PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 36, No. 2, December 1972

CERTAIN M.O.L.S. AS GROUPS

JUDITH Q. LONGYEAR

ABSTRACT. It is shown that latin squares may be composed in a natural way, and that many sets of mutually orthogonal latin squares (m.o.l.s.) connected with projective planes may be regarded as groups of m.o.l.s.

An axiom T6 is given for ternary rings. If T6 is true for a given ring, then the associated projective plane has prime power order; thus if T6 is a consequence of the definition for ternary rings, all projective planes have prime power order.

1. **Introduction and definitions.** For background material and proofs of assumed theorems, see Hall [3] or Ryser [8]. It is known that a projective plane of order n, that is, with $n+1$ points on each line, exists iff a set of $n-1$ mutually orthogonal latin squares (m.o.l.s.) of order n exists. Since the question of existence is largely unresolved for non-prime-power n, it is important to regard both planes and m.o.l.s. in as many different lights as possible.

DEFINITION 1. Let $\mathscr{C}$ be the class of all $n\times n$ arrays having all of the numbers $\{0, 1, \cdots, n-1\}$ as entries in each column. If S is any member of $\mathscr{C}$, the jth column of S may be regarded as a permutation $p(j)$ of the elements $\{0, 1, \cdots, n-1\}$, and so we may write $S=(p(0), p(1), \cdots, p(n-1))$. If T is another such array, say $T=(q(0), q(1), \cdots, q(n-1))$, define $S * T=(p(0)q(0), p(1)q(1), \cdots, p(n-1)q(n-1))$, where $p(i)q(i)$ is the usual composition of permutations. If id is the identity permutation, then $I=(\mathrm{id}, \mathrm{id}, \cdots, \mathrm{id})$ is a unit for $\mathscr{C}$.

A charming and useful consequence of this definition is given by Proposition 1. Recall that an array is a latin square if each of $\{0, 1, \cdots, n-1\}$ occurs in each row and each column, and that two arrays $(a_{i,j})$, $(b_{i,j})$ are orthogonal if the set of all $(a_{i,j}, b_{i,j})$ is exactly the set of all (i, j) for $0\leqq i, j\leqq n-1$.

PROPOSITION 1. *$S=(p(0), \ldots, p(n-1))$ is a latin square iff $p(i)^{-1}p(j)$ is a regular permutation for all i and j. If S and $T=(q(0), \cdots, q(n-1))$ are latin squares then S and T are orthogonal iff $S * T^{-1}$ is a latin square.*

Received by the editors April 24, 1972.
AMS (MOS) subject classifications (1970). Primary 05B15; Secondary 14N05.

PROOF. Since $p(i)^{-1}p(j)$ is a regular permutation exactly when its application to every element y is distinct from y, we see that $p(i)^{-1}p(j)$ is regular exactly when $p(i)^{-1}p(j)y \neq y$ or $p(j)y \neq p(i)y$. But this is the same as saying that the column j differs from the column i in the place y, which defines latinity for S since each column contains all of the set $\{0, 1, \cdots, n-1\}$.

Now suppose that S and T are latin squares, normalized so that $p(0)=q(0)=\mathrm{id}$. Clearly, $T^{-1}=(\mathrm{id}, q(1)^{-1}, \cdots, q(n-1)^{-1})$ and

$$S * T^{-1} = (\mathrm{id}, p(1)q(1)^{-1}, \cdots, p(n-1)q(n-1)^{-1}).$$

If $p(i)j=p(k)l=r$ and $q(i)j=q(k)l=s$ then $q(i)^{-1}s=j$ and $q(k)^{-1}s=l$, whence $p(i)q(i)^{-1}s=p(i)j=r=p(k)l=p(k)q(k)^{-1}s$. But that says that $p(i)q(i)^{-1}s=p(k)q(k)^{-1}s$ or that

$$(p(k)q(k)^{-1})^{-1}(p(i)q(i)^{-1})s = s. \tag{1}$$

Thus if S and T are not orthogonal, then the pair (r, s) occurs twice, say at (i, j) and (k, l), with $i \neq k$ and $j \neq l$. Then the above discussion shows that $S * T^{-1}$ is not a latin square. Conversely, if S and T are orthogonal, then (1) can only happen if $i=k$, so $S * T^{-1}$ is a latin square.

If one restricts oneself to latin squares, all of the above is equally true, mutatis mutandis, using rows and row permutations instead of columns and column permutations; however, due no doubt to what Halmos calls "a perversity not of the author, but of nature", only the column definition yields theorems stronger than Proposition 1. In fact, Mann [7] has given the row version of Proposition 1.

DEFINITION 2. With each coordinatization of each projective plane P, there is associated a set of $n-1$ normalized m.o.l.s. We take the set $\mathscr{S}=\mathscr{S}(P)$ to be these $n-1$ m.o.l.s., together with the array $I=(\mathrm{id}, \mathrm{id}, \cdots, \mathrm{id})$, which is orthogonal with every normalized latin square.

2. **Desarguesian projective planes.** In [5], Veblen constructs all Desarguesian planes. We may construct these in terms of their m.o.l.s. as follows. Let $\mathscr{G}$ be any Galois field; then the square $S_k(\mathscr{G})=S_k$ has as its (i, j)th entry the element $x_i+x_jx_k$ where the x's are the elements of $\mathscr{G}$ in some ordering. If $0=x_0$ and $1=x_1$, then each S_k is normalized, S_0 fails to be a latin square and $S_1, S_2, \cdots, S_{n-1}$ are a set of $n-1$ m.o.l.s. where n is the order of $\mathscr{G}$. It is easy to see that $S_k=(\mathrm{id}, \sigma^k, \sigma^{2k}, \cdots, \sigma^{(n-1)k})$ where σ is the permutation represented by the cycle $(0, 1, x_2, \cdots, x_{n-1})$.

For every k and j including 0,

$$S_k * S_j = (\mathrm{id}, \sigma^{k+j}, \cdots, \sigma^{(n-1)(k+j)}) = S_{k+j}.$$

If $S_k \neq I$, let j be the label assigned to the inverse of x_k in $\mathscr{G}$, then $S_j \in S$,

so $\mathscr{S}$ is closed under multiplication and taking inverses. But this means that $\mathscr{S}$ is an abelian (since $k+j=j+k$ as labeling numbers) group, so we have the following.

THEOREM 1. *If P is a Desarguesian plane, then $\mathscr{S}(P)$ is an abelian group.*

3. **Veblen-Wedderburn systems.** The famous first example of a non-Desarguesian plane, given by Veblen and Wedderburn [6], is usually written in the following collineation of order 13 taking subscripts i to $i+1$ (mod 13) for both lines and points. (See, for instance, Hall [3].)

$$
\begin{aligned}
L_0&: A_0\ A_1\ A_3\ A_9\ B_0\ C_0\ D_0\ E_0\ F_0\ G_0,\\
M_0&: A_0\ B_1\ B_8\ D_3\ D_{11}\ E_2\ E_5\ E_6\ G_7\ G_9,\\
N_0&: A_0\ C_1\ C_8\ E_7\ E_9\ F_3\ F_{11}\ G_2\ G_5\ G_6,\\
P_0&: A_0\ B_7\ B_9\ D_1\ D_8\ F_2\ F_5\ F_6\ G_3\ G_{11},\\
Q_0&: A_0\ B_2\ B_5\ B_6\ C_3\ C_{11}\ E_1\ E_8\ F_7\ F_9,\\
R_0&: A_0\ C_7\ C_9\ D_2\ D_5\ D_6\ E_3\ E_{11}\ F_1\ F_8,\\
S_0&: A_0\ B_3\ B_{11}\ C_2\ C_5\ C_6\ D_7\ D_9\ G_1\ G_8.
\end{aligned}
$$

The affine representation of this gives rise to a set of m.o.l.s. which may be briefly written as follows. Let a be the permutation (123)(456)(789) and x be the permutation (147)(258)(369), then

$$
\begin{aligned}
S_1 &= (\mathrm{id},\ a,\ a^2,\ x,\ a^2x^2,\ a^2x,\ x^2,\ ax^2,\ ax),\\
S_2 &= (\mathrm{id},\ a^2,\ a,\ x^2,\ ax,\ ax^2,\ x,\ a^2x,\ a^2x^2),\\
S_3 &= (\mathrm{id},\ x^2,\ x,\ a^2x,\ a,\ a^2,\ ax,\ a^2x^2,\ ax^2),\\
S_4 &= (\mathrm{id},\ ax,\ a^2x^2,\ ax^2,\ x,\ a,\ a^2,\ x^2,\ a^2x),\\
S_5 &= (\mathrm{id},\ ax^2,\ a^2x,\ a^2x^2,\ x^2,\ ax,\ a,\ x,\ a^2),\\
S_6 &= (\mathrm{id},\ x,\ x^2,\ ax,\ ax^2,\ a^2x^2,\ a^2x,\ a^2,\ a),\\
S_7 &= (\mathrm{id},\ a^2x,\ ax^2,\ a,\ a^2,\ x,\ a^2x^2,\ ax,\ x^2),\\
S_8 &= (\mathrm{id},\ a^2x^2,\ ax,\ a^2,\ a^2x,\ x^2,\ ax^2,\ a,\ x).
\end{aligned}
$$

Thus we have the observation that for this particular projective plane N, $\mathscr{S}(N)$ is an abelian group. For an excellent description of Veblen-Wedderburn systems, or V-W systems, see Hall [3, Chapter 12].

THEOREM 2. *If $\mathscr{V}$ is a V-W system, and if P is the projective plane derived from $\mathscr{V}$, then $\mathscr{S}=\mathscr{S}(P)$ is a group.*

PROOF. Let the rows and columns of $S_0, S_1, \ldots, S_x$ be indexed by the elements of the ternary ring $\mathscr{V}$, with 0 first and 1 second, and with the latin squares of P also indexed by $\mathscr{V}$. Then each S_m has as its (i,j)th

entry the mark $i-m\cdot j$, and we may write $S_m=(\mathrm{id}, m\sigma_1, \cdots, m\sigma_x)$ where $m\sigma_j(i)=i-m\cdot j$.

We claim that $S_0, S_1, \cdots, S_x$ are actually $S_0 = (\mathrm{id}, \mathrm{id}, \cdots, \mathrm{id})$ and $n-1$ m.o.l.s. Since $\mathscr{V}$ under addition is an abelian group, the (i,j)th place of S_0, that is $S_0(i,j)=i-0\cdot j=i$, so $S_0=(\mathrm{id}, \mathrm{id}, \cdots, \mathrm{id})$. If $m\neq 0$, and $j\neq k$ then $S_m(i,j)\neq S_m(i,k)$; for suppose otherwise. Then $s-mj=i-mk$ implies $mk=mj+0$. For $k\neq j$ there is a unique solution m to this equation. But $0\cdot k=0\cdot j+0$, so $m=0$, a contradiction.

For every m, and $i\neq l$, $S_m(i,j)\neq S_m(l,j)$, for suppose $i-mj=l-mj$, then $i=l$.

Let $m\neq p$, then if $S_m(i,j)=S_m(k,l)$ and $S_p(i,j)=S_p(k,l)$ we want to show $i=k$ and $j=l$ so as to have S_m and S_p orthogonal. But $S_m(i,j)=S_m(k,l)$ says $i-mj=k-ml$ and similarly $i-pj=k-pl$ so that $ml=mj+(k-i)$ and $pl=pj+(k-i)$. By the fifth axiom for V-W systems, there is a unique solution to $xl=xj+(k-i)$, whenever $l\neq j$. Since $m\neq p$, we have $l=j$, and so $i=k$, and S_m and S_p are orthogonal.

Now consider $\mathscr{S}$ as a set under the operation $*$. Since $\mathscr{S}$ is finite and $I=S_0\in\mathscr{S}$, we need only show that $\mathscr{S}$ is closed for $\mathscr{S}$ to be a group. If S_m and S_p are in $\mathscr{S}$, then $S_m * S_p=(\mathrm{id}, m\sigma_1 p\sigma_1, \cdots, m\sigma_x p\sigma_x)$, so

$$\begin{aligned} S_m * S_p(i,j) &= p\sigma_j m\sigma_j(i) = p\sigma_j(i-mj) = (i-mj)-pj \\ &= i-(mj-pj) = i-(m+p)j. \end{aligned}$$

If y is the label assigned to the square for $m+p$, then at each place (i,j), $S_m * S_p(i,j)=S_y(i,j)$, so $S_m * S_p=S_y$ and $\mathscr{S}$ is indeed a group.

In general, a ternary ring is a set $\mathscr{T}$ of marks and a ternary operation $a\cdot b\circ c$ defined for all a, b, c in $\mathscr{T}$. The marks must include 0 and 1 and the operation must satisfy the following axioms.

T1. $0\cdot b\circ c=a\cdot 0\circ c=c$.

T2. $1\cdot b\circ 0=b\cdot 1\circ 0=b$.

T3. For given a, b, c, there is a unique x such that $a\cdot b\circ x=c$.

T4. For given $m\neq r$ and b, c there is a unique x such that $x\cdot m\circ b=x\cdot r\circ c$.

T5. For given $a\neq b, c, d$ there is a unique pair m, r such that $a\cdot m\circ r=c$ and $b\cdot m\circ r=d$.

As Hall points out when giving this definition [3, Chapter 12], axiom T3 guarantees a unique line in each bundle of parallels through the point (a, c), axiom T4 guarantees that nonparallel lines intersect in a unique point and axiom T5 guarantees that two points not already contained in a line of a certain bundle of parallels, must be in a unique line in some other bundle.

Of course, using $\mathscr{T}$ gives an affine plane which must be extended to a projective plane.

4. **Some corollaries.** We need the following easy group theoretic results. Let P be any projective plane, and let $\mathcal{S}=\mathcal{S}(P)=\{S_0=I, S_1, \cdots, S_{n-1}\}$ be the m.o.l.s. for some coordinatization of P. Take each $S_i=(\mathrm{id}, i\sigma_1, \cdots, i\sigma_{n-1})$ and $G_j=\{\mathrm{id}, 1\sigma_j, \cdots, (n-1)\sigma_j\}$.

LEMMA. *If S is a group, then*

(1) *for every $j\neq 0$, G_j is a group and S is isomorphic with G_j under the mapping $fS_i=i\sigma_j$;*

(2) *every $i\sigma_j$ is a product of cycles each of length $l=l(i,j)$;*

(3) *every $i\sigma_j$ is a product of cycles of length l, where l does not depend on i or j;*

(4) *every $S_k\neq I$ has the same order;*

(5) *the order of each $S_k\neq I$ is a prime.*

PROOF. (i) is straightforward.

(ii) Suppose $i\sigma_j$ had cycles $(0\cdots a)$ and $(1\cdots b)$; then $(i\sigma_j)^a 0=0$ but $(i\sigma_j)^a 1=b\neq 1$, so $(i\sigma_j)^a$ would not be a regular permutation.

(iii) Suppose $k\sigma_j$ had order a and $k\sigma_i$ had order b. Then $(S_k)^a$ has jth coordinate id, whence $(k\sigma_i)^b=\mathrm{id}$ since S is a group. But then a divides b and similarly $b|a$. Thus each nonidentity coordinate permutation of S_k has the same order.

(iv) $S\cong G_1, G_2, \cdots, G_{n-1}$ and each $k\sigma_i$ and $k\sigma_j$ are different for $i\neq j$, so by the pigeon hole principle, S_k must have coordinate permutations corresponding exactly to the elements of G_1, all of which have order 1 or else the same l.

(v) If $(S_k)^{a\cdot b}=I$, then $(S_k^a)^b=I$.

COROLLARY. (i) *If $\mathcal{S}=\mathcal{S}(P)$ is a group, then P has prime power order.*

(ii) *If P is derived from a Veblen-Wedderburn system then P has prime power order.*

REMARK. For an arbitrary projective plane P with associated ternary ring $\mathcal{T}=\mathcal{T}(P)$, each $S_k\in\mathcal{S}=\mathcal{S}(P)$ has $S_k(i,j)=i-j\cdot k$ where $i-j\cdot k=x$ is the unique solution to $i\cdot b\circ x=j$, guaranteed by T3. Then each $k\sigma_j(i)=i-j\cdot k$. The jth coordinate permutation of $S_m * S_k$ is $m\sigma_j k\sigma_j$. When applied to i this yields $m\sigma_j k\sigma_j(i)=(i-j\cdot k)-j\cdot m$. It is an easy consequence of T1 and T5 that, for $j\neq 0$, there is a unique p such that $(i-j\cdot k)-j\cdot m=i-j\cdot p$.

Unfortunately p may depend on j, so that $(i-l\cdot k)-l\cdot m=i-l\cdot p'$ with $p'\neq p$. Of course, if $p'=p$ always, then $S_m * S_k=S_p$ and so $\mathcal{S}$ is a group.

COROLLARY. *If $\mathcal{G}(P)$ satisfies the following* T6 *then P has prime power order.*

T6. For given j, $l \neq 0$, and given x, y and i, there is a unique solution p to $j \cdot p \circ y = i = l \cdot p \circ x$.

I am unable to show that T6 is independent of T1 through T5 or that T6 is a consequence of T1 through T5. Of course, if T6 *is* a consequence, then all projective planes have prime power order.

References

1. L. Dickson, *Linear algebras in which division is always uniquely possible*, Trans. Amer. Math. Soc. **7** (1906), 371–390.

2. M. Hall, Jr., *Projective planes*, Trans. Amer. Math. Soc. **54** (1943), 229–277. MR **5**, 72.

3. ———, *Combinatorial theory*, Blaisdell, Waltham, Mass., 1967. MR **37** #80.

4. P. R. Halmos, *Finite dimensional vector spaces*, Ann. of Math. Studies, no. 7, Princeton Univ. Press, Princeton, N.J., 1942, p. 66. MR **4**, 11.

5. O. Veblen and W. Bussey, *Finite projective geometries*, Trans. Amer. Math. Soc. **7** (1906), 241–259.

6. O. Veblen and J. Wedderburn, *Non-desarguesian and non-pascalian geometries*, Trans. Amer. Math. Soc. **8** (1907), 379–388.

7. H. Mann. *The construction of orthogonal latin squares*, Ann. Math. Statist. **13** (1942), 418–423. MR **4**, 184; 340.

8. H. J. Ryser, *Combinatorial mathematics*, Carus Math. Monographs, no. 14, Math. Assoc. Amer.; distributed by Wiley, New York, 1963. MR **27** #51.

Department of Mathematics, Pennsylvania State University, University Park, Pennsylvania 16802