József Dénes

Algebraic and Combinatorial Characterization of Latin squares I

Matematický časopis, Vol. 17 (1967), No. 4, 249--265

Persistent URL: http://dml.cz/dmlcz/127005

Matematický časopis 17 (1967), No. 4

ALGEBRAIC AND COMBINATORIAL CHARACTERIZATION OF LATIN SQUARES I

JÓZSEF DÉNES, Budapest

The concept of the Latin square was introduced by Euler. The *Latin square* is considered by Euler as a square matrix with n^2 entries of n different elements, none of them occurring twice within any row or column of the matrix. (Without loss of generality, one may assume the elements of the Latin square to be the positive integers 1, 2, ..., n when n is called the *order* of the Latin square.) Much later, it was shown by Cayley, who investigated the multiplication tables of groups, that a multiplication table of a group is in fact an appropriately bordered special Latin square. (The multiplication table of a group is called its *Cayley table.*)

The results of Euler and Cayley made it possible to characterize Latin squares both from the algebraic and the combinatorial point of views.

Only a few authors have attempted to point out the close relationship that exists between the algebraic and combinatorial results when dealing with Latin squares ([3], [9], [10], [11], [20], [36], [42]). Particularly in practical applications it is important to exhibit the results of the theory of quasigroups and groups on the Cayley tables (on the corresponding Latin squares).

I. ELEMENTARY PROPERTIES

The Cayley table of a finite group G (considered without bordering) has the following properties:

(1) It is a *Latin square*, i. e. a square matrix $||a_{ik}||$ each row and each column of which are a permutation of the elements of G.

Since, if e.g. the element b occurred twice in the a-th row, say, at the k-th and l-th place, the solution of the equation $ax = b$ would be both $x = k$ and $x = l$, in contradiction with the group axioms.

(2) The *quadrangle criterion* holds, i.e. for any index $i, j, \ldots$ it follows from the equations $a_{ik} = a_{i_1k_1}$, $a_{il} = a_{i_1l_1}$, $a_{jk} = a_{j_1k_1}$ that $a_{jl} = a_{j_1l_1}$.

This is a trivial consequence of the group axioms, since by definition $a_{ik} =$

$= a_i a_k$ hence using the condition, we have

$$a_{jl} = a_j a_l = a_j(a_k a_k^{-1})\,(a_i^{-1}a_i)a_l = (a_j a_k)\,(a_i a_k)^{-1}\,(a_i a_l) = a_{jk}a_{ik}^{-1}a_{il} =$$

$$= a_{j_1 k_1}a_{i_1 k_1}^{-1}a_{i_1 l_1} = (a_{j_1}a_{k_1})\,(a_{i_1}a_{k_1})^{-1}(a_{i_1}a_{l_1}) = a_{j_1}a_{l_1} = a_{j_1 l_1}.$$

Conversely, any matrix $\|a_{ik}\|$ with the properties (1) and (2) is a Latin square of a group G.

To prove this, a bordering procedure has to be found showing that the Cayley table thus obtained is, in fact, a multiplication table of a group. Using as border the first row and the first column of the Latin square, the invertibility of the multiplication defined by the Cayley table thus obtained is trivial. (This is a consequence merely of property (1).) Now, only the associativity has to be proved. Let us consider arbitrary elements a, b and c. If one of them is identical with e, i.e. the unit element in the upper left corner of the Latin square defined by the bordering, it follows directly that $(ab)c = a(bc)$. If each of the elements a, b and c differs from e, then the subsquare determined by the rows e and a, and by the columns b and bc of the multiplication table is

$$\begin{array}{|cc} ab & bc \\ ab & a(bc), \end{array}$$

while the subsquare determined by the rows b and ab and by the columns e and c is

$$\begin{array}{|cc} b & bc \\ ab & (ab)c. \end{array}$$

Hence, because of the property (2) $a(bc) = (ab)c$. The property (2) was first observed by M. Frolov in 1890 [21]. Later H. Brandt [7] postulated the quadrangle criterion to hold only for quadruples in which one of the four elements is the unit element. Textbooks on the theory of finite groups (see e.g. A. Speiser [38]) adopted the criterion established by H. Brandt.

If property (2) is not required, one obtains the Cayley table of a quasigroup.

The set S is called a *quasigroup*, if there is a binary operation defined in S and if for any $a, b \in S$ the equations $ax = b$, $ya = b$ have exactly one solution.

Two quasigroups Q_1 and Q_2 (denoting the operation defined in Q_1 by 1 and that in Q_2 by 2) are called *isotopic*, if there exist permutations σ, η, ϱ, such that for any $x, y \in Q_1$

$$\sigma(x1y) = \eta(x)2\varrho(y).$$

The Latin square becomes a Cayley table as soon as it has been suitably bordered. E.g. the Latin square

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

if the border elements are inserted, the Cayley table of the cyclic group of order 4 will have the form

	1	2	3	4
1	1	2	3	4
2	2	3	4	1
3	3	4	1	2
4	4	1	2	3

Of the permutations σ, η, ϱ introduced in the definition of isotopy, σ operates on the Latin square, while η and ϱ operate on the borders.

Let us suppose, for example, that

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \qquad \eta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \qquad \varrho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}.$$

Then the Cayley table of the cyclic group of order 4 is transformed into that of its isotopic quasigroup, namely

	2	4	3	1
3	2	1	4	3
2	1	4	3	2
4	4	3	2	1
1	3	2	1	4

If $\sigma = \eta = \varrho$, the tranformation is an *isomorphism*. T. Evans [15] has shown that every quasigroup is isotopic to a *loop* (a quasigroup with a unit element). This implies that any Latin square can be so bordered that the border elements are identical with one of the rows and one of the columns of the Latin square.

Several authors have studied the *group-isotopic quasigroups*, i.e. quasigroups to which there exist isotopic groups.

T. Evans [15] has shown that a quasigroup is isotopic to a group if and only if there exist fixed permutations π_1, π_2, π_3, π_4, π_5; ϱ_1, ϱ_2, ϱ_3, ϱ_4, ϱ_5, satisfying the equation

$$\pi_5(\pi_1(x)\pi_4[\pi_2(y)\pi_3(z)]) = \varrho_5(\varrho_3[\varrho_1(x)\varrho_2(y)]\varrho_4(z))$$

where x, y, z are three arbitrary elements of the quasigroup or the group.

J. Aczél, V. D. Belousov, M. Hosszu [1] and R. H. Bruck [8] have also given a necessary and sufficient condition for a quasigroup to be group-

isotopic. If the operation 1 is defined in a quasigroup, the operation 2 in a group, then for arbitrary x, y and a fixed element z the equation

$$x1y = \varrho(x)2z2\psi(y)$$

must hold, where ϱ, ψ are two automorphisms of the group (see also [5], [28]).

The Cayley tables of the group-isotopic quasigroups are characterized by the quadrangle criterion. Isotopic groups are isomorphic. R. H. Bruck [8] proved precisely the fact that a group-isotopic quasigroup with a unit element is a group isomorphic to the given group. (See also [45].)

Consider the following quasigroups

Q_1	1	2	3	4
1	3	1	4	2
2	2	4	1	3
3	1	2	3	4
4	4	3	2	1

Q_2	1	2	3	4
1	2	4	1	3
2	4	3	2	1
3	1	2	3	4
4	2	4	1	3

Q_1 and Q_2 are isotopic and the isotopy is determined by the permutations $\eta = (1\ 3)(2\ 4)$ $\varrho = (1\ 4\ 3)$ and $\sigma = (1\ 4)$ respectively. η respresents an interchange of columns, ϱ represents an interchange of rows and σ represents a renaming of the elements.

The group-isotopic quasigroups are also called *linear quasigroups* (see [6]).

Other important types of quasigroups can be characterized as follows:

A quasigroup Q is *distributive*, if for $x, y, z \in Q$ the relations $x \,.\, yz = xy \,.\, xz$, $yz \,.\, x = yx \,.\, zx$ hold.

A quasigroup Q is *medial*, if for $x, y, u, v \in Q$ the equality $xy \,.\, uv = xu \,.\, yv$ holds.

Q is a *Stein quasigroup*, if for any two elements $x, y \in Q$ the identity $x.xy = yx$ holds.

Q is called a *Moufang-loop*, if for any three elements $x, y, z \in Q$ the identity $x(yz \,.\, x) = xy \,.\, zx$ holds.

For a detailed description of the above types of quasigroups see e.g. the paper of V. D. Belousov [6].

The concept of the *subquasigroup* can be defined analogously to that of the sub-Latin square. Let square matrix

$$A = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \vdots & & \\ a_{n1} & \dots & a_{nn} \end{vmatrix}$$

be a Latin square. If the square matrix

$$B = \begin{vmatrix} a_{ij} & a_{ik} & \dots & a_{ir} \\ a_{lj} & a_{lk} & \dots & a_{lr} \\ \vdots & & & \\ a_{pj} & a_{pk} & \dots & a_{pr} \end{vmatrix}$$

$(1 \leqq i, j, k, l, p, r, \leqq n)$ is a Latin square, then B is called the *sub-Latin square* of A. The Latin square belonging to the Cayley table of the subquasigroup Q' of any quasigroup Q is a sub-Latin square of the Latin square belonging to the Cayley table of Q. Any sub-Latin square of the Latin square belonging to the Cayley table of a quasigroup Q becomes, when bordered appropriately, the Cayley table of a subquasigroup of a quasigroup isotopic to Q. (The reason for its being not the same as but only isotopic to Q is that the bordering elements contained in the rows and columns defining the sub-Latin square may be different from those of the sub-Latin square.)

In the following diagram the Cayley table of a quasigroup of order 10 is shown which has a subquasigroup of order 4 (consisting of the elements 1, 2, 3, 4) and also one of order 5 (with elements 3, 4, 5, 6, 7) the intersection of which is a subquasigroup of order 2 (with elements 3, 4).

	0	8	9	1	2	3	4	5	6	7
5	1	9	2	8	0	6	7	4	5	3
6	8	2	1	0	9	7	5	3	4	6
7	2	1	0	9	8	5	6	7	3	4
3	0	8	9	1	2	3	4	6	7	5
4	9	0	8	2	1	4	3	5	6	7
1	5	6	7	3	4	1	2	0	8	9
2	6	7	5	4	3	2	1	8	9	0
0	7	4	3	5	6	0	9	1	2	8
8	3	5	4	6	7	8	0	9	1	2
9	4	3	6	7	5	9	8	2	0	1

The sub-Latin squares can be used for the characterization of non-simple groups. A group G is *non-simple* if, and only if, there exists a non-trivial normal subgroup N of G. Let A_0 be the Latin square belonging to the Cayley table of the group N or any group isomorphic to N, and let $A_1, A_2, \dots, A_{k-1}$ be the Latin squares belonging to the cosets $L_1, L_2, \dots, L_{k-1}$ of N in G. It follows directly from the properties of the normal subgroup that the square matrices $A_1, A_2, \dots, A_{k-1}$ are Latin squares belonging to Cayley tables. The Latin square belonging to the Cayley table of G is formed by the union of the Latin squares $A_0, A_1, \dots, A_{k-1}$ i.e. the Latin square belonging to the Cayley table of G contains the Latin squares $A_0, A_1, \dots, A_{k-1}$ as sub-Latin squares.

If the sub-Latin squares $A_0, A_1, \dots, A_{k-1}$ in the Cayley table are replaced successively by the elements $a_0, a_1, \dots, a_{k-1}$, we obtain the Cayley table

of a group which is isomorphic to the factor-group of G mod N (see [4]; the same construction is used in [37] in connection with the generalization of the Jordan-Hölder theorem).

The property mentioned above was utilized by H. Zassenhaus to characterize the normal Cayley tables of non-simple groups (see [43]).

Latin squares of order n are easy to construct if, the rows are taken to be the cyclic permutations of the elements 1, 2, ..., n (see [31]). For $n = 4$, we have the Latin square of the form

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

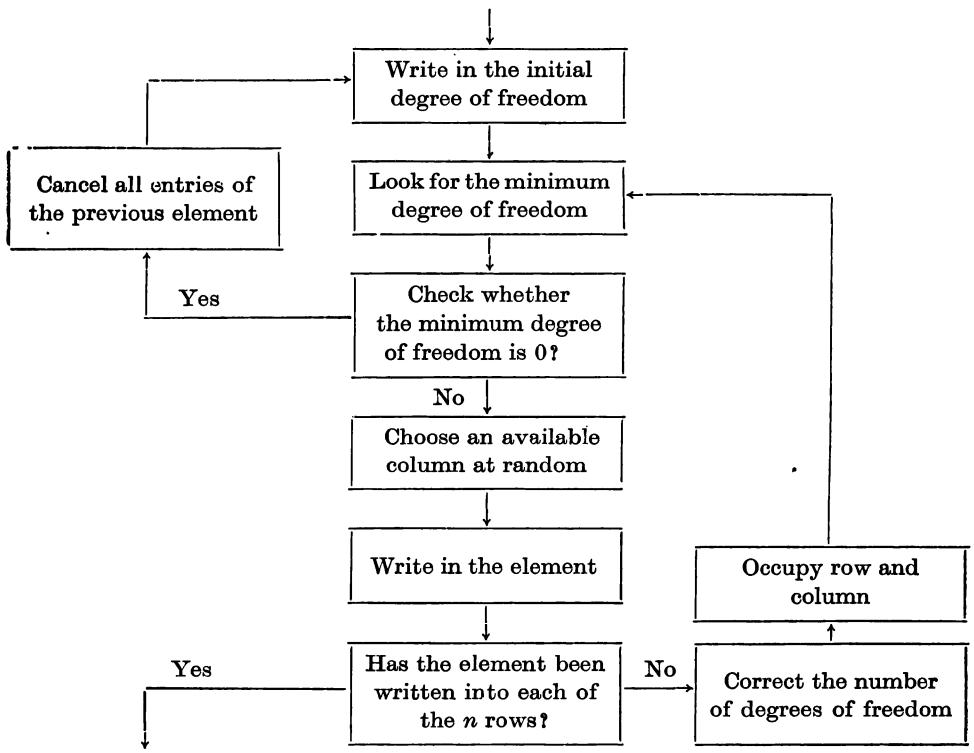
If this Latin square is bordered by its own first row and first column, we obtain the Cayley table of the cyclic group of order 4.

If one does not require this special Latin square, but wants to choose at random one out of all the possible Latin squares of order n, this can be conveniently done by means of a computer.

A practical way of constructing the Latin squares of order n, defined on the numbers 1, 2, ..., n is first to write in n 1's, in accordance with the properties of the Latin square, but otherwise arbitrarily; then to write in n 2's in a similar way into the remaining free places; and so on. On applying this procedure, it may happen that after a few steps the next element cannot be written in. In this case, it is generally sufficient to change the positions of the last element which was entered, or to start a new sequence without making any changes in the placing of the elements which have already been entered.

The above procedure can easily be programmed for a digital computer. The following flow-chart illustrates the essential part of the programme, that is, the method by which the successive elements are written in. Essentially, the procedure is the following. If one of the elements has not yet been written into all of the n rows, one can make correspond to each of the rows which do not contain this element certain degrees of freedom, expressed in terms of the number of entries in that row into which the element in question can be written in. As one can observe by taking a glance at the flow-chart at the begining of the procedure the degree of freedom is prescribed by the program. If out of n elements $n - k$ have been already written in, this is obviously k. Then, the computer is programmed to search for the rows whit the minimum degree of freedom. If several rows have the same degree of freedom, it simply selects the first one. The element in question is then written into any one of the available places in that row chosen at random. After the new element has been written in, the number

of the degrees of freedom for each row has to be recalculated accordingly. If the degree of freedom of a row becomes 0, i.e. no more entries are available, it is sufficient to change positions of the previous element. Practical experience has shown that with this procedure, in almost every case, the second trial proves to be successful (see [29]).



The procedure has been programmed and run on a Siemens 2002 computer [29]. The program contains 300 instructions and the running of the program takes only a few minutes. It is of interest to note that the element last written in has seldom to be cancelled. This happens usually only if two thirds of the square have been already completed. This fact presents an interesting empirical result in connection with the theory of truncated Latin squares to be discussed in Chapter III of this paper.

The use of computers for the construction of Latin squares is discussed by the author in detail also in [13].

II. SPECIAL TYPES OF LATIN SQUARES

Let M be a non-empty, finite subset of the natural nubers $1, 2, \ldots, n$ and let T_1 be a Latin square whose elements are the elements of this subset. Then the set M forms a quasigroup with respect to the operation 1 defined on it by means of the multiplication table which comprises T_1 bordered by its own first row and column.

Denote by Ω_n the set of all quasigroups defined on the set M by mears of such Latin squares T_1.

Ω_n is called *globally associative*, if any operations 1 and 2 with $(M)_1, (M)_2 \in \in \Omega_n$ can be associated with operations 1* and 2* where $(M)_{1^*}, (M)_{2^*} \in \Omega_n$ such that for any elements x, y, z of M, we find

$$x1(y2z) = (x1^*y)2^*z.$$

It was shown by R. Schauffler [34] that Ω_n is globally associative if and only if $n \leqq 3$.

A subset Φ_n of Ω_n is called an *associative system*, if any operations 1 and 2, where $(M)_1\,(M)_2 \in \Phi_n$ can be associated with operations 1* and 2*, where $(M)_{1^*}(M)_{2^*} \in \Phi_n$ such that for any elements x, y, z of M we have

$$x1(y2z) = (x1^*y)2^*z$$

A theorem of V. D. Belousov states that the quasigroups of any associative system are isotopic quasigroups all of which are isotopic to one and the same group.(1)(2)

As regards the use of R. Schauffler's theorem in algebraic information theory see [35].

A class of Latin squares having an interesting property which had not previously been investigated was found by B. Gordon when he was trying to solve the following problem (see [24]).(3)

When is it possible to arrange the elements of a finite group of order n into a sequence $a_1, a_2, \ldots, a_n$ such that each of the products $a_1, a_1a_2, a_1a_2a_3, \ldots,$

(1) The theorem was not proved in [5]. The proof was given by M. Hosszu in [28]. A statement similar to that of V. D. Belousov is to be found also in the paper of R. H. Bruck [8].

(2) In [10] the authors give the proof of R. Schauffler's statement by using V. D. Belousov s theorem. The rephrased theorem of R. Schauffler is there erroneously quoted as implying that it is sufficient if the elements of Ω_n are group-isotopic. Although element of Ω_4 is group-isotopic [36]; nevertheless, because of the existence of two non-isomorphic groups of order 4, the requirement of the V. D. Belousov theorem cannot be fulfilled. If $n > 4$, Ω_n cannot consist of group-isotopic quasigroups (see [36]).

(3) It was the investigation of Latin squares that led the author to the formulation in terms of group theory.

$a_1a_2 \ldots a_n$ is different from all the others? Any group with this property is called by B. Gordon *sequenceable.*

It was shown by B. Gordon [24] that a finite Abelian group is sequenceable if and only if it is a direct product of two groups A and B, such that A is a cyclic group of order 2^k ($k > 0$) and B is of odd order.

Much later than the publication of [24] E. N. Gilbert [23] obtained a special case of B. Gordon's theorem when G is a cyclic group (see also [31]).

The Latin squares belonging to the Cayley tables of sequenceable groups are important from the practical point of view.

A Latin square with elements 1, 2, ..., n is called *horizontally complete* if for any ordered pair (α, β) $(1 \leqq \alpha, \beta \leqq n; \alpha \neq \beta)$ there exists a row of the Latin square, in which α and β appear as adjacent elements; that is, if $C_{s,t}$ denotes the element at the intersection of the s-th row and t-th column of the Latin square, there exist integers s and t such that

$$C_{s,t} = \alpha; \quad C_{s,t+1} = \beta.$$

Similarly, a Latin square is *vertically complete*, if for any α and β there exist integers u and v, such that

$$C_{u,v} = \alpha; \quad C_{u+1,v} = \beta.$$

The Latin squares that are both horizontally and vertically complete are called *complete Latin squares.*

It was shown by B. Gordon that if the group G consisting of elements $a_1, a_2, \ldots, a_n$ is sequenceable, i.e. all the elements $a_1, = b_1$, $a_1a_2 = b_2, \ldots,$ $a_1a_2 \ldots a_n = b_n$ are distinct, then the matrix determined by $(c_{s,t}) = (b_s^{-1}b_t)$ is a complete Latin square. It follows obviously from the group axioms that for $s \neq s'$ and $t \neq t'$ we have $b_s^{-1}b_t \neq b_{s'}^{-1}b_t$, and $b_s^{-1}b_t \neq b_s^{-1}b_{t'}$, and so the matrix is a Latin square. Thus only the completeness has to be proved. It has to be proved that for any distinct α and β, it is possible to determine s and t such that

$$b_s^{-1}b_t = \alpha; \quad b_s^{-1}b_{t+1} = \beta.$$

(It can be proved similarly that the Latin square is also vertically complete.) By the definition of b_t and b_{t+1}

$$\alpha a_{t+1} = \beta.$$

By this equation t is uniquely determined ($t > 0$, since, the unit element of the group G is necessarily a_1, it would follow from $\alpha a_1 = \beta$ that $\alpha = \beta$). When, t has been determined, s is uniquely defined by the equation

$$b_s^{-1}b_t = \alpha.$$

An example of a complete Latin square of order 4 is

1	2	3	4
2	4	1	3
3	1	4	2
4	3	2	1

The study of sequenceable groups has started quite recently and presents therefore many unsolved problems. Some of them have been pointed out by B. Gordon (see [24]) such as:

(i) Is there any complete Latin square of odd order?(4)

(ii) What is the necessary and sufficient condition that a non-commutative group be sequenceable?

In order to formulate the following problem, we are going to use the notion of the diagonal. This is defined as follows: In a Latin square of order n a *diagonal* comprises as n distinct elements contained in distinct rows and columns of the Latin square.

The notion was introduced originally under the name of „complete mapping" by L. J. Paige (see [30]). The same notion was called later by S. Singer [38] 1 — 1 permutation. The name diagonal, first used by the author in [10], has been adopted because of the arrangement of the elements contained in a diagonal.(5)

Let us return to the sequenceable groups. A further problem pointed out by B. Gordon reads: Is it true that the existence of the diagonal in the Cayley table of a group G and the fact that G is sequenceable are mutually exclusive properties?

This question of B. Gordon is justified by of his theorem that the finite Abelian groups can be classified into two classes, namely sequenceable groups and groups with a diagonal. In fact, it had already been proved earlier by M. Hall [26] that, except when a finite Abelian group contains exactly one element of order 2, there will always be a diagonal in the Latin square belonging to its Cayley table. In the contrary case, the group is sequenceable by Gordon's theorem. It is mentioned also by B. Gordon that the results obtained for finite Abelian groups imply the conjecture that a finite group is sequenceable if and only if it has no diagonal in its Cayley table. This conjecture is however contradicted by the fact that the symmetric group of degree 3 is neither sequenceable nor contains a diagonal in its Cayley table. Thus the question can only be formulated as above. Since recently Mendelsohn

(4) This problem was solved after this paper had been written by N. S. Mendelsohn who constructed a complete Latin square of order 21.

(5) The same notion was called transversal in [44].

proved, that there exist sequenceable groups of order 21. Gordon's conjecture is disproved by the existence of such group.

P. Bateman [2] proved the existence of a diagonal in the Latin square belonging to Cayley table of arbitrary infinite group.

M. Hall and L. J. Paige [27], who investigated the problem for arbitrary finite groups, proved that for solvable groups the necessary and sufficient and for groups of even order the necessary condition for the existence of a diagonal in the Cayley table is that the 2-Sylow subgroup should be non-cyclic.(6)

M. Hall and L. J. Paige conjectured that the condition is also sufficient for unsolvable groups.

Latin squares which posses a diagonal can be characterized not only in terms of the 2-Sylow subgroups but also in terms of the representability of their unit element as a product containing exactly once as a factor each element of the group whose Cayley table defines the Latin square. If the Cayley table of the group contains a diagonal, the unit element of the group can always be obtained in the form of a product which contains each element of the group exactly once as a factor. The converse statement is not generally true.

It is easy to see that in a Cayley table of a group of order n the existence of n disjoint diagonals follows from the existence of a single diagonal, i.e. the maximal number of disjoint diagonals in the Cayley table of any group of order n is either n or 0. In fact, if there exists a diagonal formed by taking a_1 from the first, ..., a_n from the n-th row, then a_1x from the first, ..., a_nx from the n-th row (where x is an arbitrary element of the group), it follows immediately from the group axioms that each of these elements is distinct and each located in a different column, then it is evident that if x varies over the n elements of the group, we have n disjoint diagonals. It does not follow, however, from the fact that a Latin square having n disjoint diagonals that it is also a multiplication table of a group. An example of a Latin square of order n with n diagonals that is not a multiplication table of a group is given e.g. in [10], this Latin square was constructed by E. T. Parker. There exist several other examples those of A. L. Ljamzin, A. D. Keedwell, H. B. Mann and other authors.

It is still an open question, raised in [10], whether each Latin square having no diagonal belongs to a group-isotopic quasigroup.

The method of construction of Latin squares utilizing the diagonals, described in [10], made it possible to prove the following theorems.

There exists for any n ($n \geqq 4$) a Latin square of order n which contains

(6) For the groups with a cyclic 2-Sylow subgroup there is given in [12] a simple characterization by means of a regular permutation group which is isomorphic to the group in question. The regular permutation group P of order n, which is ismorphic to the finite group G of order n, will contain an odd permutation if and only if the 2-Sylow subgroup of G is cyclic.

a sub-Latin square of order 2. Or, more generally(7) there exists for any n, a Latin square of order n which contains a sub-Latin square of order k if $k \leqq \left[\frac{n}{2}\right]$.

The same method of construction utilizing the diagonals of Latin squares (so called prolongotion see [46]), is used again in [10] to disprove the following conjecture of D. W. Wall.

D. W. Wall's conjecture is that for any quasigroup Q of order n which contains m disjoint sub-quasigroups of order s, we have

$$n \geqq (m + 1)s.$$

The relation was proved by D. W. Wall for $m = 2$ with the conjecture that it holds for any m (see [41]).

Using the method for construction, mentioned above, it can also be proved that for $m > 2$ there exists a Latin square which is the union of m disjoint sub-Latin squares of arbitrary but equal order (see [10]).

It is important for this construction to have practical methods for finding the diagonals. Two such methods can be simply formulated from two properties of the Cayley tables of groups of odd order.

a) In a group of odd order two different elements cannot have equal squares. It follows that, if a_i $(i = 1, 2, \ldots n)$ is an element of a group of an odd order n, then $a_i \,.\, a_i = a_i^2$ forms a diagonal, where $i = 1, 2, \ldots, n$.

b) It was proved by K. Fenchel [19] that the order of a finite group G is an odd number if and only if the group contains for any $x \in G$, $k \in G$ a unique element $a \in G$ such that $k = axa$ holds. Consequently, if k runs through all elements of the group G with fixed $x \in G$ we find a diagonal of the form $ka^{-1} = = ax$.

The diagonals of Latin squares play an important part in the construction of orthogonal pairs of Latin squares, as will be shown in the Chapter dealing with the latter.

III. TRUNCATED LATIN SQUARES

Latin squares from which certain elements have been deleted are called *truncated Latin squares* (see [11]).

A *Latin rectangle* is a matrix of n rows and r columns in which no row and no column contains any element more than once.

---

(7) The identical theorem was proved by T. Evans in [18] mentioning that the same result was obtained also by S. K. Stein by a different method.

The relationship between truncated Latin squares and Latin rectangles is given by the theorem published in the book of H. J. Ryser [33] according to which any Latin rectangle of size $n \times r$, containing n elements can be completed to a Latin square of order n. No reference is made in Ryser's book to the fact that the theorem originates from M. Hall [25]. Further results concerning Latin rectangles are to be found in the paper of T. Evans [18].

L. Fuchs raised the following problems in connection with truncated Latin squares in his book [22].

Delete any k elements in the Cayley table of a finite group G of order n. Determine the maximum number $k = k(n)$ for which

a. the rest of the table determines G up to isomorphism;

b. the Cayley table is uniquely determined by the rest of the table.

The problem of L. Fuchs concerning the unique determination of the Cayley table was solved by the author (see [9]). The solution of the much simpler analogous problem for the case of quasigroups is to be found in [10]. The following two theorems have been proved.

The maximum number of arbitrary elements which can be deleted from a Cayley table of a group of order $n (n \neq 4)$ so that the remaining array of elements shall always determine the table uniquely is $2n - 1$. If $n = 4$ the largest number of elements which can be omitted is 3 (see [9]).

At most 3 elements can be deleted from an arbitrary chosen Latin square of order n $(n \neq 3, n > 1)$ if it is required to ensure that, whatever square was chosen, it shall always be possible to reconstruct the complete square uniquely from the remaining array of elements. For the case $n = 3$, the corresponding number of elements is 5 (see [10]).

The condition under which a Latin rectangle of size $r \times s$ can be completed to a Latin square of order n has been stated by H. J. Ryser [32], as follows: Let us denote by $N(i)$ the number of times that the integer i occurs in the Latin rectangle. Then the Latin rectangle of size $r \times s$ can be completed to a Latin square of order n if and only if the inequality $N(i) \geqq r + s - n$ holds, where $i = 1,2, \ldots, n$.

Making use of J. Ryser's theorem T. Evans [18] proved that for any n a Latin square of order n can be extended to a Latin square of order t, if $t \geqq 2n$.

The same result was obtained independently by S. K. Stein.

The same theorem can be found in [10] where the proof, as mentioned already in this paper, is formulated in terms of the diagonals of a Latin square.

T. Evans has proved that any infinite quasigroup with unit element having a finite number of generators and generating relations, has also a homomorphic image of finite order t $(t \geqq k)$ where k is a positive integer determined by the generators and the generating relations (see [16], [17]).

The notion of factorisation of a group is well known. The group G is said to be *factorisable* if it can be represented as the product of its proper subgroups A and B, that is if $G = AB$.

The definition of factorisation can be extended if one does not require that A and B should be subgroups, but only that they should be proper subsets of G. In the latter case, the group is said to be factorisable into complexes.

It is easy to show that any group of composite order can be factorised into complexes. That is, if the order of a group is a composite number n, the group G has a proper subgroup L. Let L' be an arbitrary coset of L in G and let R be a complete set of coset representatives mod L, then $G = L'R$.

Let us now apply the concept of factorisability into complexes to the Cayley tables of groups of composite order.

A Latin rectangle of size $k \times l$ where $k \times l = n$, is called *complete*, if it contains n distinct elements.

A Cayley table of composite order can be constructed as a union of complete Latin rectangles. This statement is, in fact, the interpretation in terms of combinatorics of the equality $G = L'R$ formulated above.

As an example see the following factorisation of the Latin square belonging to the Cayley table of a dihedral group of order 6 into complete Latin rectangles:

1	2	3	4	5	6
4	5	6	1	2	3
2	3	1	5	6	4
5	6	4	2	3	1
3	1	2	6	4	5
6	4	5	3	1	2

Since similar considerations hold also for quasigroups (see [41]), the above factorisation of Latin squares into complete Latin rectangles is not restricted to the case when the Latin square in question is a Cayley table of a group.

As regards the factorisation of a group into complexes there is an important theorem of A. Wagner [40] which reads as follows. Let K be an arbitrary subset of a group G of order n which contains at least $[\frac{1}{2}n + 1]$ elements. Then $K^2 = G$.

It follows from A. Wagner's theorem that in the Cayley table of a group of order n any sub-Latin rectangle which has at least $[\frac{1}{2}n + 1]$ rows and columns necessarily contains every element of the group.

Let S_n be a Latin square of arbitrary order n. A row and column of S_n are called *corresponding* if they intersect on the main diagonal starting from the left lower corner of the Latin square. The principal minor T_c of S_n is obtained by deleting $n - c$ arbitrary rows and corresponding columns in the Latin square S_n.

Denote by $k_{i_1,i_2,\ldots,i_Q}$ (where $i_1, i_2, \ldots, i_Q \in \{1,2,\ldots,n\}$ and the i_r are all different) the number of columns all of which contain the entire set of elements $a_{i_1}, a_{i_2}, \ldots, a_{i_q}$ and denote by $k^{(q)}$ the minimum of $k_{i_1},\ldots,k_{i_q}$; P. Erdős and G. Ginzburg [14] investigated the problem of finding the minimum c corresponding to given values n and $k^{(q)}$ for which there exists in an arbitrary S_n at least one T_c with the prescribed $k^{(q)}$. This minimum c was denoted by b.

It follows directly from the definition that $\binom{b}{q} \cdot b \geqq k^{(q)} \cdot \binom{n}{q}$ and assuming the main diagonal consists entirely 1's, the above inequality improves to

$$\binom{b-1}{q} b \geqq k^{(q)} \binom{n-1}{q}.$$

The theorem of P. Erdős and G. Ginzburg gives an upper bound for b if $k^{(q)} = 1$. These authors proved that in a Latin square of order n there exists a principal minor of order greater than $cn^{\frac{q}{q+1}} (\log n)^{\frac{1}{q+1}}$ (where c is a sufficiently large absolute constant) such that one of its columns contains the elements $i_1, i_2, \ldots, i_Q$ (where $i_1, i_2, \ldots, i_Q \in \{1,2,\ldots,n\}$ and the i_r are all different) and pointed out in [14] the following problems arising in connection with this statement:

1. To find bounds for b in the case when $k^{(q)} > 1$.

2. Given three positive integers n, $k^{(q)}$, d, what is the value of minimal c such that from an arbitrary S_n at least one T_c can be obtained with

$$\max \{k_{i_1,i_2,\ldots,i_Q}\} - k^{(q)} \leqq d.$$

3. Given an arbitrary S_n, what is the appropriate value of c for the maximal minor (not necessarily principal) in which all elements are different.

The author wishes to acknowledge with thanks the valuable criticism of Dr. A. D. Keedwell who read the manuscript and made comments on it from mathematical and linguistic points of view. The author expresses hereby his gratitude to Dr. A. Rosa who carefully went through the manuscript and offered some comments on the content and its presentation.

REFERENCES

[1] Aczél J., Belousov V. D., Hosszu M., *Generalized associativity and bisymmetry on quasigroups*, Acta Math. Acad. Scient. Hung. *11* (1960), 127—136.

[2] Bateman P., *Complete mappings of infinite groups*, Amer. Math. Monthly *57* (1950), 623—624.

[3] Barra J. R., Guerin R., *Extension des carres grécolatins cycliques*, Publs. Inst. Statist. Univ. Paris *12* (1963), 67—82.

[4] Baumgartner L., *Gruppentheorie*, Berlin 1921.

[5] Белоусов В. Д., *Ассоциативные системы квазигрупп*, У. М. Н. *13* (1958), вып. 3, 243.
[6] Белоусов В. Д., *Системы квазигрупп с обобщенными тождествами*, У. М. Н. *20* (1965), 75—146.
[7] Brandt H., *Über eine Verallgemeinerung des Gruppenbegriffs*, Math. Ann. *96* (1926), 360—366.
[8] Bruck R. H., *Some results in the theory of quasigroups*, Trans. Amer. Math. Soc. *56* (1944), 19—52.
[9] Dénes J., *On a problem of L. Fuchs*, Acta Scient. Math. *23* (1962), 237—241.
[10] Dénes J., Pásztor E., *A kvázicsoportok néhány problémájáról*, Magyar Tud. Akad. Mat. Oszt. közl. *13* (1963), 109—118.
[11] Dénes J., *Megjegyzések a véges csoportok elméletéhez*, Thesis 1961.
[12] Dénes J., *On some properties of commutator subgroups*, Ann. Univ. Scient. Budapest. Sec. Math. *7* (1964), 123—127.
[13] Dénes J., *Az elektronikus számológépek néhány nem szokványos felhasználása*, Gépek és programok *3* (1962), 17—54.
[14] Erdös P., Ginzburg A., *Combinatorial problem in Latin squares*, MTA Mat. Kut. Int. Közl. *8* (1963), 407—411.
[15] Evans T., *A note on the associative law*, J. London Math. Soc. *25* (1950), 196—201.
[16] Evans T., *The word problem for abstract algebra*, J. London Math. Soc. *26* (1951), 66—71.
[17] Evans T., *On multiplicative systems defined by generators and relations I.*, Proc. Cambridge Philos. Soc. *3* (1951) 637—649.
[18] Evans T., *Embedding incomplete Latin squares*, Amer. Math. monthly *67* (1960), 958—961.
[19] Fenchel K., *Eine Bemerkung über Gruppen ungerader Ordnung*, Math. Scand. *10* (1962), 182—188.
[20] Fog D., *Gruppentafeln und abstrakte Gruppentheorie*, Scand. Matematiker Kongressen i Stockholm 1934, 376—384.
[21] Frolov M., *Recherches sur les permutations carrées*, J. Math. Spec. *4* (1890), 111.
[22] Fuchs L., *Abelian groups*, Publishing House of the Hungarian Academy of Sci., Budapest 1958.
[23] Gilbert E. N., *Latin squares which contain no repeated diagram*, SIAM Rev. *7* (1965), 189—198.
[24] Gordon B., *Sequences in groups with distinct partial products*, Pacif. J. Math. *11* (1961), 1309—1313.
[25] Hall M., *An existence theorem for Latin squares*, Bull. Amer. Math. Soc. *51* (1945), 387—388.
[26] Hall M., *A combinatorial problem on Abelian groups*, Proc. Amer. Math. Soc. *3* (1952), 584—587.
[27] Hall M., Paige L. J., *Complete mappings of finite groups*, Pacif. J. Math. *5* (1955), 541—549.
[28] Hosszu M., *Belouszov egy tételéről és annak néhány alkalmazásáról*, MTA Mat. Oszt. Közl. *9* (1959), 51—56.
[29] Lockemann von W., *Ein Rechenprogramm zur Erzeugung von lateinischen Quadraten*, Elektr. Rechenanlagen *2* (1960), 129—130.
[30] Paige L. J., *Complete mappings of finite groups*, Pacific J. Math. *1* (1951), 111—115.
[31] Rényi A., *Uj módszerek és eredmények a kombinatórikus analizisben I.*, Magyar Tud. Akad. Mat. Oszt. közl. *16* (1966), 79—105.

[32] Ryser H. J., *A combinatorial theorem with an application to Latin rectangles*, Proc. Amer. Math. Soc. *2* (1951), 550—552.
[33] Ryser H. J., *Combinatorial mathematics*, John Willey and Sons Inc., New York 1963.
[34] Schauffler R., *Die Assoziativität im Ganzen, besonders bei Quasigruppen*, Math. Z. *67* (1957), 428—435.
[35] Schauffler R., *Über die Bildung von Codewörten*, Arch. Elektr. Übertrag. *10* (1956), 303—314.
[36] Schönhardt E., *Über lateinische Quadrate und Unionen*, J. Reine und Angew. Math *163* (1930), 183—229.
[37] Singer I., *A class of groups associated with Latin squares*, Amer. Math. Monthly *67* (1960), 235—240.
[38] Speiser A., *Theorie der Gruppen von endlicher Ordnung*, Berlin 1927.
[39] Šik F., *Sur les décompositions créatrices sur les quasigroupes finis*, Spisy vyd. Přírodověd. fak. Masarykovy Univ. *329* (1951), 169—186.
[40] Wagner A., *On the associative law of groups*, Rend. Mat. e Appl. *21* (1962), 60—76.
[41] Wall D. W., *Sub-quasigroups of finite quasigroups*, Pacif. J. Math. *7* (1957), 1711—1714.
[42] Wielandt H., *Arithmetical and normal structure of finite groups*, Proc. Symp. Pure Math. *6* (1962), 17—38.
[43] Zassenhaus H., *The theory of groups*, New York 1958.
[44] Dulmage A. L., Johnson D., Mendelsohn N. S., *Orthogonal Latin Squares*, Canad. Math. Bull. *2* (1959), 211—216.
[45] Albert A. A., *Quasigroups I*, Trans. Amer. Math. Soc. *54* (1943), 507—519.
[46] Белоусов В. Д., *Основы теории квазигрупп и луп*, Москва 1967.

Received November 28, 1966.

Magyar Tudományos Akadémia
Központi Fizikai Kutató Intézete,
Budapest, Hungary