Note di Matematica
Note Mat. 29 (2009), suppl. n. 1, 115-120
ISSN 1123-2536, e-ISSN 1590-0932
DOI 10.1285/i15900932v29n1supplp115
http://siba-ese.unisalento.it,

Latin Squares, Homologies and Euler's Conjecture

Christoph Hering [i]
Institute of Mathematics of the University of Tübingen, Auf der Morgenstelle 10, 72076 Tübingen, Germany
hering@uni-tuebingen.de

Andreas Krebs
Wilhelm-Schickard-Institute, University of Tübingen, Sand 13, 72076 Tübingen, Germany
krebs@informatik.uni-tuebingen.de

Abstract. We construct pairs of orthogonal Latin Squares of order n by means of suitable orthomorphisms of the cyclic group of order $n-1$. These pairs always have $n-3$ confluent common transversals. They lead to partial planes of order n with $5n-2$ lines and 5 complete points. Also, we provide an easy construction of counter examples to Euler's conjecture.

Keywords: Latin Squares, Orthomorphisms, Projective Planes

MSC 2000 classification: 51E15, 05B15

1 Introduction

In this paper we construct pairs of orthogonal Latin Squares of a given order n from orthomorphisms of cyclic groups of order $n-1$. The set of common transversals of such pairs always contains a subset consisting of $n-3$ confluent elements. Therefore they lead to partial planes of order n with $5n-2$ lines and 5 complete points. In this respect they behave differently, e.g. for $n=10$, from the pairs of orthogonal Latin Squares determined by E.T. Parker and J. W. Brown [1-3].

Our setup allows to easily find counter examples against Euler's conjecture on Latin Squares "by hand", that is without the help of computers.

2 Definitions and elementary results

In this section we will present basic properties of orthomorphisms of groups and Latin Squares. Also, we introduce the notion of an affine partial plane (Definition 6).

[i] To Norman L. Johnson, on the Occasion of his 70th Birthday

1 Definition (Commutator)**.** Let G be a group. For every map s of G into itself $\overline{s}$ is defined by $g^{\overline{s}} = g^{-1}g^s$ for all $g \in G$.

2 Definition (Orthomorphism)**.** An orthomorphism s of a group G is a permutation of (the set of elements of) G such that the commutator $\overline{s}$ is also a permutation of G.

3 Lemma. *If s is an orthomorphism of a finite group, then s^{-1} is also an orthomorphism.*

Proof. Let s be an orthomorphism and $x, y \in G$. We assume $x^{-1}x^{s^{-1}} = y^{-1}y^{s^{-1}}$; then there are $x', y' \in G$ with $x'^s = x$ and $y'^s = y$. This implies $(x'^s)^{-1}x' = (y'^s)^{-1}y'$, and reversing sides we get $y'^{-1}y'^s = x'^{-1}x'^s$ implying $x' = y'$ and hence $x = y$. QED

4 Lemma. *Let G be a group, s an orthomorphism of G and $h \in G$. Let t be the map of G into G defined by*

$$g^t = g^s h$$

for all $g \in G$. Then t is a permutation of G which fixes exactly one point. In particular, s has exactly one fixed point.

Proof. Of course t is a permutation, because s is a permutation. If g is a fixed point of t, then $g = g^t = g^s h$ and hence $g^{\overline{s}} = g^{-1}g^s = h^{-1}$. By Definition 2, for any given h we have exactly one solution g. QED

5 Remark. Thus an orthomorphism of a group G is a transversal of the set of right translations of G. (This set of course is a sharply transitive set of permutations of G, and therefore in the finite case a Latin Square).

Our notation is compatible with Dembowski [4], also compare Krebs [7].

Sets of permutations

Let n be a natural number, Ω a set of cardinality n and $\mathfrak{X}$ a subset of the symmetric group of Ω. Then $\mathfrak{X}$ is a Latin Square if for any two different elements $x, y \in \mathfrak{X}$ the quotient $x^{-1}y$ is fixed point free, and $|\mathfrak{X}| = n$. Two Latin Squares $\mathfrak{X}$ and $\mathfrak{Y}$ are orthogonal if for any $x \in \mathfrak{X}$ and $y \in \mathfrak{Y}$ the quotient $x^{-1}y$ has exactly one fixed point. (See Dembowski [4, p. 140ff].)

6 Definition (Affine Partial Plane of Order n)**.** A subset $\mathfrak{A}$ of the symmetric group S_Ω is called an affine partial plane of order n = $|\Omega|$ if for any two different elements $x, y \in \mathfrak{A}$ the quotient $x^{-1}y$ has at most one fixed point.

3 Pairs of orthogonal Latin Squares constructed from orthomorphisms of cyclic groups

In this section we will reveal some relations between orthomorphisms of groups and Latin Squares. Starting from an orthomorphism of the cyclic group of order $n-1$, we construct a Latin Square of order n. Then we produce a sufficient condition for this Latin Square to be orthogonal to its inverse. Finally, we construct transversals of the resulting pairs of Latin Squares.

Let n be a natural number, $n \geq 4$, and $\mathbb{Z}_{n-1} = \mathbb{Z}/(n-1)\mathbb{Z}$. We let s be an orthomorphism of the additive group of $\mathbb{Z}_{n-1}$ which leaves invariant 0, and t be the permutation of $\mathbb{Z}_{n-1}$ mapping x to $x+1$ for all $x \in \mathbb{Z}_{n-1}$.

Now we join a further element ∞ to $\mathbb{Z}_{n-1}$ and define permutations S and T of $K := \mathbb{Z}_{n-1} \cup \{\infty\}$ by

$$x^S = \begin{cases} 0 & \text{iff } x = \infty, \\ \infty & \text{iff } x = 0, \\ x^s & \text{otherwise.} \end{cases} \qquad x^T = \begin{cases} \infty & \text{iff } x = \infty, \\ x^t & \text{otherwise.} \end{cases}$$

With these choices we can show that:

7 Lemma. *The set*

$$\mathfrak{A} = \{T\} \cup \{(TS)^X \mid X \in \langle T \rangle\}$$

of permutations of K leads to a Latin Square.

Proof. Note that the group $\langle T \rangle$ acts on $\mathfrak{A}$, leaving T invariant.

We have to show that any quotient of two different elements in $\mathfrak{A}$ has no fixed points, i.e. for all $A, B \in \mathfrak{A}$, such that $A \neq B$, the permutation $A^{-1}B$ has no fixed point. As AB and BA have the same number of fixed points, we can assume that $B \neq T$.

Assume $A = T$ and $B = (TS)^X$, for $X \in \langle T \rangle$. Clearly $A^{-1}B = T^{-1}(TS)^X = T^{-1}T^X S^X = S^X$ has a fixed point iff S has a fixed point. But S has no fixed points, because s being an orthomorphism of $\mathbb{Z}_{n-1}$ has exactly one fixed point in $\mathbb{Z}_{n-1}$, which is 0, and $0^S = \infty$.

Now, because of the action of $\langle T \rangle$, we can assume w.l.o.g. that $A = TS$ and $B = (TS)^X$ for some $X \in \langle T \rangle$, where $X \neq 1$. Then $A^{-1}B = (TS)^{-1}(TS)^X = S^{-1}T^{-1}T^X S^X = S^{-1}S^X$. If $S^{-1}S^X$ has a fixed point, then also $S^X S^{-1}$ has a fixed point. Assume that this is the case.

Assume $\infty^{S^X S^{-1}} = \infty$, then $0 = \infty^S = \infty^{X^{-1}SX} = \infty^{SX} = 0^X$, because $X \in \langle T \rangle$ fixes ∞. But this implies that X is the identity, contrary to our assumption $X \neq 1$. Equally, if we assume that $0^{S^X S^{-1}} = 0$, then $0^{X^{-1}} = 0^{SX^{-1}S^{-1}} = \infty^{X^{-1}S^{-1}} = \infty^{S^{-1}} = 0$, also implying that X is the identity.

We now let $0 \neq i \in \mathbb{Z}_{n-1}$, and assume $i^{SXS^{-1}} = i \iff i^{X^{-1}S} = i^{SX^{-1}}$. There is a $j \in \mathbb{Z}_{n-1}, j \neq 0$, such that $X = T^j$. If $j = i$ then $i = i^{X^{-1}SXS^{-1}} = 0^{SXS^{-1}} = \infty^{XS^{-1}} = \infty^{S^{-1}} = 0 \neq i$, a contradiction. Assume that $j \neq i$. Then $(i-j)^S = i^S - j$ implies $(i-j)^s = i^s - j \iff (i-j)^s - (i-j) = i^s - i$, but since s is an orthomorphism this implies $j = 0$, again a contradiction.

Our computations also prove that $|\mathfrak{A}| = n$. QED

With the following property we can generate a pair of orthogonal Latin squares.

Property $(*)$**.** Let s be an orthomorphism of $\mathbb{Z}_{n-1}$ that fixes 0 and assume that $j^{s^2} - j \neq -2$ for $1 \leq j \leq n-1$. Let $x = (-2)^{\overline{s}^{-1}}$. Assume furthermore that the function

$$F(j) = j - (j^{\overline{s}} + 2)^{\overline{s^{-1}}^{-1}}$$

induces a bijective map of $\mathbb{Z}_{n-1}\backslash\{0, x\}$ onto $\mathbb{Z}_{n-1}\backslash\{0, 2\}$. Then we say s has Property $(*)$.

By Lemma 7 we know that $\mathfrak{A}$ and $\mathfrak{A}^{-1}$ are Latin squares. In the following theorem we show that they are actually orthogonal if the orthomorphism s has Property $(*)$.

8 Theorem. *If the orthomorphism s has Property $(*)$,*

(1) then $\mathfrak{A}$ is orthogonal to $\mathfrak{A}^{-1}$,

(2) and $\mathfrak{A} \cup \mathfrak{A}^{-1} \cup \langle T \rangle$ forms an affine partial plane.

Proof. For (1) we have to show that the quotient of an element of $\mathfrak{A}$ and an element of $\mathfrak{A}^{-1}$, that is a product of the form AB where $A, B \in \mathfrak{A}$, has exactly one fixed point. If $A = B = T$, this is trivial.

As AB and BA have the same number of fixed points, we can assume $A \neq T$. Again, $\langle T \rangle$ is acting on $\mathfrak{A}$, hence w.l.o.g. $A = (TS)^T = ST$.

For $B = T$ we obtain $AB = ST^2$. Then $\infty^{ST^2} = 0^{T^2} \neq \infty$ and $0^{ST^2} = \infty^{T^2} = \infty \neq 0$. Let $0 \neq j \in \mathbb{Z}_{n-1}$ be a fixed point, then $j^{ST^2} = j \iff j^s + 2 = j$ and $j^s - j = -2 \iff j^{\overline{s}} = -2$. This has exactly one solution, because s is an orthomorphism.

Finally, assume $B = (TS)^X$ for $X = T^i \in \langle T \rangle$, with $1 \leq i \leq n-1$, so that $AB = ST(X^{-1}TSX) = ST^2X^{-1}SX$.

Assume at first that ∞ is a fixed point. Then

$$\infty = \infty^{ST^2X^{-1}SX} \Rightarrow \infty^{X^{-1}S^{-1}} = \infty^{ST^2X^{-1}} \Rightarrow 0 = 0^{T^2X^{-1}}.$$

Hence $X = T^2$ and $AB = S^2X = S^2T^2$. Now $0^{AB} = 0^{S^2T^2} = 0^{T^2} \neq 0$, as $n \geq 4$. If $0 \neq j \in \mathbb{Z}_{n-1}$, where j is a fixed point, then $j = j^{AB} = j^{S^2T^2} \Rightarrow j^{S^2} =$

$j^{T^{-2}} \Rightarrow j^{s^2} = j-2$ and $j^{s^2} - j = -2$, a contradiction to $(*)$. So in this case, ∞ is the only fixed point of AB.

Assume now that 0 is a fixed point. Then $0 = 0^{AB} = 0^{ST^2X^{-1}SX} = \infty^{T^2X^{-1}SX} = \infty^{SX} = 0^X$, so that X is the identity and $AB = ST^2S$. By the above ∞ is not a fixed point of AB. If $0 \neq j \in \mathbb{Z}_{n-1}$ is a fixed point then $j^{ST^2S} = j \Rightarrow j^S = j^{S^{-1}} - 2 \Rightarrow j^s - j^{s^{-1}} = -2 \Rightarrow k^{s^2} - k = -2$ for $k = j^{s^{-1}}$, contradicting $(*)$. So in this case 0 is the only fixed point of AB.

Let $0 \neq j \in \mathbb{Z}_{n-1}$ be a fixed point of AB. Then $j^{ST^2X^{-1}SX} = j \iff j^{ST^2X^{-1}} = j^{X^{-1}S^{-1}}$. It follows $j^S + 2 - i = (j-i)^{S^{-1}}$. Suppose $j = i$, then $j^S + 2 - i = (j-i)^{S^{-1}} \Rightarrow j^S + 2 - i = \infty$, a contradiction.

So $j \neq i$ and

$$j^S + 2 - i = (j-i)^{S^{-1}} \Rightarrow j^S + 2 - j = (j-i)^{S^{-1}} - (j-i).$$

Since $j - i \neq 0$, this implies

$$j^s - j + 2 = (j-i)^{s^{-1}} - (j-i) \Rightarrow$$

$$j^{\overline{s}} + 2 = (j-i)^{\overline{s^{-1}}} \Rightarrow (j^{\overline{s}} + 2)^{\overline{s^{-1}}^{-1}} = j - i \Rightarrow i = j - (j^{\overline{s}} + 2)^{\overline{s^{-1}}^{-1}}.$$

So $i = F(j)$. If $j = x$, then $i = F(j) = F(x) = x - (-2+2)^{\overline{s^{-1}}^{-1}} = x = j$; this is a contradiction to $i \neq j$. Otherwise we know by Property $(*)$ that F is bijective and there is exactly one j for each i. Hence there is exactly one fixed point for each i.

In order to prove (2) we need to show additionally that AB for $A = ST$, $B = T^i$ has at most one fixed point. In this case $AB = ST^{i+1}$, hence $0^{ST^{i+1}} = \infty$, so $0, \infty$ are no fixed points. Assume $0 \neq j \in \mathbb{Z}_{n-1}$ is a fixed point of AB, then $j^{ST^{i+1}} = j$ and hence $j^s + i + 1 = j \iff j^s - j = -i - 1$. This has at most one solution for a fixed i since s is an orthomorphism. QED

Obviously $\mathfrak{A} \cap \langle T \rangle = \{T\}$ and $\mathfrak{A}^{-1} \cap \langle T \rangle = \{T^{-1}\}$, hence $|\mathfrak{A} \cup \mathfrak{A}^{-1} \cup \langle T \rangle| = 3n - 3$. From this affine partial plane we can construct a partial plane of order n. Using an appropriate projective closure derived from the Martinetti graph (see [6], Sect. 3) we obtain a partial projective plane of order n with $5n - 2$ lines and 5 complete points, where 4 of these complete points lie on the line at infinity.

9 Remark. Let $n = 10$, $s_1 = (13)(25)(48)(67)$ and $s_2 = (176)(24538)$. Then s_1 and s_2 are orthomorphisms of $\mathbb{Z}_9$ and have Property $(*)$. Hence there are partial projective planes of order 10 with 48 lines and 5 complete points.

4 Euler's Conjecture

In 1782, Euler [5] conjectured that for $n \equiv 2 \ (mod\ 4)$, there can't exist a pair of two orthogonal Latin squares of order n. However, in 1959 E.T. Parker [8] actually did construct two orthogonal Latin squares of order 10. Consider the case $n = 10$. How difficult is it to find an orthomorphisms s of $\mathbb{Z}_9$ as in Section 3, which has Property $(*)$? Can a solution be found "by hand", without a computer? It is quite reasonable to assume that there is an involutorial solution. Then s, being an orthomorphism, is a permutation of $\mathbb{Z}_9$ fixing 0 and no other point (Lemma 4). As the symmetric group S_8 contains just 105 fixed point free involutions, we have only few possibilities for s. In an obvious ordering of this set, we find the solution $s_1 = (13)(25)(48)(67)$ as the 21st possibility. Also, every particular permutation in S_8 can be dealt with very rapidly.

If we consider general fixed point free permutations in S_8, we have of course many more possibilities. However, there will be less than 1300, before we reach a solution.

In our examples, the system admits a group of homologies (dilatations) isomorphic to the cyclic group of order 9. Starting from classical examples of pairs of orthogonal Latin squares, this dilatation group looks quite natural. Also, taking the perspective of the theory of Foundations of Geometry it is manifest to take into consideration this dilatation group. However, a priori it was of course not at all easy, if not almost impossible to predict, that just this group of automorphisms might occur in the order 10 case.

References

[1] Brown, J. Wesley, E. T. Parker: *A Try For Three Order-10 Orthogonal Latin Squares*, Congressus Numerantium, **36** (1982), 143–144.

[2] Brown, J. Wesley, E. T. Parker: Classification of Turn-Squares, Proceedings of the Seminar on Combinatorics and Applications, Indian Statistical Institute, December 1982, 66–68.

[3] Brown, J. Wesley, E. T. Parker: *More on Order 10 Turn-Squares*, Ars Combinatoria **35** (1993), 125–127.

[4] P. Dembowski: Finite Geometries. Ergebnisse der Mathematik und ihrer Grenzgebiete **44**, Springer-Verlag, Heidelberg 1968.

[5] L. Euler: *Recherches sur une nouvelle espèce des quarrés magiques*, Verh. Zeeuwsch. Genootsch. Wetensch. Vlissingen, **9** (1782), 85–239.

[6] C. Hering, A. Krebs: *A partial plane of order 6 constructed from the icosahedron*, Des. Codes Cryptogr., **44** (2007), 287–292.

[7] Krebs, Andreas: Projektive Ebenen und Inzidenzmatrizen, Diplomarbeit, Tuebingen 2006.

[8] E. T. Parker: *Orthogonal Latin squares*, Proc. Nat. Acad. Sci. USA, **45** (1959), 859–862.