Boolean groupoids

by

Ahmad Shafaat (Halifax)

Abstract. A groupoid $(A, .)$ is called *Boolean* if there exists a Boolean algebra $(B, \cup, ')$ such that $A \subseteq B$ and $a \cdot b = a \cup b'$ for all $a, b \in A$. Six identities are given that characterize the class of all Boolean groupoids.

Let $(B, \cup, ')$ be a Boolean algebra. Define a binary operation on B as follows: $a \cdot b = a \cup b'$ for all $a, b \in B$. We call $(B, .)$ the *groupoid derived from* $(B, \cup, ')$ *by the polynomial* $x \cup y'$. A groupoid embeddable in a groupoid derived from a Boolean algebra by $x \cup y'$ will be called a *Boolean groupoid*. The main result (Theorem 3) of this note characterizes Boolean groupoids by six identities. In addition we make the following remarks about derived algebras in general.

Let A be an algebra on a set A and let $p_1(x_1, \ldots, x_{n_1}), \ldots, p_i(x_1, \ldots, x_{n_i}), \ldots$ be polynomials in terms of the operations of A. Then by the *algebra derived from A by the polynomials p_i* we mean the algebra on A with operations ω_i (of arity n_i) defined by: $(a_1, \ldots, a_{n_i})\omega_i = p_i(a_1, \ldots, a_{n_i})$. If K is a class of algebras of given type and K^* is the class of algebras derived from the algebras of K by some polynomials then K^* will be called a *class derived from* K. We use the notation $S(K)$ for the class of algebras embeddable in the algebras from K and $\Pi(K)$ for the class of cartesian products of algebras from K.

THEOREM 1. *If K^* is derived from a quasivariety* [1] *K then $S(K^*)$ is a quasivariety.*

THEOREM 2. *If K^* is derived from a class K defined by a set of first order sentences then $S\Pi(K^*)$ is a quasivariety.*

Theorem 2 follows from the results of Omarov [3] and Theorem 1 follows from Theorem 2 by noting that if $\Pi(K) = K$ then $\Pi(K^*) = K^*$.

If K is a quasivariety and K^* is derived from K then we call $S(K^*)$ a *quasivariety derived from* K. Mal'cev [2] considers semigroups embeddable in groups. Such semigroups form a quasivariety derived from the variety of groups. Boolean groupoids provide another example. While semigroups embeddable in groups do not form a variety Boolean groupoids do.

THEOREM 3. *Boolean groupoids form a variety defined by the following identities, in which* $x\vee y$ *stands for* $x(xy)$: (1) $x^2=y^2$, (2) $x(yx)=x$, (3) $x\vee y=y\vee x$, (4) $(x\vee y)\vee z=x\vee(y\vee z)$, (5) $(x\vee y)z=xz\vee yz$, (6) $zx\vee \vee z(x\vee y)=zx$.

Not all quasivarieties derived from the variety of Boolean algebras are varieties. Consider for example the quasivariety $K(y')$ derived by $xy=y'$. Let $(B,\cup,')$ be a Boolean algebra with $|B|>2$ and let $(B,.)$ be the groupoid defined by: $a\cdot b=b'$. Let ϱ be defined over B by: $a\equiv b(\varrho)\leftrightarrow a=b$ or b'. Then it is easy to verify that ϱ is a congruence over $(B,.)$ and $(B,.)/\varrho$ satisfies $xy=y$ identically. Since order of B is greater than 2 the groupoid $(B,.)/\varrho$ is nonsingleton. Since no nonsingleton groupoid of $K(y')$ satisfies the identity $xy=y$ it follows that the homomorphic image $(B,.)/\varrho$ of $(B,.)$ does not belong to $K(y')$. Hence $K(y')$ is not a variety.

The quasivariety $K(y')$ is *singular* in the sense that the value of every polynomial in a groupoid of $K(y')$ depends only on one of the variables occurring in the polynomial. Known results and Theorem 3 show that every nonsingular quasivariety of groupoids derived from the variety of Boolean algebras is a variety. This may well be true for algebras other than groupoids — that is, for every two element nonsingular algebra A the quasivariety $S\Pi(A)$ may be a variety.

We make one last remark before turning to the proof of our main theorem: Boolean algebras have been variously considered in terms of two binary operations or one binary operation and one unary operation and so on. The following corollary shows that Boolean algebras can also be considered in terms of one binary and one nullary operation satisfying finitely many identities.

COROLLARY 1. *Let* V *be the variety of algebras* $(B,.,o)$, *where* . *is a binary operation satisfying* (1)-(6) *and* o *is a nullary operation satisfying*: (7) $0(0x)=x$. *Then* V *is nomially equivalent to the variety of Boolean algebras, in the sense that each variety is a class derived from the other. The connection between* $\cup,'$ *on the one hand and* ., o *on the other is given by*: $x\cup y=x(xy)$, $y'=oy$, $xy=x\cup y'$, $o=(x\cup x')'$.

Proof of Theorem 3. It is easy to verify that every Boolean groupoid satisfies identities (1)-(6) in the statement of the theorem. To prove the theorem we let $(B,.)$ be a groupoid satisfying (1)-(6) and show that $(B,.)$ is Boolean. For this our first step is to collect some more identities and implications that hold in $(B,.)$.

By setting $y=x$ in (2) we have $x=x(xx)=(x\vee x)$. This together with (3) and (4) shows that $\vee$ is a semilattice operation. We write $x\leqslant y$ for $x\vee y=y$, so that $\leqslant$ is a partial order over B. Let us write 1 for the constant x^2.

LEMMA 1. *The following hold in* $(B,.)$ *identically*:
(α_1) $x\leqslant y\to xz\leqslant yz$, ($\alpha_2$) $x\leqslant y\to zx\geqslant zy$,
(α_3) $x\vee yx=1$, (α_4) $x\leqslant 1$,
(α_5) $x\leqslant xy$, (α_6) $(xy)x=1$.

Proof. (α_1), (α_2) follow directly from (5), (6) respectively. (α_3) follows from (2), and setting $y=x$ in (α_3) we get (α_4). (α_5) follows from (α_4) and (α_2). Finally (α_6) follows from (α_5), (α_1) and (α_4).

Let us call a subset I of B an *ideal* of $(B,.)$ if $xy\in I\leftrightarrow x\in I$ and $y\notin I$, for all $x,y\in B$. The following lemma gives some properties of ideals.

LEMMA 2. *Let* I *be an ideal of* $(B,.)$. *Then*:
(β_1) $x\vee y\in I\leftrightarrow x\in I$ *and* $y\in I$.
(β_2) *If* $x\equiv y(\mathrm{mod} I)$ *is defined to mean* $x\in I\leftrightarrow y\in I$ *then* $\mathrm{mod} I$ *is a congruence over* $(B,.)$.
(β_3) $(B,.)/\mathrm{mod} I$ *is a Boolean groupoid.*

Proof. $x\vee y\in I\leftrightarrow x(xy)\in I\leftrightarrow x\in I$ and $xy\notin I\leftrightarrow x\in I$ and $y\in I$. This proves (β_1).

If $x\equiv y(\mathrm{mod} I)$ then $xz\in I\leftrightarrow x\in I$ and $z\notin I\leftrightarrow y\in I$ and $z\notin I\leftrightarrow yz\in I$. Hence $xz\equiv yz$ $(\mathrm{mod} I)$ and similarly $zx\equiv zy$ $(\mathrm{mod} I)$. Since $\mathrm{mod} I$ is an equivalence relation this proves (β_2).

Let $(A,.)$ be a two element groupoid satisfying (1)-(6). We can take $A=\{0,1\}$ and $0^2=1^2=1$. By (2) $01=0$ and by (α_6) $10=1$. Hence, within isomorphism, there is a unique two element groupoid satisfying (1)-(6). Therefore, $(B,.)/\mathrm{mod} I$ is isomorphic to $(A,.)$. Also, as is simple to verify, $(A,.)$ is the groupoid derived from a suitable Boolean algebra on $\{0,1\}$ by $x\cup y'$. This proves (β_3).

Our next lemma almost completes the proof.

LEMMA 3. *For every pair of distinct elements of* B *there exists an ideal containing exactly one of the two elements.*

Proof. Let $a,b\in B$, $a\neq b$. Without loss of generality we can suppose that $b\nleqslant a$. Then $a\neq 1$, by (α_4).

Let us write R for the set of all subsets J of B such that:
(i) $a\in J$, $b\notin J$.
(ii) $x\vee y\in J\leftrightarrow x\in J$ and $y\in J$, for all $x,y\in B$.
(iii) $xy\in J\to x\in J$ and $y\notin J$, for all $x,y\in B$.

We show that R is non-empty by showing that

$$J_a=\{x;\ x\leqslant a,\ x\in B\}\in R\,.$$

Clearly J_a satisfies (i), (ii). J_a also satisfies (iii). To see this let $xy\in J_a$. Then, by (α_5), $x\leqslant xy\leqslant a$ and hence $x\in J_a$. If $y\in J_a$ then $y,xy\leqslant a$ and therefore $y\vee xy\leqslant a$. By (α_3) this implies $1\leqslant a$ and hence $a=1$. This contradicts our assumption that $a\neq 1$, and therefore $y\notin J_a$. This proves (iii) for J_a and that R is non-empty.

It is easily verified that the union of members of a chain in $(R, \subseteq)$ is also in R. (Here $\subseteq$ is the set-theoretic inclusion.) By Zorn's lemma, therefore, $(R, \subseteq)$ has a maximal element, say J. We show that J is an ideal. In view of (iii) this only requires showing that $x \in J$, $y \notin J \to xy \in J$. Thus if we write K for the set of $y \notin J$ such that $xy \notin J$ for some $x \in J$ then we need to show that K is empty.

Suppose K is not empty and let $k \in K$, $j \in J$, $jk \notin J$. Then $j \vee k \notin J$, by (ii). Since $j \vee k = j(jk)$ it follows that $jk \in K$. Consider the two subsets of B:

$$J_1 = \{x;\ x \leqslant y \vee k,\ y \in J\},$$

$$J_2 = \{x;\ x \leqslant y \vee jk,\ y \in J\}.$$

Since $k, jk \notin J$ the sets J_1, J_2 both properly contain J. We complete the proof of the lemma by showing that at least one of the two sets J_1, J_2 satisfies (i), (ii), (iii), and thus arriving at a contradiction to the maximality of J.

Clearly $a \in J_1, J_2$. Suppose that $b \in J_1, J_2$, so that $b \leqslant y_1 \vee k$, $y_2 \vee jk$ for some $y_1, y_2 \in J$. If we write $z = y_1 \vee y_2 \vee j$ then $b \leqslant z \vee k$, and by (α_1), (α_5), $b \leqslant z \vee zk = zk$. By (α_2), then, $zb \geqslant z(zk) = z \vee k \geqslant b$. Hence $b \vee zb = zb$, which by (α_3) gives $zb = 1$. Then $z(zb) = z1 = z$, by (2). Hence $b \vee z = z$. By (ii) this implies $b \in J$, a contradiction. Hence b does not belong to both J_1 and J_2, and one of J_1, J_2 satisfies (i), say J_1. It is easy to see that J_1 satisfies (ii). If xy, $y \in J_1$, then by (ii), (α_3) and (α_4) we have $1 = y \vee xy \in J_1$ and $J_1 = B$. This however is not possible since $b \notin J_1$. Hence $xy \in J_1 \to y \notin J_1$. Also, by (ii) and (α_5), $xy \in J_1 \to x \in J_1$. Hence $J_1 \in R$ and the lemma is proved.

Now the proof of Theorem 3 can be concluded as follows: By (β_3) of Lemma 2 and Lemma 3, $(B, .)$ is embeddable in a cartesian power of the two element Boolean groupoid. But cartesian powers and subgroupoids of Boolean groupoids are themselves Boolean. Hence $(B, .)$ is a Boolean groupoid.

References

[1] P. M. Cohn, *Universal Algebra*, New York 1965.
[2] A. Mal'cev, *Über die Einbettung von assoziativen Systemen in Gruppen* I, Rec. Math. (N.S.) (6) 48 (1939), pp. 331–336; II, Rec. Math. (N.S.) (8) 50 (1940), pp. 251–264.
[3] A. I. Omarov, *On compact classes of models*, Algebra i logica. Sem. 6 (1967), pp. 49–60.

SUMMER RESEARCH INSTITUTE
DALHOUSIE UNIVERSITY, Halifax

Accepté par la Rédaction le 17. 12. 1973

A characterization of locally compact fields II

by

W. Więsław (Wrocław)

Abstract. Let $(K, \mathcal{T})$ be a non-discrete topological field. Define the Krull topology in the group $G(K)$ of all its continuous automorphisms, i.e. take for a base of the zero neighbourhoods all groups $G(K) \cap G(K/M)$ for finitely generated extensions M of the fixed field of $G(K)$. It is shown that K is locally compact if and only if K is locally bounded and complete and, for every closed subfield F of K, $G(F)$ is compact in its Krull topology.

0. In my previous paper [15] I gave a characterization of locally compact fields of zero characteristic. The aim of this paper is to give a characterization of all locally compact fields. At first let us recall some definitions. For any topological field $(F, \mathcal{T})$ we write $G(F)$ for the group of all its continuous automorphisms. Let L/K be a field extension and let us denote by $G(L/K)$ the Galois group of L over K. If G is a subgroup of $G(L/K)$ we shall introduce a group topology in G taking for a base of the zero neighbourhoods in G all sets of the form $G \cap G(L/M)$, where M is a finitely generated extension of the fixed field K' of G, i.e. $M = K'(X_1, X_2, \ldots, X_s)$, $X_j \in L$ for $j = 1, 2, \ldots, s$ (algebraic over K' or not). We shall call such topology in G the *Krull topology* in G. Let $(K, \mathcal{T})$ be a topological field. A field topology $\mathcal{T}$ is said to be *locally bounded* if there exists a bounded neighbourhood A of zero, i.e. if for every neighbourhood U of zero there exists another one, V, such that $AV \subset U$.

1. The aim of this paper is to prove the following

THEOREM. *Let $(K, \mathcal{T})$ be a non-discrete topological field. Then the following conditions are equivalent:*

(1) *K is a locally bounded, complete field and, for every closed subfield F of K, $G(F)$ is compact in its Krull topology,*

(2) *K is a locally compact field,*

(3) *K is a finite extension either of the reals $\mathbf{R}$, of a p-adic number field $\mathbf{Q}_p$, or of some formal power series field over the prime field $\mathbf{Z}_p$ (i.e. a finite extension either of $\mathbf{Z}_p\langle x\rangle$ or $\mathbf{Z}_p\{x\}$).*

Proof of the theorem. The equivalence (2) $\Leftrightarrow$ (3) is the classical theorem of Pontryagin–Kowalsky–van Dantzig (see [6]).