A NOTE ON UNISERIAL LOOPS

J. JEŽEK AND T. KEPKA

ABSTRACT. All ordinal numbers α with the following property are found: there exists a loop such that its subloops form a chain of ordinal type α.

By a *uniserial* loop (or any algebraic structure) we will mean a loop Q such that the lattice of subloops of Q is a chain.

The chain of subloops of a uniserial loop Q will be denoted by $\mathbf{Cs}(Q)$. The very first question that we can ask about uniserial loops is which chains are *representable*, i.e., (a definition local to this paper) isomorphic to $\mathbf{Cs}(Q)$ for a (uniserial) loop Q. This question will be answered in this paper completely only for those chains that are well ordered, i.e., isomorphic to an ordinal number. (An ordinal number is identified with the set of all smaller ordinal numbers, and is considered as a chain with respect to the usual ordering of ordinal numbers.)

The basic notions concerning loops can be found in the book [1].

Observation 1. There are many finite and also infinite loops without nontrivial proper subloops. These loops are trivially uniserial. Thus the one-element chain and the two-element chain are both representable.

Observation 2. Let Q be a uniserial loop. The chain $\mathbf{Cs}(Q)$ is an algebraic lattice, i.e., a complete lattice every element of which is the join of a set of compact elements. Consequently, $\mathbf{Cs}(Q)$ has the following property: whenever a, b are two elements such that $a < b$ then there exist elements c, d with $a \leq c < d \leq b$, such that c is covered by d. Also, the chain has both the least and the greatest elements; thus if it is isomorphic to an ordinal number α, then α is not a limit ordinal number.

Observation 3. As it is easy to see, every finitely generated subloop of a uniserial loop is one-generated. Thus a uniserial loop is finitely generated if and only if it is one-generated (then it is countable).

Observation 4. Let Q be a uniserial loop. It follows from the last two observations that every proper subloop P of Q is countable (i.e., $|P| \leq \aleph_0$). Consequently, $|Q| \leq \aleph_1$ and $|\mathbf{Cs}(Q)| \leq 2^{\aleph_1}$.

Observation 5. It is rather easy to see that the union of a chain of uniserial loops is a uniserial loop.

Key words and phrases. loop, subloop, chain, uniserial.

The work is a part of the research project MSM0021620839, financed by MSMT and partly supported by the Grant Agency of the Czech Republic, grant #201/09/0296.

Theorem 1. *Let $P = \{a_0, a_1, a_2, \dots\}$ be an infinite countable loop with the unit element a_0. Then there exists a countable loop Q with the following properties:*

(1) *P is a proper subloop of Q;*
(2) *Q is generated by any element of $Q \setminus P$;*
(3) *Q is uniserial, provided that P is uniserial;*
(4) *$ab = ba$ for all $a, b \in Q$ such that $\{a, b\} \nsubseteq P$;*
(5) *Q is commutative, provided that P is commutative.*

Proof. Take an infinite countable set $R = \{b_0, b_1, b_2, \dots\}$ disjoint with P and define multiplication on $Q = P \cup R$ (extending the multiplication of P) by means of induction and the following rules:

(a) $b_i b_i = b_{i+1}$ for all i;
(b) for $i \neq j$ let $b_i b_j = a_k$, where k is the least number such that $a_k \notin \{b_0 b_j, \dots, b_{i-1} b_j\} \cup \{b_i b_0, \dots, b_i b_{j-1}\}$;
(c) $a_i b_j = b_j a_i = b_k$, where k is the least number such that $b_k \notin \{b_{j+1}\} \cup \{a_0 b_j, \dots, a_{i-1} b_j\} \cup \{a_i b_0, \dots, a_i b_{j-1}\} \cup \{b_j a_0, \dots, b_j a_{i-1}\} \cup \{b_0 a_i, \dots, b_{j-1} a_i\}$.

Now, it is rather easy to check that Q enjoys the five properties. □

Theorem 2. *The following conditions are equivalent for an ordinal number α:*

(i) *There exists a uniserial loop Q with $\mathbf{Cs}((Q) \simeq \alpha$.*
(ii) *There exists a commutative uniserial loop Q with $\mathbf{Cs}((Q) \simeq \alpha$.*
(iii) *$1 \leq \alpha \leq \aleph_1 + 1$, where $\aleph_1 + 1$ is the ordinal successor of the least uncountable ordinal, and α is not a limit ordinal number.*

Proof. (i) implies (iii): Since $\mathbf{Cs}(Q)$ has the largest element, α is not a limit ordinal number. Suppose that $\alpha > \aleph_1 + 1$. Denote by R the subloop of Q corresponding to $\aleph_1$ and by S the subloop corresponding to $\aleph_1 + 1$. Then S is one-generated and thus countable. Consequently, R is also countable. Now, R is the union of the uncountable chain of its proper subloops. For every proper subloop P of R denote by P' the unique cover of P in the well ordered chain of proper subloops of R, and select an element $f(P)$ in $P' \setminus P$. Clearly, f is an injective mapping of the uncountable set of proper subloops of R into the countable set R, a contradiction.

(iii) implies (ii): For every countable ordinal number γ define a countable commutative uniserial loop Q_γ as follows. Let Q_0 be an arbitrary infinite commutative loop with no non-trivial proper subloops. If $\gamma = \beta + 1$, let Q_γ be obtained from Q_β in the way described by Theorem 1. If γ is a limit ordinal number, let Q_γ be the union of the chain of the loops Q_β with $\beta < \gamma$. Finally, let Q be the union of the chain of the loops Q_γ where γ runs over all countable ordinal numbers. Clearly, Q is a uniserial loop with $\mathbf{Cs}(Q) \simeq \aleph_1 + 1$ and every positive, countable non-limit ordinal number is isomorphic to the chain of subloops of some proper subloop of Q.

(ii) implies (i): This is evident. □

Remark 1. One can easily see that the three equivalent conditions of Theorem 2 are also equivalent to the following condition: There exists an algebra A with finitely many operations such that the lattice of subalgebras of A is a chain isomorphic to α.

Remark 2. A mono-associative (alias power-associative) uniserial loop is an abelian group. Uniserial abelian groups are just cyclic and quasicyclic p-groups. It follows that we can hardly find 'new' uniserial loops in 'nice' equational classes.

Remark 3. Define a new binary operation, say $\circ$, on the set (and field) $\mathbf{Q}$ of rational numbers by means of the following rules:

(a) $a \circ a = a - 1$ for every $a \in \mathbf{Q}$;
(b) if $a, b \in \mathbf{Q}$ are such that $m = |a - b|$ is a non-zero integer, then $a \circ b = \max(a, b) - \frac{1}{m}$;
(c) if $a, b \in \mathbf{Q}$ are such that $a \neq b$ and $q = |a - b|$ is not an integer, then $a \circ b = \min(a, b) - q$.

In this way, we obtain a commutative groupoid $\mathbf{Q}(\circ)$ and every order ideal of $\mathbf{Q}$ (i.e., a nonempty subset of $\mathbf{Q}$ containing with each number all smaller ones) is a subgroupoid of $\mathbf{Q}(\circ)$. The converse is true as well. Indeed, let G be a subgroupoid od $\mathbf{Q}(\circ)$, $a \in G$, $b \in \mathbf{Q}$ and $b < a$. We have to show that $b \in G$. Anyway, $b = a - \frac{m}{n}$ for some positive integers m, n, where $n \geq 2$, and we get $a - n \in G$ by (a) and induction. Then, of course, $a - \frac{1}{n} = a \circ (a - n) \in G$ by (b). Furthermore, $(a - \frac{k}{n}) \circ (a - \frac{k+1}{n}) = a - \frac{k+2}{n}$ by (c) for every non-negative integer k. Now, using induction again, we get $a - \frac{k}{n} \in G$. In particular, $b = a - \frac{m}{n} \in G$. We have proved that G is an order ideal of $\mathbf{Q}$.

Thus the lattice of subgroupoids of $\mathbf{Q}(\circ)$ is the chain of order ideals that is isomorphic to the chain of real numbers (with the greatest element added) in which every rational number is doubled. It is not clear whether such a chain (of course, with the smallest element) is realisable by a uniserial loop.

References

[1] J. D. H. Smith, *An introduction to quasigroups and their representations,* CRC Press 2007.

Jaroslav Ježek, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 18600 Praha 8, Czech Republic
E-mail address: jezek@karlin.mff.cuni.cz

Tomáš Kepka, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 18600 Praha 8, Czech Republic
E-mail address: kepka@karlin.mff.cuni.cz