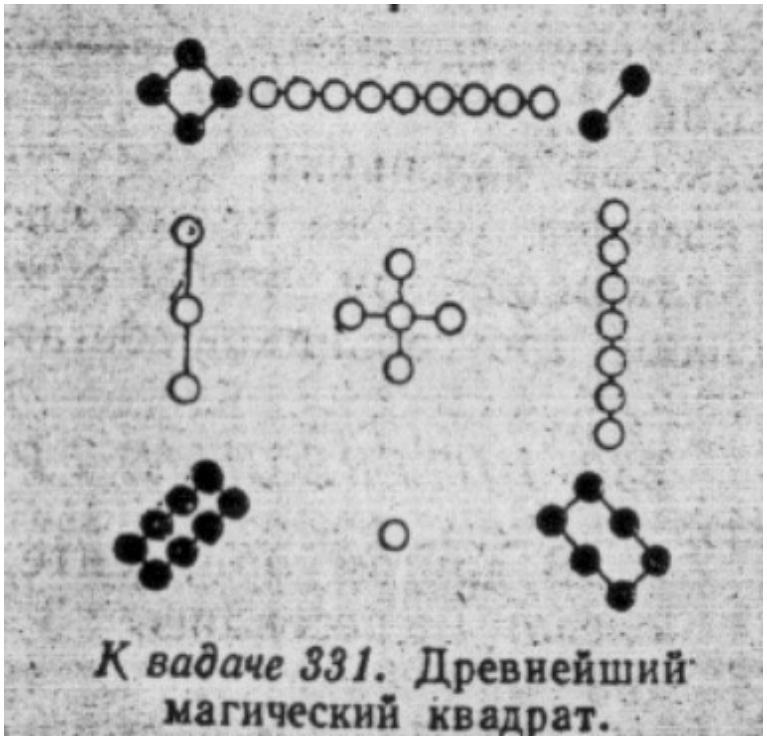
On direct decomposition of some finite quasigroups

Victor Shcherbacov

Central European University and Institute of Mathematics and Computer Science
of the Academy of Sciences of Moldova

Budapest, 2010

Magic square (China)



4	9	2
3	5	7
8	1	6

Orthogonal Latin squares

Orthogonal Latin squares

$$\begin{array}{ccc} a & b & c \\ c & a & b \\ b & c & a \end{array}$$

Orthogonal Latin squares

$$\begin{array}{cccccc} a & b & c & A & C & B \\ c & a & b & C & B & A \\ b & c & a & B & A & C \end{array}$$

Orthogonal Latin squares

$$\begin{array}{cccccc} a & b & c & A & C & B \\ c & a & b & C & B & A \\ b & c & a & B & A & C \end{array}$$

In any row, in any column any element occurs exactly one time.

Orthogonal Latin squares

a	b	c	A	C	B
c	a	b	C	B	A
b	c	a	B	A	C

In any row, in any column any element occurs exactly one time.

aA	bC	cB
cC	aB	bA
bB	cA	aC

Orthogonal Latin squares

a	b	c	A	C	B
c	a	b	C	B	A
b	c	a	B	A	C

In any row, in any column any element occurs exactly one time.

aA	bC	cB
cC	aB	bA
bB	cA	aC

Orthogonal Latin square studied Leonard Euler (1782).

$$\begin{array}{ccc} a & b & c \\ c & a & b \\ b & c & a \end{array}$$

$$\begin{array}{ccc} a & b & c \\ c & a & b \\ b & c & a \end{array}$$

- $\begin{array}{ccc} a & b & c \\ c & a & b \\ b & c & a \end{array}$
- $\begin{array}{c|ccc} \circ & a & b & c \\ \hline a & a & b & c \\ b & c & a & b \\ c & b & c & a \end{array}$
- $a \circ c = c, b \circ a = c.$

- $\begin{array}{ccc} a & b & c \\ c & a & b \\ b & c & a \end{array}$
- $\begin{array}{c|ccc} \circ & a & b & c \\ \hline a & a & b & c \\ b & c & a & b \\ c & b & c & a \end{array}$
- $a \circ c = c, b \circ a = c.$

- $\begin{matrix} a & b & c \\ c & a & b \\ b & c & a \end{matrix}$
- $\begin{array}{c|ccc} \circ & a & b & c \\ \hline a & a & b & c \\ b & c & a & b \\ c & b & c & a \end{array}$
- $a \circ c = c, b \circ a = c.$
- W. Dornte (1928), A. Suchkevich (1929), Ruth Moufang (1935) defined a quasigroup.

A binary groupoid (G, A) is a non-empty set G together with a binary operation A.

A binary groupoid (G, A) is a non-empty set G together with a binary operation A.

Definition

Binary groupoid $(Q, \circ)$ is called a quasigroup if for all ordered pairs $(a, b) \in Q^2$ there exist unique solutions $x, y \in Q$ to the equations $x \circ a = b$ and $a \circ y = b$.

Definition

An algebra $(Q, \cdot, \backslash, /)$ with the following identities :

$$x \cdot (x \backslash y) = y, \tag{1}$$

$$(y/x) \cdot x = y, \tag{2}$$

$$x \backslash (x \cdot y) = y, \tag{3}$$

$$(y \cdot x)/x = y. \tag{4}$$

is called an e-quasigroup. Trevor Evans, 1949.

- Theorem. An algebra $(Q, \cdot, \backslash, /)$ with identities (2), (3) and $x/(y\backslash x) = y$ is an e-quasigroup.

- Theorem. Groupoid $(Q, \cdot)$ is a quasigroup if and only if algebra $(Q, \cdot, \backslash, /)$ is an e-quasigroup.
- Theorem. An algebra $(Q, \cdot, \backslash, /)$ with identities (2), (3) and $x/(y\backslash x) = y$ is an e-quasigroup.

- Theorem. Groupoid $(Q, \cdot)$ is a quasigroup if and only if algebra $(Q, \cdot, \backslash, /)$ is an e-quasigroup.
- Theorem. An algebra $(Q, \cdot, \backslash, /)$ with identities (2), (3) and $x/(y\backslash x) = y$ is an e-quasigroup.
-

Definition

Groupoid $(Q, \circ)$ is an isotopic image of a groupoid $(Q, \cdot)$ if there exist permutations α, β, γ of the set Q such that $x \circ y = \gamma^{-1}(\alpha x \cdot \beta y)$. The triple (α, β, γ) is called an isotopy (an isotopism).

Definition

Let $(Q, \cdot)$ and $(H, \circ)$ be binary quasigroups, and let φ be a single valued mapping of Q into H such that

$$\varphi(x \cdot y) = \varphi x \circ \varphi y$$

Then φ is called a *homomorphism* of $(Q, \cdot)$ into $(H, \circ)$ and the set $\{\varphi x \,|\, x \in Q\}$ is called *homomorphic image* of $(Q, \circ)$ under φ.

-

Definition

Let $(Q, \cdot)$ and $(H, \circ)$ be binary quasigroups, and let φ be a single valued mapping of Q into H such that

$$\varphi(x \cdot y) = \varphi x \circ \varphi y$$

Then φ is called a *homomorphism* of $(Q, \cdot)$ into $(H, \circ)$ and the set $\{\varphi x \,|\, x \in Q\}$ is called *homomorphic image* of $(Q, \circ)$ under φ.

- If $(Q, \cdot) = (H, \circ)$, then homomorphism is called an endomorphism.

- An equivalence θ is a congruence of a groupoid $(Q, \cdot)$, if the following implications are true for all $x, y, z \in Q$:
  $x\theta y \Longrightarrow (z \cdot x)\theta(z \cdot y), x\theta y \Longrightarrow (x \cdot z)\theta(y \cdot z)$.

- An equivalence θ is a congruence of a groupoid $(Q, \cdot)$, if the following implications are true for all $x, y, z \in Q$: $x\theta y \Longrightarrow (z \cdot x)\theta(z \cdot y), x\theta y \Longrightarrow (x \cdot z)\theta(y \cdot z)$.
- A congruence θ of a quasigroup $(Q, \cdot)$ is *normal*, if the following implications are true for all $x, y, z \in Q$: $(z \cdot x)\theta(z \cdot y) \Longrightarrow x\theta y, (x \cdot z)\theta(y \cdot z) \Longrightarrow x\theta y$.

- An equivalence θ is a congruence of a groupoid $(Q, \cdot)$, if the following implications are true for all $x, y, z \in Q$: $x\theta y \Longrightarrow (z \cdot x)\theta(z \cdot y), x\theta y \Longrightarrow (x \cdot z)\theta(y \cdot z)$.
- A congruence θ of a quasigroup $(Q, \cdot)$ is *normal*, if the following implications are true for all $x, y, z \in Q$: $(z \cdot x)\theta(z \cdot y) \Longrightarrow x\theta y, (x \cdot z)\theta(y \cdot z) \Longrightarrow x\theta y$.
- In any binary quasigroup $(Q, \cdot)$ the binary relations $\hat{Q} = \{(x, x) \,|\, x \in Q\}$ and $Q \times Q$ are normal congruences of $(Q, \cdot)$. These congruences are called the diagonal congruence and universal congruence, respectively.

-

Theorem

If h is a homomorphism of a quasigroup $(Q, \cdot)$ onto a quasigroup $(H, \circ)$, then h determines a normal congruence θ on $(Q, \cdot)$ such that $Q/\theta \cong (H, \circ)$, and vice versa, a normal congruence θ induces a homomorphism from $(Q, \cdot)$ onto $(H, \circ) \cong Q/\theta$.

-

Theorem

If h is a homomorphism of a quasigroup $(Q, \cdot)$ onto a quasigroup $(H, \circ)$, then h determines a normal congruence θ on $(Q, \cdot)$ such that $Q/\theta \cong (H, \circ)$, and vice versa, a normal congruence θ induces a homomorphism from $(Q, \cdot)$ onto $(H, \circ) \cong Q/\theta$.

- If U and W are congruences on the algebra A which commute and for which $U \cap W = \hat{A} = \{(a, a) | \forall\, a \in A\}$, then the join $U \circ W = U \vee W$ of U and W is called *direct product $U \sqcap W$ of U and W*.

-

Theorem

If h is a homomorphism of a quasigroup $(Q, \cdot)$ onto a quasigroup $(H, \circ)$, then h determines a normal congruence θ on $(Q, \cdot)$ such that $Q/\theta \cong (H, \circ)$, and vice versa, a normal congruence θ induces a homomorphism from $(Q, \cdot)$ onto $(H, \circ) \cong Q/\theta$.

- If U and W are congruences on the algebra A which commute and for which $U \cap W = \hat{A} = \{(a, a) | \forall\, a \in A\}$, then the join $U \circ W = U \vee W$ of U and W is called *direct product $U \sqcap W$ of U and W*.
- An Ω-algebra A is isomorphic to a direct product of Ω-algebras B and C with isomorphism φ, i.e. $\varphi : A \to B \times C$, if and only if there exist such congruences U and W of A that $A^2 = U \sqcap W$.

Definition

A quasigroup $(Q, \cdot)$ is
medial, if $xy \cdot uv = xu \cdot yv$ for all $x, y, u, v \in Q$;
paramedial, if $xy \cdot uv = vy \cdot ux$ for all $x, y, u, v \in Q$;
left distributive, if $x \cdot uv = xu \cdot xv$ for all $x, u, v \in Q$;
right distributive, if $xu \cdot v = xv \cdot uv$ for all $x, u, v \in Q$;
distributive, if it is left and right distributive;
idempotent, if $x \cdot x = x$ for all $x \in Q$;

Definition

A quasigroup $(Q, \cdot)$ is
medial, if $xy \cdot uv = xu \cdot yv$ for all $x, y, u, v \in Q$;
paramedial, if $xy \cdot uv = vy \cdot ux$ for all $x, y, u, v \in Q$;
left distributive, if $x \cdot uv = xu \cdot xv$ for all $x, u, v \in Q$;
right distributive, if $xu \cdot v = xv \cdot uv$ for all $x, u, v \in Q$;
distributive, if it is left and right distributive;
idempotent, if $x \cdot x = x$ for all $x \in Q$;

In any medial quasigroup the map $s : x \mapsto xx$ is an endomorphism,

Definition

A quasigroup $(Q, \cdot)$ is
medial, if $xy \cdot uv = xu \cdot yv$ for all $x, y, u, v \in Q$;
paramedial, if $xy \cdot uv = vy \cdot ux$ for all $x, y, u, v \in Q$;
left distributive, if $x \cdot uv = xu \cdot xv$ for all $x, u, v \in Q$;
right distributive, if $xu \cdot v = xv \cdot uv$ for all $x, u, v \in Q$;
distributive, if it is left and right distributive;
idempotent, if $x \cdot x = x$ for all $x \in Q$;

In any medial quasigroup the map $s : x \mapsto xx$ is an endomorphism,
In any paramedial quasigroup the map $s : x \mapsto xx$ is an antiendomorphism.

Theorem

Any finite medial, paramedial quasigroup $(Q, \cdot)$ *has the following structure*

$$(Q, \cdot) \cong (A, \circ) \times (B, \cdot)$$

where $(A, \circ)$ *is a quasigroup with a unique idempotent element;* $(B, \cdot)$ *is isotope of a distributive medial quasigroup* $(B, \star)$ *(Murdoch, 1940, Shcherbacov, Pushkashu, 2010).*

Definition

A quasigroup $(Q, \cdot)$ is
unipotent, if there exists an element $a \in Q$ such that $x \cdot x = a$ for all $x \in Q$;
left semi-symmetric, if $x \cdot xy = y$ for all $x, y \in Q$;
TS-quasigroup, if $x \cdot xy = y, xy = yx$ for all $x, y \in Q$;
left F-quasigroup, if $x \cdot yz = xy \cdot e(x)z$ for all $x, y, z \in Q$, where $x \cdot e(x) = x$ for all x;
right F-quasigroup, if $xy \cdot z = xf(z) \cdot yz$ for all $x, y, z \in Q$, where $f(x) \cdot x = x$ for all x;
left SM-quasigroup, if $s(x) \cdot yz = xx \cdot yz = xy \cdot xz$ for all $x, y, z \in Q$, where $s(x) = x \cdot x$ for all x;
right SM-quasigroup, if $zy \cdot s(x) = zx \cdot yx$ for all $x, y, z \in Q$;
F-quasigroup, if it is left and right F-quasigroup;
left E-quasigroup, if $x \cdot yz = f(x)y \cdot xz$ for all $x, y, z \in Q$;
right E-quasigroup, if $zy \cdot x = zx \cdot ye(x)$ for all $x, y, z \in Q$;
E-quasigroup, if it is left and right E-quasigroup.