows faster than arbitrary primitively recursive function.

References

[1] C. Burstin, W. Mayer, *Distributive Gruppen von endlicher Ordnung*, J. reine und angew. Math. **160** (1929), 111–130.

[2] P. Dehornoy, *Sur la structure des gerbes libres*, C. R. Acad. Sci. Paris **309** (1989), 143–148.

[3] P. Dehornoy, *From large cardinals to braids via distributive algebra*, J. Knot Theory and Ramifications **4** (1995), 33–79.

[4] P. Dehornoy, *Braids and self-distributivity*, Université de Caen, Caen 1999.

[5] R. Dougherty, *Critical points in an algebra of elementary embeddings II*, In: Logic: From Foundations to Applications (W. Hughes, ed.), Oxford 1996, 103–136.

[6] J. Ježek, T. Kepka, *Selfdistributive groupoids. Part D1: Left distributive semigroups*, Université de Caen, Caen 1999.

[7] J. Ježek, T. Kepka, P. Němec, *Distributive groupoids*, Rozpravy ČSAV, Řada MPV **91**, Academia, Praha 1983.

[8] T. Kepka, *Notes on left distributive groupoids*, Acta Univ. Carolinae Math. Phys. **22**,2 (1981), 23–37.

[9] T. Kepka, P. Němec, *Selfdistributive groupoids. Part A1: Non-idempotent left distributive groupoids*, Université de Caen, Caen 1999.

[10] R. Laver, *The left distributive law and the freeness of an algebra of elementary embeddings*, Advances in Math. **91** (1992), 209–231.

[11] R. Laver, *On the algebra of elementary embeddings of a rank into itself*, Advances in Math. **110** (1995), 334–346.

[12] R. Lavr, *Braid group actions on left distributive structures and well-orderings in the braid group*, J. Pure Appl. Algebra **108** (1996), 81–98.

[13] C. S. Peirce, *On the algebra of logic*, Amer. Journal of Math. **III** (1880), 15–57.

[14] J.Ruedin, *Sur une décomposition des groupoïdes distributifs*, C.R. Acad. Sci. Paris **262** (1966), A985–A988.

[15] E. Schröder, *Über Algorithmen und Calculi*, Arch. der Math. und Phys., 2nd series, vol. **5** (1887), 225–278.

[16] M.Takasaki, *Abstractions of symmetric functions*, Tôhoku Math. J. **49** (1943), 143–207.

J.E.Purkyně University
České mládeže 8
400 96 Ústí nad Labem
Czech Republic