Groups as groupoids with one law.

By GRAHAM HIGMAN and B. H. NEUMANN in Manchester.

§ 1.

Many authors have studied axiom systems for groups; their interest has been primarily in *axiomatics*. Though a new set of axioms for groups is given in this note, it arises in answer to an *algebraic* question.

It is known [1]) that groups can be defined in terms of a single binary operation, viz. right division. Multiplication and inversion can easily be defined in terms of right division. An algebraic system which is closed under a binary operation is called a *groupoid*. Groups then are groupoids with respect to right division [2]); they can be singled out from the groupoids in general by means of certain laws (or "rules", "identical relations"), that is equations between certain expressions in variables combined by the groupoid operation, these equations being valid for all values of the variables. We say (following P. HALL) that groups form a *variety* of groupoids. Within this variety we can single out subvarieties by postulating further laws, e. g. the variety of abelian groups by the law expressing (in our case in terms of right division) the commutativity of multiplication, or the variety of groups of exponent n by the law expressing that all n^{th} powers equal the unit element.

The question we here propose is: How few laws suffice to determine the variety of groups (as a subvariety of that of groupoids), or any subvariety of the variety of groups? The answer is complete for groups and for some subvarieties:

Every variety of groups which can be defined by a finite system of laws qua subvariety of the variety of groups can be defined by a single law qua subvariety of the variety of groupoids. In particular the variety of all groups can be obtained from that of groupoids by a single law.

We draw attention in passing to the unsolved problem whether there is any variety of groups which can not be defined by a finite set of laws [3]).

---

[1]) WARD [5], LORENZEN [3].

[2]) Also, of course, with respect to multiplication, or left division, or commutation, etc.

[3]) Cf. HIGMAN [2] for a partial solution.

It is an immediate consequence of our proposition that every variety of groups to which it applies can be axiomatised by three postulates [4]): Two to ensure the existence and unicity of the result of the groupoid operation, and a further one to ensure the validity of the single law required. The last one can be so formulated as to make it formally independent of the existence and unicity postulates.

§ 2.

We denote by ϱ the binary operation which we wish to turn into right division in a group. It will be written as a right operator; if the result of ϱ operating upon the (ordered) pair a, b is c, we write

$$ab\varrho = c.$$

This notation (due, we believe, to ŁUKASIEWICZ) avoids brackets. Thus the two possible "products" of a, b, c, are $ab\varrho c\varrho$ and $abc\varrho\varrho$. The operation gives rise to two kinds of mapping of the groupoid into itself: *the right multiplications* R_a, defined for every element a of the groupoid by

$$xR_a = xa\varrho,$$

x ranging over the groupoid; and the *left multiplications* L_a, defined correspondingly by

$$xL_a = ax\varrho.$$

We denote mappings of the groupoid into itself by capitals and write them as right operators. The identical permutation of the groupoid is I. The following well-known facts will be used without explicit reference.

The mappings of the groupoid (or in fact any set) into itself form a semigroup with unit element I. *The mappings which possess left inverses are the mappings onto the groupoid; the mappings with right inverses are the one-to-one mappings. The mappings with both left and right inverses form the group of permutations of the groupoid. If* $RS = P$, *where* P *is a permutation, then the mapping* R *has a right inverse, i. e. it is one-to-one, and the mapping* S *has a left inverse, i. e. it is onto the groupoid.*

If all left and right multiplications are permutations, then the groupoid is a *quasigroup*.

It is not difficult to show, using e. g. the axiom system of LORENZEN [3], that the following two laws make the groupoid into a group, with right division as the operation ϱ:

$$xz\varrho\, yz\varrho\varrho = xy\varrho. \tag{2.1}$$

$$xx\varrho\, yy\varrho\, y\varrho\varrho = y. \tag{2.2}$$

For LORENZEN's postulate A is equivalent to saying that the system is a groupoid, (2.1) is (a slightly strengthened form of) his B, and (2.2) implies his Γ.

[4]) In the case of groups and of abelian groups this fact is not new. Cf. e. g. GARVER [1], LORENZEN [4].

Abelian groups are obtained if we subject ϱ to the further law [5]):

$$xxy\varrho\varrho = y. \tag{2.3}$$

Any other variety of groups which can be defined by a finite set of laws can be thought of as defined by just one further law (in addition to the group laws (2.1) aud (2.2)). For one only has to express all the laws in terms of *different* variables, let us say

$$u_i(x_{i1}, x_{i2}, \ldots, x_{in(i)}) = v_i(x_{i1}, x_{i2}, \ldots, x_{in(i)}) \qquad (i = 1, \ldots, m)$$

and then to combine them into the single law

$$u_1 u_2 \ldots u_m \varrho \ldots \varrho = v_1 v_2 \ldots v_m \varrho \ldots \varrho. \tag{2.4}$$

If the unit element [6]) e which is the (demonstrably constant) value of $xx\varrho$, is substituted for all the variables except those occurring in the i^{th} law $u_i = v_i$, then (2.4) leads to $u_i = v_i$ or to $eu_i\varrho = ev_i\varrho$, from which the i^{th} law again follows. It entails no loss of generality if we assume the laws so formulated that every v_i equals the unit element, so that the right-hand side of (2. 4) also equals the unit element.

§ 3.

We may then assume that the variety of groups we want to single out is defined by a law

$$w \equiv w(x_1, x_2, \ldots, x_n) = e \tag{3.1}$$

where w is some word in variables. If we want to obtain the variety of *all* groups we shall simply think of w as the empty word.

3. 2. Theorem. *The variety of groups with the law* (3.1) *is the variety of groupoids (with respect to right division* ϱ*) defined by the single law*

$$xxx\varrho w\varrho\, y\varrho z\varrho\, xx\varrho\, x\varrho\, z\varrho\varrho\varrho = y. \tag{3.21}$$

The variety of all groups in particular is defined by the law

$$xxx\varrho\, y\varrho z\varrho\, xx\varrho\, x\varrho\, z\varrho\varrho\varrho = y. \tag{3.22}$$

We can express the law (3. 21) in terms of left and right multiplications:

$$yL_{xx\varrho w\varrho}R_zR_{xx\varrho x\varrho z\varrho}L_x = y$$

or, noting that y ranges over the whole groupoid,

$$L_{xx\varrho w\varrho}R_zR_{xx\varrho x\varrho z\varrho}L_x = \mathrm{I}. \tag{3.3}$$

From this we see that L_x has a left inverse: thus all left multiplications are

[5]) (2. 2) is easily seen to follow from (2. 1) and (2. 3) and can then be omitted; cf. LORENZEN [3].

[6]) The unit element (sc. of group multiplication, which does not enter this account explicitly) is a right neutral of ϱ but not a left neutral (unless we are dealing with a group of exponent 2).

onto the groupoid. $L_{xx\varrho w\varrho}$ has, moreover, a right inverse, hence is a permutation. If we now write

$$R_z R_{xx\varrho x\varrho z\varrho} L_x = L^{-1}_{xx\varrho w\varrho}, \tag{3.31}$$

we see that R_z has a right inverse: thus all right multiplications are one-to-one. If we choose in particular $x = x'x'\varrho w\varrho$ then L_x is also a permutation, and from

$$R_z R_{xx\varrho x\varrho z\varrho} = L^{-1}_{xx\varrho w\varrho} L_x^{-1} \tag{3.32}$$

we see that $R_{xx\varrho x\varrho z\varrho}$ has — for this special choice of x — also a left inverse: thus it is a permutation. Then also

$$R_z = L^{-1}_{xx\varrho w\varrho} L_x^{-1} R^{-1}_{xx\varrho x\varrho z\varrho}$$

is a permutation. But R_z does not depend on the special choice of x, and we have shown that *all right multiplications are permutations.* But then we obtain from (3.31) for arbitrary x that also

$$L_x = R^{-1}_{xx\varrho x\varrho z\varrho} R_z^{-1} L^{-1}_{xx\varrho w\varrho}$$

is a permutation. This shows that *all left multiplications are permutations,* and *the groupoid is a quasigroup.*

Now (3.32) is seen to remain valid for arbitrary choice of x, and shows that $R_z R_{xx\varrho x\varrho z\varrho}$ does not depend on z. Hence we have identically

$$yz\varrho xx\varrho x\varrho z\varrho\varrho = yz'\varrho xx\varrho x\varrho z'\varrho\varrho. \tag{3.4}$$

Here we choose in particular $y = xx\varrho x\varrho$, and z and z' such that $xx\varrho x\varrho z\varrho = u$ and $xx\varrho x\varrho z'\varrho = v$ take arbitrarily prescribed values u and v: that is, we put $z = uL^{-1}_{xx\varrho x\varrho}$, $z' = vL^{-1}_{xx\varrho x\varrho}$. Then (3.4) becomes

$$uu\varrho = vv\varrho. \tag{3.5}$$

As u and v are arbitrary, this shows that $uu\varrho$ is a constant element. We denote this element by e and note that for all x

$$xx\varrho = ee\varrho = e. \tag{3.51}$$

Now (3.3) simplifies to

$$L_{ew\varrho} R_z R_{ex\varrho z\varrho} L_x = \mathrm{I}.$$

We observe that $L_{ew\varrho}$ does not depend on the value of w. But then — as we have a quasigroup — $ew\varrho$ and also w itself must be constant, i. e. independent of the variables $x_1, \ldots, x_n$ entering it. If we substitute in particular e for all these variables, then we obtain $w = e$ (by repeated application of $ee\varrho = e$), hence the constant value of w is e. Hence *the law* (3.1) *holds in the groupoid.*

Now (3.21) (or (3.22)) simplifies to

$$xey\varrho z\varrho ex\varrho z\varrho\varrho\varrho = y. \tag{3.6}$$

If we here put $x = y$ and observe that by (3.51)

$$ey\varrho z\varrho\, ey\varrho z\varrho\varrho = e,$$

we get

$$ye\varrho = y.$$

Thus

$$R_e = \mathrm{I},$$

in other words, *e is a right neutral element* of the operation ϱ.

Now we put $x = z = e$ in (3.6), and obtain

$$eey\varrho\varrho = y,$$

or

$$L_e^2 = \mathrm{I}.$$

Here we replace the first e by $xx\varrho$, the second by $yy\varrho$, and find that *the law* (2.2) *holds in the groupoid.*

From (3.6) we see that

$$ey\varrho z\varrho\, ex\varrho z\varrho\varrho \quad (= yL_x^{-1})$$

does not depend on z. Thus

$$ey\varrho z\varrho\, ex\varrho z\varrho\varrho = ey\varrho\, ex\varrho\varrho, \tag{3.7}$$

the right-hand side being obtained by putting $z = e$.

We put, with new variables u, v, $y = e\,u\varrho$, $x = ev\varrho$ or, equivalently, $u = ey\varrho$, $v = ex\varrho$. Then (3.7) becomes

$$uz\varrho\, vz\varrho\varrho = uv\varrho,$$

which differs from (2.1) only in the names of the variables. Hence *the law* (2.1) *is satisfied in the groupoid.*

It only remains to verify that groups with the law (3.1) satisfy (3.21), or that groups in general satisfy (3.22): This verification is straightforward, and we omit it. This completes the proof of the theorem.

§ 4.

As far as the variety of all groups is concerned, Theorem 3.2 is optimal in more than one respect. Clearly at least one law is required to single out the groups from the groupoids. If there is only one

$$u(x, y, \ldots) = v(x, y, \ldots),$$

then one of the words u, v must have length 1, i. e. consist of a single variable, and the other must involve at least three different variables and have odd length $\geqq 9$. These statements are not very difficult to prove, though the last one is laborious to verify. We omit the proofs.

Theorem 3.2 provides a uniform method to find a single law defining any sub-variety of groups which satisfies the conditions of the theorem; it may, however, be possible to define such a variety by a law in fewer variables, or by a shorter law than (3.21). Thus for abelian groups (3.21) uses five variables and the left-hand side has length 13. We now show that three variables in a word of length 5 suffice (both numbers are again the least possible).

4. 1. Theorem. *The variety of abelian groups is defined (in terms of division) by the law*

$$xyz\varrho yx\varrho\varrho\varrho = z. \tag{4. 11}$$

It is again a matter of straightforward verification — which we omit — to show that the law is satisfied in abelian groups. In terms of left and right multiplications it becomes

$$zL_yR_{yx\varrho}L_x = z,$$

that is to say,

$$L_yR_{yx\varrho}L_x = \mathrm{I}. \tag{4. 2}$$

Here we see at once that L_y has a right inverse and a left inverse, hence *the left multiplications are permutations.* Then $R_{yx\varrho}$ is also a permutation, and as $yx\varrho$ ranges over the whole groupoid, *all right multiplications are permutations,* and *the groupoid is a quasigroup.*

Next we notice that

$$L_yR_{yx\varrho} = L_x^{-1}$$

does not depend on y; hence

$$yz\varrho\, yx\varrho\varrho = tz\varrho\, tx\varrho\varrho. \tag{4. 3}$$

Here we first put $z = x$ and $y = uR_x^{-1}$, $t = vR_x^{-1}$, with arbitrary u and v. Then $yz\varrho = yx\varrho = u$, $tz\varrho = tx\varrho = v$, and (4. 3) gives

$$uu\varrho = vv\varrho.$$

Denoting this constant element again by e, we have, as before (cf. (3. 51))

$$xx\varrho = ee\varrho = e.$$

Now we put $z = x$ in (4. 11), and observe that $yx\varrho\, yx\varrho\varrho = e$. We get

$$xe\varrho = x, \quad R_e = \mathrm{I}.$$

If we now put $x = y$ in (4. 11) we also get

$$xxz\varrho\varrho = z, \; L_x^2 = \mathrm{I}. \tag{4. 4}$$

This shows that *the law* (2. 3) *is satisfied* by our groupoid.

With $t = x$ and $t = z$ in turn, (4. 3) now gives

$$yz\varrho\, yx\varrho\varrho = xz\varrho = ezx\varrho\varrho. \tag{4. 5}$$

Thus

$$xz\varrho\, yz\varrho\varrho = ezx\varrho\varrho\, ezy\varrho\varrho\varrho; \tag{4. 51}$$

applying (4. 5) again, with $e, zx\varrho, zy\varrho$ taking the place of y, z, x, we next obtain

$$ezx\varrho\varrho\, ezy\varrho\varrho = zy\varrho\, zx\varrho\varrho; \tag{4. 52}$$

we apply (4. 5) once more, with y and z interchanged:

$$zy\varrho\, zx\varrho\varrho = xy\varrho. \tag{4. 53}$$

Finally we combine (4. 51-3) to

$$xz\varrho\, yz\varrho\varrho = xy\varrho,$$

which shows that *the law* (2. 1) *is also satisfied* by the groupoid. Hence *the groupoid is an abelian group*, and the theorem follows.

§ 5.

We conclude by drawing attention to some unsolved problems. Instead of defining a certain variety of groupoids, say groups, by as few laws as possible, one may try to define it by a system of as many irredundant laws as possible — if there is an upper bound to the number of laws in an irredundant system. We can show that every irredundant system must certainly be finite if the variety can be defined by *some* finite system of laws (as is the case with all the varieties we have here considered); but that the number of laws in an irredundant system can be unbounded. It is not known whether it is bounded e. g. for the variety of groups or that of abelian groups. No variety of groupoids requiring infinitely many laws for its definition appears to be known; a related problem is to find the cardinal of the set of varieties of groupoids.[7])

Another problem is this: is there any binary operation in a group, other than right division or left division and their transposes, in terms of which all group operations can be expressed? It is not difficult to answer the same question for abelian groups: any binary operation in an abelian group in terms of which the others can be expressed is either division, $ab\varrho = a \cdot b^{-1}$, or its transpose, $ab\varrho = b \cdot a^{-1}$.

References.

[1] Garver, Raymond: A definition of group by means of three postulates. *Amer. J. Math.* **57** (1935), 276—280.

[2] Higman, Graham: Ordering by divisibility in abstract algebras. *Proc. London Math. Soc.* (3) **2** (1952), 326—336.

[3] Lorenzen, P.: Ein vereinfachtes Axiomensystem für Gruppen. *J. reine angew. Math.* **182** (1940), 50.

[4] Lorenzen, Paul: Ein Beitrag zur Gruppenaxiomatik. *Math. Z.* **49** (1944), 313—327.

[5] Ward, Morgan: Postulates for the inverse operations in a group. *Trans. Amer. Math. Soc.* **32** (1930), 520—526.

(Received April 18, 1952.)

[7]) These last problems have recently been solved.