HOMOGENEOUS QUASI-GROUPS AND THEIR COMBINATORIAL BEARINGS

by P. KESAVA MENON, F.N.A., *Director, Joint Cipher Bureau, Ministry of Defence, New DHQ Building, DHQ P. O., New Delhi-110011*

(*Received 12 May 1975*)

We define a quasi-group of order v as a set of v elements with a multiplication defined in it such that given any two of the elements x, y, z the equation $xy=z$ can be solved uniquely for the third. In this paper we shall consider only finite quasi-groups. We observe that a finite quasi-group is fully characterised by the property that its multiplication table is a Latin square, i.e., a square array in which each row and each column contains every element exactly once. We shall call a quasi-group homogeneous if every equality of expressions formed with any two distinct elements by successive application of the multiplication operation is also satisfied when those elements are replaced by any other pair of distinct elements.

The object of this paper is to construct homogeneous quasi-groups and to study their properties. Firstly, we consider certain examples of homogeneous quasi-groups. Next, we obtain some general properties of quasi-groups and bring out their bearing on an important class of combinatorial problems. Thirdly, we develop a general algebraic technique for the construction of homogeneous quasi-groups and lastly we apply this technique to important particular cases to obtain infinite classes of non-isomorphic homogeneous quasi-groups.

CERTAIN EXAMPLES OF HOMOGENEOUS QUASI-GROUPS

We have the following result :—

Theorem 1: Every element of a homogeneous quasi-group is idempotent, i.e., $x^2=x$ *for all* x.

Proof: The theorem is trivial when there is only one element. If there are only two elements and the square of one of them is equal to the other, say $x^2=y$, then on replacing the pair (x, y) by the pair (y, x) in the last relation we get $y^2=x$ because of homogeneity but then, because of the quasi-group property $xy\neq y$ in view of the first relation and $xy\neq x$ in view of the second relation. It follows that xy is not defined which shows that the square of an element cannot be the other so that $x^2=x$ and $y^2=y$. Now suppose that there are more than two elements in the homogeneous quasi-group. If $x^2=y\neq x$ and if z is an element distinct from x and y then replacing the pair (x, y) by the pair (x, z) we get $x^2=z$ so that $y=z$, a contradiction. It follows that $x^2=x$ for all x.

Corollary 1: There is no homogeneous quasi-group of order 2.

In fact there cannot be a quasi-group of order 2 in which the diagonal elements are distinct.

Corollary 2: There is (upto isomorphism) exactly one homogeneous quasi-group of order 3 namely the one whose multiplication table is

	x	y	z
x	x	z	y
y	z	y	x
z	y	x	z

In fact, xy cannot be equal to x or y since these already occur in the first row and second column respectively of the multiplication table. Hence $xy=z$ and likewise the rest of the multiplication table is completed. It is easily seen that the quasi-group is homogeneous.

In like manner it can be shown that

Corrollary 3: There is (upto isomorphism) exactly one homogeneous quasi-group of order 4 namely the one whose multiplication table is

	x	y	z	u
x	x	z	u	y
y	u	y	x	z
z	y	u	z	x
u	z	x	y	u

Corrollary 4: There are (upto isomorphism) exactly three homogeneous quasi-groups of order 5 :

	x	y	z	u	v
x	x	z	u	v	y
y	z	y	v	x	u
z	u	v	z	y	x
u	v	x	y	u	z
v	y	u	x	z	v

	x	y	z	u	v
x	x	z	u	v	y
y	u	y	v	z	x
z	v	x	z	y	u
u	y	v	x	u	z
v	z	u	y	x	v

and the one obtained by transposing the rows and columns of the last one.

The verification of the homogeneity of the quasi-groups in corollaries 3 and 4 is cumbersome but will readily follow from results to be established later.

It can be shown, by trying out all possibilities, that :—

Corollary 5: There are no homogeneous quasi-groups of order 6.

Theorem 1 shows that every relation involving only two elements x, y in a homogeneous quasi-group holds also when y is put equal to x since both sides of the

relation then reduce to x. Hence every relation in a homogeneous quasi-group involving two distinct elements is actually an identity. Homogeneity is obviously a strong condition on quasi-groups and might have led to the suspicion that they may be all of small orders had we not already known the existence of an infinite class in connection with the so-called *Steiner Triple Systems.* By definition, a *Steiner Triple System* of order v is a set of triplets of elements chosen from a given set of v elements such that every pair of distinct elements occurs in exactly one triplet. It is known that Steiner Triple Systems of order v exist if and only if $v \equiv 1$ or 3 (mod 6). A homogeneous quasi-group is associated with every Steiner Triple System. Taking the elements of a Steiner Triple System as the elements of the quasi-group we define the product xy of two elements x, y as x if $x=y$ and as the third element of the triplet containing x and y if $x \neq y$. It is easily verified that the multiplicative system obtained in this manner is a homogeneous quasi-group. In fact, it satisfies the identities :

$$(i)\ x(xy)=y, \qquad (ii)\ xy=yx, \qquad (iii)\ x^2=x$$

and all relations involving only two elements are those derivable from these identities and are therefore themselves identities. Conversely it is also true, as is well-known, that a quasi-group satisfying the above relations gives rise to a Steiner Triple System by taking (x, y, xy) as the triplet containing x, y for $x \neq y$. We note that the homogeneous quasi-group of Corollary 2 of Theorem 1 is associated with the Steiner Triple System formed by the set $[x, y, z]$. The homogeneous quasi-groups of Corollaries 3 and 4 are not associated with Steiner Triple Systems as they do not satisfy both (i) and (ii) simultaneously.

The following theorem characterises homogeneous quasi-groups.

Theorem 1a: A quasi-group is homogeneous if and only if it has the property that every member of the class of its subquasi-groups generated by arbitrary pairs of distinct elements can be mapped isomorphically onto a given one of them in such a manner that the generating elements x, y of the former correspond to the generating elements u, v respectively of the latter.

Proof: Let x, y be two arbitrary but distinct elements of the given quasi-group and let $Q(x, y)$ be the subquasi-group generated by x, y. Then an equality of two expressions in x, y is obviously a relation within the subquasi-group $Q(x, y)$. Let $Q(x, y)$ be isomorphic to $Q(u, v)$ with x, y corresponding to u, v respectively. Then it follows that the equality is satisfied if x, y are replaced by u, v in the two expressions so that it becomes an equality of expressions in u, v. Obviously the converse also holds from which since x, y are arbitrary the 'if' part of the theorem follows. We shall derive the 'only if' part of the Theorem as Corollary 4*a* of Theorem 2 given below.

Properties of Homogeneous Quasi-Groups

Lemma 1: Every subquasi-group of a homogeneous quasi-group is homogeneous.

This is an immediate consequence of the condition of homogeneity.

Theorem 1 shows that every element of a homogeneous quasi-group is by itself a subquasi-group. These subquasi-groups shall be called trivial subquasi-groups.

A homogeneous quasi-group of order greater than 1 whose subquasi-groups other than itself are all trivial shall be called a primitive homogeneous quasi-group. The homogeneous quasi-groups of Corollaries 2 to 4 of Theorem 1 are all primitive. A homogeneous quasi-group which is neither trivial nor primitive shall be called an imprimitive homogeneous quasi-group. The homogeneous quasi-group associated with a Steiner Triple System of order greater than 3 is certainly imprimitive since the elements of any triplet of the system form by themselves a subquasi-group of order 3.

Lemma 2: A primitive homogeneous quasi-group is generated by any two of its distinct elements.

In fact, the subquasi-group generated by any two distinct elements of the quasi-group must coincide with the latter in view of primitivity.

Lemma 3: A homogeneous quasi-group generated by two distinct elements is primitive.

Proof: Let Q be a homogeneous quasi-group generated by two elements x, y and let Q' be any non-trivial subquasi-group of Q. If u, v are two distinct elements of Q' then the subquasi-group generated by u, v is contained in Q' and may without loss of generality be taken to be Q' itself. Now let $f_i(x, y)(i=1,\ldots, n)$ be the distinct elements of Q. Then the elements $f_i(u, v)(i=1,\ldots, n)$ are all distinct since any equality between two of them will imply a corresponding equality of the two expressions with u, v replaced by x, y respectively in view of homogeneity. It follows that Q' contains at least as many elements as Q and therefore coincides with the latter.

Lemmas 2 and 3 show that a primitive homogeneous quasi-group may also be defined as a homogeneous quasi-group generated by two distinct elements.

Theorem 2: Any two primitive subquasi-groups of a homogeneous quasi-group are isomorphic.

Proof: Let Q_1, Q_2 be two primitive subquasi-groups of a homogeneous quasi-group and let Q_1, Q_2 be generated by the pairs of elements (x, y), (u, v) respectively. Let $f_i(x, y)$ $(i=1, 2, \ldots, n)$ be the distinct elements of Q_1. Then, by an argument similar to that in the proof of Lemma 3 it follows that $f_i(u, v)$ $(i=1, 2, \ldots, n)$ are distinct elements of Q_2. From this it follows in particular that Q_2 has at least as many elements as in Q_1 and by reversing the roles of Q_1 and Q_2 it follows that Q_2 has exactly the same number of elements as Q_1 so that $f_i(u, v)$ $(i=1, 2, \ldots, n)$ are all the elements of Q_2. Moreover, if $f_1(x, y) = x$, $f_2(x, y)=y$ then, by homogeneity, $f_1(u, v)=u$, $f_2(u, v)=v$ and if $f_i(x, y)$ $f_j(x, y)=f_k$ (x, y) then $f_i(u, v)$ $f_j(u, v)=f_k(u, v)$ so that the mapping $x\to u$, $y\to v$ defines an isomorphism of Q_1 onto Q_2.

Corollary 1a: The number of isomorphisms of a primitive subquasi-group of a homogeneous quasi-group onto any other primitive subquasi-group is exactly $n(n-1)$ where n is the order of the primitive subquasi-groups.

Proof: From the proof of Theorem 2 it follows that if (x, y), (u, v) are pairs of generating elements of two primitive subquasi-groups of Q_1, Q_2 respectively then the mapping $x\to u$, $y\to v$ defines an isomorphism of Q_1 onto Q_2. Since by Lemma 2 any pair of distinct elements can be chosen as generating elements of a primitive homogeneous quasi-group it follows that an isomorphism of Q_1 onto Q_2 is well

determined when the images of a given pair of elements of Q_1 are specified as arbitrary but distinct elements of Q_2. Since this can be done in exactly $n(n-1)$ ways where n is the order of Q_2 it follows that there are exactly $n(n-1)$ distinct isomorphisms of Q_1 onto Q_2.

Corollary 2a: The order of the group of automorphisms of a homogeneous quasi-group generated by two distinct elements is $n(n-1)$ where n is the order of the quasi-group.

Proof: By Lemma 3 the given quasi-group is primitive. The rest of the proof follows from Corollary 1*a* by identifying the two primitive subquasi-groups with the given quasi-group.

Corollary 3a: The automorphism group of a primitive homogeneous quasi-group is doubly transitive.

In fact, there is a unique automorphism which maps any pair (x, y) of distinct elements onto any other pair (u, v) of distinct elements.

Corollary 4a: If $Q(x, y)$, $Q(u, v)$ are subquasi-groups generated by any two pairs of distinct elements (x, y) and (u, v) respectively of a homogeneous quasi-group then there exists an isomorphism of $Q(x, y)$ onto $Q(u, v)$ which maps x, y into u, v respectively. This follows at once from the proof of Theorem 2.

We recall the definition of a Balanced Incomplete Block Design (or, simply design) with parameters v, k, λ as a set of subsets (called blocks), each block containing exactly k elements chosen out of a set of v elements such that any pair of distinct elements of the set is contained in exactly λ blocks. If a design with parameters v, k, λ exists then it is easily varified that each element occurs in the same number r of blocks where r is given by $r(k-1) = \lambda(v-1)$ and that the total number b of blocks is given by $bk = vr$. In particular, for $\lambda = 1$, we have

$$r = \frac{v-1}{k-1}, \quad b = \frac{v(v-1)}{k(k-1)}.$$

Let Q be a homogeneous quasi-group of order v and let $\{Q_1, \ldots, Q_b\}$ be the set of all primitive subquasi-groups of Q. If Q_1 has order k, then by what has already been proved, all the subquasi-groups Q_i have the same order k. Since any two distinct elements of Q generate a primitive subqasi-group it follows that any pair of distinct elements of Q is contained in exactly one of the subquasi-groups Q_i. Hence we have

Theorem 3: The primitive subquasi-groups of a homogeneous quasi-group Q form the blocks of a $(v, k, 1)$ *design where v is the order of Q and k is the order of a primitive subquasi-group. Consequently it also follows that each element of Q is contained in exactly* $(v-1)/(k-1)$ *primitive subquasi-groups of Q and that the total number of primitive subquasi-groups of Q is* $v(v-1)/\{k(k-1)\}$.

Theorem 3 has a partial converse.

Theorem 4: If there exists a $(v, k, 1)$ *design and a primitive homogeneous quasi-group of order k then there exists a homogeneous quasi-group of order v whose primitive subquasi-groups are isomorphic to the given quasi-group.*

Proof: Suppose there exist a design D with parameters $(v, k, 1)$ and a primitive homogeneous quasi-group P of order k. Then any one-to-one mapping of the set P onto a block B induces a primitive quasi-group structure in B isomorphic to P.

Let this be done for each of the blocks of D. A unique multiplication is thereby defined for every pair of elements of D since any pair of elements of D occurs in exactly one block. This makes D, in the first place, a quasi-group. In fact if any two of the elements in the equation $xy = z$ is chosen in D then those elements belong to a unique block B so that the third element also belongs to B and is therefore uniquely defined in view of the quasi-group structure of B. To prove the homogeneity of the quasi-group D we observe that any relation in two given elements x, y is a relation in the unique primitive homogeneous quasi-group B containing those elements and is therefore certainly valid for every pair of elements of B. The extension of the relation to any other pair of elements u, v of D follows at once from the isomorphism between the primitive quasi-group B' containing u, v and the quasi-group B. In fact, if u', v' are the images in B' of x, y respectively under the isomorphism then any relation in x, y is in the first instance carried over into the same relation in u', v' which is then also satisfied when u', v' are replaced by u, v in view of the homogeneity of B'.

As an immediate consequence of Theorems 3 and 4 we have

Theorem 5: The number of non-isomorphic homogeneous quasi-groups of order v with primitive subquasi-groups of order k is equal to the product of the number of non-isomorphic $(v, k, 1)$-designs and the number of non-isomorphic primitive quasi-groups of order k.

Proof: Two $(v, k, 1)$-designs are isomorphic if and only if there exists a one-to-one mapping between their sets of elements which maps the blocks of one into the blocks of the other. This corresponds to the fact that in any isomorphism of homogeneous quasi-groups the primitive subquasi-groups of one must go over into primitive subquasi-groups of the other. It follows that when there exists a primitive homogeneous quasi-group of order k, non-isomorphic $(v, k, 1)$-designs will give rise to non-isomorphic homogeneous quasi-groups of order v whose primitive subquasi-groups are isomorphic to the given primitive homogeneous quasi-group of order k. Moreover from the same $(v, k, 1)$-design we may construct as many non-isomorphic homogeneous quasi-groups of order v as there are non-isomorphic primitive homogeneous quasi-groups of order k. Hence the theorem follows.

From Theorem 4 we easily derive

Theorem 6: If there exists a primitive homogeneous quasi-group of order $p^r + 1$, where p is any prime number then, for all $m > 1$, there exists a homogeneous quasi-group of order $(p^{mr}-1)/(p^r-1)$ whose primitive subquasi-groups are of order $p^r + 1$.

Proof: In any finite projective geometry every line contains the same number of points and any pair of distinct points is contained in exactly one line so that if v is the total number of points of the geometry and k is the number of points in each line then on taking the lines as blocks we get a $(v, k, 1)$-design. It is also well-known that a finite projective geometry of arbitrary dimension and of order p^r where p is any prime number exists and that then the number of points in each line is $p^r + 1$ and the total number of points of the space is $(p^{mr} - 1)/(p^r - 1)$ if $m-1$ is the dimension of the space. Hence the theorem follows at once from Theorem 4.

We remark that in Corollaries 2 to 5 of Theorem 1 the orders of the primitive groups considered are all of the form specified in the hypothesis of Theorem 6. Hence the latter is applicable to all those cases except that it has no content in the case of

Corollary 5. Indeed there are no homogeneous quasi-groups of order 6 and hence there can be no homogeneous quasi-groups having primitive subquasi-groups of order 6.

Theorem 7: If there exists a primitive homogeneous quasi-group of order p^r, where p is a prime number then for all m there exists a homogeneous quasi-group of order p^{rm} whose primitive subquasi-groups are of order p^r.

Proof: This follows in the same way as Theorem 6 by considering the points of a Euclidean geometry of order p^r and dimension m as the elements and the lines of the geometry as the blocks of a design.

From Theorems 3 to 5 it follows that the problem of construction of homogeneous quasi-groups is reduced to the following two problems :—

(1) Construct all non-isomorphic primitive quasi-groups.

(2) For each value of k for which a primitive homogeneous quasi-group of order k exists construct all non-isomorphic $(v, k, 1)$–designs.

The second of these problems is combinatorial in nature and has been widely studied though a complete solution is not yet known. Apart from purely combinatorial methods both algebraic methods have been applied to obtain partial solutions. We have already used the geometric method to obtain theorem 6. We shall see below incidentally how certain algebraic methods also lead to partial solutions.

The first problem appears to be purely algebraic. For small orders all non-isomorphic solutions may be found by trial as we have done manually for orders 3 to 6, possibly with the aid of computers. But anything like an approach to a general solution seems to demand special algebraic tools. We shall give below a general algebraic method by which we construct a whole class of non-isomorphic primitive homogeneous quasi-groups for every prime power order. Whether there can be primitive homogeneous quasi-groups of non-prime power orders or whether, even for prime power orders, our method leads to all possible primitive homogeneous quasi-groups is not known.

Algebraic Technique—Construction of Homogeneous Quasi-Groups

Let G be a finite group and M the multiplicative semi-group of all mappings of G into itself. We shall denote the image of x under the mapping α by x^α or by $x\,\alpha$ when G is an additive group). If n is an integer, the mapping which maps every element into its nth power shall be denoted by n itself. In particular, the identity mapping of G is denoted by 1 and the mapping which maps every element into the identity element of G is denoted by O. If N is the *l.c.m.* of all orders of the elements of G then clearly the mapping n is defined only upto modulo N.

The semi-group M becomes a near-ring when addition is defined in M by $x^{\alpha+\beta} = x^\alpha\, x^\beta$. Addition is in general non-commutative unless G itself is commutative. However, M is a group under addition with O as the zero element, the negative of α being $\alpha\,(-1)$ which, in general is not equal to $(-1)\alpha$. The left-sided distributive law $\alpha\,(\beta + \gamma) = \alpha\beta + \alpha\gamma$ holds in M but not the right-sided distributive law. However we have $(\alpha + \beta)\,(-1) = \beta\,(-1) + \alpha\,(-1)$.

The subset U of M consisting of all $\alpha \in M$ which map the identity element of G into itself is closed under both addition and multiplication and hence is itself a

near-ring containing 1. In what follows we shall confine ourselves to mappings belonging to U.

With a given $\alpha \in U$ we define a new operation in G by $x \odot y = (xy^{-1})^{\alpha} y$.

Lemma 1a: $x \odot x = x$ for all x in G.

This follows at once from the definition of the operation $\odot$ and the fact that α maps the identity of G into itself.

Theorem 8: $(G, \odot)$ *is a quasi-group if and only if both* α *and* $(-1)\alpha + 1$ *are permutations of the elements of* G.

Proof: We may write $x \odot y$ in either of the alternative forms $(xy^{-1})^{\alpha} y$ or $(yx^{-1})^{(-1)\alpha+1} x$. From the first of these forms it follows that, for a given y, $x \odot y$ takes distinct values for distinct values of x if and only if x^{α} does so. Similarly the second form shows that for a given x, $x \odot y$ takes distinct values of distinct values of y if and only if $y^{(-1)\alpha+1}$ does so from which the theorem follows.

In what follows we shall suppose that the conditions of Theorem 8 are satisfied. We define a new composition $\odot$ in U by

$$\beta \odot \gamma = \{\beta + \gamma(-1)\}\alpha + \gamma$$

The use of the same symbol $\odot$ for compositions in both G and U is not likely to lead to any confusion.

Lemma 2a: $\beta \odot \beta = \beta$ for all β in U.

This at once follows from the definition.

Lemma 3a: $\beta \odot \gamma = \{\gamma + \beta(-1)\}\ \{(-1)\alpha - 1\} + \beta$.

Proof: $\beta + \gamma\ (-1) = \{\gamma + \beta\,(-1)\}\ (-1)$ so that

$$\{\beta + \gamma\ (-1)\}\ \alpha + \gamma = \{\gamma + \beta\ (-1)\}\ (-1)\ \alpha + \{\gamma + \beta\ (-1)\} + \beta$$
$$= \{\gamma + \beta\ (-1)\}\ \{(-1)\ \alpha + 1\} + \beta.$$

Theorem 9: $(U, \odot)$ *is a quasi-group under composition in which every element is an idempotent.*

Proof: The last part of the theorem follows at once from lemma 2a. If, for any given γ, $\beta_1 \odot \gamma = \beta_1 \odot \gamma$, then from the defining relation of $\odot$ we get $\{\beta_1 + \gamma\ (-1)\}$ $\alpha = \{\beta_2 + \gamma\ (-1)\}\ \alpha$ so that multiplying both sides on the right by the inverse of the permutation α it follows that $\beta_1 = \beta_2$. Likewise we deduce with the help of lemma 3a and the fact that $(-1)\ \alpha + 1$ is a permutation that if for any β, $\beta \odot \gamma_1 = \beta \odot \gamma_2$ then $\gamma_1 = \gamma_2$, which completes the proof.

We shall denote the subquasi-group of $(U, \odot)$ generated by the mappings O, 1 in U by $S(\alpha) = S$.

Let $Q = Q(x, y)$ be the subquasi-group of $(G, \odot)$ generated by two distinct elements x, y of G. Then we have

Theorem 10: $Q = \{(xy^{-1})^{\beta}\ y \mid \beta \in S\}$

Proof: Let us write

$$f(\beta) = (xy^{-1})\beta\, y$$

for every β in U. Then we have, for all β, γ in U,

$$f(\beta) \odot f(\gamma) = \{(xy^{-1})^{\beta}\ y.y^{-1}\ (xy^{-1})^{\gamma(-1)}\}.\ (xy^{-1})^{\gamma}\ y$$
$$= (xy^{-1})^{\{\beta+\gamma(-1)\}\alpha+\gamma y}$$

$$= (xy^{-1})^{\beta\odot\gamma}\, y = f(\beta\odot\gamma)$$

so that f is a homomorphism of the quasi-group $(U,\odot)$ into the quasi-group $(G,\odot)$. Under this homomorphism the elements 0, 1 of S have the images y, x respectively in G. It follows that the subquasi-group S of $(U,\odot)$ generated by 0, 1 is mapped onto the subquasi-group Q of $(G,\odot)$ generated by x, y which completes the proof.

Our object is to obtain conditions for Q to be a homogeneous (primitive) quasi-group and for $(G,\odot)$ to be a homogeneous quasi-group.

Theorem 11: Let z be a given non-identity element of G and let the quasi-group S be decomposed into disjoint classes $S_0, S_1, \ldots$ by putting all elements which map z into the same element in one class. Then each class S_i is a subquasi-group of S and the set $\bar{S} = \{S_0, S_1, \ldots\}$ becomes a quasi-group if the composite of two classes S_i, S_j containing β, γ respectively is defined as the class $\beta\odot\gamma$. If x, y are any elements of G such that $xy^{-1} = z$ then the quasi-group $\bar{S}$ is isomorphic to the subquasi-group $Q(x, y)$ of $(G,\odot)$ with the classes containing 0, 1 corresponding respectively to the generating elements y, x of $Q(x, y)$.

Proof: Let x, y be chosen such that $xy^{-1}=z$. Then $x\neq y$ since z is not identity. Let $Q = Q(x, y)$ be the subquasi-group of $(G,\odot)$ generated by x, y, and consider the homomorphism f of S onto Q defined in the proof of Theorem 10. The elements of S which are mapped into one and the same element of Q by f is a subquasi-group of S. In fact, if $f(\beta) = f(\gamma)$ for any β, γ in S then $f(\beta\odot\gamma) = f(\beta)\odot f(\gamma) = f(\beta)\odot f(\beta) = f(\beta)$, since the elements of Q are idempotent. The subquasi-groups corresponding to the various elements of Q obviously partition S into disjoint classes. This class division agrees with that in the statement of the theorem. In fact, the relation $f(\beta) = f(\gamma)$ which simply means that $(xy^{-1})^{\beta} y = (xy^{-1})^{\gamma} y$ reduces to $z^{\beta} = z^{\gamma}$. It is a routine matter to verify that composition of classes is well defined. Clearly f induces an isomorphism of $\bar{S}$ onto Q which shows in particular that $\bar{S}$ is a quasi-group. The classes containing 0, 1 correspond under this isomorphism to the generating elements y, x respectively of Q which completes the proof.

Corollary 1b: If S_0, S_1 are the classes containing 0, 1 respectively of S, then $\bar{S}$ is generated by S_0, S_1.

This follows at once from the fact that S_0, S_1 correspond to the generating elements y, x respectively of Q under the isomorphism between $\bar{S}$ and Q.

We may denote by S_γ the class containing γ in the decomposition $\bar{S}$ of S of Theorem 11 so that $S_\gamma = \{\beta\epsilon S / z^{\beta} = z^{\gamma}\}$. This conforms also to our notation for the classes containing 0 and 1. When it is desired to bring into evidence the dependence of the decomposition $\bar{S}$ on the choice of z we shall write $\bar{S}_z$ and $S_{\gamma,z}$ for $\bar{S}$ and S_γ respectively

Corollary 2b: For any given pair of distinct elements β, γ in S there is at least one decomposition $\bar{S}_z$ of S such that $S_{\beta,z}\neq S_{\gamma,z}$.

This follows at once from the fact that $z^{\beta} = z^{\gamma}$ for all z in G implies that $\beta = \gamma$.

The following theorems are crucial :

Theorem 12: The necessary and sufficient condition that $(G,\odot)$ is homogeneous is that for every pair z, z' of non-identity elements of G, there is an isomorphism of $\bar{S}_z$ onto $\bar{S}_{z'}$ under which $S_{0,z'}$ and $S_{1,z'}$ are mapped into $S_{0,z'}$ and $S_{1,z'}$ respectively.

Proof: Let (x, y), (u, v) be arbitrary pairs of distinct elements of G and let $xy^{-1} = z$, $uv^{-1} = z'$. Then by Theorem 11 there is an isomorphism of the subquasi-group $Q(x,y)$ onto $\bar{S}_z$ which maps x, y into $S_{1,z}$, $S_{0,z}$ respectively and likewise there is an isomorphism of $Q(u, v)$ onto $\bar{S}_{z'}$ which maps u, v into $S_{1,z'}$, $S_{0,z'}$ respectively. Since $\bar{S}_z$ is isomorphic to $\bar{S}_{z'}$ with $S_{0,z}$, $S_{1,z}$ corresponding to $S_{0,z'}$, $S_{1,z'}$ respectively it follows $Q(x, y)$ is isomorphic to $Q(u, v)$ with x, y corresponding to u, v respectively from which the theorem follows.

A special case of the above theorem is of particular importance.

Theorem 13: If every non-identity element z of G is mapped into distinct elements by distinct elements of S then $(G,\odot)$ is homogeneous.

Proof: In this case in every class division $\bar{S}_z$ the classes consist of single elements only so that $\bar{S}_z$ coincides with S and hence every subquasi-group $\bar{Q}(x, y)$ for $x \neq y$ is isomorphic to S with x, y corresponding to 1, 0 respectively. Hence the theorem follows.

Corollary 1c: Under the conditions of the theorem, S is a primitive quasi-group.

This follows from the isomorphism of S and the primitive subquasi-group $Q(x, y)$. A still more particular case of interest of Theorem 12 is given by

Theorem 14: If S has no proper subsquasi-groups of order greater than 1 then $(G,\odot)$ is homogeneous.

Proof: In this case $\bar{S}_z$ coincides with S for all z so that the homomorphism f of S onto $Q(x, y)$ becomes an isomorphism which maps 0, 1 into x, y respectively. Since x, y are arbitrary it follows that all subquasi-groups $Q(x, y)$ are isomorphic to each other with generating elements corresponding so that the theorem follows from Theorem 1a.

We shall now examine the structure of the set S.

Theorem 15: If β, γ, δ are arbitrary elements of S then $\{\beta + \gamma(-1)\}\delta + \gamma$ is also in S.

Proof: We remark that the result of Theorem 15 is apparently more general than the defining property of S to which it reduces when δ is taken to be α. Let x, y be arbitrary elements of G and let $Q(x, y)$ be the sub-quasigroup of $(G,\odot)$ generated by x, y. The elements of $Q(x, y)$ are obtained from x, y by repeated application of the quasi-group operation. From Theorem 10 and Corollary 2 *b* of Theorem 11 it follows that the value of any such expression can be written in the form $(xy^{-1})^{\beta} y$ with a unique β in S serving for all x, y though for any particular choice of x, y two such values may coincide. Let u, v, w be three expressions obtained from x, y by the quasi-group operation and let these expressions correspond to β, γ, δ respectively in S. Clearly, on substituting the expressions u, v, for x, y in the expression ω we get a new expression in x, y which corresponds to some element, say ϵ, in S. Thus writing $\omega = \omega(x, y)$ we have, on the one hand,

$$\omega(u, v) = (xy^{-1})^{\epsilon} y$$

and, on the other,

$$\omega(u, v) = (uv^{-1})^{\delta} v$$

$$= \left\{(xy^{-1})^{\beta}.y.y^{-1}\ (xy^{-1})^{\gamma(-1)}\right\}^{\delta}.\ (xy^{-1})^{\gamma}\ y$$

$$= (xy^{-1})^{\{\beta+\gamma(-1)\}\delta+\gamma}.y$$

from which we get $\epsilon = \{\beta + \gamma\ (-1)\}\ \delta + \gamma$ since x, y are arbitrary.

Taking $\gamma = 0$ in the theorem we get

Corollary 1d: If β, δ are in S then $\beta\delta$ is also in S. In other words, S is closed under multiplication.

Corrollary 2d: The elements of S which are permutations form a group under multiplication.

This follows at once from Corollary 1*d* and the finiteness of S.

Taking $\beta = 0$, $\gamma = 1$ in the Theorem we get

Corollary 3d: If δ is in S then $(-1)\ \delta + 1$ is in S.

In general we are not able to prove that S is closed under addition. However, we have

Corollary 4d: If for any γ in S there exists a β in S such that $\beta + \gamma\ (-1)$ is also in S and is a permutation then $\delta + \gamma$ is in S for all δ in S; in other words, addition of γ on the right is a one to one mapping of S onto itself.

Proof: Since the element $\beta + \gamma\ (-1)$ of S is a permutation its inverse $\{\beta + \gamma\ (-1)\}^{-1} = \tau$, say, is also in S, by Corollary 2*d*; and hence $\tau\delta$ is in S for all δ in S, by Corollary 1*d*. Taking $\tau\delta$ in place of δ in the Theorem we get the required result.

There are two important particular cases in which S is closed under addition.

Lemma 4a: If α is an automorphism of G which moves every non-identity element then $(-1)\ \alpha + 1$ is a permutation of the elements of G.

Proof: If $(x^{-1})^{\alpha}\ x = (y^{-1})^{\alpha}\ y$, then multiplying both sides of the left by x^{α} and on the right by y^{-1} we get $(xy^{-1})^{\alpha} = xy^{-1}$ so that xy^{-1} is the identity element of G and hence $x = y$.

Lemma 4*a* shows that an automorphism α with the stated property can be taken for the construction of the set S.

Theorem 16: If α is an automorphism of G which moves every non-identity element then the set S is closed under addition.

Proof: Since α is an automorphism the right distributive law $(\beta + \gamma)\ \alpha$ holds for all β, γ in U. Now let β, γ be arbitrary elements of S. Then $\beta\alpha + \gamma\ \{(-1)\alpha+1\} = \{\beta+\gamma(-1)\}\ \alpha + \gamma$ is also in S. Since, by Corollary 2*b* of Theorem 11, α^{-1} and $\{(-1)\alpha+1\}^{-1}$ are also in S it follows by Corollary 1*b* of the same theorem that $\beta\alpha^{-1}$, $\gamma\ [(-1)\alpha+1\}^{-1}$ are also in S. Hence, replacing β, γ by $\beta\alpha^{-1}$, $\gamma\{(-1)\alpha+1)\}^{-1}$ in $\beta\alpha+\gamma\ \{(-1)\alpha+1\}$ we see that $\beta+\gamma$ is in S.

The other particular case is obtained by taking α to be the mapping n which maps every element x of G into its nth power x^n. The conditions that α and $(-1)\alpha+1$ are permutations then reduce to the conditions that n and $(n-1)$ are prime to the order v of G or, in other words to the single condition that $n(n-1)$ is prime to v. It is moreover clear that in this case all the elements of S are integers so that the right distributive law holds in S and we may write the element $\{\beta+\gamma(-1)\}\ \alpha+\gamma$ in the form

$\beta n+\gamma(-n+1)$. Hence, by an argument similar to that in the proof of Theorem 16 we get

Theorem 17: If n is an integer such that $n(n-1)$ is prime to the order ν of the group G, then the set S constructed with $\alpha=n$ is closed under addition.

Corollary 1e: The set S of the theorem is the ring of residues mod N where N is the least common multiple of the orders of the elements of G.

The proof follows at once from the fact that S contains the mapping 1.

We next suppose that α, α' are two automorphisms of G which move every non-identity element so that the corresponding quasi-groups $S(\alpha)$, $S(\alpha')$ are subnear-rings of U by Theorem 16 and Corollary 1*d* of Theorem 15. Then we have

Theorem 18: A mapping φ of $S(\alpha)$ onto $S(\alpha')$ which leaves 0, 1, which are common to both $S(\alpha)$ and $S(\alpha')$, invariant is a quasi-group isomorphism if and only if it is a near ring isomorphism mapping α into α'.

Proof: Let $\odot$, $\odot'$ denote the quasi-group operations in $S(\alpha)$, $S(\alpha')$ respectively. Since α is an automorphism it commutes with the mapping (-1) so that $(-1)\alpha=-\alpha$, the negative of α, Hence it follows, as in the proof of Theorem 16, that $\beta\odot\gamma=\beta\alpha+\gamma(-\alpha+1)$ for all β, γ in $S(\alpha)$. Likewise we have $\beta'\odot'\gamma'=\beta'\alpha'+\gamma'(-\alpha'+1)$ for all β', γ' in $S(\alpha')$. Now suppose that φ is a quasi-group isomorphism of $S(\alpha)$ onto $S(\alpha')$ which maps 0, 1 into themselves respectively. If φ maps β, γ in $S(\alpha)$ into β', γ' in $S(\alpha')$ respectively, then $\beta\alpha+\gamma(-\alpha+1)$ is mapped into $\beta'\alpha'+\gamma'(-\alpha'+1)$. In particular, taking β, γ separately equal to 1, 0 and 0,1 respectively we see that φ maps α into α' and $-\alpha+1$ into $-\alpha'+1$. Moreover, taking $\gamma=0$ we see that if $\varphi(\beta)=\beta'$, then $\varphi(\beta\alpha)=\beta'\alpha$ so that, in particular, all powers of α are mapped into the same powers of α' and hence also that α and α' are of the same order. It follows that $\varphi(\beta\alpha^{-1})=\beta'\alpha'^{-1}$. Likewise, taking $\beta=0$, we get $\varphi\{\gamma(-\alpha+1)\}=\gamma'(-\alpha'+1)$, so that $-\alpha+1$ and $-\alpha'+1$ are of the same order and $\varphi\{\gamma(-\alpha+1)^{-1}\}=\gamma'(-\alpha'+1)^{-1}$. Finally replacing β and γ by $\beta\alpha^{-1}$ and $\gamma(-\alpha+1)^{-1}$ respectively in $\beta\alpha+\gamma(-\alpha+1)$ we see that $\beta+\gamma$ is mapped into $\beta'+\gamma'$ which shows that φ is an additive isomorphism. In order to prove that it is also a multiplicative isomorphism we observe that any element of $S(\alpha)$ is expressible in terms of powers of α and $-\alpha+1$ and the addition and multiplication operations. This can easily be seen by induction from the relation $\beta\odot\gamma=\beta\alpha+\gamma(-\alpha+1)$. We have already seen that if β is mapped into β' under φ then $\beta\alpha^r$, $\beta(-\alpha+1)^r$ are mapped into $\beta'\alpha'^r$, $\beta'(-\alpha'+1)^r$ respectively so that if γ is expressed in terms of sums and products of powers of α and $-\alpha+1$ it follows from induction on the total number of occurrences of powers of α and $-\alpha+1$ and by successive application of the left distributive law and the additive isomorphism of the mapping φ that $\beta\gamma$ is mapped into $\beta'\gamma'$ which completes the proof of the necessity part of the condition. The same result can also be obtained by showing, as in the proof of Theorem 15, that if φ maps β, γ, δ in $S(\alpha)$ into β', γ', δ' respectively, then $\varphi\{[\beta+\gamma(-1)]\delta+\gamma\}=\{\beta'+\gamma'(-1)\}\delta'+\gamma'$. To prove that the condition is also sufficient it is enough to observe that if φ is a near-ring isomorphism mapping α into α' then 0, 1 are mapped into themselves being the zero and the unity element respectively of both $S(\alpha)$ and $S(\alpha')$ considered as near rings and hence if β, γ are mapped into β', γ' respectively under φ then $\varphi(\beta\odot\gamma)=\varphi\{(\beta\alpha+\gamma(-\alpha+1)\}=\beta'\alpha'+\gamma'(-\alpha'+1)=\beta'\odot'\gamma'$.

APPLICATIONS OF ALGEBRAIC TECHNIQUE

We shall now apply the results of the previous section in the actual construction of certain classes of homogeneous quasi-groups, both primitive and imprimitive. We shall continue to use the same notations as in that section.

Let p be an odd prime and G a p-group in which every element other than the identity is of order p. We construct the set $S = S(\alpha)$ with $\alpha = n$, an integer, where $n \not\equiv 0, 1 \pmod{p}$ so that $n(n-1)$ is prime to p and hence to the order of the group G. Theorem 17 is therefore applicable to this case and we see that S consists of precisely the residue classes (mod p). Theorem 13 is therefore also applicable since for every non-identity element z of G, z^m are distinct for distinct residues m (mod p). Hence we get

Theorem 19: If G is a finite group in which every non-identity element is of order p, where p is an odd prime, and n is any integer different from 0, 1 (mod p), then G becomes a homogeneous quasi-group under the composition $\odot$ defined by $x \odot y = (xy^{-1})^n y$; and the primitive subquasi-groups of $(G, \odot)$ are all of order p and are isomorphic to the quasi-group formed by the set S of residues (mod p) under the composition $k \odot m = kn + m(1-n)$ for all k, m in S.

Corollary 1f : The set S of residues (mod p) becomes a primitive homogeneous quasi-group under the operation $\odot$ defined by $k \odot m = kn + m(1-n)$ where n is any given residue (mod p) different from 0, 1.

The above Corollary is, however, a particular case of a more general result that we shall prove below where we shall also consider the non-isomorphic cases.

We shall henceforth suppose that G is the additive group of the Galois Field $GF(p^m)$ where p is an arbitrary prime and m any positive integer (which we shall suppose to be greater than 1 if $p = 2$).

The mapping of G into itself defined by the multiplication of the elements of G by any given element u of the field shall be denoted by u itself. This makes the field $GF(p^m)$ a subfield of the near-ring of all mappings of G into itself which leave the zero-element of G invariant. We observe further that if $u \neq 0, 1$ then the mapping u is an automorphism of G which moves every non-zero element of G. It follows that the hypothesis of Theorem 16 is fulfilled if we take $\alpha = u$ where u is any given element of the field $GF(p^m)$ different from 0 and 1 so that the corresponding set of mappings $S = S(u)$ is a sub-ring of $GF(p^m)$. In fact, S coincides with the sub-field generated by u since it contains u and its elements are all polynomials in u. Hence we have

Theorem 20: If G is the additive group of the Galois Field $GF(p^m)$ and the mapping α of G is taken to be the multiplication by a given element u of the field different from 0, 1, then the corresponding set S consists of the elements of the subfield generated by u.

Corollory 1g: The set of elements of the primitive subquasi-group generated by x, y is given by $\{xv + y(1-v)/v \in S(u)\}$.

Multiplication of a given non-zero element z of G by distinct elements of S obviously gives rise to distinct elements of G. Hence the hypothesis of Theorem 13 is satisfied and we have

Theorem 21: The set G of elements of the Galois Field $GF(p^m)$ becomes a homogeneous quasi-group when the quasi-group operation is defined by $x \odot y = xu + y(1-u)$

where u is any given elements of the field different from 0, 1, *the primitive subquasi-groups of* $(G,\odot)$ *being of the same order as the subfield generated by* u.

We observe that the quasi-group S to which the primitive subquasi-groups of $(G,\odot)$ are isomorphic coincides with the primitive subquasi-group $Q(0, 1)$ of $(G,\odot)$ generated by 0 and 1. Hence we have

Corollary 1 h : The homogeneous quasi-group $(G,\odot)$ of Theorem 21 is primitive if and only if u is a generating element of the field $GF(p^m)$.

In fact, if u is a generating element of the field then the set S coincides with the set G.

It is now easy to settle the question of the possible isomorphism of the primitive quasi-groups $S(u)$ corresponding to distinct generating elements u of a Galois Field. In fact, we prove

Theorem 22: If u, u' are generating elements of the Galois Field $GF(p^m)$ then the corresponding primitive homogeneous quasi-groups $S(u)$, $S(u')$ under the operations $\beta\odot\gamma=\beta u+\gamma(1-u)$, $\beta'\odot'\gamma' = \beta'u'+\gamma'(1-u')$ respectively are isomorphic if and only if u, u' are roots of the same irreducible polynomial.

Proof : By Theorem 20 the elements of $S(u)$ and $S(u')$ coincide with those of the field $GF(p^m)$. Moreover, the near-ring operations of addition and multiplication in $S(u)$ and $S(u')$ coincide with addition and multiplication respectively in $GF(p^m)$. It follows that a near-ring isomorphism of $S(u)$ onto $S(u')$ is simply an automorphism of $GF(p^m)$. Since, by Theorem 18, a quasi-group isomorphism of $S(u)$, $S(u')$ which leave 0, 1 invariant is a near-ring isomorphism of $S(u)$ onto $S(u')$ which maps u into u' and *vice-versa* it follows that there exists a quasi-group isomorphism of $S(u)$ onto $S(u')$ which leave 0, 1 invariant if and only if there exists an automorphism of $GF(p^m)$ which maps u into u' the necessary and sufficient condition for which is that u and u' are roots of the same irreducible polynomial. This completes the proof of the Theorem.

Corollary 1i : There are at least $N(p^m) =$

$$\frac{1}{m}\sum_{r=0}^{k}(-1)^r \sum_{i_1<\ldots<i_r} p^{m/p_{i_1}\ldots p_{i_r}}$$

distinct primitive homogeneous quasi-group of order p^m where $p_1, \ldots, p_k$ are the distinct prime factors of m and the inner summation is over all combinations, r at a time, of the prime factors $p_1, \ldots, p_k$.

Proof : This follows at once from the fact that the irreducible polynomial having the generating elements u, u' as roots is a generating polynomial of the field and that there are exactly $N(p^m)$ distinct generating polynomials for $GF(p^m)$. Clearly the interchange of all corresponding rows and columns of a homogeneous quasi-group gives rise to a homogeneous quasi-group which we shall call the transpose of the given quasi-group. It is also clear that a transpose is primitive if and only if the given homogeneous quasi-group is primitive. We observe that the transpose of the primitive quasi-group $S(u)$ of the theorem is simply the qusi-group $S(1-u)$ since the inter-

change of rows and columns is equivalent to interchanging x and y in the right-hand side of the relation $x \odot y = xu + y(1-u)$. Hence we have

Corollary 2e: The primitive quasi-group $S(u)$ is isomorphic to its transpose if and only if $1-u = u^{p^r}$ for some r.

Corollary 3e: The primitive quasi-group is commutative if and only if $u = \frac{p+1}{2}$, p odd.

Proof: Commutativity of $S(u)$ is equivalent to the equality $xu+y(1-u) = yu+x(1-u)$ for all x, y. This is possible if and only if $2u = 1$ or $u = \frac{p+1}{2}$, p odd.