Quasigroups and Related Systems **15** (2007), 309 – 316

On finite quasigroups whose subquasigroup lattices are distributive

Konrad Pióro

Abstract

We prove that if the subquasigroup lattice of a finite quasigroup Q is distributive, then Q is cyclic (i.e., Q is generated by one element) and also, each of its subquasigroups is also cyclic. Finally, we give examples which show that the inverse implication does not hold.

It is a classical result of Group Theory, showed by Ore in [5] (see also [7]), that the subgroup lattice of a group $\mathcal{G}$ is distributive if and only if $\mathcal{G}$ is locally cyclic (i.e., each finitely generated subgroup of $\mathcal{G}$ is cyclic). In particular, a finite group $\mathcal{G}$ has a distributive subgroup lattice if and only if $\mathcal{G}$ is cyclic.

In the present paper we prove the following result for quasigroups (for definitions and simple facts of quasigroups and lattices see e.g. [1], [2], [3])

Theorem 1. *Let $\mathcal{Q} = (Q, \circ, \backslash, /)$ be a finite quasigroup such that its subquasigroup lattice $\mathcal{S}(\mathcal{Q})$ is distributive. Then $\mathcal{Q}$ and each subquasigroup of $\mathcal{Q}$ are cyclic.*

Before the proof observe that, in the contrary to groups, a subquasigroup of a cyclic quasigroup need not be cyclic. Let $\mathcal{Q}$ be a six-element quasigroup given by the following table (recall, see e.g. [1], that a finite groupoid $(Q, \circ)$ is a quasigroup if and only if the multiplication table of $\circ$ is a Latin square, i.e., each element of Q occurs exactly once in each row and each column)

2000 Mathematics Subject Classification: 05B15, 06D05, 06B15, 20N05, 08A30.
Keywords: quasigroup, cyclic quasigroup, subquasigroup, subquasigroup lattice, distributive lattice.

$\circ$	a	b	c	d	e	f
a	a	c	b	f	e	d
b	c	b	a	d	f	e
c	b	a	c	e	d	f
d	f	d	e	c	a	b
e	e	f	d	a	b	c
f	d	e	f	b	c	a

Then $\mathcal{Q} = \langle f\rangle = \langle e\rangle = \langle d\rangle$, so $\mathcal{Q}$ is cyclic. On the other hand, $\{a,b,c\}$ is a subquasigroup of $\mathcal{Q}$ which is non-cyclic, because $a\circ a = a$, $b\circ b = b$ and $c\circ c = c$. Note that the constructed quasigroup $\mathcal{Q}$ is even commutative.

Observe also that such example cannot be found among quasigroups having less than 6 elements. More precisely, it is easy to see that any two-element quasigroup is cyclic. So if a quasigroup $\mathcal{Q}$ contains a non-cyclic subquasigroup $\mathcal{G}$, then $\mathcal{G}$ must have at least three elements, say a,b,c. Next, there is $q\in Q$ which generate $\mathcal{Q}$, in particular $q\in Q\setminus G$. The elements $q\circ a$, $q\circ b$ and $q\circ c$ are pairwise different. They are also different from a,b,c (more precisely, $\{q\circ a, q\circ b, q\circ c\}\cap G=\emptyset$, because $a,b,c\in G$ and $\mathcal{G}$ is a quasigroup). At most one of them may be equal q. Thus we have obtained at least six different elements of $\mathcal{Q}$.

Theorem 1 is straightforward implied by the following more general lemma (where $\wedge$ and $\vee$ are lattice operations of infimum and supremum respectively)

Lemma 1. *Let $\mathcal{Q}=(Q,\circ,\backslash,/)$ be a finite quasigroup such that for any two different elements $p,q\in Q$*

$$(*)\ \ \langle p\circ q\rangle = (\langle p\circ q\rangle\wedge\langle p\rangle)\vee(\langle p\circ q\rangle\wedge\langle q\rangle).$$

Then all subquasigroups of $\mathcal{Q}$ are cyclic.

Obviously if the subquasigroup lattice $\mathcal{S}(\mathcal{Q})$ is distributive, then $(*)$ holds. Because $\langle p\circ q\rangle = \langle p\circ q\rangle\wedge\langle p,q\rangle = \langle p\circ q\rangle\wedge(\langle p\rangle\vee\langle q\rangle) = (\langle p\circ q\rangle\wedge\langle p\rangle)\vee(\langle p\circ q\rangle\wedge\langle q\rangle)$.

Proof. Assume that $\mathcal{Q}$ contains subquasigroups which are non-cyclic. Take a family $\mathcal{A}$ of all such subquasigroups. Since $\mathcal{Q}$ is a finite quasigroup, $\mathcal{A}$ is a finite set which is partially ordered by set-inclusion. Thus $(\mathcal{A},\subseteq)$ contains at least one minimal element, say $\mathcal{G}$. Then $\mathcal{G}$ is a subquasigroup of $\mathcal{Q}$ such that

(i) $\mathcal{G}$ is non-cyclic,

(ii) each proper (i.e., non-empty and non-equal $\mathcal{G}$) subquasigroup of $\mathcal{G}$ is cyclic.

Further,

(iii) $\mathcal{G}$ is generated by two elements.

More precisely, $\mathcal{G}$ is finite, so $\mathcal{G}$ is generated by some elements $g_1, g_2, \ldots, g_k$, i.e.,

$$\mathcal{G} = \langle g_1, g_2, \ldots, g_k \rangle.$$

Take the new subquasigroup $\langle g_1, g_2 \rangle \leq \mathcal{G}$. If $\mathcal{G} \neq \langle g_1, g_2 \rangle$, then $\langle g_1, g_2 \rangle$ is a cyclic subquasigroup. Let $\langle g_1, g_2 \rangle = \langle g' \rangle$ for some $g' \in G$. Then

$$\mathcal{G} = \langle g', g_3, \ldots, g_k \rangle.$$

Thus by simple induction on k we obtain that $\mathcal{G}$ is generated by two elements.

Let $\mathcal{B}$ be a set of all pairs (g_1, g_2) of elements of $\mathcal{G}$ which generate $\mathcal{G}$ (i.e., $\langle g_1, g_2 \rangle = \mathcal{G}$). Note that $\mathcal{B}$ is finite and non-empty.

Now from the set

$$\{g_1 \in G \colon (g_1, g_2) \in \mathcal{B} \text{ for some } g_2 \in \mathcal{G}\}$$

we choose an element g such that

$$|\langle g \rangle| = \min\{|\langle g_1 \rangle| \colon (g_1, g_2) \in \mathcal{B} \text{ for some } g_2 \in G\} \tag{1}$$

Next, from the set

$$\{g_2 \in G \colon (g, g_2) \in \mathcal{B}\}$$

we choose an element h such that

$$|\langle h \rangle| = \min\{|\langle g_2 \rangle| \colon (g, g_2) \in \mathcal{B}\} \tag{2}$$

Observe that

$$g \circ h \notin \langle g \rangle \quad \text{and} \quad g \circ h \notin \langle h \rangle \tag{3}$$

Assume for example that $g \circ h \in \langle g \rangle$. Then $h = g \backslash (g \circ h) \in \langle g \rangle$, so $\langle h \rangle \subseteq \langle g \rangle$, and consequently $\mathcal{G} = \langle g, h \rangle = \langle g \rangle$. But it is a contradiction with the assumption that $\mathcal{G}$ is not cyclic.

Thus $\langle g \rangle$, $\langle h \rangle$ and $\langle g \circ h \rangle$ are three different subquasigroups of $\mathcal{G}$. Of course $\langle g \rangle$ and $\langle h \rangle$ are not comparable (otherwise $\mathcal{G}$ would be cyclic).

By the condition $(*)$ we have

$$\langle g \circ h \rangle = (\langle g \circ h \rangle \wedge \langle g \rangle) \vee (\langle g \circ h \rangle \wedge \langle h \rangle).$$

Let

$$\mathcal{G}_1 = \langle g \circ h \rangle \wedge \langle g \rangle = \langle g \circ h \rangle \cap \langle g \rangle$$

and

$$\mathcal{G}_2 = \langle g \circ h \rangle \wedge \langle h \rangle = \langle g \circ h \rangle \cap \langle h \rangle$$

Then $\mathcal{G}_1 \subseteq \langle g \rangle$ and $\mathcal{G}_2 \subseteq \langle h \rangle$. Moreover,

$$\mathcal{G}_1 \neq \langle g \rangle \quad \text{or} \quad \mathcal{G}_2 \neq \langle h \rangle \tag{4}$$

Assume that both equalities hold. Then g and h both belong to $\langle g \circ h \rangle$, because $\mathcal{G}_1$ and $\mathcal{G}_2$ are contained in $\langle g \circ h \rangle$. Hence $\langle g, h \rangle$ is contained in $\langle g \circ h \rangle$, and consequently $\mathcal{G} = \langle g, h \rangle = \langle g \circ h \rangle$, which is impossible.

Since $\mathcal{G}_1 \subseteq \langle g \rangle \subsetneqq \mathcal{G}$, we have by the minimality of $\mathcal{G}$, that $\mathcal{G}_1$ is cyclic, i.e.,

$$\mathcal{G}_1 = \langle g_1 \rangle \ \text{ for some } g_1.$$

Analogously, $\mathcal{G}_2$ is also cyclic, i.e.,

$$\mathcal{G}_2 = \langle h_1 \rangle \ \text{ for some } h_1.$$

Assume first that

$$\langle g_1 \rangle \subsetneqq \langle g \rangle \tag{$a.1$}$$

Then $|\langle g_1 \rangle| \lneqq |\langle g \rangle|$. So by the choice of g we obtain that for each element $\overline{h}$ of $\mathcal{G}$, g_1 and $\overline{h}$ don't generate $\mathcal{G}$. In particular,

$$\langle g_1, h \rangle \subsetneqq \mathcal{G}.$$

Hence $\langle g_1, h \rangle$ has less elements than $\mathcal{G}$, so (by the minimality of $\mathcal{G}$) $\langle g_1, h \rangle$ is cyclic. Let $\overline{g_1}$ be an element of $\mathcal{G}$ such that

$$\langle g_1, h \rangle = \langle \overline{g_1} \rangle.$$

On the other hand,

$$\mathcal{G}_1 \subseteq \langle g_1, h \rangle, \quad \mathcal{G}_2 \subseteq \langle h \rangle \subseteq \langle g_1, h \rangle$$

and

$$\langle g \circ h \rangle = \mathcal{G}_1 \vee \mathcal{G}_2.$$

Thus

$$g \circ h \in \langle g \circ h \rangle \subseteq \langle g_1, h \rangle = \langle \overline{g_1} \rangle.$$

Since $\langle \overline{g_1} \rangle$ contains $g \circ h$ and h, we obtain that $\langle \overline{g_1} \rangle$ contains also g, because $g = (g \circ h)/h$. Hence, the cyclic quasigroup $\langle \overline{g_1} \rangle$ contains g and h, which implies

$$\mathcal{G} = \langle g, h \rangle = \langle \overline{g_1} \rangle.$$

But it is impossible, because we have assumed that $\mathcal{G}$ is not cyclic.

Now assume that

$$\mathcal{G}_2 = \langle h_1 \rangle \subsetneqq \langle h \rangle \tag{$a.2$}$$

Then

$$|\langle h_1 \rangle| \lneqq |\langle h \rangle|,$$

so by the choice of h we obtain that g and h_1 don't generate $\mathcal{G}$, i.e.,

$$\langle g, h_1 \rangle \subsetneqq \mathcal{G}.$$

Hence, $\langle g, h_1 \rangle$ has less elements than $\mathcal{G}$, so $\langle g, h_1 \rangle$ is cyclic (by the minimality of $\mathcal{G}$). Let $\overline{h_1}$ be an element of $\mathcal{G}$ such that

$$\langle g, h_1 \rangle = \langle \overline{h_1} \rangle.$$

Similarly as in the first case we have

$$g \circ h \in \langle g \circ h \rangle = \mathcal{G}_1 \vee \mathcal{G}_2 = \langle g_1, h_1 \rangle \subseteq \langle g, h_1 \rangle.$$

Since $\langle \overline{h_1} \rangle = \langle g, h_1 \rangle$ contains $g \circ h$ and g, we have that $\langle \overline{h_1} \rangle$ contains also h, because $h = g \backslash (g \circ h)$. This fact implies that

$$\mathcal{G} = \langle g, h \rangle = \langle \overline{h_1} \rangle.$$

Thus we again obtain a contradiction.

Summarizing we have shown that $\mathcal{G}_1 = \langle g \rangle$ and $\mathcal{G}_2 = \langle h \rangle$. But it contradicts (4), which completes the proof. $\square$

Obviously any groupoid (in particular, each quasigroup) with at most three elements in which each subgroupoid is cyclic, has at most four subgroupoids (together with the empty subgroupoid). In particular, its subgroupoid lattice is distributive.

Unfortunately, there is a four-element quasigroup with a non-distributive subquasigroup lattice, although each of its subquasigroups is cyclic. For example, let $\mathcal{Q} = \{a, b, c, d\}$ be a quasigroup defined by the following multiplication table

∘	a	b	c	d
a	c	a	d	b
b	d	b	a	c
c	b	d	c	a
d	a	c	b	d

Then $\langle a\rangle = \langle b, c\rangle = \langle b, d\rangle = \langle c, d\rangle = \mathcal{Q}$, and $\langle b\rangle = \{b\}, \langle c\rangle = \{c\}, \langle d\rangle = \{d\}$. Thus $\mathcal{Q}$ has exactly five subquasigroups $\emptyset, \langle b\rangle, \langle c\rangle, \langle d\rangle$ and $\mathcal{Q}$. These subquasigroups form the non-distributive lattice $\mathcal{M}_5$, so $\mathcal{S}(\mathcal{Q})$ is not distributive. Observe also that, for example, elements b and d (together with $b \circ d = c$) do not satisfy $(*)$ of Lemma 1.

Now we show that even commutativity is not enough as an additional assumption. Let $\mathcal{Q}$ be a commutative five-element quasigroup such that

∘	a	b	c	d	e
a	a	c	d	b	e
b	c	b	e	d	a
c	d	e	c	a	b
d	b	d	a	e	c
e	e	a	b	c	d

Then $\langle a\rangle = \{a\}, \langle b\rangle = \{b\}, \langle c\rangle = \{c\}$ and $\langle e\rangle = \langle d\rangle = \langle a, b\rangle = \langle a, c\rangle = \langle b, c\rangle = \mathcal{Q}$. Thus $\emptyset, \langle a\rangle, \langle b\rangle, \langle c\rangle$ and $\mathcal{Q}$ are all pairwise different subquasigroups of $\mathcal{Q}$. Moreover, the lattice $\mathcal{S}(\mathcal{Q})$ is isomorphic with $\mathcal{M}_5$, so it is not distributive. Note also that elements a and b do not satisfy $(*)$ of Lemma 1.

Remark 1. For any commutative quasigroup $\mathcal{Q}$ with at most four elements, if each subquasigroup of $\mathcal{Q}$ is cyclic, then the subquasigroup lattice $\mathcal{S}(\mathcal{Q})$ is distributive.

It is true for an arbitrary groupoid with at most three elements, so we take a four-element commutative quasigroup $\mathcal{Q}$. Note that if each subquasigroup of $\mathcal{Q}$ is cyclic, then $\mathcal{Q}$ has at most $|Q| + 1 = 5$ subquasigroups (because the empty set is also a subquasigroup). But if a quasigroup has at most four subquasigroups, then of course it has distributive subquasigroup lattice. Thus we can take $\mathcal{Q}$ with exactly five subquasigroups (three proper subquasigroups).

Assume that $\mathcal{S}(\mathcal{Q})$ is not distributive. Then $\mathcal{S}(\mathcal{Q})$ is isomorphic with the non-modular lattice $\mathcal{N}_5$ or with the non-distributive lattice $\mathcal{M}_5$.

First we consider the case when $\mathcal{S}(\mathcal{Q})$ is isomorphic with $\mathcal{N}_5$. Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be proper subquasigroups of $\mathcal{Q}$ such that $\mathcal{G}_1 \subsetneqq \mathcal{G}_2$. Let $\emptyset \neq \mathcal{G}_3 \subsetneqq \mathcal{Q}$ be the subquasigroup which is not comparable with $\mathcal{G}_1$ and $\mathcal{G}_2$ (i.e., $\mathcal{G}_3 \cap \mathcal{G}_2 = \emptyset$ and $\mathcal{G}_3 \vee \mathcal{G}_1 = \mathcal{Q}$). Let q generates $\mathcal{Q}$; and g_1, g_2, g_3 generate $\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3$ respectively. Of course q, g_1, g_2, g_3 are pairwise different elements, i.e., $Q = \{q, g_1, g_2, g_3\}$. Moreover, it is easy to see that $G_1 = \{g_1\}$, $G_2 = \{g_1, g_2\}$ and $G_3 = \{g_3\}$. In other words we have

$$g_1 \circ g_1 = g_1, \;\; g_3 \circ g_3 = g_3, \;\; g_2 \circ g_2 = g_1.$$

By the first equality and the definition of quasigroup we have also

$$g_2 \circ g_1 = g_2 \;\text{ and }\; g_1 \circ g_2 = g_2,$$

because each of equations $x \circ g_1 = g_1$ and $g_1 \circ x = g_1$ has exactly one solution.

These all equalities imply that $g_3 \circ g_1$ and $g_3 \circ g_2$ cannot be equal g_3, g_1 and g_2. Thus $g_3 \circ g_1 = q$ and $g_3 \circ g_2 = q$. But it is impossible, because the equation $g_3 \circ x = q$ has two different solutions. This contradiction shows that $\mathcal{S}(\mathcal{Q})$ cannot be isomorphic with $\mathcal{N}_5$.

Now assume that $\mathcal{S}(\mathcal{Q})$ is isomorphic with $\mathcal{M}_5$. Then there are pairwise different proper and non-comparable subquasigroups $\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3$ of $\mathcal{Q}$. Let g_1, g_2, g_3 generate these three subquasigroups, respectively. Let q be a generator of $\mathcal{Q}$. Of course q, g_1, g_2, g_3 are pairwise different, so $Q = \{q, g_1, g_2, g_3\}$. Hence we obtain $G_1 = \{g_1\}, G_2 = \{g_2\}, G_3 = \{g_3\}$. So

$$g_1 \circ g_1 = g_1, \quad g_2 \circ g_2 = g_2, \quad g_3 \circ g_3 = g_3.$$

Moreover, since q generate $\mathcal{Q}$ we have that $q \circ q \neq q$. Of course we can assume that $q \circ q = g_1$. Then $q \circ g_1 = g_1 \circ q$ is different from g_1 (because the equation $q \circ x = g_1$ has exactly one solution) and $q \circ g_1$ is not equal q (because q generates $\mathcal{Q}$). Of course we can assume that $g_1 \circ q = q \circ g_1 = g_2$ (replacing g_3 by g_2 if necessary).

Now observe that equalities $q \circ q = g_1$, $g_1 \circ q = g_2$ and $g_3 \circ g_3 = g_3$ imply that $g_3 \circ q$ cannot equals g_1, g_2 and g_3. So $g_3 \circ q = q$. Analogously $q \circ g_1 = g_2$, $g_1 \circ g_1 = g_1$ and $g_3 \circ g_3 = g_3$ imply $g_3 \circ g_1 = q$. But these equalities cannot hold in a quasigroup, because $g_1 \neq q$. This contradiction completes the proof.

At the end of the paper observe that if $\mathcal{G}$ is a finite group satisfying the condition $(*)$ from Lemma 1, then $\mathcal{G}$ is cyclic, and consequently its subgroup lattice $\mathcal{S}(\mathcal{G})$ is distributive. But the following example shows that for finite (and even commutative) quasigroups the condition $(*)$ is indeed weaker.

Let $\mathcal{Q} = (Q, \circ)$ be a commutative six-element quasigroup such that

$\circ$	a	b	c	d	e	f
a	a	c	f	e	b	d
b	c	b	a	f	d	e
c	f	a	d	b	e	c
d	e	f	b	d	c	a
e	b	d	e	c	a	f
f	d	e	c	a	f	b

Then $\langle a \rangle = \{a\}$, $\langle b \rangle = \{b\}$, $\langle d \rangle = \{d\}$ and $\langle c \rangle = \langle e \rangle = \langle f \rangle = \langle a, b \rangle = \langle a, d \rangle = \langle b, d \rangle = \mathcal{Q}$. So $\mathcal{Q}$ has exactly five subquasigroups (together with the empty subquasigroup) which form the non-distributive lattice $\mathcal{M}_5$.

On the other hand, we obtain by a straightforward verification that $\mathcal{Q}$ satisfies $(*)$. More precisely, if $g \in \{c, e, f\}$, then $\langle g \circ h \rangle \wedge \langle g \rangle = \langle g \circ h \rangle \wedge \mathcal{Q} = \langle g \circ h \rangle$; so $(*)$ holds. The analogous situation we have for $h \in \{c, e, f\}$. If $g, h \in \{a, b, d\}$, then $g \circ h \in \{c, e, f\}$; so $\langle g \circ h \rangle = \mathcal{Q}$ which implies $(*)$ (because then $\langle g \circ h \rangle \wedge \langle g \rangle = \langle g \rangle$ and $\langle g \circ h \rangle \wedge \langle h \rangle = \langle h \rangle$, thus the right hand side of $(*)$ equals $\langle g \rangle \vee \langle h \rangle = \mathcal{Q}$).

References

[1] **S. Burris and H. P. Sankappanawar**: *A Course in Universal Algebra*, Springer-Verlag, New York-Berlin, 1981.

[2] **G. Grätzer**: *Universal Algebra*, second edition, Springer-Verlag, New York-Heidelberg 1979.

[3] **G. Grätzer**: *General Lattice Theory*, second edition, Birkhäuser Verlag, Basel 1998.

[4] **O. Ore**: *Structures and group theory I*, Duke Math. J. **3** (1937), 149 – 173.

[5] **O. Ore**: *Structures and group theory II*, Duke Math. J. **4** (1938), 247 – 269.

[6] **K. Pióro**: *On some finite groupoids with distributive subgroupoid lattices*, Discuss. Math. Gen. Algebra Appl. **22** (2002), 25 – 31.

[7] **R. Schmidt**: *Subgroup Lattices of Groups*, Walter de Gruyter, New York 1994.

Received February 26, 2007

Institute of Mathematics, Warsaw University, ul. Banacha 2, PL-02-097 Warsaw, Poland
E-mail: kpioro@mimuw.edu.pl