APPLICATION OF NEAR RINGS TO COMBINATORIAL PROBLEMS

by P. KESAVA MENON, *Director, Joint Cipher Bureau, Ministry of Defence, Sena Bhawan, D.H.Q.P.O., New Delhi-110011*

(*Received 9 May 1974; after revision 17 September 1974*)

Quasi groups are introduced in a group with the help of the near ring of mappings of the Group where multiplication and (non-commutative) addition of mappings are defined by $x^{\alpha\beta} = (x^{\alpha})^{\beta}$ and $x^{\alpha+\beta} = x^{\alpha} \cdot x^{\beta}$. Conditions are found under which the multiplication tables of some of the quasi-group structures so defined are Latin Squares which are mutually orthogonal or have some additional properties . In particular the method leads to purely algebraic proofs of the well-known result on the existence of a complete set of mutually orthogonal Latin Squares of prime power order.

INTRODUCTION

The set M of all mappings of a group G into itself becomes a near-ring under addition and multiplication defined by

$$x^{\alpha+\beta} = x^{\alpha}x^{\beta}, \quad x^{\alpha\cdot\beta} = (x^{\alpha})^{\beta} \qquad .. \quad .. \quad .. \quad (1)$$

where x^{α} is the image of $x \in G$ under the mapping $\alpha \in M$.
We shall denote the mapping

$$x \to x^{n} \qquad .. \quad .. \quad .. \quad (2)$$

where n is an integer by n itself so that in particular, 1 is the identity mapping of G and O is mapping which maps every element of G into its identity element e. Besides being a semi-group with identity 1 under multiplication M is also a group under addition with identity element O. However $(M, +)$ is not in general commutative. Clearly the negative $-\alpha$ of α is defined by

$$x^{-\alpha} = (x^{\alpha})^{-1} \qquad .. \quad .. \quad .. \quad (3)$$

so that

$$-\alpha = \alpha(-1) \qquad .. \quad .. \quad .. \quad (4)$$

We note, however, that in general $-\alpha \neq (-1)\,\alpha$.

There is also a one-sided distributive law in M :

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma. \qquad .. \quad .. \quad .. \quad (5)$$

G is isomorphic to a subgroup of the multiplicative semigroup of M. In fact if for any $a \in G$ we define the mapping $\bar{a}$ of G by

$$x^{\bar{a}} = xa, \quad x \in G, \qquad .. \quad .. \quad .. \quad (6)$$

then the mapping

$$a \to \bar{a} \qquad .. \quad .. \quad .. \quad (7)$$

is clearly an isomorphism of G into $(M, \cdot)$. We may therefore suppose that G is embedded in M by identifying $\bar{a}$ with a. A groupoid is defined as a set S with a binary operation mapping all ordered pairs of elements of S into S.

Our object is to introduce several groupoid structures in G with the help of the mappings in M so that the multiplication tables of the new structures have interesting Combinatorial interpretations. This enables us to generalize some known results in Combinatorial theory as well as to obtain certain new ones.

We shall suppose that the rows and columns of all multiplication tables of the groupoids defined in G are indexed by the elements of G taken in a definite order and that the element in the x-th row and y-th column of a groupoid $(G, *)$ is $x * y$. The multiplication tables of two groupoids $(G, *_1)$, $(G, *_2)$ are said to be mutually orthogonal if the pair of equations

$$x *_1 y = a, \quad x *_2 y = b \qquad .. \qquad .. \qquad .. \quad (8)$$

can be solved uniquely in G for every choice of $a, b \in G$. The adjoint $*'$ of a binary operation $*$ is defined by the condition

$$x *' y = y * x \qquad .. \qquad .. \qquad .. \quad (9)$$

for all $x, y \in G$ so that the multiplication table of $(G, *')$ is the transpose of that of $(G, *)$. It follows, in particular, that self-adjoint binary operations correspond to commutative groupoids.

The multiplication table of a groupoid $(G, *)$ is called a row-latin (column-latin) square if every row (column) of the table contains each element of G exactly once. A multiplication table which is both row-latin and column-latin is called a latin square. The necessary and sufficient condition that the multiplication table of $(G, *)$ is row-latin (column-latin) is clearly that for any given x (y) and arbitrary $z \in G$ the equation

$$x * y = z \qquad .. \qquad .. \qquad .. \quad (10)$$

has a unique solution in $y(x)$.

We shall call a one to one mapping of G onto itself a permutation. The set of permutations of G form a subgroup of the multiplicative semigroup $(M, \cdot)$ containing G (considered as mappings of G). The inverse of the permutation α shall be denoted by α^{-1}.

Multiplication Tables of Groupoid $(G, *)$

Lemma 1: The multiplication table of the groupoid $(G, *)$ defined by

$$x * y = (xy^{\delta})^{\alpha} x^{\epsilon}, \ \alpha, \delta, \epsilon \in M, \qquad .. \qquad .. \qquad .. \quad (11)$$

is row-latin if α, δ are permutations.

Proof: For any $x, z \in G$ the equation

$$(xy^{\delta})^{\alpha} x^{\epsilon} = z \qquad .. \qquad .. \qquad .. \quad (12)$$

has the unique solution

$$y = \left\{ x^{-1} (zx^{-\epsilon})^{\alpha^{-1}} \right\}^{\delta^{-1}}$$

Also for a given x distinct values of z give rise to distinct values of y.

Lemma 2 : The multiplication table of the groupoid (G, *) defined by Eq. (11) is column-latin if $\alpha + \epsilon$, δ are permutations and ϵ is an endomorphism of G.

Proof : Eq. (12) can be written as

$$(xy^{\delta})^{\alpha+\epsilon} = zy^{\delta\epsilon}$$

from which it follows that given y, z it has the unique solution

$$x = (zy^{\delta\epsilon})^{(\alpha+\epsilon)^{-1}} y^{-\delta}$$

For given y, distinct values of z give rise to distinct values of x.

Theorem 1 : The multiplication table of the groupoid $(G, *)$ *defined by Eq. (11) is a latin square if* α, δ, $\alpha + \epsilon$ *are permutations and* ϵ *is an endomorphism of* G.

Proof : This follows at once from lemmas 1 and 2.

Corollary 1.1 : If the binary operation * is defined by

$$x * y = (xy^{\delta})^{\alpha}, \quad \alpha, \delta \in M, \qquad \ldots \qquad (13)$$

then the multiplication table of (G, *) is a latin square if α and δ are permutations.

Corollary 1.2 : The multiplication table of $(G, *)$ where

$$x * y = (xy)^{\alpha} x^{\epsilon} \qquad \ldots \qquad (14)$$

is a latin square if α, $\alpha + \epsilon$ are permutations and ϵ is an endomorphism.

Corollary 1.3 : The multiplication table of $(G, *)$ where

$$x * y = (xy^{-1})^{\alpha} x^{\epsilon} \qquad \ldots \qquad (15)$$

is a latin square if α, $\alpha + \epsilon$ are permutations and ϵ is an endomorphism.

Corollary 1.4 : The multiplication table of $(G, *)$ where

$$x * y = xyx \qquad \ldots \qquad (16)$$

is a latin square if G is of odd order.

Corollary 1.5 : The multiplication table of $(G, *)$ where

$$x * y = xy^{-1} \qquad \ldots \qquad (17)$$

is a latin square

Corollary 1.6 : The multiplication table of $(G, *)$ where

$$x * y = xy^{-1} x \qquad \ldots \qquad (18)$$

is a latin square if G is of odd order.

Theorem 2 : If $*_1$, $*_2$ *are defined by*

$$\begin{aligned} x *_1 y &= (xy^{\delta})^{\alpha} \\ x *_2 y &= (xy^{\delta})^{\beta} x^{\epsilon} \end{aligned} \qquad \ldots \qquad (19)$$

where α, δ, β, $\beta + \epsilon$ *are permutations and* ϵ *is an automorphism of* G, *then the multiplication tables of* $(G, *_1)$ *and* $(G, *_2)$ *are orthogonal latin squares.*

Proof : By Theorem 1 and its corollary 1.1 the multiplication tables of $(G, *_1)$ and $(G, *_2)$ are latin squares. To prove that they are orthogonal we have only to show that the equations

$$(xy^{\delta})^{\alpha} = a, \quad (xy^{\delta})^{\beta} x^{\epsilon} = b \qquad \ldots \qquad (20)$$

can be solved uniquely for any given $a, b \in G$. Substituting from the first of Eq. (20) in the second and solving it for x we get

$$x = \left\{ (a^{\alpha^{-1}} \cdot \beta)^{-1} b \right\}^{\epsilon^{-1}} \quad .. \quad .. \quad .. \quad (21)$$

Also we have

$$y^{\delta} = a^{\alpha^{-1}} x^{-1} \quad .. \quad .. \quad .. \quad (22)$$

which gives

$$y = (a^{\alpha^{-1}} x^{-1})^{\delta-1} \quad .. \quad .. \quad .. \quad (23)$$

in which we substitute for x from Eq. (21).

Corollary 2.1 : The multiplication tables of G and $(G, *)$ where

$$x * y = (xy)^{\alpha} x^{\epsilon} \quad .. \quad .. \quad .. \quad (24)$$

are mutually orthogonal latin squares if ϵ is an automorphism of G and α, $\alpha + \epsilon$ are permutations.

In particular, we have,

Corollary 2.2 : If G is a finite group and m $(m + 1)$ is prime to the order of G then the multiplication table of $(G, *)$ where

$$x * y = (xy)^{m} x \quad .. \quad .. \quad .. \quad (25)$$

is a latin square orthogonal to the multiplication table of G.

We remark that since m $(m + 1)$ is always even, corrollary 2.2 will have content only if the order n of G is odd. Since there are exactly $n \pi (1 - 2/p)$ residues m mod n, such that $m(m + 1)$ is prime to n, the product being over all distinct prime factors p of n, it follows that, when n is odd, there is always a latin square orthogonal to the multiplication table of G. We can always give one such latin square explicitly. In fact, when n is odd and $m = \frac{n-1}{2}$, clearly $m(m + 1) = \frac{n^2-1}{4}$ is always prime to n so that, from corollary 2.2, we get

Corollary 2.3 : If G is a group of odd order n, then the multiplication table of $(G, *)$ where

$$x * y = (xy)^{(n-1)/2} x \quad .. \quad .. \quad .. \quad (26)$$

is a latin square orthogonal to the multiplication table of G.

Theorem 3 : If $*_1$, $*_2$ are defined by

$$x *_1 y = (xy^{\delta})^{\alpha} x^{\epsilon} \quad .. \quad .. \quad .. \quad (27)$$
$$x *_2 y = (xy^{\delta})^{\beta} x^{\epsilon}$$

when α, β, $\alpha - \beta$, δ, $\alpha + \epsilon$, $\beta + \epsilon$ are permutation and ϵ is an automerphism of G, then the multiplication tables of $(G, *_1)$ and $(G, *_2)$ are mutually orthogonal latin squares.

Proof: By Theorem 1, the multiplication tables of $(G, *_1)$ and $(G, *_2)$ are latin squares. To show that they are orthogonal let a, b be arbitrarily given elements of G and consider the equations

$$(xy^{\delta})^{\alpha} x^{\epsilon} = a, \quad (xy^{\delta})^{\beta} x^{\epsilon} = b \qquad .. \quad .. \quad .. \quad (28)$$

From Eq. (28) we get

$$(xy^{\delta})^{\alpha-\beta} = ab^{-1}$$

so that, since $\alpha-\beta$ is a permutation

$$xy^{\delta} = (ab^{-1})^{(\alpha-\beta)^{-1}} \qquad .. \quad .. \quad .. \quad (29)$$

Substituting from (29) in (28) we get

$$x = \left[\left\{(ab^{-1})^{(\alpha-\beta)^{-1}}\right\}^{-\alpha} a \right]^{\epsilon^{-1}} \qquad .. \quad .. \quad .. \quad (30)$$

which, on substitution in

$$y = \left\{ x^{-1}(ab^{-1})^{(\alpha-\beta)^{-1}} \right\}^{\delta^{-1}} \qquad .. \quad .. \quad .. \quad (31)$$

gives the values of y also uniquely.

Corollary 3.1 : The multiplication table of $(G, *)$ where

$$x * y = (xy^{-1})^{\alpha} x^{\epsilon} \qquad .. \quad .. \quad .. \quad (32)$$

where α, $\alpha + \epsilon$ are permutations and ϵ is an automorphism of G is a latin square orthogonal to its transpose if $(-1)(\alpha + \epsilon)-\alpha$ is a permutation.

Proof : The adjoint $*'$ of $*$ is given by

$$\begin{aligned} x *'y &= (yx^{-1})^{\alpha} y^{\epsilon} = (yx^{-1})^{\alpha+\epsilon} x^{\epsilon} \\ &= (xy^{-1})^{(-1)(\alpha+\epsilon)} x^{\epsilon} \qquad .. \quad .. \quad .. \quad (33) \end{aligned}$$

Hence by Theorem 3, the multiplication tables of $(G, *)$ and $(G, *')$ are mutually orthogonal latin squares if $(-1)(\alpha + \epsilon)-\alpha$ is also a permutation.

As a special case of corollary (3.1) we get

Corollary 3.2 : If G is a finite group and m is an integer such that $m(m + 1)(2m + 1)$ is prime to the order of G then the multiplication table of $(G, *)$ where

$$x * y = (xy^{-1})^{m} x \qquad .. \quad .. \quad .. \quad (34)$$

is a latin square orthogonal to its transpose.

We observe that since $m(m + 1)(2m + 1)$ is always a multiple of 6, Corollary (3.2) will have no content unless the order of G is of the form $\pm 1 \bmod 6$. If the latter condition is satisfied we may always take m to be equal to 1 so that we have

Corollary 3.3 : If the group G is of order $6n \pm 1$ the multiplication table of $(G, *)$ where

$$x * y = xy^{-1} x \qquad .. \quad .. \quad .. \quad (35)$$

is a latin square orthogonal to its transpose.

As another application of Theorems (2) and (3) we derive the well-known theorem on the existence of $p^n - 1$ mutually orthogonal latin squares of order p^n, where p is a prime.

Let $(G, +)$ be the additive group of the Galois field $GF(p^n)$ and, for any $a \in G$, let the mapping $\bar{a}$ of G into itself be defined by

$$x^{\bar{a}} = xa, \; x \in G \qquad .. \qquad .. \qquad .. \quad (36)$$

and let the groupoid $(G, @)$ be defined by

$$x @ y = (x + y)\, a + x. \qquad .. \qquad .. \qquad .. \quad (37)$$

Then clearly $\bar{a}$ is a permutation if $a \neq 0$.

Let T denote the addition table of $(G, +)$ and let T_a be the multiplication table of $(G, @)$. Then, by Corollary 2.1 to Theorem 2, with $\alpha = \bar{a}$ and $\epsilon = 1$ we see that if $a \neq 0, -1$, then T_a is a latin square orthogonal to the latin square T. Also, by Theorem 3, it follows that T_a is orthogonal to T_b if a, b are distinct elements of G different from 0 and -1. It follows that $\{T, T_a\ (a \neq 0, -1)\}$ form a set of mutually orthogonal latin squares.

Further applications of near rings to combinatorial problems will be given subsequently.