Latin square designs. The notion of *Latin square design* (LSD) is a direct dualization of the notion of 3-net. This means that an LSD $(\mathcal{P},\mathcal{D})$ is a transversal 3-design in which the three groups are linearly ordered. The elements of $\mathcal{D}$ are thus expressed as ordered triples. Let the ordering be $(\mathcal{R},\mathcal{C},\mathcal{E})$, the letters standing for *rows*, *columns* and *entries*. This refers to the way how an LSD is obtained from a latin square, with blocks being the triples (r,c,e), where e is the symbol appearing in the cell that is determined by row r and column c.

The groups of an LSD (i.e., the sets $\mathcal{R}$, $\mathcal{C}$, $\mathcal{E}$) are called *fibres* (which is the usual way how to call groups of a transversal design in an algebraic context).

The connection of LSDs to quasigroups follows from the fact that an LSD is a dualization of a 3-net. Hence, given a set Q and bijections $\alpha\colon Q\to\mathcal{R}$, $\beta\colon Q\to\mathcal{C}$ and $\gamma\colon Q\to\mathcal{E}$, a quasigroup $(Q,\cdot)$ may be formed by setting $x\cdot y=z$ exactly when $(\alpha(x),\beta(y),\gamma(z))\in\mathcal{D}$. On the other hand, each quasigroup yields an LSD, with blocks $((x,1),(y,2),(z,3))$, $xy=z$. These blocks will be written as (x,y,z), for simplicity.

The fibres of an LSD are considered to be numbered by 1, 2 and 3. Thus $\mathcal{R}$ is the 1st fibre, $\mathcal{C}$ the 2nd fibre, and $\mathcal{E}$ the 3rd fibre.

Central automorphisms. An automorphism of an LSD is a permutation of points that induces a permutation of blocks. Every automorphism, say α, of the LSD, maps a fibre upon a fibre. Denote by $\pi(\alpha)$ the permutation of $\{1,2,3\}$ that maps i upon j if and only if α maps the ith fibre upon the jth fibre. Note that π is a homomorphism of groups that sends automorphisms of the LSD to S_3.

The automorphism α is said to be *central*, with center c, if $\pi(\alpha)$ is a transposition, and $\alpha(B)=B$ whenever B is a block that contains c.

Suppose that the LSD is nontrivial (i.e., there is more than one block). Then there exist blocks $B_1\neq B_2$ such that $\{c\}=B_1\cap B_2$. Since $\{\alpha(c)\}=\alpha(B_1)\cap\alpha(B_2)=B_1\cap B_2$, there must be $\alpha(c)=c$. In order to cover the trivial case as well, include the condition $\alpha(c)=c$ into the definition of a central automorphism.

A central automorphism with center c is called an *i-reflexion* if c belongs to the ith fibre. Another name for a central automorphism is *Bol reflexion*. An i-reflexion may also be called *left, right and middle Bol reflexion*, with $i=1,2,3$, respectively.

The existence of an i-reflexion with center c implies that the LSD possesses certain structural features. Our intention is to explain what is the algebraic interpretation of these features in the case when the LSD is obtained from a loop Q.

What determines an automorphism uniquely. Let α be an automorphism of an LSD, and let i and j be such that $1\le i<j\le 3$. The automorphism α is fully determined by knowledge of $\alpha(x)$, where x runs through the ith and jth fibre. This is because $\alpha(x_i)$ and $\alpha(x_j)$ determine $\alpha(B)$ completely whenever $B=(x_1,x_2,x_3)$ is a block.

Suppose now that there exist $i\in\{1,2,3\}$ and a point y which is not in the ith fibre such that $\alpha(x)$ is known whenever x is within the ith fibre, and $\alpha(y)$ is known as well. If B is a block that passes through y, then $\alpha(B)$ is known since images of two of its points are known. Because of that $\alpha(x)$ is known for every x that is not in the fibre of y.

An automorphism α is thus fully determined by images of a single fibre and a single point outside this fibre.

Automorphisms of an LSD over a loop. Consider an LSD given by a quasigroup Q. If α is an automorphism such that $\pi(\alpha)(i)=i$, $1\le i\le 3$, then there exists a permutation β of Q such that $\beta((x,i)) = (\beta(x),i)$ for all $x \in Q$. Hence, if $\pi(\alpha)$ is the identity there exist permutations β_i, $1 \le i \le 3$, such that a block (x,y,z) is mapped upon the block $(\beta_1(x), \beta_2(y), \beta_3(z))$. In other words, $\beta_3(xy) = \beta_1(x)\beta_2(y)$ for all $x,y \in Q$. This means that *the kernel of* π *may be identified with* $\mathrm{Atp}(Q)$.

Saying that Q possesses an *i-reflexion at $x \in Q$* will be a shortcut for saying that in the LSD induced by Q there exists an i-reflexion with center (x,i).

Lemma. *A loop Q possesses a 2-reflexion at 1 if and only if Q is a RIP loop.*

Proof. Since $(x,1,x)$ is a block for each $x \in Q$, the 2-reflexion α, if it exists, exchanges $(x,1)$ with $(x,3)$, for all $x \in Q$. This means that (x,y,z) is mapped uppon $(z,\beta(y),x)$, where β is a permutation of Q. Since $(1,y,y)$ is mapped by α upon $(y,\beta(y),1)$, there has to be $y\beta(y) = 1$. Thus $\beta(y) = y\backslash 1$. Denote $y\backslash 1$ by $I(y)$. We have $xy = z$ if and only if $zI(y) = x$. This is equivalent to $(xy)I(y) = x$ for all $x,y \in Q$, and that is a condition for Q to be a RIP loop. Arguing in the reverse order shows that if Q is a RIP-loop, then there exists a central automorphism that maps (x,y,z) upon $(z,I(y),x)$. □

Proposition. *Let Q be a RIP loop, and let c be an element of Q. The loop Q possesses a 2-reflexion at c if and only if $(yc \cdot x)c = y(cx \cdot c)$ for all $x,y \in Q$. If such a 2-reflexion exists, then it sends a block (x,y,z) upon $(cz^{-1}, c \cdot y^{-1}c, cx)$, and $x\backslash c = c(xc)^{-1} \cdot c$ for every $x \in Q$.*

Proof. Suppose that α is the 2-reflexion at c. Blocks (x,c,xc) are mapped upon (xc,c,x), and blocks (xc^{-1},c,x) are mapped upon (x,c,xc^{-1}). Thus $\alpha(x,1) = (xc,3)$ and $\alpha(x,3) = (xc^{-1},1)$.

There thus exists β, a permutation of Q, such that each block (x,y,z) is mapped upon $(zc^{-1}, \beta(y), xc)$. In particular,

$$(xc \cdot y, y^{-1}, xc) \text{ is mapped upon } \big(x, \beta(y^{-1}), (xc \cdot y)c\big).$$

Setting $x = 1$ yields $\beta(y^{-1}) = cy \cdot c$. Thus $\beta(y) = cy^{-1} \cdot c$ for every $y \in Q$, and $x(cy \cdot c) = (xc \cdot y)c$ for all $x,y \in Q$. If the latter holds, then the argument may be reversed to show that the 2-reflexion at c exists.

Assume that $x(cy \cdot c) = (xc \cdot y)c$ for all $x,y \in Q$. Then $x(c(xc)^{-1} \cdot c) = (xc)(xc)^{-1} \cdot c = c$. Hence $x\backslash c = c(xc)^{-1} \cdot c$, for every $x \in Q$. □

The following statement is a direct consequence the proposition. The part about the left Bol loops follows by a mirror argument.

Theorem. *A loop Q is a right Bol loop if and only if Q possesses a 2-reflexion (right Bol reflexion) at each $c \in Q$. The loop Q is a left Bol loop if and only if Q possesses a 1-reflexion (left Bol reflexion) at each $c \in Q$. Furthermore, if $x,y \in Q$, then*

$$x\backslash y = y(xy)^{-1} \cdot y \quad \text{if } Q \text{ is right Bol, and}$$
$$y/x = y \cdot (yx)^{-1}y \quad \text{if } Q \text{ is left Bol.}$$

Bol loops may be thus considered as an algebra in signature $(Q, \cdot, {}^{-1}, 1)$.

Conjugating reflexions. Suppose that α is a central automorphism with center c of an LSD, and that γ is another automorphism of the LSD (not necessarily central). The claim is that $\gamma\alpha\gamma^{-1}$ *is a central automorphism with center* $\gamma(c)$.

Proof. Express a block $\gamma(B)$, where B is a block of the LSD that contains c. Then $(\gamma\alpha\gamma^{-1})(\gamma(B)) = \gamma\alpha(B) = \gamma(B)$. This means that each block that contains $\gamma(c)$ is fixed by $\gamma\alpha\gamma^{-1}$. Furthermore, $\pi(\gamma\alpha\gamma^{-1})$ is a transposition because π is a homomorphism of groups. □

It is thus true that an LSD *admits all possible central automorphisms if there exists at least one central automorphism, and the group of automorphisms of the LSD is transitive upon the points of the LSD.*

Theorem. *A loop Q is Moufang if and only if the LSD of the loop admits all possible central automorphisms.*

Proof. A Moufang loop is both left and right Bol. Hence it contains all 1-reflexions and 2-reflexions. It is clear that the set of these reflexions generates a group that is transitive upon the points of the LSD. $\square$