A SET OF INDEPENDENT AXIOMS FOR A FIELD AND A CONDITION FOR A GROUP TO BE THE MULTIPLICATIVE GROUP OF A FIELD

By R. M. DICKER

[Received 17 October 1966]

1. Introduction

In (**1**) the author developed a set of five axioms for Boolean algebra using a ternary operation. In this paper, it is shown (Theorem 1) that if one of these axioms is changed the resulting system is a set of axioms for a field. It follows that addition in a field may be defined in terms of multiplication and the mapping $x \to 1-x$; hence a necessary and sufficient condition that an Abelian group should be the multiplicative group of a field is obtained (Theorem 3). This theorem is a solution to problem 69 of Fuchs (**2**). In § 7, the result is generalized to apply to the multiplicative group of a division ring.

The first three theorems are introduced in §§ 2, 3, and are proved in reverse order in §§ 4–6. The reason for this is that the motivation is clearest when the theorems are described in the order in which they were discovered; whereas the proofs, which could be made to occur in any order, are arranged so that the proof of Theorem 3 is independent of the other theorems.

2. Statement of the first theorem

Let F be a field. We define a ternary operation on F by putting

$$x(y,z) = y - xy + xz. \tag{2.1}$$

We write the operation in the form $x(y,z)$ because this is especially convenient whenever the operation satisfies the law

(i) $x(y,z)(u,v) = x(y(u,v),z(u,v))$,

as this one does. It is easy to verify that the following statements hold:

(ii) $0(x,y) = x$;

(iii) $x(0,y) = y(0,x)$;

(ii)′ $1(x,y) = y$.

It is easy to obtain multiplication from the ternary operation,

$$xy = x(0,y), \tag{2.2}$$

so that if we can define addition also from this operation, there is a

possibility of finding axioms for a field that include those above. Obviously the principle is to add everything that is needed to prove the relevant results, and then try to find redundant axioms. Note that at least one axiom must have the property of excluding direct products since the direct product of two fields is not a field. The following axiom has this property:

(iv) for all y, z, u, if $y \neq z$ then there exists x such that $x(y,z) = u$.

(This axiom was chosen with some knowledge of its implications, i.e. Lemma 6. It is perhaps surprising that it is sufficient to determine a field. Incidentally, it has long been recognized at an elementary level that certain laws of Boolean algebra remain true in a field when intersection is replaced by multiplication and the complement of x is replaced by $1-x$. A comparison of this paper and (**1**) shows that much more can be said on this subject!)

The most obvious way to define addition from the ternary operation is by defining subtraction. Clearly, $1-x = x(1,0)$ and, if $x \neq 0$, $x-y = x(1-yx^{-1})$, which can be expressed in terms of the ternary operation. The rest of the definition is not quite so obvious: $0-x = x(u,0)$, where u is the solution of $u(x,1) = 0$, so that $x \neq 1$, and $0-1 = (0-x)x^{-1}$ This is not very satisfactory, but at least addition has been obtained. It does not seem to be possible to give a definition without special cases, but we can define addition directly. We begin by noting that there is another operation similar to multiplication,

$$x \circ y = x(y,1) = x+y-xy = 1-(1-x)(1-y),$$

for which 1 is the zero and 0 is the identity. If $x \neq 0$ then x^{-1} denotes the inverse of x with respect to ordinary multiplication; similarly, if $x \neq 1$ we use x^* to denote the inverse of x with respect to $\circ$ multiplication, i.e. $x^*(x,1) = 0$. Put $m = (1-x)x^{-1}x^*$; then $m = -1$ for all $x \neq 0, 1$. We can now define addition:

$$\left.\begin{array}{ll} \text{if } x \neq 1 \text{ then} & x+y = x^*(1,0)(0,y)(x,1); \\ \text{if } y \neq 1 \text{ then} & 1+y = y^*(1,y); \\ & 1+1 = m(1,0). \end{array}\right\} \tag{2.3}$$

Before we state Theorem 1 we must make some preliminary remarks. First, suppose that a 1-field means a set with two binary operations that satisfy the usual conditions for a field, and a 2-field means a set with a ternary operation that satisfies (i)–(iv). Then 1-fields and 2-fields are equivalent in that there is a natural one-to-one correspondence between them, or, alternatively, each system can be modified to refer to a set with two binary and one ternary operations so that the two systems

become indistinguishable. In this context, it is not clear when we say 'field' whether we mean '1-field' or something more general. We assume the latter meaning.

The axioms are rewritten in order that their independence should be meaningful; also (ii)′ is redundant. The usual axioms for a field include the condition $0 \neq 1$. We need a similar condition that excludes the one-element algebra.

THEOREM 1. *Let F be a set having at least two elements, and let a ternary operation, written in the form $x(y,z)$, be defined on F. Then F is a field if and only if the following axioms are satisfied:*

(i) $(\forall x\,y\,z\,u\,v)\quad x(y,z)(u,v) = x(y(u,v),z(u,v))$;

(ii) $(\exists p)(\forall x\,y)\quad p(x,y) = x$;

(iii) $(\exists q)(\forall x\,y)\quad x(q,y) = y(q,x)$;

(iv) $(\forall y\,z\,u)\quad [y \neq z \Rightarrow (\exists x)\ x(y,z) = u]$.

The axioms (i)–(iv) *are independent, and they imply that there is a unique element* 0 *in F such that in* (ii) *and* (iii) $p = q = 0$; *that there is a unique element $1 \neq 0$ in F such that*

(ii)′ $(\forall x y)\quad 1(x,y) = y$,

(iii)′ $(\forall x y)\quad x(y,1) = y(x,1)$;

and that the element x in (iv) *is uniquely determined.*

If $x \neq 0$ the unique solution y of the equation $y(0,x) = 1$ is denoted by x^{-1}, and if $x \neq 1$ the unique solution y of $y(x,1) = 0$ is denoted by x^*. If $F = \{0,1\}$ put $m = 1$, if F contains an element $x \neq 0, 1$, put

$$m = x(1,0)(0,x^{-1})(0,x^*).$$

Then the transformation from addition and multiplication to the ternary operation is given by (2.1), *the transformation from the ternary operation to addition and multiplication is given by* (2.3) *and* (2.2), *and each transformation is the inverse of the other.*

3. Properties of the mapping $x \to 1-x$

It follows from Theorem 1 that $x(y,0) = (1-x)y$ and, if $z \neq 0$, $x(y,z) = x(y(0,z^{-1}),1)(0,z)$. Since $x(u,1) = 1-(1-x)(1-u)$, we have thus expressed $x(y,z)$ in terms of multiplication and the mapping $x \to 1-x$ only. Furthermore, since we can define addition from the ternary operation, we can define addition from multiplication and the mapping. Obviously this mapping is an involution that interchanges 0 and 1. We would like to know what else must be postulated in order to obtain a field. We rearrange this problem as follows.

Let G be an Abelian group, written multiplicatively, and let F be obtained by adjoining a zero element 0 to G. Let the mapping $f\colon F \to F$

satisfy the conditions

$$f(0) = 1 \tag{3.1}$$

and,

$$\text{for all } x, \quad f(f(x)) = x. \tag{3.2}$$

Define a ternary operation on F by putting

$$\left.\begin{aligned} x(y,0) &= f(x)y, \\ \text{if } z \neq 0, \quad x(y,z) &= f(f(x)f(yz^{-1}))z. \end{aligned}\right\} \tag{3.3}$$

Then we require that the ternary operation satisfies (i)–(iv). It is easy to see that (ii), (iii), and (iv) are already satisfied. Now (i) involves five variables, and when we take special cases of this and use (3.3), we obtain a number of complicated conditions, involving three or four variables, that must be satisfied; however, these can be deduced from one comparatively simple condition.

THEOREM 2. *Let F be given as above, and let $f: F \to F$ satisfy the conditions* (3.1) *and* (3.2). *Then the operation defined by* (3.3) *satisfies axiom* (i) *if and only if it satisfies the condition*

$$\text{for all } x, \text{ and all } y \neq 0, \quad f(f(x)f(y)) = yf(xf(y^{-1})). \tag{3.4}$$

From Theorems 1 and 2 we can immediately deduce the following solution to problem 69 of Fuchs (**2**).

THEOREM 3. *Let G be an Abelian group, written multiplicatively with* 1 *as identity element, and let F be obtained by adjoining a zero element* 0 *to G. Then G is the multiplicative group of a field if and only if there exists a mapping $f: F \to F$ that satisfies* (3.1), (3.2), *and* (3.4).

If we put $x = 1$ in (3.4), it is easy to see that (3.1) is redundant if the group G is non-trivial.

We remarked at the beginning of § 2 that we were prepared to write down as many axioms as necessary to obtain Theorem 1. The proof of Theorem 1 begins by retrieving some redundant axioms, but thereafter Theorems 1 and 3 are essentially equivalent because in each case we have to establish an operation of addition with the usual properties. Furthermore, we can transform a proof of Theorem 1 into a proof of Theorem 3, and conversely, by using (3.3). Calculations are sometimes easier in one form than in the other, and the fact that no additional axioms are necessary was first established by using a mixture of the two proofs. In § 4, we prove Theorem 3 without mention of the ternary operation. In § 5, we continue with a proof of Theorem 2 because this uses the same technique. Finally, in § 6, after the preliminary work, we deduce

Theorem 1 from Theorem 3. It is not difficult to generalize § 4 to apply to a division ring, and this is done in § 7.

4. Proof of Theorem 3

If $F = \{0, 1\}$ then Theorem 3 is trivial, so we may assume that there is an $x \neq 0, 1$. If G is the multiplicative group of a field F, then the mapping f such that $f(x) = 1 - x$ satisfies (3.1), (3.2), and (3.4). For the converse, we prove two lemmas, then we give a definition of addition and prove that this satisfies the necessary conditions.

If $x \neq 1$, we define x^* by $f(f(x^*)f(x)) = 0$. It is clear that x^* is uniquely determined.

LEMMA 1. *If $x \neq 1$ then $x^* = f(f(x)^{-1})$; if $x \neq 0, 1$ then $x^* = f(x^{-1})^{-1}$.*

Proof. The first part is obvious from $f(f(f(x^*)f(x))) = f(0)$. The second part follows by using (3.4) on the definition to obtain $xf(x^*f(x^{-1})) = 0$, but $x \neq 0$ so that $x^*f(x^{-1}) = 1$.

LEMMA 2. *If $x, y \neq 0, 1$ then $f(x)x^{-1}x^* = f(y)y^{-1}y^*$.*

Proof. Put $z = y^{-1}$; then $z \neq 0, 1$, and we see from Lemma 1 that it is sufficient to prove that

$$f(x)f(z) = xf(x^{-1})f(z^{-1})z. \tag{4.1}$$

If $xf(z^{-1}) = 1$ then $z^{-1} = f(x^{-1})$, i.e. the right-hand side of (4.1) is 1, but $f(f(x)f(z)) = zf(xf(z^{-1})) = 0$. We now assume that $xf(z^{-1}) \neq 1$. Take f of each side of (4.1), apply (3.4), and the result is

$$zf(xf(z^{-1})) = f(xf(z^{-1}))f(f(zf(x^{-1}))f(f(xf(z^{-1}))^{-1})). \tag{4.2}$$

Now clearly $f(zf(x^{-1})) = f(z)f(x^{-1}f(f(z)^{-1}))$, and (4.2) can be deduced immediately from Lemma 1 because $x^{-1}f(f(z)^{-1})$ is the inverse of $xf(z^{-1})$.

It is convenient to denote $f(x)x^{-1}x^*$, where $x \neq 0, 1$, by m. If we use Lemmas 1 and 2, we see that

$$m^2 = f(x)x^{-1}x^*f(x^{-1})xx^{-1*} = 1.$$

Definition of addition.

If $x \neq 1$ then

$$x + y = f(f(yf(x^*))f(x));$$

if $y \neq 1$ then

$$1 + y = f(f(y)y^*);$$

$$1 + 1 = f(m).$$

Note that $x + y$ is uniquely determined for all x, y, i.e. $+$ is an operation.

The proof is completed by showing that F is an Abelian group under $+$ and that the distributive law holds.

It is obvious that $0+y=y$. We have to divide the proof of $x+y=y+x$ into four cases: $x=y=1$, which is trivial; $x\neq 1$, $y=1$, and $x=1$, $y\neq 1$, which are equivalent and follow immediately from the definition; and $x, y\neq 1$. Now

$$f(yf(x^*))f(x)=f(y)f(x^*f(f(y)^{-1}))f(x)=f(x)f(y)f(x^*y^*)$$

so that, by symmetry, we have $x+y=y+x$ for the case $x, y\neq 1$.

The following obvious result reduces the number of cases that have to be considered subsequently.

LEMMA 3. *For all x in F, $f(xm)=1+x$.*

We next show that $(1+y)z=z+yz$. If $z=1$ this is obvious, and if $z\neq 1$ then

$$z+yz=f(f(yzf(z^*))f(z))=f(yzf(z^*)f(z^{-1}))z=f(ym)z$$

because $zf(z^*)f(z^{-1})=f(w)w^{-1}w^*$, where $w=f(z)$. Next note that $1+m=f(m^2)=0$; hence $x+mx=0$, i.e. mx is the additive inverse of x. Also, if $x=0$ then

$$(x+y)z=yz=xz+yz,$$

and if $x\neq 0$ then

$$(x+y)z=(1+yx^{-1})xz=xz+yz.$$

For the final step, we show that $(1+y)+z=1+(y+z)$. If $y=0$ this is trivial, and if $y\neq 0$ then $1+y\neq 1$ because $ym\neq 0$. Thus if $y=1$ we have

$$(1+1)+z=f(f(zf(f(m)^*))m)=f(f(zm^{-1})m)=1+(1+z),$$

and if $y\neq 0, 1$ then

$$(1+y)+z=f(f(zm^{-1}y^{-1})ym)$$

and

$$1+(y+z)=f(f(f(zf(y^*))f(y))m)=f(f(zf(y^*)f(y^{-1}))ym)$$
$$=f(f(zy^{-1}m)ym)$$

because $yf(y^*)f(y^{-1})=m$, as before. Thus if $x=0$ then

$$x+(y+z)=(x+y)+z$$

is trivial, and if $x\neq 0$ then

$$x+(y+z)=x(1+(yx^{-1}+zx^{-1}))$$
$$=x((1+yx^{-1})+zx^{-1})=(x+y)+z.$$

5. Proof of Theorem 2

If (i) holds and $y \neq 0$ then

$$f(f(x)f(y)) = x(y,1) = x(0(y,0), y^{-1}(1,0)(y,0))$$
$$= x(0, y^{-1}(1,0))(y,0) = f(xf(y^{-1}))y.$$

Conversely, if (3.4) holds, then we have to check several special cases of (i) because (3.3) is divided into two parts. The cases are given by

(a) $z = 0$, i.e. $x(y,0)(u,v) = x(y(u,v),u)$, and there are four subcases, $u = v = 0$; $u \neq 0$, $v = 0$; $u = 0$, $v \neq 0$; $u \neq 0$, $v \neq 0$;

(b) $z \neq 0$, and the subcases are $u = v = 0$; $u \neq 0$, $v = 0$, $z = 1$; $u \neq 0$, $v = 0$, $z \neq 1$; $u = 0$, $v \neq 0$; $u \neq 0$, $v \neq 0$, $z(u,v) = 0$; $u \neq 0$, $v \neq 0$, $z = 1$; $u \neq 0$, $v \neq 0$, $z \neq 1$, $z(u,v) \neq 0$.

In (a), the first three subcases are obvious, and the fourth is equivalent to a statement that we simplify by multiplying by v^{-1} and putting $uv^{-1} = t$. We obtain, for $t \neq 0$,

$$f(f(f(x)y)f(t)) = f(f(x)f(f(f(y)f(t))t^{-1}))t. \tag{5.1}$$

If we apply (3.4) to $f(f(y)f(t))$ we can deduce that

$$yf(t^{-1}) = f(f(f(y)f(t))t^{-1});$$

hence (5.1) is now clear if we apply (3.4) to the left-hand side.

In (b), the first, second, fourth, and sixth subcases are obvious. The third subcase reduces to

$$f(f(f(x)f(yz^{-1}))z) = f(f(x)f(f(y)f(z)^{-1}))f(z). \tag{5.2}$$

We can deduce (5.2) from (5.1) by substituting $f(yz^{-1})$ for y and $f(z)$ for t. The fifth subcase is simplified by using $f(z)^{-1} = f(uv^{-1})$, which is well defined since $u = v$ is impossible, and then

$$f(f(f(f(x)f(yz^{-1}))z)f(z)^{-1}) = f(x)f(f(y)f(z)^{-1}). \tag{5.3}$$

Clearly, (5.3) follows from (5.2). The last subcase is simplified by using $f(z)f(uv^{-1}) = f(t)$, so that $t \neq 0$, and we obtain

$$f(f(f(f(x)f(yz^{-1}))z)f(t)f(z)^{-1}) = f(f(x)f(f(f(y)f(t)f(z)^{-1})t^{-1}))t. \tag{5.4}$$

If we use (5.2) to simplify the left-hand side of (5.4), and write $f(u)$ for $f(y)f(z)^{-1}$, the resulting statement is equivalent to (5.1).

6. Proof of Theorem 1

First, we show the independence of the axioms. If F is a field in the usual sense, and a ternary operation is defined on F by (2.1) except that we put $1(1,1) = 0$, then axioms (ii), (iii), and (iv) hold because their

truth does not depend on the element $1(1,1)$, and axiom (i) does not hold. Again, if we define a ternary operation on the same set F by putting $x(y,z) = x+z$, it is easily verified that all the axioms except (ii) hold. If we consider a division ring and define a ternary operation on it by (2.1), then all the axioms except (iii) hold. Finally, if B is a Boolean algebra and we define a ternary operation on B by putting

$$x(y,z) = (x' \cap y) \cup (x \cap z)$$

as in (**1**), then it is easily seen that the first three axioms hold and that if $y \subset z$ then $y \subseteq x(y,z) \subseteq z$. Thus, if y and z are not the least and greatest elements of B, then (iv) must be false.

The next step is to make some deductions from the axioms (i)–(iv); these deductions are stated in Lemmas 4, 5, and 6.

LEMMA 4. *There is a unique element* 0 *of* F *such that in* (ii) *and* (iii) $p = q = 0$. *It also follows that*

$$x(y,y) = y \tag{v}$$

for all x, y *in* F.

Proof. If p and q satisfy (ii) and (iii) respectively, then

$$q = p(q,x) = x(q,p) \quad \text{for all } x.$$

Now if $p \neq q$ then by (iv) there is an element x such that $x(q,p) = p$, which is impossible. Thus $p = q$ for any p and q that satisfy (ii) and (iii), i.e. p is a uniquely defined element of F, which we denote by 0. Thus $x(0,0) = 0$, and (v) follows immediately from $x(0,0)(y,0) = 0(y,0)$.

LEMMA 5. F *is an Abelian group with zero relative to the operation defined by* $xy = x(0,y)$. *There exists a unique element* 1 *in* F *such that*

(ii)′ $1(x,y) = y$,

(iii)′ $x(y,1) = y(x,1)$,

for all x, y *in* F.

Proof. It follows from Lemma 4, (i), (ii), and (iii), that

$$0x = x0 = 0, \quad xy = yx$$

and

$$(xy)z = x(0,y)(0,z) = x(0,y(0,z)) = x(yz).$$

Also, from (iv), if $y \neq 0$ then there exists x such that $xy = u$. Hence F is an Abelian group with zero. Clearly, if an element 1 satisfies (ii)′ then it is the identity of this Abelian group, and so is uniquely determined. Thus we define 1 as the identity of this Abelian group, i.e. we know that $1(0,x) = x(0,1) = x$ Note that $0 \neq 1$, because not all the elements of F

are equal. Hence, by (iv), there is an element t such that $t(1,0) = 0$, and we have

$$x(1,0)(0,t(1,0))(1,0) = 0(1,0) = 1$$

and

$$t(1,0)(0,x(1,0))(1,0) = t(x(1,0),0)(1,0) = t(x(1,0)(1,0),1).$$

If we put $y = x(1,0)(1,0)$ then we have shown that $t(y,1) = 1$. By (iv), this must hold for all y, and in particular there is an x such that $y = 0$. Hence $t = 1$ and $1(y,1) = 1$ for all y. Thus we deduce that

$$1(x,0) = 1(1,0)(0,x) = 0$$

and,

$$\text{if } y \neq 0, \quad 1(x,y) = 1(x(0,y^{-1}),1)(0,y) = 1(0,y) = y,$$

i.e. we have proved (ii)′. Furthermore,

$$x(y,1) = x(1,0)(0,y(1,0))(1,0) = y(x,1).$$

Lemma 5 provides sufficient information for us to be able to make a deduction from Theorem 3. If we put $f(x) = x(1,0)$ then (3.1) and (3.2) are obviously satisfied, and it is easily seen that (3.3) defines a ternary operation identical with the given one; hence Theorem 2 implies that (3.4) holds. Thus F is a field in the usual sense.

The following interesting lemma is not essential for the proof of Theorem 1.

LEMMA 6. *The set* $S = \{(x,y)$: *all* x, y *in* F *such that* $x \neq y\}$ *with the binary operation defined by* $(x,y)(u,v) = (x(u,v), y(u,v))$ *is a group.*

Proof. Suppose, if possible, that for some $u \neq v$ we have

$$x(u,v) = y(u,v) = w, \quad \text{where } x \neq y.$$

Then there is an s such that $s(x,y) = 0$. Hence $s(x,y)(u,v) = u$ and $s(x(u,v),y(u,v)) = w$, i.e. $u = w$. Similarly, if we replace 0 by 1, $v = w$, which is impossible. Thus we must have $x = y$, so that the solution x of (iv) is unique and, equivalently, S is closed under the operation defined above. Also, the associative law follows immediately from (i), $(0,1)$ is the (two-sided) identity, and (iv) implies the existence of left inverses.

To complete the proof of Theorem 1 we note that if $x \neq 1$ we can define x^* uniquely by $x^*(x,1) = 0$. In § 4 we gave another definition of x^*, but it is clear that these two definitions are equivalent. Furthermore, the definitions of addition in § 4 and (2.3) are equivalent.

If $F = \{0,1\}$, there is only one ternary operation that satisfies (ii), (iii), and (iv); clearly, F is the field of integers mod 2, and Theorem 1 holds with $m = 1$. We may now assume that there is an $x \neq 0$, 1, and then all the results of § 4 are applicable. From the ternary operation,

we define addition by (2.3) and multiplication by (2.2). Clearly $x+f(x) = 1$ for all x, so that, if we use the usual notation for a field, $f(x) = 1-x$ and, from (3.3), $x(y,z) = y-xy+xz$ for all x, y, z. It is clear from § 2 that if we start with a field in the usual sense and define a ternary operation by (2.1), then (2.2) and (2.3) simply reproduce the original operations. Thus we have shown that the transformations between the operations are mutually inverse, and the proof of Theorem 1 is complete.

7. The multiplicative group of a division ring

The following result is a natural generalization of Theorem 3. It is not clear that all the conditions (7.1)–(7.5) are necessary. It is also possible to replace these conditions by others, e.g. (7.2) can be replaced by $f(1) = 0$, or (7.5) can be replaced by the condition that x and $f(y)y^{-1}y^*$ commute.

THEOREM 4. *Let G be a group, written multiplicatively with 1 as identity, and let D be obtained by adjoining a zero element 0 to G. Then G is the multiplicative group of a division ring if and only if there exists a mapping $f\colon D \to D$ such that, for all x, y in D,*

$$f(0) = 1, \tag{7.1}$$

$$f(f(x)) = x, \tag{7.2}$$

$$f(xy)x = xf(yx), \tag{7.3}$$

$$\text{if } y \neq 0, \text{ then } \quad f(f(x)f(y)) = f(xf(y^{-1}))y, \tag{7.4}$$

$$\text{if } x \neq 0, \text{ then } \quad f(f(x)f(y)) = xf(f(x^{-1})y). \tag{7.5}$$

Proof. Clearly, if D is a division ring then $f(x) = 1-x$ satisfies (7.1)–(7.5). Conversely, given a mapping f that satisfies (7.1)–(7.5), if we put $y = 1$ in (7.3) we see that x and $f(x)$ commute. Similarly, x^{-1} and $f(x)$ commute. We define x^* as in § 4, and Lemma 1 and its proof are still valid. We now prove that Lemma 2 is also valid: we have $f(x)x^{-1}x^* = x^{-1}f(x)f(f(x)^{-1}) = x^{-1}x^*f(x)$, and if we put $z = y^{-1}$ we see that it is sufficient to prove (4.1). If $xf(z^{-1}) = 1$ then (4.1) certainly holds, and if $xf(z^{-1}) \neq 1$ then we take f of each side of (4.1) and use (7.3) to obtain

$$f(f(x)f(z)) = z^{-1}f(zf(x^{-1})xf(z^{-1}))z.$$

If we use (7.4) on each side, cancel $f(xf(z^{-1}))z$, and rearrange, we get

$$f(z) = f(zf(x^{-1}))f(f(xf(z^{-1}))^{-1});$$

but by (7.5), $f(zf(x^{-1})) = f(z)f(f(f(z)^{-1})x^{-1})$, and $f(f(z)^{-1})x^{-1}$ is the inverse of $xf(z^{-1})$. Hence Lemma 2 is proved. Again we put $m = f(x)x^{-1}x^*$: then

$mx = xm$; hence $mx = xm$ for all x. The rest of the proof follows exactly as in § 4, except for the proof of $x+y = y+x$ when $x, y \neq 1$, which is as follows. (7.3) can be written in the form

$$x^{-1}f(xy) = f(yx)^{-1}, \quad \text{and} \quad f(x^*) = f(x)^{-1};$$

hence we have

$$\begin{aligned} f(yf(x^*))f(x) &= f(x)f(f(x^*)y) \\ &= f(x)f(x^*f(f(y)^{-1}))f(y) \\ &= f(x)f(f(f(x)^{-1})y^*)f(y) \\ &= f(xf(y^*))f(y). \end{aligned}$$

The other distributive law is obtained in a similar way by proving that $z(1+y) = z+zy$. If $z = 0$ this result is obvious, and if $z \neq 0$ then

$$z+zy = f(zyz^{-1}m)z = zf(yz^{-1}mz) = z(1+y).$$

Added in proof

P. M. Cohn (**3**) has obtained a result that can be stated exactly as Theorem 4 except that condition (7.5) is replaced by the statement of Lemma 2. This result is weaker than Theorem 4 because the non-commutative case of Lemma 2 is assumed. To emphasize the difference between these two results, it is better to state Theorem 4 with the additional condition that G has a non-trivial centre and then the conditions (7.1) and (7.5) are redundant.

REFERENCES

1. R. M. Dicker, 'A set of independent axioms for Boolean algebra', *Proc. London Math. Soc.* (3) 13 (1963) 20–30.
2. L. Fuchs, *Abelian groups* (Oxford, 1960).
3. P. M. Cohn, 'On the embedding of rings in skew fields', *Proc. London Math. Soc.* (3) 11 (1961) 511–30.

Department of Mathematics
The University
Dundee