DEMONSTRATIO MATHEMATICA
Vol. XXIV No 1-2 1991

Wiesław A. Dudek

UNIPOTENT n-ARY GROUPS

In the theory of binary quasigroups, so-called unipotent quasigroups, i.e. quasigroups with the identity aa = bb, play an important role. These quasigroups are connected with some Latin squares [3]. In the theory of Latin cubes, unipotent ternary quasigruops play a similar role.

In this note we give a natural generalization of these quasigroups to the case of n-ary (n≥3) quasigroups and groups, and we prove that every unipotent n-group (i.e. every unipotent n-ary group) is derived from some its binary retract.

The termininology and notation used in this note is standard (see for example [2], [4], [6]).

We recall only that an element z of an n-group (G,f), which satisfies the equation $f(x,x,\dots,x,z) = x$, is called the skew element to x, and is denoted $z = \bar{x}$. From the definition of an n-group follows that it is uniquely determined. Moreover, one can prove (see [4]) that

$$f(x,x,\dots,\bar{x},\dots,x) = x,$$

$$f(y,x,\dots,\bar{x},\dots,x) = y$$

for every $x,y \in G$, where $\bar{x}$ can appear at any place under the sign of the function f. The skew element to $\bar{x}$ is denoted as $\bar{\bar{x}}$.

It is clear that an element x of an n-group (G,f) is an idempotent iff $x = \bar{x}$.

Let (G,f) be an n-group and let $(G,\cdot)$ be its binary retract ([6], [7]). The binary power of x in $(G,\cdot)$ is denoted by x^k. The n-ary power of this element (i.e. the power in (G,f)) is denoted by $x^{<k>}$ and is defined as follows (see [9]):

$$x^{<k>} = \begin{cases} x & \text{for } k=0, \\ f(x^{<k-1>},x,x,\dots,x) & \text{for } k>0, \\ z:\ f(z,x^{<-k-1>},x,\dots,x) = x & \text{for } k<0. \end{cases}$$

The exponential laws given below are easily verified:

$$(x^{<r>})^{<s>} = x^{<rs(n-1)+s+r>},$$

$$f(x^{<k>}, x^{<l>},\dots, x^{<s>}) = x^{<k+l+\dots+s+1>}.$$

A minimal natural number (if exists) p such that $x^{<p>} = x$ is called an n-ary order of x and is denoted by $\mathrm{ord}_n(x)$.

Definition. An n-ary quasigroup (group) G,f) is called unipotent iff

$$f(x,x,\dots,x) = f(y,y,\dots,y) \tag{1}$$

for all $x,y \in G$. If $f(x,x,\dots,x) = b$ for all $x \in G$ and some $b \in G$, then an n-group (G,f) is called b-unipotent.

Observe that in a b-unipotent n-group $x=\bar{x}$ iff $x=b$. This means that a unipotent n-group has only one idempotent.

It is well-known (see [8], [2], [6]) that for any n-group (G,f) there exist an element $b \in G$, a binary group $(G,\cdot)$ and its automorphism θ-such that

$$f(x_1^n) = x_1 \cdot \theta x_2 \cdot \theta^2 x_3 \cdot \dots \cdot \theta^{n-2} x_{n-1} \cdot \theta^{n-1} x_n \cdot b, \tag{2}$$

where $\theta b = b$ and $\theta^{n-1}x = b\cdot x\cdot b^{-1}$ for all $x \in G$.

If an n-group (G,f) is unipotent, then putting $x_1 = x_2 = \dots = x_n = e$, in (2), where e is the identity of $(G,\cdot)$, we obtain $f(e,e,\dots,e) = b$. Thus (1) implies $f(x,x,\dots,x) = b$ and, consequently,

$$x\cdot\theta x\cdot\theta^2 x\cdot \dots \cdot\theta^{n-2}x\cdot\theta^{n-1}x = e \tag{3}$$

for all $x \in G$. Moreover, from the above remarks and (3) we obtain $b^n = e$ and

$$x\cdot\theta x\cdot\theta^2 x\cdot \dots \cdot\theta^{n-2}x\cdot b\cdot x = b.$$

Applying θ to the preceding equality and using (3) we get

$x^{-1}\cdot b\cdot\theta x = b$, which gives $\theta x = b^{-1}\cdot x\cdot b$. Thus

$$f(x_1^n) = x_1\cdot b^{-1}\cdot x_2\cdot b^{-1}\cdot x_3\cdot b^{-1}\cdot \ldots \cdot b^{-1}\cdot x_{n-1}\cdot b^{-1}\cdot x_n .$$

Let $x\circ y = x\cdot b^{-1}\cdot y$. Then $(G,\circ)$ is a group with identity b. Therefore

$$f(x_1^n) = x_1\circ x_2\circ x_3\circ \ldots \circ x_{n-1}\circ x_n \tag{4}$$

and $x^n = b$ in $(G,\circ)$.

Conversely, direct computations show that if $(G,\circ)$ is a group of a finite exponent dividing n, then an n-group (G,f) defined by the formula (4) is a unipotent n-group in which $f(x,x,\ldots,x) = e$ for all $x\in G$, where e is the identity of $(G,\circ)$.

So we have the following theorem.

Theorem. An n-groupoid (G,f) is a unipotent n-group iff the groupoid $(G,\circ)$ defined by

$$x\circ y = f(x,f(z,z,\ldots,z),f(z,z,\ldots,z),\ldots,f(z,z,\ldots,z),y) ,$$

where z is an arbitrary fixed element of G, is a group of a finite exponent dividing n, and (G,f) is an n-group derived (in the sense of Dörnte) from this group $(G,\circ)$. Moreover, the constant value of $f(z,z,\ldots,z)$ is the identity of $(G,\circ)$.

Let $\bar{x}$ be the skew element to x and let $\bar{x}^{(s+1)}$ be skew to $\bar{x}^{(s)}$, where $s>0$ and $\bar{x}^{(0)} = x$. In other words: $\bar{x}^{(1)} = \bar{x}$, $\bar{x}^{(2)} = \bar{\bar{x}}$, $\bar{x}^{(3)} = \bar{\bar{\bar{x}}}$, etc.

It is easily verified that if a unipotent n-group (G,f) is derived from a group $(G,\circ)$, then $x^{<k>} = x^{1-k}$ and $\bar{x}^{(k)} = x^{2k}$ for all $x\in G$. Thus the following proposition is true.

Proposition 1. Let (G,f) be a unipotent n-group. Then:

(i) $\bar{x}^{(k)} = x^{<n-2k+1>}$,

(ii) $\bar{x}^{(n+1)} = \bar{x}$,

(iii) $x^{<n>} = x$,

(iv) $\mathrm{ord}_n(x) = \mathrm{ord}_2(x)$,

(v) if n is odd, then the operation $x \longrightarrow \bar{x}$ is one-to-one and $\bar{x}^{(t)} = x$ for $t = \frac{n+1}{2}$.

From the Hosszú theorem it follows that all n-groups defined on a given group are isotopic. In general, these n-groups are not isomorphic [2]. Moreover, an n-group isotopic to a unipotent n-group may not be unipotent. For example, the 5-group (Z_5, f) defined by the formula

$f(x_1^5) = (x_1 + 2x_2 + 4x_3 + 3x_4 + x_5) \pmod 5$ and a unipotent 5-group (Z_5, g), where $g(x_1^5) = (x_1 + x_2 + x_3 + x_4 + x_5) \pmod 5$ are isotopic. This isotopy has the form $(\varepsilon, \theta, \theta^2, \theta^3, \varepsilon, \varepsilon)$, where $\theta x = 2x \pmod 5$ and ε is the identity mapping of Z_5. Since a 5-group (Z_5, f) is idempotent, then (Z_5, f) and (Z_5, g) are not isomorphic.

Proposition 2. Unipotent n-groups are isomorphic iff are isotopic.

This fact follows immediately from the following two lemmas.

Lemma 1. Retracts of isotopic n-groups are isomorphic.

Proof. Let n-groups (G,f) and (G,g) be isotopic. Then there exist bijections $\alpha_1, \alpha_2, \ldots, \alpha_{n+1}$ of G such that

$$\alpha_{n+1} f(x_1^n) = g(\alpha_1 x_1, \alpha_2 x_2, \ldots, \alpha_n x_n).$$

Thus $\alpha_{n+1}(x \circ y) = \alpha_1 x \,\square\, \alpha_n y$ for $x \circ y = f(x,b,b,\ldots,b,y)$ and $x \square y = g(x,b_2,b_3,\ldots,b_{n-1},y)$, where $b_i = \alpha_i b$, $i=2,3,\ldots,n-1$. Hence the retract $(G,\circ) = \mathrm{ret}_{b,\ldots,b}(G,f)$ and $(G,\square) = \mathrm{ret}_{b_2,\ldots,b_{n-1}}(G,g)$ are isotopic. This completes the proof since isotopic groups are isomorphic [1] and all retracts of a given n-group are isomorphic (see [7] and [5]).

Lemma 2. Let n-groups (G,f) and (G,g) be derived (in the sense of Dörnte) from groups $(G,\circ)$ and $(G,\square)$, respectively. Then n-groups (G,f) and (G,g) are isomorphic iff are isotopic.

Proof. If n-groups (G,f) and (G,g) are isotopic, then by Lemma 1 all retracts of (G,f) and (G,g) are isomorphic. Hence

$(G,\circ)$ and $(G,\square)$ are isomorphic too. Obviously any isomorphism $\varphi\colon (G,\circ) \longrightarrow (G,\square)$ is an isomorphism of n-groups derived from $(G,\circ)$ and $(G,\square)$.

The converse is clear.

Corollary 1. Unipotent n-groups are isomorphic iff are isotopic, i.e. iff some their retracts are isomorphic.

Proposition 3. Let an n-group (G,f) be b-derived from a group $(G,\cdot)$. Then a subset H containing the identity of $(G,\cdot)$ and an element b is an n-subgroup of (G,f) iff it is a subgroup of $(G,\cdot)$.

Proof. By the assumption an n-group (G,f) has the form $f(x_1^n) = x_1\cdot x_2\cdot\ldots\cdot x_n\cdot b$, where b and the identity e of $(G,\cdot)$ are in H. If (H,f) is an n-subgroup, then $\bar{b}\in H$. Hence $\bar{b} = b^{1-n}$ and $b^{-1} = f(\bar{b},b,\ldots,b,e,e) \in H$. Thus $xy = f(x,y,e,\ldots,e,b^{-1})\in H$ for all $x,y \in H$. Moreover, for every $x\in H$ the equation $e = f(x,z,b^{-1},e,e,\ldots,e) = x\cdot z$ has a unique solution $z\in H$, which proves that H is a subgroup of $(G,\cdot)$.

Conversely, if H is a subgroup of $(G,\cdot)$, then for all $x_1,x_2,\ldots,x_n \in H$ we have $f(x_1^n) = x_1\cdot x_2\cdot\ldots\cdot x_n\cdot b \in H$. Similarly, $\bar{x} = x^{2-n}\cdot b^{-1} \in H$ for all $x\in H$. Thus (H,f) is an n-subgroup of (G,f). The proof is complete.

The proposition just proved and the Theorem imply the following

Corollary 2. Let (G,f) be a unipotent n-group derived from a group $(G,\circ)$. Then a non-empty subset H of G is an n-subgroup of (G,f) iff it is a subgroup of $(G,\circ)$.

According to [4] an n-subgroup H of n-group (G,f) is called semi-invariant iff

$$f(x,H,H,\ldots,H) = f(H,H,\ldots,H,x)$$

for all $x\in G$, and it is called invariant iff

$$f(x,H,H,\ldots,H) = f(\underbrace{H,\ldots,H}_{i-1},x,\underbrace{H,\ldots,H}_{n-i})$$

for all $x \in G$ and $i=1,2,\ldots,n$. Obviously, every invariant n-subgroup is semi-invariant.

Proposition 4. If an n-group (G,f) is b-derived from a group $(G,\cdot)$, then a subset H containing an element b and the identity of $(G,\cdot)$ is a semi-invariant n-subgroup of (G,f) iff it is an invariant subgroup of $(G,\cdot)$.

Proof. Let H contains b and the identity of $(G,\cdot)$. In view of Proposition 3 H is an n-subgroup of (G,f) iff it is a subgroup of $(G,\cdot)$.

Suppose that an n-subgroup H is semi-invariant. Since for every $y \in G$ there exists $x \in G$ such that $y = x \cdot b$,

$$y \cdot H = y \cdot b^{-1} \cdot H = x \cdot H = x \cdot H^{n-1} \cdot b = f(x,H,\ldots,H) =$$

$$= f(H,\ldots,H,x) = H^{n-1} \cdot x \cdot b = H \cdot x \cdot b = H \cdot y.$$

Thus H is an invariant subgroup of $(G,\cdot)$.

Conversely, if H an invariant subgroup of $(G,\cdot)$, then

$$f(y,H,H,\ldots,H) = y \cdot H^{n-1} \cdot b = H \cdot y \cdot H^{n-2} \cdot b = \ldots =$$

$$H^{n-1} \cdot y \cdot b = f(H,H,\ldots,H,y)$$

for all $y \in G$, which completes our proof.

Corollary 3. If an n-group (G,f) is b-derived from a group $(G,\cdot)$, then an n-subgroup H containing an element b and the identity of $(G,\cdot)$ is invariant iff it is semi-invariant.

Corollary 4. Let (G,f) be a unipotent-group derived from a group $(G,\cdot)$. Then for any subset H of G the following conditions are equivalent:

a) H is a semi-invariant n-subgroup of (G,f),

b) H is an invariant n-subgroup of (G,f),

c) H is an invariant subgroup of $(G,\cdot)$.

REFERENCES

[1] **A.A. Albert:** Quasigroups, I, Trans. Amer. Math. Soc. 54 (1943), 507-519.

[2] **V.D. Belousov:** n-ary quasigroups. (in Russian), Štinica, Kishiniev, 1972.

[3] **J. Dénes, A.D. Keedwell:** Latin squares and their applications, Akademiai Kiado, Budapest; and Academic Press, New York 1974.

[4] **W. Dörnte:** Untersuchungen über einen verallgemeinerten Gruppenbergriff, Math. Z. 29(1928), 1-19.

[5] **W.A. Dudek:** Medial n-groups and skew elements, Proceedings of the V Universal Algebra Symposium, Turawa, 3-7 May, 1988.

[6] **W.A. Dudek, J. Michalski:** On a generalization of Hosszú theorem, Demonstratio Math. 15 (1982), 783-805.

[7] **W.A. Dudek, J. Michalski:** On retracts of polyadic groups, Demonstratio Math. 17 (1984), 281-301.

[8] **M.Hosszú:** On the explicit form of n-group operations, Publ. Math. Debrecen 10 (1963), 88-92.

[9] **J. D. Monk, F. M. Sioson:** On the general theory of m-groups, Fund. Math. 72 (1971), 233-244.

[10] **E.L. Post:** Polyadic groups, Trans. Amer. Math. Soc. 48 (1940), 208-350.

INSTITUTE OF MATHEMATICS, PEDAGOGICAL UNIVERSITY,
Al. Armii Krajowej 13/15, 42-200 CZĘSTOCHOWA, POLAND

Received October 31, 1989.