Direct Decompositions of Quasigroups and Homotopies

phd. Adrian Petrescu
associate professor
"Petru Maior" University of Tg. Mures, Romania

Proceedings of the European Integration between Tradition and Modernity
"Petru Maior" University of Târgu-Mureş
Oktober, 22-23, 2009

Abstract

In this paper we investigate direct decompositions in the category **QGR** whose objects are n-quasigroups and morphisms are quasigroup homotopies.

2000 *Mathematics Subject Classification*: 20N15, 20N05

1 Introduction

In the theory of n-quasigroups ($n \geq 2$) the role played by homotopies is as important as that played by homomorphisms. But, in many applications of n-quasigroups, isotopies and homotopies are more important than isomorphisms and homomorphisms. So, the study of homotopic properties of algebraic constructions become important.

Direct products give a means of creating n-quasigroups of huge order (applications in cryptography) than what we start with. A direct product of a family of n-quasigroups is completely determined by its factors.

The aim of the present paper is to present direct decomposition of n-quasigroups in the category **QGR** whose morphisms are quasigroup homotopies.

The second section records absolute and weak permutability of equivalence relations. Quasigroup homotopies kernels are presented in section 3. Section 4 examines direct decompositions.

To simplify the notation, we will omit the prefix n in n-quasigroup.

2 Permutability of equivalence relations

We recall two generalizations of the permutability of equivalence relations.

Let $\mathcal{S} = \{q_j \mid j \in J\}$ be a family of equivalence relations on a set A.

$\mathcal{S}$ is called **absolutely permutable** [4] if it satisfies the following condition: for any family $\{a_j \mid j \in J\}$ if $a_j \equiv a_k(\vee q_j)$ for all $j, k \in J$ there exists $a \in A$ such that $a \equiv a_j(q_j)$ for all $j \in J$.

$\mathcal{S}$ is called **weakly permutable** [1] if it satisfies the following condition: for any family $\{a_j \mid j \in J\}$ if $a_j \equiv a_k(q_j \vee q_k)$ for all $j, k \in J$ there exists $a \in A$ such that $a \equiv a_j(q_j)$ for all $j \in J$.

The concept of weak permutability is weaker than that of absolute permutability. Some useful results are:

Theorem 1. *The following are equivalent:*

(i) $\mathcal{S}$ is absolutely permutable;

(ii) $\mathcal{S}$ is weakly permutable and for any $q_j, q_k \in \mathcal{S}$, if $q_j \neq q_k$, then $q_j \vee q_k = \vee\{q_j \mid j \in J\}$.

Theorem 2. *If $\mathcal{S}$ is absolutely permutable then $q_j \circ \overline{q}_j = \vee\{q_j \mid j \in J\}$, where $\overline{q}_j = \wedge\{q_k \mid k \in J, k \neq j\}$, for all $j \in J$. If J is finite the converse is true.*

We will simplify several proofs in section 4 using the following result.

Theorem 3. *Let A and J be two sets. There exists a bijective map $f : A \to \sqcap B_j$ the cartesian product of the family $\{B_j \mid j \in J\}$ of sets if and only if there exists a family $\mathcal{S} = \{q_j \mid j \in J\}$ of equivalence relations on A such that:*

(i) $\wedge q_j = \triangle_A$;

(ii) $\vee q_j = A^2$;

(iii) $\mathcal{S}$ is absolutely permutable.

Proof. Suppose $f : A \to \sqcap B_j$. Let be $\mathcal{S} = \{q_j \mid j \in J\}$ where $q_j = \ker(p_j f)$, p_j being the j-th projection. We have $\triangle_A = \ker(f) = \wedge \ker(p_j f) = \wedge q_j$. Let $a, a' \in A$. Choose $j, k \in J$, and consider an element $b \in \sqcap B_j$ such that $p_j(b) = p_j f(a)$ and $p_k(b) = p_k f(a')$. The map f being surjective there exists $a^* \in A$ such that $b = f(a^*)$. Then $p_j f(a^*) = p_j(b) = p_j f(a)$ and $p_k f(a^*) = p_k(b) = p_k f(a')$ imply $a \equiv a^*(q_j)$ and $a^* \equiv a'(q_k)$, i.e., $a \equiv a'(q_j \circ q_k)$. In consequence $\vee q_j = A^2$. Let now $\{a_j \mid j \in J\}$ be a family of elements in A. Consider $f(a^*) = b \in \sqcap B_j$ such that $p_j(b) = p_j f(a_j)$. Then $p_j f(a^*) = p_j(b) = p_j f(a_j)$, i.e., $a^* \equiv a_j(q_j)$, $j \in J$.

Conversely, let be $\mathcal{S} = \{q_j \mid j \in J\}$ such that conditions (i)-(iii) are satisfied. Consider the map $f : A \to \sqcap A/q_j$ such that $p_j f = \text{nat} q_j : A \to A/q_j$. The map f is injective: $\ker(f) = \wedge(p_j f) = \wedge q_j = \triangle_A$. For an element $b \in \sqcap A/q_j$ let be $a_j \in A$ such that $p_j f(a_j) = p_j(b)$. Taking into account (ii) and (iii) there exists $a \in A$ such that $a \equiv a_j(q_j)$ for all $j \in J$. Hence $p_j f(a) = p_j f(a_j) = p_j(b)$, $j \in J$ imply $f(a) = b$. □

3 Normal congruent families of equivalence relations

In this section, we collect some definitions and results that will be used later. For a more detailed exposition, the reader is referred to [2] and [3].

Let $\mathcal{A} = (A, \alpha)$ and $\mathcal{B} = (B, \beta)$ be quasigroups. A **homotopy** $\varphi : \mathcal{A} \to \mathcal{B}$ is an ordered system of maps $\varphi = [f_1, \dots, f_n; f]$ from the set A to the set B such that

$$f\alpha(x_1, \dots, x_n) = \beta(f_1(x_1), \dots, f_n(x_n)) \tag{1}$$

for all $x_1, \dots, x_n \in A$.

The map f_i, $i \in \mathbb{N}_n = \{1, 2, \dots, n\}$ is known as the i-th component of φ and f-the principal component. The equality and composition of homotopies are defined componentwise.

The category **QGR** has the class of all quasigroups as its object class and its morphisms are quasigroup homotopies. Isomorphisms in **QGR** are called isotopies. They are just the homotopies having each component bijective.

The **kernel of homotopy** φ is $\ker(\varphi) = [\ker(f_1), \dots, \ker(f_n); \ker(f)]$.

A **normal congruent family of equivalences** θ on a quasigroup $\mathcal{A} = (A, \alpha)$ is an ordered system of equivalence relations on the set A, $\theta = [q_1, \dots, q_n; q]$, such that for all $a = (a_1, \dots, a_n) \in A^n$.

$$T_i^2(q_i) = q, \text{ for all } i \in \mathbb{N}_n \tag{2}$$

where $T_i : A \to A$, $T_i(x) = \alpha(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n)$ is the i-th elementary translation by a.

The kernel of homotopy $\varphi : \mathcal{A} \to \mathcal{B}$ is a normal congruent family of equivalences on $\mathcal{A}$.

We show that the converse is also true.

Let $\theta = [q_1, \dots, q_n, q]$ be a normal congruent family of equivalences on $\mathcal{A} = (A, \alpha)$. For any $a = (a_1, \dots, a_n) \in A$ $T_i^* : A/q_i \to A/q$, $T_i^*(q_i(x)) = q(T_i(x))$ is bijective for each $i \in \mathbb{N}_n$ ($q_i(x), q(x)$ – the blocks of x).

We define an n-ary operation $\overline{\alpha}$ on A/q by

$$\overline{\alpha}(q(x_1), \dots, q(x_n)) = q(\alpha(T_1^{-1}(x_1), \dots, T_n^{-1}(x_n)) \tag{3}$$

Then $(A/q, \overline{\alpha})$ is a loop having $e = \alpha(a_1, \dots, a_n)$ as a unit.

It is easy to see that $\varphi = [f_1, \dots, f_n; f] : \mathcal{A} \to (A/q, \overline{\alpha})$ defined by $f_i(x) = q(T_i(x))$, $i \in \mathbb{N}_n$ and $f(x) = q(x)$ is a homotopy and $\ker(\varphi) = \theta$.

The operation $\overline{\alpha}$ depends on a. For an another element $b = (b_1, \dots, b_n) \in A^n$ we obtain an another loop $(A/q, \beta)$. They are principal isotopic. So, the notation $\mathcal{A}/\theta = (A/q, \alpha)$ is consistent. We call $\mathcal{A}/\theta$ a **quotient quasigroup of** $\mathcal{A}$ by θ.

For an n-quasigroup $\mathcal{A}$, let $NCF(\mathcal{A})$ denote the set of normal congruent families of equivalences on $\mathcal{A}$. Define an order relation $\leq$ on $NCF(\mathcal{A})$ by setting

$$\theta_1 = [q_{11}, \dots, q_{n1}; q_1] \leq \theta_2 = [q_{12}, \dots, q_{n2}; q_2]$$

iff $q_{i1} \subseteq q_{i2}$, $i \in \mathbb{N}_n$ and $q_1 \subseteq q_2$.

If $\mathcal{S} = \{\theta_j = [q_{ij}, \dots, q_{nj}; q_j] \mid j \in J\}$ is a family of normal congruent families of equivalences on $\mathcal{A}$ then

$$\wedge\theta_j = [\wedge q_{1j}, \dots, \wedge q_{nj}; \wedge q_j]$$

and

$$\vee\theta_j = [\vee q_{1j}, \dots, \vee q_{nj}; \vee q_j]$$

are again normal congruent families of equivalences on $\mathcal{A}$. Thus $NCF(\mathcal{A})$ forms a complete lattice under $\leq$.

Now let be $\mathcal{S} = \{\theta_j \mid j \in J\} \subseteq NCF(\mathcal{A})$. Then $\mathcal{S}_i = \{q_{ij} | j \in J\}$, $i \in \mathbb{N}_n$ and $\mathcal{S}_{n+1} = \{q_j \mid j \in J\}$ are families of equivalence relations on A called **components of** $\mathcal{S}$. By (2), if one component of $\mathcal{S}$ is absolutely (weakly) permutable then all components are absolutely (weakly) permutable.

We call $\mathcal{S}$ **absolutely (weakly) permutable** if all its components are absolutely (weakly) permutable.

4 Direct decompositions in QGR

We present the homotopic properties of direct products of quasigroups.

Let $\{\mathcal{A}_j = (A_j, \alpha_j) \mid j \in J\}$ be a family of quasigroups. The direct product of this family is the quasigroup $\sqcap\mathcal{A}_j = (\sqcap A_j, \alpha)$ whose underlying set is the cartesian product $\sqcap A_j$ and operation α is defined coordinatewise. The projections $p_j : \sqcap\mathcal{A}_j \to \mathcal{A}_j$, $j \in J$, $p((a_j)_{j\in J}) = a_j$, $j \in J$ are quasigroup homomorphisms.

Theorem 4. *The category **QGR** has products.*

Proof. Let $(\sqcap\mathcal{A}_j, \{p_j \mid j \in J\})$ is a product in **QGR**. Indeed, let be $\varphi_j = [f_{1j}, \ldots, f_{nj}; f_j] : \mathcal{B} \to \mathcal{A}_j$, $j \in J$. Consider the maps $f_i, f : B \to \sqcap A_j$ defined by $p_j f_i = f_{ij}$, $i \in \mathbb{N}_n$ and $p_j f = f_j$, $j \in J$. It is easy to show that $\varphi = [f_1, \ldots, f_n; f] : \mathcal{B} \to \sqcap\mathcal{A}_j$ is the unique homotopy with $p_j f = \varphi_j$, $j \in J$. □

Let $\mathcal{A}$ be a quasigroup and let $\{\mathcal{A}_j \mid j \in J\}$ be a family of quasigroups.

Definition 1. *A decomposition of $\mathcal{A}$ as a **direct product of** $\{\mathcal{A}_j \mid j \in J\}$ is a **QGR**-isomorphism (quasigroup isotopy) $\varphi : \mathcal{A} \to \sqcap\mathcal{A}_j$. The decomposition is called **proper** if none of the homotopies $p_j\varphi$ is a **QGR**- monomorphism (a homotopy with all component injective). $\mathcal{A}$ is called **direct indecomposable** if it admits no proper direct decomposition.*

Theorem 5. *$\mathcal{A}$ has a proper direct decomposition iff there exists a family $\mathcal{S} = \{\theta_j > \triangle_A \mid j \in J\} \subseteq NCF(\mathcal{A})$ such that:*

(i) $\wedge\theta_j = \triangle_A$;

(ii) $\vee\theta_j = A^2$;

(iii) $\mathcal{S}$ is absolutely permutable.

Proof. Let $\varphi = [f_1, \ldots, f_n] : \mathcal{A} \to \sqcap\mathcal{A}_j$ be a proper direct decomposition. Put $\theta_j = \ker(p_j f)$, $j \in J$. Taking into account Theorem 3 it is easy to show that $\mathcal{S} = \{\theta_j \mid j \in J\}$ satisfies conditions (i) – (iii).

Conversely, suppose that $\mathcal{S} = \{\theta_j > \triangle_A \mid j \in J\} \subseteq NCF(\mathcal{A})$ satisfies conditions (i) – (iii). It is easy to see that all its components satisfy conditions (i) – (iii). Consider the direct product $\sqcap\mathcal{A}/\theta_j$ and the homotopy

$$\varphi = [f_1, \ldots, f_n; f] : \mathcal{A} \to \sqcap\mathcal{A}/\theta_j$$

defined by $p_j\varphi = \varphi_j$ where $\varphi_j : \mathcal{A} \to \mathcal{A}/\theta_j$ are the canonical homotopies defined in previous section.

By Theorem 3 it follows that φ is a proper direct decomposition of $\mathcal{A}$. □

By Theorem 5 and Theorem 1 we get

Theorem 6. *$\mathcal{A}$ has a proper direct decomposition iff there exists a family $\mathcal{S} = \{\theta_j > \triangle_A \mid j \in J\} \subseteq NCF(\mathcal{A})$ such that:*
(i) $\wedge\theta_j = \triangle_A$;
(ii) $\theta_j \vee \theta_k = A^2$, for any θ_j, $\theta_k \in \mathcal{S}$, $\theta_j \neq \theta_k$;
(iii) $\mathcal{S}$ is weakly permutable.

By Theorem 5 and Theorem 2 we get

Theorem 7. *(Chinese remainder theorem). $\mathcal{A}$ has a finite proper direct decomposition iff there exists a finite family $\mathcal{S} = \{\theta_j > \triangle_A \mid j \in J\} \subseteq NCF(\mathcal{A})$ such that:*
(i) $\wedge\theta_j = \triangle_A$;
(ii) $\theta_j \circ \overline{\theta}_j = A^2$, $j \in J$.

The following theorem is useful to characterize direct indecomposable quasigroups.

Theorem 8. *$\mathcal{A}$ has a proper direct decomposition iff there exists $\theta_1, \theta_2 \in NCF(\mathcal{A})$ such that:*
(i) $\theta_1, \theta_2 > \triangle_A$, $\theta_1 \neq \theta_2$;
(ii) $\theta_1 \wedge \theta_2 = \triangle_A$;
(iii) $\theta_1 \circ \theta_2 = A^2$.

Proof. Suppose that $\mathcal{A}$ has a proper direct decomposition. Let be $\mathcal{S} = \{\theta_j > \triangle_A \mid j \in J\}$ as in Theorem 5. There exists $\theta_i \in \mathcal{S}$ such that $\theta_i < A^2$. Then $\overline{\theta}_i > \triangle_A$, and $\theta_i \wedge \overline{\theta}_i = \triangle_A$. By Theorem 2, $\theta_i \circ \overline{\theta}_i = A^2$.

The converse follows by Theorem 7. □

Corollary 1. *$\mathcal{A}$ is direct indecomposable iff there is no pair $\theta_1, \theta_2 \in NCF(\mathcal{A})$, $\theta_1 \neq \theta_2$ with*
(i) $\theta_1, \theta_2 > \triangle_A$;
(ii) $\theta_1 \wedge \theta_2 = \triangle_A$;
(iii) $\theta_1 \circ \theta_2 = A^2$.

A quasigroup direct indecomposable in the subcategory **Qgr** (whose morphisms are quasigroup homomorphisms) of **QGR** can be proper decomposable in **QGR**.

Example. Let $\mathcal{A} = (A, \cdot)$ be the binary quasigroup.

	1	2	3	4	5	6	7	8
1	3	4	6	7	1	2	5	8
2	4	3	7	6	2	1	8	5
3	7	6	4	3	8	5	2	1
4	6	7	3	4	5	8	1	2
5	1	2	5	8	3	4	6	7
6	2	1	8	5	4	3	7	6
7	8	5	2	1	7	6	4	3
8	5	8	1	2	6	7	3	4

It is easy to see that only $\triangle_A$ and A^2 are normal congruences on $\mathcal{A}$. Hence $\mathcal{A}$ is direct indecomposable in Qgr. $\mathcal{A}$ is direct indecomposable in **Qgr**, but $\mathcal{A}$ has a proper direct decomposition in **QGR**: $\theta = [q_1, q_2; q]$ defined by

$$A/q_1 = \{\{1,3\},\{2,4\},\{5,7\},\{6,8\}\}$$
$$A/q_2 = \{\{1,4\},\{2,3\},\{5,8\},\{6,7\}\}$$
$$A/q = \{\{1,8\},\{2,5\},\{3,7\},\{4,6\}\}$$

and $\theta' = [q_1', q_2'; q']$ defined by

$$A/q_1' = A/q_2' = \{\{1,2,5,6\},\{3,4,7,8\}\}$$
$$A/q' = \{\{1,2,3,4\},\{5,6,7,8\}\}$$

verify conditions of Theorem 8.

References

[1] Draškovičová, H., *Permutability, distributivity of equivalence relations and direct products*, Mat. Casopis Sloven. Akad. Vied. 23 (1973), 69-87.

[2] Petrescu, A., *Normal congruent families of equivalences on n-quasigroups I*, Bull. Math. Soc. Sci. Math. Roumanie, Tome 20 (69), nr. 1-2 (1976), 173-181.

[3] Petrescu, A., *Normal congruent families of equivalences on n-quasigroups II*, Bull. Math. Soc. Sci. Math. Roumanie, Tome 21 (69), nr. 1-2 (1977), 103-111.

[4] Wenzel, G.H., *Not on a subdirect representation of universal algebras*, Acta. Math. Acad. Sci. Hungar. 18 (1967), 329-333.

Adrian Petrescu
Department of Mathematics, "Petru Maior" University Tg.Mureş
Nicolae Iorga street nr.1, 540088, Romania
e-mail: apetrescu@upm.ro