EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

# Latin Squares and Nonassociative Structures

Aleš Drápal
Charles University, Prague
School of Mathematics and Physics
2022

# Quasigroups, 3-nets and isotopy

**Definition of a quasigroup.** Let $\cdot$ be a binary operation upon a set $Q$. For every $a \in Q$ define $L_a \colon Q \to Q$ and $R_a \colon Q \to Q$ by

$$L_a \colon x \mapsto ax \text{ and } R_a \colon x \mapsto xa.$$

Call $L_a$ the *left translation* of the element $a$, and $R_a$ the *right translation*.

The pair $(Q, \cdot)$ is called a *quasigroup* if $L_a$ and $R_a$ permute $Q$ for each $a \in Q$. There are many alternative definitions of a quasigroup. We shall get to them later.

Operations of $Q$ will be denoted by different symbols. For example $+$ or $*$ or $\circ$. The choice of $\cdot$ is implicit. Hence stating that $Q$ is a quasigroup means that we are considering the pair $(Q, \cdot)$.

The application of $\cdot$ may be replaced by a juxtaposition. Thus $xy$ is the same as $x \cdot y$. It is usual to assume that the juxtaposition binds more tightly than the explicit use of an operation. E.g., $xu \cdot (yz \cdot w)$ is the same as $(x \cdot u) \cdot ((y \cdot z) \cdot w)$.

**Multiplication table.** Every binary operation may be represented by its *multiplication (or operational)* table. Both

| $+$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

and

| $*$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 2 | 1 |
| 1 | 2 | 1 | 0 |
| 2 | 1 | 0 | 2 |

are multiplication tables of a quasigroup. The operation of the quasigroup upon the left is equal to $(x + y) \bmod 3$. The formula for the operation of the quasigroup upon the right is $x * y \equiv -x - y \bmod 3$. The latter quasigroup is *idempotent*, i.e., $x * x = x$ for every $x \in Q$.

Consider the quasigroup $(\mathbb{Z}_3, +)$ and decompose it to the *border of the table* (upon the left) and the *body of the table* (upon the right):

| $+$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | | | |
| 1 | | | |
| 2 | | | |

| | | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| | 1 | 2 | 0 |
| | 2 | 0 | 1 |

**Latin squares and quasigroups.** Let $S$ be a finite set, $|S| = n$. A *latin square* over $S$ is an $n \times n$ matrix $A = (a_{ij})$ such that for every $i \in \{1, \ldots, n\}$

$$S = \{a_{i1}, \ldots, a_{in}\} = \{a_{1i}, \ldots, a_{ni}\}.$$

If $\cdot$ is a binary operation upon set $Q$, then $(Q, \cdot)$ is a quasigroup if and only if the body of the operation table is a latin square.

**Lines induced by a quasigroup.** Let $(Q, \cdot)$ be a quasigroup. Put $\mathcal{P} = Q \times Q$ and treat the set $\mathcal{P}$ as a *set of points*. Define $\mathcal{L}_i$, $1 \le i \le 3$, as sets of parallel lines *(pencils)* such that $\mathcal{L}_1 = \{r_a;\ a \in Q\}$, $\mathcal{L}_2 = \{c_a;\ a \in Q\}$ and $\mathcal{L}_3 = \{s_a;\ a \in Q\}$, where

$$\begin{aligned} r_a &= \{(a, x);\ x \in Q\} \quad \text{(the row of } a\text{)} \\ c_a &= \{(x, a);\ x \in Q\} \quad \text{(the column of } a\text{)} \\ s_a &= \{(x, y) \in Q \times Q;\ xy = a\} \quad \text{(the transversal of } a\text{)} \end{aligned}$$

**Axioms of the 3-net.** The system $(\mathcal{P}; \mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3)$ clearly fulfils the following axioms:

- $\forall p \in \mathcal{P}, \forall i \in \{1,2,3\}\, \exists!\, \ell \in \mathcal{L}_i$ such that $p \in \ell$;
- $\forall i, j \in \{1,2,3\}$, where $i \neq j$: $(\ell_i \in \mathcal{L}_i,\ \ell_j \in \mathcal{L}_j \ \Rightarrow\ |\ell_i \cap \ell_j| = 1)$

This can be put in words by saying that through each point there passes exactly one line of a given pencil, and that two lines from different pencils intersect in exactly one point.

Any system that fulfils the above two axioms is called a *3-net*.

**Theorem.** *Let $(\mathcal{P}; \mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3)$ be a 3-net. Then $|\mathcal{L}_1| = |\mathcal{L}_2| = |\mathcal{L}_3| = |\ell|$ for any $\ell \in \bigcup \mathcal{L}_i$, $i \in \{1,2,3\}$.*

*Proof.* Suppose that $1 \leq i < j \leq 3$, $\ell_i \in \mathcal{L}_i$, $\ell_j \in \mathcal{L}_j$ and $\{1,2,3\} = \{i,j,k\}$. Map $\ell_i$ upon $\ell_j$ in the following way: take $q \in \ell_i$ and consider the line $\ell_k \in \mathcal{L}_k$ that passes through $q$. This line intersects $\ell_j$ in a point, say $q'$. The mapping $q \mapsto q'$ is a bijection since through every point of $\ell_j$ there passes exactly one line of $\mathcal{L}_k$.

The mapping $q \mapsto q'$ thus also proves that $|\mathcal{L}_k| = |\ell_i|$. If $\ell_i'$ is another line from $\mathcal{L}_i$, then $|\mathcal{L}_k| = |\ell_i'| = |\ell_j|$ by the same argument. □

**Coordinatization.** Let $(\mathcal{P}; \mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3)$ be a 3-net, and let $Q$ be a set of the same cardinality as $\mathcal{L}_i$, $1 \leq i \leq 3$. Suppose that $\mu_i \colon Q \to \mathcal{L}_i$ are bijections. If $x, y \in Q$ then there exists a unique line in $\mathcal{L}_3$ that passes through the intersection of $\mu_1(x)$ and $\mu_2(y)$. This line is equal to some $\mu_3(z)$. Hence there exists a binary operation upon $Q$ such that

$$xy = z \ \Leftrightarrow\ \mu_1(x) \cap \mu_2(y) \cap \mu_3(z) \neq \emptyset. \tag{C}$$

The operation is a quasigroup since knowledge of $y$ and $z$ determines $x$ uniquely, and, similarly, knowledge of $x$ and $z$ determines $y$ uniquely.

Let $Q$ be a quasigroup and let $\mu_i \colon Q \to \mathcal{L}_i$ be a bijection for each $i \in \{1,2,3\}$. If $(C)$ holds for all $x, y, z \in Q$, then $(\mu_1, \mu_2, \mu_3)$ is called a *coordinatization* of the 3-net $(\mathcal{P}; \mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3)$.

**Proposition.** *Let $(\mathcal{P}; \mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3)$ be a 3-net, and let $Q$ and $Q'$ be quasigroups. If $\mu_i \colon Q \to \mathcal{L}_i$ and $\mu_i' \colon Q' \to \mathcal{L}_i$ are bijections such that both $(\mu_1, \mu_2, \mu_3)$ and $(\mu_1', \mu_2', \mu_3')$ are coordinatizations of the 3-net $(\mathcal{P}; \mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3)$, then the mappings $\alpha_i = (\mu_i')^{-1}\mu_i$, $1 \leq i \leq 3$, are bijections $Q \to Q'$ that fulfil*

$$xy = z \ \Leftrightarrow\ \alpha_1(x)\alpha_2(y) = \alpha_3(z).$$

*Proof.* The mapping $\alpha_i$ is a bijection since both $\mu_i \colon Q \to \mathcal{L}_i$ and $\mu_i' \colon Q' \to \mathcal{L}_i$ are bijections, $i \in \{1,2,3\}$. Let $x, y, z \in Q$ be such that $xy = z$. Then $\mu_1(x) \cap \mu_2(y) \cap \mu_3(z) \neq \emptyset$, by the definition of coordinatization. This can be written as $\mu_1'\alpha_1(x) \cap \mu_2'\alpha_2(y) \cap \mu_3'\alpha_3(z) \neq \emptyset$ since $\mu_i'\alpha_i = \mu_i'(\mu_i')^{-1}\mu_i = \mu_i$. This means that $\alpha_1(x)\alpha_2(y) = \alpha_3(z)$ holds in $Q_2$ since $(\mu_1', \mu_2', \mu_3')$ is a coordinatization of $(\mathcal{P}; \mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3)$. □

**Isotopy.** Suppose that $Q_1$ and $Q_2$ are quasigroups. Suppose that $\alpha$, $\beta$ and $\gamma$ are bijections $Q_1 \to Q_2$. The triple $(\alpha, \beta, \gamma)$ is called an *isotopy* $Q_1 \to Q_2$ if and only if

$$\forall x, y, z \in Q\colon\ xy = z \ \Leftrightarrow\ \alpha(x)\beta(y) = \gamma(z).$$

This can be also expressed as $\gamma(xy) = \alpha(x)\beta(y)$. The fact that $\alpha$, $\beta$ and $\gamma$ are bijections means that is suffices to verify $xy = z \Rightarrow \alpha(x)\beta(y) = \gamma(z)$. Indeed, if $\alpha(x)\beta(y) = \gamma(z)$ and $xy = z'$, then $\alpha(x)\beta(y) = \gamma(z')$ and $z = z'$.

Quasigroups $Q_1$ and $Q_2$ are called *isotopic* if and only if there exists an isotopy $Q_1 \to Q_2$.

**Theorem.** *Quasigroups $Q_1$ and $Q_2$ are isotopic if and only if there exists a 3-net $(\mathcal{P}; \mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3)$ that may be coordinatized both by $Q_1$ and $Q_2$.*

*Proof.* By the Proposition any two quasigroups coordinatizing the same 3-net are isotopic. Suppose now that $(\alpha_1, \alpha_2, \alpha_3)$ is an isotopy $Q_1 \to Q_2$. We shall show that both $Q_1$ and $Q_2$ may be used to coordinatize the 3-net of $Q_2$ that consists of row lines $r_b$, column lines $c_b$ and symbol lines $s_b$, $b \in Q_2$. A coordinatization $(\nu_1, \nu_2, \nu_3)$ by $Q_2$ is defined straightforwardly as $\nu_1(b) = r_b$, $\nu_2(b) = c_b$ and $\nu_3(b) = s_b$. The triple $(\nu_1, \nu_2, \nu_3)$ coordinatizes the 3-net since $xy = z$ if and only if $r_x \cap c_y \cap s_z \neq \emptyset$, for any $x, y, z \in Q_2$.

A coordinatization $(\lambda_1, \lambda_2, \lambda_3)$ by $Q_1$ is defined so that $\lambda_1(a) = r_{\alpha_1(a)}$, $\lambda_2(a) = c_{\alpha_2(a)}$ and $\lambda_3(a) = s_{\alpha_3(a)}$, for each $a \in Q_1$. Suppose that $x, y, z \in Q_1$. By the definition, $\lambda_1(x) \cap \lambda_2(y) \cap \lambda_3(z)$ is equal to $r_{\alpha_1(x)} \cap c_{\alpha_2(y)} \cap s_{\alpha_3(z)}$. This is nonempty if and only if $\alpha_1(x) \cdot \alpha_2(y) = \alpha_3(z)$. Since $(\alpha_1, \alpha_2, \alpha_3)$ is an isotopy $Q_1 \to Q_2$, the latter equality holds if and only if $xy = z$. Therefore $xy = z$ if and only if $\lambda_1(x) \cap \lambda_2(y) \cap \lambda_3(z) \neq \emptyset$. This verifies that $(\lambda_1, \lambda_2, \lambda_3)$ is a coordinatization of the 3-net upon $Q_2 \times Q_2$. □

**Elementary algebraic properties of isotopies.** *Suppose that $(\alpha, \beta, \gamma)\colon Q_1 \to Q_2$ and $(\delta, \epsilon, \eta)\colon Q_2 \to Q_3$ are isotopies. Then both $(\delta\alpha, \epsilon\beta, \eta\gamma)\colon Q_1 \to Q_3$ and $(\alpha^{-1}, \beta^{-1}, \gamma^{-1})\colon Q_2 \to Q_1$ are isotopies.*

To verify the former property consider $x, y \in Q_1$. Then $\delta\alpha(x) \cdot \epsilon\beta(y) = \eta(\alpha(x) \cdot \beta(y)) = \eta\gamma(xy)$. To verify the latter property consider $x', y' \in Q_2$. There exist unique $x, y \in Q_1$ such that $x' = \alpha(x)$ and $y' = \beta(y)$. Now, $\alpha^{-1}(x')\beta^{-1}(y') = xy = \gamma^{-1}\gamma(xy) = \gamma^{-1}(\alpha(x)\beta(y)) = \gamma^{-1}(x'y')$.

Note that $\alpha\colon Q_1 \to Q_2$ is an *isomorphism* if and only if $(\alpha, \alpha, \alpha)$ is an isotopism $Q_1 \to Q_2$.

**Autotopies and the left nucleus.** Let $Q$ be a quasigroup. An isotopy $Q \to Q$ is called an *autotopy*. All autotopies form a group. This group will be denoted by $\mathrm{Atp}(Q)$.

Consider $a \in Q$ and recall that $L_a$ denotes the left translation of the element $a$. The triple $(L_a, \mathrm{id}_Q, L_a)$ is an isotopy if and only if $L_a(x) \cdot \mathrm{id}_Q(y) = L_a(xy)$ for all $x, y \in Q$. This is the same as

$$a \cdot xy = ax \cdot y \text{ for all } x, y \in Q.$$

All $a \in Q$ that fulfil this conditions form a subset of $Q$ that is called the *left nucleus*. It is denoted by $N_\lambda(Q)$. Elements of $N_\lambda(Q)$ are those elements of $Q$ that may be described by saying that they 'associate upon the left'.

**Exercise.** Let $G$ be a group. Describe $\mathrm{Atp}(G)$.

**Local units.** Let $a$ be an element of a quasigroup $Q$. By the definition of quasigroups there exists exactly one $b \in Q$ such that $L_a(b) = a$. Denote this $b$ by $f_a$. The equality $L_a(b) = a$ may be written as $a = af_a$. The element $f_a$ is call the *right local unit* of $a$.

Similarly define the *left local unit* $e_a$ such that $e_a a = a$.

**Associative triples.** Let $Q$ be a quasigroup. A triple $(x, y, z) \in Q^3$ is said to be *associative* if $xy \cdot z = x \cdot yz$.

*Claim.* The triple $(e_a, a, f_a)$ is associative.

*Proof.* $e_a a \cdot f_a = af_a = a = e_a a = e_a \cdot af_a$.

*Corollary.* A quasigroup of finite order $n$ contains at least $n$ associative triples.

*Definitions.* A quasigroup $Q$ is said to be *idempotent* if $xx = x$ for every $x \in Q$. The quasigroup $Q$ is said to be *maximally nonassociative* if

$$\forall x, y, z \in Q\colon\ xy \cdot z = x \cdot yz \ \Leftrightarrow\ x = y = z.$$

**Exercise.** Show that a maximally nonassociative quasigroup has to be idempotent. Show that a quasigroup of finite order $n$ contains exactly $n$ associative triples if and only if it is maximally nonassociative.

**Existence of maximally nonassociative quasigroups.** There are no maximally nonassociative quasigroups of orders $2, 3, 4, 5, 6, 7, 8, 10$. Maximally nonassociative quasigroups of other orders $n$ are known to exist for $n = 9$, $n = 13$ and for all $n \geq 16$ such that $n \notin \{40, 42, 44, 56, 66, 77, 88, 90, 110\}$ if $n$ is not of the form $2p$, $p$ a prime, or $2p_1p_2$, $p_1 \leq p_2 < 2p_1$.

**Challenge.** Find a maximally nonassociative quasigroup of order $2p$, $p$ a prime.

**Global units.** An element $e \in Q$ is a called a *left unit* if $e_a = e$ for all $a \in Q$. Similarly define the *right unit*. There is at most one left unit and at most one right unit. If there exist both of them, then they coincide since $e = ef = f$. An element $e \in Q$ is the left unit if and only if $L_e = \mathrm{id}_Q$. The right unit $f$ is characterized by $R_f = \mathrm{id}_Q$. A both sided unit is also called the *neutral element*.

**Loops and reduced latin squares.** A quasigroup is called a *loop* if and only if it possesses a neutral element. Suppose that $Q$ is a loop with unit equal to 1. If $a, b \in Q$ are such that $ab = b$, then $a = 1$. This means that if $a \neq 1$, then $L_a$ fixes no point of $Q$. Similarly, if $a \neq 1$, then $R_a$ is a fixed point free permutation.

Let $Q$ be a loop on $\{1, 2, \ldots, n\}$ with 1 the unit. The body of the multiplication table contains $1, 2, \ldots, n$ in the first row (from the left to the right) and $1, 2, \ldots, n$ in the first column (from the top to the bottom). This is exactly the condition when a latin square is called *reduced*.

**Equational definition of quasigroups.** Another way of saying that $L_a$ is permutation is to say that for any $b \in Q$ there exists exactly one $x \in Q$ such that $ax = b$. This approach is used in another definition of a quasigroup which goes by saying that for any $a, b \in Q$ the equations

$$ax = b \text{ and } ya = b \text{ have unique solutions } x \text{ and } y.$$

How to express these $x$ and $y$? We have $L_a(x) = b$ and $R_a(y) = b$. Thus $x = L_a^{-1}(b)$ and $y = R_a^{-1}(b)$. By convention, set

$$L_a^{-1}(b) = a\backslash b \qquad \text{(the left division), and}$$
$$R_a^{-1}(b) = b/a \qquad \text{(the right division).}$$

What are the properties of the divisons when seen as binary operations? Since $L_x L_x^{-1}(y) = y = L_x^{-1} L_x(y)$ and $R_x R_x^{-1}(y) = y = R_x^{-1} R_x(y)$ we get equations

$$x(x\backslash y) = y = x\backslash(xy) \text{ and } (y/x)x = y = (yx)/x. \tag{D}$$

*Claim.* If $(Q, \cdot, \backslash, /)$ fulfils (D), then $(Q, \cdot)$ is a quasigroup.
*Proof.* To show that $ax = b$ possesses a unique solution note first that $a(a\backslash b) = b$, and then observe that $ax_1 = ax_2$ implies $x_1 = a\backslash(ax_1) = a\backslash(ax_2) = x_2$.

We can thus regard (D) as an alternative definition of a quasigroup. This is a definition in the sense of universal algebra. A *quasigroup* is an algebra $(Q, \cdot, \backslash, /)$ where all operations are binary and the identities of (D) are satisfied.

This definition is usually called *equational*. The original definition may be called *combinatorial*. The equational definition of loop involves a nullary operation 1, and the laws $x \cdot 1 = x = 1 \cdot x$.
*Claim.* If $Q$ is a quasigroup and $x, y \in Q$, then $x/(y\backslash x) = y = (x/y)\backslash x$. If $Q$ is a loop, then $x/1 = x = 1\backslash x$.
*Proof.* Indeed, $y = (y(y\backslash x))/(y\backslash x) = x/(y\backslash x)$ and $y = (x/y)\backslash((x/y)y) = (x/y)\backslash y$. If 1 is the unit, then $x = (x \cdot 1)/1 = x/1$ and $x = 1\backslash(1 \cdot x) = 1\backslash x$.

**Subquasigroups and congruences.** Passing between combinatorial and equational definition is usually done informally. However, it is worth remembering that the equational definition exhibits in a clear fashion that *subquasigroups* have to be closed under divisions and *congruences of quasigroups* have to be compatible with divisions.

**Exercises.** (1) If $Q$ is a finite quasigroup, then a subset closed under multiplication is a subquasigroup and an equivalence compatible with $\cdot$ is a congruence of the quasigroup.
(2) Let $Q$ be a quasigroup. Show that an equivalence $\sim$ on $Q$ is a congruence if and only if for all $x, y, z \in Q$

$$x \sim y \;\Rightarrow\; xz \sim yz,\; zx \sim zy,\; x/z \sim y/z \text{ and } z\backslash x \sim z\backslash y.$$

**Quasigroup words and reduction.** Let $X$ be a set of symbols. Denote by $W(X)$ the absolutely free algebra over $X$ in signature $(\cdot, \backslash, /)$. The elements of $W(X)$ are called *quasigroup words*. A quasigroup word is called *reduced* if it contains no subword (subterm) of one of the forms

$$(st)/t,\; (s/t)t,\; t(t\backslash s),\; t\backslash(ts),\; t/(s\backslash t) \text{ and } (t/s)\backslash t. \tag{R}$$

For $u, v \in W(X)$ write $u \to v$ if $u$ contains a subterm that has a form that occurs in (R), and if $v$ arises from $u$ by replacing this term by $s$. The transitive closure of $\to$ is denoted by $\to^*$. A word is thus reduced if and only if it is terminal with respect to $\to^*$.

The reduction decreases the size of the term. Hence for each $u \in W(X)$ there exists a reduced $v \in W(X)$ such that $u \to^* v$. The following fact appears in various contexts. Our proof will be hence brief.

**Lemma.** *Let $u, w_1, w_2 \in W(X)$ be such that $u \to^* w_1$ and $u \to^* w_2$. If both $w_1$ and $w_2$ are reduced, then $w_1 = w_2$.*

*Proof.* Let $u$ be the smallest counterexample. To get a contradiction it suffices to show that if $u \to u_1$ and $u \to u_2$, then there exists $u_3$ such that $u_1 \to^* u_3$ and $u_2 \to^* u_3$. Indeed, if $u_i \to^* w_i$, $i \in \{1, 2, 3\}$, then $w_1 = w_3 = w_2$ since both $u_1$ and $u_2$ are smaller (with respect to the length of the quasigroup word) then $u$.

Let $u_i$ be obtained from $u$ by replacing a subterm $v_i$ by $s_i$, where $v_i$ takes the form $(s_i t_i)/t_i$, $(s_i/t_i)t_i$, etc., as listed in (R), $i \in \{1, 2\}$. The situation is easy to solve if $v_2$ is a subterm of an occurence of $t_1$. In that case make $v_2 \to s_2$ in both

occurence of $t_1$ and then replace the changed subterm by $s_1$. This means that $u_2 \to^* u_1$. If $v_2$ is a subterm of $s_1$, then define $u_3$ by making the replacement $v_2 \to s_2$ within the occurence of $s_1$ in $u_2$. Both $u_1 \to^* u_3$ and $u_2 \to^* u_3$ are then true.

If there exists a subterm $a_1a_2$ of $u$ such that $v_1$ is a subterm of $a_1$ and $v_2$ a subterm of $a_2$, then the reductions commute and the existence of $u_3$ is obvious.

What remains are situations that are usually called *critical*. These are the situations when one of the terms has a root within the other term. Suppose that $v_2$ sits within $v_1$. We shall consider only the case when $v_1 = (s_1t_1)/t_1$. The other cases are similar. The only nontrivial possibility in (R) with / at the top is $t_2/(s_2\backslash t_2)$. However $t_2 = s_1t_1$ and $t_1 = s_2\backslash s_2$ is impossible. Therefore there must be $v_2 = s_1t_1$. If $s_1t_1 = (s_2/t_2)t_2$, then $t_1 = t_2$ and both replacements change $v_1$ to $s_1 = s_2/t_1$. Thus $u_1 = u_2$ and nothing has to be constructed.

If $s_1t_1 = t_2(t_2\backslash s_2)$, then $s_1 = t_2$ and $t_1 = t_2\backslash s_2$. Thus

$$v_1 \to s_1 = t_2 \text{ and } v_1 = v_2/t_1 \to s_2/t_1 = s_2/(t_2\backslash s_2) \to t_2.$$

The latter replacement shows that $u_2 \to u_1$. □

Denote by $\equiv$ the least congruence of $W(X)$ such that $W(X)/\equiv$ is a quasigroup. This is a free quasigroup with basis $\{[x]_\equiv;\, x \in X\}$. Denote by $F(X)$ the subset of $W(X)$ that is formed by all reduced words. By the Lemma for each $w \in W(X)$ there exists a unique reduced word $\rho(w)$ such that $w \to^* \rho(w)$. If $u \to v$, then $\rho(u) = \rho(v)$. From that it follows that $u \equiv v$ if and only if $\rho(u) = \rho(v)$. Hence defining operations by

$$u \cdot v = \rho(uv),\ u/v = \rho(u/v) \text{ and } u\backslash v = \rho(u\backslash v)$$

makes $F(X)$ a **free quasigroup** with basis $X$.

To get a **free loop** consider loop words in $\cdot$, $\backslash$, / and 1, and add reduction rules that change each of $s/1$, $s \cdot 1$, $1 \cdot s$ and $1\backslash s$ to $s$.

**Loops from quasigroups.** Let $Q$ be a quasigroup, and let $e$ and $f$ be elements of $Q$. Set $x * y = x/f \cdot e\backslash y$, for all $x, y \in Q$. Translations of $(Q, \cdot)$ are denoted by $L_x$ and $R_x$, while translations of $(Q, *)$ will be denoted by $\lambda_x$ and $\rho_x$, $x \in Q$. Clearly,

$$\lambda_x = L_{x/f}L_e^{-1} \text{ and } \rho_y = R_{e\backslash y}R_f^{-1},$$

for each $x, y \in Q$. Note that $x * (ef) = x/f \cdot f = x$ and $(ef) * y = e \cdot e\backslash y = y$. This means that $(Q, *)$ *is a loop, and* $ef$ *is the neutral element of this loop.*

**Principal isotopes.** An isotopy of quasigroups $(\alpha, \beta, \gamma)\colon Q_1 \to Q_2$ is called *principal* if the underlying sets of $Q_1$ and $Q_2$ coincide and $\gamma = \mathrm{id}_{Q_1}$. Call $Q_2$ a *principal isotope* of $Q_1$ if there exists a principal isotopy $Q_1 \to Q_2$.

Let $(Q, *)$ be a principal isotope of $(Q, \cdot)$. There thus exist $\alpha, \beta \in \mathrm{Sym}(Q)$ such that $x * y = \alpha(x)\beta(y)$. The translations of $(Q, \cdot)$ are denoted by $L_x$ and $R_x$, and those of $(Q, *)$ by $\lambda_x$ and $\rho_x$, $x \in Q$. Clearly,

$$\lambda_x = L_{\alpha(x)}\beta \text{ and } \rho_y = R_{\beta(y)}\alpha,$$

for each $x, y \in Q$. If $(Q, *)$ is a loop, then there must exist $x \in Q$ such that $\lambda_x = \rho_x = \mathrm{id}_Q$. If this true, then there exist $e, f \in Q$ such that $\beta = L_e^{-1}$ and $\alpha = R_f^{-1}$. If such $e$, $f$ exist, then $x * y = \alpha(x)\beta(y) = x/f \cdot e\backslash y$. This is a loop, as observed above. We have proved the following statement:

**Proposition 1.** *Let $(Q, \cdot)$ be a quasigroup. A principal isotope $(Q, *)$ of $(Q, \cdot)$ is a loop if and only if there exist $e, f \in Q$ such that $x * y = x/f \cdot e\backslash y$ for all $x, y \in Q$.*

**Quasigroups induced by isomorphism and isotopy.** Suppose that $Q$ is a quasigroup and $S$ a set. Suppose also that there exists a bijection $\gamma\colon Q \to S$. Then there is only one way how to define a quasigroup operation upon $S$, and that is by $st = \gamma(\gamma^{-1}(s)\gamma^{-1}(t))$ for all $s, t \in Q$. The quasigroup $(S, \cdot)$ is called *isomorphically induced* by $\gamma$.

Similarly, if $\alpha, \beta, \gamma$ are bijections $Q \to S$, then $st = \gamma(\alpha^{-1}(s)\beta^{-1}(t))$ yields the only quasigroup upon $S$ for which $(\alpha, \beta, \gamma)$ is an isotopy $(Q, \cdot) \to (S, \cdot)$. This is the quasigroup *isotopically induced* by $(\alpha, \beta, \gamma)$.

**Loops isotopic to a quasigroup.** Suppose that $(\alpha, \beta, \gamma)$ is an isotopy of quasigroups $Q_1 \to Q_2$. Let $(Q_1, *)$ be the quasigroup isomorphically induced by the bijection $\gamma^{-1}\colon Q_2 \to Q_1$. Isotopies may be composed. Hence

$$(\gamma^{-1}, \gamma^{-1}, \gamma^{-1})(\alpha, \beta, \gamma) = (\gamma^{-1}\alpha, \gamma^{-1}\beta, \mathrm{id}_{Q_1})$$

is a principal isotopy $(Q_1, \cdot) \to (Q_1, *)$, while $(Q_1, *) \cong (Q_2, \cdot)$. This gives immediately:

**Proposition 2.** *Each quasigroup isotopic to a quasigroup $Q$ is isomorphic to a principal isotope of $Q$.*

**Proposition 3.** *Let $(Q, \cdot, \backslash, /)$ be a quasigroup. For each loop $L$ isotopic to $Q$ there exist $e, f \in Q$ such that $L$ is isomorphic to a loop on $Q$ with multiplication $x * y = x/f \cdot e\backslash y$, for all $x, y \in Q$.*

*Proof.* By the preceding statement every loop isotopic to $Q$ is isomorphic to a principal isotope of $Q$. By Proposition 1, a principal isotope that is a loop has to be of the form $x/f \cdot e\backslash y$. □

**Exercise.** Prove directly that each loop isotopic to a group $G$ is isomorphic to $G$.

*Notational remark:* If $H$ is a subgroup of a group $G$, then it is usual to write $H = 1$ if $H$ is the trivial subgroup, that is if $|H| = 1$. Thus, if $G$ is a permutation group on $\Omega$, $H = 1$ means that $H = \{\mathrm{id}_\Omega\}$.

**Regular groups.** A permutation group on $\Omega$ is, by definition, every subgroup of $\mathrm{Sym}(\Omega)$. A permutation group $H \leq \mathrm{Sym}(\Omega)$ is *transitive* if for all $\alpha, \beta \in \Omega$ there exists $h \in H$ such that $h(\alpha) = \beta$. Note that it suffices if the former holds for a single $\alpha \in \Omega$. In a transitive group all stabilizers $H_\alpha = \{h \in H;\ h(\alpha) = \alpha\}$ are conjugate one to another. Hence if $H_\alpha = 1$ for one $\alpha \in \Omega$, then $H_\alpha = 1$ for all $\alpha \in \Omega$.

The permutation group $H \leq \mathrm{Sym}(\Omega)$ is called *regular* if it is transitive, and if $H_\alpha = 1$, for any $\alpha \in \Omega$. Note that the latter condition may also be expressed as $h = \mathrm{id}_\Omega$ whenever $h \in H$ fixes a point.

Let $G$ be a group. Then $\{L_x;\ x \in G\}$ is a regular permutation group on $G$. It is called the *left regular representation of $G$*.

Each regular permutation group may be interpreted as a left regular representation of an abstract group. To see this consider a regular group $G$ upon $\Omega$. Fix a point $\omega \in \Omega$ and identify it with the unit element 1 of an abstract group $(\Omega, \cdot)$ that will be now described. For each $\alpha \in \Omega$ denote by $\psi_\alpha$ the element of $G$ that sends $1 = \omega$ upon $\alpha$. Since $G$ is regular, the permutation $\psi_\alpha$ is determined by $\alpha$ uniquely. Furthermore, $G = \{\psi_\alpha;\ \alpha \in \Omega\}$. Put $\alpha \cdot \beta = \psi_\alpha(\beta)$. Since $G$ is a group, $\psi_\alpha\psi_\beta = \psi_\eta$ for some $\eta \in \Omega$. Now, $\eta = \psi_\eta(1) = \psi_\alpha\psi_\beta(1) = \psi_\alpha(\beta) = \alpha \cdot \beta$. Hence $\psi_\alpha\psi_\beta = \psi_{\alpha\beta}$. Applying this identity upon $\gamma \in \Omega$ gives the associative law $\alpha \cdot \beta\gamma = \alpha\beta \cdot \gamma$. As is easy to see, $\psi_\alpha^{-1} = \psi_{\alpha^{-1}}$ for each $\alpha \in \Omega$. The mappings $\psi_\alpha$ coincide with the left translations of $(\Omega, \cdot)$.

Note that denoting the neutral element by 1 is a matter of convention. If $G$ is abelian, then it may be more natural to denote the neutral element by 0 and the binary operation by $+$.

**Loops with translations closed under composition.** A loop $Q$ is said to have left translations *closed under composition* if

$$\forall x, y \in Q \; \exists z \in Q \text{ such that } L_x L_y = L_z.$$

If this is true, then $xy = L_x L_y(1) = L_z(1) = z$, implying $L_x L_y = L_{xy}$ for all $x, y \in Q$. But that is equivalent to associativity since $L_x L_y(v) = x \cdot yv$ and $L_{xy}(v) = xy \cdot v$. This proves that *a loop with left translations closed under composition has to be a group.*

**Albert's Theorem.** *A loop isotopic to a group $G$ is isomorphic to $G$.*

*Proof.* By Proposition 3 only the principal isotopes $x/f \cdot e\backslash y$ may be considered. The set of the left translations of such an isotope is equal to

$$\{L_{x/f} L_e^{-1};\ x \in G\} = \{L_x L_e^{-1};\ x \in G\} = \{L_{xe^{-1}};\ x \in G\} = \{L_x;\ x \in G\}.$$

The set of left translations of the principal isotope thus coincides with that of $G$. The left translations are closed under composition. The principal isotope thus must be a group. The both groups are isomorphic since they have coinciding left regular representations. □

It is immediate to observe that each loop of order 2 is isomorphic to $(\mathbb{Z}_2, +)$ and that each loop of order 3 is isomorphic to $(\mathbb{Z}_3, +)$.

**Theorem.** *Each loop of order $\leq 4$ is a group.*

*Proof.* What remains is the order 4. Let $Q$ be a 4-element loop with unit $e$. Suppose first that $x^2 = e$ for all $x \in Q$. Assume that $Q = \{0, 1, 2, 3\}$ and $e = 0$. The table upon the left may be completed in only one way to a latin square (on the right). The multiplication table upon the right describes a group that is isomorphic to $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$.

| | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 0 | | |
| 2 | 2 | | 0 | |
| 3 | 3 | | | 0 |

$\rightarrow$

| | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 0 | 3 | 2 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 2 | 1 | 0 |

Assume now that there exists $x \neq e$ such that $x^2 = y \neq e$. The elements $e$, $x$ and $y$ are pairwise distinct. Assume that $e = 0$, $x = 1$, $y = 2$ and verify the completion to $(\mathbb{Z}_4, +)$ below (the first cell to fill is $(3, 3)$).

| | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | | |
| 2 | 2 | | | |
| 3 | 3 | | | |

$\rightarrow$

| | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

□

**Lemma 1.** *Let $Q$ be a loop of order 5. If the mapping $x \mapsto x^2$ is a permutation of $Q$, then $Q \cong (\mathbb{Z}_5, +)$.*

*Proof.* Put $Q_1 = Q \setminus \{1\}$. Then $x \mapsto x^2$ permutes $Q_1$ and this permutations lacks a fixed point. The permutation has one or two cycles. In the former case let us assume that the permutation is equal to $(a\,b\,c\,d)$. In the latter case let it be $(a\,b)(c\,d)$. In the former case there is only one completion to a latin square (first positions to fill are $(a, d)$ and $(d, a)$):

| | 1 | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|---|
| 1 | 1 | $a$ | $b$ | $c$ | $d$ |
| $a$ | $a$ | $b$ | | | |
| $b$ | $b$ | | $c$ | | |
| $c$ | $c$ | | | $d$ | |
| $d$ | $d$ | | | | $a$ |

$\rightarrow$

| | 1 | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|---|
| 1 | 1 | $a$ | $b$ | $c$ | $d$ |
| $a$ | $a$ | $b$ | $d$ | 1 | $c$ |
| $b$ | $b$ | $d$ | $c$ | $a$ | 1 |
| $c$ | $c$ | 1 | $a$ | $d$ | $b$ |
| $d$ | $d$ | $c$ | 1 | $b$ | $a$ |

Let us now consider the case of $(a\,b)(c\,d)$.

| | 1 | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|---|
| 1 | 1 | $a$ | $b$ | $c$ | $d$ |
| $a$ | $a$ | $b$ | | | |
| $b$ | $b$ | | $a$ | | |
| $c$ | $c$ | | | $d$ | |
| $d$ | $d$ | | | | $c$ |

The table upon the right cannot be completed to a latin square since the only positions to place the four entries $a$ and $b$ into rows $c$ and $d$ are $(c, d)$ and $(d, c)$.

This shows that up to isomorphism there is only one loop $Q$ of order 5 such that $x \mapsto x^2$ permutes $Q$. The group $(\mathbb{Z}_5, +)$ fulfils this requirement. □

**Lemma 2.** *Up to isomorphism there is only one loop $Q$ of order 5 in which $x \mapsto x^2$ does not permute $Q$ and in which there exists no $x \neq 1$ such that $x^2 = 1$.*

*Proof.* Let $Q$ be such a loop. There exist $a, b, s \in Q$ such that $a^2 = b^2 = s \neq 1$ and $a \neq b$. Therefore there exists $c \in Q$ such that $Q = \{1, a, b, c, s\}$. This yields a partial table in which the only row that does not carry $s$ is the row $c$ and the only column that does not carry $s$ is the column $c$. Hence $c^2 = s$.

There has to be $s^2 \in \{a, b, c\}$. Let us assume that $s^2 = a$. If $as = 1$, then $(a, b)$ and $(a, c)$ are the only unfilled entries in the row $a$, implying $ab = c$ and $ac = b$. That means $\{b, c\} \cap \{sb, sc\} = \emptyset$. Hence $sx \in \{b, c\}$ may happen if and only if $x = a$. That is impossible. Therefore $as \neq 1$.

There thus exists $x \in \{b, c\}$ such that $ax = 1$. With no loss of generality it may be assumed that $x = b$. The rest can be completed uniquely, see below:

| | 1 | $a$ | $b$ | $c$ | $s$ |
|---|---|---|---|---|---|
| 1 | 1 | $a$ | $b$ | $c$ | $s$ |
| $a$ | $a$ | $s$ | 1 | | |
| $b$ | $b$ | | $s$ | | |
| $c$ | $c$ | | | $s$ | |
| $s$ | $s$ | | | | $a$ |

$\rightarrow$

| | 1 | $a$ | $b$ | $c$ | $s$ |
|---|---|---|---|---|---|
| 1 | 1 | $a$ | $b$ | $c$ | $s$ |
| $a$ | $a$ | $s$ | 1 | $b$ | $c$ |
| $b$ | $b$ | $c$ | $s$ | $a$ | 1 |
| $c$ | $c$ | 1 | $a$ | $s$ | $b$ |
| $s$ | $s$ | $b$ | $c$ | 1 | $a$ |

(L5.1)

□

To finish the classification of loops of order 5 it may be thus assumed that there exists $a \in Q$ such that $a^2 = 1$ and $a \neq 1$. Put $X = Q \setminus \{1, a\}$. Since both $L_a$ and $R_a$ switch 1 and $a$, both of them act upon $X$. Denote $L_a \restriction X$ by $\sigma$ and $R_a \restriction X$ by $\bar{\sigma}$. With no loss of generality it may be assumed that $X = \{b, c, d\}$ and $\sigma = (b\,c\,d)$. Note that $\bar{\sigma}$ is either $\sigma$ or $\sigma^{-1}$.

**Lemma 3.** *Up to isomorphism there is only one loop $Q$ of order 5 in which there exist at least three $x \in Q$ such that $x^2 = 1$.*

*Proof.* This follows from the comments above and from the unique completion below.

| | 1 | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|---|
| 1 | 1 | $a$ | $b$ | $c$ | $d$ |
| $a$ | $a$ | 1 | $c$ | $d$ | $b$ |
| $b$ | $b$ | | 1 | | |
| $c$ | $c$ | | | | |
| $d$ | $d$ | | | | |

$\rightarrow$

| | 1 | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|---|
| 1 | 1 | $a$ | $b$ | $c$ | $d$ |
| $a$ | $a$ | 1 | $c$ | $d$ | $b$ |
| $b$ | $b$ | $d$ | 1 | $a$ | $c$ |
| $c$ | $c$ | $b$ | $d$ | 1 | $a$ |
| $d$ | $d$ | $c$ | $a$ | $b$ | 1 |

(L5.2)

□

**Lemma 4.** *Let $Q$ be a loop of order 5 in which there exists exactly one $a \in Q$ with $a^2 = 1$, $a \neq 1$. If $L_a \neq R_a$, then the isomorphism type of $Q$ is determined uniquely.*

*Proof.* By comments above it may be assumed that $R_a \restriction X = \sigma^{-1}$. The rest follows from the unique completion below.

| | 1 | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|---|
| 1 | 1 | $a$ | $b$ | $c$ | $d$ |
| $a$ | $a$ | 1 | $c$ | $d$ | $b$ |
| $b$ | $b$ | $d$ | | | |
| $c$ | $c$ | $b$ | | | |
| $d$ | $d$ | $c$ | | | |

$\rightarrow$

| | 1 | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|---|
| 1 | 1 | $a$ | $b$ | $c$ | $d$ |
| $a$ | $a$ | 1 | $c$ | $d$ | $b$ |
| $b$ | $b$ | $d$ | $a$ | 1 | $c$ |
| $c$ | $c$ | $b$ | $d$ | $a$ | 1 |
| $d$ | $d$ | $c$ | 1 | $b$ | $a$ |

(L5.3)

□

**Lemma 5.** *Let $Q$ be a loop of order 5 in which there exists exactly one $a \in Q$ with $a^2 = 1$, $a \neq 1$. There are two classes of isomorphism to which $Q$ may belong if $L_a = R_a$ is assumed. Loops belonging to one of these two classes are opposite (i.e., mirror images) to loops from the other class.*

*Proof.* Let $X$ and $\sigma$ be as above. Since $c = 1a = ab = ba = c1$, there must be $c = d^2$. Similarly $b^2 = d$ and $c^2 = b$. The multiplication table is thus known up to products $xy$, where $x, y \in X$ and $x \neq y$. In each such case $xy \in \{1, a\}$. There two ways how to complete the table:

| | 1 | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|---|
| 1 | 1 | $a$ | $b$ | $c$ | $d$ |
| $a$ | $a$ | 1 | $c$ | $d$ | $b$ |
| $b$ | $b$ | $c$ | $d$ | 1 | $a$ |
| $c$ | $c$ | $d$ | $a$ | $b$ | 1 |
| $d$ | $d$ | $b$ | 1 | $a$ | $c$ |

and

| | 1 | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|---|
| 1 | 1 | $a$ | $b$ | $c$ | $d$ |
| $a$ | $a$ | 1 | $c$ | $d$ | $b$ |
| $b$ | $b$ | $c$ | $d$ | $a$ | 1 |
| $c$ | $c$ | $d$ | 1 | $b$ | $a$ |
| $d$ | $d$ | $b$ | $a$ | 1 | $c$ |

(L5.4/5)

To see that the two loops are not isomorphic consider the permutation type of $L_x$, $x \in X$. In the loop upon the left (L5.4) the translations take the form of a 5-cycle. Those upon the right (L5.5) consist of a 3-cycle and a transpozition. □

We have proved that there are **6 isomorphism types of loops of order 5**. One of them is the abelian group, the other are exemplified by tables (L5.1)–(L5.5).

**Exercise.** Prove that all nonassociative loops of order 5 are isotopic.

**Parastrophes and paratopy.** A *parastrophe* of a quasigroup $(Q, \cdot)$ is a quasigroup that is equal or opposite to one of the quasigroups $(Q, \cdot)$, $(Q, \backslash)$ and $(Q, /)$. The operation $x * y$ of a parastrophe thus is one of

$$xy,\ x\backslash y,\ x/y,\ yx,\ y\backslash x \text{ and } y/x.$$

It is easy to see that *a parastrophe of a parastrophe of $Q$ is a parastrophe of $Q$.*

Quasigroups $Q_1$ and $Q_2$ are said to be *paratopic* if one of them is isotopic to a parastrophe of the other. The relation 'being paratopic' is (as can be seen easily) an equivalence.

**Main class.** Two latin squares are *paratopic* if they are multiplication tables of paratopic quasigroups. A *main class* is a class of all latin squares that consists of all latin squares paratopic to one of them. The number of main classes of order $n$ hence coincides with the number of quasigroups of order $n$ up to paratopy. This number is as follows:

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| main classes | 1 | 1 | 1 | 2 | 2 | 12 | 147 | 283 657 | 19 270 853 541 |

$n = 10$: 34 817 397 894 749 939

$n = 11$: 2 036 029 552 582 883 134 196 099

The known numbers for isotopy classes are as follows:

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| isotopy cl. | 1 | 1 | 1 | 2 | 2 | 22 | 564 | 1 676 267 | 115 618 721 533 |

$n = 10$: 208 904 371 354 363 006

$n = 11$: 12 216 177 315 369 229 261 482 540

Note that for $n \geq 8$ the number of isotopy classes is just a little less than 6 times the number of main classes. This is because with $n$ big enough it becomes less and less likely that a quasigroup is isotopic to one of its nontrivial parastrophes.

The numbers for isomorphism classes of loops:

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| isomorphism cl. | 1 | 1 | 1 | 2 | 6 | 109 | 23 746 | 106 228 849 |

$n = 9$: 9 365 022 303 540

$n = 10$: 20 890 436 195 945 769 617

**Semisymmetry.** What if some parastrophes coincide? If $xy = yx$, then the quasigroup is *commutative*. Multiplication tables of commutative binary operations are symmetric across the main diagonal. If $(Q, \cdot)$ is commutative, then $x\backslash y = y/x$.

What if $xy = y/x$? Let us first show that in each quasigroup every of the following identities implies the other three:

$$x\backslash y = yx \;\Leftrightarrow\; x \cdot yx = y \;\Leftrightarrow\; xy \cdot x = y \;\Leftrightarrow\; xy = y/x. \tag{SS}$$

*Proof.* It suffices to verify the implication $x \cdot yx = y \;\Rightarrow\; xy \cdot x = y$ since the converse direction follows by a mirror argument. Suppose that $x \cdot yx = y$ holds for all $x, y \in Q$. Then $xy \cdot x = xy \cdot ((x/xy)(xy)) = x/xy$. That is equal to $y$ since $x = y \cdot xy$ is assumed. □

A quasigroup fulfilling the identities of (SS) is called *semisymmetric*. A binary operation is called *semisymmetric* if $x \cdot yx = y = xy \cdot x$. Note that a semisymmetric operation is always a quasigroup operation.

*Notational remark.* Let $a_1, \ldots, a_k$ be elements of set, say $\Omega$. Then $(a_1\, a_2\, \ldots\, a_k)$ denotes a *cycle* consisting of elements $a_1, \ldots, a_k$. These elements are implicitly assumed to be pairwise distinct. The integer $k$ is the *length* of the cycle. A cycle of length $k$ is called a *$k$-cycle*. Note that if $k \geq 3$, then

$$(a_1\, a_2\, \ldots\, a_k) = (a_2\, a_3\, \ldots\, a_1) = (a_k\, a_1\, \ldots\, a_{k-1}).$$

**Mendelsohn triple systems.** Let $\cdot$ be a binary operation on a set $Q$. Each ordered pair $(x, y)$ initializes a *walk* $a_0, a_1, a_2, \ldots$ upon $Q$ such that $a_0 = x$, $a_1 = y$ and $a_{i+2} = a_i \cdot a_{i+1}$. If the operation is semisymmetric and $x \neq y$, then these walks form cycles $(x\, y\, xy)$ since $y \cdot xy = x$ and $xy \cdot x = y$. If $x = y$, then the cycle shrinks to $(x)$ if $x = xx$, and to $(x\, xx)$ if $x \neq xx$. Recall that a quasigroup $Q$ is called idempotent if $x = xx$.

We have observed that if $\cdot$ is a semisymmetric idempotent operation upon $Q$, then each ordered pair $(x, y)$, $x \neq y$, occurs in exactly one of the 3-cycles induced by walks of the binary operation. In other words, the 3-cycles of the operation partition the complete oriented graph of $Q$.

The construction may be reversed. That is, a partition of the complete oriented graph to 3-cycles gives rise to a binary idempotent operation by setting $xy = z$ whenever the partition contains a cycle $(x\, y\, z)$. It is clear that the operation is semisymmetric.

A *Mendelsohn triple system* (MTS) upon $Q$ is a collection of 3-cycles that partitions the complete oriented graph upon $Q$. Idempotent semisymmetric quasigroups are also known as *MTS quasigroups*.

An example of an MTS on a 4-element set: cycles $(a\, b\, c)$, $(c\, b\, d)$, $(b\, a\, d)$ and $(a\, c\, d)$. The multiplication table:

| | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $a$ | $c$ | $d$ | $b$ |
| $b$ | $d$ | $b$ | $a$ | $c$ |
| $c$ | $b$ | $d$ | $c$ | $a$ |
| $d$ | $c$ | $a$ | $b$ | $d$ |

**Challenge.** Occurences of each symbol in the body of the multiplication table above may be connected by moves of a chess knight. Construct further examples of such latin squares. Are there other examples that may be obtained from an MTS quasigroup?

**Steiner triple systems.** A semisymmetric operation that is commutative yields a quasigroup in which all parastrophes coincide. This is why such quasigroups are called *totally symmetric*.

What are the commutative MTS quasigroups, i.e., idempotent totally symmetric quasigroups? The commutativity implies that with each cycle $(a\,b\,c)$ there is a cycle $(c\,b\,a)$. The cycles may be thus replaced by 3-element sets. What arises is a collection of 3-element subsets (called *blocks*) such that each 2-element subset is contained in exactly one block. These are the *Steiner triple systems* (STS).

An STS of order $n$ exists for each $n \equiv 1, 3 \bmod 6$. Numbers of STS up to isomorphism is given by the following table.

| $n$ | 1 | 3 | 7 | 9 | 13 | 15 | 19 |
|---|---|---|---|---|---|---|---|
| STS up to $\cong$ | 1 | 1 | 1 | 1 | 2 | 80 | 11 084 874 829 |

**Prolongation.** Let $(Q, *)$ be an idempotent quasigroup. Assume that $Q$ does not contain the symbol 1. Define an operation $\cdot$ upon $\hat{Q} = Q \cup \{1\}$ in such a way that

$$x \cdot 1 = 1 \cdot x = x,\ 1 \cdot 1 = 1 = x \cdot x \text{ and } x \cdot y = x * y$$

whenever $x, y \in Q$ and $x \neq y$. Then $\hat{Q}$ is a loop. The construction may be reversed whenever starting from a loop $Q$ such that $x^2 = 1$ for each $x \in Q$.

**Proposition.** *A prolongation of an idempotent totally symmetric quasigroup is totally symmetric, and all totally symmetric loops may be obtained in this way.*

*Proof.* Let $(Q, *)$ be idempotent. It is clear that $\hat{Q}$ is commutative if and only if $(Q, *)$ is commutative. Hence it is enough to show (1) that $\hat{Q}$ is semisymmetric if and only if $(Q, *)$ is semisymmetric, and (2) that each semisymmetric loop fulfils $x^2 = 1$. The latter is clear since $1 = (x \cdot 1)x = x^2$, by semisymmetry. For the former property note that $(x * y) * x = y$ if $x = y$. If $x \neq y$, then $x * y \neq x * x = x$, and thus $(x * y) * x = xy \cdot x$. On the other hand in $\hat{Q}$ the identity $xy \cdot x = y$ holds whenever $x = y$ or $1 \in \{x, y\}$. If $x \neq y$ and $1 \notin \{x, y\}$, then $xy \neq x$ and $xy \cdot x = (x * y) * x$. □

Note that by the proof *prolongations of MTS quasigroups are exactly the semisymmetric loops.*

**Affine and projective STS.** Let $V$ be a vector space over a 3-element field. The affine lines of $V$ form an STS. Such STS are called *affine*. The idempotent operation of the STS over $V$ may be expressed by $x * y = -x - y$.

A *Hall Triple System* (HTS) is an STS such that any two intersecting blocks belong to a subsystem on 9 elements. (There is only one STS of order 9, and this STS coincides with the affine plane of order 3.) Structure of Hall Triple Systems will be investigated later in this course.

Consider a projective space over a 2-element field. If the space is of dimension $n$, then it contains $2^{n+1} - 1$ points. Each line consists of three elements and any three noncollinear points belong to a Fano subplane. The lines form an STS. Such an STS is called *projective*.

Let $(Q, *)$ be the idempotent quasigroup of a projective STS. Suppose that $x, y, z$ do not belong to the same block (they are noncollinear). Consider the picture of the Fano plane with $x$, $y$ and $z$ being the three vertices of the triangle that forms the picture. Then $(x * y) * z = x * (y * z)$ is the central element. This implies that the

prolongation yields an associative loop $\hat{Q}$. In this loop (which is a group) $x^2 = 1$ for each $x \in Q$. This means that $\hat{Q}$ has to be an elementary abelian 2-group.

All projective STS thus may be derived from nonzero elements of an elementary abelian 2-group. Blocks coincide with subgroups of order 4 from which the zero is removed.

**Incidence geometries.** To understand the concept of dualization in line systems it seems useful to start with an abstract notion of incidence geometry. The main idea is that the relation 'point $p$ is upon a line $\ell$' is read as 'point $p$ is incident to line $\ell$', where the incidence is now expressed by a relation $\varepsilon \subseteq P \times L$, with $P$ being the set of *points* and $L$ the set of *lines*. This is an abstract approach in the sense that no other interaction between $P$ and $L$ is assumed but via the relation $\varepsilon$. Such systems are called (abstract) *incidence geometries*.

A definition of a 3-net in this context may be as follows: Let $\parallel$ be an equivalence upon $L$, with classes $L_1$, $L_2$ and $L_3$. The incidence geometry $(P, L)$ is called a *3-net* if

$$\forall x \in L\ \forall p \in P\ \exists!\, y \in L \text{ such that } x \parallel y \text{ and } p\,\varepsilon\, y; \text{ and} \tag{A1}$$

$$\forall x, y \in L\colon x \nparallel y\ \Rightarrow\ \exists!\, p \in P \text{ such that } p\,\varepsilon\, x \text{ and } p\,\varepsilon\, y. \tag{A2}$$

The definition of a 3-net as done before can be obtained from the definition above by replacing $y \in L$ with the set $\ell_y = \{p \in P;\, p\,\varepsilon\, y\}$, and the relation $p\varepsilon y$ by $p \in \ell_y$. Note that the definition of a 3-net requires that the classes of $\parallel$ are linearly ordered (i.e., $(L_1, L_2, L_3)$.)

**Nets and affine planes.** The definition of a 3-net may be generalized to a definition of a *$k$-net*, $k \geq 3$, by requiring that the number of classes of $\parallel$ is equal to $k$. Again, the set of parallel classes—which often are called *pencils*—is supposed to be linearly ordered.

Let us now drop the requirement of the linear ordering of classes of $\parallel$ and consider an incidence geometry defined by (A1), (A2) and

$$\forall p, q \in P\colon\ p \neq q\ \Rightarrow \exists!\, y \in L \text{ such that } p\varepsilon y \text{ and } q\varepsilon y. \tag{A3}$$

This may be interpreted by saying that any two points are connected by a unique line. (The requirement of uniqueness may be dropped since by (A1) and (A2) there cannot exist two distinct lines that would connect the points $p$ and $q$, $p \neq q$.)

A system fulfilling (A1), (A2) and (A3) is said to be an *affine plane* if the equivalence $\parallel$ contains at least three classes. (Axiomatizations of affine planes usually achieve the latter requirement by stipulating that there exist three points that are not collinear.)

For the sake of completeness let it be remarked that the usual way how an affine plane is defined is to take as axioms (A1), (A3) and the existence of three noncollinear points, under the assumption that $x \parallel y$ if and only if either $x = y$, or there exists no $p \in P$ with $p\varepsilon x$ and $p\varepsilon y$ (i.e., $x \cap y = \emptyset$). With such a definition it is straightforward to prove first that $\parallel$ is an equivalence on $L$, and then to derive (A2) from (A3).

**Collineations.** A *collineation* of an incidence geometry $(P, L, \varepsilon)$ is a pair $(\alpha, \beta)$ such that $\alpha$ permutes $P$, $\beta$ permutes $L$ and

$$p\,\varepsilon\, x\ \Leftrightarrow\ \alpha(p)\,\varepsilon\,\beta(x), \quad \text{for all } (p, x) \in P \times L.$$

To see how to connect this notion of collineation with a standard definition of collineation of a line system (i.e., a system in which lines are considered as sets of points) let us first discuss a certain property of incidence geometries that is usually assumed to be true, and that will be assumed to be true from here on when an incidence geometry will be discussed.

For each $y \in L$ put $\ell_y = \{p \in P;\, p\,\varepsilon\, y\}$. For each $p \in P$ put $c_p = \{y \in L;\, p\,\varepsilon\, y\}$ (the letter $c$ refers to lines *concurrent* to $p$. The property mentioned above states

that

$$\forall x, y \in L\ (x = y \Leftrightarrow \ell_x = \ell_y) \quad \text{and} \quad \forall p, q \in P\ (p = q \Leftrightarrow c_p = c_q).$$

In other words a line is determined completely by points incident to the line, and a point is determined completely by lines passing through the point. With this condition fufilled an incidence geometry may be turned into a system of lines $\mathcal{L} = \{\ell_y;\ y \in L\}$, where $p \varepsilon x \Leftrightarrow p \in \ell_y$.

It seems natural to define a collineation of a system of lines as a permutation of points such that a line is mapped upon a line. With an additional condition (like finiteness of the set, or the existence and uniqueness of a line passing through two points) this condition implies that the preimage of a line is a line. However, in general the latter property has to be considered as a part of definition. A collineation $\gamma$ of a system of lines thus is a permutation of points such that $\gamma(\ell)$ and $\gamma^{-1}(\ell)$ is a line whenever $\ell$ is a line.

To see that both definitions of collineation coincide let us show that if $(\alpha, \beta)$ is a collineation of $(P, L)$, then $\alpha$ is collineation of the system of lines $\{\ell_y;\ y \in L\}$, and that if $\gamma$ is a collineation of such a system of lines, then there exists $\beta$ such that $(\gamma, \beta)$ is a collineation of $(P, L)$.

*Proof.* The first step is to prove that if $(\alpha, \beta)$ is a collineation, then $\alpha(\ell_y) = \ell_{\beta(y)}$. This is true since $\alpha(p) \in \alpha(\ell_y) \Leftrightarrow p \in \ell_y \Leftrightarrow p \varepsilon y \Leftrightarrow \alpha(p) \varepsilon \beta(y) \Leftrightarrow \alpha(p) \in \ell_{\beta(y)}$, for all $(p, y) \in (P, L)$. For the converse direction assume that $(P, L)$ is an incidence geometry and $\gamma$ is a collineation of the line system $\{\ell_y;\ y \in L\}$. A line $\ell_y$ determines the element $y \in L$ completely. Hence there exists a permutation $\beta$ of $L$ such that $\gamma(\ell_y) = \ell_{\beta(y)}$. Now, $p \varepsilon y \Leftrightarrow p \in \ell_y \Leftrightarrow \gamma(p) \in \gamma(\ell_y) \Leftrightarrow \gamma(p) \in \ell_{\beta(y)} \Leftrightarrow \gamma(p) \varepsilon \beta(y)$. □

The notion of collineation need not be used only for permutations of $P \times L$. A collineation $(P, L, \varepsilon) \to (P', L', \varepsilon')$ is a pair $(\alpha, \beta)$ such that $\alpha$ is a bijection $P \to P'$, $\beta$ is a bijection $L \to L'$ and $p \varepsilon x \Leftrightarrow \alpha(p) \varepsilon' \beta(x)$. In terms of systems of lines $\gamma$ is a bijection of points that both $\gamma$ and $\gamma^{-1}$ map lines upon lines.

**Dual geometries and transversal designs.** The *dual* geometry of $(P, L, \varepsilon)$ is the geometry $(L, P, \varepsilon')$, where $p \varepsilon x \Leftrightarrow x \varepsilon' p$. Let us consider axioms (A1) and (A2) after dualization:

$$\forall p \in P\ \forall x \in L\ \exists!\, q \in P \text{ such that } p \parallel q \text{ and } q \,\varepsilon\, x; \text{ and} \tag{A1'}$$

$$\forall p, q \in P\colon p \nparallel q \ \Rightarrow\ \exists!\, x \in L \text{ such that } p \,\varepsilon\, x \text{ and } q \,\varepsilon\, x. \tag{A2'}$$

Consider a system fulfilling (A1') and (A2'). The equivalence $\parallel$ is now an equivalence of points. Classes of $\parallel$ are called *groups* (no connection to the algebraic notion of a group). Lines will be called *blocks*.

(A1') states that *each block passes through exactly one point of a group* and (A2') states that *two points from distinct groups belong to exactly one block*. A system of lines fulfilling these axioms is called a *transversal design*, provided that the number of groups is at least 3. If this number is equal to $k$, then the system is called a *transversal $k$-design*.

Groups of a transversal $k$-design are of the same size and this size is equal to the number of blocks passing through a point. Furthermore, each block is of size $k$. This is easy to prove. However, the proof may be omitted since the statement is a consequence of the fact that transversal $k$-designs dualize $k$-nets (with the exception that groups are not required to be linearly ordered).

The *order* of a transversal design is the number of points in a group. Transversal $k$-designs of order $n$ are sometimes denoted as $\mathrm{TD}(k, n)$.

**Counting and affine planes.** Let us have a $k$-net of a finite order $n$. (The order is the number of points upon a line, and this is equal to the number of lines in a pencil.)

The number of 2-elements sets $\{a,b\}$ such that $a$ and $b$ are points of the net and there exists a line $\ell$ (which is unique) that passes through both $a$ and $b$ is equal to

$$\text{`\# pencils'} \cdot \text{`\# lines in a pencil'} \cdot \text{`\# of pairs upon a line'} = kn\binom{n}{2} = \frac{kn^2(n-1)}{2}.$$

Number of all pairs of points in the net is

$$\binom{n^2}{2} = \frac{(n+1)n^2(n-1)}{2} \geq \frac{kn^2(n-1)}{2}.$$

Hence $n \geq k-1$. The equality takes place if and only if through each point there passes a line, i.e., when the $k$-net is an affine plane. We have proved:

- *If $n$ is the order of a $k$-net, then $n+1 \geq k$. The equality takes place if and only if the $k$-net is an affine plane.*
- *If $n$ the order of a transversal $k$-design, then $n+1 \geq k$. The equality takes place if and only if the design is the dual of an affine plane.*

**Projective planes.** A projective plane is a system of lines such that there exist four noncollinear points, each two lines intersect in a single point, and each two points are connected by a single line.

The notion of projective plane is self-dual. A removal of a line from a projective plane yields an affine plane. An affine plane may be completed to a projective plane by adding a new point for each pencil of lines. The lines of the pencil meet in this added point (which is called a point 'at infinity'). All points at infinity form a 'line at infinity'.

**Building an affine plane.** Let $(Q,+,\cdot,0,1)$ be an algebra such that $(Q,+,0)$ is a group, $(Q^*,\cdot)$ is a quasigroup, $Q^* = Q \setminus \{0\}$, and $x0 = 0x = 0$ for each $x \in Q$. For $a,b \in Q$ put $\ell_{a,b} = \{(\alpha,\beta) \in Q \times Q;\ \beta = a\alpha + b\}$ and $\ell_{\infty,b} = \{(b,\beta);\ \beta \in Q\}$. Set $Q_\infty = Q \cup \{\infty\}$ and put $\mathcal{L} = \{\ell_{a,b};\ (a,b) \in Q_\infty \times Q\}$. Elements of $\mathcal{L}$ will be called *lines*. The question when the line systems $\mathcal{L}$ is an affine plane is addressed below. Collineations of $\mathcal{L}$ will be discussed first.

**Collineations in the first coordinate.** Let us verify that for each $d \in Q$ the mapping $(\alpha,\beta) \mapsto (\alpha,\beta+d)$ is a collineation. This boils down to verifying

$$\ell_{a,b} \to \ell_{a,b+d} \text{ and } \ \ell_{\infty,b} \to \ell_{\infty,b}.$$

However, that is obvious since $\beta = a\alpha + b$ if and only if $\beta + d = a\alpha + (b+d)$.

**Collineations in the second coordinate.** The mapping $(\alpha,\beta) \mapsto (\alpha+c,\beta)$ is a collineation for each $c \in Q$ if and only if

$$x(y+z) = xy + xz \ \text{ for all } \ x,y,z \in Q.$$

*Proof.* A line $\ell_{\infty,b}$ is mapped upon $\ell_{\infty,b+c}$. A line $\ell_{0,b}$ is mapped upon itself. Let $(a,b) \in Q^* \times Q$. The case $c = 0$ is trivial, let us have $c \in Q^*$. If $(\alpha,\beta) \to (\alpha+c,\beta)$ is a collineation, then there has to exist $(a',b') \in Q^* \times Q$ such that

$$\beta = a\alpha + b \quad \Leftrightarrow \quad \beta = a'(\alpha+c) + b'.$$

Setting $\alpha = 0$ yields $\beta = b$ and $b = a'c + b'$. Hence $b' = -a'c + b = a'(-c) + b$.

Put now $\alpha = -c$. Then $a(-c) + b = b' = a'(-c) + b$. Therefore $a = a'$, and $a\alpha = a(\alpha+c) - ac$ for all $\alpha \in Q$. The latter equality yields the left distributive law since $a$ and $c$ are assumed to run through $Q^*$. □

**Under which conditions does $\mathcal{L}$ induce an affine plane?** Fix $a \in Q_\infty$ and put $\mathcal{L}_a = \{\ell_{a,b};\ b \in Q\}$. Claim: *Each point $(\alpha, \beta)$ belongs to exactly one $\ell \in \mathcal{L}_a$.* This is clear if $a = \infty$. Suppose that $a \in Q$, and observe that there exists exactly one $b \in Q$ such that $\beta = a\alpha + b$.

Lines of $\mathcal{L}_a$ thus partition the point set $Q \times Q$. This means that pencils of the purported affine plane have to coincide with sets $\mathcal{L}_a$.

Let $\ell$ and $\ell'$ be lines from different pencils. If $\ell \in \mathcal{L}_\infty$ or $\ell \in \mathcal{L}_0$, then one of the coordinates is fixed, and that makes $\ell$ to intersect $\ell'$ in exactly one point.

Let us have $\ell = \ell_{a,b}$ and $\ell' = \ell_{a',b'}$, where $a, a' \in Q^*$ and $b, b' \in Q$, $a \neq a'$. The lines $\ell$ and $\ell'$ intersect in exactly one point if and only if the equation $ax + b = a'x + b'$ has exactly one solution $x \in Q$. Since the equation may be written as $a'x = ax + (b - b')$, axiom (A2) holds if and only if

$$\forall a, b, c \in Q\colon\ a \neq b \ \Rightarrow\ \exists! x \in Q \text{ such that } ax + c = bx. \tag{AF2}$$

The axiom (A3) holds if any two distinct points $(\alpha, \beta)$ and $(\alpha', \beta')$ are contained in exactly one line $\ell$. If $\alpha = \alpha'$, then $\ell = \ell_{\infty,\alpha}$. Assume $\alpha \neq \alpha'$. The task is to solve equations $x\alpha + \beta = y = x\alpha' + \beta'$. The solution $(x, y)$ is determined by the value of $x$ uniquely. The equation may be written as $x\alpha + (\beta - \beta') = x\alpha'$. Hence (A3) holds if and only if

$$\forall a, b, c \in Q\colon\ a \neq b \ \Rightarrow\ \exists! x \in Q \text{ such that } xa + c = xb. \tag{AF3}$$

**Quasifield defined.** Results above bring us to the following definition. A quasifield is an algebra $(Q, +, \cdot, 0, 1)$ such that

- $(Q, +, 0)$ is a group;
- $(Q^*, \cdot, 1)$ is a loop;
- $x(y + z) = xy + xz$ for all $x, y, z \in Q$; and
- for all $a, b, c \in Q$, $a \neq b$ there exists unique $x \in Q$ such that $ax = bx + c$.

The definition above is the definition of a *left quasifield*. The right quasifield is obtained by using mirror conditions. In the following a *quasifield* means the left quasifield. For the sake of completeness recall that $Q^* = Q \setminus \{0\}$.

**Proposition.** *Let $Q$ be a quasifield. Then $a0 = 0a = 0$ for every $a \in Q$. Furthermore, $a(-b) = -ab$ and $a + b = b + a$, for any $a, b \in Q$.*

*Proof.* To prove that $a0 = 0$ write $a0$ as $a(0 + 0) = a0 + a0$. To prove the mirror equality assume that $0b \neq 0$. Then $b \neq 0$ and there exists $a \in Q^*$ such that $ab = 0b$. The equation $ax = 0x$ hence possesses two different solutions $x = b$ and $x = 0$. That is a contradiction.

Note that $0 = a0 = a(b + (-b)) = ab + a(-b)$ implies $a(-b) = -ab$, for any $a, b \in Q$.

Suppose now that $a, b \in Q$ are such that $a + b \neq b + a$. This implies $a \neq 0$ and $b \neq 0$. Put $t = b + a - b$. The assumption is that $t \neq a$. We have $t \neq 0$. There thus exists $s \neq 1$ such that $sa = t$. Let $x$ be the only solution to $x = sx + b$. Then

$$x + a - b = sx + b + a - b = sx + t = sx + sa = s(x + a).$$

The equation $y - b = sy$ thus possesses solutions $y = x$ and $y = x + a$. Hence $x = x + a$, and $a = 0$, a contradiction. □

**Prequasifields.** The definition of a prequasifield differs from that of a quasifield by relaxing the assumption of $(Q^*, \cdot)$ being a loop to $(Q^*, \cdot)$ being a quasigroup. Everything above that is true for quasifields remains to be true for prequasifields. This is also the case of the preceding proof since the equation $x = sx + b$ may be replaced by an equation $ux = sx + b$, where $u \in Q^*$ is chosen in such a way that $ua = a$.

**Prequasifields yield affine planes.** Systems $(Q,+,0,\cdot)$ describe an affine plane with lines $\ell_{a,b}$, $(a,b)\in Q_\infty\times Q$, if $(Q,+,0)$ is a group and both (AF2) and (AF3) hold. This has been proved above. (Conditions (AF2) and (AF3) imply that $(Q^*,\cdot)$ is a quasigroup, as may be verified easily.) To see that a prequasifield can be used to construct an affine plane note that (AF2) is one of its axioms, while (AF3) follows from the left distributivity since $xa=xb+c$ may be written as $x(a-b)=c$.

**Left division and the left distributive law.** Suppose that $(Q,+,0)$ is a group and that $\cdot$ is a binary operation upon $Q$ such that $(Q^*,\cdot)$ a quasigroup. If $\cdot$ and $+$ are connected by the left distributive law, then the equation $a(0+0)=a0+a0$ implies $a0=0$ like above. Set $a\backslash 0=0$, for each $a\in Q$.

The equality $a(b+c)=ab+ac$ holds for all $b,c\in Q$ if and only if $L_a\in\mathrm{End}(Q,+)$. If $a\in Q^*$, then in fact this is the same as $L_a\in\mathrm{Aut}(Q,+)$, and thus also the same as $L_a^{-1}\in\mathrm{Aut}(Q,+)$. Since $L_a^{-1}(b)=a\backslash b$ we can state that

$$(\forall x,y,z\in Q\ x(y+z)=xy+xz)\ \Rightarrow\ (\forall x,y,z\in Q\ x\backslash(y+z)=x\backslash y+x\backslash z).$$

**Principal loop isotopes of a prequasifield.** *Let $e$ and $f$ be nonzero elements of a prequasifield $(Q,+,\cdot,0)$. If $x*y=(x/f)(e\backslash y)$ for all $x,y\in Q$, then $(Q,+,*,0,ef)$ is a quasifield.*

*Proof.* If $a,b,c\in Q$, then

$$a*(b+c)=a/f\cdot e\backslash(b+c)=a/f\cdot(e\backslash b+e\backslash c)=(a/f)(e\backslash b)+(a/f)(e\backslash c)=a*b+a*c.$$

A solution to $a*x=b*x+c$, $a\neq b$, has to fulfil $a/f\cdot e\backslash x=b/f\cdot e\backslash x+c$. This determines $x$ uniquely since $e\backslash x=d$, where $d$ is the only solution to $a/f\cdot y=b/f\cdot y+c$. □

**Collineation induced by isotopy.** *The mapping $(\alpha,\beta)\mapsto(e\alpha,\beta)$ yields a collineation of the affine plane induced by a prequasifield $(Q,+,\cdot,0)$ on the affine plane induced by the quasifield $(Q,+,*,0,ef)$, where $e,f\in Q^*$ and $x*y=x/f\cdot e\backslash y$ for all $x,y\in Q$.*

*Proof.* Lines $\ell_{a,b}$ are given by solutions to $y=ax+b$. Lines $\ell^*_{a,b}$ are given by solutions to $y=a*x+b$. We have $(\alpha,\beta)\in\ell_{a,b}$ if and only if $\beta=(af)*(e\alpha)+b$, i.e., if and only if $(e\alpha,\beta)\in\ell^*_{af,b}$.

Furthermore, the line $\ell_{\infty,b}$ is mapped upon $\ell^*_{\infty,eb}$ since $\alpha=b$ if and only if $e\alpha=eb$. □

**Finite quasifields.** Let $(Q,+,0)$ be a group and $(Q^*,*)$ a quasigroup that are connected by the left distributive law. Then $a0=0$ and $a(-b)=-ab$, for all $a,b\in Q$. However there is no way how to prove $0a=0$. To see this suppose that the latter holds and change it to $0a=\varphi(a)$, where $\varphi\in\mathrm{End}(Q,+)$. That does not change the assumptions on $+$ and $\cdot$.

However, if $0a=0$ for all $a\in Q$, then there exists at most one $x\in Q$ such that $ax=bx+c$, whenever $a,b,c\in Q$ and $a\neq b$. To see this assume that $ax=bx+c$ and $ay=by+c$. Then $-bx+ax=-by+ay$, $ax-ay=bx-by$ and $a(x-y)=b(x-y)$. This is not possible if $x-y\neq 0$.

By the same token there cannot be $-bx+ax-c=-by+ay-c$ if $a,b,c,x,y\in Q$, $a\neq b$ and $x\neq y$. The mapping $x\mapsto -bx+ax-c$ is hence an injective mapping $Q\to Q$ whenever $a,b,c\in Q$ and $a\neq b$. If $Q$ is finite, then there exists $x\in Q$ such that $-bx+ax-c=0$, which means $ax=bx+c$. This shows that *in the finite case a prequasifield may be defined by assuming that $(Q,+,0)$ is a group, $(Q^*,\cdot)$ a quasigroup, $0a=0$ for all $a\in Q$, and $a(b+c)=ab+ac$ for all $a,b,c\in Q$.*

Furthermore, verifying that $(Q^*,\cdot)$ is a quasigroup may be simplified if

$$ab=0\ \Leftrightarrow\ a=0\text{ or }b=0,\text{ for all }a,b\in Q. \tag{Z}$$

If the latter holds, then each $L_a$, $a \in Q^*$, has to be injective (and thus bijective in the finite case) since $ax = ay$ if and only if $a(x - y) = 0$.

**Semifields.** A *semifield* $(S, +, \cdot, 0, 1)$ is an algebra such that $(S, +, 0)$ is a group, $(S^*, \cdot, 1)$ is a loop, and both distributive laws hold (thus $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for all $a, b, c \in S$.) A *presemifield* does not require the existence of the unit element.

By standard arguments, $a0 = 0 = 0a$ and $a(-b) = -ab = (-a)b$, for all $a, b \in S$. Each semifield is a quasifield since if $ax = bx + c$ and $a \neq b$, then $-bx + ax = (-b + a)x = c$, and that determines $x$ uniquely. For the finite (pre)semifield the quasigroup property of $\cdot$ may be replaced by (Z).

Note that the definition of a semifield differs from the definition of a division ring (a skewfield) by dropping the associativity of the multiplication.

**Nearfields.** A *nearfield* $(N, +, \cdot, 0, 1)$ is an algebra such that both $(N, +, 0)$ and $(N^*, \cdot, 1)$ are groups, and the left distributive law holds.

By standard arguments, $a0 = 0$ and $a(-b) = -ab$ for all $a, b \in N$. If $0b \neq 0$, then $a(0b) = (a0)b = 0b$ for all $a \in N$. That cannot be true if $N^*$ is nontrivial, i.e. if $|N| \geq 3$. On two elements the definition above allows for the multiplication given by $xy = y$. This is an exceptional case that is not regarded to be a nearfield. To avoid it, the axioms may be extended by stating explicitly that $0x = 0$ for all $x \in N$.

A finite nearfield fulfils the conditions of finite quasifield. An infinite nearfield need not be a quasifield. However, it may be proved that every nearfield $N$ fulfils $a + b = b + a$ and $(-a)b = -ab$, for all $a, b \in N$. A nearfield which is a quasifield is called *planar* as it determines an affine plane (and thus also a projective plane).

Note that the definition of a nearfield differs from the definition of a division ring (a skewfield) by dropping the right distributive law. In fact, our definition is that of the *left nearfield*. The *right nearfield* assumes the right distributive law.

**Connections to projective planes.** If $a$ is a point and $\ell$ a line of a projective plane then there may exist a collineation called *perspectivity* that is determined uniquely by $(a, \ell)$ ($a$ is called the center and $\ell$ the axis). Projective planes determined by division rings contain a perspectivity for each pair $(a, \ell)$. In fact this is a way how to characterize them. Assumptions of the form that a perspectivity exists for certain pairs $(a, \ell)$ gives rise to notions of quasifield, semifield, nearfield in the sense that if the respective assumptions are fulfilled, then the projective plane induces an affine plane that may be coordinatized by a quasifield or a semifield or a nearfield.

**Remarks on coordinatization and isotopy.** Note that above we have proved that affine planes coordinatized by isotopic prequasifields are isomorphic. From the geometric standpoint isotopic quasifields are nothing else but different coordinatizations of the same geometric structure.

Note that a principal isotope $x/f \cdot e\backslash y$ of a semifield is again a semifield, and that the same is true for nearfields. Two semifields (or nearfields) are said to be isotopic, if one of them is isomorphic to the principal isotope of the other. It is easy to adapt Albert's theorem to nearfields, showing thus that isotopic nearfields are isomorphic.

# Nearfields

**Definition of nearfield and commutativity.** By definition, $(N, +, \cdot, 0, 1)$ is a nearfield if $(N, +, 0)$ and $(N^*, \cdot, 1)$ are groups, $x(y+z) = xy+xz$ for all $x, y, z \in N$, and the 2-element structure with $xy = y$ is avoided. To avoid it, it may be assumed, e.g., that $0 \cdot 1 = 0$.

In every nearfield $x+y = y+x$, for every $x$ and $y$. The proof of commutativity is nontrivial in the general case. In finite case the commutativity follows from the fact that finite nearfields are quasifields. Another proof of commutativity in the finite case relies upon the fact that $x \mapsto cx$ is an automorphism of $(N, +, 0)$ for every $c \in N^*$. This means that $c = c \cdot 1$ is an automorphic image of the element 1. Hence all elements of $N^*$ are of the same order. This is possible if and only if each element of $N^*$ is of a prime order $p$. Therefore $(N, +, 0)$ is a $p$-group. A $p$-group always contains a nontrivial center. A nontrivial element of this center is an automorphic image of 1. Hence 1 belongs to the center. Each element of $N^*$ is thus central. This proves that *the additive group of a finite nearfield is an elementary abelian $p$-group, $p$ a prime.*

Further on the additive group of $(N, +)$ will always be considered to be commutative.

**Opposite elements in a nearfield.** As observed earlier, $0a = a0 = 0$ and $a(-b) = -ab$ in every nearfield $N$. In a nearfield $a + b = b + a$. Here we shall show that $(-a)b = -ab$ for all $a, b \in N$.

*Lemma. An element $a \in N$ fulfils $a^2 = 1$ if and only if $a = \pm 1$.*

*Proof.* $(-1)(-1) = -(-1) = 1$. If $a^2 = 1$, then $a(a+1) = a^2 + a = 1 + a = 1(a+1)$. If $a + 1 \neq 0$, then $a = 1$. If $a + 1 = 0$, then $a = -1$. □

*Lemma. Every $a \in N$ fulfils $(-1)a = -a$.*

*Proof.* This is clear if $a = 0$. Assume $a \neq 0$ and consider $b \in N^*$ such that $ab = 1$. Then $ba = 1$ and $(a \cdot (-1) \cdot b)(a \cdot (-1) \cdot b) = a \cdot (-1) \cdot (-1) \cdot b = a \cdot b = 1$. By the lemma, $a \cdot (-1) \cdot b = \pm 1$. If $a \cdot (-1) \cdot b = 1 = ab$, then $-a = a(-1) = a$. In such a case $0 = a + a$ and $0 = b(a + a) = ba + ba = 2$. That implies $-1 = 1$. Hence $a \cdot (-1) \cdot b = -1$ in every case. This yields $a \cdot (-1) = (-1)a$, by multiplying by $a$ on the right. Hence $(-1)a = a(-1) = -a$. □

To finish note that $-ab = (-1)ab = (-1)a \cdot b = (-a)b$, for all $a, b \in N$.

**Few notions from permutation groups.** Let $G$ be a permutation group upon $\Omega$. Recall that $G_\alpha = \{g \in G;\ g(\alpha) = \alpha\}$, for all $\alpha \in \Omega$. A similar notation is used for the *pointwise stabilizer* of $\alpha_1, \ldots, \alpha_k \in \Omega$ (assuming implicitly that the latter elements are pairwise distinct). Set

$$G_{\alpha_1,\ldots,\alpha_k} = \{g \in G;\ g(\alpha_1) = \alpha_1,\ \ldots,\ g(\alpha_k) = \alpha_k\}.$$

The group is *transitive* if for all $\alpha, \beta \in \Omega$ there exists $g \in G$ such that $g(\alpha) = \beta$. Note that for $G$ to be transitive it suffices that there exists $\alpha \in \Omega$ such that for each $\beta \in \Omega$ there exists $g \in G$ such that $g(\alpha) = \beta$.

The group $G$ is said to be 2-*transitive* if for all $\alpha, \beta, \gamma, \delta \in \Omega$ such that $\alpha \neq \beta$ and $\gamma \neq \delta$ there exists $g \in G$ such that $g(\alpha) = \gamma$ and $g(\beta) = \delta$. Note that for $G$ to be 2-transitive it suffices that there exist $\alpha, \beta \in \Omega$, $\alpha \neq \beta$, such that for all $\gamma, \delta \in \Omega$, $\gamma \neq \delta$, there exists $g \in G$ such that $g(\alpha) = \gamma$ and $g(\beta) = \delta$.

If $G$ is 2-transitive, and there exists only one $g \in G$ such that $g(\alpha) = \gamma$ and $g(\beta) = \delta$, then $g$ is said to be *sharply* 2-*transitive*.

Note that the similar notion of sharp 1-transitivity coincides with the notion of a regular permutation group. Note also that a 2-transitive permutation group is sharply 2-transitive if and only if $G_{\alpha,\beta} = 1$, whenever $\alpha, \beta \in \Omega$ and $\alpha \neq \beta$.

The permutation group $G$ is said to be a *Frobenius group* if it is transitive, but not regular, and fulfils $G_{\alpha,\beta} = 1$ whenever $\alpha, \beta \in \Omega$ and $\alpha \neq \beta$. By a well known theorem a finite Frobenius group contains a normal subgroup that consists of the identity mapping and of all mappings $g \in G$ such that $g(\alpha) = \alpha$ for no $\alpha \in \Omega$ (the regular permutations of $G$). This subgroup is normal and is called the *Frobenius kernel*. Each sharply 2-transitive group is a Frobenius group. The converse is not true.

**Affine mappings of a nearfield.** Let $N$ be a nearfield. Denote by $\mathrm{Aff}(N)$ the set of all mappings $x \mapsto ax + b$, where $a \in N^*$ and $b \in N$. The set $\mathrm{Aff}(N)$ forms a group and this group is sharply 2-transitive.

As explained above, to prove this it suffices to show that for $c, d \in N$, $c \neq d$, there exist a unique affine mapping $x \mapsto ax + b$ that sends 0 upon $c$ and 1 upon $d$. These assumptions mean that $c = a0 + b = b$ and $d = a1 + b = a + b$. Setting $a = d - c$ and $b = c$ thus does the job.

**Finite nearfields are equivalent to sharply 2-transitive groups.** Let $G$ be a sharply 2-transitive permutation group upon a finite set $N$. Choose an element of $N$ and denote it by 0. The Frobenius kernel of $G$ is a regular group upon $N$. Hence $N$ may be considered as a group $(N, +, 0)$, where $+$ is defined in such a way that the Frobenius kernel coincides with the set of left translations $L_a$, $a \in N$. (The way how to define $+$ is described in the passage about regular group.)

The Frobenius kernel is a normal subgroup of $G$. Hence if $g \in G$, then for each $a \in N$ there exists $b \in N$ such that $gL_ag^{-1} = L_b$. If $g \in G_0$, then $gL_a(0) = g(a) = b = L_b(0) = L_bg(0)$. Thus $gL_ag^{-1} = L_{g(a)}$ for each $g \in G_0$ and $a \in N$.

Choose a nonzero element of $N$ and denote it by 1. Define multiplication upon $N$ so that $0a = 0$ and $ab = \varphi_a(b)$ whenever $a, b \in N$, $a \neq 0$ and $\varphi_a$ is the unique element of $G_0$ that sends 1 upon $a$. Put $N^* = N \setminus \{0\}$ and denote by $\varphi_a^*$ the restriction of $\varphi_a$ to $N^*$. By the definition $ab = \varphi_a^*(b)$ for all $a, b \in N^*$. The group $G_0$ consists of all $\varphi_a$, $a \in N^*$. Permutations $\varphi_a^*$ coincide with left translations of $(N^*, \cdot)$. That makes $(N^*, \cdot)$ a group. Note that $\cdot$ is defined in accordance with the general procedure of deriving an abstract group from a regular group. The neutral element of $N^*$ is equal to 1 since $\varphi_1 = \mathrm{id}_N$.

The left distributive law $a(b+c) = ab+ac$ clearly holds if $a = 0$. Assume $a \in N^*$. Then $a(b + c) = \varphi_a L_b(c) = L_{\varphi_a(b)}\varphi_a(c) = L_{ab}(ac) = ab + ac$.

**Dickson nearfields.** Finite nearfields are thus equivalent to sharply 2-transitive permutation groups. All such groups are known. Their classification belongs to Zassenhaus. Here it will not be discussed. The simplest example of *proper nearfields* (that is nearfields that do not satisfy the right distributive law) are Dickson nearfields.

A *Dickson nearfield* is obtained by replacing the multiplication $\cdot$ of $\mathbb{F}_{q^2}$ (the finite field of order $q^2$), $q$ odd, by multiplication $\circ$ that is defined as follows:

$$a \circ b = \begin{cases} ab & \text{if } a \text{ is a square;} \\ ab^q & \text{if } a \text{ is a nonsquare.} \end{cases}$$

**Exercise.** Show that $(\mathbb{F}_{q^2}, +, \circ, 0, 1)$ is a nearfield, for any $q > 1$ that is a power of odd prime.

**Exercise.** The smallest order of a Dickson nearfield (and, in fact, of any proper nearfield) is 9. Prove that $(\mathbb{F}_9^*, \circ)$ is isomorphic to $Q_8$, the group of quaternions.

**Quasigroups from nearfields.** Let $(N,+,\cdot,0,1)$ be a nearfield. Choose an element $c \in N$, $c \notin \{0,1\}$, and define a binary operation $*_c$ upon $N$ by

$$x *_c y = x + (y-x)c \text{ for all } x,y \in N.$$

Suppose that $a,b \in N$.

$$\begin{aligned} a *_c y = b &\Leftrightarrow a + (y-a)c = b \Leftrightarrow y - a = (-a+b)c^{-1}, \text{ and} \\ x *_c a = b &\Leftrightarrow x + (a-x)c = b \Leftrightarrow (-a+x) + (a-x)(c) = -a+b \\ &\Leftrightarrow (a-x)(-1) + (a-x)(c) = -a+b \Leftrightarrow (a-x)(-1+c) = -a+b \\ &\Leftrightarrow a - x = (-a+b)(-1+c)^{-1}. \end{aligned}$$

Both equations thus possess a unique solution. That makes $(N,*_c)$ a quasigroup. This quasigroup is idempotent since $a *_c a = a + (a-a)c = a + 0c = a$.

**Theorem.** *Let $N$ be a nearfield, $c \in N$, $c \notin \{0,1\}$. Then* $\mathrm{Aff}(N) \leq \mathrm{Aut}(N,*_c)$.

*Proof.* The group $\mathrm{Aff}(N)$ is generated by mappings $x \mapsto x+v$, $v \in N$, and mappings $x \mapsto ux$, $u \in N^*$. The proof uses the commutativity of $+$. If $x,y \in N$, then $(x+v) *_c (y+v) = x + (y-x)c + v = (x *_c y) + v$ since $(y+v) - (x+v) = y - x$. Furthermore, $ux *_c uy = ux + (uy - ux)c = ux + u(y-x)c = u(x + (y-x)c) = u(x *_c y)$. □

**A lemma of general nature.** *Let $(Q,*)$ be an idempotent quasigroup. If $x,y \in Q$ are such that $(x,x,y)$ or $(y,x,x)$ is an associative triple, then $x = y$.*

*Proof.* Assume $x * (x * y) = (x * x) * y$. Since $(x * x) * y = x * y$ there must be $x * y = y = y * y$. Thus $x = y$. □

**Flexibility.** A binary operation $\cdot$ is said to be *flexible* if it fulfils the *flexible law* $xy \cdot x = x \cdot yx$.

Let $N$ be a nearfield, and $c \in N \setminus \{0,1\}$. The aim now is to prove that $*_c$ *is flexible if and only if* $c(1-c) = (1-c)c$. *If* $c(1-c) \neq (1-c)c$ *then* $(a,b,a)$ *is never associative if* $a,b \in N$ *and* $a \neq b$.

First note if $(Q,\cdot)$ is a quasigroup and $\alpha \in \mathrm{Aut}(Q)$, then $(a,b,c) \in Q^3$ is associative if and only if $(\alpha(a),\alpha(b),\alpha(c))$ is associative. This is because $\alpha(a)\alpha(b) \cdot \alpha(c) = \alpha(ab \cdot c)$ and $\alpha(a) \cdot \alpha(b)\alpha(c) = \alpha(a \cdot bc)$.

Consider $a,b \in N$, $a \neq b$. Since $\mathrm{Aff}(N)$ is 2-transitive, there exists $\alpha \in \mathrm{Aff}(N)$ such that $\alpha(0) = a$ and $\alpha(1) = b$. Recall that $\mathrm{Aff}(N) \leq \mathrm{Aut}(N,*_c)$. This means that $(a,b,c)$ is associative if and only if $(0,1,0)$ is associative.

Plugging $x = 0$ into $x *_c y = x + (y-x)c$ gives $0 *_c y = yc$. Furthermore, $x *_c 0 = x + (-x)c = x1 + x(-c) = x(1-c)$. Hence

$$\begin{aligned} &0 *_c (1 *_c 0) = (1 *_c 0)c = (1-c)c, \text{ and} \\ &(0 *_c 1) *_c 0 = c *_c 0 = c(1-c). \end{aligned}$$

**Flexibility in Dickson nearfields.** The operation of the Dickson nearfield upon $\mathbb{F}_{q^2}$ is denoted by $\circ$. For $i,j \in \{0,1\}$ set $i = 0$ if $c$ is square and $i = 1$ if it is a nonsquare. Similarly set $j = 0$ if $1-c$ is a square, and $j = 1$ othewise. Then

| $ij$ | 00 | 01 | 10 | 11 |
|---|---|---|---|---|
| $c \circ (1-c)$ | $c(1-c)$ | $c(1-c)$ | $c(1-c)^q$ | $c(1-c)^q = c - c^{q+1}$ |
| $(1-c) \circ c$ | $c(1-c)$ | $c^q(1-c)$ | $c(1-c)$ | $c^q(1-c) = c^q - c^{q+1}$ |

The table shows that if $c$ is a nonsquare or $1-c$ is a nonsquare, then $c \circ (1-c) = (1-c) \circ c$ implies $c = c^q$ or $1-c = (1-c)^q$. Now, $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{q^2}$ that consists of all $a \in \mathbb{F}_{q^2}$ that fulfil $a^q = a$. Since each element of $\mathbb{F}_q$ is a square in $\mathbb{F}_{q^2}$, the equality $c \circ (1-c) = (1-c) \circ c$ holds if and only if both $c$ and $1-c$ are squares.

In other words, $(\mathbb{F}_{q^2}, *_c)$ is flexible if and only if both $c$ and $1-c$ are squares, whenever $c \in \mathbb{F}_{q^2}$ and $c \notin \{0,1\}$.

**Maximal nonassociativity via nearfields.** Let $c$ be an element of a nearfield $N$ such that $c(1-c) \neq (1-c)c$. If $(x,y,z)$ is a nondiagonal associative triple in $(N, *_c)$, then the elements $x$, $y$ and $z$ have to be pairwise distinct, by the results above.

Since there exists $\alpha \in \mathrm{Aff}(N) \leq \mathrm{Aut}(N, *_c)$ such that $\alpha(0) = x$ and $\alpha(1) = y$, the quasigroup $(N, *_c)$ **is maximally nonassociative if and only if** $(0 *_c 1) *_c z \neq 0 *_c (1 *_c z)$ **for every** $z \in N$, $z \notin \{0,1\}$. Note that

$$(0 *_c 1) *_c z = c + (z-c)c \text{ and } 0 *_c (1 *_c z) = (1 + (z-1)c)c.$$

**Maximal nonassociativity via Dickson nearfields.** It may be proved that for each odd $q > 1$, $q$ a power of an odd prime, there exists $c \in \mathbb{F}_{q^2}$ such that the quasigroup $(\mathbb{F}_{q^2}, *_c)$ is maximally nonassociative. The proof is nonconstructive—the idea is to estimate the number of $c \in \mathbb{F}_{q^2}$, $c \notin \{0,1\}$, for which there exists a nondiagonal associative triple, and show that this number is less than $q^2 - 2$.

The case of $q = 3$ is easy to verify by hand. It turns out that $(\mathbb{F}_9, *_c)$ is maximally nonassociative whenever $c \notin \mathbb{F}_3$. Furthermore, if $c, d \in \mathbb{F}_9 \setminus \mathbb{F}_3$, then $(\mathbb{F}_9, *_c) \cong (\mathbb{F}_9, *_d)$.

**The weighted average.** Consider now the quasigroup $(F, *_c)$ in the case when $F$ is a field (or, more generally, a division ring), and $c \notin \{0,1\}$. The operation

$$x *_c y = x + (y-x)c = x(1-c) + yc$$

is known as the *weighted average*. It fulfils the *medial* law $xy \cdot uv = xu \cdot yv$. That may easily be verified directly. Another way how to prove it is to use a construction below. The connection to the construction is by the fact that both $x \mapsto xc$ and $x \mapsto x(1-c)$ are automorphisms of the group $(F, +, 0)$.

Another name for the medial law is the *entropic* law.

**A construction.** Let $(G, +)$ be an Abelian group, and let $\alpha$ and $\beta$ be commuting automorphisms of $(G, +)$ (thus $\alpha\beta = \beta\alpha$). Furthermore, let $c$ be an element of $G$. For $x, y \in G$ set

$$x * y = \alpha(x) + \beta(y) + c.$$

Then $(G, *)$ is quasigroup isotopic to $(G, +)$. If $x, y, u, v \in G$, then

$$\begin{aligned}(x * y) * (u * v) &= (\alpha(x) + \beta(y) + c) * (\alpha(u) + \beta(v) + c) \\ &= \alpha^2(x) + \alpha\beta(y) + \beta\alpha(u) + \beta^2(v) + \alpha(c) + \beta(c) + c \\ &= \alpha^2(x) + \alpha\beta(u) + \beta\alpha(y) + \beta^2(v) + \alpha(c) + \beta(c) + c \\ &= (x * u) * (y * v).\end{aligned}$$

Note that if $c = 0$ and $\alpha + \beta = \mathrm{id}_G$, then $x * x = x$. This is the case of the weighted average. Idempotent medial quasigroups are flexible. Indeed if $(Q, \cdot)$ is such a quasigroup, then $x \cdot yx = xx \cdot yx = xy \cdot xx = xy \cdot x$.

**Toyoda theorem.** *Let $(Q, *)$ be a medial quasigroup. Then $Q$ may be equipped with the structure of an abelian group in such a way that there exist $\alpha, \beta \in \mathrm{Aut}(Q, +)$ and $c \in Q$ that fulfil $\alpha\beta = \beta\alpha$ and $x * y = \alpha(x) + \beta(y) + c$, for all $x, y \in Q$.*

The proof of Toyoda theorem takes about one page. One of the methods is to use properties of autotopisms.

**Quasigroups induced by a coordinatization of an affine plane.** A finite affine plane may be obtained from $(Q, +, \cdot, 0, 1)$, where $(Q, +, 0)$ is a group, $(Q^*, \cdot, 1)$ a loop, if $0a = a0 = 0$ for all $a \in Q$ and the equation $ax + c = bx$ has a unique solution whenever $a, b \in Q$ and $a \neq b$. This is what will be assumed further on. In infinite case the existence of the affine plane also needs the condition that the equation $xa + c = xb$ has a unique solution whenever $a, b \in Q$ and $a \neq b$.

For each $c \in Q^*$ define a binary operation $*_c$ on $Q$, $c \in Q^*$, by

$$a *_c b = a + cb \text{ for every } a, b \in Q.$$

If $x *_c b = a$, then $x + cb = a$ and $x = a - cb$. If $a *_c y = b$, then $a + cy = b$, $cy = -a + b$ and $y = c\backslash(-a + b)$ ($c\backslash 0$ is defined as 0). This shows that $(Q, *_c)$ is a quasigroup for all $c \in Q^*$.

Suppose now that $c, d \in Q^*$ and $c \neq d$. Let us consider $u, v \in Q$ and ask for which $(x, y) \in Q^2$

$$x *_c y = u \text{ and } x *_d y = v.$$

Any such $(x, y)$ fulfils $x = u - cy$ and $x = v - dy$. Thus $cy - u = -x = dy - v$. Therefore $cy = dy - v + u$. Since $c \neq d$ there exists only one $y \in Q$ that fulfils the latter equality, and $(u - cy, y)$ is the only solution to the equations above.

The latter fact may be expressed also by saying that the quasigroups $(Q, *_c)$ and $(Q, *_d)$ are orthogonal, in the sense described below.

**Orthogonality.** Quasigroups $(Q, \cdot)$ and $(Q, *)$ are said to be *orthogonal* if for all $u, v \in Q$ there exists exactly one pair $(x, y) \in Q \times Q$ such that $xy = u$ and $x * y = v$. Two latin squares of the same order (and the same set of symbols) are said to be *orthogonal* if they may be interpreted as multiplication tables of orthogonal quasigroups.

A set of quasigroups $(Q, *_1)$, ..., $(Q, *_k)$ is said to be *mutually orthogonal* if $(Q, *_i)$ and $(Q, *_j)$ are orthogonal whenever $1 \leq i < j \leq k$. Similarly define *mutually orthogonal latin squares*. The latter is often abbreviated as MOLS.

If $(Q, +, \cdot, 0, 1)$ coordinatizes an affine plane and $|Q| = n$, then $(Q, *_c)$, $c \in Q^*$ is a set of $n - 1$ mutually orthogonal quasigroups. The affine plane induced by $(Q, +, \cdot, 0, 1)$ thus yields $n - 1$ mutually orthogonal latin squares of order $n$.

For each $n \geq 2$ denote by $N(n)$ the maximum size of MOLS of order $n$. We shall explain why $N(n) \leq n - 1$ and why a set of $n - 1$ MOLS describes an affine plane of order $n$ or, and thus also a a projective plane of order $n$. (The order of an affine plane is the number of points upon a line. The order of an projective plane is the number of points upon a line diminished by one.)

**Transversal designs from orthogonal quasigroups.** Suppose that $(Q, *_i)$, $1 \leq i \leq k$, is a set of mutually orthogonal quasigroups, $k \geq 2$. Put $\Omega = Q \times \{\infty, 0, 1, \ldots, k\}$. Construct a block design upon $\Omega$ with groups $Q \times \{\infty\}$, $Q \times \{0\}$, $Q \times \{1\}$, ..., $Q \times \{k\}$ in such a way that $\{(a_\infty, \infty), (a_0, 0), (a_1, 1), \ldots, (a_k, k)\}$ is a block if and only if there exist $x, y \in Q$ such that $(a_\infty, a_0, a_1, \ldots, a_k) = (x, y, x *_1 y, \ldots, x *_k y)$.

A block is thus fully determined by $x = a_\infty$ and $y = a_0$. If $1 \leq i \leq k$, then it is also fully determined by $x = a_\infty$ and $x *_i y = a_i$, or by $y = a_0$ and $x *_i y = a_i$. If $1 \leq i < j \leq k$ then for any $a_i$ and $a_j$ there exist unique $x, y \in Q$ such that $x *_i y = a_i$ and $x *_j y = a_j$. This means that there exists a unique block that passes through $(a_i, i)$ and $(a_j, j)$. We have verified that the design is a transversal $(k + 2)$-design of order $n = |Q|$.

**Orthogonal quasigroups from transversal designs.** Let us have a transversal $(k+2)$-design, $k \geq 2$. Denote the groups by $G_\infty$, $G_0$ and $G_i$, $1 \leq i \leq k$. The groups are of the same size. Let $Q$ be a set for which there exist bijections $\gamma_j \colon Q \to G_j$, $j \in \{\infty, 0, 1, \ldots, k\}$. Bijections $\gamma_\infty$, $\gamma_0$ and $\gamma_i$, $1 \leq i \leq k$, provide a quasigroup $(Q, *_i)$ in which $x *_i y = z$ whenever there exists a block of the design that passes through $\gamma_\infty(x)$, $\gamma_0(y)$ and $\gamma_i(z)$.

Suppose that $1 \leq i < j \leq k$ and consider $u, v \in Q$. There exists exactly one block $B$ of the design that passes through $\gamma_i(u)$ and $\gamma_j(v)$. Let $x, y \in Q$ be such that $\gamma_\infty(x) \in B$ and $\gamma_0(y) \in B$. Then $x *_i y = u$ and $x *_j y = v$. The block $B$ is determined uniquely by $(i, j, u, v)$. There thus exists a unique pair $(x, y) \in Q \times Q$ such that $x *_i y = u$ and $x *_j y = v$. This means that quasigroups $(Q, *_1)$, $\ldots$, $(Q, *_k)$ are mutually orthogonal.

**Maximum number of orthogonal latin squares.** A transversal $(k+2)$-design of order $n$ satisfies $k + 2 \leq n + 1$, and the equality holds if and only if the design is a dual of an affine plane.

Therefore $k \leq N(n) \leq n - 1$, and $N(n) = n - 1$ if and only if there exists a projective plane of order $n$. If $n$ is a power of a prime, then $N(n) = n - 1$. It is widely believed that there are no other $n > 1$ with $N(n) = n - 1$. Lower estimates of $N(n)$ are a popular topic. For the upper estimates the following seem to be the only results available:

- $N(6) = 1$ (a classical result belonging to Euler);
- $N(10) \leq 8$ (one of the first big achievements of computer based combinatorics);
- $N(n) \leq n - 2$ if $n \equiv 1, 2 \bmod 4$ and $n$ cannot be expressed as a sum of two integer squares. (This is known as Bruck-Ryser Theorem.)

There are many constructions of two orthogonal latin squares. The construction is more difficult if $n = 4k + 2$. A pair of orthogonal latin squares exists for each $n > 2$, $n \neq 6$. Thus $N(n) \geq 2$ if $n > 2$ and $n \neq 6$.

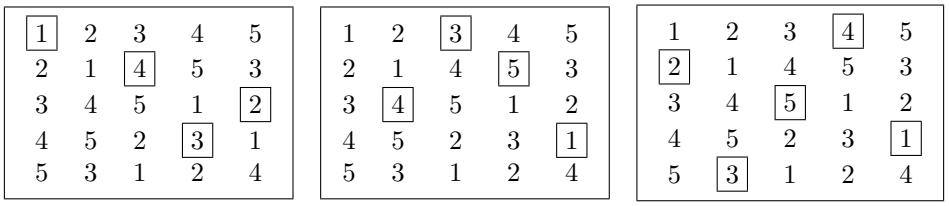
**Definition of a transversal.** Let $L$ be a latin square. A set $T$ of cells of $L$ is called a *transversal* if

(1) in each row there occurs exactly one cell of $T$;
(2) in each column there occurs exactly one cell of $T$; and
(3) every symbol occurs in exactly one cell of $T$.

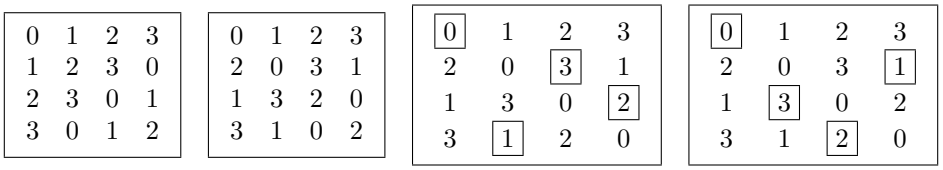
It is easy to observe that isotopic transformations map a transerval upon a transversal, and that a transformation of a latin square upon its parastrophe maps transversals upon transversals. The number of transversals hence is an invariant of the main class of a given latin square.

**Transversals in order 5.** Let $L$ be a latin square. To find a transversal one may start from a cell in the uppermost row, look for a cell in the next row which is not in a conflict with the chosen cell (i.e., contains a different symbol and is in a different row) and continue in the similar manner further on. This can lead to a stalemate—at some row there is no way how to continue. Two examples of partial transversals that cannot be completed are the two cases upon the left below. The latin square in question is a representative of the (only) isotopy class of latin squares of order 5 that are not isotopic to a latin square induced by addition modulo 5. This square possesses exactly three transversals, all of them pass through the cell

in the leftmost column that carries the symbol 2. One of them is upon the right.




**Transversals in order 4.** The latin square upon the left is given by addition modulo 4. As will proved later, this square possesses no transversal. Next to it there is an isotopic square which was obtained by switching middle two rows and columns. By flipping the intercalate in the bottom right corner there arises a latin square that yields the multiplication table of a Klein group. The indicated two transversals comprise all transversals that pass through the cell in the left top corner. This latin square possesses eight transversals.




**Transversals and complete mappings.** Let $Q$ be a quasigroup. A mapping $\varphi\colon Q \to Q$ is said to be *complete* if

- $\varphi$ is a permutation of $Q$; and
- the mapping $x \mapsto x\varphi(x)$ is also a permutation of $Q$.

If $\varphi$ is a complete mapping of $Q$, then the cells $(x, \varphi(x))$ form a transversal in the multiplication table of $Q$. On the other hand, for each transversal $T$ of the multiplication table there exists a permutation $\varphi$ such that $(x, \varphi(x))$ are the cells of $T$. This is because cells of $T$ cover all rows and all columns. The fact that each symbol occurs exactly once in a cell of $T$ means that $x \mapsto x\varphi(x)$ permutes $Q$. Transversals and complete mappings thus describe the same phenomenon.

**Transversals and orthogonal squares.** Let $(Q, \cdot)$ be a quasigroup. Let $(Q, *)$ be a quasigroup orthogonal to $(Q, \cdot)$. Choose $a \in Q$. For each $x \in Q$ there is only one solution $y$ to $x * y = a$. Denote this solution by $\varphi_a(x)$ (thus $\varphi_a(x)$ gives the result of division of $a$ by $x$ in $(Q, *)$). Since $y$ is determined uniquely, $\varphi_a$ is a permutation of $Q$. For each $b \in Q$ there exists exactly one pair $(x, y)$ such that $xy = b$ and $x * y = a$. Since $y$ is equal to $\varphi_a(x)$, by the definition of $\varphi_a$, the existence and uniqueness of $(x, y)$ may be rephrased by saying that for each $b$ there exists exactly one $x \in Q$ such that $x\varphi_a(x) = b$. In others words, $x \mapsto x\varphi_a(x)$ is a permutation of $Q$. The mapping $\varphi_a$ is complete for each $a \in Q$.

If $a \neq b$, then $\varphi_a(x) \neq \varphi_b(x)$ for each $x \in Q$. This means that the transversals $T_a = \{(x, \varphi_a(x));\, x \in Q\}$ form a decomposition of the multiplication table of $(Q, \cdot)$.

The process described above may be reversed in the sense that if $L$ is a latin square of order $n$ that is partitioned by transversals $T_1, \ldots, T_n$, then this partition yields an orthogonal latin square. To define such a square consider a bijection $\gamma$ of $\{1, \ldots, n\}$ upon the set of symbols, and put $\gamma(k)$ into cell $(i, j)$ if $(i, j)$ belongs to $T_k$.

**No transversals modulo $2^n$.** Consider the addition modulo $2^n$, $n \geq 1$. First note that if $\alpha$ permutes $\mathbb{Z}_{2^n}$, then

$$\sum_{i \in \mathbb{Z}_{2^n}} \alpha(i) \equiv \sum_{i=0}^{2^n-1} i \equiv 2^{n-1} \bmod 2^n$$

This is because $i + (2^n - i) \equiv 0 \bmod 2^n$ whenever $0 \leq i < 2^{n-1}$.

Suppose now that $\varphi$ is a complete mapping of $(\mathbb{Z}_{2^n}, +)$. Since $\varphi$ permutes $\mathbb{Z}_{2^n}$, there has to be $\sum \varphi(x) = 2^{n-1}$. Since $\psi\colon x \to x + \varphi(x)$ also permutes $\mathbb{Z}_{2^n}$, there has to be $\sum \psi(x) = 2^{n-1}$. However

$$\sum \psi(x) = \sum (x + \varphi(x)) = \sum x + \sum \varphi(x) = 2^{n-1} + 2^{n-1} = 0,$$

a contradiction. Thus **the addition table modulo $2^n$ possesses no transversal**.

**Groups of odd order.** If $G$ is a group of odd order then the main diagonal is a transversal of the multiplication table of $G$. In other words $x \mapsto x^2$ permutes $G$.

To verify this it suffices to show that $x^2 = y^2$ implies $x = y$, for any $x, y \in Q$. Choose $m = 2k + 1$ such that the orders of both $x$ and $y$ divide $m$. Thus $x^m = 1 = y^m$, and

$$x = x^{m+1} = x^{2(k+1)} = (x^2)^{k+1} = (y^2)^{k+1} = y^{m+1} = y.$$

**Complete mappings and groups.** If $\varphi$ is a complete mapping of a group $G$, then $R_a\varphi$ is also a complete mapping of $G$, for any $a \in G$. Indeed $x \mapsto x\varphi(x)$ is a permutation of $G$ if and only $x \mapsto x\varphi(x)a$ is a permutation of $G$.

Note that the latter observation may not be generalized to loops since the associativity of groups is involved. The observation has an important consequence: Each complete mapping of a group induces a set of complete mappings all of which together partition the multiplication table into transversals. A transversal of a group multiplication table thus induces a latin square that is orthogonal to the table.

**Orthomorphisms.** An *orthomorphism* of a group $G$ is a permutation $\psi$ of $G$ such that $x \mapsto x^{-1}\psi(x)$ is a permutation of $G$.

If $\psi$ is an orthomorphism, then $\varphi\colon x \mapsto x^{-1}\psi(x)$ is a complete mapping since $\psi(x) = x\varphi(x)$. If $\varphi$ is a complete mapping of $G$, then $x \mapsto x\varphi(x)$ is an orthomorphism. There is thus a 1–1 connection between orthomorphisms and complete mappings.

Note that what is here called a complete mapping or an orthomorphism, might be precised by calling it a left complete mapping or a left orthomorphism (the right complete mapping would refer to $\varphi(x)x$ and the right orthomorphism to $\varphi(x)x^{-1}$). Note also that the notion of orthomorphism may be generalized to quasigroups, by writing $x\backslash\psi(x)$ in place of $x^{-1}\psi(x)$.

**Orthomorphisms and automorphisms.** An automorphism $\alpha$ of a group $G$ is said to be *fixed point free* if $\alpha(x) = x$ implies $x = 1$, for all $x \in G$. **An automorphism of a finite group is an orthomorphism if and only if it is fixed point free.** Indeed, $x^{-1}\varphi(x) = y^{-1}\varphi(y) \Leftrightarrow yx^{-1} = \varphi(yx^{-1})$.

There are many groups which offer a plenty of fixed point free automorphisms. If $V$ is a vector space then an invertible linear mapping $\varphi \in GL(V)$ is fixed point free if and only if 1 is not its eigenvalue. If $V$ is an elementary abelian $p$ group, then $V$ may be equipped with the structure of a finite field, say $F$. In such a case the mapping $x \mapsto \lambda x$ is a fixed point free automorphism of $(F, +)$ whenever $\lambda \in F^*$, $\lambda \neq 1$. In fact, a complete set of mutually orthogonal latin squares may be constructed in this way.

**Orthomorphisms and normal subgroups.** Let $N$ be a normal subgroup of a finite group $G$, and let $\nu$ be an orthomorphism of $N$. Suppose that $G/N$ is of order $k$ and that $t_1, \ldots, t_k$ are representatives of cosets modulo $N$. Suppose also that $\tilde{\psi}$ is an orthomorphism of $G/N$. Set $\psi(nt_i) = \nu(n)t_j$ whenever $\tilde{\psi}(t_iN) = t_jN$, $n \in N$ and $1 \leq i \leq k$. The claim is that $\psi$ is an orthomorphism of $G$.

*Proof.* The fact that $\psi$ permutes $G$ follows immediately from the definition. Suppose that $x^{-1}\psi(x) = y^{-1}\psi(y)$. Assume that $x = nt_i$ and $y = mt_j$. Then $(t_iN)^{-1}\tilde{\psi}(t_iN) = (t_jN)^{-1}\tilde{\psi}(t_jN)$, which results in $t_iN = t_jN$ and $i = j$. Assume that $t_kN = \tilde{\psi}(t_iN)$, and put $t = t_i = t_j$ and $s = t_k$.

The assumption is that $(nt)^{-1} \cdot \nu(n)s = (mt)^{-1} \cdot \nu(m)s$. Cancelling $t^{-1}$ on the left and $s$ on the right yields $n^{-1}\nu(n) = m^{-1}\nu(m)$ and $n = m$. Hence $x = y$. □

**The existence of a complete mapping in a finite group.** As shown above, the existence of a complete mapping in a group may be proved via factorization. Normal subgroups of solvable groups are more easily accessible. Hence it is no wonder that they were the first for which it was proved that

> a group of even order possesses a complete mapping if and only if its Sylow 2-group is **not** cyclic.

The complete proof of this fact depends upon the Classification of Finite Simple Groups (CFSG).

**Ryser's conjecture** states that in each latin square of odd order there exists a transversal. The least order for which it is not known whether the conjecture holds is equal to eleven.

In fact, Ryser originally conjectured that the order of a latin square has the same parity as the number of transversals it possesses. This is true for even orders, as proved by Balasubramanian. On the other hand, there exist latin squares of odd order with even number of transversals.

**Filling a latin square row by row.** A *latin rectangle* is a $k \times n$ table such that each of the $k$ rows contains each of the $n$-element symbols, and no symbol appears twice in the same column. Latin squares thus are the $n \times n$ latin rectangles.

Using a result that is known as Hall's matching theorem it is not difficult to show that each latin rectangle may be completed to a latin square.

**Smetaniuk** proved that an $n \times n$ array that is filled in at most $n - 1$ cells may be completed to a latin squares if there are no two cells in the same row or column that would be filled by the same symbol.

**Exercise.** Let $G$ be a group. Describe all subsquares of the multiplication table of $G$.

**Left and right isotopes.** Let $Q$ be a loop, and let $e$ be an element of $Q$. A full name for the loop $(Q,*)$, $x*y = x/e\cdot y$, might be the *left loop principal isotope* induced by $e$. For simplicity let this be called a *left isotope*. Similarly, $x*y = x\cdot f\backslash y$ defines the *right isotope* induced by $f$.

Suppose that $x*y = x\cdot f\backslash y$. What are the left isotopes of $(Q,*)$? Denote by $/\!\!/$ the right division in $(Q,*)$. Thus $x/\!\!/y = z \Leftrightarrow x = z*y \Leftrightarrow x = z\cdot f\backslash y \Leftrightarrow z = x/(f\backslash y)$. The operation of the left isotope of $(Q,*)$ induced by $e$ thus is $x/\!\!/e*y = (x/(f\backslash e))\cdot(f\backslash y)$. If $(f,e)$ runs through $Q\times Q$, then $(f\backslash e, e)$ runs through $Q\times Q$ too. This implies:

> *(1) The set of left isotopes of right isotopes of $Q$ coincides with the set of all principal loop isotopes of $Q$, and*
> *(2) the set of right isotopes of left isotopes of $Q$ also coincides with the set of all principal loop isotopes of $Q$.*

The statement above was proved under the assumption that $Q$ is a loop. In fact it holds for every quasigroup $Q$.

**LIP loops.** A loop $Q$ is said to possess left inverses if

$$\forall x\in Q\ \exists y\in Q \text{ such that } L_y = L_x^{-1}.$$

As will be proved, if $Q$ possesses left inverses then

$$x(1/x\cdot y) = y,\ 1/x\cdot(xy) = y,\ x\backslash 1\cdot(xy) = y \text{ and } x(x\backslash 1\cdot y) = y$$

for all $x,y\in Q$. On the other hand, if any of these identities holds, then $Q$ possesses left inverses. To prove the latter is easy since $x(1/x\cdot y) = y$ means that $L_xL_{1/x} = \mathrm{id}_Q$, and the other identities may be intepreted similarly.

Let $x,y\in Q$ be such that $L_x^{-1} = L_y$. Then $y(xz) = z$ for all $z\in Q$. Setting $z = 1$ yields $yx = 1$ and $y = 1/x$. Setting $z = x\backslash 1$ yields $y = x\backslash 1$. The assumption $L_x^{-1} = L_y$ also means that $x(yz) = z$ for all $z\in Q$. Thus $xy = 1$, and $y = x\backslash 1$. Setting $z = y\backslash 1$ gives $x = y\backslash 1$. Hence $y = 1/(y\backslash 1) = 1/x$ too.

A loop that possesses left inverses thus fulfils all of the four identities. Therefore $1/x = x\backslash 1$ for each $x\in Q$. If $1/x = x\backslash 1$, then the notation $x^{-1}$ may be used.

Saying that $Q$ 'possesses left inverses' refers to the fact that the set $\{L_x;\ x\in Q\}$ is closed under the taking of an inverse permutation. A more traditional way of saying that $Q$ possesses left inverses is to say that $Q$ has the *left inverse property* (LIP). Furthermore, instead of saying that $Q$ has the left inverse property it is usual to say that $Q$ is a *LIP loop*. As explained above, if $Q$ is a LIP loop, then

$$\forall x,y\in Q\quad x\cdot x^{-1}y = x^{-1}\cdot xy = y.$$

This may be also expressed as $L_x^{-1} = L_{x^{-1}}$. RIP loops fulfil $yx\cdot x^{-1} = y = yx^{-1}\cdot x$. That means $R_x^{-1} = R_{x^{-1}}$.

**Left isotopes and LIP loops.** Let $(Q,*)$ be a left isotope of a loop $Q$, say $x*y = x/e\cdot y$. For $x\in Q$ denote by $\lambda_x$ the left translation of $(Q,*)$, and by $L_x$ the left translation of $Q$. Then $\lambda_x = L_{x/e}$. Hence

$$\{\lambda_x;\ x\in Q\} = \{L_x;\ x\in Q\}.$$

This implies that $Q$ is a LIP loop (i.e., posseses left inverses) if and only if $(Q,*)$ is a LIP loop. We have proved:

(1) A left isotope of a LIP loop is a LIP loop; and
(2) A right isotope of a RIP loop is a RIP loop.

**Left Bol loops.** Let $Q$ be a loop. The following is equivalent:

(1) The set $L_Q = \{L_x;\, x \in Q\}$ is closed under *twists* (i.e., if $\alpha, \beta \in L_Q$, then $\alpha\beta\alpha \in L_Q$);
(2) the set $L_Q = \{L_x;\, x \in Q\}$ is closed under *inverted twists* (i.e., if $\alpha, \beta \in L_Q$, then $\alpha\beta^{-1}\alpha \in L_Q$);
(3) if $x, y \in Q$, then $L_x L_y L_x = L_{x\cdot yx}$;
(4) each right isotope of $Q$ is a LIP loop;
(5) each isotope of $Q$ is a LIP loop;
(6) $Q$ satisfies the identitity $x(y \cdot xz) = (x \cdot yx)z$.

*Proof.* First note that $L_x L_y L_x = L_{x\cdot yx}$ means that $x \cdot (y \cdot xz) = (x \cdot yx)z$. Hence (3) $\Leftrightarrow$ (6). If $L_x L_y L_x = L_z$, then $z = L_z(1) = L_x L_y L_x(1) = x \cdot yx$. Hence (1) $\Leftrightarrow$ (3) $\Leftrightarrow$ (6).

If $Q$ satisfies (2) then $Q$ is a LIP loop since $L_x^{-1} = L_1 L_x^{-1} L_1 \in L_Q$. Thus $L_x = L_{x^{-1}}^{-1}$ and $L_x L_y L_x = L_x L_{y^{-1}}^{-1} L_x \in L_Q$, for any $x, y \in Q$. Hence (2) $\Rightarrow$ (1). To prove the converse by the same method it suffices to show that the identity of (6) implies the left inverse property. That follows from setting $y = 1/x$. Indeed, then $x(1/x \cdot xz) = xz$, and so $1/x \cdot xz = z$. Therefore (1) $\Rightarrow$ (2). We have shown that (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) $\Leftrightarrow$ (6).

Clearly, (5) $\Rightarrow$ (4). The converse follows from the fact that each loop isotope of $Q$ is isomorphic to a principal loop isotope, each principal loop isotope is a left isotope of a right isotope, and each left isotope of a LIP loop is a LIP loop.

To finish it thus suffices to verify (2) $\Leftrightarrow$ (4). Consider $f \in Q$ and denote by $\lambda_x$ the left translation of $(Q, *)$, $x * y = x \cdot f\backslash y$. Clearly, $\lambda_x = L_x L_f^{-1}$. What does it mean that the set $\{L_x L_f^{-1};\, x \in Q\}$ is closed under inversions? This means that for each $x \in Q$ there exists $y \in Q$ such that $L_x L_f^{-1} L_y L_f^{-1} = \mathrm{id}_Q$. Hence $L_f^{-1} L_x L_f^{-1} L_y = \mathrm{id}_Q$, $L_y^{-1} L_f L_x^{-1} L_f = \mathrm{id}_Q$ and $L_y = L_f L_x^{-1} L_f$. In other words, $(Q, *)$ is a LIP loop if and only if for each $x \in Q$ there exists $y \in Q$ such that $L_f L_x^{-1} L_f = L_y$. This is true for all $f \in Q$ if and only if the set $L_Q$ is closed under inverted twists. □

The identity $x(y \cdot xz) = (x \cdot yx)z$ is known as the *left Bol law*. Loops that fulfil this law are called *left Bol loops* or just *Bol loops*. The *right Bol* loops are those that fulfil the *right Bol law* $z(xy \cdot x) = (zx \cdot y)x$.

**Moufang loops.** A loop $Q$ is called *Moufang* if it is both the left and the right Bol loop. Moufang loops are thus those loops that satisfy both identities $x(y\cdot xz) = (x \cdot yx)z$ and $z(xy \cdot x) = (zx \cdot y)x$.

The variety of Moufang loops is much bigger than the variety of groups. Nevertheless, Moufang loops are not so far from groups as other loop varieties. This is well documented by the *Moufang's theorem*:

> Let $Q$ be a Moufang loop. If $x, y, z \in Q$ are such that $x \cdot yz = xy \cdot z$, then $\langle x, y, z\rangle$ is a group.

The theorem of Moufang may be rephrased by saying that associating elements generate an associating subloop (i.e., a group).

The proof of the theorem is relatively complicated and needs several pages.

**Operations in a LIP loop.** The left division of a LIP loop is dispensible since $x\backslash y = x^{-1}y$ for all elements $x$ and $y$ of a LIP loop $Q$. LIP loops may thus be considered as algebras in signature $(\cdot, /, {}^{-1}, 1)$ such that

$$x \cdot 1 = x = 1 \cdot x,\ (x^{-1})^{-1} = x,\ x^{-1} \cdot xy = y \text{ and } (y/x)x = y = (yx)/x.$$

**IP loops.** A loop $Q$ is said to have the *inverse property* if it is both a LIP loop and a RIP loop. Loops with inverse property are called IP loops. An IP loop may be considered as an algebra in signature $(\cdot, {}^{-1}, 1)$ such that

$$x \cdot 1 = x = 1 \cdot x,\ (x^{-1})^{-1} = x \text{ and } x^{-1} \cdot xy = y = yx \cdot x^{-1}.$$

*Lemma.* If $x, y \in Q$ and $Q$ is an IP loop, then

$$(xy)^{-1} = y^{-1}x^{-1}.$$

*Proof.* The statement may be modified to $y^{-1} = (x\backslash y)^{-1}x^{-1}$, by writing $y$ as $x\backslash y$. Now,

$$\begin{aligned} y^{-1} = (x\backslash y)^{-1}x^{-1} &\Leftrightarrow\ y^{-1}x = (x\backslash y)^{-1} \ \Leftrightarrow\ x = y(x\backslash y)^{-1} \\ &\Leftrightarrow\ x \cdot (x\backslash y) = y \ \Leftrightarrow\ y = y. \end{aligned}$$

□

**IP Bol loops are Moufang.** A left Bol loop $Q$ is a LIP loop. A right Bol loop is a RIP loop. A Moufang loop is hence an IP loop. The statement to prove is:

*Lemma.* A RIP left Bol loop is Moufang.

*Proof.* In a left Bol loop $x(y \cdot xz) = (x \cdot yx)z$. If such loop is an IP loop, then

$$(x(y \cdot xz))^{-1} = (z^{-1}x^{-1} \cdot y^{-1})x^{-1} \text{ and } ((x \cdot yx)z)^{-1} = z^{-1}(x^{-1}y^{-1} \cdot x^{-1}),$$

yielding thus the right Bol law. □

**Flexibility and the Moufang law.** The *flexible law* is the identity $x \cdot yx = xy \cdot x$. Note that a loop $Q$ is flexible if and only if $L_xR_x = R_xL_x$ for all $x \in Q$.

*Lemma.* A loop $Q$ is Moufang if and only if $Q$ is a flexible Bol loop.

*Proof.* Let $Q$ be a Moufang loop. Then $Q$ is an IP loop such that $x\cdot(y\cdot xz) = (x\cdot yx)z$ for all $x, y, z \in Q$. Setting $z = x^{-1}$ yields $xy = (x\cdot yx)x^{-1}$. Therefore $xy\cdot x = x\cdot yx$.

Let $Q$ be a left Bol loop that is flexible. It is enough to verify that $Q$ is a RIP loop. The flexibility induces the identity $x \cdot (y \cdot xz) = (xy \cdot x)z$. Setting $z = x^{-1}$ yields $xy = (xy \cdot x)x^{-1}$. □

**Two Moufang identities.** *Let $Q$ be a loop. The following is equivalent:*

(1) *$Q$ is Moufang;*
(2) *$Q$ fulfils $x(y \cdot xz) = (xy \cdot x)z$;*
(3) *$Q$ fulfils $z(x \cdot yx) = (zx \cdot y)x$;*
(4) *$(R_xL_x, L_x^{-1}, L_x) \in \mathrm{Atp}(Q)$ for all $x \in Q$; and*
(5) *$(R_x^{-1}, L_xR_x, R_x) \in \mathrm{Atp}(Q)$ for all $x \in Q$.*

*Proof.* Setting $z = 1$ yields the flexible law in both of the identities above. The flexible law changes them into a Bol identity. Flexible Bol loops are Moufang. It remains to observe that

$$\begin{aligned} x(y \cdot xz) = (xy \cdot x)z &\Leftrightarrow\ L_x(yz) = x \cdot yz = (xy \cdot x)(x\backslash z) = R_xL_x(y) \cdot L_x^{-1}(z); \\ z(x \cdot yx) = (zx \cdot y)x &\Leftrightarrow\ R_x^{-1}(z) \cdot L_xR_x(y) = (z/x)(x \cdot yx) = zy \cdot x = R_x(zy). \end{aligned}$$

□

**Autotopisms describing Bol loops.** The left Bol loop identity may be expressed as $x \cdot yz = (x \cdot yx)(x\backslash z)$. Hence

$$\begin{aligned} Q \text{ is left Bol} &\Leftrightarrow\ (L_xR_x, L_x^{-1}, L_x) \in \mathrm{Atp}(Q) \text{ for all } x \in Q; \\ Q \text{ is right Bol} &\Leftrightarrow\ (R_x^{-1}, R_xL_x, R_x) \in \mathrm{Atp}(Q) \text{ for all } x \in Q. \end{aligned}$$

**Switching translations.** Let $Q$ be an IP loop. Denote the operation of the inverse as a mapping $I$. Thus $I(x) = x^{-1}$ for each $x \in Q$. Then

$$IR_xI = L_x^{-1} \text{ and } IL_xI = R_x^{-1} \text{ for every } x \in Q.$$

*Proof.* If $x, y \in Q$, then $IR_xI(y) = I(y^{-1}x) = (y^{-1}x)^{-1} = x^{-1}y = L_x^{-1}(y)$. □

**Switching components of an isotopism.** *Suppose that $Q$ is an IP loop and that $\alpha, \beta, \gamma \in \mathrm{Sym}(Q)$. If $(\alpha, \beta, \gamma) \in \mathrm{Atp}(Q)$, then $(\gamma, I\beta I, \alpha) \in \mathrm{Atp}(Q)$.*

*Proof.* The assumption is that $\alpha(x)\beta(y) = \gamma(xy)$ for all $x, y \in Q$. This can be expressed as $\alpha(x) = \gamma(xy)(\beta(y))^{-1} = \gamma(xy) \cdot I\beta(y)$. Replacing $x$ with $xy^{-1}$ yields

$$\alpha(xI(y)) = \gamma(x) \cdot I\beta(y). \text{ Thus } \alpha(xy) = \gamma(x) \cdot I\beta I(y).$$

□

**The third Moufang identity.** *A loop $Q$ fulfils the identity*

$$xy \cdot zx = x(yz \cdot x) \;\Leftrightarrow\; (L_x, R_x, L_xR_x) \in \mathrm{Atp}(Q) \text{ for each } x \in Q.$$

*Each such loop is a flexible IP loop.*

*Proof.* To get the RIP set $z = 1/x$. Then $xy = x((y \cdot 1/x)x)$, and thus $y = (y \cdot 1/x)x$ for all $x, y \in Q$. To get flexibility set $z = 1$. The flexibility implies that the identity is equivalent to its mirror image $xy \cdot zx = (x \cdot yz)x$. That yields the LIP. □

**The equivalence of Moufang identities.** *Let $Q$ be a loop. Each of the following identities is equivalent to $Q$ being Moufang:*

$$x(y \cdot xz) = (xy \cdot x)z, \tag{lM}$$
$$(zx \cdot y)x = z(x \cdot yx), \tag{rM}$$
$$xy \cdot zx = x(yz \cdot x), \text{ and} \tag{mMl}$$
$$xy \cdot zx = (x \cdot yz)x. \tag{mMr}$$

*Proof.* We already know that (lM) ⇔ (rM). By flexibility, (mMl) ⇔ (mMr). Composing autotopism expressions of (lBol) and (rM) implies that

$$(L_xR_x, L_x^{-1}, L_x)\,(R_x^{-1}, L_xR_x, R_x) = (L_x, R_x, L_xR_x) \in \mathrm{Atp}(Q)$$

in every Moufang loop $Q$. Thus (lM) ⇒ (mM). To get the converse implication note that switching components of $(L_x, R_x, L_xR_x)$ yields $(L_xR_x, IR_xI, L_x) = (R_xL_x, L_x^{-1}, L_x)$ since loops fulfilling (mM) are flexible IP loops. □

**Description of nuclei.** Similar technique may be used to prove that in a Moufang loop $N_\lambda(Q) = N_\rho(Q) = N_\mu(Q)$. Recall that if $Q$ is a loop, then

$$N_\lambda(Q) = \{a \in Q;\ a \cdot xy = ax \cdot y \text{ for all } x, y \in Q\};$$
$$N_\mu(Q) = \{a \in Q;\ x \cdot ay = xa \cdot y \text{ for all } x, y \in Q\}; \text{ and}$$
$$N_\rho(Q) = \{a \in Q;\ x \cdot ya = xy \cdot a \text{ for all } x, y \in Q\}.$$

It is clear that

$$a \in N_\lambda(Q) \;\Leftrightarrow\; (L_a, \mathrm{id}_Q, L_a) \in \mathrm{Atp}(Q), \text{ and}$$
$$a \in N_\rho(Q) \;\Leftrightarrow\; (\mathrm{id}_Q, R_a, R_a) \in \mathrm{Atp}(Q).$$

**Middle nucleus and translations.** Let $Q$ be a loop. Then

$$a \in N_\mu(Q) \;\Leftrightarrow\; (R_a, L_a^{-1}, \mathrm{id}_Q) \in \mathrm{Atp}(Q) \;\Leftrightarrow\; (R_a^{-1}, L_a, \mathrm{id}_Q) \in \mathrm{Atp}(Q).$$

*Proof.* Indeed, $x \cdot ay = xa \cdot y$ holds for all $x, y \in Q$ if and only if $xy = xa \cdot a\backslash y$ or, alternatively, $x/a \cdot ay = xy$, for all $x, y \in Q$. □

**Nuclei in Bol loops and Moufang loops.**

(1) Let $Q$ be left Bol. Then $N_\lambda(Q) = N_\mu(Q)$.
(2) Let $Q$ be right Bol. Then $N_\rho(Q) = N_\mu(Q)$.
(3) Let $Q$ be Moufang. Then $N_\lambda(Q) = N_\mu(Q) = N_\rho(Q)$.

*Proof.* It suffices to verify the first claim. Recall that in every left Bol loop $(L_xR_x, L_x^{-1}, L_x) \in \mathrm{Atp}(Q)$, for every $x \in Q$. The equality

$$(L_a^{-1}, \mathrm{id}_Q, L_a^{-1})\,(L_aR_a, L_a^{-1}, L_a) = (R_a, L_a^{-1}, \mathrm{id}_Q)$$

thus implies that $(L_a, \mathrm{id}_Q, L_a) \in \mathrm{Atp}(Q)$ if and only if $(R_a, L_a^{-1}, \mathrm{id}_Q) \in \mathrm{Atp}(Q)$. □

**The left and right alternative laws.** These are the laws $x \cdot xz = xx \cdot z$ and $zx \cdot x = z \cdot xx$, respectively. Loops satisfying these laws are said to have the *left* or *right alternative property*. The loops themselves are then known as LAP and RAP loops.

The left Bol law $x(y \cdot xz) = (x \cdot yx)z$ yields the left alternative law by setting $y = 1$. Left Bol loops are thus LAP loops, while right Bol loops are RAP loops.

**Exercise.** A loop $Q$ is a left Bol loop if and only if each loop isotope of $Q$ fulfils the LAP. A loop $Q$ is a right Bol loop if and only if each loop isotope of $Q$ fulfils the RAP.

**Power associativity.** A loop $Q$ is said to be *left power associative* if it is LIP and fulfils

$$L_{x^i}L_{x^j}(y) = L_x^{i+j}(y) \text{ for all } x, y \in Q \text{ and all } i, j \in \mathbb{Z}.$$

The left power associativity may be paraphrased by saying that terms of the form

$$x^{\pm 1}x^{\pm 1}\cdots x^{\pm 1}y$$

are independent of bracketing.

It may be proved that left Bol loops are left power associative. The proof is not difficult.

**Diassociativity.** A loop $Q$ is said to be *diassociative* if the subloop $\langle x, y\rangle$ is associative (and thus a group) for any choice $x, y \in Q$.

Moufang loops are diassociative. This follows, e.g., from flexibility and Moufang's theorem. There exist direct proofs of diassociativity in Moufang loops. However, they are not much simpler than the proof of the Moufang's theorem.

## Extra loops

In this section it will be proved that Moufang loops with squares in the nucleus coincide with loops fulfilling the identity $xy{\cdot}xz = x(yz{\cdot}x)$. Such loops are called extra loops. The section concludes by a construction of extra loops that encompasses the loop of octonions, which is probably the most well known Moufang loop.

Other results of this section include a proof that all nuclei are associative subloops (i.e., groups).

**From autotopisms to nuclear elements.** Let $Q$ be a loop and let $\alpha, \beta, \gamma \in \mathrm{Sym}(Q)$.

(1) $(\alpha, \mathrm{id}_Q, \gamma) \in \mathrm{Atp}(Q) \Rightarrow \exists\, a \in N_\lambda(Q)$ such that $\alpha = \gamma = L_a$;
(2) $(\mathrm{id}_Q, \beta, \gamma) \in \mathrm{Atp}(Q) \Rightarrow \exists\, a \in N_\rho(Q)$ such that $\beta = \gamma = R_a$; and
(3) $(\alpha, \beta, \mathrm{id}_Q) \in \mathrm{Atp}(Q) \Rightarrow \exists\, a, b \in N_\mu(Q)$ such that $ab = 1$, $\alpha = R_a = R_b^{-1}$ and $\beta = L_a^{-1} = L_b$.

*Proof.* If $(\alpha, \mathrm{id}_Q, \gamma) \in \mathrm{Atp}(Q)$, then $\alpha(x)y = \gamma(xy)$ for all $x, y \in Q$. Setting $y = 1$ yields $\alpha = \gamma$, setting $x = 1$ provides $ay = \gamma(y)$, where $a = \alpha(1)$.

Suppose that $(\alpha, \beta, \mathrm{id}_Q) \in \mathrm{Atp}(Q)$. Then $\alpha(x)\beta(y) = xy$ for all $x, y \in Q$. Substitutions $x = 1$ and $y = 1$ give $\beta = L_a^{-1}$, where $a = \alpha(1)$, and $\alpha = R_b^{-1}$, where $b = \beta(1)$. Thus $x/b \cdot a\backslash y = xy$ for all $x, y \in Q$. Putting $x = b$ provides $L_b = L_a^{-1} = \beta$, and $y = a$ yields $R_b^{-1} = R_a = \alpha$. Therefore $L_aL_b = R_aR_b = \mathrm{id}_Q$ and thus $1 = \mathrm{id}_Q(1) = L_aL_b(1) = ab = R_aR_b(1) = ba$. □

**LIP and RIP elements.** Let $Q$ be a loop. An element $a \in Q$ is said to be a *LIP element* if there exists $b \in Q$ such that $L_a^{-1} = L_b$. Arguments used in case of LIP loops may be applied without a change to show that if $L_a^{-1} = L_b$, then $b = 1/a = a\backslash 1$. Hence $b$ may be denoted by $a^{-1}$. If $x \in Q$, then $a^{-1}(ax) = x = a(a^{-1}x)$.

*RIP elements* are defined symmetrically. An element that is both RIP and LIP is called an *IP element*.

**Nuclei and inverse properties.** If $(L_a, \mathrm{id}_Q, L_a) \in \mathrm{Atp}(Q)$, $Q$ a loop, then $(L_a^{-1}, \mathrm{id}_Q, L_a^{-1}) \in \mathrm{Atp}(Q)$. Therefore for each $a \in N_\lambda(Q)$ there exists $b \in N_\lambda(Q)$ such that $L_a^{-1} = L_b$. This shows that *elements of the left nucleus satisfy the LIP, and that $N_\lambda(Q)$ is closed under inverses.* Similarly *elements of the right nucleus satisfy the RIP, and $N_\rho(Q)$ is closed under inverses.*

If $c \in N_\mu(Q)$, then $(R_c^{-1}, L_c, \mathrm{id}_Q) \in \mathrm{Atp}(Q)$. By the statement above there exist $a, b \in N_\mu(Q)$ such that $R_c^{-1} = R_a = R_b^{-1}$ and $L_c = L_a^{-1} = L_b$. Hence $c = b$. This means that *each element of a middle nucleus is an IP element, and $N_\mu(Q)$ is closed under inverses.*

**Nuclei are groups.** *Let $Q$ be a loop. Then each of sets $N_\lambda(Q)$, $N_\mu(Q)$ and $N_\rho(Q)$ is an associative subloop of $Q$ (i.e., a group).*

*Proof.* Suppose that $a, b \in N_\lambda(Q)$. Then

$$(L_a, \mathrm{id}_Q, L_a)(L_b, \mathrm{id}_Q, L_b) = (L_aL_b, \mathrm{id}_Q, L_aL_b) \in \mathrm{Atp}(Q).$$

Therefore there exists $c \in N_\lambda(Q)$ such that $L_c = L_aL_b$. Since $c = L_c(1) = L_aL_b(1) = ab$, we have $ab \in N_\lambda(Q)$ for all $a, b \in N_\lambda(Q)$. If $a, b, c \in N_\lambda(Q)$, then $a \cdot bc = ab \cdot c$. This proves that $N_\lambda(Q)$ is a subsemigroup of $Q$ in which every element possesses an inverse. That makes $N_\lambda(Q)$ a group.

The case of $N_\rho(Q)$ can be obtained by mirroring. To prove that $N_\mu(Q)$ is a semigroup closed under inverses start from

$$(R_a^{-1}, L_a, \mathrm{id}_Q)(R_b^{-1}, L_b, \mathrm{id}_Q) = (R_{ab}^{-1}, L_{ab}, \mathrm{id}_Q), \text{ for all } a, b \in N_\mu(Q).$$

□

**The nucleus.** If $Q$ is a loop, then $N(Q) = N_\lambda(Q) \cap N_\rho(Q) \cap N_\mu(Q)$ is called the *nucleus* of $Q$. In general all three nuclei may by pairwise distinct. Since each of them is a subloop of $Q$, the nucleus always is an associative subloop of $Q$. In some cases, like in Moufang loops, all three nuclei coincide and are equal to $N(Q)$.

**Inverted Moufang indentities.** Let $Q$ be a Moufang loop. Then

$$(xy \cdot z)x^{-1} = x(y \cdot zx^{-1}) \text{ and } x^{-1}(y \cdot zx) = (x^{-1}y \cdot z)x.$$

*Proof.* This is essentially only one identity since $x = (x^{-1})^{-1}$. The identity can be also expressed as $xy{\cdot}z = x(y{\cdot}zx^{-1})x$. The right hand is equal to $xy{\cdot}(zx^{-1}{\cdot}x) = xy{\cdot}z$, by (Mm). □

The argument might be reversed. Since both

$$(xy \cdot z)(x\backslash 1) = x(y \cdot z(x\backslash 1)) \text{ and } (xy \cdot z)(1/x) = x(y \cdot z(1/x))$$

yield the IP property, as may be verified readily, each of them is an equivalent formulation of the Moufang identity.

**An identity induced by squares in nucleus.** Let $Q$ be a Moufang loop such that $x^2 \in N(Q)$ for every $x \in Q$. Then $Q$ satisfies the identity

$$(xy \cdot z)x = x(y \cdot zx). \tag{mE}$$

*Proof.* $(xy \cdot z)x = (xy \cdot z)(x^{-1} \cdot x^2) = ((xy \cdot z)x^{-1})x^2 = (x(y \cdot zx^{-1}))x^2 = x(y \cdot (zx^{-1})x^2) = x(y \cdot zx)$. □

**Equivalence of the extra identities.** The identity (mE) is equivalent to each these two identities:

$$xy \cdot xz = x(yx \cdot z) \text{ and} \tag{lE}$$

$$zx \cdot yx = (z \cdot xy)x. \tag{rE}$$

*Proof.* Let us first verify that each of the three identities yields a flexible IP loop. The flexibility may be obtained by setting $z = 1$. Further on, only (mE) and (lE) will be considered since (rE) is a mirror image of (lE).

In the case of $(xy \cdot z)x = x(y \cdot zx)$ set $z = 1/x$ to get the RIP, and $y = x\backslash 1$ to obtain the LIP. For $xy \cdot xz = x(yx \cdot z)$ set $z = x\backslash 1$ to get the RIP. To obtain the LIP consider first the equality

$$xy \cdot (x \cdot yz) = x(yx \cdot yz) = x \cdot y(xy \cdot z).$$

The RIP implies the existence of two sided inverses. Setting $z = (xy)^{-1}$ gives $xy \cdot (x \cdot y(xy)^{-1}) = xy$. Hence $x \cdot y(xy)^{-1} = 1$. Since $x^{-1}$ is the two sided inverse, $y(xy)^{-1} = x^{-1}$. Applying the RIP yields $y = x^{-1}(xy)$.

Writing $(xy \cdot z)x = x(y \cdot zx)$ as $(xy \cdot z/x)x = x \cdot yz$ shows that $Q$ satisfies (mE) if and only if

$$\forall x \in Q \ (L_x, R_x^{-1}, R_x^{-1}L_x) \in \mathrm{Atp}(Q).$$

Expressing $xy \cdot xz = x(yx \cdot z)$ as $(x(y/x) \cdot xz = x \cdot yz$ yields the formulation

$$\forall x \in Q \ (L_xR_x^{-1}, L_x, L_x) \in \mathrm{Atp}(Q).$$

Since we are dealing with IP loops, a switching of coordinates and the identity $IR_x^{-1}I = L_x$ provide

$$(L_xR_x^{-1}, L_x, L_x) \in \mathrm{Atp}(Q) \ \Leftrightarrow \ (L_x, R_x^{-1}, L_xR_x^{-1}) \in \mathrm{Atp}(Q).$$

The rest follows from the flexibility. □

**Extra loops are Moufang loops with squares in the nucleus.** Identities (mE), (rE) and (lE) are known as the *extra* identities. A loop satisfying an extra identity is said to be an *extra loop*. A loop $Q$ is extra if and only if $Q$ is a Moufang loop such that $x^2 \in N(Q)$ for each $x \in Q$.

*Proof.* As shown above, Moufang loops with nuclear squares fulfil (mE). To prove the converse consider an extra loop $Q$. Both $(L_xR_x^{-1}, L_x, L_x)$ and $(L_x, R_x^{-1}, R_x^{-1}L_x)$ are autotopisms for each $x \in Q$. Hence

$$(R_x^{-1}L_x, L_x, L_x)(L_x^{-1}, R_x, L_x^{-1}R_x) = (R_x^{-1}, L_xR_x, R_x)$$

is an autotopism of $Q$ for each $x \in Q$ too. This means that $Q$ is a Moufang loop since these autotopisms describe the identity (rM).

By the (mM) identity, $(L_x, R_x, L_xR_x) \in \mathrm{Atp}(Q)$ for every $x \in Q$. Therefore

$$(L_x, R_x, L_xR_x)(L_x^{-1}, R_x, L_x^{-1}R_x) = (\mathrm{id}_Q, R_x^2, L_xR_xL_x^{-1}R_x)$$

is an autotopism for each $x \in Q$. Hence $x^2 = R_x^2(1) \in N_\rho(Q) = N(Q)$, for each $x \in Q$. □

**The centre.** For a loop $Q$ put

$$Z(Q) = \{a \in N(Q);\ ax = xa \text{ for every } x \in Q.\}$$

This is the *centre* of $Q$. An element $a \in N(Q)$ thus belongs to the centre if and only if $L_a = R_a$.

Central elements are IP elements since $Z(Q) \subseteq N_\mu(Q)$. If $a, b \in Z(Q)$, then $L_{ab} = L_{ba} = L_bL_a = R_bR_a = R_{ab}$ and $L_{a^{-1}} = L_a^{-1} = R_a^{-1} = R_{a^{-1}}$. That makes $Z(Q)$ a subgroup of $N(Q)$.

A subloop $Z$ of $Q$ is said to be *central* if $Z \leq Z(Q)$.

Consider a central subloop $Z \leq Q$. If $x, y \in Q$ and $a, b \in Z$, then $xa = yb$ implies $y = xc = cx$, where $c = ab^{-1} = b^{-1}a$. This shows that $Q$ may be partitioned into cosets $xZ = Zx$. We have $xZ \cdot yZ = xyZ$ for all $x, y \in Q$, and this defines the structure of a factor loop $Q/Z$. (Later we shall pay attention to conditions under which a factor loop $Q/S$ may be defined if $S \leq Q$ is not necessary central.)

**Involutory Moufang loops are groups.** A loop $Q$ is said to be *involutory* if $x^2 = 1$ for all $x \in Q$. As is well known, involutory groups are commutative, and thus coincide with the class of elementary abelian 2-groups. Let us observe that the same is true for Moufang loops.

They are commutative since if $x, y \in Q$, then $xy \cdot yx = xy^2x = x^2 = 1$, and that implies $yx = (xy)^{-1} = xy$. Hence $y = x^2y = x(xy) = xyx$ for all $x, y \in Q$. They are associative since $zx \cdot y = y \cdot zx = y \cdot zx^{-1} = x(y \cdot zx^{-1})x = xy \cdot z = z \cdot xy$.

**A journey to octonions.** A 4-element vector space may be represented by a triangle. The vertices correspond to nonzero vectors. The sum of two distinct vertices is the third vertex.

An 8-element vector space may be represented by a Fano plane. The vertices correspond to nonzero vectors. The sum of two distinct vertices is the vertex that completes the line passing through the two vertices.

Suppose that $v_0$, $v_1$ and $v_2$ are pairwise distinct nonzero elements of a 8-element vector space $V$ such that $v_2 \neq v_0 + v_1$. Define a sequence of vectors $v_i$, $i \geq 0$, by setting $v_{i+3} = v_i + v_{i+1}$. Thus

$$v_3 = v_0 + v_1,\ v_4 = v_1 + v_2,\ v_5 = v_2 + v_3 = v_0 + v_1 + v_2, v_6 = v_3 + v_4 = v_0 + v_2,$$
$$v_7 = v_4 + v_5 = v_0,\ v_8 = v_5 + v_6 = v_1 \text{ and } v_9 = v_6 + v_7.$$

Hence $v_i$, $0 \le i \le 6$, are all nonzero vectors of $V$, the indices $i$ may be computed modulo 7, and $\{v_i, v_{i+1}, v_{i+3}\}$, $0 \le i \le 6$, are all lines of the Fano plane that is induced by $V$.

We have obtained a representation of Fano plane upon an oriented cycle of 7 elements. Let it be called a *circular representation of Fano plane*.

Let us get oriented. An oriented triangle may be thought of as a representation of the quaternion group $Q_8$. If the triangle is oriented as $(a_0\ a_1\ a_2)$, then there exists a unique quaternion group upon $\{a_i, -a_i;\ 0 \le i \le 2\} \cup \{-1, 1\}$ such that $a_i^2 = -1$ and $a_i a_{i+1} = a_{i-1}$, $i \in \mathbb{Z}_3$.

Suppose now that each line of a Fano plane obtains one of two possible orientations. This yields seven oriented 3-cycles each of which is further on interpreted as a quaternion group. Elements $-1$ and 1 are considered to be common for all of the seven quaternion groups. Denote by $U$ their union. Any two elements $x, y \in U$ occur in one of these groups, and so their product is well defined. This makes $U$ a loop, and this loop is diassociative. The set $Z = \{-1, 1\}$ is a central subgroup, and $U/Z \cong (V, +)$.

The question is whether there exists an orientation that makes $U$ a Moufang loop (and thus also an extra loop). In fact, there exist several such orientations. However, loops produced by these orientations are mutually isomorphic.

The orientation that is standardly used to produce a Moufang loop is based upon the circular representation of Fano plane. This results in setting $U = \{e_i, -e_i;\ 0 \le i \le 6\} \cup \{-1, 1\}$ where $-1$ is a central element equal to each $e_i^2$, and $e_i e_{i+1} = e_{i+3}$, $0 \le i \le 6$. This loop is known as the loop of *octonions*. More precisely $U$ is the loop of octonion units, similarly as $\{\pm 1, \pm \mathrm{i}, \pm \mathrm{j}, \pm \mathrm{k}\}$ is the group of quaternion units. (Quaternions $\mathbb{H}$ are a division ring upon $\mathbb{R}^4$ and octonions $\mathbb{O}$ are an algebra upon $\mathbb{R}^8$.)

In fact $U$ is up to isomorphism the only Moufang loop $Q$ of order 16 for which there exists a central subloop $Z = \{1, z\}$ such that $x^2 = z$ for each $x \in Q \setminus Z$.

We shall now show that if such a loop $Q$ exists, then it has to be isomorphic to $U$. However, the very existence of $Q$ will be verified later.

*Proof.* First note that there exists an 8-element vector space $V$ such that $(V, +) \cong Q/Z$. This is because $Q/Z$ is an involuntory Moufang loop. If $x, y \in Q \setminus Z$ and $y \notin \{x, xz\}$, then $\langle x, y\rangle/Z$ is isomorphic to Klein group, and $\langle x, y\rangle$ is a group isomorphic to the group of quaternions $Q_8$. This follows from the diassociativity of $Q$ (a direct proof is also possible). Hence $xy = yxz$ and $xyx = y$.

Denote the nonzero vectors of $V$ by $v_i$, $0 \le i \le 6$, so that each $\{v_i, v_{i+1}, v_{i+3}\}$ is a line of the corresponding Fano plane. For $i \in \{0, 1, 2\}$ choose any $e_i$ such that $e_i Z = v_i$. Set $e_3 = e_0 e_1$, $e_4 = e_1 e_2$, $e_5 = e_2 e_3$ and $e_6 = e_3 e_4$. Then $e_i Z = v_i$ for every $i \in \{0, \dots, 6\}$. The choice and definitions of $e_i$ establish an orientation $(v_i, v_{i+1}, v_{i+3})$ of a line for $i \in \{0, 1, 2, 3\}$. It remains to observe that the Moufang law forces out this orientation for the remaining values of $i$ as well. Now, $e_4 e_5 = e_1 e_2 \cdot e_2 e_3 = e_2 e_1 z \cdot z e_3 e_2 = e_2 e_1 \cdot e_3 e_2 = e_2 \cdot e_1 e_3 \cdot e_2 = e_2 e_0 e_2 = e_0$. Similarly, $e_5 e_6 = e_2 e_3 \cdot e_3 e_4 = e_3 \cdot e_2 e_4 \cdot e_3 = e_3 e_1 e_3 = e_1$. Finally, $e_6 e_0 = e_3 e_4 \cdot e_0 = (e_0 e_1 \cdot e_4) e_0 = z(e_1 e_0 \cdot e_4) e_0 = z(e_1 \cdot e_0 e_4 e_0) = z e_1 e_4 = e_4 e_1 = e_2$. □

**A construction using quadratic forms.** Let $V$ be a vector space over a field $F$. A mapping $g\colon V \to F$ is said to be a *quadratic form* if $h\colon (x, y) \mapsto g(x + y) - g(x) - g(y)$ is a bilinear form $V \times V \to F$ and $g(\lambda x) = \lambda^2 g(x)$ for all $x \in V$ and $\lambda \in F$. If $\mathrm{char}(F) = 2$, then the bilinear form is alternating (which means that $h(x, x) = 0$ for every $x \in V$).

Recall that if $h\colon V \times V \to F$ is alternating and bilinear, then $h(x, y) = -h(y, x)$, for all $x, y \in F$ (no assumption on $\mathrm{char}(F)$ is being made here). Recall also that

a multilinear mapping $f\colon V^n \to F$ is said to be *alternating* if $f(x_1, \ldots, x_n) = 0$ whenever $x_i = x_j$, where $1 \le i < j \le n$. If $\sigma \in S_n$ and $f$ is alternating, then $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = (-1)^{\mathrm{sgn}(\sigma)} f(x_1, \ldots, x_n)$. Alternating multilinear mappings in characteristic two thus are symmetric.

**Theorem.** *Let $V$ be a vector space over a field $F$,* $\mathrm{char}(F) = 2$*, and let $q\colon V \times V \to F$ be such that for each $v \in V$ the mapping $x \mapsto q(x, v)$ is a quadratic form, while the mapping $x \mapsto q(v, x)$ is a linear form. Put $Q = V \times F$ and define a binary operation upon $Q$ by*

$$(u, a)(v, b) = (u + v, q(u, v) + a + b)$$

*and assume that $q(u + v, u) = q(u, u) + q(v, u)$ for all $u, v \in V$. Then $(Q, \cdot)$ is a Moufang loop. Furthermore, the mapping $A\colon V \times V \times V \to F$ defined by $A(u, v, w) = q(u + v, w) + q(u, w) + q(v, w)$ is an alternating trilinear mapping, and a triple of elements $((u, a), (v, b), (w, c)) \in Q^3$ is associative if and only if $A(u, v, w) = 0$.*

*Proof.* The multilinearity of $A$ follows directly from the assumptions on $q$. Clearly, $A(u, v, w) = A(v, u, w)$ and $A(u, u, v) = 0$, for any $u, v, w \in V$. To verify that $A$ is an alternating trilinear form it thus remains to show that $A(u, v, u) = 0$. This follows from $q(u+v, u) + q(u, u) + q(v, u) = q(u, u) + q(v, u) + q(u, u) + q(v, u) = 0$.

The neutral element is $(0, 0)$ since $q(u, 0) = q(0, u)$ for all $u \in V$. The operation $\cdot$ thus yields a loop. Each element $(0, a)$ is central and $(u, a) = (u, 0)(0, a)$. A triple $((u, a), (v, b), (w, c))$ is thus associative if and only if the triple $((u, 0), (v, 0), (w, 0))$ is associative. Now, $((u, 0) \cdot (v + w, q(v, w)) = (u + v + w, q(u, v + w) + q(v, w))$ is equal to $(u + v, q(u, v)) \cdot (w, 0) = (u + v + w, q(u + v, w) + q(u, v))$ if and only if $A(u, v, w) = q(u, w) + q(v, w) + q(u + v, w)$ is equal to 0 since $q(u, v + w) = q(u, v) + q(u, w)$.

To verify that $(Q, \cdot)$ is a Moufang loop it suffices to show that

$$(u, 0)(v, 0) \cdot (w, 0)(u, 0) = (u, 0)((v, 0)(w, 0) \cdot (u, 0)).$$

Note that $(v, 0)(w, 0) \cdot (u, 0) = (v+w, q(v, w))(u, 0) = (v+w+u, q(v+w, u)+q(v, w))$. The left hand side of the Moufang identity is

$$(u + v, q(u, v)) \cdot (w + u, q(w, u)) = (v + w, q(u, v) + q(w, u) + q(u + v, w + u)),$$

while the right hand side is equal to

$$(u, 0) \cdot (u+v+w, q(v+w, u)+q(v, w)) = (v+w, q(u, u+v+w)+q(v+w, u)+q(v, w)).$$

The question thus is whether

$$q(u, v) + q(u + v, u) + q(w, u) + q(u + v, w) = q(u, v) + q(u, u) + q(v, u) + q(w, u) + q(u + v, w)$$

is equal to

$$q(u, v) + q(u, u) + q(u, w) + q(v + w, u) + q(v, w).$$

That really holds since $q(v, u) + q(w, u) + q(v + w, u) = A(v, w, u)$ is equal to $A(u, v, w) = q(u + v, w) + q(u, w) + q(v, w)$. □

**Parameters for quadratic forms.** Let $F$ be a field of characteristic 2, let $V$ be a vector space over $F$, and let $b_1, \ldots, b_n$ be a basis of $V$. A quadratic form $g\colon V \to F$ is fully determined by values of $g$ at $b_i$ and $b_i + b_j$, $1 \le i < j \le n$. This fact follows from the formula

$$g\left(\sum \lambda_i b_i\right) = \sum_i \lambda_i^2 g(b_i) + \sum_{i<j} \lambda_i \lambda_j (g(b_i) + g(b_j) + g(b_i + b_j))$$

that may be easily proved. Whenever $g(b_i)$, $g(b_j)$ and $g(b_i + b_j)$ are given, then the formula defines a quadratic form.

Suppose now that $n = 3$ and set

$$q\left(\sum \lambda_i b_i, \sum \nu_i b_i\right) = \lambda_1^2(\nu_1+\nu_2+\nu_3) + \lambda_2^2(\nu_2+\nu_3) + \lambda_3^2\nu_3 + \lambda_1\lambda_2\nu_3 + \lambda_1\lambda_3\nu_2 + \lambda_2\lambda_3\nu_1.$$

Fixing any value of the second coordinate thus yields a quadratic form, while fixing any value for the first coordinate provides a linear form. Set $A(u,v,w) = q(u,w) + q(v,w) + q(u+v,w)$. This is a trilinear form. Suppose that $u = \sum \lambda_i b_i$, $v = \sum \rho_i b_i$ and $w = \sum \nu_i b_i$. Since $\lambda_i^2 + \rho_i^2 = (\lambda+\rho_i)^2$ the first part of the formula defining $q$ contributes nothing to $A(u,v,w)$. Let now $\{i,j,k\} = \{1,2,3\}$. Then $\lambda_i\lambda_j\nu_k + \rho_i\rho_j\nu_k + (\lambda_i+\rho_i)(\lambda_j+\rho_j)\nu_k = \lambda_i\rho_j\nu_k + \lambda_j\rho_i\nu_k$. Since $A(u,v,w)$ is obtained by summing over all $i,j,k$, there has to be $A(u,v,w) = \det(u,v,w)$ (i.e., a determinant of the matrix in which the columns are formed by coefficients of $u$, $v$ and $w$, respectively). Thus $A(u,v,u) = 0$, and that shows that $q$ as defined can be used to build a Moufang loop on $V \times F$. The operation of the loop is $(u,a)(v,b) = (u+v, q(u,v)+a+b)$.

Use now the same formula for $F = \{0,1\}$. To see that the construction yields a Moufang loop in which $(u,a)(u,a) = (0,1)$ whenever $u \neq 0$ we have to show that if at least one of $\lambda_i \in F$ is nonzero and $u = \lambda_1 b_1 + \lambda_2 b_2 + \lambda_3 b_3$, then $q(u,u) = 1$.

It is easy to verify that

$$q(u,u) = \lambda_1\lambda_2\lambda_3 + \lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_1\lambda_3 + \lambda_1 + \lambda_2 + \lambda_3.$$

This yields 1 if $\lambda_1 = \lambda_2 = \lambda_3 = 1$. If $\lambda_3 = 0$, then the formula to consider is $\lambda_1\lambda_2 + \lambda_1 + \lambda_2$. That is equal to 0 if and only if $\lambda_1 = \lambda_2 = 0$. We can thus conclude by stating:

**The loop of octonion units.** There exists a Moufang loop $Q$ upon elements $\pm 1, \pm e_0, \ldots, \pm e_6$ such that $(-1)(\pm e_i) = \mp e_i$, $e_i^2 = -1$, $-1$ is a central element, $e_i e_j = -e_j e_i$ if $0 \leq i \leq 6$, and

$$e_i e_{i+1} = e_{i+3},\ e_i e_{i+2} = e_{i-1},\ e_i e_{i+3} = -e_{i+1}$$

for each $i \in \{0,\ldots,6\}$, with the indices computed modulo 7.

Let $V$ be a vector space over $F$ with nonzero vectors $v_0, \ldots, v_6$ such that $v_i + v_{i+1} = v_{i+3}$ for each $i \in \{0,\ldots,6\}$. Denote by $\pi$ the mapping $\pm e_i \mapsto v_i$, $\pm 1 \mapsto 0$. Then $\pi$ is a homomorphism $(Q,\cdot) \to (V,+)$. A triple $(x,y,z) \in Q^3$ is associative if and only if $\det(\pi(x),\pi(y),\pi(z)) = 0$ since the trilinear mapping $A$ coincides with the determinant. The associativity is thus equivalent to linear dependence.

**Preliminaries involving permutation groups.** Let $G$ be a permutation group upon a set $\Omega$. Fix an element $\omega \in \Omega$. The set of all $g \in G$ that fixes $\omega$ is said to be the *stabilizer* of $G$ at $\omega$. It is a subgroup and is denoted by $G_\omega$.

**Lemma 1.** *Suppose that $g \in G$ and $\alpha = g(\omega)$. Then $G_\alpha = gG_\omega g^{-1}$. If $G$ is transitive, then $G_\omega \cap Z(G) = 1$.*

*Proof.* Let $h$ be an element of $G$. Then $h \in G_\alpha \Leftrightarrow h(\alpha) = \alpha \Leftrightarrow hg(\omega) = g(\omega) \Leftrightarrow g^{-1}hg(\omega) = \omega \Leftrightarrow g^{-1}hg \in G_\omega \Leftrightarrow h \in gG_\omega g^{-1}$. Suppose that $G$ is transitive and that $h \in Z(G)$ fixes $\omega$. Since $G$ is transitive, for each $\alpha \in \Omega$ there exists $g \in G$ such that $g(\omega) = \alpha$. Since $h \in G_\omega$, $ghg^{-1} \in G_\alpha$. Therefore $h = ghg^{-1} \in G_\alpha$. Hence $h(\alpha) = \alpha$ for each $\alpha \in \Omega$. Thus $h = \mathrm{id}_\Omega$. □

Recall that if $S$ is a subset of a group $G$, then $N_G(S) = \{g \in G;\, gSg^{-1} = S\}$ is called the *normalizer* of $S$, and $C_G(S) = \{g \in G;\, gs = sg \text{ for all } s \in S\}$ the *centralizer* of $S$. Both $N_G(S)$ and $C_G(S)$ are subgroups of $G$. To prove that $H \leq G$ is a subgroup of $N_G(S)$ it suffices to verify that $hSh^{-1} \subseteq S$ for every $h \in H$. Indeed, $h^{-1}S(h^{-1})^{-1} \subseteq S$ is the same as $S \subseteq hSh^{-1}$. Similarly for centralizers.

**Lemma 2.** *Let $g$ be an element of $G$. Then $G_{g(\omega)} = G_\omega$ if and only if $g \in N_G(G_\omega)$.*

*Proof.* By Lemma 1, $G_{g(\omega)} = G_\omega$ if and only if $gG_\omega g^{-1} = G_\omega$, which is the same as $g \in N_G(G_\omega)$. □

**Lemma 3.** *Let $h$ and $g$ be elements of $G$. Then $hG_\omega = gG_\omega$ if and only if $g(\omega) = h(\omega)$, while $G_\omega h = G_\omega g$ if and only if $g^{-1}(\omega) = h^{-1}(\omega)$.*

*Proof.* Since $(G_\omega h)^{-1} = h^{-1}G_\omega$, only the first equality needs to be verified. Now, $hG_\omega = gG_\omega \Leftrightarrow h^{-1}g \in G_\omega \Leftrightarrow h^{-1}g(\omega) = \omega \Leftrightarrow g(\omega) = h(\omega)$. □

A set $\Gamma \subseteq \Omega$ is said to be a *block* (of $G$) if it is nonempty and satisfies the implication

$$g(\gamma) \in \Gamma \Rightarrow g(\Gamma) \subseteq \Gamma$$

for all $g \in G$ and $\gamma \in \Gamma$.

**Lemma 4.** *Let $\Gamma$ be a block. If $g \in G$, then either $g(\Gamma) = \Gamma$ or $g(\Gamma) \cap \Gamma = \emptyset$. In any case, $g(\Gamma)$ is a block of $G$ as well.*

*Proof.* Suppose first that there exist $\beta, \gamma \in \Gamma$ such that $g(\gamma) = \beta$. Then $g(\Gamma) \subseteq \Gamma$ by the definition of a block. Since $g^{-1}(\beta) = \gamma$, $g^{-1}(\Gamma) \subseteq \Gamma$ too. Hence $g(\Gamma) = \Gamma$. We have proved that this is true whenever $\gamma(\Gamma) \cap \Gamma \neq \emptyset$.

To prove that $g(\Gamma)$ is always a block, consider $\alpha \in g(\Gamma)$ and $h \in G$ such that $h(\alpha) = \beta \in g(\Gamma)$. Then $hg(g^{-1}(\alpha)) = g(g^{-1}(\beta))$, and thus $g^{-1}hg(g^{-1}(\alpha)) = g^{-1}(\beta)$. Both $g^{-1}(\alpha)$ and $g^{-1}(\beta)$ belong to $\Gamma$. Therefore $g^{-1}hg(\Gamma) = \Gamma$, which means $h(g(\Gamma)) = g(\Gamma)$. We have shown that $g(\Gamma)$ is a block. □

Blocks $\Gamma_1$ and $\Gamma_2$ are said to be *conjugate* if there exists $g \in G$ such that $g(\Gamma_1) = \Gamma_2$. The relation 'to be conjugate' clearly is an equivalence upon the set of all blocks of $G$.

**Corollary 5.** *Suppose that $G$ is transitive. If $\Gamma$ is a block of $G$, then the set of all $g(\Gamma)$, $g \in G$, partitions the set $\Omega$. Furthermore, two blocks are conjugate if and only if they induce the same partition of $\Omega$.*

*Proof.* Indeed, the transitivity ensures that the sets $g(\Gamma)$ are blocks that cover all of $\Omega$. Moreover, any two such blocks are conjugate. The rest follows from Lemma 4 in an immediate fashion. □

An equivalence $\sim$ of $\Omega$ is said to be *stable under* $G$ if

$$\alpha \sim \beta \;\Leftrightarrow\; g(\alpha) \sim g(\beta) \text{ for each } \alpha, \beta \in \Omega \text{ and } g \in G.$$

In fact it is enough to prove that the implication

$$\alpha \sim \beta \;\Rightarrow\; g(\alpha) \sim g(\beta) \text{ for each } \alpha, \beta \in \Omega \text{ and } g \in G.$$

is satisfied, since then $g(\alpha) \sim g(\beta)$ implies $\alpha = g^{-1}g(\alpha) \sim g^{-1}g(\beta) = \beta$.

**Lemma 6.** *Let $\sim$ be a stable equivalence. If $\alpha \in \Omega$ and $g \in G$, then $[\alpha]_\sim$ and $[g(\alpha)]_\sim$ are conjugate blocks. If $G$ is transitive, then the blocks of $\sim$ form a partition of $\Omega$ by conjugate blocks. On the other hand, every such partition induces a stable equivalence.*

*Proof.* By the definition of stable equivalence, $g([\alpha]_\sim) = [g(\alpha)]_\sim$, for every $\alpha \in \Omega$ and each $g \in G$. If $\Gamma = [\omega]_\sim$ and $g(\omega) \in \Gamma$, then $g(\Gamma) = \Gamma$. Hence each block of $\sim$ is a block of $G$. The rest follows from Corollary 5. □

**Lemma 7.** *For $\alpha, \beta \in \Omega$ set $\alpha \sim \beta \Leftrightarrow G_\alpha = G_\beta$. The equivalence $\sim$ is stable under $G$. Furthermore, suppose that $G$ is transitive, that $\omega \in \Omega$ and that $\Gamma = \{\alpha \in \Omega;\ G_\omega \subseteq G_\alpha\}$. If $\Gamma$ is a block of $G$, then $\Gamma = [\omega]_\sim$.*

*Proof.* If $G_\alpha = G_\beta$ and $g \in G$, then $G_{g(\alpha)} = G_{g(\beta)}$, by Lemma 1. Suppose now that $G$ is transitive and that $\omega$ and $\Gamma$ are as in the statement. Suppose that $\alpha \in \Gamma$ and let $g \in G$ be such that $g(\omega) = \alpha$. Then $G_\omega \subseteq gG_\omega g^{-1} = G_\alpha$, by Lemma 1 and the definition of $\Gamma$. Since $g(\Gamma) = \Gamma$ there is also $g^{-1}(\omega) \in \Gamma$, and so $G_\omega \subseteq g^{-1}G_\omega g$. Therefore $G_\omega = gG_\omega g^{-1} = G_\alpha$. □

The following characterization of blocks is nearly self-evident. Note that it differs from the definition of a block by considering the defining property just for one element, i.e. the element $\omega$.

**Lemma 8.** *Suppose that $\Gamma$ is a subset of the orbit $G(\omega)$ that contains $\omega$. The following is equivalent:*

(1) *$\Gamma$ is a block;*
(2) *the ensuing implication holds for all $g \in G$:*

$$g(\omega) \in \Gamma \;\Rightarrow\; g(\Gamma) \subseteq \Gamma \text{ and } g^{-1}(\omega) \in \Gamma;$$

(3) *the ensuing implication holds for all $g \in G$:*

$$g(\omega) \in \Gamma \;\Rightarrow\; g(\Gamma) = \Gamma.$$

*Proof.* Points (2) and (3) are equivalent since if (2) holds, then $g^{-1}(\omega) \in \Gamma$ implies $g^{-1}(\Gamma) \subseteq \Gamma$. If $\Gamma$ is a block, then (3) holds, by Lemma 4. For the converse assume that $g(\gamma) \in \Gamma$ for some $\gamma \in \Gamma$ and $g \in G$. Since $\Gamma \subseteq G(\omega)$, there exists $h \in G$ such that $h(\omega) = \gamma$. This gives $h(\Gamma) = \Gamma$, $gh(\omega) \in \Gamma$ and $gh(\Gamma) = \Gamma$. Hence $g(\Gamma) = \Gamma$. □

**Lemma 9.** *Let $H \leq G$ be such that $G_\omega \leq H$. Then $\Gamma = H(\omega)$ (the orbit of $\omega$ under the action of $H$) is a block of $G$, and $H = \{g \in G;\ g(\omega) \in \Gamma\}$.*

*Proof.* Let $g \in G$ be such that $g(\omega) \in H(\omega)$. Then $g(\omega) = h(\omega)$ for some $h \in H$. Therefore $h^{-1}g \in G_\omega \leq H$, and thus $g \in H$. Hence $g(H(\omega)) = (gH)(\omega) = H(\omega)$. That makes $H(\omega)$ a block. If $g(\omega) \in \Gamma$, $g \in G$, then there exists $h \in H$ such that $g(\omega) = h(\omega)$. Hence $h^{-1}g \in G_\omega \leq H$, and so $g = h(h^{-1}g) \in H$. □

**Lemma 10.** *Let $\Gamma \subseteq G(\omega)$ be a block of $G$ such that $\omega \in \Gamma$. Put $H = \{h \in G;\ h(\omega) \in \Gamma\}$. Then $H$ is a subgroup of $G$ that contains $G_\omega$, and $\Gamma = H(\omega)$.*

*Proof.* Since $\Gamma$ is a block within the orbit of $\omega$, there has to be $H = \{h \in G;\ h(\Gamma) = \Gamma\}$, by Lemma 8. This implies that $H$ is a subgroup of $G$ and that $\Gamma = H(\omega)$. □

Note that $\{\omega\}$ is always a block of $G$ and that the orbit $G(\omega)$ is also a block.

Lemmas 9 and 10 establish a 1-to-1 correspondence between blocks $\Gamma \subseteq G(\omega)$ that include $\omega$, and subgroups of $G$ that contain $G_\omega$. The correspondence respects inclusions. Hence it yields an isomorphism between the lattice of blocks that are subsets of $G(\omega)$ and contain $\omega$, and the interval $[G_\omega, G]$ in the lattice of all subgroups of $G$. If $G(\omega) \neq \{\omega\}$, then $G_\omega \neq G$. In such a case the interval $[G_\omega, G]$ contains only two elements (two subgroups) if and only if there exists no block that is a proper subset of $G(\omega)$ and contains at least two elements.

The permutation group $G$ is said to be *primitive* if it is nontrivial and the only blocks of $G$ are $\Omega$ and $\{\alpha\}$, $\alpha \in \Omega$. Since $G(\omega)$ is a block, a primitive group has to be transitive. In view of the correspondence described above, the following claim may be stated without a proof.

**Lemma 11.** *A nontrivial transitive permutation group $G$ is primitive if and only if $G_\omega$ is a maximal subgroup of $G$.*

**Lemma 12.** *If $H \trianglelefteq G$ and $\Gamma$ is an orbit of $H$, then $\Gamma$ is a block.*

*Proof.* Suppose that $\omega \in \Gamma$ and put $K = HG_\omega$. This is a subgroup of $G$, since $H \trianglelefteq G$. If $k \in K$, then there exists $h \in H$ such that $k(\omega) = h(\omega)$. Thus $\Gamma = K(\omega)$. The statement follows from Lemma 9. □

**Lemma 13.** *Let $\sim$ be the equivalence upon $\Omega$ given by $G_\alpha = G_\beta$. Assume that $G$ is transitive and put $\Gamma = [\omega]_\sim$. Then $\Gamma$ is a block of $G$, and $\{g \in G;\ g(\omega) \in \Gamma\} = N_G(G_\omega)$.*

*Proof.* The set $\Gamma$ is a block by Lemmas 7 and 6. By Lemma 2, $\Gamma = N_G(G_\omega)(\omega)$. The rest follows from Lemma 9 since $N_G(G_\omega)$ contains $G_\omega$. □

Suppose that $U \leq V$ are groups and that $S \subseteq V$. Call $S$ a *left transversal* to $U$ in $V$ if $SU = V$, $1 \in S$, and $s_1U = s_2U \Rightarrow s_1 = s_2$, whenever $s_1, s_2 \in S$. The *right transversal* is defined in a mirror way. A set that is both left and right transversal is known as a *two-sided tranversal*, or just a *transversal*. The notion of transversal is sometimes defined without stipulating that the transversal contains the unit element 1.

The *core* of $U$ in $V$ is the greatest normal subgroup $N \trianglelefteq V$ that is contained in $U$. Note that $N = \bigcap_{g \in V} gUg^{-1}$.

**Lemma 14.** *Let $S$ be a subset of $G$ that contains $\mathrm{id}_G$. $S$ is the left transversal to $G_\omega$ in $G$ if and only if for each $\alpha \in G(\omega)$ there exists exactly one $s \in S$ such that $s(\omega) = \alpha$. Similarly, the set $S$ is the right transversal to $G_\omega$ in $G$ if and only if for each $\alpha \in G(\omega)$ there exists exactly one $s \in S$ such that $s(\alpha) = \omega$.*

*Proof.* This follows from the description of cosets of $G_\omega$, as given in Lemma 3. □

**Lemma 15.** *If $G$ is transitive, then the core of $G_\omega$ is trivial.*

*Proof.* By Lemma 1, the core of $G_\omega$ is equal to the intersection of all $G_\alpha$, $\alpha \in \Omega$. Of course, the only permutation that fixes each $\alpha \in \Omega$ is the identity. □

**Proposition 16.** *Suppose that $T$ is a left transversal to $G_\omega$ in $G$, and that $X \subseteq G$ generates $G$. For each $\alpha \in G(\omega)$ denote by $t_\alpha$ that element of $T$ which sends $\omega$ upon $\alpha$. Then*

$$G_\omega = \langle t_{x(\alpha)}^{-1} x t_\alpha;\ \alpha \in G(\omega) \text{ and } x \in X \rangle.$$

*Proof.* For $S \subseteq G$ set $S^{\pm 1} = \{s, s^{-1};\ s \in S\}$. Each element of $G$ may be thus expressed as $x_n \cdots x_1$, where $x_i \in X^{\pm 1}$, $1 \leq i \leq n$. Denote by $Y$ the set of all

elements $t^{-1}_{x(\alpha)} x t_\alpha$, $\alpha \in G(\omega)$ and $x \in X$. If $\beta = x(\alpha)$, then the inverse of such an element is equal to $t^{-1}_{x^{-1}(\beta)} x^{-1} t_\beta$. Hence

$$Y^{\pm 1} = \{t^{-1}_{x(\alpha)} x t_\alpha;\ \alpha \in G(\omega) \text{ and } x \in X^{\pm 1}\}.$$

Note that $Y^{\pm 1} \subseteq G_\omega$ and that $t_\omega = \mathrm{id}_\Omega$.

Suppose now that $g = x_n \cdots x_1 \in G_\omega$, where $x_1, \ldots, x_n \in X^{\pm 1}$. Put $\alpha_i = x_i \cdots x_1(\omega)$, $0 \leq i < n$, and insert $t_{\alpha_i} t^{-1}_{\alpha_i} = t_{\alpha_i} t^{-1}_{x_i(\alpha_{i-1})}$ in between $x_{i+1}$ and $x_i$, $1 \leq i < n$. That makes

$$g = t_\omega g t_\omega = t^{-1}_\omega x_n \cdots x_1 t_\omega = \left(t^{-1}_{x_n(\alpha_{n-1})} x_n t_{\alpha_{n-1}}\right) \cdots \left(t^{-1}_{x_1(\alpha_0)} x_1 t_{\alpha_0}\right)$$

an element of $\langle Y \rangle$. □

**Quasigroup congruences.** Let $Q$ be a quasigroup. Set

$$\begin{aligned} \mathrm{LMlt}(Q) &= \langle L_x;\ x \in Q \rangle, \\ \mathrm{RMlt}(Q) &= \langle R_x;\ x \in Q \rangle \text{ and} \\ \mathrm{Mlt}(Q) &= \langle L_x, R_x;\ x \in Q \rangle. \end{aligned}$$

Call these groups the *left multiplication group*, the *right multiplication group* and the *multiplication group* of $Q$, respectively.

**Proposition 17.** *Let $Q$ be a quasigroup. An equivalence $\sim$ on $Q$ is a congruence if and only if for all $x, y, z \in Q$*

$$x \sim y \ \Rightarrow\ xz \sim yz,\ zx \sim zy,\ x/z \sim y/z \text{ and } z\backslash x = z\backslash y.$$

*Proof.* If $*$ is a binary operation on $Q$, then $\sim$ is compatible with $*$ if and only if $x \sim y \Rightarrow x * z \sim y * z$ and $z * x \sim z * y$ holds for all $x, y, z \in Q$. To see that this is true consider $a, b, c, d \in Q$ such that $a \sim b$ and $c \sim d$. If the implication holds for all $x, y, z \in Q$, then $a * c \sim b * c \sim b * d$.

Due to this fact the proof may be restricted to verifying implications $x \sim y \Rightarrow z/x \sim z/y$ and $x \sim y \Rightarrow x\backslash z \sim y\backslash z$. It is enough to prove the latter implication because of mirror symmetry. Before doing so let us observe that all implications assumed may be considered as equivalences. E.g., we have $x \sim y \Leftrightarrow xz \sim yz$. To prove the converse direction suppose that $xz \sim yz$. By the assumptions of the statement $(xz)/z \sim (yz)/z$. However $(xz)/z = x$ and $(yz)/z = y$. Similarly in the other cases.

Thus $x\backslash z \sim y\backslash z \Leftrightarrow z \sim x(y\backslash z) \Leftrightarrow z/(y\backslash z) \sim (x(y\backslash z))/(y\backslash z)$. Now, $z/(y\backslash z) = y$ and $x(y\backslash z))/(y\backslash z) = x$. □

**Theorem 18.** *Let $Q$ be a quasigroup and let $\sim$ be an equivalence upon $Q$. The equivalence $\sim$ is a congruence of $Q$ if and only if it is stable under* $\mathrm{Mlt}(Q)$.

*Proof.* The equivalence $\sim$ is stable under $\mathrm{Mlt}(Q)$ if $x \sim y$ implies $g(x) \sim g(y)$ for each $x, y \in Q$ and $g \in G$. For the implication to hold it suffices if it holds for generators of $\mathrm{Mlt}(Q)$ and the inverses of these generators. That follows from Proposition 17 since $R_z(x) = xz$, $L_z(x) = zx$, $R_z^{-1}(x) = x/z$ and $L_z^{-1}(x) = z\backslash x$. □

**Corollary 19.** *Let $S$ be a nonempty subset of a quasigroup $Q$. The set $S$ is a block of a congruence if and only if it is a block of* $\mathrm{Mlt}(Q)$. *Each such block determines exactly one congruence of $Q$.*

*Proof.* Indeed, blocks of a stable equivalence are blocks of the permutation group, and each block of a transitive group fully determines a stable equivalence. □

**Corollary 20.** *Let $Q$ be a quasigroup, $|Q| > 1$. The quasigroup is simple if and only if* $\mathrm{Mlt}(Q)$ *is a primitive permutation group.*

*Proof.* Recall that a transitive group is said to be primitive if it possesses no non-trivial block (i.e., a block that differs from the underlying set and contains more than than one element.) □

**Inner mapping group.** Let $Q$ be a loop. The stabilizer $(\mathrm{Mlt}\, Q)_1$ is known as the *inner mapping group*. It is denoted by $\mathrm{Inn}(Q)$. Thus $\varphi \in \mathrm{Inn}(Q)$ if and only if $\varphi(1) = 1$ and $\varphi \in \mathrm{Mlt}(Q)$.

**Theorem 21.** *Let $Q$ be a loop. Then* $\mathrm{Inn}(Q) = \langle L_{xy}^{-1} L_x L_y, R_{yx}^{-1} R_x R_y, R_x^{-1} L_x; x, y \in Q \rangle$.

*Proof.* Use Proposition 16 with $G = \mathrm{Mlt}(Q)$, $X = \{L_y, R_y;\ y \in Q\}$ and $T = \{L_y;\ y \in Q\}$. Note that $T$ is indeed a (left) transversal to $\mathrm{Inn}(Q)$ since $L_y(1) = y$ for every $y \in Q$, and $L_1 = \mathrm{id}_Q$.

By Proposition 16 the set of all $L_{xy}^{-1} L_x L_y$ and $L_{yx}^{-1} R_x L_y$ generate $\mathrm{Inn}(Q)$. Obviously, $R_x^{-1} L_x \in \mathrm{Inn}(Q)$. The rest follows from $L_y = R_y(R_y^{-1} L_y)$ and $L_{yx}^{-1} = (R_{yx}^{-1} L_{yx})^{-1} R_{yx}^{-1}$. □

Mappings $L_{xy}^{-1} L_x L_y$, $R_{yx}^{-1} R_x R_y$, $R_x^{-1} L_x$ are known as the *standard generators* of $\mathrm{Inn}(Q)$. There are many other mappings that belong to $\mathrm{Inn}(Q)$. For example $[L_x, R_y] = L_x^{-1} R_y^{-1} L_x R_y \in \mathrm{Inn}(Q)$ for all $x, y \in Q$.

**Normal subloops.** Let $\sim$ be a congruence of a loop $Q$. If $x \sim 1$ and $y \sim 1$, then $xy \sim 1$, $x/y \sim 1$ and $x\backslash y \sim 1$ since $1 = 1 \cdot 1 = 1/1 = 1\backslash 1$. The set $[1]_\sim$ is thus a subloop of $Q$.

A subloop of a loop $Q$ is called *normal* if it is a block of a congruence. By Corollary 19 the normal subloop determines exactly one congruence of $Q$. Denote the congruence by $\sim$. Blocks of $\sim$ are the blocks of $\mathrm{Mlt}(Q)$ conjugate to $N = [1]_\sim$. Hence they are equal to $L_x(N) = xN = Nx = R_x(N)$. A block $xN = Nx$ is called a *coset* of $N$. The fact that $N$ is a normal subloop of $Q$ is denoted, like in groups, by $N \trianglelefteq Q$.

**Theorem 22.** *Let $Q$ be a loop and let $N$ be a subloop of $Q$. The following is equivalent:*

(i) *$N$ is normal;*
(ii) *$\varphi(N) \subseteq N$ for each $\varphi \in \mathrm{Inn}(Q)$;*
(iii) *$\varphi(N) = N$ for each $\varphi \in \mathrm{Inn}(Q)$;*
(iv) *$xN = Nx$, $x(yN) = (xy)N$ and $(Ny)x = N(yx)$ for all $x, y \in Q$.*

*Proof.* If $N$ is a block of a congruence $\sim$, $x \in N$ and $\varphi \in \mathrm{Inn}(Q)$, then $1 = \varphi(1) \sim \varphi(x)$. Hence (i) $\Rightarrow$ (ii). If (ii) holds and $\varphi \in \mathrm{Inn}(Q)$, then both $\varphi(N) \subseteq N$ and $\varphi^{-1}(N) \subseteq N$ are true. Thus $\varphi(N) = N$, and (ii) $\Rightarrow$ (iii). The condition (iv) can be also expressed as $L_{xy}^{-1} L_x L_y(N) = N$, $R_{yx}^{-1} R_x R_y(N) = N$ and $R_x^{-1} L_x(N) = N$. In view of Theorem 21 this means that (iii) $\Leftrightarrow$ (iv).

It remains to prove (iii) $\Rightarrow$ (i). Each element of $\mathrm{Mlt}(Q)$ may be written as $L_x\varphi$, where $\varphi \in \mathrm{Inn}(Q)$ and $x \in Q$. (This is because the set of all left translations forms a transversal to $\mathrm{Inn}(Q)$.) If $x \in N$, then $L_x\varphi(N) = xN = N$. If $x \notin N$, then $L_x\varphi(N) = xN$ and $xN \cap N = \emptyset$. This means that $N$ is a block of $\mathrm{Mlt}(Q)$. □

**Centres.** Recall that the *centre* of a loop $Q$ is defined as the set of all $z \in Q$ such that $z \in N(Q) = N_\lambda(Q) \cap N_\mu(Q) \cap N_\rho(Q)$ and that $zx = xz$ for all $x \in Q$.

The following facts are direct enough to be stated without a proof.

**Lemma 23.** *Let $a$ be an element of a loop $Q$. Then*

(1) *$a \in N_\lambda \Leftrightarrow R_{yx}^{-1} R_x R_y(a) = a$ for all $x, y \in Q$;*
(2) *$a \in N_\mu \Leftrightarrow [L_x, R_y](a) = a$ for all $x, y \in Q$; and*

(3) $a \in N_\rho \Leftrightarrow L_{xy}^{-1} L_x L_y(a) = a$ *for all* $x, y \in Q$;

**Theorem 24.** *Let $Q$ be a loop. Then $Z(Q)$ is a normal subloop of $Q$. An element $z \in Q$ belongs to $Z(Q)$ if and only if $\varphi(z) = z$ for all $\varphi \in \mathrm{Inn}(Q)$. Furthermore, $Z(\mathrm{Mlt}(Q)) = \{L_z;\ z \in Z(Q)\} = \{R_z;\ z \in Z(Q)\}$ and $N_{\mathrm{Mlt}(Q)}(\mathrm{Inn}(Q)) = \mathrm{Inn}(Q)Z(\mathrm{Mlt}(Q))$.*

*Proof.* If $a \in Z(Q)$, then $a$ is fixed by every standard generator of $\mathrm{Inn}(Q)$, by Lemma 23 and Theorem 21. Thus each $\varphi \in \mathrm{Inn}(Q)$ fixes every $a \in Z(Q)$. For the converse direction use Lemma 23 and observe again that $T_x(a) = a \Leftrightarrow ax = xa$.

Since $N(Q)$ is a subloop of $Q$, the product $ab$ belongs to $N(Q)$ for all $a, b \in Z(Q)$. Therefore $L_{ab} = L_a L_b = R_a R_b = R_{ba} = R_{ab}$. Also, $L_{a^{-1}} = L_a^{-1} = R_a^{-1} = R_{a^{-1}}$. Hence $Z(Q)$ is a subloop of $Q$. Since $\mathrm{Inn}(Q)$ fixes each element of $a \in Z(Q)$ it has to be a normal subloop, by Theorem 22. That makes $Z(Q)$ a block of $\mathrm{Mlt}(Q)$. Elements $z \in Z(Q)$ have been characterized as those elements of $Q$ that are fixed by each $\varphi \in \mathrm{Inn}(Q)$. In other words $z \in Z(Q) \Leftrightarrow \mathrm{Inn}(Q) \subseteq (\mathrm{Mlt}(Q))_z$. By Lemma 7, $z \in Z(Q) \Leftrightarrow \mathrm{Inn}(Q) = (\mathrm{Mlt}(Q))_z$.

If $z \in Z(Q)$, then $L_z = R_z$ and both $L_z R_x = R_x L_z$ and $R_z L_x = L_x R_z$ are clearly true for each $x \in Q$. Hence $L_z \in Z(\mathrm{Mlt}(Q))$. If $\psi \in Z(\mathrm{Mlt}(Q))$ and $\varphi \in \mathrm{Inn}(Q)$, then $\varphi(\psi(1)) = \psi(\varphi(1)) = \psi(1)$. Hence $\psi(1) = z \in Z(Q)$, and $L_z^{-1}\psi \in \mathrm{Inn}(Q)$. No nontrivial element of $\mathrm{Inn}(Q)$ may be central, say by Lemma 1. This verifies the description of $Z(\mathrm{Mlt}(Q))$ and shows that $\mathrm{Inn}(Q)Z(\mathrm{Mlt}(Q)) = \{\psi \in \mathrm{Mlt}(Q);\ \psi(1) \in Z(Q)\}$. The latter group is also equal to $N_{\mathrm{Mlt}(Q)}(\mathrm{Inn}(Q))$, by Lemma 13. □

**Nilpotency.** Let $\mathcal{S}$ be a set of subsets of a set $X$. Suppose that $X \in \mathcal{S}$ and that $\mathcal{S}$ contains the least element, say $I$. Thus $I \subseteq X$ for each $X \in \mathcal{S}$. In the application below $X = Q$, $Q$ a loop, and $I$ is the trivial subloop, i.e. $I = \{1\}$.

Suppose that upon $\mathcal{S}$ there are defined two transformations, say $\alpha$ and $\beta$. Let both of them *respect inclusions*, i.e., if $S_1, S_1 \in \mathcal{S}$ and $S_1 \subseteq S_2$, then $\alpha(S_1) \subseteq \alpha(S_2)$ and $\beta(S_1) \subseteq \beta(S_2)$. Futhermore, let both of them be *monotonous*, with $\alpha(S) \supseteq S$ and $\beta(S) \subseteq S$, for every $S \in \mathcal{S}$.

Finally, let $\alpha$ and $\beta$ be interconnected by

$$\beta\alpha(S) \subseteq S \ \text{ and } \ \alpha\beta(S) \supseteq S, \ \text{ for every } S \in \mathcal{S}.$$

In such a situation it is possible to build *lower series* $X \supseteq \beta(X) \supseteq \beta^2(X) \supseteq \ldots$, and *upper series* $I \subseteq \alpha(I) \subseteq \alpha^2(I) \subseteq \ldots$. It is well known that the lower series ends at $I$ if and only if the upper series ends at $X$, and that, if the latter is true, then both series are of equal length. If the length is $n+1$, then $n$ is the *nilpotency class* of $\mathcal{S}$ (with respect to $\alpha$ and $\beta$) and $\mathcal{S}$ is said to be *nilpotent*. Of course, if $\mathcal{S}$ is deterministically derived from an object $\mathcal{O}$, then the notions of nilpotency and nilpotency class are related to that object.

The objects in question now are loops, and the systems of subsets are the normal subloops of a loop $Q$. If $N \trianglelefteq Q$, then there obviously exists a unique $M \trianglelefteq Q$ such that $N \leq M$ and $M/N = Z(Q/N)$. This is the operator $\alpha$. The normal subloops $\alpha^i(1)$, $i \geq 0$, are the *iterated centers* $Z_i(Q)$, with $Z_1(Q) = Z(Q)$ and $Z_{i+1}(Q)/Z_i(Q) = Z(Q/Z_i(Q))$.

The inclusion $M = \alpha(N) \supseteq N$ follows from the fact that $N/N$ is the trivial subgroup of $Q/N$. Hence $N/N \leq Z(Q/N)$. Suppose now that $N_1 \leq N_2$ are normal subloops of $Q$. Denote by $\pi$ the homomorphism $Q/N_1 \to Q/N_2$, $xN_1 \mapsto xN_2$. If $M \trianglelefteq Q$ is such that $N_1 \leq M$ and $M/N_1 \leq Z(Q/N_1)$, then $\pi(M/N_1) \leq Z(Q/N_2)$. Express $\pi(M/N_1)$ as $L/N_2$. Then $M \leq L$. Setting $M = \alpha(N_1)$ yields $\alpha(N_1) \leq \alpha(N_2)$.

Let us now show that for each $N \trianglelefteq Q$ there exists the least normal subloop $M \trianglelefteq Q$ such that $M \leq N$ and $N/M \leq Z(Q/M)$. The operator $\beta$ is defined so that $\beta(N) = M$.

To verify the existence of $M$ first note that $\mathrm{Mlt}(Q/N)$ coincides with the action of $\mathrm{Mlt}(Q)$ upon the cosets modulo $N$. Indeed, cosets are conjugate blocks, and hence $\mathrm{Mlt}(Q)$ acts upon them. Now, $L_x$ sends $yN$ upon $x(yN) = (xy)N = L_{xN}(yN)$. The action of $L_x$ coincides with $L_{xN}$, and this is similarly true for every $R_x$. The coincidence is transferred to the multiplication groups since these groups are generated by the left and the right translations.

The fact that $aN$ belongs to $Z(Q/N)$ thus means that each standard generator of $\mathrm{Inn}(Q)$ maps $aN$ upon $aN$, by Theorem 24. If $M_i$, $i \in I$, are all $M_i \trianglelefteq Q$ such that $M_i \leq N$ and $N/M_i \leq Z(Q/M_i)$, then $M = \bigcap M_i$ is a normal subloop of $Q$. Each standard generator of $\mathrm{Inn}(Q)$ maps $aM_i$, $a \in N$, to $aM_i$, for every $i \in I$. Hence it maps $aM = a(\bigcap M_i) = \bigcap(aM_i)$ upon $aM$, which implies $N/M \leq Z(Q/M)$.

The obvious inclusion $N/N \leq Z(Q/N)$ implies $\beta(N) \leq N$. Consider now normal subloops $N_1$ and $N_2$ such that $N_1 \leq N_2$. Let $M \trianglelefteq Q$ be such that $N_2/M \leq Z(Q/M)$. Consider $a \in N_1$ and $\varphi \in \mathrm{Inn}(Q)$. Then $\varphi(aM) = aM$ since $a \in N_2$ and $N_2/M \leq Z(Q/M)$. Furthermore, $aN_1 = N_1$ and $\varphi(N_1) = N_1$, because $N_1 \trianglelefteq Q$. Hence $\varphi(a(M \cap N_1)) = a(M \cap N_1)$. Therefore $a(M \cap N_1) \in Z(Q/(N_1 \cap M))$, and thus $N_1/(M \cap N_1) \leq Z(Q/(M \cap N_1))$. Setting $M = \beta(N_2)$ implies that $\beta(N_1) \leq \beta(N_2) \cap N_1 \leq \beta(N_2)$.

It remains to verify that $\beta\alpha(N) \leq N$ and $\alpha\beta(N) \geq N$, for every $N \trianglelefteq Q$. If $M = \alpha(N)$, then $M/N = Z(Q/N)$. Hence $N \geq K$, where $K = \beta(M)$ is the least normal subloop such that $K \leq M$ and $M/K \leq Z(Q/K)$. Therefore $\beta\alpha(N) \leq N$. To see $\alpha\beta(N) \geq N$, just note that $N/\beta(N) \leq Z(Q/\beta(N))$.

This is why the first steps in the theory of nilpotent loops resemble those in the theory of nilpotent groups. A loop $Q$ is thus *nilpotent of class* $k$ if and only if $Z_k(Q) = Q$ and $k \geq 0$ is the least possible. Furthermore, each loop of nilpotency class 2 may be, up to isomorphism, expressed by an operation upon $G \times Z$, where both $(G, +)$ and $(Z, +)$ are abelian groups, and

$$(a, u) \cdot (b, v) = (a + b, u + v + \vartheta(a, b)) \text{ for all } u, v \in Z \text{ and } a, b \in G,$$

where $\vartheta\colon G \times G \to Z$ fulfils $\vartheta(0, a) = \vartheta(a, 0) = 0$, for all $a \in G$.

To see this consider a loop of nilpotency class two, and set $Z = Z(Q)$. From each coset modulo $Z$ choose exactly one element. The chosen elements form a set, say $G$, and this set may be endowned with the structure of the factorloop $Q/Z$. The factorloop is an abelian group. The operation of $G$ will thus be written additively. If $g_i \in G$ and $z_i \in Z$, $i \in \{1, 2\}$, then there exists $g_3 \in G$ and $z_3 \in Z$ such that $g_1 g_2 = g_3 z_3$. Note, that $(g_1 z_1)(g_2 z_2) = g_3(z_3 z_1 z_2)$ and that $g_3 = g_1 + g_2$. Denote $z_3$ by $\vartheta(g_1, g_2)$. This yields $g_1 z_1 \cdot g_2 z_2 = (g_1 + g_2)(\vartheta(g_1, g_2) z_1 z_2)$. Writing elements of $Z$ additively thus shows that $Q$ is isomorphic to a loop with operation

$$(g_1, z_1) \cdot (g_2, z_2) = (g_1 + g_2, \vartheta(g_1, g_2) + z_1 + z_2).$$

To get $(0, 0)$ as the neutral element of this loop it suffices to assume that the neutral element of $Q$ is the element that is chosen from $Z$ (which is also a coset). Such a choice also stipulates that $\vartheta(g, 0) = 0 = \vartheta(0, g)$ for all $g \in G$.

The definition of nilpotency by means of the operators $\alpha$ and $\beta$ allows to introduce further concepts for which the term nilpotency may be used. These concepts are not discussed here. The nilpotency defined above is sometimes called *central nilpotency* in order to distinguish it from those other concepts.

**Left and right nuclei.** Let $Q$ be a loop. By Lemma 23, $N_\lambda(Q)$ are the points fixed by $(\mathrm{RMlt}(Q))_1$, and $N_\rho(Q)$ are the points fixed by $(\mathrm{LMlt}(Q))_1$. A similar characterization in terms of the multiplication groups is as follows:

**Proposition 25.** *Let $Q$ be a loop. Then*

(1) $\{L_a;\, a \in N_\lambda(Q)\} = C_{\mathrm{Mlt}(Q)}(\mathrm{RMlt}(Q)) = C_{\mathrm{Sym}(Q)}(\mathrm{RMlt}(Q))$, *and*

(2) $\{R_a;\, a \in N_\rho(Q)\} = C_{\mathrm{Mlt}(Q)}(\mathrm{LMlt}(Q)) = C_{\mathrm{Sym}(Q)}(\mathrm{LMlt}(Q))$.

*Proof.* If $a \in N_\lambda(Q)$ and $x, y \in Q$, then $L_a R_x(y) = a \cdot yx = ay \cdot x = R_x L_a(y)$. Hence $[L_a, R_x] = \mathrm{id}_Q$ if and only if $a \in N_\lambda(Q)$. If $\varphi \in (\mathrm{Sym}(Q))_1$ and $[L_a\varphi, R_x] = \mathrm{id}_Q$ for each $x \in Q$, then $a\varphi(yx) = a\varphi(y) \cdot x$ for all $x, y \in Q$. Setting $y = 1$ yields $L_a = L_a\varphi$. Thus $\varphi = \mathrm{id}_Q$. □

**Proposition 26.** *Let $Q$ be a loop. If $\mathrm{RMlt}(Q) \trianglelefteq \mathrm{Mlt}(Q)$, then $N_\lambda(Q) \trianglelefteq Q$. If $\mathrm{LMlt}(Q) \trianglelefteq \mathrm{Mlt}(Q)$, then $N_\rho(Q) \trianglelefteq Q$.*

*Proof.* If $\mathrm{RMlt}(Q) \trianglelefteq \mathrm{Mlt}(Q)$, then the centralizer of $\mathrm{RMlt}(Q)$ is also a normal subgroup of $\mathrm{Mlt}(Q)$. In such a case $N_\lambda(Q)$ is an orbit of a normal subgroup of $\mathrm{Mlt}(Q)$. The rest follows from Lemma 12 and Corollary 19. □

**Proposition 27.** *If $Q$ is a left Bol loop, then $\mathrm{RMlt}(Q) \trianglelefteq \mathrm{Mlt}(Q)$ and $N_\lambda(Q) \trianglelefteq Q$. If $Q$ is a right Bol loop, then $\mathrm{LMlt}(Q) \trianglelefteq \mathrm{Mlt}(Q)$ and $N_\rho(Q) \trianglelefteq Q$. If $Q$ is a Moufang loop, then $N(Q) \trianglelefteq Q$ and both $\mathrm{LMlt}(Q)$ and $\mathrm{RMlt}(Q)$ are normal subgroups of $\mathrm{Mlt}(Q)$.*

*Proof.* By Proposition 26 it suffices to show that $\mathrm{RMlt}(Q) \trianglelefteq \mathrm{Mlt}(Q)$ if $Q$ is left Bol, that is if $x(y \cdot xz) = (x \cdot yx)z$ for all $x, y, z \in Q$. The latter identity can be written as $L_x R_{xz} = R_z L_x R_x$. This means $L_x^{-1} R_z L_x = R_{xz} R_x^{-1}$. Nothing more is needed since $Q$ is a LIP loop and $\mathrm{RMlt}(Q)$ is generated by the right translations $R_x$, $x \in Q$. □

**Transversals.** Let $H \leq G$ be groups. A pair $(A, B)$ of subsets of $G$ is said to form *$H$-connected* transversals if $A$ is a left transversal to $H$ in $G$, $B$ is a right transversal to $H$ in $G$, and $[a, b] \in H$ for all $(a, b) \in A \times B$.

**Lemma 28.** *Let $Q$ be a loop. Put $G = \mathrm{Mlt}(Q)$ and $H = \mathrm{Inn}(Q)$. Furthermore, set $A = \{L_x;\, x \in Q\}$ and $B = \{R_x;\, x \in Q\}$. Then $(A, B)$ forms $H$-connected transversals, $\langle A, B\rangle = G$, and the core of $H$ in $G$ is trivial.*

*Proof.* As follows from Lemma 14 both $A$ and $B$ are both-sided transversals of $H$ to $G$. The core of $H$ in $G$ is trivial by Lemma 15. Finally, $L_x R_y(1) = R_y L_x(1) = xy$ for all $x, y \in Q$. □

There seems to be nothing remarkable in Lemma 28. The point is that the statement may be reversed. The proof is not long, but will not be included. We have:

**Theorem 29.** *Let $G$ and $H$ be groups, and $A$ and $B$ subsets of $G$ such that $H \leq G$, $(A, B)$ forms $H$-connected transversals, $\langle A, B\rangle = G$, and the core of $H$ in $G$ is trivial. Then there exists a loop $Q$ such that $G = \mathrm{Mlt}(Q)$, $H = \mathrm{Inn}(Q)$, $A = \{L_x;\, x \in Q\}$ and $B = \{R_x;\, x \in Q\}$.*

## Pseudoautomorphisms and constructions of Moufang loops

Let $Q$ be a loop, $c \in Q$ and $g$ a permutation of $Q$. Call $g$ a *left pseudoautomorphism* with *companion* $c$ if

$$cg(x) \cdot g(y) = c \cdot g(xy) \quad \text{for all} \quad x, y \in Q.$$

A *right pseudoautomorphism* $f$ with companion $d$ fulfils $f(x) \cdot f(y)d = f(xy)d$. It may happen that a permutation, say $h$, is both a left and right pseudoautomorphism (in fact this is always the case when $Q$ is Moufang). Then $h$ is called a *pseudoautomorphism*. If $h$ is a pseudoautomorphism, then it may be necessary to distinguish between a *left* companion (corresponding to $c$) and a *right* companion (corresponding to $d$). Note that a left pseudoautomorphism may have more than one companion, and that this is true for right pseudoautomorphisms as well.

Denote by $\mathrm{LPs}(Q)$ the set of all $(c, f)$ such that $f$ is a left pseudoautomorphism with companion $c$, and by $\mathrm{RPs}(Q)$ the set of all $(g, d)$ such that $g$ is a right pseudoautomorphism with companion $d$.

Both $\mathrm{LPs}(Q)$ and $\mathrm{RPs}(Q)$ may be regarded as groups. To understand this let us first observe that

$$\begin{aligned}(c, g) \in \mathrm{LPs}(Q) &\;\Leftrightarrow\; (L_c g, g, L_c g) \in \mathrm{Atp}(Q); \text{ and}\\ (f, d) \in \mathrm{RPs}(Q) &\;\Leftrightarrow\; (f, R_d f, R_d f) \in \mathrm{Atp}(Q).\end{aligned}$$

The key connection between autotopisms and pseudoautomorphisms follows from a simple observation:

$$(c, g) \in \mathrm{LPs}(Q) \;\Rightarrow\; g(1) = 1 \text{ and } (f, d) \in \mathrm{RPs}(Q) \;\Rightarrow\; f(1) = 1.$$

This is obvious since $cg(x) \cdot g(1) = cg(x)$ for all $x \in Q$. The point is that an autotopism $(\alpha, \beta, \gamma)$ with $\alpha(1) = 1$ or $\beta(1) = 1$ yields a pseudoautomorphism. We shall prove:

$$\begin{aligned}&(\alpha, \beta, \gamma) \in \mathrm{Atp}(Q) \text{ and } \beta(1) = 1 \;\Rightarrow\; (\alpha(1), \beta) \in \mathrm{LPs}(Q) \text{ and } \alpha = \gamma = L_{\alpha(1)}\beta;\\ &(\alpha, \beta, \gamma) \in \mathrm{Atp}(Q) \text{ and } \alpha(1) = 1 \;\Rightarrow\; (\alpha, \beta(1)) \in \mathrm{RPs}(Q) \text{ and } \beta = \gamma = R_{\beta(1)}\alpha.\end{aligned}$$

*Proof.* Assume $\beta(1) = 1$. Setting $y = 1$ in $\alpha(x)\beta(y) = \gamma(xy)$ yields $\alpha = \gamma$. Setting $x = 1$ gives $L_{\alpha(1)}\beta = \alpha$. □

This makes $\mathrm{LPs}(Q)$ a group with unit $(1, \mathrm{id}_Q)$ and operations

$$(c, f)(d, g) = (cf(d), fg) \text{ and } (c, f)^{-1} = (f^{-1}(c\backslash 1), f^{-1}).$$

To see why the operations are defined as stated, observe that

$$\begin{aligned}(L_c f, f, L_c f)(L_d g, g, L_d g) &= (L_c f L_d g, fg, L_c f L_d g),\\ (L_c f, f, L_c f)^{-1} &= (f^{-1}L_c^{-1}, f^{-1}, f^{-1}L_c^{-1}),\end{aligned}$$

$L_c f L_d g(1) = cf(d)$ and $f^{-1}L_c^{-1}(1) = f^{-1}(c\backslash 1)$. Similarly, $\mathrm{RPs}(Q)$ is a group with operations

$$(f, c)(g, d) = (fg, f(d)c) \text{ and } (f, c)^{-1} = (f^{-1}, f^{-1}(1/c)).$$

The group $\mathrm{LPs}(Q)$ is thus isomorphic to the subgroup of $\mathrm{Atp}(Q)$ formed by all $(\alpha, \beta, \gamma) \in \mathrm{Atp}(Q)$ such that $\beta(1) = 1$. The isomorphism sends $(\alpha, \beta, \gamma)$ upon $(\alpha(1), \beta)$.

The following observation is obvious but important:

$$(c, \mathrm{id}_Q) \in \mathrm{LPs}(Q) \Leftrightarrow c \in N_\lambda(Q) \text{ and } (\mathrm{id}_Q, d) \in \mathrm{RPs}(Q) \Leftrightarrow d \in N_\rho(Q).$$

**Pseudoautomorphisms with two companions.** *Let $Q$ be a loop. Suppose that $c, d \in Q$ and that $f$ permutes $Q$.*

(1) *Assume $(c, f) \in \mathrm{LPs}(Q)$. Then $f^{-1}(c\backslash 1) = 1/f^{-1}(c)$, and $(d, f) \in \mathrm{LPs}(Q) \Leftrightarrow c/d \in N_\lambda(Q)$.*
(2) Assume $(f, c) \in \mathrm{RPs}(Q)$. *Then $f^{-1}(1/c) = f^{-1}(c)\backslash 1$ and $(f, d) \in \mathrm{RPs}(Q) \Leftrightarrow d\backslash c \in N_\rho(Q)$.*

*Proof.* Suppose that $(c, f) \in \mathrm{LPs}(Q)$. Then $f(y) = cf(f^{-1}(c\backslash 1)) \cdot f(y)$ is equal to $cf(f^{-1}(c\backslash 1) \cdot y)$ for every $y \in Q$. Setting $y = f^{-1}(c)$ and cancelling $c$ yields $1 = f(f^{-1}(c\backslash 1) \cdot f^{-1}(c))$. Thus $1 = f^{-1}(c\backslash 1) \cdot f^{-1}(c)$ and $f^{-1}(c\backslash 1) = 1/f^{-1}(c)$.

Suppose now that $(d, f)$ also belongs to $\mathrm{LPs}(Q)$. Then $(c, f) \cdot (f^{-1}(d\backslash 1), f^{-1}) = (c(d\backslash 1), \mathrm{id}_Q) \in \mathrm{LPs}(Q)$ as well. Hence $n = c(d\backslash 1) \in N_\lambda(Q)$. Recall that $n$ is an LIP element. Therefore $d(d\backslash 1) = 1 = n^{-1}(c(d\backslash 1)) = (n^{-1}c)(d\backslash 1)$, implying $n^{-1}c = d$, $c = nd$ and $n = c/d$.

If $n = c/d \in N_\lambda(Q)$, then $n^{-1}c = d$ and $(L_n^{-1}L_c f, f, L_n^{-1}L_c f) \in \mathrm{Atp}(Q)$. This yields $(d, f) \in \mathrm{LPs}(Q)$ since $L_n^{-1}L_c f(1) = n^{-1}c = d$. □

**When a pseudoautomorphism is an automorphism.** *If $(c, f) \in \mathrm{LPs}(Q)$, then $f \in \mathrm{Aut}(Q)$ if and only if $c \in N_\lambda(Q)$. If $(f, c) \in \mathrm{RPs}(Q)$, then $f \in \mathrm{Aut}(Q)$ if and only if $c \in N_\rho(Q)$.*

*Proof.* Note that $f \in \mathrm{Aut}(Q) \Leftrightarrow (1, f) \in \mathrm{LPs}(Q) \Leftrightarrow (f, 1) \in \mathrm{RPs}(Q)$. □

**Companions and the inverse property.** *Let $Q$ be an IP loop. Then $(c, f) \in \mathrm{LPs}(Q)$ if and only if $(f, c^{-1}) \in \mathrm{RPs}(Q)$. If $(c, f) \in \mathrm{LPs}(Q)$, then $f(x^{-1}) = (f(x))^{-1}$, for every $x \in Q$.*

*Proof.* Suppose that $(c, f) \in \mathrm{LPs}(Q)$. Setting $y = x^{-1}$ in $cf(xy) = cf(x) \cdot f(y)$ gives $c = cf(x) \cdot f(x^{-1})$. Since $Q$ is an IP loop, $c = cf(x) \cdot (f(x))^{-1}$. Hence $(f(x))^{-1} = f(x^{-1})$ for every $x \in Q$. Inverting $cf(x^{-1}y^{-1}) = cf(x^{-1}) \cdot f(y^{-1})$ therefore yields $f(y) \cdot f(x)c^{-1} = f(yx)c^{-1}$. □

**Commutators and associators.** Let $Q$ be a loop. If $x, y \in Q$, then $[x, y] = (yx)^{-1}(xy)$ is called the *commutator* of $x$ and $y$. If $Q$ is diassociative, then the commutator may be bracketed in any way that respects the order of variables. To get a direct proof of this fact for Moufang loops note that $(x^{-1}y^{-1})(xy) = x^{-1}(y^{-1} \cdot xy)$ since $x((x^{-1}y^{-1}) \cdot xy) = (x(x^{-1}y^{-1})x)y = y^{-1}x \cdot y$ and $y^{-1} \cdot xy = y^{-1}x \cdot y$ as $y^{-1}(xy)y^{-1} = y^{-1}x$. The remaining equalities may be obtained by mirroring.

If $x, y, z \in Q$, then $[x, y, z] = (x \cdot yz)\backslash(xy \cdot z)$ is called the *associator* of $x$, $y$ and $z$.

**Standard generators in a Moufang loop.** *Suppose that $x$ and $y$ are elements of a Moufang loop $Q$. Then* $\mathrm{RPs}(Q)$ *contains*

$$(R_x^{-1}L_x, x^3),\ (L_{xy}^{-1}L_xL_y, [y^{-1}, x^{-1}]),\ (R_{yx}^{-1}R_xR_y, [x, y]) \text{ and } ([L_x, R_y], [y, x^{-1}]).$$

*Furthermore, $L_{xy}^{-1}L_xL_y = [R_x^{-1}, L_y]$ and $R_{yx}^{-1}R_xR_y = [L_x^{-1}, R_y]$.*

*Proof.* Since $(R_z^{-1}, L_zR_z, R_z)$ and $(L_z, R_z, L_zR_z)$ are autotopisms for each $z \in Q$, there are also autotopisms

$$(R_x^{-1}L_x, L_xR_x^2, R_xL_xR_x) \text{ and } (L_{xy}^{-1}L_xL_y, R_{xy}^{-1}R_xR_y, M_{xy}^{-1}M_xM_y),$$

where $M_z = L_zR_z$. Now, $L_xR_x^2(1) = x^3$ and $R_{xy}^{-1}R_xR_y(1) = (yx)(y^{-1}x^{-1}) = [y^{-1}, x^{-1}]$. Hence both $(R_x^{-1}L_x, x^3)$ and $(L_{xy}^{-1}L_xL_y, [y^{-1}, x^{-1}])$ belong to $\mathrm{RPs}(Q)$.

Further autotopisms are

$$(L_{yx}^{-1}L_xL_y, R_{yx}^{-1}R_xR_y, -) \text{ and } ([L_x, R_y], R_x^{-1}M_yR_xM_y^{-1}, -),$$

with $L_{yx}^{-1}L_xL_y(1) = (yx)^{-1}(xy) = [x,y]$ and $R_x^{-1}M_yR_xM_y^{-1}(1) = R_x^{-1}(y\cdot y^{-2}x\cdot y) = R_x^{-1}(y^{-1}x\cdot y) = [y,x^{-1}]$. The former case yields $([x,y], R_{yx}^{-1}R_xR_y) \in \mathrm{LPs}(Q)$. Hence $(R_{yx}^{-1}R_xR_y, [y,x]) \in \mathrm{RPs}(Q)$.

The equation $xy\cdot zx = x\cdot yz\cdot x$ implies $L_{xy} = M_xL_yR_x^{-1}$ and $R_{zx} = M_xR_zL_x^{-1}$. Hence $L_{xy}^{-1}L_xL_y = R_xL_y^{-1}M_x^{-1}L_xL_y = [R_x^{-1}, L_y]$. Proceeding in the mirror way yields $R_{zx}^{-1}R_xR_z = L_xR_z^{-1}M_x^{-1}R_xR_z = [L_x^{-1}, R_z]$. □

**Associators and the right nucleus.** Recall that the associator $[x,y,z]$ is defined as $(x\cdot yz)\backslash(xy\cdot z)$. There is certain amount of arbitrary decision in this definition. Each of / and \ is eligible to use, and there is no obvious reason for the order of $x\cdot yz$ and $xy\cdot z$. However, this is not a big deal since associators are nearly always used in situations when the way of their definition matters much less than it might have been expected.

*Suppose that $x$, $y$ and $z$ are elements of a loop $Q$. If $[x,y,z] \in N_\rho(Q)$, then*

$$z = L_{xy}^{-1}L_xL_y(z)\cdot[x,y,z].$$

*Proof.* Multiplying the equality to be proved by $xy$ upon the left yields

$$xy\cdot z = (xy)(((xy)\backslash(x\cdot yz))[x,y,z]).$$

Since $[x,y,z] \in N_\rho(Q)$, the right hand side is equal $(x\cdot yz)[x,y,z]$. The equation $xy\cdot z = (x\cdot yz)[x,y,z]$ is true since this is the definition of $[x,y,z]$. □

The above statement has a number of variations and extensions. However, at this point a detailed treatment will be restricted only to the case of loops $Q$ that are of nilpotency class two. For such a loop there exist abelian groups $(G,+)$ and $(Z,\cdot)$ such that $Z \le Z(Q)$ and $(Q/Z,\cdot) \cong (G,+)$. The operation in $Q$ is thus written multiplicatively, while in $Q/Z$ additively. The situation that is of main interest is that of $Z = Z(Q)$. However, for formal reasons it is better to assume that $Z \le Z(Q)$ and $Q/Z$ is abelian.

**Associators and commutators as mappings between two abelian groups.** Let $(G,+)$ and $(Z,\cdot)$ be abelian groups such that $Q/Z = G$ and $Z \le Z(Q)$, where $Q$ is a loop. *Then there exist mappings $C\colon G\times G\to Z$ and $A\colon G\times G\times G\to Z$ such that for all $u,v,w\in Q$:*

$$[u,v] = z \;\Leftrightarrow\; C(uZ,vZ) = z \quad\text{and}\quad [u,v,w] = z \;\Leftrightarrow\; A(uZ,vZ,wZ) = z.$$

*Proof.* Consider $u,v,w \in Q$ and put $z = [u,v,w]$. Thus $(u\cdot vw)z = uv\cdot w$. If $a,b,c \in Z(Q)$, then clearly $(ua(vb\cdot wc))z = (ua\cdot vb)wc$. The case of the commutator is similar. □

**Associators, commutators and inner mappings.** *Let $Q$, $G$, $Z$, $C$ and $A$ be as above. If $u,v,w\in Q$, then $C(uZ,vZ)\cdot C(vZ,uZ) = 1$,*

$$\begin{aligned}
R_u^{-1}L_u(v) &= v\cdot C(uZ,vZ),\\
L_{uv}^{-1}L_uL_v(w) &= w\cdot A(uZ,vZ,wZ)^{-1},\\
R_{vu}^{-1}R_uR_v(w) &= w\cdot A(wZ,vZ,uZ),\\
[L_u,R_v](w) &= w\cdot A(uZ,wZ,vZ)^{-1} \text{ and}\\
[R_v,L_u](w) &= w\cdot A(uZ,wZ,vZ).
\end{aligned}$$

*Proof.* Suppose first that $vu\cdot z = uv$. Then $uv\cdot z^{-1} = vu$, $z = C(uZ,vZ)$ and $z^{-1} = C(vZ,uZ)$.

Suppose now that $z\in Q$ is such that $R_u^{-1}L_u(v) = vz$. Then $z\in Z$ and $(uv)/u = vz$ yields $uv = vu\cdot z$.

The case of $L_{uv}^{-1}L_uL_v(w)$ follows from a result above. If $z \in Q$ is such that $R_{vu}^{-1}R_uR_v(w) = wz$, then $z \in Z$ and $wv \cdot u = wz \cdot vu = (w \cdot vu)z$. Hence $z = (w \cdot vu)\backslash(wv \cdot u) = [w, v, u]$.

If $[L_u, R_v](w) = wz$, then $u \cdot wv = (u \cdot wz)v = (uw \cdot v)z$ and $z^{-1} = [u, w, v]$. □

**Associators and automorphic inner mappings.** *Let $Q$, $G$, $Z$ and $A$ be as above.*

(1) *If $L_{xy}^{-1}L_xL_y \in \mathrm{Aut}(Q)$ for all $x, y \in Q$, then $A(a, b, c + d) = A(a, b, c) \cdot A(a, b, d)$ for all $a, b, c, d \in G$.*
(2) *If $R_{yx}^{-1}R_xR_y \in \mathrm{Aut}(Q)$ for all $x, y \in Q$, then $A(a + b, c, d) = A(a, c, d) \cdot A(b, c, d)$ for all $a, b, c, d \in G$.*
(3) *If $[L_x, R_y] \in \mathrm{Aut}(Q)$ for all $x, y \in Q$, then $A(a, b + c, d) = A(a, b, d) \cdot A(a, c, d)$ for all $a, b, c, d \in G$.*

*Proof.* Let $x, y \in Q$ be such that $L_{xy}^{-1}L_xL_y \in \mathrm{Aut}(Q)$. If $w_1, w_2 \in Q$, then $L_{xy}^{-1}L_xL_y(w_1w_2) = L_{xy}^{-1}L_xL_y(w_1)L_{xy}^{-1}L_xL_y(w_2)$. Therefore

$$w_1w_2 \cdot [x, y, w_1w_2]^{-1} = (w_1 \cdot [x, y, w_1]^{-1})(w_2 \cdot [x, y, w_2]^{-1}).$$

The rest follows from the centrality of associators.

The other cases are similar. □

**Moufang loops of nilpotency class two.** *Let $Q$ be a loop with a central subloop $Z$ such that $(Q/Z, \cdot) = (G, +)$, where $G$ is an abelian group. Then there exists a mapping $A\colon G \times G \times G \to Z$ such that $A(xZ, yZ, zZ) = [x, y, z]$ for all $x, y, z \in Q$. The loop is Moufang if and only if*

$$A(a, b, c) = A(b, c, a) = A(c, a, b) = A(b, a, c)^{-1} = A(a, c, b)^{-1} = A(c, b, a)^{-1},$$
$$A(a, a, b) = 1 \quad \textit{and} \quad A(a, b, c + d) = A(a, b, c) \cdot A(a, b, d)$$

*holds for any choice of $a, b, c, d \in Q$.*

*An equivalent condition is that*

$$A(a, a, b) = A(b, a, a) = 1,\ A(a + b, c, d) = A(a, c, d) \cdot A(b, c, d),$$
$$A(a, b + c, d) = A(a, b, d) \cdot A(a, c, d) \ \textit{and}\ A(a, b, c + d) = A(a, b, c) \cdot A(a, b, d),$$

*for all $a, b, c, d \in Q$.*

*Proof.* The former condition on $A$ clearly implies the latter condition. To get the converse implication it suffices to prove $A(a, b, c)^{-1} = A(b, a, c)$ since $A(a, b, c)^{-1} = A(a, c, b)$ may be obtained by a mirror argument. The proof follows from $1 = A(a + b, a + b, c) = A(a, b, c)\,A(b, a, c)\,A(a, a, c)\,A(b, b, c) = A(a, b, c)\,A(b, a, c)$.

If $x$ and $y$ are elements of a Moufang loop $Q$, then $L_{xy}^{-1}L_xL_y$, $R_{yx}^{-1}R_xR_y$ and $[L_x, R_y]$ are automorphisms since they are pseudoautomorphisms with central companions. Thus $A(a, b, c + d) = A(a, b, c) \cdot A(a, b, d)$, and similarly in the other two cases. The equalities $A(a, a, b) = A(b, a, a) = 1$ follow from the diassociativity (in fact, all that is needed here are the alternative laws).

Let now $A$ fulfil the conditions of the statement. Then $A(-a, b, c) = A(a, b, c)^{-1}$ for all $a, b, c \in G$. Therefore $A(-a, a, b) = 1$, and that implies $(1/x) \cdot xy = (1/x)x \cdot y = y$ for all $x, y \in Q$. That makes $Q$ a LIP loop. The RIP may be be proved by a mirror argument.

This yields $[R_x^{-1}, L_y] = [L_y, R_x]$ since if $z \in Q$, then $[R_x^{-1}, L_y](z) = z \cdot [y, z, x^{-1}]$ and $[L_y, R_x](z) = z \cdot [y, z, x]^{-1}$. Because $L_{xy}^{-1}L_xL_y(z) = z \cdot [x, y, z]^{-1}$, the identity $[L_y, R_x] = L_{xy}^{-1}L_xL_y$ holds as well. Therefore

$$L_{xy}^{-1}L_xL_yR_x = [R_x^{-1}, L_y]R_x = R_xL_y^{-1}R_x^{-1}L_yR_x = R_x[L_y, R_x].$$

Multiplying this equality by $[R_x, L_y]$ upon the right yields $L_{xy}^{-1} L_x R_x L_y = R_x$. That may be written as $L_x R_x L_y = L_{xy} R_x$. And that is the same as the Moufang identity $x(yz \cdot x) = xy \cdot zx$. □

**Example of a commutative Moufang loop.** Let $V$ be a vector space over a field $F$. Suppose that $\mathrm{char}(F) = 3$ and $\dim(V) = 3$.

Upon $V \times F$ define a loop $Q$ by

$$(u, a)(v, b) = (u + v, a + b + (u_3 - v_3)(u_1 v_2 - u_2 v_1)),$$

where $u = (u_1, u_2, u_3)$ and $v = (v_1, v_2, v_3)$. This is obviously a commutative loop (in any characteristic) of nilpotence class two. To show that this is a Moufang loop it is thus enough to verify that $A$ is a trilinear alternating form.

Consider $u, v, w \in V$. Then

$$(u, 0)(v, 0) \cdot (w, 0) = (u + v, (u_3 - v_3)(u_1 v_2 - v_2 v_1)) \cdot (w, 0)$$

is equal to $(u + v + w, X)$, where $X$ evaluates to

$$\begin{aligned}
&(u_3 - v_3)(u_1 v_2 - v_2 v_1) + (u_3 + v_3 - w_3)((u_1 + v_1)w_2 - (u_2 + v_2)w_1) \\
&= u_1 u_3 v_2 - u_1 v_2 v_3 - u_2 u_3 v_1 + u_2 v_1 v_3 \\
&\quad + u_1 u_3 w_2 + u_3 v_1 w_2 - u_2 u_3 w_1 - u_3 v_2 w_1 \\
&\quad + u_1 v_3 w_2 + v_1 v_3 w_2 - u_2 v_3 w_1 - v_2 v_3 w_1 \\
&\quad - u_1 w_2 w_3 - v_1 w_2 w_3 + u_2 w_1 w_3 + v_2 w_1 w_3.
\end{aligned}$$

Similarly,

$$(u, 0) \cdot (v, 0)(w, 0) = (u, 0)(v + w, (v_3 - w_3)(v_1 w_2 - v_2 w_1))$$

yields $(u + v + w, Y)$, where $Y$ is equal to

$$\begin{aligned}
&(v_3 - w_3)(v_1 w_2 - v_2 w_1)) + (u_3 - v_3 - w_3)(u_1(v_2 + w_2) - u_2(v_1 + w_1)) \\
&= v_1 v_3 w_2 - v_1 w_2 w_3 - v_2 v_3 w_1 + v_2 w_1 w_3 \\
&\quad + u_1 u_3 v_2 + u_1 u_3 w_2 - u_2 u_3 v_1 - u_2 u_3 w_1 \\
&\quad - u_1 v_2 v_3 - u_1 v_3 w_2 + u_2 v_1 v_3 + u_2 v_3 w_1 \\
&\quad - u_1 v_2 w_3 - u_1 w_2 w_3 + u_2 v_1 w_3 + u_2 v_1 w_3.
\end{aligned}$$

Since $A(u, v, w) = X - Y$, the value of $A(u, v, w)$ is equal to

$$u_3 v_1 w_2 - u_3 v_2 w_1 + 2u_1 v_3 w_2 - 2u_2 v_3 w_1 - u_1 v_2 w_3 + u_2 v_1 w_3.$$

In characteristic 3 this coincides with $\det(u, v, w)$. The determinant is, of course, a trilinear alternating form.

Note that $(u, a)(u, a) = (-u, -a)$ and that $(u, a)(-u, -a) = (0, 0)$ for all $(u, a) \in V \times F$. The neutral element of the loop $Q$ is equal to $(0, 0)$. Note that if the neutral element is also denoted by 1, then $x^3 = 1$ for each $x \in Q$.

When referring to a *commutative Moufang loop* it is quite common to use an abbreviation CML. A CML $Q$ in which $x^3 = 1$ holds for each $x \in Q$ is said to be a CML of *exponent three*.

**A central endomorphism.** *Let $Q$ be a CML. The mapping $x \mapsto x^3$ is an endomorphism of $Q$. Put $Z = \{x^3;\ x \in Q\}$. Then $Z \leq Z(Q)$. The loop $Q/Z$ is of exponent three.*

*Proof.* Since $Q$ is diassociative, $\langle x, y \rangle$ is a commutative group for any choice of $x, y \in Q$. Therefore $(xy)^n = x^n y^n$ for any $n \geq 1$. The only fact to prove thus is that $x^3 \in Z(Q)$. Because $Q$ is commutative it suffices to show that $x^3 \in N(Q)$. Since $Q$ is Moufang, $T_x$ is an automorphism with (the right) companion $x^3$. This implies that $x^3 \in N(Q)$ if and only if $R_x^{-1} L_x \in \mathrm{Aut}(Q)$. If $Q$ is commutative, then $R_x^{-1} L_x$ is equal to $\mathrm{id}_Q$, which certainly is an automorphism of $Q$. □

**Structure of CML.** A CML $Q$ has a *torsion part*, which is the subloop of all elements of finite order. A CML that is equal to its torsion part is said to be a *torsion CML*. A torsion CML that contains no element of order three has to be an abelian group since each element of such a CML can be expressed as a cube. From this it is not difficult to prove that each torsion CML $Q$ may be uniquely expressed as $G \times S$, where $G$ is an abelian group that contains no element of order three and $S$ is the subloop of all elements that are of order $3^k$ for some $k \geq 0$.

A more difficult proof shows that *each finitely generated CML is nilpotent*.

**CML of exponent three and HTS.** The abbreviation HTS refers to a *Hall Triple System*. This is an STS with the property that each three elements that do not form a block are contained in an affine subsystem of order 9.

Let $V$ be a vector space over $\mathbb{F}_3$. The operation $*$ of the affine STS upon $V$ is given by $x * y = -x - y$. This implies

$$x * (y * z) = x * (-y - z) = -x + y + z = (-x - y) * (-x - z) = (x * y) * (x * z).$$

The operation of HTS is thus (self)*distributive*.

To prove the converse, consider elements $x$, $y$ and $z$ of a distributive STS quasigroup $(Q, *)$. Denote $z$ by $[0,0]$, $y$ by $[1,0]$ and $x$ by $[0,1]$. Set

$$\begin{array}{lll} [2,0] = [0,0] * [1,0], & [0,2] = [0,0] * [0,1], & [1,1] = [0,2] * [2,0], \\ [2,2] = [0,0] * [1,1], & [1,2] = [1,0] * [1,1], & [2,1] = [0,1] * [1,1]. \end{array}$$

Ensuing additions are performed modulo 3. If $[a,b] * [c,d] = [e,f]$ and $e = -a - c$ and $f = -b - d$, then $[a,b] * [e,f] = [c,d]$ and $c = -a - e$ and $d = -b - f$. For $a, b, c, d \in \mathbb{F}_3$ the equation $[a,b] * [c,d] = [-a - c, b - d]$ thus holds for the six affine lines of $V = F \times F$. The six missing lines are those that pass through $(2,2)$, with the exception of $\{(0,0),(1,1),(2,2)\}$, and the lines $\{(0,0),(2,1),(1,2)\}$, $\{(0,2),(1,0),(2,1)\}$ and $\{(2,0),(0,1),(1,2)\}$. The distributivity implies

$$\begin{aligned} &[0,0] * [1,1] = [0,0] * ([2,0] * [0,2]]) = ([0,0] * [2,0]) * ([0,0] * [0,2]), \\ &[1,0] * [0,1] = ([0,0] * [2,0]) * ([0,0] * [0,2]) = [0,0] * [1,1] = [2,2], \\ &[2,1] * [1,2] = [1,1] * ([0,1] * [1,0]) = [1,1] * [2,2] = [0,0], \\ &[1,0] * [2,1] = [1,0] * ([0,0] * [1,2]) = [2,0] * [1,1] = [0,2], \text{ and} \\ &[2,0] * [2,1] = [0,0] * ([1,0] * [1,2]) = [0,0] * [1,1] = [2,2]. \end{aligned}$$

Equalities $[0,1] * [1,2] = [2,0]$ and $[0,2] * [1,2] = [2,2]$ may be obtained by a mirror argument. The mapping $(a,b) \mapsto [a,b]$ thus yields a surjective homomorphism of $(V, *)$ upon the subsystem of $Q$ generated by $x$, $y$ and $z$. If the homomorphism is not injective, then either $\{x,y,z\}$ is a block, or $x = y = z$. This proves that distributive STS systems are exactly the HTS systems.

To get the connection to CMLs fix an element $a$ of an STS quasigroup $Q$. Then $xy = x/a*a\backslash y = (x*a)*(a*y)$ is a commutative loop operation with $a = a*a$ being the unit. Note that $xx = x * a$ and that $x \cdot xx = xx \cdot x = x^3 = a$. If the operation star is distributive, then $xy = a * (x * y)$. In such a case $xy \cdot x = (a * (x * y)) \cdot x = (x*y)*(x*a) = x*(a*y)$. Therefore $(x \cdot yz)x = x*(a*(yz)) = x*(y*z)$. Furthermore, $xy \cdot zx = (a*(x*y)) \cdot (a*(x*z)) = (x*y)*(x*z) = x*(y*z)$. This verifies that $(Q, \cdot)$ is a CML of exponent three. Note that $(xy)^{-1} = (xy)^2 = a*(xy) = a*(a*(x*y)) = x*y$. This can be used to get a converse construction.

Indeed, if $Q$ is a CML of exponent three, then $x * y = (xy)^2$ is an idempotent commutative quasigroup that is semisymmetric since $x * (y * x) = x * (xy)^2 = x^2(xy) = y$. Hence $(Q, *)$ is an STS quasigroup. To prove the distributivity note that $x*(y*z) = x*(yz)^2 = x^2(yz) = x(yz)x = xy \cdot zx = (xy)^2 * (xz)^2 = (x*y)*(x*z)$.

Let us mention in passing that it is easy to verify that the identity $x^2 \cdot yz = xy \cdot xz$ in fact describes the variety of CML loops.

We may thus conclude by the following.

**Characterization of HTS with CML involved.** *An STS system given by an idempotent operation $*$ is an HTS if and only if the operation $*$ is distributive. In such a case for any $a \in Q$ the operation $xy = a * (x * y)$ is a CML of exponent three, and $x * y = (xy)^2$ for all $x, y \in Q$. If $(Q, \cdot)$ is a CML of exponent three, then $x * y = (xy)^2$ provides $Q$ with a structure of HTS.*

**Code loops. Their associators and commutators.** A Moufang loop $Q$ is said to be a *code loop* if it contains a two-element central subloop $Z$ such that $Q/Z$ is a finite elementary abelian 2-group.

The connection of code loops to error correcting codes (more precisely to double even binary codes) will be explained later. Let us now record several facts that may be derived from results obtained earlier. The factor loop $Q/Z$ may be identified with a vector space $V$ over $F = \{0, 1\}$.

The loop $Q$ is of nilpotence class two. An isomorphic copy of $Q$ may be thus constructed upon $V \times F$, with an operation $(u, a)(v, b) = (u + v, \vartheta(u, v) + a + b)$, where $\vartheta \colon V \times V \to F$ fulfils $\vartheta(u, 0) = \vartheta(0, u) = 0$, for every $u \in V$.

There exist mappings $C \colon V \times V \to F$ and $A \colon V \times V \times V \to F$ such that the isomorphic copy of $Q$ fulfils

$$[(u, a), (v, b)] = (0, C(u, v)) \qquad \text{and} \qquad [(u, a), (v, b), (w, c)] = (0, A(u, v, w)).$$

Note that since the element $1 \in F$ fulfils $-1 = 1$, the signs (or inverses) relating to $A(u, v, w)$ bear no effect. This means that $A$ may be regarded as a trilinear alternating (and thus symmetric) form $V \to F$.

The loop $Q$ satisfies the law $x(y \cdot zx) = (xy \cdot z)x$ since $Q$ is an extra loop. Thus

$$\begin{aligned} x(y \cdot zx) &= \big((y \cdot zx)x\big)[x, y \cdot zx] = \big((y \cdot xz)x\big)[x, z][x, y \cdot zx] \\ &= \big((yx \cdot z)x\big)[y, x, z][x, z][x, y \cdot zx] \\ &= \big((xy \cdot z)x\big)[y, x][y, x, z][x, z][x, y \cdot zx]. \end{aligned}$$

Hence $[y, x][y, x, z][x, z][x, y \cdot zx] = 1 = [x, y, z][x, y][x, z][x, y \cdot zx]$. Therefore

$$A(u, v, w) = C(u, v) + C(u, w) + C(u, u + v + w)$$

for all $u, v, w \in V$. This may be further simplified after recalling that $[x, y] = x^2y^2(xy)^2$ for all $x, y \in Q$. The latter equality holds because of the diassociativity and because $x^2$ is central and $x^3 = x^{-1}$. It follows by $[x, y] = x^3y^3xy = x^2(xyxy)y^2$.

If $z \in Z$, then $(xz)^2 = x^2$. Hence there exists a mapping $P \colon V \to Z$ such that $P(xZ) = 0$ if $x \in Q$ is of order 1 or 2, and $P(xZ) = 1$ if $x$ is of order 4. The identity $[x, y] = x^2y^2(xy)^2$ means that

$$C(u, v) = P(u) + P(v) + P(u + v) \quad \text{for all } u, v \in V.$$

This implies that

$$C(u, u + v) = P(u) + P(u + v) + P(v) = C(u, v).$$

Therefore $C(u, u + v + w) = C(u, v + w)$ and

$$\begin{aligned} A(u, v, w) &= C(u, v) + C(u, w) + C(u, v + w) \\ &= P(u) + P(v) + P(w) + P(u{+}v) + P(u{+}w) + P(v{+}w) + P(u{+}v{+}w), \end{aligned}$$

for all $u, v, w \in V$. The commutator and associator of $Q$ are thus fully determined by the mapping $P$.

**Combinatorial degree.** Let $V$ be a vector space over the 2-element field $F = \{0,1\}$, and let $P\colon V \to F$ be such that $P(0) = 0$. The mapping $P$ is said to be of *combinatorial degree* 0 if $P(v) = 0$ for all $v \in V$. The mapping $P$ is said to be of *combinatorial degree* $k \geq 1$ if

$$(u_1, \ldots, u_k) \mapsto \sum_{1 \leq j \leq k} \sum_{1 \leq i_1 < \cdots < i_j \leq k} P(u_{i_1}) + \cdots + P(u_{i_k})$$

is a $k$-linear map, and $P$ is not of combinatorial degree $k-1$. Note that $P$ is of combinatorial degree 1 if and only if it it is a nontrivial linear form, and of combinatorial degree 2 if and only if it is a quadratic form that is not a linear form.

We have seen that squares of a code loop yield a mapping of a combinatorial degree 3. For the converse direction consider a mapping $P\colon V \to F = \{0,1\}$, $P(0) = 0$, that is of combinatorial degree at most 3. Set $C(u,v) = P(u) + P(v) + P(u+v)$ and $A(u,v,w) = C(u,v) + C(u,w) + C(u,v+w)$, for all $u, v, w \in V$. The mapping $A$ is a symmmetric trilinear form $V \to F$. It is alternating since, e.g., $A(u,v,v) = 2C(u,v) + C(u,2v) = 0$. Our aim now is to prove that each $P$ that is of combinatorial degree at most three, $P(0) = 0$, induces a code loop the structure of which is determined by $P$ uniquely, up to isomorphism.

**Code loops from square mappings of combinatorial degree three.** Let $P\colon V \to \{0,1\}$, $P(0) = 0$, be of combinatorial degree at most 3. Define $C$ and $A$ as above.

Our aim is to show that there exists a code loop $Q$ such that $Q/Z$ may be identified with $V$, and $P$ is induced by the square mapping $x \mapsto x^2$. We shall proceed by assuming that $Q$ exists and derive from that a formula for the operation. To prove the existence of $Q$ it will then suffice to verify that the obtained formula really gives a code loop. For that a construction established earlier may be used. That is the construction of a Moufang loop with operation $(u,a)(v,b) = (u+v, q(u,v) + a + b)$, where $q\colon V \times V \to F$ is linear in the second coordinate and quadratic in the first coordinate, with $q(u+v,v) = q(u,v) + q(v,v)$ for all $u, v \in V$.

Let $b_1, \ldots, b_n$ be a basis of $V$, and let $e_1, \ldots, e_n \in Q$ be such that $b_i = e_i Z$ for each $i \in \{1, \ldots, n\}$. Each element of $Q$ may be uniquely expressed in a *normal form* as

$$(e_{i_1}(e_{i_2}(\cdots(e_{i_{k-1}}e_{i_k}))))z, \text{ where } 1 \leq i_1 < \cdots < i_k \leq n \text{ and } z \in Z.$$

This follows from the fact that $e_{i_1}(e_{i_2}(\cdots e_{i_k}))$ projects upon $\sum \lambda_j b_j$, where $\lambda_j = 1$ if $j$ occurs in the sequence $i_1, \ldots, i_k$, while otherwise $\lambda_j = 0$. We shall identify $Q$ with $V \times F$ in such a way that

$$(e_{i_1}(e_{i_2}(\cdots e_{i_k})))z \mapsto \begin{cases} (\sum \lambda_j b_j, 0) & \text{if } z = 1, \\ (\sum \lambda_j b_j, 1) & \text{if } z \neq 1. \end{cases}$$

Assume $k \geq 1$, put $j = i_1$ and $y = e_{i_2}(\cdots(e_{i_{k-1}}e_{i_k}))$. If $i \in \{1, \ldots, k\}$, then

$$e_i(e_j y) = \begin{cases} e_i(e_{i_1}(e_{i_2}(\cdots(e_{i_{k-1}}e_{i_k})))) \text{ if } i < j, \\ (e_{i_2}(\cdots(e_{i_{k-1}}e_{i_k})))\, e_j^2 \text{ if } i = j, \text{ and} \\ (e_i e_j)y\, [e_i, e_j, y] = (e_j e_i)y\, [e_i, e_j][e_i, e_j, y] = e_j(e_i y)\, [e_i, e_j] \text{ if } i > j. \end{cases}$$

The last equality follows from $(e_j e_i)y = e_j(e_i y)\, [e_j, e_i, y]$ and $[e_j, e_i, y] = [e_i, e_j, y]$.

To multiply $x = e_{i_1}(e_{i_2}(\cdots(e_{i_{k-1}}e_{i_k})))$ by $e_i$ from the left thus means to shift $e_i$ to the right until it reaches $e_{i_\ell}$, where $i \leq i_\ell$. During its travel to the right $e_i$ produces all $[e_i, e_{i_j}]$ where $i_j < i$, and also $e_i^2$ if $i = i_\ell$. In the latter case $e_i = e_{i_\ell}$ is

removed from the list. Writing this in the language of $V \times F$ gives

$$(b_i, 0)\left(\sum_j \lambda_j b_j, 0\right) = \left(\sum_j (\lambda_j + \delta_{ij}) b_j,\ \lambda_i P(e_i) + \sum_{i>j} \lambda_j C(e_i, e_j)\right),$$

where $\delta_{ij} \in \{0, 1\}$ is equal to 1 if and only if $i = j$.

For the case of a general product note that $e_\ell x \cdot y = (e_\ell \cdot xy)[e_\ell, x, y]$. If $e_\ell x$ is in a normal form, $y$ is in a normal form, and the transformation of $xy$ into a normal form has been already performed, the final step of transformation of $e_\ell x \cdot y$ into a normal form rests in putting $[e_\ell, x, y]$ together with all $[e_\ell, e_j]$ such that $e_j$ occurs in the normal form of $y$ and $j < \ell$. If $e_\ell$ occurs in the normal form of $y$, then $e_\ell$ is removed from the normal form, while $e_\ell^2$ contributes to the element of $Z$ that appears as the rightmost element of the normal form. To see that the latter is true note that while $e_\ell$ interacts with the normal form of $xy$, the interaction is restricted to the part on the left in which there occur indices $\leq \ell$. This part of the normal form of $xy$ coincides with the corresponding left part of $y$ since $\ell$ is the smallest index occuring in $x$.

This gives a recursive procedure for a transformation into a normal norm of any two products. Let the projection of $e_\ell x$ be $u = \sum \lambda_i b_i$ and suppose that $y$ projects to $v = \sum \nu_i b_i$. The mapping $A$ is trilinear. The contribution of associators thus amounts to the sum of all $A(\lambda_i b_i, \lambda_j b_j, \nu_k b_k)$, where $i < j$. The product of $(u, 0)$ and $(v, 0)$ is thus equal to $(u + v, q(u, v))$, where

$$q(u, v) = \sum_k \nu_k \left(\lambda_k P(b_k) + \sum_{i>k} \lambda_i C(b_i, b_k) + \sum_{i<j} \lambda_i \lambda_j A(b_i, b_j, b_k)\right).$$

The mapping $q$ clearly is linear in the second variable. Sums of quadratic forms are quadratic forms. Hence to prove that $q$ is quadratic in the first variable it suffices to verify that the mapping

$$q_k(u) = \lambda_k P(b_k) + \sum_{i>k} \lambda_i C(b_i, b_k) + \sum_{i<j} \lambda_i \lambda_j A(b_i, b_j, b_k)$$

is quadratic for each $k \in \{1, \ldots, n\}$. Let $u = \sum \lambda_i b_i$ and $v = \sum \nu_i b_i$. The contributions of $P$ and $C$ in $q_k(u) + q_k(v) + q_k(u + v)$ amount to

$$(\lambda_k + \nu_k + (\lambda_k + \nu_k))P(b_k) + \sum_{i>k} ((\lambda_i + \nu_i + (\lambda_i + \nu_i))C(b_i, b_k).$$

This vanishes. Since $\lambda_i \lambda_j + \nu_i \nu_j + (\lambda_i + \nu_i)(\lambda_j + \nu_j)$ yields $\lambda_i \nu_j + \lambda_j \nu_i$ we see that

$$q_k(u) + q_k(v) + q_k(u + v) = \sum_{i,j} \lambda_i \nu_j A(b_i, b_j, b_k)$$

is bilinear. It remains to verify that $q(u + v, v) = q(u, v) + q(v, v)$. To see this observe first that $q(u, v)$ may be also expressed as

$$\sum_k \nu_k \left(\lambda_k P(b_k) + \sum_{i>k} \lambda_i C(b_i, b_k)\right) + \sum_{\{i,j,k\}} (\lambda_i \lambda_j \nu_k + \lambda_i \nu_j \lambda_k + \nu_i \lambda_j \lambda_k) A(b_i, b_j, b_k).$$

The sum upon the right runs over all 3-element subsets of $\{1, \ldots, n\}$. The formula is independent of the ordering of the subset. To see the connection to the original expression of $q(u, v)$, assume $i < j < k$ and note that the original formula carries

$$\nu_k \lambda_i \lambda_j A(b_i, b_j, b_k) + \nu_j \lambda_i \lambda_k A(b_i, b_k, b_j) + \nu_i \lambda_j \lambda_k A(b_j, b_k, b_i)$$

and that these are all occurences of $A(b_{\sigma(i)}, b_{\sigma(j)}, b_{\sigma(k)})$ in the formula, where $\sigma$ is a permutation of $\{i, j, k\}$.

Since $(\lambda_k+\nu_k)P(b_k)=\lambda_kP(b_k)+\nu_kP(b_k)$ and $(\lambda_i+\nu_i)C(b_i,b_k)=\lambda_iC(b_i,b_k)+\nu_iC(b_i,b_k)$ the proof of $q(u+v,v)=q(u,v)+q(v,v)$ requires verification only for the coefficients of $A(b_i,b_j,b_k)$. However,

$$(\lambda_i+\nu_i)(\lambda_j+\nu_j)\nu_k+(\lambda_i+\nu_i)\nu_j(\lambda_k+\nu_k)+\nu_i(\lambda_j+\nu_j)(\lambda_k+\nu_k)$$

evaluates to

$$\lambda_i\lambda_j\nu_k+\lambda_i\nu_j\lambda_k+\nu_i\lambda_j\lambda_k+3\nu_i\nu_j\nu_k$$

which is exactly the aggregated contribution of $q(u,v)+q(v,v)$.

This verifies that the procedure yields a code loop. If at the beginning there had been a code loop $Q$ the squares of which induce $P$, the constructed loop is isomorphic to $Q$ since $q(u,v)$ expresses products of elements in a normal form. A normal form depends upon the choice of basis. The formula for $q(u,v)$ thus provides loops isomorphic to $Q$ for any choice of basis $b_1,\dots,b_n$.

Consider now a situation when at the beginning there was only a mapping $P$ of combinatorial degree at most three, $P(0)=0$. By means of $q(u,v)$ we have constructed a code loop in which squaring is given by $\tilde{P}(u)=q(u,u)$. The question is whether $\tilde{P}=P$. If this is true, then by the argument above the formula for $q(u,v)$ provides a code loop the isomorphism type of which does not dependent upon the choice of basis.

The proof of $\tilde{P}=P$ is divided into two steps. Assume $1\le i<j<k\le n$. We have

$$\begin{aligned}
(b_k,0)(b_k,0)&=(0,P(b_k)),\\
(b_i+b_k,0)^2&=(0,P(b_i)+P(b_j)+C(b_k,b_i))=(0,P(b_i+b_k)),\ \text{and}\\
(b_i+b_j+b_k,0)^2&=(0,P(b_i)+P(b_j)+P(b_k)\\
&\quad+C(b_j,b_i)+C(b_k,b_j)+C(b_k,b_i)+A(b_i,b_j,b_k))\\
&=(0,P(b_i)+P(b_j)+P(b_k)+P(b_i+b_j)+P(b_j+b_k)\\
&\quad+P(b_i+b_k)+A(b_i,b_j,b_k))\\
&=(0,P(b_i+b_j+b_k)).
\end{aligned}$$

This shows that $\tilde{P}$ and $P$ agree at all values $b_i$, $b_i+b_j$ and $b_i+b_j+b_k$. Hence they agree everywhere, as will be proved now.

**Values that determine the square mapping completely.** *Let $P\colon V\to\{0,1\}$, $P(0)=0$, be a mapping of combinatorial degree at most three. Let $b_1,\dots,b_n$ be a basis of $V$. Then $P$ is completely determined by all of the values $P(b_i)$, $P(b_i+b_j)$ and $P(b_i+b_j+b_k)$, where $i,j,k\in\{1,\dots,n\}$.*

*Proof.* For each $u=\sum\lambda_iu_i\in V$ denote by $|u|$ the number of $i\in\{1,\dots,n\}$ such that $\lambda_i=1$. Call $|u|$ the *weight* of $u$. The value of $P(u)$ is known if $|u|\le3$. We shall show by induction that each $P(u)$ may be expressed as a sum of $P(w)$, where $|w|\le3$. To do so express $u$ as $v+e_i+e_j+e_k$, where $|u|-3=|v|\ge1$. Then $A(v+e_i,e_j,e_k)=A(v,e_j,e_k)+A(e_i,e_j,e_k)$. The expression of $A(v+e_i,e_j,e_k)$ by means of $P$ is a sum of $P(u)$ and of $P$-values for vectors of weight $<|u|$. The expressions of $A(v,e_j,e_k)$ and $A(e_i,e_j,e_k)$ also consists of sums of $P(w)$, where $|w|<|u|$. Hence $P(u)$ may be expressed as such a sum too, and that makes the induction applicable. □

**Existence and uniqueness of code loops.** *Let $V$ be a vector space over $F=\{0,1\}$ with a basis $b_1,\dots,b_n$. For each mapping $P\colon V\to F$, $P(0)=0$, that is of combinatorial degree at most three there exists, up to isomorphism, a unique code loop $(Q,\cdot,1)$ with a central subloop $Z$, $|Z|=2$, where $V$ is identified with $Q/Z$ in such a way that $P(xZ)=0$ if $x^2=1$ and $P(xZ)=1$ otherwise. Such a loop is*

*always isomorphic to a loop $V[P]$ that is defined upon $V \times F$ in such a way that if $u = \sum \lambda_i b_i$, $v = \sum \nu_i b_i$ and $a, b \in F$, then $(u, a) \cdot (v, b) = (u + v, a + b + c)$, where $c$ is equal to*

$$\sum_k \nu_k \left( \lambda_k P(b_k) + \sum_{i>k} \lambda_i C(b_i, b_k) \right) + \sum_{\{i,j,k\}} (\lambda_i \lambda_j \nu_k + \lambda_i \nu_j \lambda_k + \nu_i \lambda_j \lambda_k) A(b_i, b_j, b_k),$$

*with $C(x, y) = P(x)+P(y)+P(x+y)$ and $A(x, y, z) = C(x, z)+C(y, z)+C(x+y, z)$ for all $x, y, z \in V$.*

*If $P_i \colon V \to F$, $P_i(0) = 0$, $i \in \{1, 2\}$ are two mappings of combinatorial degree three, then $V[P_1] \cong V[P_2]$ if and only if there exists a linear automorphism $\alpha \in \mathrm{Aut}(V)$ such that $P_2(v) = P_1(\alpha(v))$ for each $v \in V$.*

*Proof.* Only the part about the isomorphism of $V[P_1]$ and $V[P_2]$ requires a proof. Assume first the existence of $\alpha$ and extend it to a permutation $\bar{\alpha}$ of $V \times F$, $\bar{\alpha}(u, a) = (\alpha(u), a)$. The mapping $\bar{\alpha}$ induces a loop $Q$ upon $V \times F$ such that $\bar{\alpha} \colon Q \cong V[P_1]$. The square of $(u, a)$ in $Q$ is equal to $\bar{\alpha}^{-1}((\bar{\alpha}(u, a))^2) = \bar{\alpha}^{-1}((\alpha(u), a)^2) = \bar{\alpha}^{-1}(0, P_1(\alpha(u))) = \bar{\alpha}^{-1}(0, P_2(u)) = (0, P_2(u))$. Therefore $Q \cong P_2[V]$. Since $Q$ is defined in such a way that $Q \cong V[P_1]$, there must be $V[P_1] \cong V[P_2]$.

For the converse direction suppose that $\psi \colon V[P_2] \cong V[P_1]$. Since both $P_1$ and $P_2$ are of combinatorial degree three, the central associator elements of both $V[P_1]$ and $V[P_2]$ are equal to $(0, 0)$ and $(0, 1)$. Therefore $\psi$ induces a linear automorphism $\alpha$ such that for each $(u, a) \in V \times F$ there exists $b \in F$ such that $\psi(u, a) = (\alpha(u), b)$. Hence $(0, P_2(u)) = \psi((u, a)(u, a)) = (\alpha(u), b)(\alpha(u), b) = (0, P_1\alpha(u))$. □

**Connection to error correcting codes.** A *binary linear code* $D$ is any vector subspace of $F^n$, $F = \{0, 1\}$, $n \geq 1$. The term *code* is being used when $\min\{|u|; u \in D, u \neq 0\}$ is relatively large if compared to $\dim(D)$ and $n$. A binary linear code $D$ is called *doubly even* if 4 divides $|u|$ for each $u \in D$. An example of doubly even code is the extended binary Golay code of length $n = 24$.

Let $D$ be a doubly even code. For $u \in D$ set $P(u) = 0$ if 8 divides $|u|$, and $P(u) = 1$ if $|u| \equiv 4 \bmod 8$. If $u, v \in D$, set $C(u, v) = 0$ if $|u \cap v|$ is divisible by 4. Otherwise set $C(u, v) = 1$. (If $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$, then $u \cap v = (u_1 v_1, \ldots, u_n v_n)$.)

Since $|u + v| = |u| + |v| - 2|u \cap v|$ we have $4P(u + v) \equiv 4P(u) + 4P(v) - 4|u \cap v|/2 \bmod 8$. Hence $P(u + v) \equiv P(u) + P(v) + |u \cap v|/2 \bmod 2$. Therefore $C(u, v) = P(u) + P(v) + P(u + v)$.

Since $|(u + v) \cap w| = |(u \cap w)| + |(v \cap w)| - 2|u \cap v \cap w|$ there has to be

$$2C(u + v, w) \equiv 2C(u, w) + 2C(v, w) - 2|u \cap v \cap w| \bmod 4.$$

Put $A(u, v, w) = 0$ if $|u \cap v \cap w|$ is even. Otherwise set $A(u, v, w) = 1$. The congruence above shows that

$$A(u, v, w) \equiv C(u + v, w) + C(u, w) + C(v, w) \bmod 2$$

for all $u, v, w \in V$. It is clear that $A(u, u, v) = 0$. The equality $A(u + v, w, z) = A(u, w, z) + A(v, w, z)$ follows from $(u + v) \cap w \cap z = u \cap w \cap z + v \cap w \cap z$ since $A(u, v, w)$ gives the parity of $|u \cap v \cap w|$.

The mapping $P$ therefore is of combinatorial degree at most 3. As such it induces a code loop upon $D \times F$. It may be proved that for each code loop $Q$ there exists a code $D$ that induces a loop isomorphic to $Q$.

The loop induced by the extended binary Golay code is known as *Parker loop*. The Parker loop may be used as a departing point of the construction of the Monster (or Friendly Giant), the largest sporadic finite simple group.