

# ON TRANSITIVE COMMUTATIVE IDEMPOTENT QUASIGROUPS

ARNOLD NEUMAIER

(Received 20 May 1975)

Communicated by W. D. Wallis

## Abstract

Commutative idempotent quasigroups with a sharply transitive automorphism group  $G$  are described in terms of so-called Room maps of  $G$ . Orthogonal Room maps and skew Room maps are used to construct Room squares and skew Room squares. Very general direct and recursive constructions for skew Room maps lead to the existence of skew Room maps of groups of order prime to 30. Also some nonexistence results are proved.

*1980 Mathematics subject classification (Amer. Math. Soc.):* primary 05 B 15; secondary 20 N 05.

## 1. Room squares and orthogonal ci-quasigroups

1.1. Let  $r$  be an odd integer.

A *Room square* of side  $r$  is an arrangement of  $r+1$  distinct objects in a square array of side  $r$  satisfying

- (i) each of the  $r^2$  cells of the array is either empty or contains exactly two distinct objects,
- (ii) each row and each column of the array contains each of the  $r+1$  objects exactly once,
- (iii) every unordered pair of distinct objects occurs in exactly one cell of the array.

The square is *skew*, if, in addition,

(iva) cell  $(i, i)$  contains the pair  $i, \infty$ ,

(ivb) cell  $(i, k)$  is empty if and only if  $i \neq k$  and cell  $(k, i)$  is not empty; here cell  $(i, k)$  is the cell in row  $i$  and column  $k$ .

A Room square is known to exist if and only if  $r \neq 3, 5$ ; see for example Wallis (1973a, 1974).

**1.2.** We refer to a commutative idempotent quasigroup  $(Q, *)$  as a *ci-quasigroup*.

Two ci-quasigroups  $(Q, *)$  and  $(Q, **)$  are *orthogonal* if and only if the equations  $x * y = a$ ,  $x ** y = b$  have at most one solution  $\{x, y\} \subseteq Q$  (as unordered pair), for every  $a, b \in Q$ ; they are *skew orthogonal* if and only if, in addition,  $x = y = z = t$  is the only possibility to satisfy the equations  $x * y = z ** t$ ,  $x ** y = z * t$ .

Note that the two quasigroups are never orthogonal if considered simply as quasigroups.

**1.3.** By row and column permutation and renumbering of elements we may standardize any Room square such that the diagonal cells  $(i, i)$  contain the pair  $i, \infty$ , where  $\infty$  is a fixed element. If we define two operations  $*$  and  $**$  on the set  $Q = \{1, \dots, r\}$  by

$x * y = z$  if and only if  $x = y = z$ , or  $x \neq y$  and the pair  $x, y$  is in row  $z$ ,

$x ** y = z$  if and only if  $x = y = z$ , or  $x \neq y$  and the pair  $x, y$  is in column  $z$ ,

a simple verification shows that  $(Q, *)$  and  $(Q, **)$  are a pair of (skew) orthogonal ci-quasigroups if and only if the given square is a standardized (skew) Room square.

Conversely, from (skew) orthogonal ci-quasigroups  $(Q, *)$ ,  $(Q, **)$  one may construct a standardized (skew) Room square, defining

$x, \infty$  is in cell  $(x, x)$  for every  $x \in Q$ ,

$x, y$  is in cell  $(x * y, x ** y)$  for every pair  $x, y \in Q, x \neq y$ ,

the other cells are empty.

The proofs are straightforward and thus omitted; see Bruck (1963).

## 2. Room maps and sharply transitive ci-quasigroups

A ci-quasigroup  $(Q, *)$  is *sharply transitive* if and only if it possesses a group  $G$  of automorphisms, sharply transitive on  $Q$ . We describe sharply transitive ci-quasigroups within the group  $G$ .

**2.1.** Let  $G$  be a finite group. We call a map  $\varphi: G \rightarrow G$  a *Room map* if and only if

$$(1) \quad \varphi(1) = 1,$$

$$(2) \quad \varphi(x^{-1}) = \varphi(x) \quad (x \in G),$$

$$(3) \quad \{\varphi(x)x \mid x \in G\} = G.$$

A Room map  $\varphi$  satisfying

$$(4) \quad \varphi(x) = \varphi(y) \Rightarrow y = x \quad \text{or} \quad y = x^{-1} \quad (x, y \in G)$$

is called *strong*; if, moreover,

$$(5) \quad \varphi(x) = \varphi(y)^{-1} \Rightarrow x = y = 1 \quad (x, y \in G)$$

then  $\varphi$  is called *skew*.

EXAMPLE. The trivial map  $\sigma$  with  $\sigma(x) = 1$  for every  $x \in G$  is a Room map. Suppose  $\varphi_1$  and  $\varphi_2$  are Room maps. If

$$(6) \quad \varphi_1(x) \varphi_2(x)^{-1} = \varphi_1(y) \varphi_2(y)^{-1} \Rightarrow y = x \quad \text{or} \quad y = x^{-1} \quad (x, y \in G)$$

then we say  $\varphi_1$  and  $\varphi_2$  are *orthogonal*; if, in addition,

$$(7) \quad \varphi_1(x) \varphi_2(x)^{-1} = \varphi_2(y) \varphi_1(y)^{-1} \Rightarrow x = y = 1 \quad (x, y \in G)$$

then  $\varphi_1$  and  $\varphi_2$  are said to be *skew orthogonal*.

From the definitions we see immediately that  $\varphi$  is strong if and only if  $\varphi$  and  $\sigma$  are orthogonal, and  $\varphi$  is skew if and only if  $\varphi$  and  $\sigma$  are skew orthogonal.

2.2. If  $G$  has odd order, and if  $\varphi$  is a Room map of  $G$ , define the operation  $*_\varphi$  on  $G$  by

$$(8) \quad u *_\varphi v = \varphi(x)w \quad \text{where} \quad x^2 = uv^{-1} \quad \text{and} \quad w = xv$$

(equivalently,  $u = xw$  and  $v = x^{-1}w$ ). Since  $G$  has odd order, the map  $x \rightarrow x^2$  is a permutation of  $G$ , thus  $*_\varphi$  is well defined. Because of  $\varphi(x) = x *_\varphi x^{-1}$ , distinct maps  $\varphi$  yield distinct operations.

$(G, *_\varphi)$  is a ci-quasigroup! Because of  $u = 1u$ ,  $u = 1^{-1}u$  we have  $u *_\varphi u = \varphi(1)u = u$ . If  $u = xw$ ,  $v = x^{-1}w$  then  $u *_\varphi v = \varphi(x)w = \varphi(x^{-1})w = v *_\varphi u$ . Finally,  $u *_\varphi v = t$  has the solution  $u = x^2v$  where  $\varphi(x)x = v^{-1}t$  determines  $x$ .

We remark that  $G$  operates on the constructed ci-quasigroup by right multiplication as a sharply transitive group of automorphisms.

If  $G$  is abelian and written additively then (8) simplifies to

$$(8a) \quad u *_\varphi v = \frac{u+v}{2} + \varphi\left(\frac{u-v}{2}\right).$$

As a curiosity, we obtain from every noncommutative group  $G$  of odd order via the trivial Room map a (commutative!) ci-quasigroup  $(G, \circ)$  by  $x \circ y = z$  if and only if  $zx^{-1}zy^{-1} = 1$  if and only if  $x = zy^{-1}z$  if and only if  $y = zx^{-1}z$  if and only if  $z = tx$  where  $t^2 = yx^{-1}$ .

An application of Room maps of groups of even order will be made in a forthcoming paper.

2.3. Let  $(Q, *)$  be a ci-quasigroup, and  $G$  a sharply transitive group of automorphisms of  $(Q, *)$ . Fix  $a \in Q$ . Define a map  $\varphi: G \rightarrow G$  by

$$a^{\varphi(x)} = a^x * a^{x^{-1}} \quad (x \in G).$$

Then  $a^{\varphi(1)} = a * a = a$ , whence  $\varphi(1) = 1$ ; moreover

$$a^{\varphi(x^{-1})} = a^{x^{-1}} * a^x = a^x * a^{x^{-1}} = a^{\varphi(x)}$$

and therefore  $\varphi(x^{-1}) = \varphi(x)$ . Finally,  $Q$  has an odd number of elements, since the operation  $'$  defined by  $x' * x = a$  is an involution fixing only the element  $a$ . Now the order of  $G$  equals that number and thus is odd. Therefore the map  $x \rightarrow x^2$  is a permutation of  $G$ . Now  $a^{\varphi(x)x} = (a^x * a^{x^{-1}})^x = a^{x^2} * a$ , and we get  $\{a^{\varphi(x)x} \mid x \in G\} = a^G$ , from where  $\{\varphi(x)x \mid x \in G\} = G$  follows. Thus  $\varphi$  is a Room map.

If we fix an element  $b = a^t \in Q$  ( $t \in G$ ) instead of  $a$ , then we get a Room map  $\varphi'$  related to  $\varphi$  by  $\varphi'(x) = t\varphi(t^{-1}xt)t^{-1}$ . Therefore,  $\varphi$  and  $\varphi'$  are equivalent by the automorphism  $x \rightarrow txt^{-1}$  of  $G$  (in the sense of the next section).

Because of  $*_{\varphi} = *$ , which one verifies easily, we get distinct Room maps from distinct ci-quasigroups.

2.4. We say,  $G$  is a sharply transitive group of automorphisms of a standardized Room square, if  $G$  is a sharply transitive group of automorphisms of both corresponding ci-quasigroups  $(Q, *)$  and  $(Q, **)$ . Then:

**THEOREM 1.** *A (skew) Room square with a sharply transitive group  $G$  of automorphisms exists if and only if  $G$  has odd order, and  $G$  admits a pair of (skew) orthogonal Room maps. In particular, if there is a strong (skew) Room map of  $G$  then we may construct from it a (skew) Room square.*

**PROOF.** From the preceding, it suffices to prove the following.

**LEMMA 1.** *Let  $\varphi, \psi$  be Room maps of  $G$ .  $*_{\varphi}$  and  $*_{\psi}$  are (skew) orthogonal if and only if  $\varphi$  and  $\psi$  are (skew) orthogonal.*

**PROOF (of the Lemma).** From the definition,  $u *_{\varphi} v = a$ ,  $u *_{\psi} v = b$  if and only if  $x^2 = uv^{-1}$ ,  $a = \varphi(x)xv$ ,  $b = \psi(x)xv$ . Thus every  $x$  leads to at most one solution  $\{u, v\}$ . Since  $x$  and  $x'$  give the same solution only if  $x' = x$  or  $x' = x^{-1}$ ,  $*_{\varphi}$  and  $*_{\psi}$  are orthogonal if and only if  $a = \varphi(x)xv$ ,  $b = \psi(x)xv$  determines  $\{x, x^{-1}\}$  uniquely, or, eliminating  $v$ , if and only if the equation  $\varphi(x)\psi(x)^{-1} = ab^{-1}$  determines  $\{x, x^{-1}\}$  uniquely. But this is equivalent to (6), that is  $\varphi$  and  $\psi$  are orthogonal.

Now suppose  $x *_{\varphi} y = z *_{\psi} t$ ,  $x *_{\psi} y = z *_{\varphi} t$ . Then with  $u^2 = xy^{-1}$ ,  $v^2 = zt^{-1}$  this is equivalent to  $\varphi(u)uy = \psi(v)vt$ ,  $\psi(u)uy = \varphi(v)vt$ , or, eliminating  $t$  and  $y$ , to  $\psi(u)\varphi(u)^{-1} = \varphi(v)\psi(v)^{-1}$ . Now  $*_{\varphi}$  and  $*_{\psi}$  are skew orthogonal if and only if we may conclude  $u = v = 1$ , that is if and only if  $\varphi$  and  $\psi$  are skew orthogonal.

### 3. Equivalence and multipliers

3.1. Let  $G$  be a finite group and  $\text{Aut } G$  the full group of automorphisms of  $G$ .

LEMMA 2. *If  $\varphi$  is a Room map, then, for every  $t \in \text{Aut } G$ , the map  $\varphi^t$ , defined by*

$$\varphi^t(x) = \varphi(x^{t^{-1}})^t$$

*is a Room map. We say  $\varphi^t$  is a shift of  $\varphi$ .*

(1) and (2) are easily verified; (3) follows from the computation

$$\{\varphi^t(x)x \mid x \in G\} = \{\varphi^t(x^t)x^t \mid x \in G\} = \{\varphi(x)x \mid x \in G\} = \{\varphi(x)x \mid x \in G\}^t = G^t = G.$$

Call two Room maps equivalent if one is a shift of the other. Two equivalent Room maps lead to isomorphic ci-quasigroups  $(G, *_\varphi)$  and  $(G, *_\varphi^t)$ ; in fact  $t$  is an isomorphism from  $(G, *_\varphi)$  to  $(G, *_\varphi^t)$ .

PROBLEM. Are there in any group  $G$  inequivalent Room maps leading to isomorphic ci-quasigroups?

3.2. Call an automorphism  $t \in \text{Aut } G$  a multiplier of  $\varphi$ , if  $\varphi^t = \varphi$ . Denote by  $\text{Mult } \varphi$  the set of all multipliers of  $\varphi$ . We show that  $\text{Mult } \varphi$  is a group: If  $s, t \in \text{Mult } \varphi$  then, using the multiplier property and the definition

$$\varphi^{ts^{-1}}(x) = \varphi(x^{s^{-1}t})^{s^{-1}} = \varphi^t(x^s)^{s^{-1}} = \varphi(x^s)^{s^{-1}} = \varphi^s(x^s)^{s^{-1}} = \varphi(x).$$

Therefore  $ts^{-1} \in \text{Mult } \varphi$ , and  $\text{Mult } \varphi$  is indeed a group.

LEMMA 3. *If  $t \in \text{Mult } \varphi$ ,  $a \in G$ , then the map  $(t, a)$  defined by*

$$x^{(t,a)} = x^t a$$

*is an automorphism of  $(G, *_\varphi)$ .*

PROOF.  $u^{(t,a)} *_\varphi v^{(t,a)} = u^t a *_\varphi v^t a = \varphi(x^t) w^t a$  if and only if  $u^t a = x^t w^t a$ ,  $v^t a = (x^t)^{-1} w^t a$ . Since  $t$  is an automorphism of  $G$ , this is equivalent to  $u = x w$ ,  $v = x^{-1} w$ . Thus we have  $u *_\varphi v = \varphi(x) w$  or

$$(u *_\varphi v)^{(t,a)} = (\varphi(x) w)^{(t,a)} = (\varphi(x) w)^t a = \varphi(x)^t w^t a = \varphi^t(x^t) w^t a.$$

But  $t$  is a multiplier of  $\varphi$ , that is  $\varphi^t = \varphi$ . Therefore

$$(u *_\varphi v)^{(t,a)} = \varphi^t(x^t) w^t a = \varphi(x^t) w^t a = u^{(t,a)} *_\varphi v^{(t,a)},$$

and the lemma is proved.

By a straightforward computation we get the product and inversion rules:

$$(s, a)(t, b) = (st, a^t b), \quad (t, a)^{-1} = (t^{-1}, (a^{t^{-1}})^{-1}).$$

Consequently,  $(\text{Mult } \varphi) \times G$  is a split (semidirect) product.

**3.3.** Now we characterize the group  $(\text{Mult } \varphi) \times G$  within the group of all automorphisms of  $(G, *_{\varphi})$ :

**THEOREM 2.** *Let  $G$  be a group of odd order, and  $\varphi$  a Room map of  $G$ . Then the split product  $(\text{Mult } \varphi) \times G$  is the normalizer  $\mathcal{N}(G)$  of  $G$  in the full group of automorphisms of  $(G, *_{\varphi})$ . Moreover, if  $G$  is abelian and  $\varphi = \sigma$  is the trivial Room map, then  $\text{Mult } \varphi = \text{Aut } G$ , and  $(\text{Aut } G) \times G$  is the full group of automorphisms of  $(G, *_{\varphi})$ .*

**PROOF.** (a) We compute easily  $(t, a)^{-1}(1, b)(t, a) = (1, a^{-1}b^t a)$ ; thus the normalizer in question contains the group  $(\text{Mult } \varphi) \times G$ .

(b) Let  $s$  be an element of  $\mathcal{N}(G)$ . Setting  $t = s(1, 1^s)^{-1}$  we have  $1^t = 1^s(1^s)^{-1} = 1$ , and  $t \in \mathcal{N}(G)$ , that is

$$(9) \quad t^{-1} G t = G,$$

$$(10) \quad (x *_{\varphi} y)^t = x^t *_{\varphi} y^t \quad \text{for every } x, y \in G.$$

From (9), for every  $z \in G$ ,  $G$  contains an element  $z'$  with  $t^{-1}(1, z)t = (1, z')$ . We have  $z' = 1^{(1, z^t)} = 1^{t^{-1}(1, z)t} = 1^{(1, z)} = z^t$  for all  $z \in G$ . Thus we get

$$y^t z^t = y^t z' = y^{t(1, z')} = y^{t^{-1}(1, z)t} = y^{(1, z)} = (yz)^t,$$

and  $t$  is an element of  $\text{Aut } G$ .

Finally, since from (10)

$$\varphi^t(x) = \varphi(x^{t^{-1}})^t = (x^{t^{-1}} *_{\varphi} (x^{t^{-1}})^{-1})^t = x *_{\varphi} x^{-1} = \varphi(x),$$

$t$  is in  $\text{Mult } \varphi$ , and we have  $s = t(1, 1^s) = (t, 1^s) \in (\text{Mult } \varphi) \times G$ .

Thus proceeding for every  $s \in \mathcal{N}(G)$  we arrive at  $\mathcal{N}(G) \subseteq (\text{Mult } \varphi) \times G$ , and the first part follows.

(c) If  $\varphi = \sigma$  then trivially  $\text{Mult } \varphi = \text{Aut } G$ . It remains to show that, if  $G$  is abelian, every automorphism of  $(G, *_{\varphi})$  is in  $(\text{Aut } G) \times G$ . We use the additive notation (8a), and obtain  $u *_{\varphi} v = (u+v)/2$ . Thus any automorphism  $s$  of  $(G, *_{\sigma})$  satisfies  $[(x+y)/2]^s = (x^s + y^s)/2$ . Define the permutation  $t$  by  $x^t = x^s - 0^s$ . Then

$$(11) \quad \left(\frac{x+y}{2}\right)^t = \frac{x^t + y^t}{2}, \quad 0^t = 0.$$

$y = 0$  gives  $(x/2)^t = x^t/2$  for every  $x \in G$ , and (11) simplifies to  $(x+y)^t = x^t + y^t$ , that is  $t$  is an automorphism of  $G$ . Thus  $s = t(1, 0^s) = (t, 0^s) \in (\text{Aut } G) \times G$ .

I was not able to modify the proof of the last part to include the nonabelian case. Therefore we may ask:

**PROBLEM.** Is there a group  $G$  (necessarily nonabelian) such that the ci-quasigroup constructed from the trivial Room map possesses an automorphism not contained in  $(\text{Aut } G) \times G$ ?

#### 4. A general lemma for constructing strong room maps

**4.1.** We begin with a very general construction lemma and then specialize more and more to get more concrete results.

**LEMMA 4.** Let  $G$  be a group of odd order, and  $H$  a subset of  $G$  with the property

$$(12) \quad H \cap H^{-1} = \varphi, \quad H \cup H^{-1} = G - \{1\},$$

where  $H^{-1}$  denotes the set of inverses of elements of  $H$ . If  $\pi, \alpha$  are permutations of  $G$  such that

$$(13) \quad 1^\pi = 1^\alpha = 1,$$

$$(14) \quad (x^{-1})^{\alpha\pi} = x^\pi x^2 \quad \text{for every } x \in G,$$

$$(15) \quad H^\alpha = H,$$

then the map  $\varphi$  defined by

$$(16) \quad \varphi(x) = \begin{cases} 1 & \text{if } x = 1, \\ (x^{-1})^\pi x^{-1} & \text{if } x \in H, \\ x^\pi x & \text{if } x \in H^{-1} \end{cases}$$

is a Room map.  $\varphi$  is strong if

$$(17) \quad \{x^\pi x \mid x \in G\} = G.$$

**REMARKS.** (17) is only a convenient sufficient condition for  $\varphi$  to be strong! A set  $H$  satisfying (12) exists in every group of odd order: For  $x \neq 1$ , put one of  $x, x^{-1}$  in  $H$ , the other in  $H^{-1}$ ; we have  $x \neq x^{-1}$  since  $x^2 = 1$  implies  $x = 1$ .

**PROOF** (of Lemma 4). Verifications of (1) and (2) are trivial. To prove (3), consider  $\{\varphi(x)x \mid x \in G\} = \{1\} \cup \{(x^{-1})^\pi \mid x \in H\} \cup \{x^\pi x^2 \mid x \in H^{-1}\}$ . By (13) and (14), this is equal to  $\{1^\pi\} \cup \{(x^{-1})^\pi \mid x \in H\} \cup \{(x^{-1})^{\alpha\pi} \mid x \in H^{-1}\} = (\{1\} \cup H^{-1} \cup H^\alpha)^\pi$ . By (15),  $H^\alpha = H$ , and with (12) the expression reduces to  $G^\pi = G$ . From the definition

of strongness,  $\varphi$  is strong if all  $x^\pi x$  with  $x \in H^{-1}$  are different. But this is guaranteed by (17).

The construction of Lemma 4 is very general, since every Room map  $\varphi$  may be constructed in this way: The permutation  $\pi$ , defined by  $x^\pi = \varphi(x)x^{-1}$  for all  $x$ , and the identity mapping  $\alpha$  satisfies (13)–(15) and the condition (18) below for any  $H$  with (12). ( $\pi$  is a permutation since  $\varphi$  is a Room map and (2) and (3) hold.)

The value of the construction lies in the freedom of  $H$ . If we take for  $\alpha, \pi$  workable permutations, for example automorphisms of  $G$ , which satisfy (13), (14) and (17), then we may try to find a set  $H$  meeting (12) and (15) to obtain a strong Room map.

**4.2.** To analyze the conditions under which (12) and (15) are soluble, denote by  $-1$  the permutation  $x \rightarrow x^{-1}$ . Let  $A$  be the group generated by  $\alpha$  and  $(-1)\alpha(-1)$ . Then  $\varepsilon \in A$  if and only if it has a representation  $\varepsilon = \alpha^{i_1}(-1)\alpha^{i_2}(-1)\dots\alpha^{i_n}(-1)$  where  $n$  is an even integer. Thus we have

$$(-1)\alpha(-1) = \alpha^0(-1)\alpha^{i_1}(-1)\dots\alpha^{i_n}(-1)\alpha^0(-1) \in A,$$

and therefore  $(-1)A = A(-1)$ . Denote by  $x^A$  the set of all  $x^\varepsilon, \varepsilon \in A$ .

**LEMMA 5.** *A set  $H$  satisfying (12) and (15) exists if and only if*

$$(18) \quad x^A \cap x^{(-1)A} = \emptyset \quad \text{for every } x \neq 1,$$

*or, equivalently, if and only if*

$$(18a) \quad x^{-1} \notin x^A \quad \text{for every } x \neq 1.$$

**PROOF.** The equivalence of (18) and (18a) is immediate.

(a) **Necessity:** We have  $1^\alpha = 1, H^\alpha = H$ , and from (12) we get  $H^{(-1)\alpha} = H^{-1}$ . Hence  $H$  is fixed under  $A$ . Let  $H = \bigcup_{x \in X} x^A$  be the partition of  $H$  into  $A$ -orbits. Then  $H^{-1} = \bigcup_{x \in X} x^{A(-1)} = \bigcup_{x \in X} x^{(-1)A}$ . From (12),  $\emptyset = H \cap H^{-1} \supseteq x^A \cap x^{(-1)A}$ , and we obtain (18).

(b) **Sufficiency:** Set  $H_0 = \emptyset$ . Suppose we have already found a subset  $H_i$  of  $G$  with

$$(19) \quad H_i \cap H_i^{-1} = \emptyset, \quad 1 \notin H_i \quad \text{and} \quad H_i^A = H_i.$$

If  $G = \{1\} \cup H_i \cup H_i^{-1}$  we are finished. Otherwise we take an  $x \in G$  with  $x \neq 1, x \notin H_i, x \notin H_i^{-1}$ , and we define  $H_{i+1} = H_i \cup x^A$ .

Clearly,  $H_{i+1}^A = H_{i+1}$ . If  $1 \in H_{i+1}$  then  $1 \in x^A$ , and we have the contradiction  $x = 1$ . If  $z \in H_{i+1} \cap H_{i+1}^{-1}$  then by (18), either  $z \in H_i$  or  $z \in H_i^{-1}$ . If the second holds, replace  $z$  by  $z^{-1}$ ; hence we may assume  $z \in H_i$ . Now by (19)  $z \notin H_i^{-1}$ , thus  $z \in x^A$ , from which we may deduce the contradiction  $x \in H_i$ . Therefore such a  $z$  cannot exist, and we conclude  $H_{i+1} \cap H_{i+1}^{-1} = \emptyset$ .

Repeating this process we finally arrive at a subset  $H = H_m$  satisfying (12) and (15).

**5. Direct constructions for skew room maps**

**5.1.** Let  $R$  be a commutative, associative ring with identity 1. A (not necessarily abelian) group  $G$  is an  $R$ -group provided that  $R$  operates on  $G$ , and the following assertions hold:

$$\begin{aligned}
 1^\alpha &= 1, x^1 = x \quad \text{for every } \alpha \in R, x \in G, \\
 x^{\alpha+\beta} &= x^\alpha x^\beta \quad \text{for every } \alpha, \beta \in R, x \in G, \\
 x^{\alpha\beta} &= (x^\alpha)^\beta \quad \text{for every } \alpha, \beta \in R, x \in G.
 \end{aligned}$$

Note that nothing is required for the operation of  $R$  on products in  $G$ !  
 $R^*$  denotes the group of units of  $R$ .

**LEMMA 6.** *Let  $G$  be an  $R$ -group. Suppose  $R$  contains an element  $\alpha$  such that*

(20) 
$$\alpha - 1, \alpha, \alpha + 1 \in R^*,$$

(21) 
$$\text{there is an odd integer } t \text{ satisfying } \alpha^t = 1.$$

*Then we may construct a set  $H$  satisfying (12) and (15), and for every such set  $H$  the map defined by*

(22) 
$$\varphi(x) = \begin{cases} 1 & \text{if } x = 1, \\ x^\varepsilon & \text{if } x \in H, \\ x^{-\varepsilon} & \text{if } x \in H^{-1} \end{cases}$$

*(where  $\varepsilon = (1 - \alpha)(1 + \alpha)^{-1}$ ) is a skew Room map over  $G$ .*

**PROOF.** (a) We have  $(-1)\alpha(-1) = \alpha$  since  $-1, \alpha \in R$  and  $R$  is commutative. Hence  $A$  is generated by  $\alpha$ . Now, if  $x^{-1} \in x^A$  then  $x^{-1} = x^{\alpha^i}$  for some integer  $i$ . But then  $x^{\alpha^{2i}} = x$ . Since  $\alpha$  has odd order,  $x^{\alpha^t} = x$ , or  $x = x^{-1}$ , whence  $x = 1$ , and (18a) holds. By Lemma 5 we may construct a subset  $H$  of  $G$  with the required properties.

(b) Now we want to apply Lemma 4. (13) is satisfied by hypothesis, and as to (14), with  $\pi = -2(1 + \alpha)^{-1}$ ,  $(x^{-1})^{\alpha\pi} = x^{-\alpha\pi} = x^{+2\alpha(\alpha+1)^{-1}} = x^{-2(1+\alpha)^{-1}+2} = x^\pi x^2$ . Application of Lemma 4 yields the Room map (22) from (16); for

$$x^\pi x = x^{\pi+1} = x^{-2(1+\alpha)^{-1}+1} = x^{(\alpha-1)(1+\alpha)^{-1}} = x^{-\varepsilon},$$

and similarly  $(x^{-1})^\pi x^{-1} = x^\varepsilon$ . Since  $\varepsilon$  is a unit, (17) is valid, and  $\varphi$  is strong.

(c) It remains to show that  $\varphi$  is skew. Indeed, if  $\varphi(x) = \varphi(y)^{-1}$ ,  $x \neq 1$ ,  $y \neq 1$ , then we may assume  $x, y \in H$  since  $\varphi(z^{-1}) = \varphi(z)$  for all  $z$ . But then by (22)  $x^\varepsilon = y^{-\varepsilon}$ , or  $(xy)^\varepsilon = 1$ . Now  $\varepsilon$  is a unit, hence we get  $xy = 1$ , or  $y = x^{-1}$ . But  $x \in H, y = x^{-1} \in H$ , contradicting (12). Thus, (5) holds, and  $\varphi$  is skew.

REMARK. If  $R$  operates faithfully on  $G$ , and if a subset  $H$  of  $G$  satisfying (12) and (15) exists then (21) is valid: For suppose the least positive integer with  $\alpha^t = 1$  be even,  $t = 2s$ . Then  $\alpha^t - 1 = (\alpha^s - 1)(\alpha^s + 1)$ , and  $\alpha^s - 1 \neq 0$ , that is there is an  $x \in G$  with  $x^{\alpha^s - 1} \neq 1$ , since  $R$  is faithful on  $G$ . Taking  $z = x^{\alpha^s - 1}$ , we obtain  $z^{\alpha^s} = z^{-1} \in z^A \cap z^{(-1)A}$ , opposing Lemma 5.

5.2. Now we are able to prove concrete, that is existence, results. There are three important classes of  $R$ -groups  $G$ :

- I.  $G$  is any finite group of exponent  $e$ , and  $R$  is the Ring  $\mathbb{Z}/e\mathbb{Z}$  of integers modulo  $e$ ,
- II.  $G$  is an abelian group, and  $R$  is the ring of all endomorphisms of  $G$ ,
- III.  $G$  is any finite group,  $\alpha$  an automorphism of  $G$  satisfying

$$(23) \quad xx^\alpha = x^\alpha x \quad \text{for every } x \in G,$$

and  $R$  is the ring of all rational expressions in  $\alpha$ , which are well defined (that is the denominator is a permutation).  $R$  operates on  $G$  in an obvious way. We note that  $f(\alpha)$  possesses an inverse if and only if  $f(\alpha)$  is an automorphism. From Lemma 6 we obtain immediately:

THEOREM 3. *Let  $G$  be a group of odd order. If there is an automorphism  $\alpha$  such that*

$$(24) \quad \alpha - 1, \alpha, \alpha - 1 \in \text{Aut } G,$$

$$(23) \quad xx^\alpha = x^\alpha x \quad \text{for every } x \in G,$$

$$(21) \quad \alpha^t = 1 \quad \text{for an odd integer } t,$$

*then  $G$  admits a skew Room map.*

A Fermat prime is a prime of the form  $2^t + 1$ ; from elementary number theory,  $t = 2^k$  follows. Write  $f_k = 2^{2^k} + 1$  if  $f_k$  is prime. The only known Fermat primes are the primes  $f_0 = 3, f_1 = 5, f_2 = 17, f_3 = 257, f_4 = 65537$ . ( $f_5, f_6, f_7$  and  $f_8$  are known to be composite.)

THEOREM 4. *If  $G$  is the elementary abelian group of order  $q = p^i, p$  an odd prime, then, with possible exception of  $p = 3, i = 2$ , and  $p = f_k, i = 1, G$  possesses a skew Room map.*

PROOF. Let  $R = \text{GF}(q)$  be the Galois field of order  $q$ . We may assume that  $G$  be the additive group of  $R$ . If  $\rho$  is a primitive element of  $\text{GF}(q)$ , then, with  $q = 2^s t + 1$  and  $t$  odd,  $\alpha = \rho^{2^s t}$  is an endomorphism of  $G$  of odd order  $t$ .  $\alpha - 1, \alpha, \alpha + 1$  are automorphisms if and only if  $\alpha \neq 0, \pm 1$ . But  $0 \neq \rho^{2^s t}$  for every  $i$ , and  $1 = \rho^{2^s t}, -1 = \rho^{2^s t - 1}$ ; hence  $\alpha \neq 0, \pm 1$  if and only if  $t \neq 1$ . Thus, if  $t \neq 1$  then we may apply Lemma 6 to

obtain the theorem; if  $t = 1$  then  $q = p^i = 2^2 + 1$  and the rest of the theorem follows from the next lemma.

**LEMMA 7.** *If  $p$  is a prime, and  $p^i = 2^s + 1$  then either  $i = 2, p = 3$ , or  $i = 1$  and  $p$  is a Fermat prime  $p = f_k$ .*

**PROOF.** For  $i = 1$ , the lemma is clear; thus let  $i \geq 2$ . From  $p^i = 2^s + 1$  we get

$$(25) \quad p^d - 1 \mid p^i - 1 = 2^s \quad \text{for every } d \text{ which divides } i.$$

In particular,  $p - 1 = 2^r$ , and  $r \mid s$  since  $i \geq 2$ . Hence  $(2^r + 1)^i = 2^s + 1$ , and modulo  $2^{r+1}$  we obtain  $1 + i2^r \equiv 2^s + 1$  or  $2^{r+1} \mid i2^r$ . Thus  $2 \mid i$ , and from (25) we see  $p^2 - 1 = 2^u$ . But  $p = 1 + 2^r$ , and from  $1 + 2^u = p^2 = (1 + 2^r)^2$  we get, after simplification,  $2^{u-r} = 2 + 2^r$ . This equation is only valid if  $r = 1, u = 3$ , and we have  $p = 1 + 2^r = 3$ . Now, if  $i = 2^a b, b$  odd, then by (25)  $3^b - 1$  is a power of 2. But we just had shown that  $b$  had to be even if  $b \geq 2$ . Therefore  $b = 1, i = 2^a$ , and for  $a \geq 2$  we have the contradiction  $5 \mid 2^s$ , for 5 divides  $80 = 3^4 - 1$ , which divides  $3^i - 1$ , which divides  $2^s$ . Hence  $a \leq 1$ , or  $i = 1, 2$ .

**THEOREM 5.** *Let  $G$  be a finite group of odd exponent  $e$ . If  $e$  contains no Fermat prime divisor  $f_k$  then  $G$  admits a skew Room map.*

**PROOF.** Let  $e = \pi p_i^{r_i}$ , where the  $p_i$  are distinct primes, and  $r_i$  are positive integers. Let  $\varepsilon_i$  be a primitive root modulo  $p_i^{r_i}$ , and  $p_i = 2^{s_i} t_i + 1, t_i$  odd. Since  $p_i$  is not Fermat,  $t_i > 1$ . The element  $\alpha_i = \varepsilon_i 2^{s_i}$  has mod  $p_i^{r_i}$  odd order, and, since  $t_i > 1, \alpha_i \neq 0, \pm 1 \pmod{p_i}$ , that is  $\alpha_i - 1, \alpha_i, \alpha_i + 1$  are prime to  $p_i$ .

From the Chinese remainder theorem, we get an integer  $\alpha$  of odd order such that  $\alpha - 1, \alpha, \alpha + 1$  are prime to  $e$ . Applying Lemma 6 with  $R = \mathbb{Z}/e\mathbb{Z}$  the ring of integers modulo  $e$ , the theorem follows.

**REMARK.** Theorem 4 was proved originally by Mullin and Nemeth (1969) for starters of  $G$ , which are equivalent to Room maps by Section 8.

### 6. The product construction

**THEOREM 6.** *Let  $G_0$  be a group of odd order with abelian normal subgroup  $G$  of exponent  $e$ , prime to 3. If both  $G$  and  $G_0/G$  admit a pair of (skew) orthogonal Room maps then a pair of (skew) orthogonal Room maps of  $G_0$  exists. In particular, if both  $G$  and  $G_0/G$  admit strong (skew) Room maps, then so does  $G_0$ .*

PROOF. (a) Let  $T_0$  be a left transversal of  $G_0/G$ ,  $1 \in T_0$ . The map  $'$  defined by  $t^{-1}G = t'G$  ( $t, t' \in T_0$ ) is an involution of  $T_0$  fixing only 1. Select one of  $t, t'$  for every  $\{t, t'\} \subseteq T_0 - \{1\}$  and call the resulting set  $S$ . Then we have

$$T := S \cup S^{-1} \cup \{1\}, \quad S \cap S^{-1} = \emptyset, \quad 1 \notin S, \quad G_0 = TG, \quad |T| = (G_0 : G).$$

The maps

$$t: g \rightarrow g^t = t^{-1}gt \quad (t \in T, g \in G)$$

are automorphisms of  $G$ . Considering  $t$  as a unit in the ring of endomorphisms of  $G$ , exponents such as  $-t^{-1}, 1+t, \dots$  make sense.

We identify  $G_0$  with  $G_0/G \times G$  by

$$(tG, g) = tg \quad (t \in T, g \in G),$$

and one verifies the equation

$$(tG, g)^{-1} = (t^{-1}G, g^{-t^{-1}}).$$

(b) Now we take (skew) orthogonal Room maps  $\varphi, \varphi'$  of  $G$ , and  $\Phi, \Phi'$  of  $G_0/G$ . We may find an integer  $k$  satisfying

$$(k, e) = (k+1, e) = (k^t-1, e) \quad \text{for every odd } f$$

(take, for example,  $k$  with  $\left(\frac{k}{p}\right) = -1$ ,  $k \not\equiv -1 \pmod p$  for every prime  $p$  dividing 3; this is possible since there are  $(p-1)/2 > 1$  quadratic nonresidues mod  $p$ ). Define

$$\omega_t(g) = \begin{cases} \varphi(g) & \text{if } t = 1, \\ g^{kt^{-1}} & \text{if } t \in S, \\ g^{-k} & \text{if } t \in S^{-1}, \end{cases}$$

$$\varphi_0(tG, g) = (\Phi(tG), \omega_t(g)),$$

$$\varphi'_0(tG, g) = \begin{cases} (G, \varphi'(g)) & \text{if } t = 1, \\ (\Phi'(tG), 1) & \text{if } t \in S \cup S^{-1}. \end{cases}$$

We verify easily

$$\varphi_0(g) = \varphi(g), \quad \varphi'_0(g) = \varphi'(g) \quad \text{if } g \in G,$$

$$\varphi_0(x)G = \varphi_0(xG), \quad \varphi'_0(x)G = \varphi'_0(xG) \quad \text{if } x \in G,$$

and a straightforward proof yields:  $\varphi'_0$  is a Room map, and is trivial if and only if both  $\varphi'$  and  $\Phi'$  are trivial.

(c) To prove that  $\varphi_0$  is a Room map first note that

$$(26) \quad \omega_{t^{-1}}(g^{-t^{-1}}) = \omega_t(g).$$

For  $t = 1$ , the left side equals  $\varphi(g^{-1}) = \varphi(g) = \omega_t(g)$ . For  $t \in S$  we have

$$\omega_{t^{-1}}(g^{-t^{-1}}) = (g^{-t^{-1}})^{-k} = g^{kt^{-1}} = \omega_t(g),$$

and for  $t \in S^{-1}$ :  $\omega_{t^{-1}}(g^{-t^{-1}}) = (g^{-t^{-1}})^{kt} = g^{-k} = \omega_t(g)$ .

Now  $\varphi_0(1) = \varphi(1) = 1$ , and by (26), if

$$\begin{aligned} x = (tG, g): \varphi_0(x^{-1}) &= \varphi_0(t^{-1}G, g^{-t^{-1}}) = (\Phi(t^{-1}G), \omega_{t^{-1}}(g^{-t^{-1}})) \\ &= (\Phi(tG), \omega_t(g)) = \varphi_0(tG, g) = \varphi_0(x). \end{aligned}$$

Therefore (1) and (2) are valid.

Finally suppose  $\varphi_0(x)x = \varphi_0(y)y$ . In the factor group we have

$$\Phi(xG)xG = \varphi_0(x)GxG = \varphi_0(y)GyG = \Phi(yG)yG,$$

and, since  $\Phi$  is a Room map,  $xG = yG$ . Suppose  $xG = yG = tG$ ,  $\Phi(tG) = uG$ , where  $t, u \in T$ , and  $x = (tG, g)$ ,  $y = (tG, h)$ . Then

$$u\omega_t(g)tg = (\Phi(tg), \omega_t(g))tg = \varphi_0(tG, g)tg = \varphi_0(x)x,$$

and similarly,  $u\omega_t(h)th = \varphi_0(y)y$ , whence  $u\omega_t(g)tg = u\omega_t(h)th$ , or:

$$\omega_t(g)g^{t^{-1}} = \omega_t(h)h^{t^{-1}}.$$

If  $t = 1$  then we obtain  $\varphi(g)g = \varphi(h)h$ , or  $g = h$  since  $\varphi$  is a Room map. If  $t \in S$  then  $g^{kt^{-1}}g^{t^{-1}} = h^{kt^{-1}}h^{t^{-1}}$ , or  $g^{k+1} = h^{k+1}$ , or  $g = h$  since  $(k+1, e) = 1$ . If  $t \in S^{-1}$  then  $g^{-k}g^{t^{-1}} = h^{-k}h^{t^{-1}}$ . Setting  $m = gh^{-1}$  we obtain  $m = m^{kt}$  (since  $G$  is abelian). Now the order  $f$  of  $t$  divides the order of  $G_0$  and thus is odd. By hypothesis,  $(k^f - 1, e) = 1$ , and from  $m = m^{k^f} = m^{k^f}$ , or  $m^{k^f-1} = 1$  we get  $m = 1$ , that is  $g = h$ . In every case we arrived at  $g = h$ , thus  $x = y$ . Therefore all the  $\varphi_0(x)x$  are distinct, and (3) follows. Thus  $\varphi_0$  is a Room map.

(d) To prove orthogonality we have to show that

$$\varphi_0(x)\varphi'_0(x)^{-1} = \varphi_0(y)\varphi'_0(y)^{-1}$$

is possible only for  $x = y$  or  $x = y^{-1}$ . Since (2) is valid we may assume  $x, y \in G \cup S^{-1}G$ . In the factor group we get  $\Phi(xG)\Phi'(xG)^{-1} = \Phi(yG)\Phi'(yG)^{-1}$ , whence  $xG = yG$  since  $\Phi$  and  $\Phi'$  are orthogonal. Now if  $x, y \in G$  then

$$\varphi(x)\varphi'(x)^{-1} = \varphi_0(x)\varphi'_0(x)^{-1} = \varphi_0(y)\varphi'_0(y)^{-1} = \varphi(y)\varphi'(y)^{-1},$$

and  $x = y$  or  $x = y^{-1}$  from the orthogonality of  $\varphi, \varphi'$ . And if  $x, y \in tG$ ,  $t \in S^{-1}$ ,  $x = (tG, g)$ ,  $y = (tG, h)$ ,  $\Phi(tG) = uG$ ,  $\Phi'(tG) = u'$  we have

$$\begin{aligned} \varphi_0(x)\varphi'_0(x)^{-1} &= \varphi_0(tG, g)\varphi'_0(tG, g)^{-1} = (\Phi(tG), \omega_t(g))(\Phi'(tG), 1)^{-1} \\ &= u\omega_t(g)u'^{-1} = ug^{-k}u'^{-1}, \end{aligned}$$

and similarly  $\varphi_0(y)\varphi'_0(y)^{-1} = uh^{-k}u'^{-1}$ . Thus we have

$$ug^{-k}u'^{-1} = uh^{-k}u'^{-1}g^{-k} = h^{-k},$$

and  $g = h$  because of  $(k, e) = 1$ . Therefore  $x = y$ .

(e) Now suppose  $\varphi, \varphi'$  and  $\Phi, \Phi'$  are skew orthogonal. From

$$\varphi_0(x)\varphi'_0(x)^{-1} = \varphi'_0(y)\varphi_0(y)^{-1}$$

we get from the skew orthogonality in the factor group  $xG = yG = G$ , that is  $x, y \in G$ , and then  $x = y = 1$  since  $\varphi$  and  $\varphi'$  are skew orthogonal in  $G$ . Thus  $\varphi_0$  and  $\varphi'_0$  are skew orthogonal.

From the proof, we restate the simplest part as

**COROLLARY.** *If  $G_1$  is a group of odd order, and  $G_2$  is an abelian group of order prime to 2.3, and if  $\varphi_1, \varphi'_1$  resp.  $\varphi_2, \varphi'_2$  are (skew) orthogonal Room maps of  $G_1$  resp.  $G_2$  then the maps  $\varphi, \varphi'$  of the direct product  $G_1 \times G_2$  defined by*

$$\varphi(a, x) = \begin{cases} (1, \varphi_2(x)) & \text{if } a = 1, \\ (\varphi_1(a), 1) & \text{if } a \neq 1, \end{cases}$$

$$\varphi'(a, x) = \begin{cases} (1, \varphi'_2(x)) & \text{if } a = 1, \\ (\varphi'_1(a), x^2) & \text{if } a \in H, \\ (\varphi'_1(a), x^{-2}) & \text{if } a \in H^{-1}, \end{cases}$$

where  $H$  is a set with  $H \cap H^{-1} = \emptyset$ ,  $H \cup H^{-1} = G_1 - \{1\}$ , are a pair of (skew) orthogonal Room maps.

**PROBLEM.** Is there a product construction if  $G$  is nonabelian or if the order of  $G$  is not prime to 3?

**6.2.** Now we use the theorem to prove

**THEOREM 7.** *Every group  $G$  of order prime to 2.3.5 admits a skew Room map.*

**PROOF.**  $G$  has odd order, and thus is solvable. Now any minimal normal subgroup  $H$  of  $G$  is elementary abelian, and has an order prime to 2.3.5. For groups of Fermat prime order  $\neq 3, 5$ , Chong (1972) proves the existence of skew strong starters which are equivalent to skew adders for the patterned starter, and by Theorem 9 (Section 8) these groups admit skew Room maps. For the other elementary abelian groups of order prime to 2.3.5, Theorem 4 guarantees the existence of a skew Room map. Thus  $H$  admits a skew Room map.

Induction on the order of  $G$  (beginning with the trivial group of order 1 where  $\sigma$  is a skew Room map) proves the theorem.

We may slightly extend Theorem 7:

**THEOREM 7a.** *Let  $G$  be a group of odd order. Suppose  $G$  possesses a chain*

$$(27) \quad G = G_0 \geq G_1 \geq \dots \geq G_k = 1$$

*with normal subgroups  $G_i$  of  $G$  and abelian factors  $G_i/G_{i+1}$  of an order prime to 3 (for  $i \geq 1$ ; for  $i = 0$  nothing is required). Then, if all factors  $G_i/G_{i+1}$  (including  $i = 0$ ) possess strong (skew) Room maps,  $G$  admits a strong (skew) map, too.*

**PROOF.** The theorem is trivial if  $k = 1$ . Now proceed by induction on  $k$ . If  $G$  satisfies the stated conditions then  $G/G_{k-1}$  does, but with  $k-1$  instead of  $k$ . By induction,  $G/G_{k-1}$  admits a strong (skew) Room map. Since  $G_{k-1} = G_{k-1}/G_k$  possesses a strong (skew) Room map, we may apply Theorem 6 yielding a strong (skew) Room map of  $G$ .

**REMARK.** Every solvable group possesses a chain (27) with normal subgroups  $G_i$  of  $G$  and abelian factors  $G_i/G_{i+1}$  for all  $i$ .

### 7. A nonexistence theorem for skew room maps

**LEMMA 8.** *Let  $G$  be a group of odd order, and  $H$  a set with  $H \cap H^{-1} = \emptyset$ ,  $H \cup H^{-1} = G - \{1\}$ . If  $\varphi$  is a skew Room map of  $G$ , then*

$$\{\varphi(x), \varphi(x)^{-1} \mid x \in H\} = G - \{1\},$$

*and every element is obtained exactly once on the left.*

**PROOF.** Since  $\varphi$  is strong, all  $\varphi(x)$ , where  $x$  runs over  $H$ , are distinct; the same holds for the  $\varphi(x)^{-1}$ . But  $\varphi$  is skew, and therefore every  $\varphi(x)$  is distinct from every  $\varphi(x')^{-1}$  ( $x' \neq x \neq 1$ ). Thus  $\{\varphi(x), \varphi(x)^{-1} \mid x \in H\}$  is a set of  $|H| + |H| = |G| - 1$  elements. But since  $\varphi$  is strong and  $\varphi(1) = 1$ , the element 1 is not in that set, and the assertion follows.

Now let  $\varphi$  be a Room map of  $G$ , and  $\tau: G \rightarrow \mathbb{Z}/n\mathbb{Z}$  a homomorphism of  $G$  onto  $\mathbb{Z}/n\mathbb{Z}$ . Then the kernel  $\text{Ker } \tau$  has order  $|G|/n$ . From (3), counting multiplicities,

$$\{x^\tau \mid x \in G\} = G^\tau = \{\varphi(x)^\tau + x^\tau \mid x \in G\}.$$

Summing up the squares of the elements we obtain ( $x$  runs over  $G$ ):

$$\sum (x^\tau)^2 \equiv \sum (\varphi(x)^\tau + x^\tau)^2 \equiv \sum (\varphi(x)^\tau)^2 + 2 \sum \varphi(x)^\tau x^\tau + \sum (x^\tau)^2 \pmod{n},$$

or

$$\sum (\varphi(x)^\tau)^2 \equiv -2 \sum \varphi(x)^\tau x^\tau \equiv -\sum \varphi(x)^\tau x^\tau - \sum \varphi(x^{-1})^\tau (x^{-1})^\tau \equiv 0 \pmod{n},$$

since

$$\varphi(x^{-1})^\tau (x^{-1})^\tau = \varphi(x)^\tau (x^{-1})^\tau = \varphi(x)^\tau (-x^\tau) = -\varphi(x)^\tau x^\tau.$$

Therefore, if  $\varphi$  is skew,

$$0 \equiv 2 \sum (\varphi(x)^r)^2 \equiv \sum (\varphi(x)^r)^2 + \sum (-\varphi(x)^r)^2 \equiv 2 \sum (x^r)^2 \pmod{n},$$

since  $-\varphi(x)^r = (\varphi(x)^{-1})^r$ ,  $\varphi(1)^r = 0$ , and the preceding lemma. But

$$\sum (x^r)^2 \equiv |G|n^{-1} \cdot \sum_{i=0}^{n-1} i^2 \equiv |G|n^{-1} \cdot \frac{n(n-1)(2n-1)}{6} \pmod{n}.$$

Thus

$$|G| \cdot \frac{(n-1)(2n-1)}{3} \equiv 0 \pmod{n},$$

or

$$(28) \quad 3 \mid |G|n^{-1}(n-1)(2n-1).$$

From this we deduce

**THEOREM 8.** *Suppose a group  $G$  of odd order contains a normal subgroup  $K$  of order prime to 3 with cyclic factor group of order divisible by 3. Then  $G$  admits no skew Room map.*

**COROLLARY.** *An abelian group of odd order possessing a nontrivial cyclic 3-Sylow-group admits no skew Room map.*

**PROOF.** Suppose  $G$  admits a skew Room map. By hypothesis,  $G/K$  is cyclic, isomorphic to  $\mathbf{Z}/n\mathbf{Z}$ , say. Therefore a homomorphism from  $G$  onto  $\mathbf{Z}/n\mathbf{Z}$  exists, and (28) is valid. By assumption,  $n \equiv 0 \pmod{3}$ . (28) yields  $3 \mid |G|n^{-1}$ . But  $|G|n^{-1}$  is the order of  $K$  and prime to 3, a contradiction.

**REMARK.** The corollary was proved in terms of skew strong starters (compare with Section 8) in Wallis and Mullin (1973).

## 8. Room maps and starters

**8.1.** For Room squares with a sharply transitive group of automorphisms another description is available: the starter-approach. Starters are widely used in the literature on Room squares and one-factorizations of complete graphs; see for example Mullin and Nemeth (1969), Wallis *et al.* (1972), Wallis (1973b), Wallis and Mullin (1973) and Anderson (1974). We derive a one-to-one correspondence between starters and Room maps.

Let  $G$  be a group of odd order.

A *starter* for  $G$  is a partition  $X = \{\{x_i, y_i\} \mid i \in I\}$  of  $G - \{1\}$  into 2-sets such that  $\{x_i y_i^{-1} \mid i \in I\} \cup \{y_i x_i^{-1} \mid i \in I\} = G - \{1\}$ .

A *right adder* for  $X$  is a subset  $A = \{a_i \mid i \in I\}$  of  $G - \{1\}$  such that all  $a_i$  are distinct, and  $\{x_i a_i \mid i \in I\} \cup \{y_i a_i \mid i \in I\} = G - \{1\}$ ; similarly, a *left adder* for  $X$  is a subset  $A = \{a_i \mid i \in I\}$  of  $G - \{1\}$  such that all  $a_i$  are distinct, and

$$\{a_i x_i \mid i \in I\} \cup \{a_i y_i \mid i \in I\} = G - \{1\}.$$

The adder  $A$  is *skew* if and only if  $\{a_i, a_i^{-1} \mid i \in I\} = G - \{1\}$ .

Every group of odd order admits a starter  $X_0 = \{\{x, x^{-1}\} \mid x \in H\}$ , where  $H$  is a subset of  $G$  with  $H \cap H^{-1} = \emptyset$ ,  $H \cup H^{-1} = G - \{1\}$ . This starter is called the *patterned starter*.

**THEOREM 9.** *Let  $G$  be a finite group of odd order,  $H$  a subset of  $G$  with  $H \cap H^{-1} = \emptyset$ ,  $H \cup H^{-1} = G - \{1\}$ .*

1. *If  $\varphi$  is a Room map of  $G$  then*

$$X_\varphi = \{\{x\varphi(x)^{-1}, x^{-1}\varphi(x)^{-1}\} \mid x \in H\}$$

*is a starter for  $G$ . If  $\varphi'$  is a Room map (skew) orthogonal to  $\varphi$  then*

$$A_{\varphi, \varphi'} = \{\varphi(x)\varphi'(x)^{-1} \mid x \in H\}$$

*is a right (skew) adder for  $X_\varphi$ . In particular,  $X$  is the patterned starter, and if  $\varphi$  is a strong (skew) Room map then*

$$A_\varphi = \{\varphi(x)^{-1} \mid x \in H\}$$

*is a right (skew) adder for the patterned starter.*

2. *If  $X = \{\{x_i, y_i\} \mid i \in I\}$  is a starter for  $G$  then the map  $\varphi_X$  defined by*

$$\varphi_X(1) = 1, \quad \varphi_X(t_i) = \varphi_X(t_i^{-1}) = x_i^{-1} t_i = y_i^{-1} t_i^{-1},$$

*where  $t_i^2 = x_i y_i^{-1}$  is a Room map. If  $A = \{a_i \mid i \in I\}$  is a right (skew) adder for  $X$  then the map  $\varphi_{X,A}$  defined by*

$$\varphi_{X,A}(1) = 1, \quad \varphi_{X,A}(t_i) = \varphi_{X,A}(t_i^{-1}) = a_i^{-1} x_i^{-1} t_i = a_i^{-1} y_i^{-1} t_i^{-1},$$

*where  $t_i^2 = x_i y_i^{-1}$  is a Room map (skew) orthogonal to  $\varphi_X$ .*

**PROOF.** Since  $G$  has odd order the map  $x \rightarrow x^2$  is a permutation; so the  $t_i$ 's are well defined. By definition of a starter,  $\{t_i, t_i^{-1} \mid i \in I\} = G - \{1\}$ , and therefore  $\varphi_X$  and  $\varphi_{X,A}$  are well defined. The verification of the starter resp. Room map axioms is then straightforward and will be omitted.

**8.2.** During preparation of this paper I received a paper of Gross and Leonard (1975) on adders for the patterned starter in nonabelian groups proving some of the results above. They work with left adders for the patterned starter which are related to Room maps by Theorem 9 via the following.

**LEMMA 9.** *If  $A = \{a_i | i \in I\}$  is a right adder for the patterned starter then  $A' = \{a_i^{-1} | i \in I\}$  is a left adder for the patterned starter, and conversely.*

**PROOF.** Let the patterned starter be  $X = \{\{x_i, x_i^{-1}\} | i \in I\}$ . Then  $A$  is a right adder for  $X$  if and only if  $\{x_i a_i, x_i^{-1} a_i | i \in I\} = G - \{1\}$ , or, taking inverses, if and only if  $\{a_i^{-1} x_i^{-1}, a_i^{-1} x_i | i \in I\} = G - \{1\}$ , that is if and only if  $A'$  is a left adder for  $X$ .

**COROLLARY.** *To every strong Room map  $\varphi$  a left adder of the patterned starter  $\{\{x, x^{-1}\} | x \in H\}$  is associated by  $A' = \{\varphi(x) | x \in H\}$ ; conversely, every left adder of the patterned starter corresponds to a strong Room map.*

By the corollary, Theorem 1 of Gross and Leonard (1975), together with their Theorem 4 is, if  $H$  is abelian, equivalent to the special case of Theorem 6 of this paper, where the pairs of orthogonal Room maps are composed of the trivial map and a strong Room map, each.

By Lemma 9, the existence of right adders is equivalent to the existence of left adders (for the patterned starter only!); in particular Theorem 2 of Gross and Leonard (1975) may be replaced by the 'dual' of Theorem 1, giving an existence criterion for right adders in extensions of abelian groups not depending on the factor system.

Theorem 6 of Gross and Leonard (1975) is equivalent to Theorem 7 here.

## References

- B. A. Anderson (1974), 'A class of starter induced 1-factorizations', in *Graphs and combinatorics* (Lecture Notes in Mathematics 406, Springer, New York and Berlin), 180–185.
- R. H. Bruck (1963), 'What is a loop?', *Studies in modern algebra* (Math. Association of America), 59–99.
- B. C. Chong (1972), *Existence and construction of Room squares by the theory of loop and application to experimental design* (M.Sc. thesis, University of Singapore).
- K. B. Gross and P. A. Leonard (1975), 'Adders for the patterned starter in nonabelian groups', *J. Austral. Math. Soc.* **21**, 185–193.
- R. C. Mullin and E. Nemeth (1969), 'An existence theorem for Room squares', *Canad. Math. Bull.* **12**, 493–497.
- W. D. Wallis (1973a), 'A Room square of side 257', *Proc. of the Fourth Southeastern Conference on Combinatorics, Graph Theory and Computing*, 533.
- W. D. Wallis (1973b), 'On one-factorizations of complete graphs', *J. Austral. Math. Soc.* **16**, 167–171.

- W. D. Wallis (1974), 'Solution of the Room square existence problem', *J. Combinatorial Theory A*, **17**, 379–383.
- W. D. Wallis and R. C. Mullin (1973), 'Recent advances on complementary and skew Room squares', *Proc. of the Fourth Southeastern Conference on Combinatorics, Graph Theory and Computing*, 521–532.
- W. D. Wallis, A. P. Street and J. S. Wallis (1972), *Combinatorics: Room squares, sum-free sets, Hadamard matrices* (Lecture Notes in Mathematics 292, Springer, New York and Berlin).

Fachbereich Mathematik  
Technische Universität  
D-1000 Berlin 12  
West Germany