# FINITE NETS, I. NUMERICAL INVARIANTS

R. H. BRUCK

**Introduction.** A finite net $N$ of degree $k$, order $n$, is a geometrical object of which the precise definition will be given in §**1**. The geometrical language of the paper proves convenient, but other terminologies are perhaps more familiar. A finite affine (or Euclidean) plane with $n$ points on each line ($n \geqslant 2$) is simply a net of degree $n + 1$, order $n$ (Marshall Hall [1]). A loop of order $n$ is essentially a net of degree 3, order $n$ (Baer [1], Bates [1]). More generally, for $3 \leqslant k \leqslant n + 1$, a set of $k - 2$ mutually orthogonal $n \times n$ latin squares may be used to define a net of degree $k$, order $n$ (and conversely) by paralleling Bose's correspondence (Bose [1]) between affine planes and complete sets of orthogonal latin squares.

In the language of latin squares, the problem (explained in §**1**) of imbedding a net of $N$ of degree $k$, order $n$ in a net $N'$ of degree $k + 1$, order $n$ becomes the problem of finding an $n \times n$ latin square orthogonal to each of $k - 2$ given mutually orthogonal $n \times n$ latin squares. Similarly, adjunction of a line corresponds to the determination of a common "transversal" (in the terminology of Euler [1]) to the $k-2$ orthogonal squares. Further details of a historical nature will be found in the bibliography.

On each finite net $N$ we define an integer $\phi(N)$, which may be regarded as an invariant in several ways. A necessary condition that a line can be adjoined to $N$ is that $\phi(N) = 1$. (A necessary and sufficient condition is given in Theorem 1 (i).) We define a direct product $N_1 \times N_2$ of nets $N_i$ of the same degree and study the relation between $\phi(N_1 \times N_2)$ and the $\phi(N_i)$ (Theorem 4). From these considerations we deduce the existence of nets of every order $n$ to which no line can be adjoined (Theorem 5). Next we study the relation between the $\phi$'s of homomorphic nets (Theorem 6) and we conclude the paper with an explicit evaluation of $\phi$ for nets of degree 3 (Theorem 7).

**1. Nets and the imbedding problem.** Let $k$, $n$ be positive integers, with $k \geqslant 3$. A (finite) *net* $N$ of degree $k$, order $n$, is a system of undefined objects called "points" and "lines" together with an incidence relationship ("point is on line" or "line passes through point") such that: (i) $N$ contains $k$ (non-empty) classes of lines. (ii) Two lines $a$, $b$ of $N$, belonging to distinct classes, have a unique common point $P$. (iii) Each point $P$ of $N$ is on exactly one line of each class. (iv) Some line of $N$ has exactly $n$ distinct points. It is easy to show that every line of $N$ has exactly $n$ distinct points, that every class of lines contains exactly $n$ distinct lines and that $N$ consists of $n^2$ distinct points, $kn$ distinct lines. Moreover, either $n = 1$ or $n \geqslant k - 1$.

Received October 8, 1949.



https://doi.org/10.4153/CJM-1951-012-7 Published online by Cambridge University Press

If $S$ is a subset of the points of the net $N$ (of degree $k$, order $n$) such that each line of $N$ contains exactly one point of $S$, we shall say that *$S$ can be adjoined as a line to $N$.* Considering the $n$ lines of each class, we see that $S$ must consist of exactly $n$ distinct points, no two collinear. If the $n^2$ points of $N$ can be partitioned into $n$ disjoint sets $S_1, \ldots, S_n$, each of which can be adjoined as a line to $N$, then the $S_j$ may be regarded as constituting the $n$ lines of an additional class. In this way $N$ can be *imbedded* in a net $N'$ of degree $k+1$, order $n$, consisting of the points and lines of $N$ (with the same incidence relations) plus one additional class of "parallels". Conversely, if the net $N$ of order $n$, degree $k$ is a subnet of net $N'$ of order $n$, degree $k+1$ (a subnet in the sense that a point and line of $N$ are incident in $N$ if and only if they are incident in $N'$) then $N$, $N'$ must have the same points, and one of the line-classes of $N'$ may be regarded as consisting of $n$ disjoint point-sets $S_j$, each of which can be adjoined as a line to $N$. The present paper will be concerned primarily with *necessary* conditions that a line may be adjoined to a net.

**2. The integers represented by a net.** Let $N$ be a finite net and let $f$ be a single-valued function from the points of $N$ to the rational integers. We shall say that the rational integer $m$ is *represented on $N$ by $f$* if $f$ sums to $m$ over the points of each line of $N$, and *represented positively* if, in addition, $f$ takes on only non-negative values. Again, if $u$ is a positive integer, we shall say that $m$ is *represented* mod $u$ *on $N$ by $f$* if $f$ sums to $m$ mod $u$ on each line of $N$. The least positive integer represented on $N$ will be denoted by $\phi(N)$. Clearly $\phi(N)$ is an invariant of $N$. Moreover, $\phi(N)$ is the (positive) greatest common divisor of the integers represented on $N$.

THEOREM 1. *Let $N$ be a finite net of degree $k$, order $n$. Then*: (i) *A necessary and sufficient condition that a line can be adjoined to $N$ is that* 1 *be positively represented on $N$.* (ii) *$n$ is positively represented on $N$.* (iii) *$k-1$ is represented on $N$.* (iv) $\phi(N)|(n, k-1)$. (v) *If $n$ is an affine plane (i.e., if $k = n+1$,)* $\phi(N) = n$. (vi) *With at most a finite number of exceptions, every positive integer divisible by $\phi(N)$ is positively represented on $N$.*

COROLLARY. *A necessary condition that a line can be adjoined to $N$ is that* $\phi(N) = 1$.

*Proof.* (i) If $S$ can be adjoined as a line to $N$, define $f(P) = 1$ or $0$ according as $P$ is or is not in $S$. Then 1 is positively represented on $N$ by $f$. Conversely, if 1 is positively represented on $N$ by some $f$, let $S$ be the set of points $P$ for which $f(P) \neq 0$. Then each line of $N$ contains exactly one point $P$ of $S$ (and, incidentally, $f(P) = 1$.) Hence $S$ can be adjoined to $N$ as a line.

(ii) If $f'(P) = 1$ for every point $P$ of $N$, then $f'$ represents $n$ positively on $N$.

(iii) Select an arbitrary point $C$ of $N$ and define $h$ as follows: $h(C) = k-n$; $h(P) = 1$ if $P$ is distinct from but collinear with $C$; $h(P) = 0$ otherwise. If $a$ is a line through $C$, $h$ sums, over $a$, to $k-n+n-1 = k-1$. If $a$ is a line not through $C$, the $k-1$ lines through $C$ which are not in the same class as

https://doi.org/10.4153/CJM-1951-012-7 Published online by Cambridge University Press

$a$ meet $a$ in $k - 1$ distinct points; hence $h$ sums to $k - 1$ over $a$ in this case also. Therefore $h$ represents $k - 1$ on $N$.

(iv) By (ii) and (iii), $\phi(N)$ divides $n$, $k - 1$ and their greatest common divisor $(n, k - 1)$.

(v) Let $\phi(N)$ be represented by $f$ on the affine plane $N$, and let $s$ be the sum of $f$ over the $n^2$ points of $N$. Considering the sum of the sums of $f$ over the $n$ lines of some class, we find $n\phi(N) = s$. On the other hand, if $C$ is a point of $N$, every point of $N$ (other than $C$) lies on exactly one of the $n + 1$ lines through $C$. Considering the sum of the sums over the $n + 1$ lines through $C$, we find $nf(C) + s = (n+1)\phi(N)$. Since $s = n\phi(N)$, $nf(C) = \phi(N)$. Therefore $n|\phi(N)|n$, so $\phi(N) = n$. And, incidentally, $f(C) = 1$ for every point $C$ of $N$.

(vi) In view of (ii), every positive integral multiple of $n$ is positively represented on $N$. Next let $r$ be an integer divisible by $\phi(N)$, in the range $0 < r < n$. Certainly $r$ is represented on $N$ by some function $f$. Let $m'$ be the least value assumed by $f$. Then, if $f'$ is the function defined in (ii) and if $m$ is any integer satisfying $m \geqslant -m'$, the integer $r + mn$ is positively represented on $N$ by $f + mf'$. Therefore, in every congruence class of integers mod $n$ divisible by $\phi(N)$, there is at most a finite number of positive integers not represented positively on $N$.

This completes the proof of Theorem 1. The Corollary follows from (i).

**3. A characterization of $\phi$.** If $N$ is a net of degree $k$, order $n$, we shall assume henceforth that the $k$ classes of "parallel" lines have been numbered (arbitrarily, but once and for all) from 1 to $k$. Thus, if $1 \leqslant i \leqslant k$, an $i$-line of $N$ is a line of class $i$. In terms of an arbitrary "centre" $C$ ($C$ a point of $N$) we introduce a coordinate system as follows: For $1 \leqslant i \leqslant k$, the $n$ lines of class $i$ are numbered from 1 to $n$, the $i$-line through $C$ being assigned the number 1. The $i$-line numbered $x$ is designated by $(i, x)$. We also introduce $k$ point-functions $I_i$, the indicators, by defining $I_i(P) = x$ if $(i, x)$ is the $i$-line through the point $P$.

If $f$ is a single-valued function from the integer-range $1 \leqslant x \leqslant n$ to the integers, we shall designate by $f(*)$ the sum $f(1) + f(2) + \ldots + f(n)$. In terms of these notations we may prove two theorems.

THEOREM 2. *Let $N$ be a net of degree $k$, order $n$. Then a necessary and sufficient condition that the integer $m$ be represented on $N$ is that $m$ be represented* mod $n$ *on $N$.*

THEOREM 3. *Let $N$ be a net of degree $k$, order $n$. Then $\phi(N)$ is the smallest positive integer $s$ with the following property: If $f_1, \ldots, f_k$ are single-valued functions from the integer-range $1 \leqslant x \leqslant n$ to the integers, such that*

$$f_i(1) \equiv 0 \bmod n \qquad (i = 1, \ldots, n), \tag{1}$$

$$\sum_{i=1}^{k} f_i(I_i(P)) \equiv 0 \bmod n \tag{2}$$

*for each point $P$ of $N$, then*

$$sf_1(*) \equiv 0 \bmod n.$$

https://doi.org/10.4153/CJM-1951-012-7 Published online by Cambridge University Press

*Proof.* If $a_1, \ldots, a_{kn}$ are the $kn$ lines and $P_1, \ldots, P_{n^2}$ are the $n^2$ points of $N$, in arbitrary arrangements, define the *line-point incidence matrix* $A$ of $N$ by putting 1 or 0 in the $u$th row, $v$th column of $A$ according as $P_v$ does or does not lie on $a_u$. Also define $U$ to be the column vector of order $kn$ with every element 1. Let $X$ be a column vector of order $n^2$ and let $m$ be an arbitrary integer. Then $m$ is represented on $N$ if and only if

$$AX = mU \tag{3}$$

for an integral $X$. In view of Theorem 1 (ii), (3) has a *rational* solution $X$ with every component equal to $m/n$. If $r = \operatorname{rank} A$, there exist unimodular matrices $T$, $Q$ (with rational integral components) such that

$$TAQ = \begin{pmatrix} D_r & 0 \\ 0 & 0 \end{pmatrix}, \qquad D_r = \operatorname{diag}(e_1, e_2, \ldots, e_r), \tag{4}$$

where the positive integers $e_j$ are the *invariant divisors* of $A$; thus $e_j | e_{j+1}$ for $j = 1, 2, \ldots, r - 1$. Setting $TU = V$, $X = QY$, we see that (3) may be reduced to

$$e_j y_j = m v_j \qquad (j = 1, \ldots, r). \tag{5}$$

A necessary and sufficient condition that (3) have an integral solution $X$ is that (5) yield integral values for $y_1, \ldots, y_r$. In particular, by the definition of $\phi(N)$, if

$$d_j = (e_j, v_j), \quad e_j = h_j d_j \qquad (j = 1, \ldots, r), \tag{6}$$

then $\phi(N)$ is the least common multiple

$$\phi(N) = [h_1, \ldots, h_r]. \tag{7}$$

Next let $u$ be any integer divisible by $e_r$ (and hence by each $e_j$.) Clearly $m$ is represented mod $u$ on $N$ if and only if $AX = mU$ mod $u$ for an integral $X$, or, equivalently, if and only if $e_j y_j \equiv m v_j$ mod $u$ for integral $y_j$ ($j = 1, \ldots, r$). Since $e_j | u$, the latter congruences imply $e_j | m v_j$, $h_j | m$, $\phi(N) | m$. However, if $\phi(N) | m$, $m$ is certainly represented on $N$. Thus Theorem 2 will be proved when we show that $e_r | n$.

For $i = 1, \ldots, k$, let the row-vector $R_i$ denote the sum of the $n$ rows of $A$ corresponding to the lines of class $i$. Since each point lies on exactly one $i$-line $R_i$ has each component equal to 1; thus $R_1 = R_2 = \ldots = R_k$. Let $B$ be the matrix of $1 + k(n - 1)$ rows obtained by deleting from $A$ the rows corresponding to the 2-line, 3-line, $\ldots$, $k$-line through the centre $C$. Clearly, since $R_i = R_1$, $T'A = \begin{pmatrix} B \\ 0 \end{pmatrix}$ for a unimodular matrix $T'$; hence $B$ has the same rank and invariant divisors as $A$. There is therefore no loss of generality in assuming that, in (4), the first $r$ rows of $T$ have zeros in the columns matching with the $k - 1$ rows of $A$ omitted in $B$. With this understanding, let $V_j$ be the $j$th row of $T$ ($j = 1, \ldots, r$); by (4), since $Q$ is unimodular, $e_j$ is the greatest

https://doi.org/10.4153/CJM-1951-012-7 Published online by Cambridge University Press

common divisor of the components of $V_jA$. For any fixed $j$, let $g_i(x)$ denote the component of $V_j$ in the column corresponding to the line $(i, x)$ of $N$; thus $g_i(1) = 0$ for $i > 1$. In $V_jA$, the column corresponding to point the $P$ has component

$$(8) \qquad \sum_{i=1}^{k} g_i(I_i(P)) \equiv 0 \bmod e_j.$$

When $P = C$, (8) reduces to $g_1(1) \equiv 0 \bmod e_j$; hence

$$(9) \qquad g_i(1) \equiv 0 \bmod e_j \qquad (i = 1, \ldots, k).$$

Selecting a fixed line $(i, x)$ and summing the congruence (8) over the $n$ points $P$ of $(i, x)$, we derive

$$(10) \qquad \sum_{u \neq i} g_u(*) + ng_i(x) \equiv 0 \bmod e_j.$$

From (10), (9), $ng_i(x) \equiv ng_i(1) \equiv 0 \bmod e_j$. Thus, if $d = (n, e_j)$ and $e_j = de'$, we have $g_i(x) \equiv 0 \bmod e'$ for all $i$, $x$. Since $T$ is unimodular, the greatest common divisor of the components of $V_j$ is 1; therefore $e' = 1$ and $e_j | n$. In particular $e_r | n$, proving Theorem 2.

In similar fashion, letting the $g_i$ be arbitrary rational-valued functions such that $g_i(1) = 0$ for $i > 1$, and replacing the congruences (8) by equations, we may deduce that $g_i(x) = 0$ for all $i, x$. This shows that the rows of $B$ are linearly independent, so that

$$(11) \qquad r = 1 + k(n - 1).$$

To prove Theorem 3, let $V_j$ have (integer-valued) components $g_i(x)$, as above, and let $f_i(x) = n_j g_i(x)$ where $n = n_j e_j$. Then (9) and (8) become (1) and (2) respectively. On the other hand, $V_jU = v_j$, in the notation of (5), and hence

$$(12) \qquad \sum_{i=1}^{k} f_i(*) = n_j v_j.$$

Multiplying (5) by $n_j$, we get $ny_j = m.n_j v_j$. Therefore $m$ is represented on $N$ if and only if $m.n_j v_j \equiv 0 \bmod n$ for $j = 1, \ldots, r$. To replace (10) we have $\sum_{u \neq i} f_u(*) \equiv 0 \bmod n$, whence, by (12), $n_j v_j \equiv f_i(*)$ for $i = 1, \ldots, k$. In particular, $n_j v_j \equiv f_1(*) \bmod n$. Thus, by the definition of $s$, $s.n_j v_j \equiv sf_1(*) \equiv 0 \bmod n$, for $j = 1, \ldots, r$. Hence $s$ is represented on $N$, $\phi(N) | s$.

We must prove the converse. Certainly $AX = \phi(N)U$ for an integral $X$. Let $f_1, \ldots, f_k$ be integer-valued functions satisfying (1) and (2), and let $V$ be the row-vector with $f_i(x)$ in the column corresponding to line $(i, x)$. Then $VA$ has component $\sum_{i=1}^{k} f_i(I_i(P))$ in the column corresponding to point $P$, while $VU = \sum_{i=1}^{k} f_i(*)$. Thus the equation $VAX = \phi(N) VU$, together with the congruences (2), implies that

$$(13) \qquad \phi(N) \sum_{i=1}^{k} f_i(*) \equiv 0 \bmod n.$$

By the same methods as before, we deduce from (1) and (2) that (13) is equivalent to $\phi(N)f_1(*) \equiv 0 \bmod n$. Since $s$ is the least positive integer such that $sf_1(*) \equiv 0 \bmod n$ for all such functions $f_i$, $s|\phi(N)$. Therefore $\phi(N) = s$. This completes the proofs of Theorems 2, 3.

**3. Direct products of nets.** Let $N_1$, $N_2$ be nets of orders $n_1$, $n_2$ respectively, and of the same degree $k$. The *direct product* $N = N_1 \times N_2$ is defined as follows: (i) The points of $N$ are the ordered pairs $(P_1, P_2)$, with $P_j$ a point of $N_j$. (ii) For $i = 1, \ldots, k$, the $i$-lines of $N$ are the ordered pairs $(a_1, a_2)$, with $a_j$ an $i$-line of $N_j$. (iii) $(P_1, P_2)$ lies on $(a_1, a_2)$ in $N$ if and only if $P_j$ lies on $a_j$ in $N_j$ for $j = 1, 2$. It is easy to verify that $N$ is a net of degree $k$, order $n_1n_2$. Making the obvious identifications one may establish the commutative and associative laws for direct products.

If $N_1$ has a coordinate system centered about $C_1$, with indicators $I_i$, and $N_2$ has a coordinate system centered about $C_2$, with indicators $J_i$, we introduce a natural coordinate system for $N = N_1 \times N_2$ as follows: Take $C = (C_1, C_2)$ as centre. If $a_j$ is the $i$-line $(i, x_j)$ of $N_j$ $(j = 1, 2,)$ denote by $(i; x_1, x_2)$ the $i$-line $(a_1, a_2)$ of $N$. Define the indicators $I_i$ of $N$ by $I_i(P_1, P_2) = (x_1, x_2)$ where $(i; x_1, x_2)$ is the $i$-line of $N$ through $(P_1, P_2)$. Moreover, if $f(x_1, x_2)$ is a function from the integer-domain $1 \leqslant x_1 \leqslant n_1$, $1 \leqslant x_2 \leqslant n_2$ to the integers, denote by $f(*, x_2)$ the sum $f(1, x_2) + f(2, x_2) + \ldots + f(n_1, x_2)$. Similar meanings are assigned to $f(x_1, *)$ and $f(*, *)$.

THEOREM 4. *Let $N_j$ be a net of order $n_j$ and degree $k$, for $j = 1, 2$, and let $N = N_1 \times N_2$. Write*

$$(14) \qquad d = (n_1, n_2), \qquad n_1 = dq_1, \qquad n_2 = dq_2.$$

*Then there exist positive integers $a$, $b$ such that*

$$(15) \qquad (q_1, \phi(N_1)) \,.\, (q_2, \phi(N_2)) = a \,.\, \phi(N),$$

$$(16) \qquad (d, k-1) \,.\, \phi(N) = b\,[\phi(N_1), \phi(N_2)],$$

$$(17) \qquad ab \mid (d, k-1).$$

COROLLARY 1. *If $(n_1, n_2, k-1) = 1$, then $\phi(N_1 \times N_2) = \phi(N_1)\phi(N_2)$.*

COROLLARY 2. *If $(q_1q_2, k-1) = 1$, then $\phi(N_1 \times N_2) = 1$.*

COROLLARY 3. *For any finite net $N$, $\phi(N \times N) = 1$.*

*Proof.* In the present notation the content of Theorem 3 may be expressed as follows: $\phi(N)$ is the least positive integer such that, for integer-valued functions $f_i$, the congruences

$$(18) \qquad f_i(1, 1) \equiv 0 \bmod n_1n_2,$$

$$(19) \qquad \sum_{i=1}^{k} f_i(I_i(P_1), J_i(P_2)) \equiv 0 \bmod n_1n_2$$

for all points $(P_1, P_2)$ of $N$, imply

$$\phi(N)f_1(*, *) \equiv 0 \bmod n_1n_2. \tag{20}$$

Keeping $P_1$ fixed in (19), select a line $(i, x_2)$ of $N_2$ and sum over all points $P_2$ of $(i, x_2)$. Then

$$\sum_{j \neq i} f_j(I_j(P_1), *) + n_2f_i(I_i(P_1), x_2) \equiv 0 \bmod n_1n_2. \tag{21}$$

Since the sum in (21) is independent of $x_2$, we have

$$n_2f_i(I_i(P_1), x_2) \equiv n_2f_i(I_i(P_1), 1) \bmod n_1n_2,$$

i.e.

$$f_i(x_1, x_2) \equiv f_i(x_1, 1) \bmod n_1 \tag{22}$$

for all $i$, $x_1$, $x_2$ in their respective ranges. Similarly,

$$f_i(x_1, x_2) \equiv f\,(1, x_2) \bmod n_2. \tag{23}$$

Since $d$ divides $n_1$, $n_2$, we deduce from (22), (23) and (18) that

$$f_i(x_1, x_2) \equiv 0 \quad \bmod d. \tag{24}$$

Returning to (21), choose any line $(j, x_1)$ of $N_1$, with $j \neq i$, and sum over all points $P_1$ of $(j, x_1)$. There results

$$\sum_{p \neq i, j} f_p(*, *) + n_1f_j(x_1, *) + n_2f_i(*, x_2) \equiv 0 \bmod n_1n_2 \tag{25}$$

for all $i, j$ $(i \neq j)$ and $x_1$, $x_2$. As in the proof of Theorem 3, $f_p(*, *) \equiv f_1(*,*)$ mod $n_1n_2$. And since, by Theorem 1, $\phi(N)$ divides $k - 1$, $(k - 1)f_1(*, *) \equiv 0$ mod $n_1n_2$. Therefore (25) is equivalent to

$$f_1(*, *) \equiv n_1f_j(x_1, *) + n_2f_i(*, x_2) \bmod n_1n_2. \tag{26}$$

Since $k \geqslant 3$, and since in (26) the only restriction is $i \neq j$, (26) is equivalent to

$$f_1(*, *) \equiv n_1f_1(x_1, *) + n_2f_1(*, x_2) \bmod n_1n_2. \tag{27}$$

Define $t_1$, $t_2$ as the least positive integers such that

$$t_1n_2f_1(*, x_2) \equiv 0, \qquad t_2n_1f_1(x_1, *) \equiv 0 \qquad \bmod n_1n_2 \tag{28}$$

for all $f_i$ satisfying (18), (19). By (27), $t_1t_2f_1(*, *) \equiv 0 \bmod n_1n_2$. Hence, by the property (20) of $\phi(N)$,

$$\phi(N) \mid t_1t_2. \tag{29}$$

Since $q_1d = n_1$, (24) implies $q_1n_2f_1(*, x_2) \equiv 0 \bmod n_1n_2$. Thus $t_1 \mid q_1$. Similarly,

$$t_j \mid q_j \qquad (j = 1, 2). \tag{30}$$

Since the $q_j$ are relatively prime, so are the $t_j$. Next choose any fixed value for $x_2$ and define functions $F_i(x_1) = f_i(x_1, x_2)$. From (22), $F_i(x_1) \equiv f_i(x_1, 1)$ mod $n_1$. Thus, from (18), $F_i(1) \equiv 0 \bmod n_1$. Moreover, by (19),

$$\sum_{i=1}^{k} F_i(I_i(P_1)) \equiv \sum_{i=1}^{k} f_i(I_i(P_1), \quad J_i(C_2)) \equiv 0 \bmod n_1.$$

Therefore, by Theorem 3, $0 \equiv \phi(N_1)F_1(*) \equiv \phi(N_1)f_1(*, x_2) \bmod n_1$, and so $\phi(N_1)n_2f_1(*, x_2) \equiv 0 \bmod n_1n_2$. Hence (and similarly)

$$t_j \mid \phi(N_j) \qquad (j = 1, 2). \tag{31}$$

By (30), (31), $t_j$ divides the greatest common divisor of $q_j$ and $\phi(N_j)$. Hence (29) implies (15) for some positive integer $a$.

To obtain (16), let $g_i(x_1)$ be any set of integer-valued functions satisfying equations analogous to (1), (2) for $N_1$, and set $f_i(x_1, x_2) = n_2g_i(x_1)$. Then the $f_i$ will satisfy (18), (19). Therefore $\phi(N)f_1(*, *) = \phi(N)(n_2)^2g_1(*) \equiv 0$ mod $n_1n_2$, $\phi(N)n_2g_1(*) \equiv 0 \bmod n_1$, $\phi(N_1) \mid \phi(N)n_2$. Since $\phi(N_1) \mid (n_1, k-1)$ and since $(n_1, n_2) = d$, we may improve the last statement to $\phi(N_1) \mid (d, k-1)\phi(N)$. Similarly for $\phi(N_2)$. Hence the least common multiple $[\phi(N_1), \phi(N_2)]$ divides $(d, k-1)\phi(N)$, proving (16) for some positive integer $b$.

Eliminating $\phi(N)$ from (15), (16), we derive $ab[\phi(N_1), \phi(N_2)] = (d, k-1)$ $(q_1, \phi(N_1))(q_2, \phi(N_2))$. Since the integers $(q_j, \phi(N_j))$ are relatively prime divisors of $[\phi(N_1), \phi(N_2)]$, we have (17). This completes the proof of Theorem 4. In the case of Corollary 1, $a = b = 1$, by (17), and then $\phi(N) = \phi(N_1)$ $\phi(N_2)$ by (16) and the fact that $(\phi(N_1), \phi(N_2))$ is a divisor of $(n_1, n_2, k-1) = 1$.

In the case of Corollary 2, the left-hand side of (15) is 1, since, for example, $(q_1, \phi(N_1))$ divides $(q_1, k-1) = 1$. Thus $\phi(N) = 1$. And Corollary 3 corresponds to the special case $q_1 = 1 = q_2$ of Corollary 2.

THEOREM 5. *Let $n > 1$ be a positive integer with factorization $n = \Pi p(i)^{m(i)}$ where the $p(i)$ are distinct primes and the $m(i)$ are positive integers. Let* $r = \min$ $(p(1)^{m(1)}, p(2)^{m(2)}, \ldots .)$. *Then there exists a net $N$ of order $n$, degree $r + 1$, such that $\phi(N) = r > 1$. In particular, no line can be adjoined to $N$.*

COROLLARY. *If $k$ is any integer such that $3 \leqslant k \leqslant r + 1$, there exists a net $N$ of order $n$, degree $k$.*

*Proof.* For any prime $p$ and positive integer $m$, let $\mathrm{E}(p, m)$ be an affine plane of order $p^m$ (and degree $p^m + 1$.) Such a plane exists, for example, the plane obtained by using coordinates (in the familiar manner of elementary plane geometry) from the field $\mathrm{GF}(p^m)$. For each $i$, we may define a net $N_i$ of degree $r+1$, order $p(i)^{m(i)}$ from an $\mathrm{E}(p(i), m(i))$ by deleting some $(p(i)^{m(i)}+1)-(r+1)$ classes of lines. Set $N = N_1 \times N_2 \times \ldots .$ By an obvious extension of Corollary 1 to Theorem 4, $\phi(N) = \phi(N_1)\phi(N_2) \ldots .$ For exactly one $i$, $N_i = \mathrm{E}(p(i), m(i))$ and $\phi(N_i) = p(i)^{m(i)} = r$. For all other $i$, lines can be adjoined to $N_i$, so $\phi(N_i) = 1$. Therefore $\phi(N) = r > 1$. As for the Corollary we need merely delete some $r + 1 - k$ classes of lines from $N$.

**4. Homomorphic nets.** Let $N$, $N'$ be nets of the same degree $k$. A *homomorphism* $\theta$ of $N$ upon $N'$ is a single-valued, exhaustive mapping of $N$ upon $N'$ which maps points upon points, $i$-lines upon $i$-lines (for $i = 1, \ldots, k$) and preserves incidence. The requirement that $i$-lines be mapped upon $i$-lines may seem artificial. The obvious generalization, however, is no more necessary than the little used concept of "anti-homomorphism" in group theory, and adds complications to the proofs. (See Bates [1] for a similar restriction in regard to 3-nets.)

A homomorphism $\theta$ of $N$ upon $N'$ is called an *isomorphism* if it is one-to-one, and a *zero homomorphism* if $N'$ has order one. A net $N$ is *simple* if its only homomorphisms upon nets are isomorphisms and zero homomorphisms.

LEMMA 1. *Let $N$, $N'$ be nets of respective orders $n$, $n'$ and of the same degree $k$. Let $\theta$ be a homomorphism of $N$ upon $N'$. For each point $P'$ of $N'$, let $M(P')$ be the subset of $N$ consisting of all points $P$ of $N$ such that $P\theta = P'$ and of all lines $a$ of $N$ such that $a\theta$ passes through $P'$. Then $n = mn'$ for a positive integer $m$, and each $M(P')$ is a subnet of $N$, of order $m$, degree $k$.*

COROLLARY. *Every finite affine plane is a simple net.*

*Proof.* Consider one of the sets $M = M(P')$. Then $M$ contains lines of each of the $k$ classes in $N$, since the $k$ lines through $P'$ are images under $\theta$. If $a$, $b$ are lines of distinct classes in $N$, such that $a\theta$, $b\theta$ pass through $P'$, the intersection point $P = a \,.\, b$ satisfies $P\theta = P'$, and hence is in $M$. If $Q$ is in $M$, each of the $k$ lines through $Q$ is in $M$. Hence $M$ is a net of degree $k$ and of some order $m$. In particular, for each $i$, $M$ has exactly $m$ $i$-lines, and these are precisely the $i$-lines of $N$ which map into the $i$-lines through $P'$. If $Q'$ is a point of $N'$, distinct from $P'$, the $i$-line through $P'$ and the $j$-line through $Q'$ ($j \neq i$) must meet in a point $R'$ of $N'$. Then $M(R')$, $M(P')$ have the same $i$-lines, hence the same order $m$; and $M(Q')$, $M(R')$ have the same $j$-lines, hence the same order $m$. Therefore each of the $(n')^2$ subnets $M(P')$ has order $m$, showing that $(n')^2m^2 = n^2$ or $n = mn'$.

As for the Corollary, if the net $N$ has order $n = k - 1$, then $k - 1 = mn'$. But either $n' = 1$ or $n' \geqslant k - 1$; and the second alternative gives $n' = k - 1$, $m = 1$. Hence every homomorphism of $N$ upon a net is either a zero homomorphism or an isomorphism. Thus $N$ is simple. This Corollary offers a partial explanation of the lack of success in attempting to define homomorphisms of projective planes (Marshall Hall [1]).

With the notation of Lemma 1, define $D$ to be the greatest common divisor of all the integers $\phi(P') = \phi(M(P'))$. Also write

$$d = (m, n'), \qquad m = du, \qquad n' = dv. \tag{32}$$

THEOREM 6. *Let $N$ be a net of degree $k$, order $n = mn'$, possessing a proper homomorphism $\theta$ upon a net $N'$ of order $n'$. (Thus $m, n' \geqslant k - 1$.) Then*

$$\phi(N) \mid [\phi(N'), (u, D)], \qquad \phi(N') \mid (d, k - 1)\phi(N). \tag{33}$$

https://doi.org/10.4153/CJM-1951-012-7 Published online by Cambridge University Press

*Proof.* If $\phi(N)$ is represented on $N$ by the point function $f(P)$, define $g(P') = \sum f(P)$ where the sum is taken over the $m^2$ points $P$ such that $P\theta = P'$. Then it is easy to see that $g$ represents $m\phi(N)$ on $N'$. Hence $\phi(N') \mid m\phi(N)$. By (32) and the fact that $\phi(N') \mid (n', k-1)$, we deduce the second relation of (33). If $a, b, c$ are integers, one readily verifies the identity $([a, b], [a, c]) = [a, (b, c)]$. Thus the relation

$$\phi(N) \mid [\phi(N'), (u, \phi(C'))], \tag{34}$$

holding for every point $C'$ of $N'$, implies the first relation of (33). We complete the proof by establishing (34).

Let $\theta'$ be any one-to-one mapping of the points of $N'$ into the points of $N$, such that $P'\theta'\theta = P'$. Thus $P'\theta'$ is in $M(P')$ for each $P'$ of $N'$. Choose any point $C'$ as centre in $N'$ and take $C = C'\theta'$ as centre in $N$. Let $I_i$, $J_i$ be the indicator functions for $N$, $N'$ respectively. As an additional notation, define

$$I_i(P') = I_i(P'\theta'), \qquad P' \text{ in } N'. \tag{35}$$

If $f(x)$ is a function from the integer-range $1 \leqslant x \leqslant n$ to the integers, define $f(*)$ as before. Also define

$$f(i, P') = \sum{}' f(x), \tag{36}$$

where the sum in (36) is taken over all $x$ such that $(i, x)$ is a line of $M(P')$. Now let $f_i$ be functions satisfying (1), (2) of Theorem 3. For any point $P'$ of $N'$, and any line $(i, x)$ of $M(P')$, sum (2) over all points $P$ common to $(i, x)$ and $M(P')$. Thus

$$\sum_{j \neq i} f_j(j, P') + mf_i(x) \equiv 0 \bmod n. \tag{37}$$

Since the second term of (37) is independent of the choice of $(i, x)$ in $M(P')$,

$$f_i(x) \equiv f_i(I_i(P')) \bmod n', \qquad (i, x) \text{ in } M(P'). \tag{38}$$

By (38), $f_i(x)$ is determined mod $n'$ by the line $(i, x') = (i, x)\theta$ of $N'$. Thus (mod $n'$) we may define a set of integer-valued functions $F_i(x')$, on the range $1 \leqslant x' \leqslant n'$, by

$$F_i(x') \equiv f_i(x) \bmod n' \qquad \text{if } (i, x)\theta = (i, x'). \tag{39}$$

Clearly the $F_i$ satisfy the conditions corresponding to (1), (2) for N′. Therefore, by Theorem 3,

$$\phi(N')F_1(*) \equiv 0 \bmod n'. \tag{40}$$

Next pick $j \neq i$ and consider the line $(j, 1)$ of $N'$. By (39), (38),

$$F_i(*) \equiv \sum{}' f_i(I_i(P')) \bmod n' \tag{41}$$

where the sum in (41) is over the points $P'$ of $(j, 1)$. Moreover $f_j(j, P') = f_j(j, C')$ for $P'$ on $(j, 1)$, since, for each $P'$ of $(j, 1)$, the $j$-lines of $M(P')$ are

https://doi.org/10.4153/CJM-1951-012-7 Published online by Cambridge University Press

those lines $(j, x)$ such that $(j, x)\theta = (j, 1)$. Hence, if in (37) we sum over all points $P'$ of $(j, 1)$, there results

$$\sum_{p \neq i, j} f_p(*) + n' f_j(j, C') + mF_i(*) \equiv 0 \bmod n. \tag{42}$$

As in the proof of Theorem 5, (42) is equivalent to

$$f_1(*) \equiv n' f_1(1, C') + mF_1(*) \bmod n. \tag{43}$$

If $t$ is the least positive integer such that

$$tn' f_1(1, C') \equiv 0 \bmod n \tag{44}$$

for all functions $f_i$ satisfying (1), (2), then (40), (43) imply $[\phi(N'), t] f_1(*) \equiv 0 \bmod n$. Hence

$$\phi(N) \mid [\phi(N'), t]. \tag{45}$$

Since $C$ is the centre for $M(C')$ as well as for $N$, and since $m \mid n$, the $f_i$ satisfy conditions analogous to (1), (2) for the net $M(C')$. And since $f_1(1, C')$ denotes for $M(C')$ the sum analogous to $f_1(*)$ for $N$, $\phi(C') f_1(1, C') \equiv 0 \bmod m$. Inasmuch as $n = mn'$, this and (44) imply $t \mid \phi(C')$. Again, from (38), if $(1, x)$ is in $M(C')$, $f_1(x) \equiv f_1(I_1(C')) \equiv f_1(1) \equiv 0 \bmod n'$ and therefore $f_1(1, C') \equiv 0 \bmod n'$. Moreover, $un' . n' = nv$, by (32), so that $un'f(1, C') \equiv 0 \bmod n$. Hence $t \mid u$. Therefore

$$t \mid (u, \phi(C')). \tag{46}$$

And (45), (46) combine to give (34). This completes the proof of Theorem 6.

**5. Explicit evaluation of $\phi$ for nets of degree 3.** A set $G$ together with an operation (.) is called a *loop* provided: (i) if $a, b$ are in $G$, $a . b$ is a uniquely determined element of $G$; (ii) if $a, b$ are in $G$ there exists a unique $x$ in $G$ such that $x . a = b$ and a unique $y$ in $G$ such that $a . y = b$; (iii) there exists a (unique) element 1 of $G$ such that $a . 1 = 1 . a = a$ for every $a$ in $G$. A loop is a group if and only if it obeys the associative law $(a . b) . c = a . (b . c)$. The concepts of homomorphism, normal subloop and quotient loop are quite similar to the corresponding concepts in group theory (Albert [1], Baer [2], Bruck [1]). For our purposes the essential facts are these: If the loop $G$ of order $n$ possesses a homomorphism $\theta$ upon a loop $G'$ of order $n'$, then the kernel $H$ of $\theta$ is a normal subloop of $G$ and $G/H$ is isomorphic to $G'$. Moreover $H$ has order $m$ where $n = mn'$, and each element of $G'$ is the image under $\theta$ of precisely $m$ distinct elements of $G$. Finally, there is a one-to-one correspondence between the normal subloops of $G$ and the homomorphisms of $G$ upon loops.

From a loop $G$ of order $n$, we form a net $N = N(G)$ of order $n$, degree 3, as follows: The points of $N$ are the $n^2$ ordered pairs $(x, y)$ of elements of $G$. Each $a$ of $G$ determines: (i) a 1-line $x = a$ whose points are the $n$ points $(a, y)$; (ii) a 2-line $y = a$ whose points are the $n$ points $(x, a)$; (iii) a 3-line $x . y = a$

whose points are the $n$ points $(x, y)$ with $x \cdot y = a$. As shown in Bates [1], every net of order $n$, degree 3 may be so defined in terms of a suitable loop $G$ of order $n$. We define $\phi(G) = \phi(N(G))$.

THEOREM 7. *Let $G$ be a finite loop of order $n$. If $G$ contains a normal subloop $H$ of odd order such that the quotient loop $G/H$ is a cyclic group of even order, then $\phi(G) = 2$. In all other cases, $\phi(G) = 1$.*

COROLLARY 1. *Necessary and sufficient conditions that $\phi(G) = 2$ are that $n = m \cdot 2^t$ for $m$ odd, $t \geqslant 1$, that $G$ contain a normal subloop $K$ of order $m$, and that $G/K$ be the cyclic group of order $2^t$.*

COROLLARY 2. *If $n = 4m + 2$, then $\phi(G) = 2$ if and only if $G$ contains a subloop of order $2m + 1$.*

COROLLARY 3. *If $G$ is a group of order $n = 4m + 2$, then $\phi(G) = 2$.*

*Proof.* Take $C = (1, 1)$ as the centre of the net $N(G)$ and define indicators $I_i (i = 1, 2, 3)$ so that if $P = (x, y)$ then $I_1(P) = x$, $I_2(P) = y$, $I_3(P) = x \cdot y$. Conditions (1), (2) of Theorem 3 become

$$f_1(1) \equiv f_2(1) \equiv f_3(1) \equiv 0 \bmod n, \tag{47}$$

$$f_1(x) + f_2(y) + f_3(x \cdot y) \equiv 0 \bmod n, \tag{48}$$

for all $x, y$ of $G$. Setting, in turn, $x = 1$ and $y = 1$ in (48), we find, by (47), that $-f_3(x) \equiv f_1(x) \equiv f_2(x) \equiv f(x)$, say, mod $n$ so that (47), (48) can be replaced by

$$f(x \cdot y) \equiv f(x) + f(y) \bmod n \tag{49}$$

for all $x, y$ of $G$. In view of (49), the mapping $x \rightarrow f(x)$ is a homoorphism of $G$ upon some subgroup $Z$ of the additive group of the integers mod $n$. Thus $Z$ is a cyclic group.

Conversely, if $G$ is homomorphic to a cyclic group $Z$ of order $n'$, we may assume without loss of generality that $Z$ is a subgroup of the additive group of integers mod $n$ and that the homomorphism is given by (49). Also $n = mn'$ where $m$ is the order of the kernel, and exactly $m$ elements of $G$ map upon each element of $Z$. If $t$ is the sum of the elements of $Z$ it is easily verified (compare Paige [1]) that $t$ is the unit 0 if $n'$ is odd and the unique element of order two if $n'$ is even. In any case, by Theorem 3, $\phi(G)$ is the least positive integer $s$ such that

$$sf(*) \equiv smt \equiv 0 \bmod n \tag{50}$$

for all integer-valued $f$ satisfying (49). Clearly $\phi(G) \mid 2$.

If $n'$ is even, $t$ has order two. If also $m$ is odd, (50) implies that $2 \mid \phi(G)$. Therefore $\phi(G) = 2$, proving the first statement of Theorem 7.

Next suppose that $G$ is such that there exists no $f$ for which $m$ is odd and $n'$

https://doi.org/10.4153/CJM-1951-012-7 Published online by Cambridge University Press

is even. If $m$ is odd, $n'$ is odd and $t \equiv 0$, so that $f(*) \equiv 0 \bmod n$. If $m$ is even, $f(*) \equiv mt \equiv 0$, since $2t \equiv 0 \bmod n$. Therefore $\phi(G) = 1$. This completes the proof of Theorem 7. The Corollaries are immediate consequences of known facts about loops and groups.

## BIBLIOGRAPHY

A. A. Albert
[1] *Quasigroups* I, Trans. Amer. Soc., vol. 54 (1943), 502-519;
*Quasigroups* II, *loc. cit.*, vol. 55 (1944), 401-419.
Reinhold Baer
[1] *Nets and groups*, Trans. Amer. Math. Soc., vol. 46 (1939), 110-141;
*Nets and groups*. II, *loc. cit.*, vol. 47 (1940), 435-439.
[2] *The homomorphism theorems for loops*, Amer. J. Math., vol. 67 (1945), 450-460.
P. T. Bateman
[1] *A remark on infinite groups*, Amer. Math. Monthly, vol. 57 (1950), 623-624.
Grace E. Bates
[1] *Free loops and nets and their generalizations*, Amer. J. Math., vol. 69 (1947), 499-550.
G. Bol
[1] *Geweben und Gruppen*, Math. Ann., vol. 114 (1937), 414-431.
R. C. Bose
[1] *On the application of the properties of Galois fields to the problem of construction of hyper-Graeco-latin squares*, Sankya, Indian Journal of Statistics, vol. 3 (1938), 323-338.
R. C. Bose and K. R. Nair
[1] *On complete sets of latin squares*, Sankya, vol. 5 (1942), 361-382.
R. H. Bruck
[1] *Contributions to the theory of loops*, Trans. Amer. Math. Soc., vol. 60 (1946), 245-354.
R. H. Bruck and H. J. Ryser
[1] *The non-existence of certain finite projective planes*, Can. J. Math., vol. 1 (1949), 88-93.
L. Euler
[1] *Recherches sur une nouvelle espèce de quarrés magiques*, Collected works, series prima, vol. 7, 291-392.
R. A. Fisher and F. Yates
[1] *The* 6 × 6 *latin squares*, Proc. Camb. Phil. Soc., vol. 30 (1934), 492-507.
[2] *Statistical tables for agricultural, biological and medical research* (Edinburgh, 1943.)
Marshall Hall
[1] *Projective planes*, Trans. Amer. Math. Soc., vol. 54 (1943), 29-77.
M. G. Kendall
[1] *Who discovered the latin square?*, American Statistician, vol. 2 (1948), 13.
F. W. Levi
[1] *Finite geometrical systems* (University of Calcutta, 1942.)
C. C. MacDuffee
[1] *The theory of matrices* (New York, 1946.)
H. F. MacNeish
[1] *Euler squares*, Ann. of Math., vol. 23 (1921-2), 221-227.
H. B. Mann
[1] *The construction of orthogonal squares*, Ann. of Math. Statistics, vol. 13 (1942), 418-423.
[2] *On orthogonal latin squares*, Bull. Amer. Math. Soc., vol. 50 (1944), 249-257.
[3] *Analysis and design of experiments* (New York, 1949.)
H. W. Norton
[1] *The* 7 × 7 *squares*, Ann. Eugen., vol. 9 (1939), 269-307.

L. J. Paige
[1] *A note on finite abelian groups*, Bull. Amer. Math. Soc., vol. 53 (1947), 590-593.
[2] *Neofields*, Duke Math. J., vol. 16 (1949), 39-60.
Albert Sade
[1] *Enumération des carrés latins. Application au* $7^e$ *ordre. Conjecture pour les ordres supérieurs*. (Published by the author, Marseille, 1948.)
W. L. Stevens
[1] *The completely orthogonalized latin square*, Ann. Eugen., vol. 9 (1939), 82-93.
G. Tarry
[1] *Le problème de* 36 *officiers*, Compte Rendu de l'Association Française pour l'Avancement de Science Naturel, vol. 1 (1900), 122-123; vol. 2 (1901), 170-203.

*University of Wisconsin*

## Vol. II, No. 2: Errata

## WATER WAVES OVER A CHANNEL OF FINITE DEPTH

ALBERT E. HEINS

p. 216: Instead of $L_+(w)$, read $1/L_+(w)$. Also, for exp $[\chi(w)]$ in this expression read exp $[-\chi(w)]$.

p. 221: Multiply $|L_+(\pm\kappa)|^2$ by $b$.

Multiply $|L_+(\pm\kappa')|^2$ by $b\rho_0$.

Divide the expression for $\left|\dfrac{L_+(\pm\kappa)}{L_+(\pm\kappa')}\right|^2$ by $\rho_0^2$.

In the formulas for $t_1$ and $t_2$, $\kappa\rho_0/2$ and $2\kappa'/\rho_0$ should be replaced by $2\kappa$ and $2\kappa'$, respectively.

https://doi.org/10.4153/CJM-1951-012-7 Published online by Cambridge University Press