

# STRUCTURE OF ABELIAN QUASI-GROUPS

BY

D. C. MURDOCH

## INTRODUCTION

One of the most noticeable features of non-associative group-like systems is that the lack of associativity removes nearly all the power from the commutative law. For example, although many properties of groups are retained in systems which satisfy certain generalized associative laws, the addition of the commutative law does not usually reduce these systems to anything analogous to abelian groups. The properties which one usually associates with an abelian group, and which one would wish to retain in any non-associative generalization of this concept, are

- (a) Indices may be distributed:  $(ab)^r = a^r b^r$ .
- (b) All subgroups are normal.
- (c) The subgroups form a Dedekind structure.

A fourth property which naturally comes to mind is that every abelian group is a direct product of cyclic groups. This, however, does not lend itself to generalization since the cyclic group itself loses all its simplicity when the associative law is relaxed. It will therefore play no part in the considerations of this paper.

A definition of an *abelian quasi-group* which retains the above three properties has previously been given<sup>(1)</sup>. It is a system closed under multiplication, which satisfies the quotient axiom and the generalized associative-commutative law  $(ab)(cd) = (ac)(bd)$ . It is the purpose of this paper to give a complete account of the structure of these systems. The problem of constructing all abelian quasi-groups is solved in the sense that it is reduced to a group-theoretical problem. It is first shown, by consideration of the problem of extension, that every abelian quasi-group is a direct product of a self-unit quasi-group (one in which every element is a right unit) and one which contains an idempotent element. This latter type can always be constructed by performing certain transformations on the Cayley square of an abelian group, while the self-unit quasi-groups result from two applications of the same process. The results appear to indicate that the classic problems of extension, automorphisms, etc., although more cumbersome to handle, are not essentially more difficult than for abelian groups.

---

Presented to the Society in part October 28, 1939, under the title *Further theory of quasi-groups*, and in part April 26, 1940, under the title *A characterization of abelian quasi-groups*; received by the editors April 15, 1940.

<sup>(1)</sup> D. C. Murdoch, *Quasi-groups which satisfy certain generalized associative laws*, American Journal of Mathematics, vol. 61 (1939), pp. 509–522.

The results of §II, on extensions by a factor group with unique right unit, are not essential to the main arguments of the paper. Attention is drawn to the three theorems which give the key to the construction of all abelian quasi-groups by labelling them the first, the second, and the third structure theorems.

# I. ABELIAN QUASI-GROUPS AND THEIR FUNDAMENTAL PROPERTIES

**1. Abelian quasi-groups.** We shall understand by an *abelian quasi-group*  $\mathfrak{G}$  a system of elements which satisfies the following three postulates:

(A) For any ordered pair of elements  $a, b$  of  $\mathfrak{G}$  there is a unique product  $ab$  which is an element of  $\mathfrak{G}$ .

(B) If  $a, b$  are any two elements of  $\mathfrak{G}$ , there exist in  $\mathfrak{G}$  unique elements  $x$  and  $y$  such that  $ax=b, ya=b$ .

(C) If  $a, b, c, d$  are any four elements of  $\mathfrak{G}$ , then

$$(1) \quad (ab)(cd) = (ac)(bd).$$

With the exception of the last section, this paper is concerned exclusively with abelian quasi-groups, and we shall therefore use the term quasi-group, except in that section, to mean abelian quasi-group. We shall also confine our attention to finite quasi-groups. With this restriction any subset of  $\mathfrak{G}$  which is closed under multiplication will form a subquasi-group. Finally, we shall, where convenient, use the terms subgroup and factor group to mean subquasi-group and factor quasi-group without implying that the systems in question are associative. This will lead to no confusion since we shall have no occasion to consider subquasi-groups or factor quasi-groups which are groups in the ordinary sense.

For convenience of reference we shall list some of the chief properties of abelian quasi-groups previously obtained<sup>(2)</sup>.

1. If  $a$  and  $b$  are two elements of a quasi-group  $\mathfrak{G}$  and  $\phi(a), \psi(a)$  denote two "powers" of  $a$ , then

$$\phi(a)\phi(b) = \phi(ab), \quad \psi[\phi(a)] = \phi[\psi(a)].$$

This generalizes the index law  $(ab)^r = a^r b^r$  of abelian groups. It may be stated more generally as follows:

1 (a). If  $a_1, \dots, a_n$  and  $b_1, \dots, b_n$  are two sets of elements of  $\mathfrak{G}$  and if  $\phi(a_1, \dots, a_n)$  denotes some product formed from the elements  $a_1, \dots, a_n$ , then

$$\begin{aligned} \phi(a_1, \dots, a_n)\phi(b_1, \dots, b_n) &= \phi(a_1 b_1, \dots, a_n b_n), \\ \psi[\phi(a_1, \dots, a_n)] &= \phi[\psi(a_1), \dots, \psi(a_n)]. \end{aligned}$$

This may be proved by induction on the total number of elements multiplied together to form  $\phi(a_1, \dots, a_n)$ .

<sup>(2)</sup> For proofs, see D. C. Murdoch, op. cit.

2. Every element  $a$  of  $\mathfrak{G}$  has a right unit  $e_a$ . All right units of  $\mathfrak{G}$  form a subgroup  $\mathfrak{R}$  and  $a \rightarrow e_a$  is a homomorphic mapping of  $\mathfrak{G}$  on  $\mathfrak{R}$ .

We shall refer to  $\mathfrak{R}$  as the right unit group of  $\mathfrak{G}$ .

3. If  $\mathfrak{H}$  is any subgroup of  $\mathfrak{G}$ , two cosets  $a\mathfrak{H}$  and  $b\mathfrak{H}$  are either identical or have no elements in common.

This follows from the necessary and sufficient conditions for the existence of coset expansions as given by Hausmann and Ore<sup>(3)</sup>, or it may be proved independently as follows:

If  $a\mathfrak{H}$  and  $b\mathfrak{H}$  contain common elements, there exist elements  $h_1$  and  $h_2$  of  $\mathfrak{H}$  such that  $ah_1 = bh_2$ . We then have

$$a\mathfrak{H} = (ae_a)(h_1\mathfrak{H}) = (ah_1)(e_a\mathfrak{H}) = (bh_2)(e_a\mathfrak{H}) = (be_a)\mathfrak{H} = b_1\mathfrak{H}.$$

Hence there is an element  $h_3$  of  $\mathfrak{H}$  such that  $ah_1 = (be_a)h_3$  and by repetition of the above argument,  $a\mathfrak{H} = b_n\mathfrak{H}$  where  $b_n$  is defined by  $b_n = b_{n-1}e_a$  and  $b_1 = be_a$ . But since  $\mathfrak{G}$  is finite there exists an  $n$  such that  $b_n = b$ , and therefore  $a\mathfrak{H} = b\mathfrak{H}$ .

4. Every element of a coset  $a\mathfrak{H}$  defines the same coset  $(ah)\mathfrak{H}$  which is independent of  $h$ , and is equal to  $a\mathfrak{H}$  if and only if  $\mathfrak{H}$  contains  $e_a$ . Every subgroup  $\mathfrak{H}$  of  $\mathfrak{G}$  is normal in the sense that its cosets form a factor group  $\mathfrak{G}/\mathfrak{H}$  homomorphic to  $\mathfrak{G}$ .

It follows from (1) that left (or right) multiplication by an idempotent element  $e$  is an automorphism of  $\mathfrak{G}$ . The properties of the factor group  $\mathfrak{G}/\mathfrak{H}$  may therefore be stated as follows:

5. If  $\mathfrak{R}$  is the right unit group, and  $\mathfrak{H}$  any subgroup of  $\mathfrak{G}$ , the factor group  $\mathfrak{G}/\mathfrak{H}$  has a unique right unit if and only if  $\mathfrak{H} \supseteq \mathfrak{R}$ . The mapping of every coset  $a\mathfrak{H}$  on the coset defined by any element of  $a\mathfrak{H}$  is an automorphism of  $\mathfrak{G}/\mathfrak{H}$  equivalent to right multiplication by the idempotent element  $\mathfrak{H}$ .

Finally, it is known that the subgroups of  $\mathfrak{G}$  which contain any given subgroup form a Dedekind structure. Hence principal chains between  $\mathfrak{G}$  and any fixed minimal subgroup all have the same length. That principal chains terminating in different minimal subgroups need not have the same length is illustrated by the example in §8.

2. **Cyclic quasi-groups.** A cyclic quasi-group is one which is generated by a single element. In general not much can be said about such systems, since the usual machinery for dealing with powers breaks down owing to the lack of the associative law. We shall give two results, however, which hold in the abelian case.

**THEOREM 1.** *The automorphisms of a cyclic abelian quasi-group form an abelian group.*

**Proof.** Let  $\mathfrak{G}$  be an abelian quasi-group generated by an element  $a$  and

(3) B. A. Hausmann and O. Ore, *Theory of quasi-groups*, American Journal of Mathematics, vol. 59 (1937), pp. 983–1004. See also D. C. Murdoch, op. cit., p. 512.

let  $S$  and  $T$  be any two automorphisms of  $\mathfrak{G}$ . Then if  $a^S = \phi_1(a)$  and  $a^T = \phi_2(a)$ , we have

$$a^{ST} = \phi_1[\phi_2(a)], \quad a^{TS} = \phi_2[\phi_1(a)],$$

whence  $ST = TS$  by 1, §1.

It follows from this theorem that a cyclic quasi-group can contain at most one idempotent element, for it is easily shown that the automorphisms of  $\mathfrak{G}$  defined by multiplication by two distinct idempotent elements do not commute. More generally, we can prove:

**THEOREM 2.** *A cyclic abelian quasi-group contains only one minimal subgroup.*

**Proof.** Let  $\mathfrak{R}_1$  and  $\mathfrak{R}_2$  be two minimal subgroups of  $\mathfrak{G}$  and let  $\phi(a)$  be any element of  $\mathfrak{R}_1$  where  $a$  is a generating element of  $\mathfrak{G}$ . Now if  $\psi(a)$  is any element of  $\mathfrak{R}_2$  then  $\phi[\psi(a)] = \psi[\phi(a)]$  is an element of both  $\mathfrak{R}_1$  and  $\mathfrak{R}_2$ . Hence  $\mathfrak{R}_1$  and  $\mathfrak{R}_2$  have a non-void crosscut and since both are minimal they must be identical.

It follows from Theorem 2 that the subgroups of a cyclic quasi-group always form a Dedekind structure.

**3. Direct products.** Given two quasi-groups  $\mathfrak{G}$  and  $\mathfrak{H}$  it is always possible to construct a third quasi-group  $\mathfrak{G} \times \mathfrak{H}$  which we shall call their *direct product*. The direct product is defined as the quasi-group consisting of all element pairs  $(g, h)$ , where  $g$  belongs to  $\mathfrak{G}$  and  $h$  to  $\mathfrak{H}$ , in which multiplication is defined by

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2).$$

The multiplication so defined satisfies (1) and the ordinary laws of direct products hold with one important exception. This is that the component quasi-groups  $\mathfrak{G}$  and  $\mathfrak{H}$  are not necessarily subgroups of  $\mathfrak{G} \times \mathfrak{H}$ . If  $\mathfrak{H}$  contains an idempotent element, then  $\mathfrak{G}$  will be a subgroup of  $\mathfrak{G} \times \mathfrak{H}$  but otherwise this will not in general be the case. It should also be noted that the right unit group of  $\mathfrak{G} \times \mathfrak{H}$  is the direct product of the right unit groups of  $\mathfrak{G}$  and  $\mathfrak{H}$ .

**4. The right unit series.** Let  $\mathfrak{R}_1$  be the right unit group of  $\mathfrak{G}$ ,  $\mathfrak{R}_2$  the right unit group of  $\mathfrak{R}_1$ ,  $\mathfrak{R}_3$  that of  $\mathfrak{R}_2$ , and so on. Since  $\mathfrak{G}$  is assumed finite, we must finally reach a subgroup  $\mathfrak{R}_t$  which is its own right unit group. Such a quasi-group, in which every element is a right unit, shall be called *self-unit*. This series of subgroups,

$$\mathfrak{G} \supset \mathfrak{R}_1 \supset \mathfrak{R}_2 \supset \cdots \supset \mathfrak{R}_t$$

shall be called the *right unit series* of  $\mathfrak{G}$ , and the number  $t$  of distinct successive right unit subgroups in the series, the *length* of  $\mathfrak{G}$ .

We shall use the letter  $U$  throughout to denote the mapping of each element of a quasi-group on its right unit. The right unit series can then be written

$$\mathfrak{G} \supset \mathfrak{G}^U \supset \mathfrak{G}^{U^2} \supset \dots \supset \mathfrak{G}^{U^t}.$$

It should also be noted that the final term  $\mathfrak{R}_t = \mathfrak{G}^{U^t}$  of this series is the maximal self-unit subgroup of  $\mathfrak{G}$  in the sense that every self-unit subgroup is contained in it. For if  $\mathfrak{R}$  is self-unit we have

$$\mathfrak{R} = \mathfrak{R}^{U^t} \subset \mathfrak{R}_t.$$

The factor group  $\mathfrak{G}/\mathfrak{R}_t$  will also have length  $t$  and its maximal self-unit subgroup will be a single idempotent element.

Let  $\mathfrak{F}_i$  be the factor group  $\mathfrak{R}_{i-1}/\mathfrak{R}_i$ ,  $i=1, 2, \dots, t$ , where  $\mathfrak{R}_0 = \mathfrak{G}$ . Then each  $\mathfrak{F}_i$  has a unique right unit. Since  $U$  is a homomorphism which maps each  $\mathfrak{R}_{i-1}$  on  $\mathfrak{R}_i$  we have for  $i=1, 2, \dots, t-1$ ,

$$\frac{\mathfrak{R}_{i-1}}{\mathfrak{R}'_i} \simeq \frac{\mathfrak{R}_i}{\mathfrak{R}_{i+1}} \simeq \mathfrak{F}_{i+1},$$

where  $\mathfrak{R}'_i$  is the subgroup of  $\mathfrak{R}_{i-1}$  consisting of all elements of  $\mathfrak{R}_{i-1}$  which have right units in  $\mathfrak{R}_{i+1}$ . Evidently  $\mathfrak{R}'_i \supseteq \mathfrak{R}_i$  and therefore  $\mathfrak{F}_i$  contains a subgroup  $\mathfrak{M}_i \simeq \mathfrak{R}'_i/\mathfrak{R}_i$  such that

$$\frac{\mathfrak{F}_i}{\mathfrak{M}_i} \simeq \mathfrak{F}_{i+1}.$$

These results may be summed up as follows:

**THEOREM 3.** *Let  $\mathfrak{G} = \mathfrak{R}_0 \supset \mathfrak{R}_1 \supset \dots \supset \mathfrak{R}_t$  be the right unit series of  $\mathfrak{G}$  and let  $\mathfrak{F}_i$  be the factor group  $\mathfrak{R}_{i-1}/\mathfrak{R}_i$ ,  $i=1, 2, \dots, t$ . Then each  $\mathfrak{F}_i$  has a unique right unit, and is an extension of some quasi-group  $\mathfrak{M}_i$  by the factor group  $\mathfrak{F}_{i+1}$ .*

**COROLLARY.** *If  $g$  is the order of  $\mathfrak{G}$  and  $m_i$  the order of  $\mathfrak{M}_i$ ,  $f$  that of  $\mathfrak{F}_t$ , and  $r$  that of  $\mathfrak{R}_t$ , then*

$$g = m_1 m_2 m_3 \dots m_{t-1} \cdot f^t \cdot r.$$

Any or all of the  $m_i$  may be unity, but a quasi-group of length  $t$  must be divisible by the  $t$ th power of an integer, namely  $f^t$ . If each  $m_i$  is unity, then all the factor groups  $\mathfrak{F}_i$  are isomorphic.

From the preceding it follows that any quasi-group of length  $t$  can be obtained from its maximal self-unit subgroup either by a series of  $t$  extensions by factor groups having unique right unit, or by a single extension by a factor group of length  $t$  whose maximal self-unit subgroup is a single element. We shall therefore turn now to a study of the process of extension. We shall first treat the problem of the extension of any quasi-group  $\mathfrak{G}$  by a factor group  $\mathfrak{F}$  with unique right unit. The same problem when  $\mathfrak{F}$  does not have a unique right unit becomes very complicated. One special case, however, can be completely solved, namely the case in which  $\mathfrak{G}$  is self-unit and the maximal self-

unit subgroup of  $\mathfrak{F}$  consists of a single element. This case is sufficient for our purposes and will be treated in §III.

## II. EXTENSIONS BY A FACTOR GROUP WITH UNIQUE RIGHT UNIT

**5. Extensions which preserve the right unit group.** Let  $\mathfrak{S}$  be any given quasi-group with right unit group  $\mathfrak{R}$  and let  $\mathfrak{F}$  be a quasi-group with unique right unit  $e$ . It is required to construct an abelian quasi-group  $\mathfrak{G}$  containing  $\mathfrak{S}$  as subgroup and such that  $\mathfrak{G}/\mathfrak{S} \simeq \mathfrak{F}$ . We shall consider only the case in which the extended group  $\mathfrak{G}$  has the same right unit group as  $\mathfrak{S}$ , namely  $\mathfrak{R}$ . It is clear from §3 that one such extension  $\mathfrak{G}$  always exists, namely the direct product  $\mathfrak{S} \times \mathfrak{F}$ . We shall use Latin capitals for elements of  $\mathfrak{S}$  and small Greek letters for elements of  $\mathfrak{F}$  other than the right unit  $e$ .

If  $\mathfrak{G}$  is an extension of  $\mathfrak{S}$  by  $\mathfrak{F}$ , having right unit group  $\mathfrak{R}$ , then  $\mathfrak{G}$  splits into cosets modulo  $\mathfrak{S}$  of the form

$$\mathfrak{G} = g_e \mathfrak{S} + g_\sigma \mathfrak{S} + g_\tau \mathfrak{S} + \cdots.$$

Here  $g_e \in \mathfrak{S}$  and the representatives  $g_e, g_\sigma, g_\tau, \cdots$  multiply according to the law

$$(2) \quad g_\sigma g_\tau = g_{\sigma\tau} C_{\sigma,\tau},$$

where the elements of the factor set  $C_{\sigma,\tau}$  belong to  $\mathfrak{S}$ . Since  $\mathfrak{G}$  has right unit group  $\mathfrak{R}$ , each representative  $g_\sigma$  has a right unit  $E_\sigma$  in  $\mathfrak{R}$ . Hence every element of  $\mathfrak{R}$  is the right unit of at least one element in each coset  $g_\sigma \mathfrak{S}$ . Thus it is always possible to choose a set of representatives  $\{g_\sigma\}$  all of which have the same right unit. Such a set shall be called a *normal* set of representatives.

Taking right units of (2) we have

$$E_\sigma E_\tau = E_{\sigma\tau} C'_{\sigma,\tau},$$

where  $C_{\sigma,\tau}$  is the right unit of  $C_{\sigma,\tau}$ . Hence if  $\{g_\sigma\}$  is a normal set of representatives the elements of the factor set must all have the same right unit. If  $\mathfrak{S}$  is self-unit, this implies that all  $C_{\sigma,\tau}$  are equal, and since any element of  $\mathfrak{S}$  may then be chosen as factor set it follows that only one extension is possible in this case, namely the direct product.

If  $\mathfrak{S}$  is not self-unit more possibilities occur, but a factor set for any extension can always be chosen so that its elements all have the same right unit. An analysis similar to that of Schreier<sup>(4)</sup> for ordinary groups yields the following:

**THEOREM 4.** *Let  $\mathfrak{S}$  have right unit group  $\mathfrak{R}$  and  $\mathfrak{F} (e, \sigma, \tau, \cdots)$  have right*

<sup>(4)</sup> O. Schreier, *Über die Erweiterung von Gruppen* I, Monatshefte für Mathematik und Physik, vol. 34 (1926), pp. 165–180, or H. Zassenhaus, *Lehrbuch der Gruppentheorie*, vol. 1, pp. 89–93.

unit  $e$ . The necessary and sufficient conditions for the existence of an abelian extension  $\mathfrak{G}$  of  $\mathfrak{S}$  by  $\mathfrak{F}$  having right unit group  $\mathfrak{R}$  are that there exist elements  $C_{\sigma,\tau}$  in  $\mathfrak{S}$  and  $E_\sigma$  in  $\mathfrak{R}$  satisfying the following three conditions:  $C_{\sigma,e}$  are equal for all  $\sigma$ ,

$$(3) \quad E_\sigma E_\tau = E_{\sigma\tau} C'_{\sigma,\tau},$$

$$(4) \quad C_{\sigma\tau,\mu\rho} [C_{\sigma,\tau} C_{\mu,\rho}]^{S_{\sigma\tau \cdot \mu\rho}} = C_{\sigma\mu,\tau\rho} [C_{\sigma,\mu} C_{\tau,\rho}]^{S_{\sigma\mu \cdot \tau\rho}},$$

where the operation  $S_\sigma$  is defined by  $E_\sigma X^{S_\sigma} = X$ .

**Proof.** The necessity of these conditions follows from (2),  $E_\sigma$  being the right unit of the coset representative  $g_\sigma$ . Condition (4) arises from imposing the law (1) on the extended quasi-group. We shall sketch the proof of sufficiency insofar as it differs from the corresponding proof in the case of groups.

Let  $C_{\sigma,\tau}$  and  $E_\sigma$  be given satisfying the three conditions of the theorem. We then construct the set  $\mathfrak{G}$  of all elements  $g_\sigma A$  where  $\sigma$  belongs to  $\mathfrak{F}$  and  $A$  to  $\mathfrak{S}$ . These  $g_\sigma A$  are to be considered simply as undefined symbols. We shall show that  $\mathfrak{G}$  supplies the required extension when multiplication is defined by

$$(5) \quad (g_\sigma A)(g_\tau B) = g_{\sigma\tau} [C_{\sigma,\tau} (AB)^{S_{\sigma\tau}}].$$

To prove this it is necessary to show, (i) that  $\mathfrak{G}$  contains a subgroup  $\bar{\mathfrak{S}}$  isomorphic to  $\mathfrak{S}$ ; (ii) that the right unit of every element  $g_\sigma A$  lies in the right unit group  $\mathfrak{R}$  of  $\bar{\mathfrak{S}}$ ; (iii) that  $\mathfrak{G}$  is abelian; and (iv) that  $\mathfrak{G}/\bar{\mathfrak{S}} \simeq \mathfrak{F}$ .

First, let  $\bar{\mathfrak{S}}$  consist of all elements  $g_e A$ . Then  $\bar{\mathfrak{S}} \simeq \mathfrak{S}$  under the correspondence  $g_e A \leftrightarrow C_{e,e} A$ . For we have

$$\begin{aligned} (g_e A)(g_e B) &= g_e [C_{e,e} (AB)^{S_e}] \leftrightarrow C_{e,e} [C_{e,e} (AB)^{S_e}] \\ &= (C_{e,e} C_{e,e}) [C'_{e,e} (AB)^{S_e}] \\ &= (C_{e,e} C_{e,e}) (AB) = (C_{e,e} A)(C_{e,e} B), \end{aligned}$$

since from (3)  $C'_{e,e} = E_e$ .

To prove (ii) we shall show that every element  $g_\sigma A$  of  $\mathfrak{G}$  has a right unit  $g_e X_A$ , where  $X_A$  is defined by

$$C_{e,e} X_A = C_{\sigma,e} X_A = E_\sigma E_A,$$

in which  $E_A$  is the right unit of  $A$ . For we have from (5)

$$(g_\sigma A)(g_e X_A) = g_\sigma [C_{\sigma,e} (AX_A)^{S_\sigma}].$$

However, using the notation  $E_\sigma^{(l)}$  for the left unit of  $E_\sigma$ , we have

$$\begin{aligned} E_\sigma [C_{\sigma,e} (AX_A)^{S_\sigma}] &= (E_\sigma^{(l)} C_{\sigma,e}) [E_\sigma (AX_A)^{S_\sigma}] \\ &= (E_\sigma^{(l)} C_{\sigma,e}) (AX_A) = (E_\sigma^{(l)} A) (C_{\sigma,e} X_A) \\ &= (E_\sigma^{(l)} A) (E_\sigma E_A) = E_\sigma A, \end{aligned}$$

and therefore  $C_{\sigma,e} (AX_A)^{S_\sigma} = A$  and  $(g_\sigma A)(g_e X_A) = g_e A$ .

Now  $g_e X_A$  as an element of  $\overline{\mathfrak{S}}$  corresponds to  $C_{e,e} X_A$  in  $\mathfrak{S}$ . But since  $C_{e,e} X_A = E_e E_A$ , this element lies in  $\mathfrak{R}$  and therefore  $g_e X_A$  lies in  $\overline{\mathfrak{R}}$ , the right unit group of  $\overline{\mathfrak{S}}$ . Hence every element of  $\mathfrak{G}$  has a right unit in  $\overline{\mathfrak{R}}$  as required.

It is clear from (5) that  $\mathfrak{G}/\overline{\mathfrak{S}} \simeq \mathfrak{F}$ , and therefore it remains only to prove that  $\mathfrak{G}$  is abelian. Since this proof is straightforward, though cumbersome, we shall not give it in full here. It is only necessary to note that the operation  $S_e$  may be distributed over elements of  $\mathfrak{S}$  in the following manner:

$$(6) \quad (AB)^{S_e} = A^{S_e} B^{S'_e},$$

where  $S'_e$  is defined by  $E'_e B^{S'_e} = B$ , where  $E'_e$  is the right unit of  $E_e$ . This follows from the law (1).

A problem which naturally suggests itself, but which will not be considered here, is the extension of  $\mathfrak{S}$  by  $\mathfrak{F}$  in such a way that the right unit group of the extension  $\mathfrak{G}$  is not  $\mathfrak{R}$  but some subgroup of  $\mathfrak{S}$  containing  $\mathfrak{R}$ . Conditions similar to those of Theorem 4 can be derived if the factor group satisfies certain restrictions. The existence of such an extension, however, remains problematical since the direct product does not satisfy the conditions of the problem.

**6. Equivalent factor sets.** Two factor sets  $C_{\sigma,\tau}$ ,  $D_{\sigma,\tau}$  and corresponding unit sets  $E_\sigma$ ,  $\overline{E}_\sigma$  are said to be *equivalent* if there exists in  $\mathfrak{S}$  a set of elements  $A_\sigma$  such that

$$(7) \quad \overline{E}_\sigma = E_\sigma A'_\sigma, \quad C_{\sigma,\tau}(A_\sigma A_\tau)^{S_{\sigma\tau}} = A_{\sigma\tau} D_{\sigma,\tau}^{S_{\sigma\tau}},$$

where  $A'_\sigma$  is the right unit of  $A_\sigma$ . This equivalence relation is seen to be reflexive on putting  $A_\sigma = E_\sigma$  and applying (3). The symmetry and transitivity of the relation are not immediately obvious from (7), but they necessarily follow from the following:

**THEOREM 5.** *The necessary and sufficient condition that two factor sets  $(E_\sigma, C_{\sigma,\tau})$  and  $(\overline{E}_\sigma, D_{\sigma,\tau})$  give rise to isomorphic extensions of  $\mathfrak{S}$  in which each coset  $g_\sigma \mathfrak{S}$  is mapped on  $\bar{g}_\sigma \mathfrak{S}$  is that they are equivalent.*

**Proof.** 1. If  $\{g_\sigma\}$  is a set of representatives with right units  $E_\sigma$  and factor set  $C_{\sigma,\tau}$ , and if  $\{\bar{g}_\sigma\}$  is a second set of representatives, corresponding to the same extension, with right units  $\overline{E}_\sigma$  and factor set  $D_{\sigma,\tau}$ , since  $\bar{g}_\sigma$  belongs to the coset  $g_\sigma \mathfrak{S}$  we have

$$\bar{g}_\sigma = g_\sigma A_\sigma, \quad A_\sigma \in \mathfrak{S},$$

and therefore  $\overline{E}_\sigma = E_\sigma A'_\sigma$ . Moreover,

$$\begin{aligned} \bar{g}_\sigma \bar{g}_\tau &= (g_\sigma A_\sigma)(g_\tau A_\tau) = g_{\sigma\tau} [C_{\sigma,\tau}(A_\sigma A_\tau)^{S_{\sigma\tau}}], \\ \bar{g}_\sigma \bar{g}_\tau &= \bar{g}_{\sigma\tau} D_{\sigma,\tau} = (g_{\sigma\tau} A_{\sigma\tau}) D_{\sigma,\tau} = g_{\sigma\tau} (A_{\sigma\tau} D_{\sigma,\tau}^{S_{\sigma\tau}}). \end{aligned}$$

This gives (7), and the factor sets are therefore equivalent.



2. Conversely, if the factor sets are equivalent let  $\mathfrak{G}$  and  $\overline{\mathfrak{G}}$  be the corresponding extensions. We shall show that the mapping

$$\bar{g}_\sigma A \rightarrow g_\sigma(A_\sigma A^{S_\sigma})$$

is an isomorphism between  $\mathfrak{G}$  and  $\overline{\mathfrak{G}}$ . For if

$$\bar{g}_\tau B \rightarrow g_\tau(A_\tau B^{S_\tau}),$$

then the product  $(\bar{g}_\sigma A)(\bar{g}_\tau B) = \bar{g}_{\sigma\tau}[D_{\sigma,\tau}(AB)^{\bar{S}_{\sigma\tau}}]$  is mapped on the element

$$(8) \quad g_{\sigma\tau}[A_{\sigma\tau}(D_{\sigma,\tau}(AB)^{\bar{S}_{\sigma\tau}})^{S_{\sigma\tau}}] = g_{\sigma\tau}\{(A_{\sigma\tau}D_{\sigma,\tau}^{S_{\sigma\tau}})[A'_{\sigma\tau}(AB)^{\bar{S}_{\sigma\tau}S'_{\sigma\tau}}]\}.$$

However,

$$\begin{aligned} [g_\sigma(A_\sigma A^{S_\sigma})][g_\tau(A_\tau B^{S_\tau})] &= g_{\sigma\tau}\{C_{\sigma,\tau}[(A_\sigma A_\tau)(A^{S_\sigma}B^{S_\tau})]^{S_{\sigma\tau}}\} \\ &= g_{\sigma\tau}\{[C_{\sigma,\tau}(A_\sigma A_\tau)^{S_{\sigma\tau}}][C'_{\sigma,\tau}(A^{S_\sigma}B^{S_\tau})^{S'_{\sigma\tau}}]\}. \end{aligned}$$

Since, by (3),  $C'_{\sigma\tau} = (E_\sigma E_\tau)^{S_{\sigma\tau}}$  this is seen by means of (6) to be equal to

$$g_{\sigma\tau}\{[C_{\sigma,\tau}(A_\sigma A_\tau)^{S_{\sigma\tau}}](AB)^{S_{\sigma\tau}}\}.$$

In view of (7) this is identical with the right member of (8) since

$$X = \bar{E}_\sigma X^{\bar{S}_\sigma} = (E_\sigma A'_\sigma)X^{\bar{S}_\sigma} = E_\sigma[A'_\sigma X^{\bar{S}_\sigma S'_\sigma}].$$

The two extensions are therefore isomorphic.

### III. EXTENSION BY A FACTOR GROUP WITHOUT UNIQUE RIGHT UNIT

**7. The first structure theorem.** It follows from §4 that every abelian quasi-group  $\mathfrak{G}$  is an extension of its maximal self-unit subgroup  $\mathfrak{R}$  by a factor group  $\mathfrak{F}$  having the following two properties:

- (a)  $\mathfrak{F}$  contains a unique idempotent element  $e$ .
- (b) If  $\mathfrak{F}$  has length  $t$ , then  $U^t$  maps every element of  $\mathfrak{F}$  on  $e$ .

We shall now study extensions of this type and shall prove that  $\mathfrak{G}$  must in fact be the direct product  $\mathfrak{R} \times \mathfrak{F}$ .

Let  $\mathfrak{R}$  be any self-unit quasi-group and let  $\mathfrak{F}$  be a quasi-group having properties (a) and (b). Let  $\mathfrak{G}$  be an extension of  $\mathfrak{R}$  by  $\mathfrak{F}$  and let  $\{g_\sigma\}$  be a set of representatives of the cosets of  $\mathfrak{G}$  modulo  $\mathfrak{R}$ . Thus we have

$$\mathfrak{G} = g_e \mathfrak{R} + g_\sigma \mathfrak{R} + g_\tau \mathfrak{R} + \cdots,$$

where  $g_e \in \mathfrak{R}$ , and where

$$(9) \quad (g_\sigma \mathfrak{R})(g_\tau \mathfrak{R}) = (g_\sigma g_\tau) \mathfrak{R} = g_{\sigma\tau} \mathfrak{R}.$$

Since  $\mathfrak{R}$  is not the whole right unit group of  $\mathfrak{G}$  the coset  $g_\sigma \mathfrak{R}$  does not in general contain  $g_\sigma$ . Let  $g_\sigma s \mathfrak{R}$  be the coset which contains  $g_\sigma$ . By 5, §1,  $g_\sigma \mathfrak{R} \rightarrow g_\sigma s \mathfrak{R}$  is an automorphism of  $\mathfrak{G}/\mathfrak{R}$ , namely the inverse of right multiplication by  $\mathfrak{R}$ . Since  $\mathfrak{G}/\mathfrak{R} \simeq \mathfrak{F}$  it follows that  $S$  is an automorphism of  $\mathfrak{F}$  and

is defined by  $\sigma^s e = \sigma$ . Thus  $S$  leaves invariant every element of  $\mathfrak{F}$  whose right unit is  $e$ , and every coset  $g_\sigma \mathfrak{R}$  which contains its defining element  $g_\sigma$ . From (9) it follows that  $g_\sigma g_\tau$  and  $g_{\sigma\tau}$  belong to the same coset, namely,  $g_{(\sigma\tau)s} \mathfrak{R}$ , and hence we have

$$(10) \quad g_\sigma g_\tau = g_{(\sigma\tau)s} C_{\sigma,\tau},$$

where the elements of the factor set  $C_{\sigma,\tau}$  belong to  $\mathfrak{R}$ .

Owing to property (b) in  $\mathfrak{F}$ , it follows that the homomorphism  $U^t$  when applied to  $\mathfrak{G}$  gives a one-to-one mapping of the elements in each coset  $g_\sigma \mathfrak{R}$  onto  $\mathfrak{R}$ . Hence we can choose for the representative  $g_\sigma$  that element of  $g_\sigma \mathfrak{R}$  which is mapped on any element of  $\mathfrak{R}$  that we please. It is evident, therefore, that in any extension a set of representatives  $\{g_\sigma\}$  can be chosen such that each one is mapped by  $U^t$  onto the same element of  $\mathfrak{R}$ , say  $R$ .

Assuming such a choice of  $\{g_\sigma\}$  to have been made, and applying  $U^t$  to (10), we see that each element of the factor set is also mapped on  $R$  by  $U^t$ . But since  $\mathfrak{R}$  is self-unit,  $U^t$  is an automorphism of  $\mathfrak{R}$ , and it follows that all elements of the factor set are equal to that (unique) element of  $\mathfrak{R}$  mapped on  $R$  by  $U^t$ . It follows that any extension of  $\mathfrak{R}$  by  $\mathfrak{F}$  can be obtained by a factor set all of whose elements are equal, and since the choice of  $R$  is arbitrary, any such factor set gives rise to the same extension. Hence there is only one extension possible and this must be the direct product. We have therefore proved:

**THEOREM 6.** (First structure theorem.) *Every abelian quasi-group is the direct product of its maximal self-unit subgroup by a quasi-group which contains a single idempotent element.*

This theorem reduces the consideration of abelian quasi-groups to that of two types, (i) quasi-groups which contain an idempotent element, (ii) self-unit quasi-groups. We deal with these in order in the following sections.

#### IV. CONSTRUCTION OF ABELIAN QUASI-GROUPS<sup>(5)</sup>

**8. Quasi-groups containing an idempotent element.** The results of this section are based on the following:

**THEOREM 7.** *Let  $\mathfrak{G}$  be an abelian quasi-group and let  $S$  and  $T$  be any two automorphisms of  $\mathfrak{G}$  such that  $ST = TS$ . If a second operation  $\times$  be defined in  $\mathfrak{G}$  by means of the equation*

$$(11) \quad a \times b = a^T b^S,$$

*then the elements of  $\mathfrak{G}$  form a second abelian quasi-group under the operation  $\times$ .*

<sup>(5)</sup> Some of the results of this section were proved in the special case of quasi-groups with a unique right unit by A. Suskewitsch, in his paper, *On a generalization of the associative law*, these Transactions, vol. 31 (1929), pp. 204-214.

The proof is immediate since it is only necessary to verify that  $(a \times b) \times (c \times d) = (a \times c) \times (b \times d)$ . We shall use the notation  $(\mathfrak{G}, T, S)$  to denote the quasi-group in which multiplication is defined by (11). The theorem then states that if the permutations  $T^{-1}$  and  $S^{-1}$  are performed on the vertical and horizontal title lines respectively of the Cayley square for  $\mathfrak{G}$ , the resulting square is still that of an abelian quasi-group, namely  $(\mathfrak{G}, T, S)$ . It is clear too that  $T$  and  $S$  are automorphisms of  $(\mathfrak{G}, T, S)$  as well as of  $\mathfrak{G}$ . More generally, any automorphism of  $\mathfrak{G}$  which commutes with both  $T$  and  $S$  is also an automorphism of  $(\mathfrak{G}, T, S)$ . Thus if  $\bar{\mathfrak{G}} = (\mathfrak{G}, T, S)$  we may write  $\mathfrak{G} = (\bar{\mathfrak{G}}, T^{-1}, S^{-1})$ . However both  $\mathfrak{G}$  and  $\bar{\mathfrak{G}}$  will in general have automorphisms which are not automorphisms of the other.

In particular the above theorem holds when  $\mathfrak{G}$  is an abelian group. This suggests the following:

**DEFINITION.** *If there exist in a quasi-group  $\mathfrak{G}$  two commutative automorphisms  $T^{-1}$ ,  $S^{-1}$  such that  $\bar{\mathfrak{G}} = (\mathfrak{G}, T^{-1}, S^{-1})$  is an abelian group, then  $\mathfrak{G} \simeq (\bar{\mathfrak{G}}, T, S)$  shall be called a group representation of  $\mathfrak{G}$  or simply a representation.*

Let  $\mathfrak{G} = (\bar{\mathfrak{G}}, T, S)$  where  $\bar{\mathfrak{G}}$  is a quasi-group with commutative automorphisms  $S$  and  $T$ . Let  $\mathfrak{H}$  be any subgroup of  $\bar{\mathfrak{G}}$ . The elements of  $\mathfrak{H}$  will also form a subgroup of  $\mathfrak{G}$  if and only if  $a^T b^S \in \mathfrak{H}$  for all  $a$  and  $b$  in  $\mathfrak{H}$ . A sufficient condition for this is that  $\mathfrak{H}$  be invariant under  $T$  and  $S$ . If  $\mathfrak{H}$  contains the right unit group  $\bar{\mathfrak{R}}$  of  $\bar{\mathfrak{G}}$  this condition is also necessary. For in that case

$$a^T e_a^S \in \mathfrak{H}$$

for all  $a$  in  $\mathfrak{H}$ . But, since  $\bar{\mathfrak{R}}$  is clearly a characteristic subgroup  $e_a^S$  belongs to  $\bar{\mathfrak{R}}$ , and therefore to  $\mathfrak{H}$ . Hence  $a^T \in \mathfrak{H}$  for all  $a$  in  $\mathfrak{H}$  and similarly  $a^S$  also belongs to  $\mathfrak{H}$ . We have therefore proved:

**THEOREM 8.** *Let  $\bar{\mathfrak{G}}$  be a quasi-group with right unit group  $\bar{\mathfrak{R}}$  and commutative automorphisms  $T$  and  $S$ . If  $\mathfrak{H}$  is a subgroup of  $\bar{\mathfrak{G}}$  containing  $\bar{\mathfrak{R}}$ , then the necessary and sufficient condition that  $\mathfrak{H}$  be also a subgroup of  $(\bar{\mathfrak{G}}, T, S)$  is that it be invariant under  $T$  and  $S$ .*

The following theorem enables us to construct all abelian quasi-groups which contain an idempotent element, from abelian groups.

**THEOREM 9.** (Second structure theorem.) *Every abelian quasi-group  $\mathfrak{G}$  which contains an idempotent element has a representation of the form  $(\bar{\mathfrak{G}}, T, S)$  where  $\bar{\mathfrak{G}}$  is an abelian group<sup>(6)</sup>.*

<sup>(6)</sup> This theorem exposes a misstatement in the author's previous paper (loc. cit., p. 522), where an example is given with the statement that it cannot be constructed from an abelian group by this method. The example in question can be so constructed from the direct product of two cyclic groups of order 3.

**Proof.** The proof consists in showing that there exist automorphisms  $T$  and  $S$  of  $\mathfrak{G}$  such that  $(\mathfrak{G}, T^{-1}, S^{-1})$  is an abelian group. Let  $e$  be an idempotent element of  $\mathfrak{G}$  and denote by  $S$  and  $T$  respectively the automorphisms defined by left and right multiplication by  $e$ . We then have

$$(12) \quad a^T = ae, \quad a^S = ea.$$

Since  $e(ae) = (ea)e$ , we have  $ST = TS$ . Moreover,

$$a^T(bc^{S^{-1}}) = (ae)(bc^{S^{-1}}) = (ab)(ec^{S^{-1}}) = (ab)c,$$

and therefore an abelian quasi-group containing an idempotent element satisfies the associative law

$$(13) \quad (ab)c = a^T(bc^{S^{-1}}).$$

We now define the operation  $\times$  by means of the equation

$$a \times b = a^{T^{-1}}b^{S^{-1}}.$$

On applying (13) it is easily seen that

$$(a \times b) \times c = a \times (b \times c).$$

Finally, since  $a \times e = a^{T^{-1}}e = a$ , and  $e \times a = ea^{S^{-1}} = a$ , it is clear that under the operation  $\times$  the elements of  $\mathfrak{G}$  form a group with unit element  $e$ . Moreover it is an abelian group since by Theorem 7 it is an abelian quasi-group. Denoting this group by  $\bar{\mathfrak{G}} = (\mathfrak{G}, T^{-1}, S^{-1})$ , we have then  $\mathfrak{G} = (\mathfrak{G}, T, S)$ , which is the required representation of  $\mathfrak{G}$ .

The converse of the above theorem, namely that every quasi-group of the form  $(\mathfrak{G}, T, S)$ , where  $\mathfrak{G}$  is an abelian group, contains an idempotent element, is certainly true since the unit element of  $\mathfrak{G}$  will remain idempotent in  $(\mathfrak{G}, T, S)$ . However quasi-groups so formed may contain subgroups which have no idempotent element. This is illustrated by the example given below:

	1	2	3	4	5	6	7	8	9		1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	1	1	3	2	8	7	9	4	6	5
2	2	3	1	5	6	4	8	9	7	2	3	2	1	7	9	8	6	5	4
3	3	1	2	6	4	5	9	7	8	3	2	1	3	9	8	7	5	4	6
4	4	5	6	7	8	9	2	3	1	4	7	9	8	6	5	4	2	1	3
( $\alpha$ ) 5	5	6	4	8	9	7	3	1	2	( $\beta$ ) 5	9	8	7	5	4	6	1	3	2
6	6	4	5	9	7	8	1	2	3	6	8	7	9	4	6	5	3	2	1
7	7	8	9	2	3	1	5	6	4	7	5	4	6	1	3	2	8	7	9
8	8	9	7	3	1	2	6	4	5	8	4	6	5	3	2	1	7	9	8
9	9	7	8	1	2	3	4	5	6	9	6	5	4	2	1	3	9	8	7

Table ( $\alpha$ ) is the cyclic group  $\mathfrak{G}$  of order 9, while table ( $\beta$ ) is the quasi-group

$(\mathfrak{G}, S, S^{-1})$  where  $S$  is the automorphism which maps each element of  $\mathfrak{G}$  on its square. This quasi-group contains three subgroups of order 3, one having three idempotent elements and the other two none.

If  $\overline{\mathfrak{G}}$  is an abelian group, then by Theorem 8 every subgroup of  $\overline{\mathfrak{G}}$  which is invariant under  $T$  and  $S$  is also a subgroup of  $(\overline{\mathfrak{G}}, T, S)$ . Similarly every subgroup of  $(\overline{\mathfrak{G}}, T, S)$  which is invariant under  $T$  and  $S$  (i.e., every subgroup which contains  $e$ , the unit of  $\overline{\mathfrak{G}}$ ) is also a subgroup of  $\overline{\mathfrak{G}}$ . We therefore have a structure isomorphism between the structure  $\Sigma_1$  of all subgroups of  $(\overline{\mathfrak{G}}, T, S)$  which contain  $e$ , and the structure  $\Sigma_2$  of all subgroups of  $\overline{\mathfrak{G}}$  which are invariant under  $T$  and  $S$ .

The idempotent elements of  $\mathfrak{G}$  form a subgroup  $\mathfrak{Q}$  in which every element is its own right (and left) unit. If the elements of  $\mathfrak{Q}$  are denoted by  $e_1, e_2, \dots$ , then corresponding to each  $e_i$  we can construct a representation of  $\mathfrak{G}$  as in Theorem 9. Thus if  $e_i a = a^{S_i}$  and  $a e_i = a^{T_i}$ , then  $(\mathfrak{G}, T_i^{-1}, S_i^{-1})$  is an abelian group with unit element  $e_i$ .

**THEOREM 10.** *The abelian groups  $(\mathfrak{G}, T_i^{-1}, S_i^{-1})$  constructed as in Theorem 9 from the different idempotent elements of  $\mathfrak{G}$  are all isomorphic.*

**Proof.** Let  $e_1$  and  $e_2$  be two idempotent elements and  $T_1, S_1$ , and  $T_2, S_2$  the corresponding automorphisms of  $\mathfrak{G}$ . Let  $\mathfrak{G}_1 = (\mathfrak{G}, T_1^{-1}, S_1^{-1})$  and  $\mathfrak{G}_2 = (\mathfrak{G}, T_2^{-1}, S_2^{-1})$ . Any isomorphic mapping of  $\mathfrak{G}_1$  on  $\mathfrak{G}_2$  must certainly map  $e_1$  on  $e_2$  since these are the unit elements of the two groups. We shall show that such a mapping is furnished by the automorphism  $S_1 T_2 S_1^{-1}$  of  $\mathfrak{G}$ .

First,  $S_1 T_2 S_1^{-1}$  takes  $e_1$  into  $e_2$  since  $e_1^{S_1 T_2} = e_2^{S_1} = e_1 e_2$ . It remains to show therefore that

$$(a^{T_1^{-1}} b^{S_1^{-1}}) S_1 T_2 S_1^{-1} = (a^{S_1 T_2 S_1^{-1}})^{T_2^{-1}} (b^{S_1 T_2 S_1^{-1}})^{S_2^{-1}},$$

or, in other words, that in the automorphism group of  $\mathfrak{G}$ ,  $T_2$  is the transform of  $T_1$  by  $S_1 T_2 S_1^{-1}$  and similarly  $S_2$  is the transform of  $S_1$  by  $S_1 T_2 S_1^{-1}$ . This follows since for all  $a$

$$\begin{aligned} a^{S_1 T_2 S_1^{-1} T_2 S_1} &= e_1 [((e_1 a) e_2)^{S_1^{-1}} e_2] = [(e_1 a) e_2] (e_1 e_2) \\ &= [(e_1 a) e_1] e_2 = [e_1 (a e_1)] e_2 = a^{T_1 S_1 T_2}. \end{aligned}$$

Hence  $S_1 T_2 S_1^{-1} T_2 S_1 = T_1 S_1 T_2$  or  $T_2 = (S_1 T_2 S_1^{-1})^{-1} T_1 (S_1 T_2 S_1^{-1})$  and similarly  $S_2 = (S_1 T_2 S_1^{-1})^{-1} S_1 (S_1 T_2 S_1^{-1})$ .

It is easily shown that if  $(\mathfrak{G}, T, S)$  is a group it must be one of the groups defined, in the manner of Theorem 9, by means of an idempotent element of  $\mathfrak{G}$ . For the unit element  $e$  of  $(\mathfrak{G}, T, S)$  must be invariant under  $T$  and  $S$  and therefore is an idempotent element of  $\mathfrak{G}$ . That  $T$  and  $S$  are the automorphisms defined by (12) readily follows. Hence from Theorem 10 it follows that a quasi-group can be represented in the form  $(\overline{\mathfrak{G}}, T, S)$  by only one abelian group  $\overline{\mathfrak{G}}$ .

**9. Further transformations of the Cayley square.** We have seen that if  $\mathfrak{G}$  contains an idempotent element  $e$  and if  $S$  and  $T$  are defined by (12), then  $(\mathfrak{G}, T^{-1}, S^{-1})$  is an abelian group. We shall now show that the restrictions that  $e$  be idempotent and  $S$  and  $T$  automorphisms are not essential. Let  $g$  be an arbitrary element of  $\mathfrak{G}$  and define the operations  $S_g$  and  $T_g$  by the equations

$$aS_g = ga, \quad aT_g = ag.$$

However for typographical reasons we shall drop the subscripts and write  $S = S_g$  and  $T = T_g$ . Using  $S'$  and  $S''$  to denote left multiplication by the right unit  $e_g$  and the left unit  $e'_g$  respectively, and  $T'$ ,  $T''$  to denote right multiplication by the same elements, we have from (1) the following distributive laws:

$$(ab)^S = a^S b^{S'} = a^{S''} b^S, \quad (ab)^T = a^T b^{T'} = a^{T''} b^T.$$

The same laws hold for the inverse operations  $S^{-1}$ ,  $T^{-1}$ . Thus  $S$  and  $T$  can be thought of as "pseudo-automorphisms" which become true automorphisms if  $g$  is idempotent. We can now generalize Theorem 9 as follows:

**THEOREM 11.** *If  $\mathfrak{G}$  is any abelian quasi-group, and if  $S$  and  $T$  respectively denote left and right multiplication by a fixed element  $g$ , then  $(\mathfrak{G}, T^{-1}, S^{-1})$  is an abelian group.*

**Proof.** If we define the operation  $\times$  by

$$a \times b = a^{T^{-1}} b^{S^{-1}},$$

we then have

$$\begin{aligned} (14) \quad (a \times b) \times (c \times d) &= (a^{T^{-1}} b^{S^{-1}})^{T^{-1}} (c^{T^{-1}} d^{S^{-1}})^{S^{-1}} \\ &= (a^{T^{-2}} b^{S^{-1} T^{-1}}) (c^{T^{-1} S'^{-1}} d^{S^{-2}}). \end{aligned}$$

But from (1),  $g(ae_g) = (e'_g a)g$  for all  $a$ , and therefore  $T'S = S''T$ , or  $S^{-1}T'^{-1} = T^{-1}S''^{-1}$ . Thus (14) is symmetric in  $b$  and  $c$ , and hence  $(a \times b) \times (c \times d) = (a \times c) \times (b \times d)$ . Moreover  $(\mathfrak{G}, T^{-1}, S^{-1})$  has a unit element, namely,  $gg$ . For

$$a \times gg = a^{T^{-1}} g = a, \quad gg \times a = ga^{S^{-1}} = a.$$

Hence  $(\mathfrak{G}, T^{-1}, S^{-1})$  is an abelian quasi-group with unit element and therefore an abelian group.

It is easy to show similarly that  $(\mathfrak{G}, 1, S_g)$ ,  $(\mathfrak{G}, 1, S_g^{-1})$ ,  $(\mathfrak{G}, T_g, 1)$  and  $(\mathfrak{G}, T_g^{-1}, 1)$  are all abelian quasi-groups. In the second of these  $g$  is a unique left unit and in the fourth, a unique right unit. These results may be stated in terms of transformations of the Cayley square as follows:

Given the Cayley square of an abelian quasi-group  $\mathfrak{G}$ ,

(i)  $(\mathfrak{G}, 1, S_g^{-1})$  is obtained by replacing the horizontal title line by the  $g$ th row;

(ii)  $(\mathfrak{G}, T_g^{-1}, 1)$  is obtained by replacing the vertical title line by the  $g$ th column;

(iii)  $(\mathfrak{G}, T_g^{-1}, S_g^{-1})$  is obtained by performing the replacements (i) and (ii) simultaneously;

(iv)  $(\mathfrak{G}, 1, S_g)$  is obtained by replacing each element  $x$  of the horizontal title line by the element of that line, which occurs above the element  $x$  in the  $g$ th row;

(v)  $(\mathfrak{G}, T_g, 1)$  is obtained by replacing each element  $x$  in the vertical title line by the element in that line, which occurs to the left of the element  $x$  in the  $g$ th column.

**10. Self-unit quasi-groups.** In view of Theorems 6 and 9 the only remaining problem in the characterization of all abelian quasi-groups is to construct those self-unit quasi-groups which do not contain an idempotent element. If  $\mathfrak{G}$  is any such quasi-group, the mapping  $U$ , of each element on its right unit, is an automorphism of  $\mathfrak{G}$  which leaves no element unchanged. If we define a new operation  $\times$  in  $\mathfrak{G}$  by means of the equation

$$a \times b = ab^U = ae_b,$$

it is clear that in the resulting quasi-group  $(\mathfrak{G}, 1, U)$  every element is idempotent. Moreover  $U$  is also an automorphism of  $(\mathfrak{G}, 1, U)$ . We may state this result as follows:

**THEOREM 12.** (Third structure theorem.) *Every self-unit quasi-group which does not contain an idempotent element has the form  $\mathfrak{G} = (\overline{\mathfrak{G}}, 1, U^{-1})$ , where  $\overline{\mathfrak{G}}$  is a quasi-group in which every element is idempotent, and  $U$  an automorphism of  $\overline{\mathfrak{G}}$  which changes every element. Moreover  $U$  is the automorphism of  $\mathfrak{G}$  which maps each element on its right unit.*

Thus every abelian quasi-group has one of the following three forms:

(a)  $(\mathfrak{G}, T, S)$ , where  $\mathfrak{G}$  is an abelian group, and  $S$  and  $T$  commutative automorphisms of  $\mathfrak{G}$ ;

(b)  $(\overline{\mathfrak{G}}, 1, S)$ , where  $\overline{\mathfrak{G}}$  has the form (a) and  $S$  is an automorphism of  $\overline{\mathfrak{G}}$ ;

(c) direct products of types (a) and (b).

The quasi-group  $\mathfrak{G} = (\overline{\mathfrak{G}}, 1, U)$ , where  $\overline{\mathfrak{G}}$  is self-unit and  $a^U = e_a$ , is again self-unit and contains only idempotent elements. In such a quasi-group left and right multiplication by any element are automorphisms. Let  $e_1, e_2, e_3, \dots$  be the elements of  $\mathfrak{G}$ , and denote by  $S_i$  and  $T_i$  the automorphisms defined respectively by left and right multiplication by  $e_i$ , and by  $S_{i,j}, T_{i,j}$  the automorphisms corresponding to the product  $e_i e_j$ . The following relations are then easily verified:

$$(15) \quad S_{i,j} = S_i^{-1} S_j S_i = T_j^{-1} S_i T_j, \quad T_{i,j} = T_i^{-1} T_j T_i = S_i^{-1} T_j S_i.$$

Thus although  $S_i T_i = T_i S_i$ ,  $S_i$  cannot commute with  $S_j$  or  $T_j$  for  $j \neq i$ .

If  $\mathfrak{A}$  is the automorphism group of  $\mathfrak{G}$ , then any element of  $\mathfrak{A}$  which commutes with all  $S_i$  must be the identity. For if  $(e_i a)^S = e_i a^S$  we have  $e_i^S = e_i$ . Now from (15) left multiplication by a product  $e_i e_j$  is the transform of  $S_j$  by  $S_i$ . Applying this, we find that left multiplication by  $(e_i e_j)(e_k e_m)$  is equivalent to the automorphism

$$S_i^{-1} S_j^{-1} S_i S_k^{-1} S_m S_k S_i^{-1} S_j S_i.$$

Since by (1) this must be unaltered by the interchange of  $j$  and  $k$  we find, on equating the two expressions, that for all  $m$

$$S_m S_k S_i^{-1} S_j S_k^{-1} S_i S_j^{-1} = S_k S_i^{-1} S_j S_k^{-1} S_i S_j^{-1} S_m,$$

and therefore

$$(16) \quad S_k S_i^{-1} S_j S_k^{-1} S_i S_j^{-1} = 1, \quad T_k T_i^{-1} T_j T_k^{-1} T_i T_j^{-1} = 1,$$

the second relation following in a similar manner. Thus although a commutator  $S_i S_j S_i^{-1} S_j^{-1}$  cannot be equal to the unit element for  $i \neq j$  the "three element commutators" of the form (16) are all equal to the unit.

The following two examples will illustrate the large number of automorphisms enjoyed by quasi-groups of this type:

(a)		1	2	3	(b)		1	2	3	4	5
	1	1	3	2		1	1	5	4	3	2
	2	3	2	1		2	3	2	1	5	4
	3	2	1	3		3	5	4	3	2	1
						4	2	1	5	4	3
						5	4	3	2	1	5

In (a) we have the rather surprising situation that every permutation of the elements is an automorphism. The automorphism group is therefore the full symmetric group. In (b) we have  $T_1 = (2 \ 3 \ 5 \ 4)$ ,  $T_2 = (1 \ 5 \ 3 \ 4)$ ,  $T_3 = (1 \ 4 \ 5 \ 2)$ ,  $T_4 = (1 \ 3 \ 2 \ 5)$ ,  $T_5 = (1 \ 2 \ 4 \ 3)$ ,  $S_i = T_i^2$  and  $S_1 S_2 = (1 \ 3 \ 5 \ 2 \ 4)$ . These, with their powers, give twenty automorphisms. A quasi-group of this type always contains an automorphism which changes every element. For example,  $a^{S_1 S_2^{-1}} \neq a$  for all  $a$  since  $e_1 a \neq e_2 a$ . Hence every such quasi-group gives rise to another, namely  $(\mathfrak{G}, 1, S_1 S_2^{-1})$ , which is self-unit but contains no idempotent element.

## V.

**11. Some non-abelian quasi-groups.** In Theorem 9 it was shown that an abelian quasi-group which contains an idempotent element  $e$  satisfies the associative law

$$(17) \quad (ab)c = a^T(bc^{S^{-1}}),$$



where  $S$  and  $T$  are commutative automorphisms defined by (12). It is natural, therefore, to consider quasi-groups which satisfy (17) but which are not necessarily abelian.

Let  $\mathfrak{G}$  be a quasi-group, with commutative automorphisms  $S$  and  $T$ , which satisfies (17). It follows as in Theorem 9 that the operation  $\times$  defined by

$$(18) \quad a \times b = a^{T^{-1}}b^{S^{-1}}$$

is associative. The elements of  $\mathfrak{G}$  therefore form, under this operation, a group<sup>(7)</sup> which we shall denote by  $\overline{\mathfrak{G}}$ . Since  $S$  and  $T$  are also automorphisms of  $\overline{\mathfrak{G}}$  the unit element  $e$  of  $\overline{\mathfrak{G}}$  is invariant under both  $S$  and  $T$ , and hence by (18),  $e$  is an idempotent element of  $\mathfrak{G}$  and  $S$  and  $T$  are defined by (12). Hence every quasi-group which satisfies the associative law (17) has the form  $(\overline{\mathfrak{G}}, T^{-1}, S^{-1})$  where  $\overline{\mathfrak{G}}$  is a group (not necessarily abelian), and  $T$  and  $S$  are commutative automorphisms of  $\overline{\mathfrak{G}}$ .

The transform  $a_c$  of  $a$  by  $c$  can be defined in  $\mathfrak{G}$  by the equation

$$c^{T^{-1}}a_c^{S^{-1}} = a^{T^{-1}}c^{S^{-1}}.$$

We then have

$$(ab)_c = a_mb_n$$

where  $m = c^{T^{-1}}$  and  $n = c^{S^{-1}}$ , and it is easily shown that those elements which are transformed into themselves by all elements of  $\mathfrak{G}$  form an abelian sub-quasi-group, the center of  $\mathfrak{G}$ . These are, of course, exactly the elements of the center of  $\overline{\mathfrak{G}}$ . A quasi-group satisfying (17) is therefore abelian if and only if

$$a^{T^{-1}}b^{S^{-1}} = b^{T^{-1}}a^{S^{-1}},$$

for all elements  $a$  and  $b$  of  $\mathfrak{G}$ .

**THEOREM 13.** *In a quasi-group satisfying (17) there exist coset expansions with respect to any subquasi-group  $\mathfrak{S}$  which is invariant under  $T$ .*

**Proof.** Let  $h_1$  and  $h_2$  be elements of  $\mathfrak{S}$  and let  $ah_1 = bh_2$ . Then for any element  $ah$  of the coset  $a\mathfrak{S}$  we have, since  $\mathfrak{S}^T = \mathfrak{S}$ ,

$$ah = a(h_1^{T^{-1}}h_3) = (a^{T^{-1}}h_1^{T^{-1}})h_3^S = (bh_2)^{T^{-1}}h_3^S = b(h_2^{T^{-1}}h_3) = bh_4.$$

Hence  $a\mathfrak{S} \subset b\mathfrak{S}$ , and similarly  $b\mathfrak{S} \subset a\mathfrak{S}$ . Therefore two cosets which have an element in common are identical.

Since  $T$  is defined by (12),  $\mathfrak{S}$  is invariant under  $T$  if and only if it contains the idempotent element  $e$ . Thus coset expansions exist for all subquasi-groups of  $\mathfrak{G}$  which contain  $e$ . A subquasi-group  $\mathfrak{S}$  containing  $e$  is said to be *normal* if

$$a^{T^{-1}}\mathfrak{S} = \mathfrak{S}^{S^{-1}}a,$$

---

(7) The associative law together with the left and right quotient axioms imply the existence of a unit element.

for all  $a$  in  $\mathcal{G}$ . This condition is necessary and sufficient for the existence of a quotient group  $\mathcal{G}/\mathcal{H}$  homomorphic to  $\mathcal{G}$ . It is clear that the normal subquasi-groups of  $\mathcal{G}$  which contain  $e$  are simply the normal subgroups of the group  $\bar{\mathcal{G}} = (\mathcal{G}, T, S)$  and therefore the usual theorems concerning these will carry over to the quasi-group.

UNIVERSITY OF SASKATCHEWAN,  
SASKATOON, CANADA.