Quasigroups and Related Systems **14** (2006), 123 – 132

# Anti fuzzy Lie ideals of Lie algebras

*Muhammad Akram*

## Abstract

In this paper we apply the Biswas's idea of anti fuzzy subgroups to Lie ideals of Lie algebras. We introduce the notion of anti fuzzy ideals in Lie algebras and investigate some of their properties.

## 1. Introduction

Lie algebras were discovered by Sophus Lie (1842-1899) while he was attempting to classify certain "smooth" subgroups of general linear groups. The groups he considered are now called Lie groups. He found that by taking the tangent space at the identity element of such a group, one obtained a Lie algebra. Problems about the group could be reduced to problems about the Lie algebra in which form they usually proved more tractable. There are many applications of Lie algebras, such as spectroscopy of molecules, atoms, nuclei and hadrons. Physical applications of Lie algebras include rotations and vibrations of molecules (vibron model), collective modes in nuclei (interacting boson model), the atomic shell model, the nuclear shell model, and the quark model of hadrons.

The notion of fuzzy sets was first introduced by L. A. Zadeh [12]. Fuzzy set theory has been developed in many directions by many scholars and has evoked great interest among mathematicians working in different fields of mathematics. There have been wide-ranging applications of the theory of fuzzy sets, from the design of robots and computer simulation to engineering and water resources planning. A. Rosenfeld [9] introduced the fuzzy sets in the realm of group theory. Since then many mathematicians have been involved in extending the concepts and results of abstract algebra to the

2000 Mathematics Subject Classification: 04A72, 17Bxx
Keywords: (Anti) fuzzy ideal, Lie algebra.
This research work was supported by PUCIT.

broader frame work of the fuzzy setting. Fuzzy ideals in Lie algebras have been studied in [2, 3, 7, 8, 10, 11]. In this paper we apply the Biswas's idea of anti fuzzy subgroups to Lie ideals of Lie algebras. We introduce the notion of anti fuzzy ideals in Lie algebras and investigate some of their properties.

## 2. Preliminaries

In this section we review some elementary aspects that are necessary for this paper.

**Definition 2.1.** A *Lie algebra* is a vector space $L$ over a field $F$ (equal to $\mathbf{R}$ or $\mathbf{C}$) on which $L \times L \to L \quad (x, y) \to [x, y]$ is defined satisfying the following axioms:

(L1) $[x, y]$ is bilinear,

(L2) $[x, x] = 0$ for all $x \in L$ ,

(L3) $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$ for all $x, y, z \in L$ (Jacobi identity).

In this paper by $L$ will be denoted a Lie algebra. We note that the multiplication in a Lie algebra is not associative, i.e., it is not true in general that $[[x, y], z] = [x, [y, z]]$. But it is *anti commutative*, i.e., $[x, y] = -[y, x]$.

**Definition 2.2.** Let $L_1$ and $L_2$ be Lie algebras over a field $F$. A linear transformation $f : L_1 \to L_2$ is called a *Lie homomorphism* if $f([x, y]) = [f(x), f(y)]$ for all $x,\ y \in L_1$.

**Definition 2.3.** A subspace $H$ of Lie algebra $L$ is called *Lie subalgebra* if $[x, y] \in H$ for $x, y \in H$. A subspace $I$ of $L$ is called *Lie ideal* of Lie algebra if for all $x \in I,\ y \in L$ implies $[x, y] \in I$, i.e., $[I, L] \subseteq I$.

**Definition 2.4.** A *fuzzy set* $\gamma$, i.e., a map $\gamma : L \to [0, 1]$, is called a *fuzzy Lie subalgebra* of $L$ if

(a) $\gamma(x + y) \geqslant \min\{\gamma(x), \gamma(y)\}$,

(b) $\gamma(\alpha x) \geqslant \gamma(x)$,

(c) $\gamma([x, y]) \geqslant \min\{\gamma(x), \gamma(y)\}$

hold for all $x, y \in L$ and $\alpha \in F$.

**Definition 2.5.** A fuzzy subset $\gamma : L \to [0,1]$ satisfying $(a)$, $(b)$ and

(d) $\gamma([x,y]) \geqslant \gamma(x)$

is called a *fuzzy Lie ideal* of $L$.

A fuzzy ideal of $L$ is a fuzzy subalgebra [2] such that $\gamma(-x) \geqslant \gamma(x)$ holds for all $x \in L$. According to Zadeh's extension principle the bracket $[\cdot,\cdot]$ on $L$ can be extended to the bracket $\ll \cdot,\cdot \gg$ defined on the set of all anti fuzzy sets on $L$ in the following way

$$\ll \gamma, \lambda \gg (x) = \inf\{\max\{\gamma(y), \lambda(z)\} \,|\, y, z \in L,\ [y,z] = x\},$$

where $\gamma, \lambda$ are anti fuzzy sets on $L$ and $x \in L$.

## 3. Anti fuzzy Lie ideals

**Definition 3.1.** Let $L$ be a Lie algebra. A fuzzy subset $\gamma$ of $L$ is called an *anti fuzzy Lie ideal* of $L$ if the following axioms are satisfied:

(AF1) $\gamma(x+y) \leqslant \max(\{\gamma(x), \gamma(y)\}$,

(AF2) $\gamma(\alpha x) \leqslant \gamma(x)$,

(AF3) $\gamma([x,y]) \leqslant \gamma(x)$ for all $x, y \in L$ and $\alpha \in F$.

**Example 3.2.** Let $\Re^2 = \{(x,y) : x, y \in R\}$ be the set of all 2-dimensional real vectors. Then $\Re^2$ with $[x,y] = x \times y$ is a real Lie algebra. Define a fuzzy set of $\Re^2$ by

$$\gamma(x,y) = \begin{cases} 0 & \text{if } x = y = 0, \\ 1 & \text{otherwise.} \end{cases}$$

By routine computations, we can easily check that $\gamma$ is an anti fuzzy Lie ideal of $\Re^2$.

The following lemma is obvious.

**Lemma 3.3.** *Let $\gamma$ be an anti fuzzy Lie ideal of $L$ then*

(i) $\gamma(0) \leqslant \gamma(x) \quad \forall\, x \in L$,

(ii) $\gamma([x,y]) \leqslant \min\{\gamma(x), \gamma(y)\} \ \ \forall\, x, y \in L$,

(iii) $\gamma([x,y]) = \gamma(-[y,x]) = \gamma([y,x]) \ \ \forall x, y \in L$.

**Theorem 3.4.** *Let $\gamma$ be an anti fuzzy Lie ideal in a Lie algebra $L$. Then $\gamma$ is an anti fuzzy Lie ideal of $L$ if and only if the set $L(\gamma; t) = \{x \in L | \gamma(x) \leqslant t\}$, $t \in [0, 1]$, is a Lie ideal of $L$ when it is nonempty.*

*Proof.* Assume that $\gamma$ is an anti fuzzy Lie ideal of $L$ and let $t \in [0, 1]$ be such that $L(\gamma; t) \neq \emptyset$. Let $x$, $y \in L$ be such that $x \in L(\gamma; t)$, and $y \in L(\gamma; t)$. Then $\gamma(x) \leqslant t$ and $\gamma(y) \leqslant t$. It follows that

$$\gamma(x + y) \leqslant \max\{\gamma(x), \gamma(y)\} \leqslant t,$$

$$\gamma(\alpha x) \leqslant \gamma(x) \leqslant t,$$

$$\gamma([x, y]) \leqslant \gamma(x) \leqslant t$$

so that $x + y \in L(\gamma; t)$, $\alpha x \in L(\gamma; t)$ and $[x, y] \in L(\gamma; t)$. Hence $L(\gamma; t)$ is a Lie ideal of $L$.

Conversely, suppose that $L(\gamma; t) \neq \emptyset$ is a Lie ideal of $L$ for every $t \in [0, 1]$. Assume that $\gamma(x + y) > \max\{\gamma(x), \gamma(y)\}$ for some $x, y \in L$. Taking

$$t_0 := \frac{1}{2}\{\gamma(x + y) + \max\{\gamma(x) + \gamma(y)\}\},$$

we have $\gamma(x + y) > t_0 > \max\{\gamma(x), \gamma(y)\}$. So, $x + y \notin L(\gamma; t)$, $x \in L(\gamma; t)$ and $y \in L(\gamma; t)$. This is a contradiction. Hence $\gamma(x + y) \leqslant \max\{\gamma(x), \gamma(y)\}$ for all $x, y \in L$.

Similarly we can show that $\gamma(\alpha x) \leqslant \gamma(x)$ and $\gamma([x, y]) \leqslant \gamma(x)$. This completes the proof. □

**Theorem 3.5.** *If $\gamma$ and $\rho$ are anti fuzzy Lie ideals of a Lie algebra $L$, then the function $\gamma \vee \rho : L \to [0, 1]$ defined by*

$$(\gamma \vee \rho)(x) = \max\{\gamma(x), \rho(x)\}$$

*is an anti fuzzy Lie ideal of $L$.*

*Proof.* Let $x, y \in L$ and $\alpha \in F$. Then

$$\begin{aligned}(\gamma \vee \rho)(x + y) &= \max\{\gamma(x + y), \rho(x + y)\}\\ &\leq \max\{\max\{\gamma(x), \gamma(y)\}, \max\{\rho(x), \rho(y)\}\}\\ &= \max\{\max\{\gamma(x), \rho(x)\}, \max\{\gamma(y), \rho(y)\}\}\\ &= \max\{(\gamma \vee \rho)(x), (\gamma \vee \rho)(y)\},\end{aligned}$$

$$(\gamma \vee \rho)(ax) = \max\{\gamma(ax), \rho(ax)\} \leqslant \max\{\gamma(x), \rho(x)\} = (\gamma \vee \rho)(x),$$

$$(\gamma \vee \rho)([x, y]) = \max\{\gamma([x, y]), \rho([x, y])\} \leqslant \max\{\gamma(x), \rho(x)\} = (\gamma \vee \rho)(x).$$

Hence $(\gamma \vee \rho)$ is an anti fuzzy Lie ideal of $L$. □

**Definition 3.6.** For a family of fuzzy sets $\{\gamma_i | i \in I\}$ in a Lie algebra $L$, the *union* $\bigvee \gamma_i$ of $\{\gamma_i | i \in I\}$ is defined by

$$(\bigvee \gamma_i)(x) = \sup\{\gamma_i(x) | i \in I\},$$

for each $x \in L$.

**Theorem 3.7.** *If $\{\gamma_i | i \in I\}$ is a family of anti fuzzy Lie ideals of Lie algebras $L$ then so is $\bigvee \gamma_i$.*

*Proof.* Straightforward. □

**Theorem 3.8.** *Let $f : L_1 \to L_2$ be an epimorphism of Lie algebras. If $\nu$ is an anti fuzzy Lie ideal of $L_2$ and $\gamma$ is the pre-image of $\nu$ under $f$. Then $\gamma$ is an anti fuzzy Lie ideal of $L_1$.*

*Proof.* For any $x, y \in L_1$ and $\alpha \in F$,

$$\begin{aligned}\gamma(x+y) &= \nu(f(x+y)) = \nu(f(x)+f(y))\\ &\le \max\{\nu(f(x)), \nu(f(y))\} = \max\{\gamma(x), \gamma(y)\},\\ \gamma(\alpha x) &= \nu(f(\alpha x)) = \nu(\alpha f(x)) \le \nu(f(x)) = \gamma(x),\end{aligned}$$

and

$$\gamma([x,y]) = \nu(f([x,y])) \le \nu(f(x)) = \gamma(x).$$

Hence $\gamma$ is an anti fuzzy Lie ideal of $L_1$. □

**Definition 3.9.** Let $L_1$ and $L_2$ be two Lie algebras and $f$ be a function of $L_1$ into $L_2$. If $\gamma$ is a fuzzy set in $L_2$, then the *preimage* of $\gamma$ under $f$ is the fuzzy set in $L_1$ defined by

$$f^{-1}(\gamma)(x) = \gamma(f(x)) \quad \forall x \in L_1.$$

**Theorem 3.10.** *Let $f : L_1 \to L_2$ be an onto homomorphism of Lie algebras. If $\gamma$ is an anti fuzzy Lie ideal of $L_2$, then $f^{-1}(\gamma)$ is an anti fuzzy Lie ideal of $L_1$.*

*Proof.* Let $x_1, x_2 \in L_1$ and $\alpha \in F$, then

$$\begin{aligned}f^{-1}(\gamma)(x_1+x_2) &= \gamma(f(x_1)+f(x_2)) \leqslant \max\{\gamma(f(x_1)), \gamma(f(x_2))\}\\ &= \max\{f^{-1}(\gamma)(x_1), f^{-1}(\gamma)(x_2)\},\\ f^{-1}(\gamma)(\alpha x_1) &= \gamma(f(\alpha x_1)) \leqslant \gamma(\alpha f(x_1)) = \alpha f^{-1}(\gamma)(x_1),\\ f^{-1}(\gamma)([x,y]) &= \gamma(f([x,y])) = \gamma([f(x), f(y)]) \leqslant \gamma(f(x)) = f^{-1}(\gamma)(x).\end{aligned}$$

Hence $f^{-1}(\gamma)$ is an anti fuzzy Lie ideal of $L_1$. □

**Theorem 3.11.** *Let $f : L_1 \to L_2$ be an onto homomorphism of Lie algebras. If $\gamma$ is an anti fuzzy Lie ideal of $L_2$, then $f^{-1}(\gamma^c) = (f^{-1}(\gamma))^c$.*

*Proof.* Let $\gamma$ be an anti fuzzy Lie ideal of $L_2$. Then for $x \in L_1$,

$$f^{-1}(\gamma^c)(x) = \gamma^c(f(x)) = 1 - \gamma(f(x)) = 1 - f^{-1}(\gamma^c)(x) = (f^{-1}(\gamma))^c(x).$$

That is $f^{-1}(\gamma^c) = (f^{-1}(\gamma))^c$. □

**Definition 3.12.** Let $\gamma$ be a fuzzy set in a Lie algebra $L$ and $f$ a mapping defined on $L$. Then the fuzzy set $\gamma^f$ in $f(L)$ defined by

$$\gamma^f(y) = \inf_{x \in f^{-1}(y)} \gamma(x)$$

for every $y \in f(L)$, is called the *image* of $\gamma$ under $f$. A fuzzy set $\gamma$ in $L$ has the inf *property* if for any subset $A \subseteq L$, there exists $a_0 \in A$ such that $\gamma(a_0) = \inf\limits_{a \in A} \gamma(a)$.

**Theorem 3.13.** *A Lie algebra homomorphism image of an anti fuzzy Lie ideal having the* inf *property is an anti fuzzy Lie ideal.*

*Proof.* Let $f : L_1 \to L_2$ be an epimorphism of $L_1$ onto $L_2$ and $\gamma$ be a fuzzy Lie ideal of $L_1$ with the inf property. Consider $f(x), f(y) \in f(L_1)$. Let $x_0, y_0 \in f^{-1}(f(x))$ be such that

$$\gamma(x_0) = \inf_{t \in f^{-1}(f(x))} \gamma(t) \quad \text{and} \quad \gamma(y_0) = \inf_{t \in f^{-1}(f(y))} \gamma(t)$$

respectively. Then

$$\begin{aligned} \nu(f(x) + f(y)) &= \inf_{t \in f^{-1}(f(x)+f(y))} \gamma(t) \leqslant \gamma(x_0 + y_0) \leqslant \max\{\gamma(x_0) + \gamma(y_0)\} \\ &= \max\{\inf_{t \in f^{-1}(f(x))} \gamma(t), \inf_{t \in f^{-1}(f(y))} \gamma(t)\} \\ &= \max\{\nu(f(x)) + \nu(f(y))\}, \end{aligned}$$

$$\nu(f(\alpha x)) = \inf_{t \in f^{-1}(f(\alpha x))} \gamma(t) \leqslant \gamma(x_0) \leqslant \max\{\gamma(x_0)\} = \nu(f(x)),$$

$$\begin{aligned} \nu([f(x), f(y)]) = \nu(f([x,y])) &= \inf_{t \in f^{-1}(f([x,y]))} \gamma(t) \leqslant \gamma([x_0, y_0]) \\ &\leqslant \gamma(x_0) = \nu(f(x)). \end{aligned}$$

Consequently, $\nu$ is an anti fuzzy Lie ideal of $L_2$. □

**Definition 3.14.** Let $L_1$ and $L_2$ Lie algebras and $f$ a function of $\gamma$ is a fuzzy set in $L_1$, then the *anti image* of $\gamma$ under $f$ is the fuzzy set defined by $f(\gamma)(y) =$

$$\begin{cases} \inf\{\gamma(t) \mid t \in L_1, f(t) = y\}, & \text{if } f^{-1}(y) \neq \emptyset \ , \\ 1, & \text{otherwise.} \end{cases}$$

**Definition 3.15.** Let $L_1$ and $L_2$ be any sets and let $f : L_1 \to L_2$ be any function. A fuzzy set $\gamma$ is called *$f$-invariant* if and only if for $x, y \in L_1$, $f(x) = f(y)$ implies $\gamma(x) = \gamma(y)$.

**Theorem 3.16.** *Let $f : L_1 \to L_2$ be an epimorphism of Lie algebras. Then $\gamma$ is an $f$-invariant anti fuzzy Lie ideal of $L_1$ if and only if $f(\gamma)$ is an anti fuzzy Lie ideal of $L_2$.*

*Proof.* Let $x, y \in L_2$ and $\alpha \in F$. Then there exist $a, b \in L_1$ such that $f(a) = x$ , $f(b) = y$, $x + y = f(a + b)$ and $\alpha x = \alpha f(a)$. Since $\gamma$ is $f$-invariant,

$$\begin{aligned} f(\gamma)(x + y) &= \gamma(a + b) \leqslant \max\{\gamma(a), \gamma(b)\} = \max\{f(\gamma)(x), f(\gamma)(y)\}, \\ f(\gamma)(\alpha x) &= \gamma(\alpha a) \leqslant \gamma(a) = f(\gamma)(x), \\ f(\gamma)([x, y]) &= \gamma([a, b]) = [\gamma(a), \gamma(b)] \leqslant \gamma(a) = f(\gamma)(x). \end{aligned}$$

Hence $f(\gamma)$ is an anti fuzzy Lie ideal of $L_2$.

Conversely, if $f(\gamma)$ is an anti fuzzy Lie ideal of $L_2$, then for any $x \in L_1$

$$\begin{aligned} f^{-1}(f(\gamma))(x) = f(\gamma)(f(x)) &= \inf\{\gamma(t) \mid t \in L_1, f(t) = f(x)\} \\ &= \inf\{\gamma(t) \mid t \in L_1, \gamma(t) = \gamma(x)\} = \gamma(x). \end{aligned}$$

Hence $f^{-1}(f(\gamma)) = \gamma$ is an anti fuzzy Lie ideal by Theorem 3.10. □

**Definition 3.17.** An ideal $A$ of Lie algebra $L$ is said to be *characteristic* if $f(A) = A$, for all $f \in \mathrm{Aut}(L)$, where $\mathrm{Aut}(L)$ is the set of all automorphisms of $L$. Anti fuzzy Lie ideal $\gamma$ of Lie algebra $L$ is said to be *anti fuzzy characteristic* if $\gamma^f(x) = \gamma(x)$, for all $x \in L$ and $f \in$Aut$(L)$.

**Lemma 3.18.** *Let $\gamma$ be an anti fuzzy Lie ideal of a Lie algebra $L$ and let $x \in L$. Then $\gamma(x) = s$ if and only if $x \in L(\gamma; s)$ and $x \notin L(\gamma; t)$ , for all $s > t$ .*

*Proof.* Straightforward. □

**Theorem 3.19.** *An anti fuzzy Lie ideal is characteristic if and only if each its level set is a characteristic Lie ideal.*

*Proof.* Suppose that $\gamma$ is anti fuzzy characteristic and let $s \in Im(\gamma)$, $f \in$Aut$(L)$ and $x \in L(\gamma; s)$. Then $\gamma^f(x) = \gamma(x)$ implies $\gamma(f(x)) \leqslant s$ whence $f(x) \in L(\gamma; s)$. Thus $f(L(\gamma; s)) \subseteq L(\gamma; s)$.

Let $x \in L(\gamma; s)$ and $y \in L$ such that $f(y) = x$. Then $\gamma(y) = \gamma^f(y) = \gamma(f(y)) = \gamma(x) \leqslant s$, consequently $y \in L(\gamma; s)$. So, $x = f(y) \in L(\gamma; s)$. Thus, $L(\gamma; s) \subseteq f(L(\gamma; s))$. Hence $f(L(\gamma; s)) = L(\gamma; s)$, i.e., $L(\gamma; s)$ is characteristic.

Conversely, suppose that each level Lie ideal of $\gamma$ is characteristic and let $x \in L$, $f \in Aut(L)$, $\gamma(x) = s$. Then, by virtue of Lemma 3.18, $x \in L(\gamma; s)$ and $x \notin L(\gamma; t)$ , for all $s > t$. It follows from the assumption that $f(x) \in f(L(\gamma; s)) = L(\gamma; s)$, so that $\gamma^f(x) = \gamma(f(x))) \leqslant s$. Let $t = \gamma^f(x)$ and assume that $s > t$. Then $f(x) \in L(\gamma; t) = f(L(\gamma; t))$, which implies from the injectivity of $f$ that $x \in L(\gamma; t)$, a contradiction. Hence $\gamma^f(x) = \gamma(f(x)) = s = \gamma(x)$ showing that $\gamma$ is an anti fuzzy characteristic. □

**Definition 3.20.** Let $\gamma$ be an anti fuzzy Lie ideal in $L$. Define a sequence of anti fuzzy Lie ideals in $L$ putting $\gamma^0 = \gamma$ and $\gamma^n = [\gamma^{n-1}, \gamma^{n-1}]$ for $n > 0$. If there exists a positive integer $n$ such that $\gamma^n = 0$, then an anti fuzzy Lie ideal $\gamma$ is called *solvable*.

**Theorem 3.21.** *Homomorphic image of a solvable anti fuzzy Lie ideal is a solvable anti fuzzy Lie ideal.*

*Proof.* Let $f : L_1 \to L_2$ be a homomorphism of Lie algebras. Suppose that $\gamma$ is a solvable anti fuzzy Lie ideal in $L_1$. We prove by induction on $n$ that $f(\gamma^n) \supseteq [f(\gamma)]^n$, where $n$ is any positive integer. First we claim that $f([\gamma, \gamma]) \supseteq [f(\gamma), f(\gamma)]$. Let $y \in L_2$, then

$$
\begin{aligned}
& f(\ll \gamma, \gamma \gg)(y) = \inf\{\ll \gamma, \gamma \gg (x) \mid f(x) = y\} \\
& = \inf\{\inf\{\max\{\gamma(a), \gamma(b)\} \mid a, b \in L_1, [a, b] = x, f(x) = y\}\} \\
& = \inf\{\max\{\gamma(a), \gamma(b)\} \mid a, b \in L_1, [a, b] = x, f(x) = y\} \\
& = \inf\{\max\{\gamma(a), \gamma(b)\} \mid a, b \in L_1, [f(a), f(b)] = x\} \\
& = \inf\{\max\{\gamma(a), \gamma(b)\} \mid a, b \in L_1, f(a) = u, f(b)] = v, [u, v] = y\} \\
& \leq \inf\{\max\{\inf_{a \in f^{-1}(u)} \gamma(a), \inf_{b \in f^{-1}(v)} \gamma(b)\} \mid [u, v] = y\} \\
& = \inf\{\max(f(\gamma)(u), f(\gamma)(v)) \mid [u, v] = y\} = \ll f(\gamma), f(\gamma) \gg (y).
\end{aligned}
$$

Now for $n > 1$, we get $f(\gamma^n) = f([\gamma^{n-1}, \gamma^{n-1}]) \supseteq [f(\gamma^{n-1}), f(\gamma^{n-1})] \supseteq [(f(\gamma))^{n-1}, (f(\gamma))^{n-1}] = (f(\gamma))^n$. This completes the proof. □

**Definition 3.22.** Let $\gamma$ be an anti fuzzy Lie ideal in $L$ and let $\gamma_n = [\gamma, \gamma_{n-1}]$ for $n > 0$, where $\gamma_0 = \gamma$. If there exists a positive integer $n$ such that $\gamma_n = 0$ then $\gamma$ is called *nilpotent*.

Using the same method as in the proof of Theorem 3.21, we can prove the following two theorems.

**Theorem 3.23.** *Homomorphic image of a nilpotent anti fuzzy Lie ideal is a nilpotent anti fuzzy Lie ideal.*

**Theorem 3.24.** *If $\gamma$ is a nilpotent anti fuzzy Lie ideal, then it is solvable.*

**Theorem 3.25.** *Let $I$ be a Lie ideal of a Lie algebra $L$. If $\gamma$ is an anti fuzzy Lie ideal of $L$, then the fuzzy set $\overline{\gamma}$ of $L/I$ defined by*

$$\overline{\gamma}(a+I) = \inf_{x\in I} \gamma(a+x)$$

*is an anti fuzzy Lie ideal of the quotient Lie algebra $L/I$.*

*Proof.* Clearly, $\overline{\gamma}$ is well-defined. Let $x+I,\ y+I \in L/I$, then

$$\begin{aligned}\overline{\gamma}(x+I)+(y+I)) &= \overline{\gamma}_A((x+y)+I) = \inf_{z\in I} \gamma((x+y)+z)\\ &= \inf_{z=s+t\in I} \gamma((x+y)+(s+t))\\ &\leqslant \inf_{s,\ t\in I} \max\{\gamma(x+s), \gamma(y+t)\}\\ &= \max\{\inf_{s\in I}\gamma(x+s), \inf_{t\in I}\gamma(y+t)\}\\ &= \max\{\overline{\gamma}(x+I), \overline{\gamma}(y+I)\},\end{aligned}$$

$$\overline{\gamma}(\alpha(x+I)) = \overline{\gamma}(\alpha x+I) = \inf_{z\in I}\gamma(\alpha x+z) \leqslant \inf_{z\in I}\gamma(x+z) = \overline{\gamma}(x+I),$$

$$\overline{\gamma}([x+I, y+I]) = \overline{\gamma}([x,y]+I) = \inf_{z\in I}\gamma([x,y]+z) \leqslant \inf_{z\in I}\gamma(x+z) = \overline{\gamma}(x+I).$$

Hence $\overline{\gamma}$ is an anti fuzzy Lie ideal of $L/I$. □

## References

[1] **R. Biswas:** *Fuzzy subgroups and anti fuzzy subgroups*, Fuzzy Sets and Systems **44**, (1990), 121 – 124.

[2] **B. Davvaz:** *Fuzzy Lie algebras*, Intern. J. Appl. Math. **6** (2001), 449 – 461.

[3] **B. Davvaz:** *A note on fuzzy Lie algebras*, Intern. JP J. Algebra Number Theory Appl. **2** (2002), 131 – 136.

[4] **W. A. Dudek:** *Fuzzy subquasigroups*, Quasigroups and Related Systems **5** (1998), 81 – 98.

[5] **J. E. Humphreys:** *Introduction to Lie algebras and representation theory*, Springer, New York 1972.

[6] **A. K. Katsaras and D. B. Liu:** *Fuzzy vector spaces and fuzzy topological vector spaces*, J. Math. Anal. Appl. **58** (1977), 135 – 146.

[7] **C. G. Kim and D. S. Lee:** *Fuzzy Lie ideals and fuzzy Lie subalgebras*, Fuzzy Sets and Systems **94** (1998), 101 – 107.

[8] **Q. Keyun, Q. Quanxi and C. Chaoping:** *Some properties of fuzzy Lie algebras*, J. Fuzzy Math. **9** (2001), 985 – 989.

[9] **A. Rosenfeld:** *Fuzzy groups*, J. Math. Anal. Appl. **35** (1971), 512 – 517.

[10] **S. E. Yehia:** *Fuzzy ideals and fuzzy subalgebras of Lie algebras*, Fuzzy Sets and Systems **80** (1996), 237 – 244.

[11] **S. E. Yehia:** *The adjoint representation of fuzzy Lie algebras*, Fuzzy Sets and Systems **119** (2001), 409 – 417.

[12] **L. A. Zadeh:** *Fuzzy sets*, Information Control **8** (1965), 338 – 353.

Received September 25, 2006

Punjab University College of Information Technology
University of the Punjab
Old Campus, P. O. Box 54000,
Lahore, Pakistan.
E-mail: m.akram@pucit.edu.pk

# Actions of a subgroup of the modular group on an imaginary quadratic field

*Muhammad Ashiq* and *Qaiser Mushtaq*

**Abstract**

The imaginary quadratic fields are defined by the set $\{a+b\sqrt{-n} : a,b \in Q\}$ and are denoted by $Q(\sqrt{-n})$, where $n$ is a square-free positive integer. In this paper we have proved that if $\alpha = \frac{a+\sqrt{-n}}{c} \in Q^*(\sqrt{-n}) = \{\frac{a+\sqrt{-n}}{c} : a, \frac{a^2+n}{c}, c \in Z,\ c \neq 0\}$, then $n$ does not change its value in the orbit $\alpha G$, where $G =< u,v : u^3 = v^3 = 1 >$. Also we show that the number of orbits of $Q^*(\sqrt{-n})$ under the action of $G$ are $2[d(n)+2d(n+1)-6]$ and $2[d(n)+2d(n+1)-4]$ according to $n$ is odd or even, except for $n=3$ for which there are exactly eight orbits. Also, the action of $G$ on $Q^*(\sqrt{-n})$ is always intransitive.

## 1. Introduction

It is well known [6] that the modular group $PSL(2,Z)$, where $Z$ is the ring of integers, is generated by the linear-fractional transformations $x : z \longrightarrow \frac{-1}{z}$ and $y : z \longrightarrow \frac{z-1}{z}$ and has the presentation $< x,y : x^2 = y^3 = 1 >$.

Let $v = xyx$, and $u = y$. Then $(z)v = \frac{-1}{z+1}$ and thus $u^3 = v^3 = 1$. So the group $G =< u,v >$ is a proper subgroup of the modular group $PSL(2,Z)$ [1].

The algebraic integer of the form $a+b\sqrt{n}$, where $n$ is square free, forms a quadratic field and is denoted by $Q(\sqrt{n})$. If $n > 0$, the field is a called *real quadratic field*, and if $n < 0$, it is called an *imaginary quadratic field.* The integers in $Q(\sqrt{1})$ are simply called the *integers.* The integers in $Q(\sqrt{-1})$ are called *Gaussian integers*, and the integers in $Q(\sqrt{-3})$ are called *Eisenstein integers.* The algebraic integers in an arbitrary quadratic field do not

2000 Mathematics Subject Classification: 05C25, 11E04, 20G15
Keywords: Imaginary quadratic field, linear fractional transformation, extension field, coset diagram.

necessarily have unique factorization. For example, the fields $Q(\sqrt{-5})$ and $Q(\sqrt{-6})$ are not uniquely factorable. All other quadratic fields $Q(\sqrt{n})$ with $n \leqslant 7$ are uniquely factorizable.

A number is said to be square free if its prime decomposition contains no repeated factors. All primes are therefore trivially square free.

Let $F$ be an extension field of degree two over the field $Q$ of rational numbers. Then any element $x \in F - Q$ is of degree two over $Q$ and is a primitive element of $F$. Let $F(x) = x^2 + bx + c$, where $b, c \in Q$, be the minimal polynomial of such an element $x \in F$. Then $2x = -b \pm \sqrt{b^2 - 4c}$ and so $F = Q(\sqrt{b^2 - 4c})$. Here, since $b^2 - 4c$ is a rational number $\frac{l}{m} = \frac{lm}{m^2}$ with $l, m \in Z$, we obtain $F = Q(\sqrt{lm})$ with $l, m \in Z$. In fact it is possible to write $F = Q(\sqrt{n})$ , where $n$ is a square free integer.

The imaginary quadratic fields are usually denoted by $Q(\sqrt{-n})$, where $n$ is a square free positive integer. We shall denote the subset

$$\left\{\frac{a + \sqrt{-n}}{c} : a, \frac{a^2 + n}{c}, c \in Z, c \neq 0\right\}$$

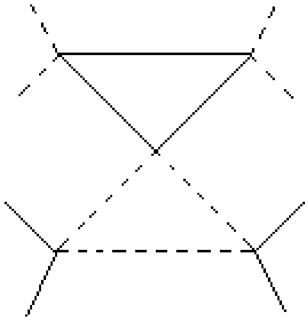
by $Q^*(\sqrt{-n})$. The imaginary quadratic fields are very useful in different branches of mathematics. For example, [3] the Bianchi groups are the groups $PSL_2(O_n)$, where $O_n$ is the ring of integers of the imaginary quadratic number field $Q(\sqrt{-n})$. Also it is known that $O_n$ is an Euclidean ring if and only if $n = 1, 2, 3, 7$ or $11$.

In [2, 4], many properties of $Q(\sqrt{n})$ have been discussed. Here we discuss some fundamental results of $G =< u, v : u^3 = v^3 = 1 >$ on $Q^*(\sqrt{-n})$.

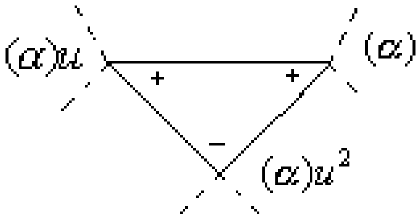
## 2. Coset diagrams

We use coset diagrams, as defined in [4] and [5], for the group $G$ and study its action on the projective line over imaginary quadratic fields. The coset diagrams for the group $G$ are defined as follows. The three cycles of the transformation $u$ are denoted by three unbroken edges of a triangle permuted anti-clockwise by $u$ and the three cycles of the transformation $v$ are denoted by three broken edges of a triangle permuted anti-clockwise by $v$. Fixed points of $u$ and $v$, if they exist, are denoted by heavy dots. This graph can be interpreted as a coset diagram with the vertices identified with the cosets of $Stab_{v_1}(G)$, the stabilizer of some vertex $v_1$ of the graph, or as 1-skeleton of the cover of the fundamental complex of the presentation which corresponds to the subgroup $Stab_{v_1}(G)$. Let $\alpha G$ denote the orbit of $\alpha$ in an action of $G$ on $Q^*(\sqrt{-n})$.

For instance, in the case of $G$ acting on the projective line over the field $Q^*(\sqrt{n})$, a fragment of a coset diagram will look as follows:

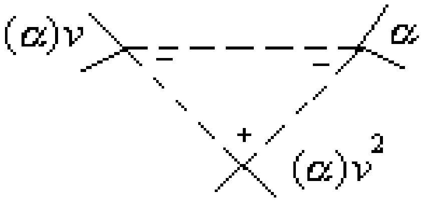


(1) If $k \neq 1, 0, \infty$ then of the vertices $k, ku, ku^2$ of a triangle, in a coset diagram for the action of $G$ on any subset of the projective line, one vertex is negative and two are positive.



(2) If $k \neq -1, 0, \infty$ then of the vertices $k, kv, kv^2$ of a triangle, in a coset diagram for the action of $G$ on any subset of the projective line, one

vertex is positive and two are negative.



**Theorem 1.** *If* $\alpha = \frac{a+\sqrt{-n}}{c} \in Q^*(\sqrt{-n})$, *then* $n$ *does not change its value in* $\alpha G$.

*Proof.* Let $\alpha = \frac{a+\sqrt{-n}}{c}$ and $b = \frac{a^2+n}{c}$. Since $(\alpha)u = \frac{\alpha-1}{\alpha} = 1 - \frac{1}{\alpha} = 1 - \frac{c}{a+\sqrt{-n}} = \frac{b-a+\sqrt{-n}}{b}$. Therefore, the new values of $a$ and $c$ for $(\alpha)u$ are $b-a$ and $b$ respectively. The new value of $b$ for $(\alpha)u$ is $\frac{(b-a)^2+n}{b} = -2a+b+c$. Now $(\alpha)v = \frac{-1}{\alpha+1} = \frac{-c}{a+c+\sqrt{-n}} = \frac{-a-c+\sqrt{-n}}{b+c+2a}$. Therefore the new values of $a$ and $c$ for $(\alpha)v$ are $-a-c$ and $2a+b+c$ respectively. The new value of $b$ for $(\alpha)v$ is $\frac{(-a-c)^2+n}{2a+b+c} = c$. Similarly, we can calculate the new values of $a, b$ and $c$ for $(\alpha)u^2, (\alpha)v^2, (\alpha)uv, (\alpha)u^2v, (\alpha)vu, (\alpha)uv^2, (\alpha)vu^2$ and $(\alpha)v^2u$ as follows:

| $\alpha$ | $a$ | $b$ | $c$ |
|---|---|---|---|
| $(\alpha)u$ | $b-a$ | $-2a+b+c$ | $b$ |
| $(\alpha)v$ | $-a-c$ | $c$ | $2a+b+c$ |
| $(\alpha)u^2$ | $c-a$ | $c$ | $-2a+b+c$ |
| $(\alpha)v^2$ | $-a-b$ | $2a+b+c$ | $b$ |
| $(\alpha)uv$ | $a-2b$ | $b$ | $-4a+4b+c$ |
| $(\alpha)u^2v$ | $3a-b-2c$ | $-2a+b+c$ | $-4a+b+4c$ |
| $(\alpha)vu$ | $a+2b$ | $4a+b+4c$ | $c$ |
| $(\alpha)v^2u$ | $3a+2b+c$ | $4a+4b+c$ | $2a+b+c$ |
| $(\alpha)uv^2$ | $3a-2b-c$ | $-4a+4b+c$ | $-2a+b+c$ |
| $(\alpha)vu^2$ | $3a+b+2c$ | $2a+b+c$ | $4a+b+4c$ |

*Table* 1

From the above information we see that all the elements of $\alpha G$ are in $Q^*(\sqrt{-n})$. That is, $n$ does not change its value in $\alpha G$. □

As we know from [5] the real quadratic irrational numbers are fixed points of the elements of $PSL(2,Z) =< x^2 = y^3 = 1 >$ except for the group theoretic conjugates of $x, y^{\pm 1}$ and $(xy)^n$. Now we want to see that when imaginary quadratic numbers are fixed points of the elements of $G$.

## 3. Existence of fixed points in $Q^*(\sqrt{-3})$

**Remark 1.** Let $(z)u = z$. Then $\frac{z-1}{z} = z$ gives $z^2 - z + 1 = 0$. Thus $z = \frac{1 \pm \sqrt{-3}}{2} \in Q^*(\sqrt{-3})$. Similarly, $(z)v = z$ implies $\frac{-1}{z+1} = z$. So, $z^2 + z + 1 = 0$ gives $z = \frac{-1 \pm \sqrt{-3}}{2} \in Q^*(\sqrt{-3})$.

**Theorem 2.** *The fixed points under the action of $G$ on $Q^*(\sqrt{-n})$ exist only if $n = 3$.*

*Proof.* Let $g$ be a linear-fractional transformation in $G$. Then, $(z)g$ can be taken as $\frac{az+b}{cz+d}$ where $ad - bc = 1$. Let $\frac{az+b}{cz+d} = z$ which yields us the quadratic equation $cz^2 + (d-a)z - b = 0$. It has the imaginary roots only if $(d-a)^2 + 4bc < 0$ or $(d+a)^2 - 4(ad-bc) < 0$ or $(a+d)^2 < 4$. That is, $a + d = 0, \pm 1$.

If $a + d = 0$ then $g$ is an involution. But there is no involution in $G$. Now, if $a + d = \pm 1$ then as $(trace(g))^2 = \det(g)$, order of $g$ will be three and hence it is conjugate to the linear fractional transformations $u^{\pm 1}$ and $v^{\pm 1}$. Since the fixed points of the linear fractional transformations $u$ and $v$ (by Remark 1) are $\frac{1 \pm \sqrt{-3}}{2}$ and $\frac{-1 \pm \sqrt{-3}}{2}$ respectively, therefore, the roots of the quadratic equation $cz^2 + (d-a)z - b = 0$ belong to the imaginary quadratic field $Q^*(\sqrt{-3})$. If two elements of $G$ are conjugate, then their corresponding determinants are also equivalent. □

## 4. Orbits of $Q^*(\sqrt{-n})$

**Definition 1.** If $\alpha = \frac{a+\sqrt{-n}}{c} \in Q^*(\sqrt{-n})$ is such that $ac < 0$ then $\alpha$ is called a *totally negative imaginary quadratic number* and *totally positive imaginary quadratic number* if $ac > 0$.

As $b = \frac{a^2+n}{c}$, therefore, $bc$ is always positive. So, $b$ and $c$ have same sign. Hence an imaginary quadratic number $\alpha = \frac{a+\sqrt{-n}}{c} \in Q^*(\sqrt{-n})$ is totally negative if either $a < 0$ and $b, c > 0$ or $a > 0$ and $b, c < 0$. Similarly $\alpha = \frac{a+\sqrt{-n}}{c} \in Q^*(\sqrt{-n})$ is totally positive if either $a, b, c > 0$ or $a, b, c < 0$.

**Theorem 3.**

(*i*) *If $\alpha$ is a totally negative imaginary quadratic number then $(\alpha)u$ and $(\alpha)u^2$ are both totally positive imaginary quadratic numbers.*

(*ii*) *If $\alpha$ is a totally positive imaginary quadratic number then $(\alpha)v$ and $(\alpha)v^2$ are both totally negative imaginary quadratic numbers.*

*Proof.* (*i*) Let $\alpha = \frac{a+\sqrt{-n}}{c}$ be a totally negative imaginary quadratic number. Here there are two possibilities: either $a < 0$ and $b, c > 0$ or $a > 0$ and $b, c < 0$.

Let $a < 0$ and $b, c > 0$. We can easily tabulate the following information.

| $\alpha$ | $a$ | $b$ | $c$ |
|---|---|---|---|
| $(\alpha)u$ | $b-a$ | $-2a+b+c$ | $b$ |
| $(\alpha)u^2$ | $c-a$ | $c$ | $-2a+b+c$ |

From the above information, we see that the new values of $a, b$ and $c$ for $(\alpha)u$ and $(\alpha)u^2$ are positive. Therefore, $(\alpha)u$ and $(\alpha)u^2$ are totally positive imaginary quadratic numbers.

Now, let $a > 0$ and $b, c < 0$. Then the new values of $a, b$ and $c$ for $(\alpha)u$ and $(\alpha)u^2$ are negative. Therefore, $(\alpha)u$ and $(\alpha)u^2$ are totally positive imaginary quadratic numbers.

(*ii*) Let $\alpha = \frac{a+\sqrt{-n}}{c}$ be a totally positive imaginary quadratic number. Here there are two possibilities: either $a, b, c > 0$ or $a, b, c < 0$.

Let $a, b, c > 0$. Then one can easily tabulate the following information.

| $\alpha$ | $a$ | $b$ | $c$ |
|---|---|---|---|
| $(\alpha)v$ | $-a-c$ | $c$ | $2a+b+c$ |
| $(\alpha)v^2$ | $-a-b$ | $2a+b+c$ | $b$ |

From the above information, we see that the new value of $a$ for $(\alpha)v$ and $(\alpha)v^2$ is negative and the new values of $b$ and $c$ for $(\alpha)v$ and $(\alpha)v^2$ are positive. Therefore, $(\alpha)v$ and $(\alpha)v^2$ are totally negative imaginary quadratic numbers.

Now, let $a, b, c < 0$. Then the new value of $a$ for $(\alpha)v$ and $(\alpha)v^2$ is positive and the new values of $b$ and $c$ for $(\alpha)v$ and $(\alpha)v^2$ are negative. Therefore, $(\alpha)v$ and $(\alpha)v^2$ are totally negative imaginary quadratic numbers. □

**Theorem 4.**

(*i*) *If $\alpha = \frac{a+\sqrt{-n}}{c}$ where $c > 0$ then the numerator of every element in $\alpha G$ is also positive.*

(*ii*) *If $\alpha = \frac{a+\sqrt{-n}}{c}$ where $c < 0$ then the numerator of every element in* *the orbit $\alpha G$ is also negative.*

*Proof.* $(i)$ Since $\alpha = \frac{a+\sqrt{-n}}{c}$ with $c > 0$, therefore, $b$ is also positive. As $b$ and $c$ always have the same sign. Using this fact we can easily see from the information given in Table 1 that every element in $\alpha G$ has positive numerator.

$(ii)$ Since $\alpha = \frac{a+\sqrt{-n}}{c}$ with $c < 0$, therefore, $b$ is also negative. As $b$ and $c$ always have the same sign. Using this fact we can easily see from the information given in Table 2 that every element in $\alpha G$ has negative numerator. □

For $\alpha = \frac{a+\sqrt{-n}}{c} \in Q^*(\sqrt{-n})$, we define $\|\alpha\| = |a|$.

**Theorem 5.**

$(i)$ *Let $\alpha$ be a totally negative imaginary quadratic number. Then* $\|(\alpha)u\| > \|\alpha\|$ *and* $\left\|(\alpha)u^2\right\| > \|\alpha\|$, *and*

$(ii)$ *Let $\alpha$ be a totally positive imaginary quadratic number. Then* $\|(\alpha)v\| > \|\alpha\|$ *and* $\left\|(\alpha)v^2\right\| > \|\alpha\|$.

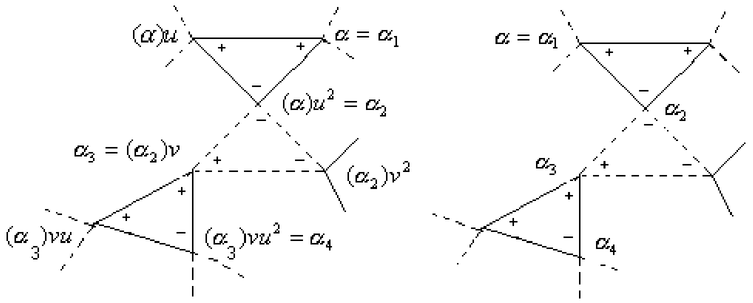
*Proof.* $(i)$ Let $\alpha$ be a totally negative imaginary quadratic number. Then either, $a < 0$ and $b, c > 0$ or $a > 0$ and $b, c < 0$. Let us take $a < 0$ and $b, c > 0$. Then, by Theorem 3$(i)$ $(\alpha)u$ and $(\alpha)u^2$ both are totally positive imaginary quadratic numbers. Thus, $\|(\alpha)u\| = |b-a| > |a| = \|\alpha\|$, and $\left\|(\alpha)u^2\right\| = |c-a| >= |a| = \|\alpha\|$. Similarly, we have the same result for $a > 0$ and $b, c < 0$.

$(ii)$ Let $\alpha$ be a totally positive imaginary quadratic number. Then either, $a$, $b$, $c > 0$ or $a$, $b$, $c < 0$. Let us take $a, b, c > 0$. Now, using the information given in Table 1, we can easily see that $\|(\alpha)v\| = |-a-c| = |a+c| > |a| = \|\alpha\|$ and $\left\|(\alpha)v^2\right\| = |-a-b| = |a+b| > |a| = \|\alpha\|$. Similarly, we have the same result for $a, b, c < 0$. □

**Theorem 6.** *Let $\alpha$ be a totally positive or negative imaginary quadratic number. Then there exists a sequence $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ such that $\alpha_i$ is alternately totally negative and totally positive number for $i = 1, 2, 3, \ldots, m-1$ and $\|\alpha_m\| = 0$ or 1.*

*Proof.* Let $\alpha = \alpha_1$ be a totally positive imaginary quadratic number. Then, by Theorem 3$(i)$, $(\alpha)u$ or $(\alpha)u^2$ is a totally negative imaginary quadratic number. If $(\alpha)u$ is a totally negative imaginary quadratic number, then put $\alpha_2 = (\alpha)u$ and by Theorem 5$(i)$, $\|(\alpha_1)\| > \|\alpha_2\|$. Now if $(\alpha)u^2$ is a totally negative imaginary quadratic number, then put $\alpha_2 = (\alpha)u^2$. In this case we have also $\|(\alpha_1)\| > \|\alpha_2\|$.

Now if $(\alpha)u$ a is totally negative imaginary quadratic number, then $(\alpha)uv$ or $(\alpha)uv^2$ is a totally positive imaginary quadratic number. If $(\alpha)uv$ is a totally positive imaginary quadratic number, put $(\alpha)uv = \alpha_3$ and so by Theorem 5$(ii)$ $\|(\alpha)uv\| < \|(\alpha)u\| < \|\alpha\|$ or $\|\alpha_3\| < \|\alpha_2\| < \|\alpha_1\|$ and continuing in this way we obtain an alternate sequence $\alpha_1, \alpha_2, \ldots, \alpha_m$ of totally positive and totally negative numbers such that $\|\alpha_1\| > \|\alpha_2\| > \|\alpha_3\| > \ldots > \|\alpha_m\|$. Since $\|\alpha_1\|, \|\alpha_2\|, \|\alpha_3\|, \ldots, \|\alpha_m\|$ is a decreasing sequence of non negative integers, therefore, it must terminate and that happens only when ultimately we reach at an imaginary quadratic number $\alpha_m = \frac{a\prime+\sqrt{-n}}{c}$ such that $\|\alpha_m\| = |a'| = 0$ or 1. It can be shown diagrammatically as:



□

**Theorem 7.** *There are exactly eight orbits of $Q^*(\sqrt{-n})$ under the action of the group $G$ when $n = 3$.*

*Proof.* As we have seen in Theorem 6, we get a decreasing sequence of non negative integers $\|\alpha_1\|, \|\alpha_2\|, \|\alpha_3\|, \ldots, \|\alpha_m\|$ such that $\|\alpha_1\| > \|\alpha_2\| > \|\alpha_3\| > \ldots > \|\alpha_m\|$ which must terminate and that happens only when ultimately we reach at an imaginary quadratic number $\alpha_m = \frac{a\prime+\sqrt{-3}}{c}$ such that $\|\alpha_m\| = |a'| = 0$ or 1.

If $\alpha_m = \frac{1\pm\sqrt{-3}}{2}$ or $\frac{-1\pm\sqrt{-3}}{2}$ then because $\frac{\pm1\pm\sqrt{-3}}{2}$ are the fixed points of $u$ and $v$, therefore, we cannot reach at an imaginary quadratic number whose norm is equal to zero. So in this case there are four orbits, namely $\frac{1+\sqrt{-3}}{2}G$, $\frac{1-\sqrt{-3}}{2}G$, $\frac{-1+\sqrt{-3}}{2}G$ and $\frac{-1-\sqrt{-3}}{2}G$ of $Q^*(\sqrt{-3})$.

Now, if we reach at an imaginary quadratic number $\alpha_m = \frac{a\prime+\sqrt{-3}}{c}$ such that $\|\alpha_m\| = |a\prime| = 0$ then $\alpha_m = \frac{\sqrt{-3}}{c}$. Since $\alpha_m = \frac{\sqrt{-3}}{c} \in Q^*(\sqrt{-3})$, therefore, $c = \pm1, \pm3$. That is, $\alpha_m = \frac{\sqrt{-3}}{1}, \frac{\sqrt{-3}}{3}, \frac{\sqrt{-3}}{-1}$, and $\frac{\sqrt{-3}}{-3}$.

Now, if $\alpha = \frac{\sqrt{-3}}{1}$, we can easily calculate the new values of $a$, $b$, and $c$ as:

| $\alpha$ | $0$ | $3$ | $1$ |
|---|---|---|---|
| $(\alpha)u$ | $3$ | $4$ | $3$ |
| $(\alpha)v$ | $-1$ | $1$ | $4$ |
| $(\alpha)u^2$ | $1$ | $1$ | $4$ |
| $(\alpha)v^2$ | $-3$ | $4$ | $3$ |

Hence from the above table, we see that $\sqrt{-3}$, $\frac{1+\sqrt{-3}}{4}$ and $\frac{-1+\sqrt{-3}}{4}$ lie in $\alpha G$.

Similarly, if $\alpha = \frac{\sqrt{-3}}{-1}$, then $-\sqrt{-3}$, $\frac{-1+\sqrt{-3}}{-4}$ and $\frac{1+\sqrt{-3}}{-4}$ lie in $\alpha G$, if $\alpha = \frac{\sqrt{-3}}{3}$, then $\frac{\sqrt{-3}}{3}$, $\frac{1+\sqrt{-3}}{1}$ and $\frac{-1+\sqrt{-3}}{1}$ lie in $\alpha G$, and if $\alpha = \frac{\sqrt{-3}}{-3}$, then $\frac{\sqrt{-3}}{-3}$, $\frac{1+\sqrt{-3}}{-1}$ and $\frac{-1+\sqrt{-3}}{-1}$ lie in $\alpha G$.

Thus, $\frac{\sqrt{-3}}{1}$, $\frac{\sqrt{-3}}{-1}$, $\frac{\sqrt{-3}}{3}$, and $\frac{\sqrt{-3}}{-3}$ lie in four different orbits. Hence there are exactly eight orbits of $Q^*(\sqrt{-n})$ for $n = 3$. □

**Remark 2.**

1. If $\alpha = \frac{a+\sqrt{-n}}{c} \in Q^*(\sqrt{-n})$ then $Stab_\alpha(G)$ is non-trivial only if $n = 3$. Particularly, if $\alpha = \frac{\pm 1 \pm \sqrt{-3}}{2}$ then $Stab_\alpha(G) \cong C_3$.
2. In $Q^*(\sqrt{-3})$, there are four elements of norm zero, namely $\frac{\sqrt{-3}}{1}$, $\frac{\sqrt{-3}}{-1}$, $\frac{\sqrt{-3}}{3}$, and $\frac{\sqrt{-3}}{-3}$.
3. In $Q^*(\sqrt{-3})$, there are twelve elements of norm one, namely $\frac{\pm 1 \pm \sqrt{-3}}{2}$, $\frac{\pm 1 \pm \sqrt{-3}}{4}$, and $\frac{\pm 1 \pm \sqrt{-3}}{1}$.

**Theorem 8.** *Let $\alpha \in Q^*(\sqrt{-n})$, where $n \neq 3$. Then*

*$(i)$ if $\alpha = \sqrt{-n}$, then $\sqrt{-n}$, $\frac{1+\sqrt{-n}}{n+1}$ and $\frac{-1+\sqrt{-n}}{n+1}$ lie in $\alpha G$,*

*$(ii)$ if $\alpha = \frac{\sqrt{-n}}{n}$, then $\frac{\sqrt{-n}}{n}$, $\frac{1+\sqrt{-n}}{1}$ and $\frac{-1+\sqrt{-n}}{1}$ lie in $\alpha G$,*

*$(iii)$ if $\alpha = \frac{\sqrt{-n}}{2}$, where $n$ is even and $l_1 = \frac{n}{2}$, then $\alpha$ is the only element of norm zero in $\alpha G$,*

*$(iv)$ if $\alpha = \frac{\sqrt{-n}}{n_1}$, where $k_1 = \frac{n}{n_1}$ and $n_1 \neq 1$, $2$ or $n$, then $\alpha$ is the only element of norm zero in $\alpha G$, and*

*$(v)$ if $\alpha = \frac{1+\sqrt{-n}}{c_1}$, where $1 + n = c_1 c_2$ and $c_1 \neq 1$ or $n+1$, then $\alpha$ is the only element of norm one in $\alpha G$.*

*Proof.* $(i)$ If $\alpha = \sqrt{-n}$, then, we can easily tabulate the following information.

| $\alpha$ | $0$ | $n$ | $1$ |
|---|---|---|---|
| $(\alpha)u$ | $n$ | $n+1$ | $n$ |
| $(\alpha)v$ | $-1$ | $1$ | $n+1$ |
| $(\alpha)u^2$ | $1$ | $1$ | $n+1$ |
| $(\alpha)v^2$ | $-n$ | $n+1$ | $n$ |

Hence from the above table, we see that $\sqrt{-n}$, $\frac{1+\sqrt{-n}}{n+1}$ and $\frac{-1+\sqrt{-n}}{n+1}$ lie in $\alpha G$.

$(ii)$ If $\alpha = \frac{\sqrt{-n}}{n}$, then we can calculate the new values of $a$, $b$, and $c$ as:

| $\alpha$ | $0$ | $1$ | $n$ |
|---|---|---|---|
| $(\alpha)u$ | $1$ | $n+1$ | $1$ |
| $(\alpha)v$ | $-n$ | $n$ | $n+1$ |
| $(\alpha)u^2$ | $n$ | $n$ | $n+1$ |
| $(\alpha)v^2$ | $-1$ | $n+1$ | $1$ |

Hence from the above table, we see that $\frac{\sqrt{-n}}{n}$, $\frac{1+\sqrt{-n}}{1}$ and $\frac{-1+\sqrt{-n}}{1}$ lie in $\alpha G$.

$(iii)$ If $\alpha = \frac{\sqrt{-n}}{2}$, then we can calculate the new values of $a$, $b$, and $c$ as:

| $\alpha$ | $0$ | $l_1$ | $2$ |
|---|---|---|---|
| $(\alpha)u$ | $l_1$ | $l_1+2$ | $l_1$ |
| $(\alpha)v$ | $-2$ | $2$ | $l_1+2$ |
| $(\alpha)u^2$ | $2$ | $2$ | $l_1+2$ |
| $(\alpha)v^2$ | $-l_1$ | $l_1+2$ | $l_1$ |

Hence from the above table, we see that $\alpha$ is the only element of norm zero in $\alpha G$.

$(iv)$ Let $\alpha = \frac{\sqrt{-n}}{n_1}$, where $k_1 = \frac{n}{n_1}$ and $n_1 \neq 1$ or $n$, then

| $\alpha$ | $0$ | $k_1$ | $n_1$ |
|---|---|---|---|
| $(\alpha)u$ | $k_1$ | $n_1+k_1$ | $k_1$ |
| $(\alpha)v$ | $-n_1$ | $n_1$ | $n_1+k_1$ |
| $(\alpha)u^2$ | $n_1$ | $n_1$ | $n_1+k_1$ |
| $(\alpha)v^2$ | $-k_1$ | $n_1+k_1$ | $k_1$ |

Hence from the above table, we see that $\alpha$ is the only element of norm zero in $\alpha G$.

$(v)$ Let $\alpha = \frac{1+\sqrt{-n}}{c_1}$, where $1+n = c_1c_2$ and $c_1 \neq 1$ or $n+1$, then the new values of $a$, $b$, and $c$ can be calculated as:

| $\alpha$ | $1$ | $c_2$ | $c_1$ |
|---|---|---|---|
| $(\alpha)u$ | $c_2-1$ | $-2+c_1+c_2$ | $c_2$ |
| $(\alpha)v$ | $-1-c_1$ | $c_1$ | $2+c_1+c_2$ |
| $(\alpha)u^2$ | $c_1-1$ | $c_1$ | $-2+c_1+c_2$ |
| $(\alpha)v^2$ | $-1-c_2$ | $2+c_1+c_2$ | $c_2$ |

If $c_1=2$, then $\|(\alpha)u^2\|=1$ implies that $(\alpha)u^2=\frac{1+\sqrt{-n}}{c_2}$. If $c_1=-2$, then $\|(\alpha)v\|=1$ implies that $(\alpha)v=\frac{1+\sqrt{-n}}{c_2}$. That is, $\frac{1+\sqrt{-n}}{2}$ and $\frac{1+\sqrt{-n}}{(\frac{n+1}{2})}$ lie in the same orbit, and $\frac{1+\sqrt{-n}}{-2}$ and $\frac{1+\sqrt{-n}}{-(\frac{n+1}{2})}$ lie in the same orbit.

Now if $c_1\neq 1,2$ or $\frac{n+1}{2},n+1$, that is, $c_2\neq n+1,\frac{n+1}{2}$ or 1, then $\frac{1+\sqrt{-n}}{c_1}$ lie in $\alpha G$. □

**Example 1.** By using Theorem 8, the orbits of $Q^*(\sqrt{-14})$ are:

$(i)$ $\sqrt{-14}$, $\frac{1+\sqrt{-14}}{15}$ and $\frac{-1+\sqrt{-14}}{15}$ lie in $\sqrt{-14}G$,

$(ii)$ $\frac{\sqrt{-14}}{-1}$, $\frac{1+\sqrt{-14}}{-15}$ and $\frac{-1+\sqrt{-14}}{-15}$ lie in $\frac{\sqrt{-14}}{-1}G$,

$(iii)$ $\frac{\sqrt{-14}}{14}$, $\frac{1+\sqrt{-14}}{1}$ and $\frac{-1+\sqrt{-14}}{1}$ lie in $\frac{\sqrt{-14}}{14}G$,

$(iv)$ $\frac{\sqrt{-14}}{-14}$, $\frac{1+\sqrt{-14}}{-1}$ and $\frac{-1+\sqrt{-14}}{-1}$ lie in $\frac{\sqrt{-14}}{-14}G$,

$(v)$ $\frac{\sqrt{-14}}{2}$ lies in $\frac{\sqrt{-14}}{2}G$,

$(vi)$ $\frac{\sqrt{-14}}{-2}$ lies in $\frac{\sqrt{-14}}{-2}G$,

$(vii)$ $\frac{\sqrt{-14}}{7}$ lies in $\frac{\sqrt{-14}}{7}G$,

$(viii)$ $\frac{\sqrt{-14}}{-7}$ lies in $\frac{\sqrt{-14}}{-7}G$,

$(ix)$ $\frac{1+\sqrt{-14}}{3}$ lies in $\frac{1+\sqrt{-14}}{3}G$,

$(x)$ $\frac{-1+\sqrt{-14}}{3}$ lies in $\frac{-1+\sqrt{-14}}{3}G$,

$(xi)$ $\frac{1+\sqrt{-14}}{-3}$ lies in $\frac{1+\sqrt{-14}}{-3}G$,

$(xii)$ $\frac{-1+\sqrt{-14}}{-3}$ lies in $\frac{-1+\sqrt{-14}}{-3}G$,

$(xiii)$ $\frac{1+\sqrt{-14}}{5}$ lies in $\frac{1+\sqrt{-14}}{5}G$, .

$(xiv)$ $\frac{-1+\sqrt{-14}}{5}$ lies in $\frac{-1+\sqrt{-14}}{5}G$,

$(xv)$ $\frac{1+\sqrt{-14}}{-5}$ lies in $\frac{1+\sqrt{-14}}{-5}G$, and

$(xvi)$ $\frac{-1+\sqrt{-14}}{-5}$ lies in $\frac{-1+\sqrt{-14}}{-5}G$.

So, there are sixteen orbits of $Q^*(\sqrt{-n})$.

**Remark 3.**

1. If $\alpha=\frac{a+\sqrt{-n}}{c}\in Q^*(\sqrt{-n})$, then $\alpha G$ contains the conjugates of the ele-

ments of $\alpha G$. Since $\alpha = \frac{a+\sqrt{-n}}{c}$ and $\overline{\alpha} = \frac{a-\sqrt{-n}}{c}$ lie in two different orbits, therefore, $\alpha G$ and $\overline{\alpha}G$ are always disjoint.

2. The elements of norm zero and one in $Q^*(\sqrt{-n})$, play a vital role to identify the orbits of $Q^*(\sqrt{-n})$.

**Definition 2.** If $n$ is a positive integer then $d(n)$ denotes the arithmetic function defined by the number of positive divisors of $n$.

For example, $d(1) = 1, d(2) = 2, d(3) = 2, d(4) = 3, d(5) = 2$ and $d(6) = 4$.

**Theorem 9.** *If $n \neq 3$, then the total number of orbits of $Q^*(\sqrt{-n})$ under the action of $G$ are:*

(*i*) $2\,[d(n) + 2d(n+1) - 6]$ *if $n$ is odd, and*

(*ii*) $2\,[d(n) + 2d(n+1) - 4]$ *if $n$ is even.*

*Proof.* First suppose that $n$ is odd, that is $n+1$ is even. Let the divisors of $n$ are $\pm 1$, $\pm n_1$, $\pm n_2$, $\pm, \ldots, \pm n$ and the divisors of $n+1$ are $\pm 1$, $\pm 2$, $\pm m_1$, $\pm m_2$, $\pm, \ldots, \pm \frac{(n+1)}{2}$, $\pm(n+1)$. Then by Theorem 8($i$), there exist two orbits of $Q^*(\sqrt{-n})$ corresponding to the divisors $\pm 1$ of $n$ and $\pm(n+1)$ of $n+1$. By Theorem 8($ii$), there exist two orbits of $Q^*(\sqrt{-n})$ corresponding to the divisors $\pm n$ of $n$ and $\pm 1$ of $n+1$. By Theorem 8($v$), there exists four orbits of $Q^*(\sqrt{-n})$ corresponding to the divisors $\pm 2$, $\pm(\frac{n+1}{2})$ of $n+1$. Now we are left with $2d(n) - 4$ and $4d(n+1) - 16$. Thus total orbits are $2d(n)-4+4d(n+1)-16+8 = 2d(n)+4d(n+1)-12 = 2[d(n)+2d(n+1)-6]$.

Now if $n$ is even, then the total orbits are $[2d(n)-4]+[4d(n+1)-8]+4 = 2d(n) + 4d(n+1) - 8 = 2[d(n) + 2d(n+1) - 4]$. □

**Example 2.** Now, by using Theorem 9,

(*i*) the orbits of $Q^*(\sqrt{-14})$ are:

$2[d(n) + 2d(n+1) - 4] = 2[d(14) + 2d(15) - 4] = 2[4 + 8 - 4] = 16$,

and

(*ii*) the orbits of $Q^*(\sqrt{-15})$ are:

$2[d(n) + 2d(n+1) - 6] = 2[d(15) + 2d(16) - 6] = 2[4 + 10 - 6] = 16$.

**Theorem 10.** *There are $2d(n)$ elements of $Q^*(\sqrt{-n})$ of norm zero under the action of $G$.*

*Proof.* As we have seen in Theorem 6, we get a decreasing sequence of non-negative integers $\|\alpha_1\|, \|\alpha_2\|, \|\alpha_3\|, \ldots, \|\alpha_m\|$ such that $\|\alpha_1\| > \|\alpha_2\| > \|\alpha_3\| > \ldots > \|\alpha_m\|$ which must terminate and that happens only when ultimately we reach at an imaginary quadratic number $\alpha_m = \frac{a\prime + \sqrt{-n}}{c}$ such that $\|\alpha_m\| = |a\prime| = 0$. Thus $\alpha_m = \frac{\sqrt{-n}}{c}$. Since $\alpha_m = \frac{\sqrt{-n}}{c} \in Q^*(\sqrt{-n})$, therefore, $c$ must be a divisor of $n$. Hence there are $2d(n)$ elements of $Q^*(\sqrt{-n})$ of norm zero under the action of $G$. □

**Theorem 11.** *There are* $4d(n+1)$ *elements of* $Q^*(\sqrt{-n})$ *of norm one under the action of* $G$.

*Proof.* As we have seen in Theorem 6, there exists a decreasing sequence of non-negative integers $\|\alpha_1\|, \|\alpha_2\|, \|\alpha_3\|, \ldots, \|\alpha_m\|$ such that $\|\alpha_1\| > \|\alpha_2\| > \|\alpha_3\| > \ldots > \|\alpha_m\|$ which must terminate and that happens only when ultimately we reach at an imaginary quadratic number $\alpha_m = \frac{a\prime + \sqrt{-n}}{c}$ such that $\|\alpha_m\| = |a\prime| = 1$. Then $\alpha_m = \frac{\pm 1 + \sqrt{-n}}{c}$, where $b = \frac{a^2+n}{c} = \frac{1+n}{c}$, that is, $c$ must be a divisor of $n+1$. Hence there are $4d(n+1)$ elements of $Q^*(\sqrt{-n})$ of norm one under the action of $G$. □

**Corollary.** *The action of* $G$ *on* $Q^*(\sqrt{-n})$ *is intransitive.*

*Proof.* If $n$ is even, then the minimum value of $n$ in $Q^*(\sqrt{-n})$ is two. So, by Theorem 9, the total number of orbits are $2[d(n) + 2d(n+1) - 4] = 2[2 + 2(2) - 4] = 4$. So, the action of $G$ on $Q^*(\sqrt{-n})$ must be intransitive.

Now, if $n$ is odd, then the minimum value of $n$ in $Q^*(\sqrt{-n})$ is five, when $n \neq 3$. So, by Theorem 10, the total number of orbits are $2[d(n) + 2d(n+1) - 6] = 2[2+2(4)-6] = 8$. So, the action of $G$ on $Q^*(\sqrt{-n})$ is intransitive.

According to Theorem 7, there are exactly eight orbits of $Q^*(\sqrt{-n})$ when $n = 3$ under the action of the group $G$. Hence the proof. □

## References

[1] **M. Ashiq and Q. Mushtaq:** *Finite presentation of a linear-fractional group*, Algebra Colloquium **12** (2005), 585 – 589.

[2] **M. Aslam, Q. Mustaq, T. Maqsood and M. Ashiq:** *Real quadratic irrational numbers and the group* $< x, y : x^2 = y^6 = 1 >$, Southeast Asian Bull. Math. **27** (2003), 409 – 415.

[3] **A. W. Mason:** *Free quotients of subgroups of the Bianchi groups whose kernels contain many elementary matrices*, Math. Proc. Camb. Phil. Soc. **116** (1994), 253 – 273.

[4] **Q. Mushtaq:** *Modular group acting on real quadratic fields*, Bull. Austral. Math. Soc. **37** (1988), 303 – 306.

[5] **Q. Mushtaq:** *On word structure of the modular group over finite and real quadratic fields*, Disc. Math. **178** (1998), 155 – 164.

[6] **W. W. Stothers:** *Subgroups of the modular group*, Proc. Camb. Philos. Soc. **75** (1974), 139 – 154.

Received February 14, 2006

M. Ashiq
Department of Basic Sciences & Humanities, College of E & ME, National University of Sciences and Technology, Rawalpindi, Pakistan,
E-mail: ashiqjaved@yahoo.co.uk

Q. Mushtaq
Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
E-mail: qmushtaq@isb.apollo.net.pk

Quasigroups and Related Systems **14** (2006), 147 – 155

# On primal ideals over semigroups

*Shahabaddin Ebrahimi Atani and Ahmad Yousefian Darani*

### Abstract

Let $S$ be a commutative cancellation torsion-free additive semigroup with identity 0 and let $S \neq \{0\}$. This paper is devoted to study some properties of primal ideals and quasi-primary ideals of the semigroup $S$. First, a number of results concerning of these ideals are given. Second, we characterize primal ideals and quasi-primary ideals of a Prüfer semigroup and show that in such semigroup, the three concepts: primary, quasi-primary, and primal coincide.

## 1. Introduction

Throughout this paper $S$ will be a commutative cancellation torsion-free additive semigroup with identity 0 and let $S \neq \{0\}$. We will study the structure of primal ideals and quasi-primary ideals of $S$. Our interest is motivated by the work [2].

Fuchs in [1] introduced the concept of a primal ideal, where a proper ideal $I$ of $S$ is said to be primal if the elements of $S$ which are not prime to $I$ form an ideal (see section 3). Fuchs and Mosteig proved in [2] that in a Prüfer domain of finite character every non-zero ideal is the intersection of a finite number of primal ideals, and moreover, the $P$-primal ideals form a semigroup under ideal multiplication. A similar result is established for decomposition into the intersection (even into the products) of quasi-primary ideals. The purpose of this paper is to explore some basic facts of these class of ideals of a semigroup. In the second section we characterize the semigroups in which every ideal is prime and prove that a semigroup is a group if and only if every its proper ideal is prime. We show also that every ideal over a Prüfer semigroup is quasi-primary and characterize primal

2000 Mathematics Subject Classification: 13A02, 13F05, 20M14
Keywords: Prüfer semigroup, oversemigroup, primal, quasi-primary ideal.

ideals of a Prüfer semigroup. Connection between the primal ideals, the quasi-primary and the primary ideals of such semigroups are studied too.

Before we state some results let us introduce some notation and terminologies. Let $S$ be a semigroup. Then $G = \{a-b : a, b \in S\}$ is a torsion-free ablian group with respect to the addition and $S$ is a subsemigroup of $G$. $G$ is called the *quotient group* of $S$. Any semigroup $T$ between $S$ and $G$ is called an *oversemigroup* of $S$ (see [3]).

By an *ideal* of $S$ we mean a non-empty subset $I$ of $S$ such that for all $a \in I$ and for all $b \in S$ we have $a + b \in I$, that is, $I + S = I$. Thus for $x \in S$, $x + S = \{x + y : y \in S\}$ is the principal ideal generated by $x$. If $I, J$ are ideals of $S$, then $I + J = (I + S) + (J + S) = (I + J) + S$ is an ideal of $S$ too. For $a \in S$ and an ideal $I$ of $S$, by $a + I$, we mean the sum $a + I = (a + S) + (I + S)$, which is an ideal of $S$. A proper ideal $I$ of a semigroup $S$ is called *maximal* if there does not exist an ideal $J$ of $S$ with $I \subset J \subset S$, where $\subset$ denotes the strict inclusion. An element $a \in S$ is called a *unit* if $a + b = 0$ for some $b \in S$. If $U(S)$ is the set of units in $S$ and $0 \in U(S)$, then $U(S)$ is a subgroup of $G$ and $M = S - U(S) \neq \emptyset$ is a maximal ideal of $S$. A *prime ideal* in a semigroup $S$ is any proper ideal $P$ of $S$ such that for $a, b \in S$ $a + b \in P$ implies either $a \in P$ or $b \in P$. The maximal ideal is a prime ideal (see [3]).

Let $I$ be an ideal of $S$. The set

$$\operatorname{rad}(I) = \{a \in S : na \in I \text{ for some positive integer } n\}$$

is an ideal of $S$. It is called the *radical* of $I$. A proper ideal $I$ of $S$ is *primary* if for $a, b \in S$ $a + b \in I$ implies either $a \in I$ or $b \in \operatorname{rad}(I)$. If $I$ is primary, then $P = \operatorname{rad}(I)$ is a prime ideal of $S$ and $I$ is called a *$P$-primary ideal* of $S$. The set $\{a \in S : a + J \subseteq I\}$, where $I, J$ are ideals, is denoted by $(I : J)$.

A non-empty subset $T$ of a semigroup $S$ is called an *additive system* of $S$ if $a, b \in T$ implies $a + b \in T$ and $0 \in T$. $S_T = \{s - t : s \in S, t \in T\}$ is an oversemigroup of $S$ which is called the *quotient semigroup* of $S$. If $P$ is a prime ideal of $S$, then $T = S - P$ is an additive system of $S$. In this case the quotient semigroup $S_T$ is denoted by $S_P$.

Throughout this paper we shall assume unless otherwise stated, that $S$ is a semigroup with the maximal ideal $M = S - U(S) \neq \emptyset$.

Let $S$ be a semigroup with quotient group $G$. We say that $S$ is a *valuation semigroup* if $g \in S$ or $-g \in S$ for each $g \in G$, so its ideals are linearly ordered by inclusion (see [3, Lemma 4]). We say that $S$ is a *Prüfer semigroup* if $S_P$ is a valuation semigroup for every prime ideal $P$ of $S$. An ideal of a semigroups $S$ is *irreducible* if, for ideals $J$ and $K$ of $S$, $I = J \cap K$ implies that either $I = J$ or $I = K$.

## 2. Quasi-primary ideals

An ideal of $S$ is called *quasi-primary* if its radical is a prime ideal of $S$.

**Lemma 2.1.** *Let $I$ be an ideal of a semigroup $S$. Then:*

($i$) *if $I$ contains a unit of $S$, then $I = S$,*

($ii$) *$S$ is a subgroup of $G$ if and only if $S$ has exactly one ideal.*

*Proof.* ($i$) Let $a$ be a unit of $S$ such that $a \in I$. Then $a + b = 0$ for some $b \in S$, so $0 = a + b \in I + S = I$. If $z \in S$, then $z = 0 + z \in I + S = I$. Therefore $I = S$.

($ii$) Let $S$ be a subgroup of $G$ and let $I$ be an ideal of $S$. Then there exists $a \in I$ such that $a$ is a unit of $S$; hence $I = S$ by ($i$). Conversely, it is enough to show that every element of $S$ is a unit. Suppose that $c \in S$. Then $c + S \neq \emptyset$ is an ideal of $S$, so $c + S = S$; whence $c + d = 0$ for some $d \in S$. It is easy to see that $S$ is a subgroup of $G$. □

**Theorem 2.2.** *Let $S$ be a semigroup. Then $S$ is a subgroup of $G$ if and only if every proper ideal of $S$ is prime.*

*Proof.* If $S$ is a subgroup of $G$, then the result is clear. Conversely, let $a$ be a non-zero and non-unit element of $S$. By assumption, $a + a + S = I$, where $I$ is prime, and so $a + a \in I$ implies $a \in I$. Thus $a = a + 0 = a + a + b$ for some $b \in S$, and since $S$ is a cancellation semigroup, we can cancel $a$ to obtain $a + b = 0$, showing that $a$ is unit, as required. □

**Lemma 2.3.** *Let $I, J$ and $K$ be ideals of a semigroup $S$. Then:*

($i$) *$I = (I + S_M) \cap S$,*

($ii$) *$K = I \cap J$ if and only if $K + S_M = (I + S_M) \cap (J + S_M)$.*

*Proof.* ($i$) Since $I \subseteq (I + S_M) \cap S$ is trivial, we will prove the reverse inclusion. Let $u \in (I + S_M) \cap S$. There exist $a \in I$ and $t \in S - M$ such that $u = a - t$, so $u + t = a \in I$ and $t + b = 0$ for some $b \in S$; hence $u = u + t + b \in I + S = I$, as required.

($ii$) Suppose first that $K = I \cap J$. Clearly, $K + S_M \subseteq (I + S_M) \cap (J + S_M)$. For the reverse inclusion, assume that $z \in (I + S_M) \cap (J + S_M)$. Then there are elements $a \in I$, $b \in J$ and $t, u \in S - M$ such that $z = a - t = b - u$, so $a + u = (a - t) + u + t = (b - u) + u + t = b + t \in I \cap J$ since $t, u$ are units of $S$; hence $z = a - t = (a + u) - (t + u) \in K + S_M$, as needed. The reverse implication follows from $(i)$. □

**Lemma 2.4.** *For ideals $I$ and $J$ of a semigroup $S$ the following statements hold:*

$(i)$ $\operatorname{rad}(I + J) = \operatorname{rad}(I) \cap \operatorname{rad}(J) = \operatorname{rad}(I \cap J)$. *Moreover, $I + J = S$ if and only if* $\operatorname{rad}(I) + \operatorname{rad}(J) = S$.

$(ii)$ *If $N$ is an additive system of $S$, then $I + S_N = S_N$ if and only if $I \cap N \neq \emptyset$.*

$(iii)$ *If $N$ is an additive system of $S$, then* $\operatorname{rad}(I + S_N) = \operatorname{rad}(I) + S_N$.

*Proof.* $(i)$ Is straightforward.

$(ii)$ If $I + S_N = S_N$, then $0 \in I + S_N$, so $0 = a - t$ for some $a \in I$ and $t \in N$; hence $a = t \in I \cap N$. Conversely, assume that $u \in I \cap N$. As $u$ is a unit of $S_N$, $I + S_N = S_N$ by Lemma 2.1.

$(iii)$ Since $\operatorname{rad}(I) + S_N \subseteq \operatorname{rad}(I + S_N)$ is trivial, we will prove the reverse inclusion. Suppose that $z \in \operatorname{rad}(I + S_N)$. Then there exist a positive integer $n$ such that $nz \in I + S_N$, so $nz = a - t$ for some $a \in I$, $t \in N$. As $n(z + t) = a + (n - 1)t \in I$, we get $z + t \in \operatorname{rad}(I)$. It follows that $z = z + t - t \in \operatorname{rad}(I) + S_N$, as required. □

**Lemma 2.5.** *Let $I$ be an ideal of $S$ with* $\operatorname{rad}(I) = M$. *Then $I$ is $M$-primary.*

*Proof.* Since $I \subseteq M \neq S$, an ideal $I$ is proper. Let $a, b \in S$ be such that $a + b \in I$ but $b \notin \operatorname{rad}(I)$. But $M$ is maximal and $b \notin M$, so must be $M + (b + S) = S$. Then from Lemma 2.4 it follows $I + (b + S) = S$, i.e., $0 = c + (b + s)$ for some $c \in I$, $s \in S$. Therefore, we have $a = a + 0 = a + b + c + s \in I + S = I$, as needed. □

**Proposition 2.6.** *Let $P$ be a prime ideal of a semigroup $S$, and let $I$ be a quasi-primary ideal of $S_P$ with a prime radical $Q$. Then $I \cap S$ is a quasi-primary ideal of $S$ with a prime radical $Q \cap S$.*

*Proof.* Since $Q$ is a prime ideal of $S_P$, $Q' = Q \cap S$ is a prime ideal of $S$ with $Q' \subseteq P$ and $Q' + S_P = Q$ by [3, Proposition 2], so all that remains to be verified that $Q'$ is the radical of $I \cap S$. Let $a \in \operatorname{rad}(I \cap S)$. Then $na \in I$ for some positive integer $n$; hence $a \in Q$. Thus, $a \in Q'$. Conversely, if $b \in Q'$, then $mb \in I \cap S$ for some positive integer $m$; so $b \in \text{rad}(I \cap S)$, as required. □

**Proposition 2.7.** *Let $I$ be a quasi-primary ideal of a semigroup $S$ with a prime radical $P$. Then $I + S_P$ is a primary ideal (so quasi-primary) of $S_P$. In particular, $(I + S_P) \cap S$ is a quasi-primary ideal of $S$.*

*Proof.* By Lemma 2.4 we have $\text{rad}(I+S_P) = P+S_P$, so it is a maximal ideal of $S_P$ by [3, Corollary 3]. Now Lemma 2.5 shows that $I + S_P$ is primary. The last claim follows from Proposition 2.6. □

**Proposition 2.8.** *Every ideal of a valuation semigroup $S$ is quasi-primary.*

*Proof.* Let $I$ be an ideal of $S$ with radical $P$. Let $a, b \in S$ such that $a+b \in P$. Then there exists a positive integer $n$ such that $n(a + b) \in I$. Since $S$ is a valuation semigroup, either $a+S \subseteq b+S$ or $b+S \subseteq a+S$. We may assume that $a + S \subseteq b + S$. Then there is an element $c \in S$ such that $a = b + c$, so $2na = na + nb + nc \in I + S = I$; hence $a \in P$. □

**Theorem 2.9.** *Every ideal of a Prüfer semigroup $S$ is quasi-primary.*

*Proof.* Let $I$ be an ideal of $S$. By Theorem 2.8, the ideal $I + S_M$ of the valuation semigroup $S_M$ is quasi-primary; hence Proposition 2.6 and Lemma 2.3 imply that $I = (I + S_M) \cap S$ is quasi-primary. □

## 3. Primal ideals

An element $s \in S$ is called *prime to $I$* if $(r + s) \in I$ $(r \in S)$ implies that $r \in I$, that is, $(I : s) = (I : (s)) = I$. An ideal $I$ of $S$ is called *primal* if the elements of $S$ that are not prime to $I$ form an ideal (see [1]).

**Lemma 3.1.** *Let $I$ be an ideal of a semigroup $S$ and let $P$ be the set of elements of $S$ which are not prime to $I$. If $P$ is an ideal of $S$, then $P$ is prime.*

*Proof.* Let $a, b \in S - P$. Then $(I : a) = (I : b) = I$. If $s \in (I : a + b)$, then $a + b + s \in I$, whence $s + a \in (I : b) = I$. Therefore $s \in (I : a) = I$, consequently $(I : a + b) = I$. Thus $a + b \notin P$. □

If $I$ is a primal ideal of $S$, then, by Lemma 3.1, $P$ is a prime ideal of $S$ called the *adjoint prime ideal* of $I$. In this case we also say that $I$ is a *$P$-primal ideal.*

**Theorem 3.2.** *For an ideal $I$ of a semigroup $S$, the following statements are equivalent.*

- $(i)$ *$I$ is primal with the adjoint prime ideal $P$,*
- $(ii)$ *If $a + b \in I$ and $b \notin I$, then $a \in P$ and conversely, for every $a \in P$ there exists an element $b \in S - I$ such that $a + b \in I$.*

*Proof.* $(i) \Rightarrow (ii)$ Let $a + b \in I$ with $b \notin I$. Then $b \in (I : a) - I$; hence $a \in P$. If $a \in P$, then $I \subset (I : a)$ because $I$ is primal. So, there is an element $x$ of $(I : a)$ which is not in $I$. Thus $a + x \in I$ and $x \notin I$.

$(ii) \Rightarrow (i)$ It is enough to show that $P + S \subseteq P$. Let $x + y \in P + S$ where $x \in P$, $y \in S$. Then there exists $c \notin I$ such that $x + c \in I$ by (ii), and hence $x + y + c \in I$ with $c \notin I$. Thus $x + y \in P$ by $(ii)$. □

**Lemma 3.3** *Let $Q$ be a $P$-primary ideal of a semigroup $S$, and let $a \in S$.*

- $(i)$ *If $a \in Q$, then $(Q : a) = S$.*
- $(ii)$ *If $a \notin Q$, then $(Q : a)$ is $P$-primary.*
- $(iii)$ *If $a \notin P$, then $(Q : a) = Q$.*

*Proof.* The proof is straightforward. □

**Proposition 3.4.** *A $P$-primary ideal is primal.*

*Proof.* It is enough to show that the set of elements of $S$ which are not prime to $Q$ is just $P$. Suppose that $s$ is such element of $S$ which is not prime to $Q$. Then $Q \subset (Q : s)$. Hence there exists $a \in (Q : s)$ with $a \notin Q$ and $a+s \in Q$. Therefore, $s \in P$ because $Q$ is primary. Conversely, if $s \notin P$, then $(Q : s) = Q$ by Lemma 3.3. □

**Proposition 3.5.** *Let $I$ be a $Q$-primal ideal of a semigroup $S$, and let $P$ be a prime ideal of $S$. Then:*

- $(i)$ *$I = (I + S_P) \cap S$ for $Q \subseteq P$,*
- $(ii)$ *$I \subset (I + S_P) \cap S$ for $Q \nsubseteq P$.*

*Proof.* $(i)$ Clearly, $I \subseteq (I + S_P) \cap S$. For $x \in (I + S_P) \cap S$ we have $x = c - d \in S$ for some $c \in I$ and $d \notin P$. Therefore, $x + d = c \in I$. As $d \notin Q$, $d$ is prime to $I$; hence $x \in I$.

(*ii*) Since $Q \nsubseteq P$, there is $y \in Q$ such that $y \notin P$. So $y + u \in I$ for some $u \notin I$ by Theorem 3.2. Then $u = (y + u) - y \in (I + S_P) \cap S$. But $u \notin I$, so $I \subset (I + S_P) \cap I$. □

**Corollary 3.6.** *Let $I$ be a $Q$-primal ideal of a semigroup $S$, and let $T$ be a quotient semigroup of $S$. Then either $I = (I + T) \cap S$ or $I \subset (I + T) \cap S$.*

*Proof.* By [3, Proposition 2], $T = S_P$ for some prime ideal $P$ of $S$. The rest follows from Proposition 3.5. □

**Proposition 3.7.** *Let $P$ be a prime ideal of a semigroup $S$, and let $I$ be a $Q$-primal ideal of $S_P$. Then $I \cap S$ is a primal ideal of $S$ with the adjoint prime ideal $Q \cap S$.*

*Proof.* As $Q$ is prime ideal of $S_P$, by [3, Proposition 2], $Q' = Q \cap S$ is a prime ideal of $S$ with $Q' \subseteq P$ and $Q' + S_P = Q$. To prove that $Q'$ is exactly the set of elements non-prime to $I \cap S$ let $z \notin Q \cap S$. Then $z \notin Q$, so $(I :_{S_P} z) = I$. Thus $(I \cap S : z) = I \cap S$, whence $z$ is prime to $I \cap S$. If $z \in Q \cap S$, then $z \in Q$, so there exists $u \in S_P$ with $z + u \in I$ and $u \notin I$ by Theorem 3.2. We can write $u = x - y$ for some $x \in S$, $y \in S - P$. If $x \in I$, then $x = u + y \in I$ with $y \notin Q$, so $u \in I$, a contradiction. So we can assume that $x \notin I$. Since $z + u \in I$ implies $z + x \in I \cap S$, we get $x \in (I \cap S : z)$. But $x \notin I$, so $z$ is not prime to $I \cap S$. □

**Corollary 3.8.** *Let $I$ be a $Q$-primal ideal of a quotient semigroup $T$ of $S$. Then $I \cap S$ is a primal ideal of $S$ with the adjoint prime ideal $Q \cap S$.*

*Proof.* Follows from [3, Proposition 2] and Proposition 3.7. □

**Proposition 3.9.** *Let $I$ be an ideal of a semigroup $S$ such that $(I : a) = P$ is a prime ideal of $S$ for some $a \in S - I$. Then $(I + S_P) \cap S$ is a $P$-primal ideal of $S$.*

*Proof.* Let $J = (I + S_P) \cap S$. First, we show that $(J : a) = P$. If $t \in P = (I : a)$, then $t + a \in I \subseteq J$; hence $t \in (J : a)$. For the reverse inclusion, assume that $u \in (J : a)$, so $u + a = c - d \in J$ for some $c \in I$, $d \notin P$. Thus $u + a + d = c \in I$. Consequently $u + d \in (I : a) = P$. So, $u \in P$ since $P$ is prime. As $P \neq S$, we get $a \notin J$. Therefore, in $P$ no elements prime to $J$.

Let us show that every $b \notin P$ is prime to $J$. Clearly, $J \subseteq (J : b)$. To prove $(J : b) \subseteq J$, assume that $c \in (J : b)$, so $c + b = e - f \in I$ for some $e \in I$, $f \notin P$; hence $c = e - (b + f) \in J$ since $(b + f) \notin P$. Thus, $(J : b) \subseteq J$, which completes the proof. □

**Lemma 3.10.** *Every irreducible ideal of a semigroup $S$ is primal.*

*Proof.* Let $I$ be an irreducible ideal of $S$. Assume that $P$ is the set of elements of $S$ which are not prime to $I$. To prove that $P + S \subseteq P$ let $a+s \in P+S$ where $a \in P$, $s \in S$. Then $I \subset (I : a)$ because $a \in P$. Clearly, $I \subseteq (I : a) \cap (I : s) \subseteq (I : a + s)$. If $I = (I : a) \cap (I : s)$, then $I = (I : s)$ since $I$ is irreducible. Let $t \in (I : a + s)$. Then $t + a \in (I : s) = I$, so $t \in (I : a)$; hence $I \subset (I : a) = (I : a+s)$. If $I \neq (I : a) \cap (I : s)$, then again $I \subset (I : a + s)$, that is, $a + s$ is not prime to $I$. Thus $a + s \in P$. □

**Proposition 3.11.** *An ideal $I$ of a Prüfer semigroup is irreducible if and only if it is primal.*

*Proof.* By Lemma 3.10, it is sufficient to show that if $I$ is $P$-primal, then $I$ is irreducible. If $I = J \cap K$ for ideals $J$, $K$, then $I+S_M = (J+S_M)\cap(K+S_M)$ by Lemma 2.3. Since $S_M$ is a valuation semigroup, either $I+S_M = J+S_M$ or $I + S_M = K + S_M$. Because $M$ contains $P$ then by Proposition 3.5 $I + S_M = J + S_M$ gives $I = (I + S_M) \cap S = (J + S_M) \cap S$. Hence $J \subseteq (J + S_M) \cap S = I$. The case $I + S_M = K + S_M$ is similar. So, $I$ is irreducible. □

**Proposition 3.12.** *An ideal $I$ of a valuation semigroup $S$ is a primal ideal of $S$ with the adjoint prime ideal $P = \{a \in S : (a + S) + I \subset I\}$.*

*Proof.* Let $I = J \cap K$ for ideals $J, K$ of $S$. Then either $J \subseteq K$ or $K \subseteq J$ because $S$ is a valuation semigroup. So either $I = J$ or $I = K$. Therefore, $I$ is irreducible, and hence $I$ is primal by Proposition 3.10. Let us show that $P$ is an ideal of $S$. Let $a + s \in P + S$ where $a \in P$, $s \in S$. Then $(a+S)+I \subset I$; hence $(a+s)+S+I \subseteq (a+S)+I \subset I$, so $a+s \in P$. Thus, $P$ is an ideal of $S$. To prove that $P$ is prime let $x + y \in P$ with $x \notin P$. Then $(x+S)+I = I$ and $(y+S)+I = (x+y+S)+I \subset I$, whence $y \in P$.

To prove that $P$ is the set of elements of $S$ which are not prime to $I$ consider $u \in P$. Then $(u + S) + I \subset I \subseteq (I : u)$. Suppose that $(I : u) = I$. If $v \in (I : u) = I$, then $u+v \in I$, so $v \in (u+S)+I$; hence $I = (u+S)+I$, a contradiction. □

**Corollary 3.13.** *Every ideal of a oversemigroup of a valuation semigroup is primal.*

*Proof.* This follows from [3, Lemma 4] and Proposition 2.12. □

**Theorem 3.14.** *Every ideal of a Prüfer semigroup is primal.*

*Proof.* If $I$ is an ideal of a Prüfer semigroup $S$, then $I = (I + S_M) \cap S$ by Lemma 2.3, so, by Proposition 3.12, the ideal $I + S_M$ of $S_M$ is primal. Proposition 3.7 completes the proof. □

**Corollary 3.15** *An ideal of a Prüfer semigroup is primal* (*resp. quasi-primary*) *if and only if it is primary.*

*Proof.* Follows from Theorem 2.9 and Theorem 3.14. □

## References

[1] **L. Fuchs**: *On primal ideals*, Proc. Amer. Math. Soc. **1** (1950), 1 – 6.

[2] **L. Fuchs and E. Mosteig**: *Ideal theory in Prüfer domains*, J. Algebra **252** (2002), 411 – 430.

[3] **M. Kanemitsu**: *Oversemigroups of a valuation semigroup*, SUT Journal Math. **2** (2000), 185 – 197.

Received September 14, 2005

S. E. Atani
Department of Mathematics
University of Guilan
P.O. Box 1914, Rasht
Iran
E-mail: ebrahimi@guilan.ac.ir

A. Y. Darani
Department of Mathematics
University of Guilan
P.O. Box 1914, Rasht
Iran
E-mail: yousefian@guilan.ac.ir

# Finite hexagonal quasigroups

*Mea Bombardelli*

## Abstract

In this article some examples of finite hexagonal (idempotent, medial and semisymmetric) quasigroups are given. The main goal is to determine the set of possible orders of finite hexagonal quasigroups.

## 1. Introduction

Hexagonal quasigroups are defined by V. Volenec in [1] as follows:

**Definition.** A quasigroup $(Q,\cdot)$ is said to be *hexagonal* if it is idempotent, medial and semisymmetric, i.e., if the equalities

$$\begin{aligned} &a\cdot a=a,\\ &ab\cdot cd=ac\cdot bd,\\ &a\cdot ba=ab\cdot a=b \end{aligned}$$

hold for all its elements.

Study of hexagonal quasigroups in [1] and [2] is motivated by

**Example 1.** On the set $\mathbb{C}$ of complex numbers the operation $*$ is defined by:

$$a*b=\frac{1-i\sqrt{3}}{2}\,a+\frac{1+i\sqrt{3}}{2}\,b.$$

If we identify the complex numbers with the points of the Euclidean plane, the points $a$, $b$ and $a*b$ are the vertices of a positively oriented equilateral triangle.

2000 Mathematics Subject Classification: 20N05
Keywords: hexagonal quasigroup, finite quasigroups, order, IM quasigroup

In this paper, we'll give some examples of finite hexagonal quasigroups, and answer the question: *for which positive integers $n$ there exists a hexagonal quasigroup of order $n$?*

We'll need some elementary results.

**Lemma 1.** *Let $(Q_1, \cdot_1)$, $(Q_2, \cdot_2), \dots, (Q_n, \cdot_n)$ be hexagonal quasigroups, and let $\circ$ be the operation defined on $Q = Q_1 \times Q_2 \times \ldots \times Q_n$ by:*

$$(x_1, x_2, \dots, x_n) \circ (y_1, y_2, \dots, y_n) = (x_1 \cdot_1 y_1, x_2 \cdot_2 y_2, \dots, x_n \cdot_n y_n).$$

*Then $(Q, \circ)$ is a hexagonal quasigroup.*

Therefore, if a hexagonal quasigroup of order $m$ exists, then there exists hexagonal quasigroup of order $m^n$, for each $n \in \mathbb{N}$. If hexagonal quasigroups of orders $k_1$, $k_2$,… $k_n$ exist, then a hexagonal quasigroup of order $k_1 k_2 \cdots k_n$ exists.

A *subquasigroup* of the quasigroup $(Q, \cdot)$ is any subset $S \subset Q$ such that $(S, \cdot)$ is a quasigroup. Obviously, any subquasigroup of a hexagonal quasigroup is hexagonal.

For any quasigroup $(Q, \cdot)$ and its subset $A$, the smallest quasigroup that contains $A$ is the intersection of all subquasigroups of $Q$ that contain $A$.

**Example 2.** Let $(D, *)$ be the smallest subquasigroup of $(\mathbb{C}, *)$ (as in Example 1) that contains 0 and 1. $D$ can be represent by triangular lattice with the same operation as in $(\mathbb{C}, *)$: the product of two points $a$ and $b$ is the third vertex of regular triangle with vertices $a$ and $b$.

If $q = \frac{1}{2} + i\frac{\sqrt{3}}{2}$, then $D = \{x + qy : x, y \in \mathbb{Z}\}$, and it can be identified with the set $\{(x, y) : x, y \in \mathbb{Z}\}$. It's easy to verify:

$$\begin{aligned}(x_1, y_1) * (x_2, y_2) &= (1 - q)(x_1 + qy_1) + q(x_2 + qy_2) \\ &= (x_1 + y_1 - y_2, x_2 + y_2 - x_1).\end{aligned}$$

We obtained an important example of hexagonal quasigroup:

**Theorem 1.** *Let $(G, +)$ be a commutative group. The set $G \times G$ with the operation*

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 + y_1 - y_2, x_2 + y_2 - x_1)$$

*is a hexagonal quasigroup.*

Therefore, a hexagonal quasigroup of order $n^2$ exists for any $n \in \mathbb{N}$.

The following characterization of hexagonal quasigroups was given in [1].

**Theorem 2.** *A hexagonal quasigroup on the set $Q$ exists if and only if on the same set exists commutative group with automorphism $\varphi$ satisfying*

$$(\varphi \circ \varphi)(a) - \varphi(a) + a = 0 \tag{1}$$

*for all $a \in Q$.*

Given such commutative group $(Q, +)$, the quasigroup is obtained by

$$a \cdot b = a + \varphi(b - a). \tag{2}$$

Note that from (1) it follows

$$\varphi^3(x) = \varphi(\varphi(x) - x) = \varphi \circ \varphi(x) - \varphi(x) = (\varphi(x) - x) - \varphi(x) = -x$$

and $\varphi^6(x) = x$ for all $x \in Q$.

## 2. Commutative hexagonal quasigroups

Let us use the Theorem 2 to study commutative hexagonal quasigroups. We wish to find all commutative groups $Q$ which have an automorphism $\varphi$ that satisfies (1), with additional condition that the operation $\cdot$ defined by (2) is commutative. In other words,

$$a + \varphi(b - a) = b + \varphi(a - b),$$
$$\varphi(b - a) - \varphi(a - b) = b - a$$

for all $a, b \in Q$. Therefore

$$\varphi(x) + \varphi(x) = x \tag{3}$$

must hold for all $x \in Q$.

From (1) it follows $\varphi(\varphi(x)) + \varphi(\varphi(x)) + x + x = \varphi(x) + \varphi(x)$ and using (3) we obtain $\varphi(x) + x + x = \varphi(x) + \varphi(x) = x$. It follows

$$\varphi(x) + x = 0 \qquad \text{and} \qquad \varphi(x) = x + x.$$

Therefore, $x + x + x = 0$ for all $x \in Q$, i.e., each element of the group $G$ is of order 3 or 1. The only finite groups which satisfy that condition are $(\mathbb{Z}_3)^n$, and the group of order 1.

On the other hand, if $x+x+x=0$, $\forall x \in Q$, then $\varphi(x)=x+x=-x$ is an automorphism that satisfies (1), and the operation defined by (2) is commutative.

We have proved:

**Theorem 3.** *The only finite commutative hexagonal quasigroups with more than one element, are the quasigroups obtained in the way described in Theorem* 2 *from the group* $(\mathbb{Z}_3)^n$*, for some* $n \in \mathbb{N}$.

From each group $(\mathbb{Z}_3)^n$ we obtain unique hexagonal quasigroup of order $3^n$.

**Example 3.** From $(\mathbb{Z}_3)^2$ we obtain hexagonal quasigroup of order 9:

| $\cdot$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 2 | 1 | 6 | 8 | 7 | 3 | 5 | 4 |
| 1 | 2 | 1 | 0 | 8 | 7 | 6 | 5 | 4 | 3 |
| 2 | 1 | 0 | 2 | 7 | 6 | 8 | 4 | 3 | 5 |
| 3 | 6 | 8 | 7 | 3 | 5 | 4 | 0 | 2 | 1 |
| 4 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 5 | 7 | 6 | 8 | 4 | 3 | 5 | 1 | 0 | 2 |
| 6 | 3 | 5 | 4 | 0 | 2 | 1 | 6 | 8 | 7 |
| 7 | 5 | 4 | 3 | 2 | 1 | 0 | 8 | 7 | 6 |
| 8 | 4 | 3 | 5 | 1 | 0 | 2 | 7 | 6 | 8 |

## 3. Cyclic groups

The automorphism $\varphi(x)=kx$ ($k$ is relatively prime to $n$) of the group $\mathbb{Z}_n$ satisfies (1) if and only if $k^2-k+1 \equiv 0 (\mathrm{mod}\ n)$.

We need to determine for which $n \in \mathbb{N}$ the obtained quadratic congruence has solution $k$ (in that case $k$ and $n$ are relatively prime), or to determine the possible factors of $k^2-k+1$ for $k \in \mathbb{Z}$.

Evidently, since $k^2-k+1$ is odd, $n$ cannot be even.

Let us determine all odd primes $p$ for which $p \mid k^2-k+1$, for some $k \in \mathbb{Z}$. If $p \mid k^2-k+1$, then so do $p$ divides the number $4(k^2-k+1)=(2k-1)^2+3$, that is $p \mid a^2+3$ where $a=2k-1$ is an odd integer. It suffices to determine for which $p$ exists $x \in \mathbb{Z}$ such that $x^2 \equiv -3 (\mathrm{mod}\ p)$ (if such an even integer $x$ exists, then $x+p$ is odd integer that satisfies the condition).

It is equivalent to $\left(\frac{-3}{p}\right)=1$, which (since $p$ is an odd integer) is equivalent to $\left(\frac{p}{3}\right)=1$, i.e., $p \equiv 0 (\mathrm{mod}\ 3)$ or $p \equiv 1 (\mathrm{mod}\ 3)$. The solutions are

$p = 3$ and all primes of the form $p = 6l + 1$, $l \in \mathbb{Z}$. Factors of $k^2 - k + 1$ cannot be primes of the form $6l - 1$.

This proves the following:

**Theorem 4.** *The cyclic group $\mathbb{Z}_n$ has an automorphism that satisfies* (1) *if and only if its order $n$ is a product of primes from the set $\{3\} \cup \{6l + 1 : l \in \mathbb{Z}\}$, i.e., if and only if $n$ is an odd integer without any prime factor that is congruent to* $-1$ *modulo* 6.

**Example 4.** Group $\mathbb{Z}_7$ has two such automorphisms, $\varphi(x) = 3x$ and $\varphi(x) = 5x$. So we obtain two hexagonal quasigroups of order 7.

| $\cdot$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 1 | 5 | 1 | 4 | 0 | 3 | 6 | 2 |
| 2 | 3 | 6 | 2 | 5 | 1 | 4 | 0 |
| 3 | 1 | 4 | 0 | 3 | 6 | 2 | 5 |
| 4 | 6 | 2 | 5 | 1 | 4 | 0 | 3 |
| 5 | 4 | 0 | 3 | 6 | 2 | 5 | 1 |
| 6 | 2 | 5 | 1 | 4 | 0 | 3 | 6 |

| $\cdot$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 1 | 3 | 1 | 6 | 4 | 2 | 0 | 5 |
| 2 | 6 | 4 | 2 | 0 | 5 | 3 | 1 |
| 3 | 2 | 0 | 5 | 3 | 1 | 6 | 4 |
| 4 | 5 | 3 | 1 | 6 | 4 | 2 | 0 |
| 5 | 1 | 6 | 4 | 2 | 0 | 5 | 3 |
| 6 | 4 | 2 | 0 | 5 | 3 | 1 | 6 |

## 4. Conclusion

The following theorem is well-known.

**Theorem 5.** *Let $m_1$ and $m_2$ be relatively prime positive integers, and $G$ be commutative group of order $m_1 m_2$, whose automorphism $\varphi$ satisfies* (1). *Then there exist groups $G_1$ and $G_2$ such that $G = G_1 \times G_2$, $|G_1| = m_1$, $|G_2| = m_2$, with automorphisms that satisfy* (1).

Theorem 5 allows us to deal with groups of order $p^k$ only, in order to determine which groups have "good" automorphism.

So far, we know that finite hexagonal quasigroup can have orders $p^{2k}$ for any prime $p$, $3^k$, and $p^k$ where $p$ is a prime of the form $6l + 1$.

Let $G$ be finite commutative group with automorphism $\varphi$ which satisfies (1). For $x \in G$ let us denote

$$S_x = \{x, \varphi(x), \varphi^2(x), \varphi^3(x), \varphi^4(x), \varphi^5(x), \ldots\}.$$

It is clear that $\{S_x : x \in G\}$ is a partition of the set $G$. Since $\varphi^6(x) = x$, for all $x \in G$, the set $S_x$ has 6 elements at most, i.e., it may have 1, 2, 3 or 6 elements. The only $x$ for which $\operatorname{Card} S_x = 1$ is $x = 0$.

Card $S_x = 2$ when $x = \varphi^2(x)$, that is when $x + x + x = 0$.
Card $S_x = 3$ when $x = \varphi^3(x)$, i.e., $x = -x$.
Let

$$a = \text{Card}\,\{S_x : x \in G, |S_x| = 2\},$$

$$b = \text{Card}\,\{S_x : x \in G, |S_x| = 3\},$$

$$c = \text{Card}\,\{S_x : x \in G, |S_x| = 6\}.$$

The number of elements of $G$ equals $|G| = 1 + 2a + 3b + 6c$.

Now we can finally solve remaining problems: the existence of hexagonal quasigroup of order $2^{2m-1}$, or of order $p^{2m-1}$ for $p$ prime of the form $6l - 1$.

Suppose the group $G$ of order $2^{2m-1}$ has an automorphism that satisfies (1). Since its order is not divisible by 3, $a = 0$, and $|G| = 1 + 3b + 6c \equiv 1(\text{mod } 3)$. But, $2^{2m-1} \equiv 2(\text{mod } 3)$, which is a contradiction.

Let now $p$ be a prime number of the form $6l - 1$, and let $G$ be the group of order $p^{2m-1}$, with an automorphism which satisfies (1). That group has no element of order two, and no element of order three, so $a = 0$ and $b = 0$. It follows $p^{2m-1} = 1 + 6c$, which is impossible since $p^{2m-1} \equiv -1(\text{mod } 6)$.

This finally proves:

**Theorem 6.** *A finite hexagonal quasigroup of order $n = m \cdot l^2$, where $m$ is square-free, exists if and only if $m$ is an odd integer with no prime factor congruent to $-1$ modulo 6.*

## References

[1] **V. Volenec**: *Hexagonal quasigroups*, Arch. Math., Brno, **27a** (1991), 113 – 122.

[2] **V. Volenec**: *Regular triangles in hexagonal quasigroups*, Rad Hrvat. Akad. Znan. Umjet., Mat. Znan., **467(11)** (1994), 85 – 93.

Department of Mathematics
University of Zagreb
Bijenička 30
10000 Zagreb
Croatia
E-mail: Mea.Bombardelli@math.hr

Received May 2, 2006

# On n-ary semigroups with adjoint neutral element

*Wiesław A. Dudek and Vladimir V. Mukhin*

## Abstract

We prove that we can adjoint an $n$-ary neutral element to an $n$-ary semigroup iff this semigroup is derived from a binary semigroup.

According to the general convention used in the theory of $n$-ary groupoids the sequence of elements $x_i, x_{i+1}, \ldots, x_j$ will be denoted by $x_i^j$. For $j < i$ it is the empty symbol. If $x_{i+1} = x_{i+2} = \ldots = x_{i+t} = x$, then instead of $x_{i+1}^{i+t}$ we will write $\overset{(t)}{x}$. In this convention the symbol $f(x_1, \ldots, x_n)$ will be written as $f(x_1^n)$. Similarly, the symbol $f(x_1^i, \overset{(t)}{x}, x_{i+t+1}^n)$ means $f(x_1, \ldots, x_i, \underbrace{x, \ldots, x}_{t}, x_{i+t+1}, \ldots, x_n)$.

An $n$-ary groupoid $(G, f)$ is called $(i,j)$-*associative* if

$$f(x_1^{i-1}, f(x_i^{n+i-1}), x_{n+i}^{2n-1}) = f(x_1^{j-1}, f(x_j^{n+j-1}), x_{n+j}^{2n-1}) \qquad (1)$$

holds for all $x_1, \ldots, x_{2n-1} \in G$. If this identity holds for all $1 \leqslant i < j \leqslant n$, then we say that the operation $f$ is *associative* and $(G, f)$ is called an *$n$-ary semigroup*. It is clear that an $n$-ary groupoid is associative if and only if it is $(1,j)$-associative for all $j = 2, \ldots, n$. In the binary case (i.e. for $n = 2$) it is a usual semigroup.

An $n$-ary semigroup $(G, f)$ in which for all $x_0, x_1, \ldots, x_n \in G$ and all $i \in \{1, \ldots, n\}$ there exists an element $z_i \in G$ such that

$$f(x_1^{i-1}, z, x_{i+1}^n) = x_0, \qquad (2)$$

is called an *$n$-ary group*. It is clear that for $n = 2$ we obtain a usual group.

Note by the way that in many papers $n$-ary semigroups ($n$-ary groups) are called $n$-semigroups ($n$-groups, respectively). Moreover, in many papers,

2000 Mathematics Subject Classification: 20N05
Keywords: monoid, neutral element, $n$-ary semigroup

where the arity of the basic operation does not play a crucial role, is used the term *polyadic semigroups* (*polyadic groups*) (cf. [8]).

In the paper [1] written by W. Dörnte (under inspiration of Emmy Noether), he observed that any $n$-ary groupoid $(G, f)$ of the form

$$f(x_1^n) = x_1 \circ x_2 \circ \ldots \circ x_n \circ b,$$

where $(G, \circ)$ is a group and $b$ belongs to the center of this group, is an $n$-ary group but for every $n > 2$ there are $n$-ary groups which are not of this form. In the first case we say that an $n$-ary groupoid $(G, f)$ is $b$-*derived* (or *derived* if $b$ is the identity of $(G, \circ)$) from the group $(G, \circ)$, in the second – *irreducible.* Obviously, an $n$-ary operation derived from a binary associative operation is also associative in the above sense. An $n$-ary operation $b$-derived from an associative operation can be associative also in the case when $b$ is not in the center. For example, the ternary operation $b$-derived from the multiplication of a nilpotent associative algebra of index 7 (the product of any 7 elements is 0) is trivially associative for every $b$.

In some $n$-ary groupoids there exists an element $e$ (called an *$n$-ary neutral element*) such that

$$f(\overset{(i-1)}{e}, x, \overset{(n-i)}{e}) = x \tag{3}$$

holds for all $x \in G$ and for all $i = 1, \ldots, n$. There are $n$-ary semigroups (groups) with two, three and more neutral elements [9]. Also there are $n$-ary semigroups (groups too) in which all elements are neutral. All $n$-ary groups with this property are derived from the commutative group of the exponent $k|(n-1)$ [2]. In $n$-ary group the set of neutral elements (if it is non-empty) forms an $n$-ary subgroup [5, 6]. In ternary groups each two neutral elements form a ternary subgroup. Other important properties of neutral elements one can find in [7] and [12].

As is it well known, to any semigroup $(G, \circ)$ we can adjoint the identity $e \notin G$ in this way that $(G \cup \{e\}, \diamond)$ is a semigroup containing $(G, \circ)$ as its semigroup. For this it is sufficient to define the operation $\diamond$ as the extension of $\circ$ putting $x \diamond y = x \circ y$ for $x, y \in G$, $e \diamond e = e$ and $x \diamond e = e \diamond x = x$ for $x \in G$.

Natural question is: *Is it possible to find the analogous construction for $n$-ary semigroups?* We prove below that the answer is positive.

First we characterize $n$-ary semigroups containing at least one $n$-ary neutral element.

**Lemma 1.** *An $n$-ary semigroup containing the neutral element is derived from a binary semigroup.*

*Proof.* Let $e$ be the neutral element of an $n$-ary semigroup $(G,f)$. It is clear that $(G,\circ)$, where $x\circ y = f(x,\overset{(n-2)}{e},y)$, is a semigroup and $e$ is its neutral element. Direct computations shows that $(G,f)$ is derived from $(G,\circ)$. □

From the above proposition we can deduce the following result firstly proved by W. Dörnte.

**Corollary 1.** *An $n$-ary group is derived from a binary group if and only if it has the neutral element.*

Note that any $(i,j)$-associative $n$-ary groupoid $(G,f)$ with the neutral element in the center is an $n$-ary semigroup [3, 10, 11]. Such groupoid is associative also in the case when in the center of $(G,f)$ lies at least one *neutral polyad* (*sequence*), i.e., the sequence of elements $a_2^n\in G$ such that $f(x,a_2^n)=f(a_2^n,x)=x$ holds for all $x\in G$ [3, 11]. Neutral sequences are in all $n$-ary groups ([8]), but not in all $n$-ary semigroups.

**Lemma 2.** *An $n$-ary semigroup derived from a binary semigroup possess a neutral sequence if and only if it contains the neutral element.*

*Proof.* Let $(G,f)$ be derived from a semigroup $(G,\circ)$. If $a_2^n$ is a neutral sequence of $(G,f)$, then $e=a_2\circ a_3\circ\ldots\circ a_n$ belongs to $G$ and $x\circ e = x\circ a_2\circ a_3\circ\ldots\circ a_n = f(x,a_2^n)=x$ for all $x\in G$. Similarly $e\circ x = x$. This means that $e$ is the identity of $(G,\circ)$. Hence it is the neutral element of an $n$-ary semigroup derived from $(G,\circ)$.

The converse statement is obvious. □

**Corollary 2.** *If an $n$-ary semigroup without neutral elements is derived from a binary semigroup then it does not possess any neutral sequence.*

**Proposition 1.** *A neutral element can be adjoint to any $n$-ary semigroup derived from a binary semigroup.*

*Proof.* Let $n$-ary semigroup $(G,f)$ be derived from a binary semigroup $(G,\circ)$. Then to $(G,\circ)$ we can add the identity $e\notin G$ in this way that $(G\cup\{e\},\circ)$ becomes a semigroup with $(G,\circ)$ as its subsemigroup. In an $n$-ary semigroup $(G\cup\{e\},g)$ derived from $(G\cup\{e\},\circ)$ the element $e$ is neutral and $f(x_1^n)=g(x_1^n)$ for $x_1^n\in G$. So, to $(G,f)$ we can adjoint the neutral element $e\notin G$. □

**Proposition 2.** *If an $n$-ary semigroup $(G,f)$ do not contains any neutral elements, then to $(G,f)$ we can adjoint the neutral element if and only if $(G,f)$ is derived from a binary semigroup.*

*Proof.* If to an $n$-ary semigroup $(G,f)$ we can adjoint the neutral element $e\notin G$, then on $G\cup\{e\}$ we can define the $n$-ary operation $g$ such that $g(x_1^n)=f(x_1^n)$ for all $x_1^n\in G$. By Lemma 1, an $n$-ary semigroup $(G\cup\{e\},g)$ is derived from the semigroup $(G\cup\{e\},*)$, where $x*y=g(x,\overset{(n-2)}{e},y)$. Obviously $(G,*)$ is a subsemigroup of $(G\cup\{e\},*)$. If not, then there are $a,b\in G$ such that $e=a*b$ which contradicts to the assumption on $e$. This means that $(G,f)$ is an $n$-ary subsemigroup of $(G\cup\{e\},g)$ and it is derived from $(G,*)$.

The converse statement follows from Proposition 1. □

As a consequence of the above two propositions we obtain the following

**Theorem 1.** *To an $n$-ary semigroup $(G,f)$ we can adjoint the neutral element if and only if $(G,f)$ is derived from a binary semigroup.*

From the above proofs it follows that in an $n$-ary semigroup $(G,f)$ derived from a semigroup $(G,\circ)$ the adjoint $n$-ary neutral element is the adjoint identity of $(G,\circ)$.

**Corollary 3.** *An $n$-ary semigroup $(G,f)$ can be embedded into an $n$-ary semigroup with neutral element if and only if it is derived from a binary semigroup.*

**Corollary 4.** *An $n$-ary group $(G,f)$ can be embedded into an $n$-ary group derived from a binary group if and only if $(G,f)$ has at least one neutral element.*

This means that to $n$-ary groups without neutral element we do not adjoint any neutral element.

**Theorem 2.** *For every $n>2$ there exists at least one $n$-ary semigroup (group) to which any $n$-ary neutral element cannot be adjoint.*

*Proof.* It is sufficient to prove that for every $n>2$ there exists at least one $n$-ary group without neutral elements.

At first consider the multiplicative group $G=T(3,\mathbb{K})$ of triangular matrices of the form $\begin{bmatrix}1&x&y\\0&1&z\\0&0&1\end{bmatrix}$, where $\mathbb{K}$ is a field of non-zero characteristic $p$. Then the map

$$\theta\begin{bmatrix}1&x&y\\0&1&z\\0&0&1\end{bmatrix}=\begin{bmatrix}1&\alpha x&y\\0&1&\beta z\\0&0&1\end{bmatrix},$$

where $\alpha$ is a primitive root of unity of degree $n-1$ and $\alpha\beta = 1$, is an automorphism of this group. It is not difficult to verify that the set $G$ with the operation

$$f(A_1, A_2, \ldots, A_n) = A_1 \cdot \theta(A_2) \cdot \theta^2(A_3) \cdot \ldots \cdot \theta^{n-1}(A_n) \cdot B, \qquad (4)$$

where $B = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, is an $n$-ary group.

This group do not contains any $n$-ary neutral element. Indeed, if $A$ is its $n$-ary neutral element, then we have $f(X, A, A, \ldots, A) = f(A, X, A, \ldots, A)$ for all $X \in G$. Whence, according to (4), we conclude $X \cdot \theta A = A \cdot \theta X$. Taking the identity matrix as $X$, we get $\theta A = A$. This proves that the matrix $A$ belongs to the center of the group $(G, \cdot)$. Thus $X \cdot A = A \cdot \theta X = \theta X \cdot A$, which implies $\theta X = X$ for all $X \in G$. This is not true. So, $(G, f)$ is an $n$-ary group without neutral elements.

Now we give the another example of $n$-ary group without $n$-ary neutral elements.

Let $\mathbb{C}$ be the set of complex numbers and let $\omega$ be the primitive $(n-1)$-th root of unity. Then $G = \mathbb{C}^3$ with the operation

$$\mathbf{x} \bullet \mathbf{y} = (x_1, x_2, x_3) \bullet (y_1, y_2, y_3) = (x_1 + y_1, x_2 + y_2 + x_1 y_3, x_3 + y_3)$$

is a group and $\theta(x_1, x_2, x_3) = (\omega x_1, \omega^2 x_2, \omega x_3)$ is its automorphism.

It is not difficult to verify that $(G, g)$, where

$$g(\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_n}) = \mathbf{x_1} \bullet \theta(\mathbf{x_2}) \bullet \theta^2(\mathbf{x_3}) \bullet \ldots \bullet \theta^{n-1}(\mathbf{x_n}),$$

is an $n$-ary group. It is isomorphic to an $n$-ary group of triangular matrices from the proof of Theorem 3 in [4].

Similarly as in the previous case we can prove that $(G, g)$ is not derived from any binary group. □

## References

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

[2] **W. A. Dudek**: *Autodistributive n-groups*, Commentationes Math. Annales Soc. Math. Polonae, Prace Matematyczne **23** (1983), 1 – 11.

[3] **W. A. Dudek**: *On $(i, j)$-associative n-groupoids with the non-empty center*, Ricerche di Matematica (Napoli) **35** (1986), 105 – 111.

[4] **W. A. Dudek**: *On the class of weakly semiabelian polyadic groups*, Discrete Math. Appl. **6** (1996), 427 – 433 (translation from Diskretn. Mat. **8** (1996), 40 – 46).

[5] **W. A. Dudek**: *Idempotents in $n$-ary semigroups*, Southeast Asian Bull. Math. **25** (2001), 97 – 104.

[6] **A. M. Gal'mak**: *$n$-ary subgroups of identities*, (Russian), Vesti Nats. Akad. Navuk Belarussi, ser. Fiz.-mat. **2** (2003), 25 – 30.

[7] **M. S. Pop**: *On some relations on $n$-monoids*, Carpatian J. Math. **20** (2004), 87 – 94.

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

[9] **D. W. Robinson**: *$n$-groups with identity elements*, Math. Mag. **31** (1958), 255 – 258.

[10] **B. Trpenovski**: *On $n$-groupoids containing central neutral elements*, (Makedonian), Bull. Soc. Math. et Phys. R. P. Macédoine **14** (1963), 31 – 39.

[11] **B. Trpenovski and G. Čupona**: *Finitary associative operations with neutral elements*, (Makedonian), Bull. Soc. Math. et Phys. R. P. Macédoine **12** (1961), 15 – 24.

[12] **D. Zupnik**: *Polyadic semigroups*, Publ. Math. (Debrecen), **14** (1967), 273 – 279.

Received December 28, 2005

W. A. Dudek
Institute of Mathematics and Computer Science, Wroclaw University of Technology,
50-370 Wrocław, Poland
E-mail: dudek@im.pwr.wroc.pl

V. V. Mukhin
Department of Mathematics, Cherepovets State University, 162 600 Cherepovets,
Russia
E-mail: mukhin@chsu.ru

Quasigroups and Related Systems **14** (2006), 169 – 178

# Left regular and intra-regular ordered semigroups in terms of fuzzy subsets

*Niovi Kehayopulu and Michael Tsingelis*

## Abstract

In this paper we extend some results concerning ideals of left regular and intra-regular ordered semigroups to fuzzy ordered semigroups. A theory of fuzzy sets on ordered groupoids and ordered semigroups can be developed. Some results on ordered groupoids-semigroups have been already given by the same authors. The aim of writing this paper is to show the way we pass from the theory of ordered semigroups based on ideals or from the theory of *poe*-semigroups (i.e. ordered semigroups having a greatest element "$e$") based on ideal elements to the theory of ordered semigroups based on fuzzy ideals. Then we also have the way we pass from the theory of semigroups based on ideals to the theory of semigroups based on fuzzy ideals.

## 1. Introduction

Given a set $S$, a fuzzy subset of $S$ (or a fuzzy set in $S$) is, by definition, an arbitrary mapping $f : S \to [0, 1]$ where $[0, 1]$ is the usual closed interval of real numbers. If the set $S$ bears some structure, one may distinguish some fuzzy subsets of $S$ in terms of that additional structure. This important concept of the fuzzy set was first introduced by Zadeh in [28]. Since then, many papers on fuzzy sets appeared showing the importance of the concept and its applications to logic, set theory, group theory, groupoids, real analysis, measure theory, topology, etc. The concept of a fuzzy set introduced by Zadeh, was applied in [2] to generalize some of the basic concepts of general topology. Rosenfeld [26] was the first who considered the case when $S$ is a

2000 Mathematics Subject Classification: 06F05, 06D72, 08A72
Keywords: Ordered semigroup; *poe*-semigroup; left regular, intra-regular ordered semigroup; left ideal, ideal; semiprime subset; left ideal element, ideal element, semiprime element in a *poe*-semigroup; fuzzy left ideal, fuzzy semiprime subset.
This research has been supported by the Special Research Account of the University of Athens (grant no. 70/4/5630).

groupoid. He gave the definition of a fuzzy subgroupoid and the fuzzy left (right, two-sided) ideal of $S$ and justified these definitions by showing that a (conventional) subset $A$ of a groupoid $S$ is a (conventional) subgroupoid or a left (right, two-sided) ideal of $S$ if the characteristic function

$$f_A : S \to [0,1] \mid a \to f_A(x) := \begin{cases} 1 & \text{if} \quad x \in A \\ 0 & \text{if} \quad x \notin A \end{cases}$$

is, respectively, a fuzzy subgroupoid or a fuzzy left (right, two-sided) ideal of $S$. Kuroki has been first studied the fuzzy sets on semigroups [19–24]. See also Liu's paper [25] where "fuzzy" analogous of several further important notions, e.g. those of bi-ideals or interior ideals have been defined and justified in a similar fashion. Fuzzy sets on semigroups have been also considered by Kehayopulu, Xie and Tsingelis in [18] and by Kehayopulu and Tsingelis in [10–12,15]. Fuzzy pseudo-symmetric ideals of semigroups and their radicals have been studied by K. P. Shum, Chen Degang and Wu Congxin in [27]. A theory of fuzzy sets on ordered groupoids and ordered semigroups can be developed. We endow $S$ with the structure of an ordered groupoid or semigroup and define "fuzzy" analogous for several notions that have been proved to be useful in the theory of ordered semigroups. Following the terminology given by Zadeh, if $S$ is an ordered groupoid (resp. ordered semigroup), a fuzzy subset of $S$ (or a fuzzy set in $S$) is any mapping of $S$ into the real closed interval [0,1]. Based on the terminology given by Zadeh, fuzzy sets in ordered groupoids have been first considered by Kehayopulu and Tsingelis in [13,16,17]. Moreover, each ordered groupoid can be embedded into an ordered groupoid having a greatest element in terms of fuzzy sets [16]. The aim of writing this paper is to show the way we pass from the theory of ordered semigroups based on ideals to the theory of *poe*-semigroups based on ideal elements, and then to the theory of ordered semigroups based on fuzzy ideals. Then we have the way we pass from the theory of semigroups -without order- based on ideals to the theory of semigroups based on fuzzy ideals. The paper serves as an example to have an easy comparison among the theory of ordered semigroups (or semigroups) based on ideals, the theory of *poe*-semigroups (i.e. ordered semigroups having a greatest element "$e$") based on ideal elements and the theory of ordered semigroups based on fuzzy ideals.

Croisot [4] connects the matter of decompositions of a semigroup $S$ with two other sets of conditions on $S$, regularity and semiprime conditions. Croisot uses the term "inversif" instead of "regular". The following decomposition theorems are well known. A semigroup $S$ is a disjoint union of left simple subsemigroups (equivalently, $S$ is left regular) if and only if every left ideal of $S$ is semiprime. It might be also noted that a semigroup $S$ is left regular if and only it is just a union of left simple subsemigroups of $S$. The results remain true if we replace the word "left" by "right" [3]. A semigroup $S$ is a union of groups, equivalently, a union of disjoint groups if and only if it is both left regular and right regular [3]. A semigroup $S$ is intra-regular if and only if it is a union of simple semigroups (cf. [3]). The characterizations mentioned above can be expressed by means of Green's relations as well. For details we refer to [3]. It has been proved in [7] that a *poe*-semigroup $S$ is left regular if and only if every left ideal element of $S$ is semiprime, equivalently, if every left ideal of $S$ is semiprime. Moreover, a *poe*-semigroup $S$ is left regular if and only if it is a union of left simple subsemigroups of $S$. Exactly as in semigroups, the left regularity of *poe*-semigroups can be expressed in terms of Green's relations as well (cf. [7]). Furthermore, an ordered semigroup $S$ is left regular if and only if every left ideal of $S$ is semiprime, equivalently, if $S$ is a union of left regular subsemigroups of $S$. In addition, an ordered semigroup $S$ is left regular if and only if it is a complete semilattice of left regular and simple semigroups. For details we refer to [14]. The following structure theorem is known as well: An ordered semigroup $S$ is intra-regular if and only if it is a semilattice of simple semigroups, equivalently, if $S$ is a union of simple subsemigroups of $S$ [9]. Moreover, an ordered semigroups $S$ is intra-regular if and only if the ideals of $S$ are semiprime (cf. [9; Remark 3]). In addition, a *poe*-semigroup is a semilattice of simple semigroups if and only if it is a semilattice of simple *poe*-semigroups.

In the present paper we first give some further characterizations of left (resp. right) regular and intra-regular ordered semigroups in terms of right ideals and semiprime subsets, then we characterize the left regular, right regular and intra-regular *poe*-semigroups in terms of left ideal elements, right ideal elements and semiprime ideal elements. Finally we characterize the left regular, right regular and intra-regular ordered semigroups in terms of fuzzy left, fuzzy right ideals and fuzzy semiprime subsets.

By a *poe*-groupoid we mean an ordered groupoid (*po*-groupoid [1]) $S$ having a greatest element "$e$" (i.e. $e \geqslant a \ \forall \ a \in S$). A $\vee$-semigroup is a semigroup at the same time a semilattice under $\vee$ such that $a(b\vee c) = ab\vee ac$ and $(a\vee b)c = ac\vee bc$ for all $a, b, c \in S$ [1]. A *poe*-semigroup or $\vee$e-semigroup is a *po*-semigroup or $\vee$-semigroup having a greatest element "$e$".

## 2. A characterization of left regular and intra-regular ordered semigroups in terms of semiprime left ideals

If $(S,\cdot,\leqslant)$ is an ordered groupoid and $H\subseteq S$, we denote $H$ the subset of $S$ defined as follows:

$$(H]=\{t\in S\mid t\leqslant h \text{ for some } h\in H\}.$$

If $(S,\cdot,\leqslant)$ is an ordered groupoid, a non-empty subset $A$ of $S$ is called a *left* (resp. *right*) ideal of $S$ if 1) $SA\subseteq A$ (resp. $AS\subseteq A$) and 2) If $a\in A$ and $S\ni b\leqslant a$, then $b\in A$. $A$ is called an *ideal* of $S$ if it is both a left and a right ideal of $S$ [6]. For an ordered semigroup $S$, we denote by $L(a)$, $R(a)$, $I(a)$ the left ideal, right ideal, and the ideal of $S$, respectively, generated by $a$ $(a\in S)$. For each $a\in S$, we have $L(a)=(a\cup Sa]$, $R(a)=(a\cup aS]$, and $I(a)=(a\cup Sa\cup aS\cup SaS]$ [6].

An ordered semigroup $(S,\cdot,\leqslant)$ is called *left* regular if for every $a\in S$ there exists $x\in S$ such that $a\leqslant xa^2$ . Equivalent definitions: 1) $A\subseteq(SA^2]$ for every $A\subseteq S$. 2) $a\in(Sa^2]$ for every $a\in S$. An ordered semigroup $(S,\cdot,\leqslant)$ is called *right* regular if for every $a\in S$ there exists $x\in S$ such that $a\leqslant a^2x$. Equivalent definitions: 1) $A\subseteq(A^2S]$ for every $A\subseteq S$. 2) $a\in(a^2S]$ for every $a\in S$ [8]. $S$ is called *intra-regular* if for every $a\in S$ there exist $x,y\in S$ such that $a\leqslant xa^2y$. Equivalent Definitions: 1) $A\subseteq(SA^2S]$ for every $A\subseteq S$. 2) $a\in(Sa^2S]$ for every $a\in S$ [9].

A subset $T$ of an ordered groupoid $S$ is called *semiprime* if $a\in S$, $a^2\in T$ imply $a\in T$. Equivalent Definition: $A\subseteq S$, $A^2\subseteq T$ imply $A\subseteq T$ [7].

**Proposition 2.1.** *For an ordered semigroup $(S,\cdot,\leqslant)$ the following are equivalent:*

1) *$S$ is left regular.*
2) *Every left ideal of $S$ is semiprime.*
3) *$L(a)$ is a semiprime left ideal of $S$ for every $a\in S$.*
4) *$L(a^2)$ is a semiprime left ideal of $S$ for every $a\in S$.*

*Proof.* 1) $\Longrightarrow$ 2). Cf. [14]. It can be independently proved as follows: Let $L$ be a left ideal of $S$ and $a\in S$, $a^2\in L$. Since $S$ is left regular, there exists $x\in S$ such that $a\leqslant xa^2$. Since $a^2\in L$ and $L$ is a left ideal of $S$, we have $xa^2\in SL\subseteq L$. Since $S\ni a\leqslant xa^2\in L$ and $L$ is a left ideal of $S$, we have $a\in L$.

2 $\Longrightarrow$ 3) $\Longrightarrow$ 4). It is obvious.

4) $\Longrightarrow$ 1). Let $a\in S$. Since $a^2\in L(a^2)$ and $L(a^2)$ is semiprime, we have $a\in L(a^2)=(a^2\cup Sa^2]$. Then $a\leqslant a^2$ or $a\leqslant xa^2$ for some $x\in S$. If $a\leqslant a^2$, then $a\leqslant aa\leqslant aa^2$. Thus $S$ is left regular. □

In a similar way we prove the following two propositions.

**Proposition 2.2.** *For an ordered semigroup $(S, \cdot, \leqslant)$ the following are equivalent:*

1) *$S$ is right regular.*
2) *Every right ideal of $S$ is semiprime.*
3) *$R(a)$ is a semiprime right ideal of $S$ for every $a \in S$.*
4) *$R(a^2)$ is a semiprime right ideal of $S$ for every $a \in S$.* □

**Proposition 2.3.** *For an ordered semigroup $(S, \cdot, \leqslant)$ the following are equivalent:*

1) *$S$ is intra-regular.*
2) *Every ideal of $S$ is semiprime.*
3) *$I(a)$ is a semiprime ideal of $S$ for every $a \in S$.*
4) *$I(a^2)$ is a semiprime ideal of $S$ for every $a \in S$.* □

## 3. A characterization of left regular and intra-regular *poe*-semigroups is terms of left ideal elements

An element $a$ of an ordered groupoid $S$ is called a *left* (resp. *right*) *ideal element* if $xa \leqslant a$ (resp. $ax \leqslant x$) for all $x \in S$ [1]. An element which is both a left and a right ideal element is called an *ideal element*. One can easily see that in *poe*-groupoids, an element $a$ is a left (resp. right) ideal element if and only if $ea \leqslant a$ (resp. $ae \leqslant a$) [5]. We denote by $l(a)$, $r(a)$, $i(a)$ the left ideal element, right ideal element and the ideal element of $S$, respectively, generated by $a$ $(a \in S)$. For a $\vee e$-semigroup $S$, we have $l(a) = ea \vee a$, $r(a) = ae \vee a$ and $i(a) = a \vee ea \vee ae \vee eae$ for all $a \in S$ (cf. also [5]).

Let $(S, \cdot, \leqslant)$ be an ordered semigroup. Suppose that $S$ has a greatest element "$e$", that is $S$ is a *poe*-semigroup. Then, one can easily see that $S$ is left (resp. right) regular if and only if $a \leqslant ea^2$ (resp. $a \leqslant a^2e$) for every $a \in S$. $S$ is intra-regular if and only if $a \leqslant ea^2e$ for every $a \in S$. For further information concerning the left, right ideal elements and the left, right regularity and intra-regularity (in *poe*-semigroups) we refer to [5]. An element $t$ of an ordered groupoid $S$ is said to be *semiprime* if for every $a \in S$ such that $a^2 \leqslant t$, we have $a \leqslant t$ [5].

**Proposition 3.1.** *Let $(S, \cdot, \leqslant)$ be a poe-semigroup. We consider the statements:*

1) *$S$ is left regular.*
2) *Every left ideal element of $S$ is semiprime.*

3) *$l(a)$ is a semiprime left ideal element of $S$ for every $a \in S$.*

4) *$l(a^2)$ is a semiprime left ideal element of $S$ for every $a \in S$.*

*Then* 1) $\Longrightarrow$ 2)*. In particular, if $S$ is a $\vee e$-semigroup, then the properties* 1) $-$ 4) *are equivalent.*

*Proof.* 1) $\Longrightarrow$ 2). Let $a$ be a left ideal element of $S$ and $t \in S$ such that $t^2 \leqslant a$. Then, since $S$ is left regular, we have $t \leqslant et^2 \leqslant ea \leqslant a$.

Let now $S$ be a $\vee e$-semigroup. Then

2) $\Longrightarrow$ 3) $\Longrightarrow$ 4). It is obvious.

4) $\Longrightarrow$ 1). Let $a \in S$. Since $a^2 \leqslant l(a^2)$ and $l(a^2)$ is a semiprime element of $S$, by 4), we have $a \leqslant l(a^2) = a^2 \vee ea^2$. Then $a^2 \leqslant a^3 \vee ea^3 \leqslant ea^2$, so $a \leqslant ea^2$, and $S$ is left regular. □

In a similar way the following two propositions hold true.

**Proposition 3.2.** *Let $(S, \cdot, \leqslant)$ be a poe-semigroup. We consider the statements:*

1) *$S$ is right regular.*

2) *Every right ideal element of $S$ is semiprime.*

3) *$r(a)$ is a semiprime right ideal element of $S$ for every $a \in S$.*

4) *$r(a^2)$ is a semiprime right ideal element of $S$ for every $a \in S$.*

*Then* 1) $\Longrightarrow$ 2)*. In particular, if $S$ is a $\vee e$-semigroup, then the properties* 1) $-$ 4) *are equivalent.* □

**Proposition 3.3.** *Let $(S, \cdot, \leqslant)$ be a poe-semigroup. We consider the statements:*

1) *$S$ is intra-regular.*

2) *Every ideal element of $S$ is semiprime.*

3) *$i(a)$ is a semiprime ideal element of $S$ for every $a \in S$.*

4) *$i(a^2)$ is a semiprime ideal element of $S$ for every $a \in S$.*

*Then* 1) $\Longrightarrow$ 2)*. In particular, if $S$ is a $\vee e$-semigroup, then the properties* 1) $-$ 4) *are equivalent.* □

For the equivalence 1) $\Longleftrightarrow$ 2) cf. also [5].

## 4. A characterization of left regular and intra-regular ordered semigroups in terms of fuzzy subsets

If $S$ is a groupoid or an ordered groupoid and $A \subseteq S$, the fuzzy subset $f_A$ of $S$ is the characteristic function of $A$ defined as follows:

$$f_A : S \to [0,1] \mid a \to f_A(x) := \begin{cases} 1 & \text{if} \quad x \in A \\ 0 & \text{if} \quad x \notin A. \end{cases}$$

Let $(S, \cdot, \leqslant)$ be an ordered groupoid. A fuzzy subset $f$ of $S$ is called a *fuzzy left ideal* of $S$ if 1) $f(xy) \geqslant f(y)$ for every $x, y \in S$ and 2) If $x \leqslant y$, then $f(x) \geqslant f(y)$.

A fuzzy subset $f$ of $S$ is called a *fuzzy right ideal* of $S$ if 1) $f(xy) \geqslant f(x)$ for every $x, y \in S$ and 2) If $x \leqslant y$, then $f(x) \geqslant f(y)$ [13].

A fuzzy subset $f$ of $S$ is called a *fuzzy ideal* of $S$ if it is both a fuzzy right and a fuzzy left ideal of S. Equivalent Definition: 1) $f(xy) \geqslant max\{f(x), f(y)\}$ for every $x, y \in S$ and 2) If $x \leqslant y$, then $f(x) \geqslant f(y)$ [13].

**Definition 4.1.** Let $S$ be a groupoid or an ordered groupoid. A fuzzy subset $f$ of $S$ is called *semiprime* if $f(a) \geqslant f(a^2)$ for every $a \in S$.

For an equivalent definition of the semiprime fuzzy subsets we refer to [18].

**Remark 4.2.** If $f$ is a semiprime fuzzy left ideal of $S$, then $f(a) = f(a^2)$ for every $a \in S$. In fact, let $a \in S$. Since $S$ is a fuzzy left ideal of $S$, we have $f(xy) \geqslant f(y)$ for each $x, y \in S$, so $f(a^2) \geqslant f(a)$. Since $f$ is semiprime, we have $f(a) \geqslant f(a^2)$, hence we have $f(a) = f(a^2)$. Similarly, if $f$ is a semiprime fuzzy right ideal of $S$, then $f(a) = f(a^2)$ for every $a \in S$.

**Lemma 4.3.** [13] *A non-empty subset $L$ of an ordered groupoid $(S, \cdot, \leqslant)$ is a left ideal of $S$ if and only if the characteristic function $f_L$ is a fuzzy left ideal of $S$.*

**Lemma 4.4.** *A non-empty subset $R$ of an ordered groupoid $(S, \cdot, \leqslant)$ is a right ideal of $S$ if and only if the characteristic function $f_R$ is a fuzzy right ideal of $S$.* □

**Lemma 4.5.** (Cf. also [18]) *A non-empty subset $A$ of a groupoid $(S, .)$ or an ordered groupoid $(S, \cdot, \leqslant)$ is a semiprime subset of $S$ if and only if the fuzzy subset $f_A$ of $S$ is semiprime.* □

**Proposition 4.6.** *An ordered semigroup $(S, \cdot, \leqslant)$ is left (resp. right) regular if and only if the fuzzy left (resp. fuzzy right) ideals of $S$ are semiprime.*

*Proof.* Let $S$ be left regular, $f$ a fuzzy left ideal of $S$ and $a \in S$. Since $S$ is left regular, there exists $x \in S$ such that $a \leqslant xa^2$. Then, since $f$ is a fuzzy left ideal of $S$, we have $f(a) \geqslant f(xa^2) \geqslant f(a^2)$. Thus $f$ is semiprime.

Conversely, let $a \in S$. Since $L(a^2)$ is a left ideal of $S$, by Lemma 4.3, the characteristic function $f_{L(a^2)}$ is a fuzzy left ideal of $S$. By hypothesis, $f_{L(a^2)}$ is semiprime. By Lemma 4.5, $L(a^2)$ is a semiprime left ideal of $S$. Then, by Proposition 2.1, $S$ is left regular.

In a similar way we prove $S$ is right regular if and only it the fuzzy right ideals of $S$ are semiprime. □

**Remark 4.7.** Each of the following two conditions also characterizes the left regular ordered semigroups.

1) $f_{L(a)}$ is a semiprime fuzzy left ideal of $S$ for every $a \in S$.
2) $f_{L(a^2)}$ is a semiprime fuzzy left ideal of $S$ for every $a \in S$.

**Remark 4.8.** Each of the following two conditions also characterizes the right regular ordered semigroups.

1) $f_{R(a)}$ is a semiprime fuzzy right ideal of $S$ for every $a \in S$.
2) $f_{R(a^2)}$ is a semiprime fuzzy right ideal of $S$ for every $a \in S$.

In a similar way we have the following:

**Proposition 4.9.** *An ordered semigroup $S$ is intra-regular if and only if the fuzzy ideals of $S$ are semiprime.* □

**Remark 4.10.** Each of the following two conditions also characterizes the intra-regular ordered semigroups.

1) $f_{I(a)}$ is a semiprime fuzzy ideal of $S$ for every $a \in S$.
2) $f_{I(a^2)}$ is a semiprime fuzzy ideal of $S$ for every $a \in S$. □

**Acknowledgement.** We would like to express our warmest thanks to the editor of the journal Professor Wieslaw A. Dudek for editing, communicating the paper and the useful discussions concerning this paper we had. We also express our warmest thanks to the referee of the paper for his time to read the paper very carefully and his useful comments.

## References

[1] **G. Birkhoff:** *Lattice Theory*, Amer. Math. Soc., Coll. Publ., Vol. **XXV**, Providence, Rhode Island, 1967.

[2] **C. I. Chang:** *Fuzzy topological space*, J. Math. Anal. Appl. **24** (1965), 338 − 353.

[3] **A. H. Clifford and G.B. Preston:** *The Algebraic Theory of Semigroups* Vol. **I**, Amer. Math. Soc., Providence, Rh. Island (1961), Math. Surveys 7.

[4] **R. Croisot:** *Demi-groupes inversifs et demi-groupes réunions des demi-groupes simples*, Ann. Sci. École Norm. Sup. **70** (1953), 361 – 379.

[5] **N. Kehayopulu:** *On intra-regular* $\vee e$*-semigroups*, Semigroup Forum **19** (1980), 111 – 121.

[6] **N. Kehayopulu:** *On weakly prime ideals of ordered semigroups*, Math. Japonica **35** (1990), 1051 – 1056.

[7] **N. Kehayopulu:** *On left regular ordered semigroups*, Math. Japonica **35** (1990), 1057 – 1060.

[8] **N. Kehayopulu:** *On right regular and right duo ordered semigroups*, Math. Japonica **36** (1991), 201 – 206.

[9] **N. Kehayopulu:** *On intra-regular ordered semigroups*, Semigroup Forum **46** (1993), 271 – 278.

[10] **N. Kehayopulu and M. Tsingelis:** *A note on fuzzy sets in semigroups*, Sci. Math. **2** (1999), 411 – 413 (electronic).

[11] **N. Kehayopulu and M. Tsingelis:** *A characterization of weakly prime and weakly semiprime ideals of semigroups in terms of fuzzy subsets*, Sovremennaja Algebra **4** (1999), no. 24, 85 – 88.

[12] **N. Kehayopulu and M. Tsingelis:** *A note on fuzzy sets of groupoids-semigroups*, Sci. Math. **3** (2000), 247 – 250 (electronic).

[13] **N. Kehayopulu and M. Tsingelis:** *Fuzzy sets in ordered groupoids*, Semigroup Forum **65** (2002), 128 – 132.

[14] **N. Kehayopulu and M. Tsingelis:** *On left regular ordered semigroups*, Southeast Asian Bull. Math. **25** (2002), 609 – 615.

[15] **N. Kehayopulu and M. Tsingelis:** *On semigroups which are groups*, J. Fuzzy Math. **11** (2003), 751 – 755.

[16] **N. Kehayopulu and M. Tsingelis:** *The embedding of an ordered groupoid into a poe-groupoid in terms of fuzzy sets*, Inform. Sci. **152** (2003), 231 – 236.

[17] **N. Kehayopulu and M. Tsingelis:** *Fuzzy bi-ideals in ordered semigroups*, Inform. Sci. **171** (2005), 13 – 28.

[18] **N. Kehayopulu, X.-Y. Xie and M. Tsingelis:** *A characterization of prime and semiprime ideals of semigroups in terms of fuzzy subsets*, Soochow J. Math. **27** (2001), 139 – 144.

[19] **N. Kuroki:** *Fuzzy bi-ideals in semigroups*, Comment. Math. Univ. St. Pauli **28** (1980), 17 – 21.

[20] **N. Kuroki:** *On fuzzy ideals and fuzzy bi-ideals in semigroups*, Fuzzy Sets and Systems **5** (1981), 203 – 215.

[21] **N. Kuroki:** *Fuzzy semiprime ideals in semigroups*, Fuzzy Sets and Systems **8** (1982), 71 – 79.

[22] **N. Kuroki:** *On fuzzy semigroups*, Inform. Sci. **53** (1991), 203 – 236.

[23] **N. Kuroki:** *Fuzzy generalized bi-ideals in semigroups*, Inform. Sci. **66** (1992), 235 – 243.

[24] **N. Kuroki:** *Fuzzy semiprime quasi-ideals in semigroups*, Inform. Sci. **75** (1993), 201 – 211.

[25] **W.-J. Liu:** *Fuzzy invariant subgroups and fuzzy ideals*, Fuzzy Sets and Systems **8** (1982), 133 – 139.

[26] **A. Rosenfeld:** *Fuzzy groups*, J. Math. Anal. Appl. **35** (1971), 512 – 517.

[27] **K. P. Shum, Chen Degang and Wu Congxin:** *Fuzzy pseudo-symmetric ideals of semigroups and their radicals* (Chinese), Mohu Xitong yu Shuxue, **13** (1999), 1 – 3.

[28] **L. A. Zadeh:** *Fuzzy sets*, Inform. and Control **8** (1965), 338 – 353.

Received November 14, 2005

University of Athens, Department of Mathematics, 157 84 Panepistimiopolis, Greece
E-mail: nkehayop@math.uoa.gr

Quasigroups and Related Systems **14** (2006), 179 – 190

# On the prime graph of $L_2(q)$ where $q = p^\alpha < 100$

Behrooz Khosravi and Seyyed Sadegh Salehi Amiri

**Abstract**

Let $G$ be a finite group. We construct the prime graph of $G$ as follows: the vertices of this graph are the prime divisors of $|G|$ and two vertices $p$ and $q$ are joined by an edge if and only if $G$ contains an element of order $pq$. The prime graph of $G$ is denoted by $\Gamma(G)$.

Mina Hagie (Comm. Algebra, 2003) determined finite groups $G$ such that $\Gamma(G) = \Gamma(S)$, where $S$ is a sporadic simple group. In this paper we determine finite groups $G$ such that $\Gamma(G) = \Gamma(L_2(q))$ for some $q < 100$.

## 1. Introduction

Let $G$ be a finite group. We denote by $\pi(G)$ the set of all prime divisors of $|G|$. If $|\pi(G)| = n$, then $G$ is called a $K_n-$*group*.

The *prime graph* (Gruenberg-Kegel graph) $\Gamma(G)$ of a group $G$ is the graph whose vertex set is $\pi(G)$, and two distinct primes $p$ and $q$ are joined by an edge (we write $p \sim q$) if and only if $G$ contains an element of order $pq$. Let $t(G)$ be the number of connected components of $\Gamma(G)$ and let $\pi_1$, $\pi_2$, ..., $\pi_{t(G)}$ be the connected components of $\Gamma(G)$. If $2 \in \pi(G)$, then we always suppose $2 \in \pi_1$. Also the set of orders of the elements of $G$ is denoted by $\pi_e(G)$. Obviously $\pi_e(G)$ is partially ordered by divisibility. Therefore it is uniquely determined by $\mu(G)$, the subset of its maximal elements. We know that $\mu(L_2(q)) = \{p, (q-1)/d, (q+1)/d\}$ and $\mu(PGL(2,q)) = \{p, (q-1), (q+1)\}$ where $q = p^\alpha$ and $d = (2, q-1)$. Also we know that the prime graph components of $L_2(q)$ are cliques (i.e., complete subgraphs).

The structure of finite groups $G$ with disconnected prime graph has been determined by Gruenberg and Kegel (1975) and they have been described

2000 Mathematics Subject Classification: 20D05, 20D60, 20D08

Keywords: Prime graph, order elements, simple group, linear group.

in [9, 13, 16]. It has been proved that $t(G) \leqslant 6$ [9, 13, 16], and we know that the diameter of $\Gamma(G)$ is at most 5 (see[14]).

Mina Hagie in [8] determined finite groups $G$ such that $\Gamma(G) = \Gamma(S)$ where $S$ is a sporadic simple group. Also in [12] finite groups were determined which have the same prime graph as a CIT simple group. In this paper we determine finite groups $G$ such that $\Gamma(G) = \Gamma(L_2(q))$, where $q < 100$ is a prime power. Throughout this paper we denote by $(a, b)$, the greatest common divisor of $a$ and $b$.

## 2. Preliminary results

**Lemma 2.1.** ([5]) *Let $G$ be a finite group, $H$ a subgroup of $G$ and $N$ a normal subgroup of $G$. Then*

(1) *if $p$ and $q$ are joined in $\Gamma(H)$, then $p$ and $q$ are joined in $\Gamma(G)$;*

(2) *if $p$ and $q$ are joined in $\Gamma(G/N)$, then $p$ and $q$ are joined in $\Gamma(G)$.*

*In fact if $xN \in G/N$ has order $pq$, then there is a power of $x$ which has order $pq$.*

**Lemma 2.2.** ([1]) *If $G$ is a simple $K_3-$group, then $G$ is isomorphic to one of the following groups: $A_5$, $A_6$, $L_2(7)$, $L_2(8)$, $L_2(17)$, $L_3(3)$, $U_3(3)$ and $U_4(2)$.*

**Lemma 2.3.** ([1]) *If $G$ is a simple $K_4-$group, then $G$ is isomorphic to one of the following groups:*
*$A_7$, $A_8$, $A_9$, $A_{10}$, $M_{11}$, $M_{12}$, $J_2$, $L_3(4)$, $L_3(5)$, $L_3(7)$, $L_3(8)$, $L_3(17)$, $L_4(3)$, $O_5(4)$, $O_5(5)$, $O_5(7)$, $O_5(9)$, $O_7(2)$, $O_8^+(2)$, $G_2(3)$, ${}^3D_4(2)$, ${}^2F_4(2)'$, $Sz(8)$, $Sz(32)$, $U_3(4)$, $U_3(5)$, $U_3(7)$, $U_3(8)$, $U_3(9)$, $U_4(3)$, $U_5(2)$, $L_2(q)$,*
*where $q$ is a prime power satisfying $q(q^2-1) = (2, q-1)2^{\alpha_1}3^{\alpha_2}p^{\alpha_3}r^{\alpha_4}$, $\alpha_i \in \mathbb{N}$ $(1 \leqslant i \leqslant 4)$ and 2, 3, $p$, $r$ are distinct primes.*

The next lemma is an immediate consequence of Theorem A in [16]:

**Lemma 2.4.** *If $G$ is a finite group whose prime graph is disconnected, then one of the following holds: $G$ is a Frobenius group or a $2-$Frobenius group; or $G$ has a normal series $1 \trianglelefteq N \trianglelefteq M \trianglelefteq G$ such that $G/M$ and $N$ are $\pi_1-$groups, $N$ is a nilpotent $\pi_1-$group and $M/N$ is a non-abelian simple group.*

**Corollary 2.1.** [16] *If $G$ is a solvable group with disconnected prime graph, then $t(G) = 2$ and $G$ is either Frobenius or $2-$Frobenius group and $G$ has* *exactly two components, one of which consists of the primes dividing the lower Frobenius complement.*

The next lemma follows from [2] and the structure of Frobenius complements:

**Lemma 2.5.** *Let $G$ be a Frobenius group of even order and let $H$, $K$ be Frobenius complement and Frobenius kernel of $G$, respectively. Then $t(G) = 2$ and the prime graph components of $G$ are $\pi(H)$, $\pi(K)$ and $G$ has one of the following structures:*

($a$) $2 \in \pi(K)$ *and all Sylow subgroups of $H$ are cyclic;*

($b$) $2 \in \pi(H)$, *$K$ is an abelian group, $H$ is a solvable group, the Sylow subgroups of odd order of $H$ are cyclic groups and the $2-$Sylow subgroups of $H$ are cyclic or generalized quaternion groups;*

($c$) $2 \in \pi(H)$, *$K$ is an abelian group and there exists $H_0 \leqslant H$ such that $|H : H_0| \leqslant 2$, $H_0 = Z \times SL(2, 5)$, $\pi(Z) \cap \{2, 3, 5\} = \emptyset$ and the Sylow subgroups of $Z$ are cyclic.*

Also the next lemma follows from [2] and the properties of Frobenius groups:

**Lemma 2.6.** *Let $G$ be a $2-$Frobenius group of even order, i.e. $G$ has a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$, such that $K$ and $G/H$ are Frobenius groups with kernels $H$ and $K/H$, respectively. Then*

($a$) *$t(G) = 2$, $\pi_1 = \pi(G/K) \cup \pi(H)$ and $\pi_2 = \pi(K/H)$;*

($b$) *$G/K$ and $K/H$ are cyclic, $|G/K| \mid (|K/H|-1)$ and $G/K \leqslant Aut(K/H)$;*

($c$) *$H$ is nilpotent and $G$ is a solvable group.*

**Lemma 2.7.** *Let $L$ be a finite group with $t(L) = 3$. If $G$ is a finite group such that $\Gamma(G) = \Gamma(L)$, then $G$ has a normal series $1 \trianglelefteq N \trianglelefteq M \trianglelefteq G$ such that $G/M$ and $N$ are $\pi_1-$groups, $N$ is a nilpotent $\pi_1-$group and $M/N$ is a non-abelian simple group, where $t(M/N) \geqslant 3$. Also $|G/M| \mid |Out(M/N)|$.*

*Proof.* The first part of theorem follows from the above lemmas. Since $t(G) = 3$, it follows that $t(G/N) \geqslant 3$. Moreover, we have $Z(G/N) = 1$. For any $xN \in G/N$ and $xN \notin M/N$, $xN$ induces an automorphism of $M/N$ and this automorphism is trivial if and only if $xN \in Z(G/N)$. Therefore $G/M \leqslant Out(M/N)$ and since $Z(G/N) = 1$, the result follows. □

**Lemma 2.8.** ([7]) *The equation $p^m - q^n = 1$, where $p$ and $q$ are prime numbers and $m, n > 1$, has only one solution, namely $3^2 - 2^3 = 1$.*

**Lemma 2.9.** ([7]) *With the exceptions of the relations* $(239)^2-2(13)^4=-1$ *and* $(3)^5-2(11)^2=1$ *every solution of the equation* $p^m-2q^n=\pm1$*;* $p$*,* $q$ *prime;* $m,n\geqslant 1$*, has exponents* $m=n$*=2.*

**Lemma 2.10.** (Zsigmondy Theorem) ([17]) *Let* $p$ *be a prime and* $n$ *be a positive integer. Then one of the following holds:*

$(i)$ *there is a prime* $p'$ *such that* $p'|(p^n-1)$ *but* $p'\nmid(p^m-1)$ *for every* $1\leqslant m<n$*;*

$(ii)$ $p=2$*,* $n=1$ *or 6;*

$(iii)$ $p$ *is a Mersenne prime and* $n=2$*.*

**Lemma 2.11.** ([15, Proposition 3.2]) *Let* $G$ *be a finite group and* $H$ *a normal subgroup of* $G$*. Suppose* $G/H$ *is isomorphic to* $PSL(2,q)$*,* $q$ *odd and* $q>5$*, and that an element* $t$ *of order* 3 *in* $G\backslash H$ *has no fixed points on* $H$*. Then* $H=1$*.*

## 3. Main results

In this section we determine finite groups $G$ satisfying $\Gamma(G)=\Gamma(L_2(q))$, where $q<100$ is a prime power.

**Theorem 3.1.** *Let* $L$*=* $L_2(q)$ *where* $q<100$*. If* $G$ *is a non-abelian simple group such that* $\Gamma(G)$ *is a subgraph of* $\Gamma(L)$ *and* $\pi_i(L)\subseteq\pi_i(G)$ *for* $2\leqslant i\leqslant 3$*, then* $G$ *is one of the groups in the* 2nd *column of Table* 1*.*

In the table, $X$ is one of the following non-abelian simple groups: $L_2(q)$ such that $q=p^\alpha$ is a prime power and $q\neq 7^2$, $16\leqslant q<100$.

*Proof.* By assumptions we have $\pi(G)\subseteq\pi(L)$. We consider three steps:

Step 1. If $|\pi(L)|=3$, then $L\cong L_2(5)$, $L_2(7)$, $L_2(8)$, $L_2(9)$ or $L_2(17)$, by Lemma 2.2. Also $G$ is a simple $K_3-$group, since $G$ is a non-abelian simple group. Now by using the atlas of finite groups [6], it follows that the result holds.

Table 1.

| $L$ | $G$ | $L$ | $G$ |
|---|---|---|---|
| $L_2(5)$ | $L_2(5)$, $L_2(9)$ | $L_2(11)$ | $L_2(11)$, $M_{11}$ |
| $L_2(7)$ | $L_2(7)$, $L_2(8)$ | $L_2(13)$ | $L_2(13)$, $G_2(3)$ |
| $L_2(8)$ | $L_2(7)$, $L_2(8)$ | $L_2(49)$ | $A_7$, $L_2(49)$, $L_3(4)$, $U_4(3)$ |
| $L_2(9)$ | $L_2(5)$, $L_2(9)$ | $X$ | $X$ |

Step 2. If $|\pi(L)|$=4, then $L$ is isomorphic to one of the following groups: $L_2(11)$, $L_2(13)$, $L_2(16)$, $L_2(19)$, $L_2(23)$, $L_2(25)$, $L_2(27)$, $L_2(31)$, $L_2(32)$, $L_2(37)$, $L_2(47)$, $L_2(49)$, $L_2(53)$, $L_2(73)$, $L_2(81)$ and $L_2(97)$, by Lemma 2.3. Since $G$ is a non-abelian simple group and $\Gamma(G)$ is a subgraph of $\Gamma(L)$, it follows that $G$ is a simple $K_3-$group or a simple $K_4-$group. For each $L$, there exists a prime number $p$ in $\pi_i(L)$, for $2 \leqslant i \leqslant 3$, which is not in $\pi(G)$, for every simple $K_3-$group $G$ [6]. So $G$ is a simple $K_4-$group. Then $G$ is one of the groups listed in Lemma 2.3. Since the proofs of these cases are similar, we do only one of them, namely $L_2(11)$.

Let $L = L_2(11)$ and $G$ be a simple $K_4-$group such that $\Gamma(G)$ is a subgraph of $\Gamma(L)$. Since $G$ and $L$ are $K_4-$groups, it follows that $\pi(G) = \pi(L)$. Therefore $\pi(G) = \{2, 3, 5, 11\}$. Hence by using Lemma 2.3 and [6], it follows that $G \cong M_{11}, M_{12}, U_5(2)$ or $L_2(q)$ where $q$ is a prime power satisfying $q(q^2 - 1) = (2, q - 1)2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}11^{\alpha_4}$, where $\alpha_i \in \mathbb{N}$ $(1 \leqslant i \leqslant 4)$. We know that $2 \sim 5$ in $M_{12}$ and $3 \sim 5$ in $U_5(2)$, but $2 \not\sim 5$ and $3 \not\sim 5$ in $\Gamma(L)$. Hence $G \cong M_{11}$ or $G \cong L_2(q)$ where $q$ is a prime power satisfying $q(q^2 - 1) = (2, q - 1)2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}11^{\alpha_4}$, where $\alpha_i \in \mathbb{N}$ $(1 \leqslant i \leqslant 4)$.

If $\Gamma(G) = \Gamma(L_2(q))$ is a subgraph of $\Gamma(L)$, it follows that $\Gamma(L_2(11)) = \Gamma(L_2(q))$, since the components of $L_2(q)$ are cliques. Now we prove that $q$=11. We know that $\mu(L_2(11)) = \{5, 6, 11\}$. Note that $\{p\}$ is a prime graph component of $G \cong L_2(q)$ where $q = p^\alpha$, and so $p \not\sim p'$ for every prime number $p' \neq p$. As $\Gamma(L_2(11)) = \Gamma(L_2(q))$, it follows that $\Gamma(L_2(q))$ has the same components as $\Gamma(L_2(11))$. Also $2 \sim 3$ in $\Gamma(L_2(11))$ and hence $q \neq 2^\alpha$ and $q \neq 3^\alpha$ where $\alpha \in \mathbb{N}$. Therefore $q = 5^\alpha$ or $q = 11^\beta$ for some $\alpha, \beta \in \mathbb{N}$.

If $q = 5^\alpha$, then $4 \mid (q - 1)$ and so $\mu(L_2(q)) = \{5, (5^\alpha - 1)/2, (5^\alpha + 1)/2\}$. Also 2 divides $(5^\alpha - 1)/2$ and hence $2 \in \pi((5^\alpha - 1)/2)$. Therefore $(5^\alpha + 1)/2 = 11^k$ for some $k > 0$. Then $5^\alpha - 2 \cdot 11^k = -1$ and as this diophantine equation has no solution, by Lemma 2.9, we have a contradiction. If $q = 11^\beta$, then we consider two cases: if $\beta$ is even, then $4 \mid (11^\beta - 1)$ and so $2 \mid (11^\beta - 1)/2$ which implies that $(11^\beta + 1)/2 = 5^k$, for some $k > 0$. Again by using Lemma 2.9 we get a contradiction. If $\beta$ is odd, then $2 \mid (11^\beta + 1)/2$ and hence $(11^\beta - 1)/2 = 5^k$, for some $k > 0$. Now by using Lemma 2.9, it follows that $\beta = k$=1. Therefore $G \cong L_2(11)$ and the result follows.

The proof of the other cases are similar and we omit them for convenience.

Step 3. Let $|\pi(L)| = 5$. Now by using [6], we can see that $L$ is isomorphic to one of groups $L_2(29)$, $L_2(41)$, $L_2(43)$, $L_2(59)$, $L_2(61)$, $L_2(64)$, $L_2(67)$, $L_2(71)$, $L_2(79)$, $L_2(83)$ or $L_2(89)$. In Steps 1 and 2 we use Lemmas 2.2 and

2.3. But in this step we have no result about simple $K_5-$group. Therefore we use the following method to get the result. Since $\Gamma(L)$ has three components and $\pi_i(L) \subseteq \pi_i(G)$ for $2 \leqslant i \leqslant 3$, it follows that $\Gamma(G)$ has at least three components, by Lemma 2.1. Now by using the table of non-abelian simple groups with at least three components (see [10]), we consider all possibilities. Again the proof of these cases are similar and for convenience we do one of them, namely $L_2(29)$.

Let $L = L_2(29)$. We know that $\mu(L_2(29)) = \{29, 14, 15\}$. If $G \cong A_p$ where $p$ and $p-2$ are prime numbers, then we get a contradiction, since $2, 3 \in \pi_1(A_p)$ and $\Gamma(G)$ is a subgraph of $\Gamma(L_2(29))$. If $G \cong A_1(q)$ where $4 \mid (q+1)$, then $q = 29^k$ or $(q-1)/2 = 29^k$ for some $k \in \mathbb{N}$. Since $4 \nmid (29^k + 1)$, thus $q \neq 29^k$. So $(q-1)/2 = 29^k$. Then the third component of $\Gamma(G)$ is $\pi(q) = \{3, 5\}$, which is a contradiction, since $q$ is a prime power. If $G \cong A_1(q)$ where $4 \mid (q-1)$, then $q = 29^k$ or $(q+1)/2 = 29^k$. First let $q = 29^k$ and $k > 1$. Then $q - 1 = 29^k - 1$ has a prime divisor $p$ where $p \notin \{2, 7\}$, by Zsigmondy theorem, which is a contradiction. If $k$=1, then $G \cong L_2(29)$. If $(q+1)/2 = 29^k$, then $\pi(q) = \{3, 5\}$, which is a contradiction. If $G \cong A_1(q)$ where $4 \mid q$, then $q - 1 = 29^k$ or $q + 1 = 29^k$ and these diophantine equations have no solution by Lemma 2.8, a contradiction. If $G \cong {}^2B_2(q)$ where $q = 2^{2n+1} > 2$, then $q-1$ is equal to a power of 3, 5, 7, 29 or $q-1 = 3^\alpha 5^\beta$ for some, $\alpha$, $\beta \in \mathbb{N}$. The equation $q-1 = 7^\alpha$ has only one solution, namely $\alpha = n = 1$. Since $29 \notin \pi(Sz(8))$, we get a contradiction. Also the diophantine equations $q-1 = 3^\alpha$, $q-1 = 5^\beta$ or $q-1 = 29^\gamma$ have no solution by Lemma 2.8. If $q - 1 = 3^\alpha 5^\beta$, then $3 \mid (2^2 - 1)$, $5 \mid (2^4 - 1)$ and so $q-1$ has a prime divisor, except 3, 5 for every $n > 2$ by Zsigmondy theorem, which is a contradiction. Also $29 \notin \pi(Sz(32))$ and so $n \neq 2$. Therefore this case is impossible. Since the cases ${}^2D_p(3)$ where $p = 2^n + 1$, $n \geqslant 2$, ${}^2D_{p+1}(2)$ where $p = 2^n - 1$, $n \geqslant 2$, $G_2(q)$ where $3 \mid q$ and ${}^2G_2(q)$ where $q = 3^{2n+1}$ have similar proofs, we consider only one of them, namely ${}^2D_p(3)$. If $G \cong {}^2D_p(3)$ where $p = 2^n + 1$, $n \geqslant 2$, then $2, 3 \in \pi_1({}^2D_p(3))$. Since $\Gamma(G)$ is a subgraph of $\Gamma(L_2(29))$ and $2 \not\sim 3$ in $\Gamma(L_2(29))$, we get a contradiction.

If $G \cong F_4(q)$ such that $2 \mid q$, $q > 2$, then $\pi_1(G)$ contains at least three prime numbers, by Zsigmondy theorem. Since $\Gamma(G)$ is a subgraph of $\Gamma(L_2(29))$, this gives a contradiction.

By the same method we can show that $G \not\cong {}^2F_4(q)$ where $q = 2^{2n+1} > 2$.

Since $\pi_i(L) \subseteq \pi_i(G)$ for $i$=2,3, it follows that $G$ is not isomorphic to the following groups: $A_2(2)$, $A_2(4)$, ${}^2A_5(2)$, $E_7(2)$, $E_7(3)$, ${}^2E_6(2)$, $M_{11}$, $M_{22}$,

$M_{23}$, $M_{24}$, $J_1$, $J_3$, $J_4$, $HS$, $Sz$, $ON$, $Ly$, $Co_2$, $F_{23}$, $F'_{24}$, $M$, $B$ or $Th$.

If $G \cong E_8(q)$, then $\pi_1(G)$ contains at least three prime numbers by Zsigmondy theorem, which is a contradiction. Now the proof of this theorem is complete. □

**Corollary 3.1.** *Let $L= L_2(q)$, where $q < 100$ and $G$ be a finite simple group such that $|G| = |L|$. Then $G$ is isomorphic to $L$.*

*Proof.* Straightforward from Theorem 3.1. □

**Theorem 3.2.** *Let $L= L_2(q)$, where $q < 100$ and $G$ be a finite group satisfying $\Gamma(G) = \Gamma(L)$. Then $G$ is one of the groups in 2nd column of Table 2 ($\overline{G}$ means $G/O_\pi(G)$).*

*Proof.* Since $t(L) \geqslant 3$, we can apply Lemma 2.4. Also note that $G$ is neither a Frobenius group nor a 2-Frobenius group by Lemmas 2.5 and 2.6. Therefore $G$ has a normal series $1 \trianglelefteq N \trianglelefteq M \trianglelefteq G$ such that $G/M$ and $N$ are $\pi_1-$groups, $N$ is a nilpotent $\pi_1-$group and $M/N$ is a non-abelian simple group, such that $M/N$ satisfies the following conditions:

$$\left\{\begin{array}{ll} (1) & \Gamma(M/N) \text{ is a subgraph of } \Gamma(G); \\ (2) & \pi_i(L) \subseteq \pi_i(G) \subseteq \pi(L) \text{ for } i = 2,\ 3; \\ (3) & \Gamma(G) = \Gamma(L). \end{array}\right. \qquad (*)$$

Case I. Since $L_2(5)$ and $L_2(9)$ have the same prime graph, we only consider one of them. So let $L = L_2(5)$. By $(*)$ and Theorem 3.1, it follows that $M/N \cong L_2(5)$ or $M/N \cong L_2(9)$. First let $M/N \cong L_2(5)$. We note that $Out(L_2(5)) \cong Z_2$ [6]. Therefore $G/M \leqslant Out(L_2(5)) \cong Z_2$, by Lemma 2.7. If $G/M \cong Z_2$, then since $L_2(5).2$ has an element of order 6, it follows that $\Gamma(L_2(5).2)$ is not a subgraph of $\Gamma(L)$. Thus $G = M$ and $G/O_\pi(G) \cong L_2(5)$ Where $\pi \subseteq \{2\}$. Let $M/N \cong L_2(9)$. We know that $Out(L_2(9)) \cong Z_2 \times Z_2$ and there exists three involutions in $Z_2 \times Z_2$.

By using the notations of atlas $L_2(9).2_1$ and $L_2(9).2_2$ have elements of order 6 and 10, respectively [6]. Thus $\Gamma(L_2(9).2_1)$ and $\Gamma(L_2(9).2_2)$ are not subgraphs of $\Gamma(L)$, and $G = M$. By the atlas of finite groups, $\Gamma(L_2(9)) = \Gamma(L_2(9).2_3)$. So $G/N \cong L_2(9)$ or $G/N \cong L_2(9).2_3$. If $2 \in \pi(N)$, then let $P \in Syl_2(N)$ and $Q \in Syl_3(G)$. Since $N$ is a nilpotent group, $P$ *char* $N$ and $N \trianglelefteq G$, we conclude that $P \trianglelefteq G$. Also $2 \not\sim 3$ in $\Gamma(L)$, so $Q$ acts fixed point freely on $P$. Hence $QP$ is a Frobenius group, with kernel $P$ and complement Frobenius $Q$. Therefore $Q$ is cyclic. This is a contradiction since $L_2(9)$ has no element of order 9. Hence we have $N$=1 and $G \cong L_2(9)$ or $L_2(9).2_3$.

Table 2.

| $L$ | $G$ |
|---|---|
| $L_2(5)$ | $\overline{G} \cong L_2(5)$, $\pi \subseteq \{2\}$ $L_2(9)$, $L_2(9).2_3$ |
| $L_2(7)$ | $L_2(7)$ or $\overline{G} \cong L_2(8)$ $\pi \subseteq \{2\}$ |
| $L_2(8)$ | $L_2(7)$ or $\overline{G} \cong L_2(8)$ $\pi \subseteq \{2\}$ |
| $L_2(9)$ | $\overline{G} \cong L_2(5)$, $\pi \subseteq \{2\}$ $L_2(9)$, $L_2(9).2_3$ |
| $L_2(11)$ | $L_2(11)$ or $M_{11}$ |
| $L_2(13)$ | $\overline{G} \cong L_2(13)$ or $G_2(3)$ $\pi \subseteq \{2,3\}$ |
| $L_2(16)$ | $\overline{G} \cong L_2(16)$, $\pi \subseteq \{2\}$ |
| $L_2(17)$ | $L_2(17)$ |
| $L_2(19)$ | $L_2(19)$ |
| $L_2(23)$ | $L_2(23)$ |
| $L_2(25)$ | $L_2(25)$, $L_2(25).2_3$ |
| $L_2(27)$ | $L_2(27)$ |
| $L_2(29)$ | $L_2(29)$ |
| $L_2(31)$ | $L_2(31)$ |
| $L_2(32)$ | $\overline{G} \cong L_2(32)$, $\pi \subseteq \{2\}$ |
| $L_2(37)$ | $\overline{G} \cong L_2(37)$, $\pi \subseteq \{2,3\}$ |
| $L_2(41)$ | $L_2(41)$ |
| $L_2(43)$ | $L_2(43)$ |
| $L_2(47)$ | $L_2(47)$ |
| $L_2(49)$ | $L_2(49)$, $L_2(49).2_3$, $\overline{G} \cong L_3(4)$, $L_3(4).2'_2$ $L_3(4).2''_3$, $L_3(4).2''_2$, $L_3(4).2'_3$, $U_4(3)$, $U_4(3).2_3$, $A_7$ $\pi \subseteq \{2,3\}$ |
| $L_2(53)$ | $L_2(53)$ |
| $L_2(59)$ | $L_2(59)$ |
| $L_2(61)$ | $\overline{G} \cong L_2(61)$, $\pi \subseteq \{2,3,5\}$ |
| $L_2(64)$ | $\overline{G} \cong L_2(64))$, $\pi \subseteq \{2\}$ |
| $L_2(67)$ | $L_2(67)$ |
| $L_2(71)$ | $L_2(71)$ |
| $L_2(73)$ | $\overline{G} \cong L_2(73)$, $\pi \subseteq \{2,3\}$ |
| $L_2(79)$ | $L_2(79)$ |
| $L_2(81)$ | $L_2(81)$ , $L_2(81).2_3$ |
| $L_2(83)$ | $L_2(83)$ |
| $L_2(89)$ | $L_2(89)$ |
| $L_2(97)$ | $\overline{G} \cong L_2(97)$, $\pi \subseteq \{2,3\}$ |

Case II. Since $L_2(7)$ and $L_2(8)$ have the same graph, we only consider one of them. So let $L = L_2(7)$. By $(*)$ and Theorem 3.1 it follows that $M/N \cong L_2(7)$ or $M/N \cong L_2(8)$. First let $M/N \cong L_2(7)$. Therefore $G/M \leqslant Out(L_2(7)) \cong Z_2$ by Lemma 2.7. Since $L_2(7).2$ has an element of order 6, $\Gamma(L_2(7).2)$ is not a subgraph of $\Gamma(L)$, thus $G = M$. We know that $N$ is a 2−group. If $2 \in \pi(N)$, then $M$ has a solvable $\{2,3,7\}$−subgroup $H$, since $L_2(7)$ contains a 7:3 subgroup [6]. Since there exist no edge between 2, 3 and 7 in $\Gamma(L)$, it follows that $t(H)$= 3, a contradiction since $t(H) \leqslant 2$, by Remark 2.1. Therefore $N = 1$ and $G = L_2(7)$. Let $M/N \cong L_2(8)$. As $L_2(8).3$ has an element of order 6 and $Out(L_2(8)) \cong Z_3$, then $\Gamma(L_2(8).3)$ is not a subgraph of $\Gamma(L)$. Therefore $G = M$ and $G/O_\pi(G) \cong L_2(8)$ where $\pi \subseteq \{2\}$.

Case III. $L = L_2(11)$. By $(*)$ and Theorem 3.1, it follows that $M/N \cong L_2(11)$ or $M/N \cong M_{11}$. We consider both cases simultaneously. Since $Out(L_2(11)) \cong Z_2$, $Out(M_{11})$=1 and $L_2(11).2$ has an element of order 10, in each case it follows that $G = M$. We know that $N$ is a $\{2, 3\}-$group. If $2 \in \pi(N)$, then $M$ has a solvable $\{2, 5, 11\}-$subgroup $H$, since $L_2(11)$ and $M_{11}$ have a 11:5 subgroup. Then $\Gamma(L)$ yields $t(H)$=3, which is a contradiction, since $t(H) \leqslant 2$, by Remark 2.1. Similarly $3 \notin \pi(N)$. Hence $N$=1 and $G \cong L_2(11)$ or $M_{11}$.

Case IV. Since $L_2(13)$, $L_2(16)$, $L_2(17)$, $L_2(29)$, $L_2(32)$, $L_2(37)$, $L_2(41)$, $L_2(53)$, $L_2(61)$, $L_2(73)$, $L_2(89)$ and $L_2(97)$ have similar proofs, we consider only one of them. So let $L = L_2(13)$. By $(*)$ and Theorem 3.1, it follows that $M/N \cong L_2(13)$ or $M/N \cong G_2(3)$. Let $M/N \cong L_2(13)$. Since $Out(L_2(13)) \cong Z_2$ and $L_2(13).2$ has an element of order 14, it follows that $\Gamma(L_2(13).2)$ is not a subgraph of $\Gamma(L)$. Thus $G = M$ and $G/O_\pi(G) \cong L_2(13)$ where $\pi \subseteq \{2, 3\}$. By the same method easily we can show that, if $M/N \cong G_2(3)$, then $G/O_\pi(G) \cong G_2(3)$, where $\pi \subseteq \{2, 3\}$.

Case V. Since $L_2(19)$, $L_2(23)$, $L_2(27)$, $L_2(31)$, $L_2(43)$, $L_2(47)$, $L_2(59)$, $L_2(67)$, $L_2(71)$, $L_2(79)$ and $L_2(83)$ have similar proofs, we only consider a few of them. Let $L = L_2(19)$. Similar to the last cases, $M/N \cong L_2(19)$. Since $Out(L_2(19)) \cong Z_2$ and $L_2(19).2$ has an element of order 6, it follows that $\Gamma(L_2(19).2)$ is not a subgraph of $\Gamma(L)$, and so $G = M$. We know that $L_2(19)$ has a 19:9 subgroup [6]. If $2 \in \pi(N)$, then $M$ has a solvable $\{2, 3, 19\}-$subgroup $H$ and $\Gamma(L)$ yields $t(H)$=3, a contradiction since $t(H) \leqslant 2$. It follows that $2 \notin \pi(N)$. Similarly, if $5 \in \pi(N)$, then $M$ has a solvable $\{3, 5, 19\}-$subgroup $H$. Hence $\Gamma(L)$ yields $t(H)$=3, a contradiction. This yields $5 \notin \pi(N)$. Now $N$=1 and $G \cong L_2(19)$. Let $L = L_2(43)$. We know that $Out(L_2(43)) \cong Z_2$, $L_2(43).2 \cong PGL(2, 43)$ and $PGL(2, 43)$ has an element of order 6, so $\Gamma(L_2(43).2)$ is not a subgraph of $\Gamma(L)$, and $G = M$. Since $L_2(43)$ contains a $43 : 21$ subgroup, then $N = 1$ and $G \cong L_2(43)$.

Case VI. $L = L_2(25)$. In this case we have $M/N \cong L_2(25)$. We note that $Out(L_2(25)) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and by using the notations of the atlas of finite groups we know that $L_2(25).2_1$ and $L_2(25).2_2$ have element of order 26 and 10, respectively [6]. Thus $\Gamma(L_2(25).2_1)$ and $\Gamma(L_2(25).2_2)$ are not subgraphs of $\Gamma(L)$, and in this case $G = M$. By using the atlas of finite groups, $\Gamma(L_2(25)) = \Gamma(L_2(25).2_3)$. So $G/N \cong L_2(25)$ or $G/N \cong L_2(25).2_3$. If $3 \in \pi(N)$, then let $P \in Syl_3(N)$ and $Q \in Syl_5(G)$. We know that $N$ is nilpotent and $P$ *char* $N$, $N \lhd G$. Therefore $P \unlhd G$. Since $3 \not\sim 5$ in $\Gamma(L)$, so $QP$ is a Frobenius group, with kernel $P$ and complement Frobenius $Q$. Therefore $Q$ is cyclic. This is a contradiction since $L_2(25)$ has no element of order 25. By the same method we can show that $2 \notin \pi(N)$. Therefore $N = 1$ and $G \cong L_2(25)$ or $G \cong L_2(25).2_3$.

Case VII. $L = L_2(49)$. In this case we have $M/N \cong L_2(49), A_7, L_3(4)$ or $U_4(3)$. First let $M/N \cong L_2(49)$. We know that $Out(L_2(49)) \cong Z_2 \times Z_2$ and by using the notations of atlas, $L_2(49).2_1$ and $L_2(49).2_2$ have elements of order 10 and 14, respectively. Therefore $\Gamma(L_2(49).2_1)$ and $\Gamma(L_2(49).2_2)$ are not subgraphs of $\Gamma(L)$, and so in this case $G = M$. But $\Gamma(L_2(q)) = \Gamma(L_2(49).2_3)$, so $G/N \cong L_2(49)$ or $G/N \cong L_2(49).2_3$. If $2 \in \pi(N)$, then let $P \in Syl_2(N)$ and $Q \in Syl_7(G)$. Since $2 \not\sim 7$ in $\Gamma(L)$, so $QP$ is a Frobenius group. Therefore $Q$ is cyclic. This is a contradiction, since $L_2(49)$ has no element of order 49. By the same method we can show that $3 \notin \pi(N)$. Therefore $N = 1$ and $G \cong L_2(49)$, $G \cong L_2(49).2_3$. Let $M/N \cong A_7$. Since $Out(A_7) \cong \mathbb{Z}_2$ and $A_7.2$ has an element of order 10, it follows that $\Gamma(A_7.2)$ is not a subgraph of $\Gamma(L)$, and so $G = M$. Hence $G/O_\pi(G) \cong A_7$ where $\pi \subseteq \{2,3\}$. Let $M/N \cong L_3(4)$. We know that $Out(L_3(4)) \cong \mathbb{Z}_2 \times S_3$. Similar to the last cases it follows that by the notations in the atlas of finite groups, $G/O_\pi(G) \cong L_3(4)$, $L_3(4).2'_2$, $L_3(4).2''_2$, $L_3(4).2'_3$ or $L_3(4).2''_3$ where $\pi \subseteq \{2,3\}$. Let $M/N \cong U_4(3)$. We note that $Out(U_4(3)) \cong D_8$. Then similarly we conclude that by the notations of the atlas $G/N \cong U_4(3)$ or $G/N \cong U_4(3).2_3$, since $2 \nsim 5$ in $\Gamma(L)$. Hence $G/O_\pi(G) \cong U_4(3)$ or $U_4(3).2_3$ where $\pi \subseteq \{2,3\}$. Since $U_4(3).2_1$, $U_4(3).2_2$, $U_4(3).2_3$ and $U_4(3).4$ have element of order 10, then $\Gamma(U_4(3).2_1)$, $\Gamma(U_4(3).2_2)$, $\Gamma(U_4(3).2_3)$ and $\Gamma(U_4(3).4)$ are not subgraphs of $\Gamma(L)$, and $G = M$.

Case VIII. $L = L_2(64)$. By assumption we have $M/N \cong L_2(64)$. We note that $Out(L_2(64)) \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. Since $L_2(64).2$ and $L_2(64).3$ have elements of order 6, thus $\Gamma(L_2(64).2)$ and $\Gamma(L_2(64).3)$ are not subgraphs of $\Gamma(L)$. Therefore $G = M$ and $G/O_\pi(G) \cong L_2(64)$ where $\pi \subseteq \{2\}$.

Case IX. $L = L_2(81)$. By $(*)$, it follows from Theorem 3.1 that $M/N \cong L_2(81)$. Since $Out(L_2(81)) \cong Z_2 \times Z_4$ and $L_2(81).2_1$ and $L_2(81).2_2$ have element of order 82 and 6, respectively, thus $\Gamma(L_2(81).2_1)$ and $\Gamma(L_2(81).2_2)$ are not subgraphs of $\Gamma(L)$, and in these cases $G = M$. But $\Gamma(L_2(81) = \Gamma(L_2(81).2_3$. If $2 \in \pi(N)$, then let $P \in Syl_2(N)$ and $Q \in Syl_3(G)$. Therefore $P \trianglelefteq G$. Since $2 \not\sim 3$ in $\Gamma(L)$, so $QP$ is a Frobenius group, with kernel $P$ and complement Frobenius $Q$. Therefore $Q$ is cyclic. This is a contradiction, since $L_2(81)$ has no element of order $3^4$. By the same method we can show $5 \notin \pi(N)$. Therefore $N$=1 and $G \cong L_2(81)$ or $L_2(81).2_3$. □

## Acknowledgements

The authors would like to thank the referee for valuable suggestions. The first author was supported in part by grants from IPM (No. 83200023 and 84200024). So the first author would like to thank IPM for financial support. We dedicate this paper to our family.

# References

[1] **Y. Bugeaud, Z. Cao and M. Mignotte**: *On simple $K_4-$ groups*, J. Algebra **241** (2001), 658 – 668.

[2] **G. Y. Chen**: *On Frobenius and $2-$Frobenius group*, J. Southwest China Normal Univ. **20 (5)** (1995), 485 – 487.

[3] **G. Y. Chen**: *A new characterization of sporadic simple groups*, Algebra Colloq. **3 (1)** (1996), 49 – 58.

[4] **G. Y. Chen**: *A new characterization of $PSL_2(q)$*, Southeast Asian Bull. Math. **22** (1998), 257 – 263.

[5] **N. Chigira, N. Iiyori and H. Yamaki**: *Non-abelian Sylow Subgroups of finite groups of even order*, Invent. Math. **139** (2000), 525 – 539.

[6] **J. Conway, R. Curtis, S. Norton, R. Parker and R. Wilson**: *Atlas of finite groups*, Clarendon Press, Oxford (1985).

[7] **P. Crescenzo**: *A Diophantine equation which arises in the theory of finite groups*, Advances in Math. **17** (1975), 25 – 29.

[8] **M. Hagie**: *The prime graph of a sporadic simple group*, Comm. Algebra **31 (9)** (2003), 4405 – 4424.

[9] **N. Iiyori and H. Yamaki**: *Prime graph components of the simple groups of Lie type over the field of even characteristic*, J. Algebra **155** (1993), 335–343.

[10] **A. Iranmanesh, S. H. Alavi and B. Khosravi**: *A Characterization of $PSL(3,q)$ where q is an odd prime power*, J. Pure and Applied Algebra **170** (2002), 243 – 254.

[11] **A. Khosravi and Behrooz Khosravi**: *Quasirecognition of the simple group ${}^2G_2(q)$ by the prime graph*, Siberian Math. J. (to appear).

[12] **Behrooz Khosravi, Behnam Khosravi and Bahman Khosravi**: *Groups with the same prime graph as a CIT simple group*, Houston J. Math. (to appear).

[13] **A. S. Kondtrat'ev**: *Prime graph components of finite groups*, Math. USSR, Sb. **67** (1990), 235 – 247 (translation from Mat. Sb. **180** (1989), 787 – 797).

[14] **M. S. Lucido**: *The diameter of the prime graph of finite group*, J. Group Theory **2** (1999), 157 – 172.

[15] **W. B. Stewart**: *Groups having strongly self-centralizing 3-centeralizers*, Proc. London Math. Soc. **26** (1973), 653 – 680.

[16] **J. S. Williams**: *Prime graph components of finite groups*, J. Algebra **69** (1981), 487 – 513.

[17] **K. Zsigmondy**: *Zur Theorie der Potenzreste*, Monatsh Math. Phys. **3** (1892), 265 – 284.

Received September 13, 2006

Department of Pure Mathematics
Faculty of Mathematics and Computer Sci.
Amirkabir University of Technology (Tehran Polytechnic)
424, Hafez Ave.
Tehran 15914, IRAN,
and
Institute for Studies in Theoretical Physics and Mathematics (IPM)
E-mail: khosravibbb@yahoo.com

# The application of DES, IDEA and AES in strong encryption

*Czesław Kościelny*

**Abstract**

The concept of strong encryption by means of DES and IDEA in [9, pp. 295, 324] has been mentioned. In the paper this thought concerning the commonly used DES, IDEA and AES algorithms has been developed and generalized.

## 1. Introduction

It has been announced in [2] that
*... the Data Encryption Standard became effective July 1977. It was reaffirmed in 1983, 1988, 1993, and 1999. The DES has now been withdrawn. The use of DES is permitted only as a component function of TDEA*, and that
*with the withdrawal of the FIPS 46-3 standard:*
*1. Triple DES (i.e., TDEA), as specified in ANSI X9.52, Keying Options 1 and 2, is recognized as the only FIPS approved DES algorithm.*
*2. Other implementations of the DES function are no longer authorized for protection of Federal government information.*
*Note: Through the year 2030, Triple DES (TDEA) and the FIPS 197 Advanced Encryption Standard (AES) will coexist as FIPS approved algorithms - thus, allowing for a gradual transition to AES. (The AES is a new symmetric based encryption standard approved by NIST.)*

In the light of the presented paper the above decision seems to be irrational because the protection of data by means of the Triple Data Encryption Algorithm is much more weaker than that offered by DES, used according to the method discussed in this work.

The paper is addressed to application researchers well acquainted with the standards [1], [4] and with the IDEA [3].

2000 Mathematics Subject Classification: 68P25, 94A60, 11T71
Keywords: DES, IDEA, AES, block ciphers, strong encryption

## 2. DES, IDEA and AES as a reason of contention

DES, IDEA and AES belong to a class of iterated block ciphers involving the sequential repetition of a round function and a particular subkey for each round. For any iterated block cipher encryption procedure is described by means of the equation

$$C = E(ks(K), M), \tag{1}$$

where $E$ denotes two-variable encrypting function, $K-$ a secret key chosen by the user, and $M-$ a message to be encrypted. The secret key $K$ is not directly applied in the encryption operation, but it serves as input data for the function $ks$, generating a key schedule, i.e. subkeys for each iteration. A number of cryptologists suspect that the function $ks$ intends to "inject" into the cryptogram as much additional information about bits of the secret key $K$ as possible during the encryption process instead of maximizing the diffusion and confusion. This additional information may deliver – to the privileged circle of the initiated – a manner of deciphering cryptograms without the knowledge of the secret key. To verify the justness of this suspicion one ought to find and analyze an explicit function $F$, which, taking into account both the encryption and key schedule generation algorithms, will allow to express symbolically the cryptogram

$$C = F(K, M), \tag{2}$$

and to compute it in one step, using the secret key $K$ and the message $M$. But in the case of the iterated block ciphers this task is almost unfeasible.

The author shows in next section how to eliminate this bone of contention.

## 3. DES–768, IDEA–832, and AES–1408:1664:1920

It has been verified by the author that it is possible to encrypt data using the DES with the 768-bit key, IDEA with 832-bit key and bringing into play the AES with the key length equal to 1408 bits, 1664 bits or 1920 bits. In the case of the strong version of these algorithms the encrypting/decrypting procedures exactly conform to standards [1] and [4]. To transform DES and AES into strong ciphers it simply suffices to eliminate the key expansion algorithms, i.e. to generate arbitrarily the set of subkeys $K_s$ for all iterations and to use it as a secret key. Then, applying the same encrypting algorithm $E$ as in (1), we now compute the cryptogram of the message $M$ according to

$$C = E(K_s, M), \tag{3}$$

and we are sure that all bits of our modified secret key $K_s$ participate in the encryption process. Thus, since DES needs sixteen 48-bit subkeys, in this way we will obtain the 768-bit secret key to protect a 64-bit block of data. The IDEA needs fifty two 16-bit subkeys for protecting 64-bit plaintext block - it means that the modified secret key for this algorithm can contain 832 bits. Similarly, AES−128, AES−192, AES−256, apply eleven, thirteen and fifteen 128-bit subkeys for encrypting a 128-bit message block, respectively. Making use of these sets of subkeys as secret keys we can now safeguard a 128-bit block of data with secret keys of 1408, 1664 and 1920 bits.

## 4. Strong symmetric-key block ciphers related to DES and to AES

Introducing small changes into the considered cryptographic algorithms we can further strengthen their protecting power. Discussing DES from this point of view we can treat the initial permutation $IP$, primitive functions $S_1 - S_8$ (S-boxes), permutation $P$ and selection function $E$ as variables and in this way enlarge additionally the key space. Since there can be

- $x = 64!$ permutations $IP$,
- $y = (4 \cdot 16!)^8$ sets of 8 S-boxes,
- $z = 32!$ permutations $P$,
- $u = 2^{40}$ selection functions $E$,

then the increase of a secret key length will be

$$\Delta_{DES} = \lfloor \frac{\ln(x \cdot y \cdot z \cdot u)}{\ln(2)} \rfloor, \tag{4}$$

that is 1591 bits. Thus, taking into account the previous section, we can use DES for protection 64-bit data block with key containing 2359 bits.

Some aspects of strong AES encryption have been already considered in [6]. In the instance of AES, we can get any from 30 irreducible polynomials of degree 8 over $GF(2)$ to compute in $GF(256)$. The transformation `SubBytes()` may be replaced by any permutation of 256 elements, one can replace `ShiftRows()` and `InvShiftRows()` transformations by a pair of random mutually invertible permutations acting on elements of the `State` array, and `MixColumns()` and `InvMiColumns()` transformations by a pair of random mutually invertible 4 x 4 non-singular matrices over $GF(256)$. In this manner we can get the full protecting power of the AES (with the secret key up to 3736 bits).

## 5. Conclusions

In the paper an important application-oriented problem concerning the data security, has been presented. The author hopes that this work may have some influence on the future standardization policy in cryptography.

The method presented, with regard to IDEA, may be exactly tested by the reader by means of the `topicIDEA` Maple 10 package [7] available in the Maple Application Center. The author also worked aut `StrongDES` and `genericAES` Maple 10 packages more interesting from the point of view of teaching and research than the latter, allowing the reader to test the presented method in the case of DES and AES and to explore precisely these algorithms.

## References

[1] **NIST**: *Data encryption standard (DES)*, FIPS PUB 46-3, October 1999

[2] **W. C. Barker**: *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, NIST Special Publication 800-67, May 2004

[3] **X. Lai and J. Massey**: *A proposal for a new block encryption standard*, Damgard, editor, Advances in Cryptology Eurocrypt'90: Workshop on the Theory and Application of Cryptographic Techniques, Aarhus, Denmark, May 1990, Proceedings, volume 473 of Lecture Notes in Computer Science, Springer-Verlag, 1991

[4] **NIST**: *Advanced Encryption Standard (AES)*, FIPS PUB 197, 2001

[5] **B. Schneier**: *Applied Cryptography*, (Second Edition): Protocols, Algorithms, and Cource Code in C, John Wiley & Sons, 1996.

[6] **C. Kościelny**: *AES with the increased confidentiality*, Quasigroups and Related Systems **13** (2005), 265 – 268.

[7] **C. Kościelny**: *The* `topicIDEA` *package*, January 2006 `http://www.maplesoft.com/applications/`

Received January 29, 2006

Academy of Management in Legnica, Faculty of Computer Science, ul. Reymonta 21, 59-220 Legnica, Poland
and
Wrocław University of Applied Informatics, ul. Słubicka 29-33, 53-615 Wrocław, Poland
E-mail: c.koscielny@wsm.edu.pl

Quasigroups and Related Systems **14** (2006), 195 − 206

# A graphical technique to obtain homomorphic images of $\Delta(2,3,11)$

*Qaiser Mushtaq* and *Munir Ahmed*

### Abstract

In this paper we have developed a technique by which a suitably created fragment of a coset diagram for the action of $PSL(2,Z)$ or $PGL(2,Z)$ on projective lines over Galois fields $F_p$, $p \equiv \pm 1 (\text{mod } 11)$, can be used to obtain a family of permutation groups $\Delta(2,3,11) = < x, y : x^2 = y^3 = (xy)^{11} = 1 >$ .

## 1. Introduction

It is well known that the modular group $PSL(2,Z)$ is generated by the linear fractional transformations $x : z \to -1/z$ and $y : z \to (z-1)/z$, satisfying the relations $x^2 = y^3 = 1$. The extended modular group $PGL(2,Z)$ is generated by the linear fractional transformations $x : z \to -1/z$, $y : z \to (z-1)/z$, and $t : z \to 1/z$, such that $x^2 = y^3 = t^2 = (xt)^2 = (yt)^2 = 1$.

Let $q = p^m$ where $m > 0$ and $p$ is a prime number. A number $\omega \in F_q$ is said to be a non-zero square in $F_q$ if $\omega \equiv a^2 \pmod{p}$ for some non-zero element $a$ in $F_q$. The projective lines over a finite field $F_q$, $F_q \cup \{\infty\}$, is denoted by $PL(F_q)$.

The group $PGL(2,q)$ is a group consisting of all the transformations $z \to (az+b)/(cz+d)$, where $a$, $b$, $c$, $d \in F_q$ and $ad - bc \neq 0$. The group $PSL(2,q)$ is a group containing transformations $z \to (az+b)/(cz+d)$ where $a$, $b$, $c$, $d \in F_q$ and $ad - bc$ is a non-zero square in $F_q$.

Let $\Delta(l,m,n)$ denote the triangle group $< x, y : x^l = y^m = (xy)^k = 1 >$. The triangle group $\Delta(l,m,k)$ is infinite for $k \geqslant 6$. For $k \leqslant 5$, $\Delta(2,3,k)$ is trivial, $S_3$, $A_4$, $S_4$, and $A_5$ respectively. The group $\Delta(2,3,6)$ is an extension by the cyclic group $C_6$ of a free abelian group of rank 2. For $k = 7$, the triangle group $\Delta(2,3,k)$ is a Hurwitz group [1]. The group $\Delta(2,3,k)$,

2000 Mathematics Subject Classification: 05C38, 15A15, 05A15
Keywords: Diagram, group, homomorphic image.

when $k = 8, 9$ and $10$ are known to be less interesting. There is relatively less information available about $\Delta(2, 3, 11)$. We therefore consider $\Delta(2, 3, 11)$ and use coset diagrams for the actions of $PGL(2, Z)$ on $PL(F_p)$, $p \equiv \pm 1(mod\ 11)$ and see for what values of $p$ these actions evolve triangle groups $\Delta(2, 3, 11)$ as subgroups of $S_{p+1}$.

A coset diagram for $PGL(2, Z)$ consists of a set of small triangles and a set of edges. The three cycles of $y$ are denoted by small triangles whose vertices are permuted counter-clockwise by $y$ and any two vertices which are interchanged by $x$ are joined by an edge. The action of $t$ is represented by reflection about a vertical line of axis in the case of $PGL(2, Z)$. The fixed points of $x$ and $y$ are denoted by heavy dots.

Let $PSL(2, Z)$ act on a space $\Omega$. If an element $(xy)^{n_1}\left(xy^{-1}\right)^{n_2}\cdots\left(xy^{-1}\right)^{n_l}$ of $PSL(2, Z)$ fixes an element of $\Omega$, then the patch of the coset diagram is called a *circuit.* We denote it by $(n_1, n_2, ..., n_l)$. For a given sequence of positive integers $(n_1, n_2, n_3, ..., n_{2k})$ the circuit of the type

$$(n_1, n_2, n_3, \ldots, n_{2k'}, n_1, n_2, n_3, \ldots, n_{2k'}, \ldots, n_1, n_2, n_3, \ldots, n_{2k'}),$$

where $k'$ divides $k$, is said to be a *periodic circuit of length* $2k'$. A trivial circuit consists of a path followed by its own inverse. A portion of a coset diagram is called a *fragment* of a coset diagram. First of all we construct a fragment composed of two connected, non-trivial circuits such that neither of them is periodic and more than two vertices in the fragment are fixed by $(xy)^{11}$. Corresponding to two circuits we have two words (elements of $PSL(2, Z)$), yielding a polynomial $f(z)$ in $Z[z]$ as in [4]. A homomorphism $\alpha : PGL(2, Z) \rightarrow PGL(2, q)$ is called *non-degenerate* if $x$, $y$, $t$ do not belong to $Ker(\alpha)$. Of course $\alpha$ gives rise to an action of $PGL(2, Z)$ on $PL(F_q)$. Two non-degenerate homomorphisms $\alpha$ and $\beta$ are called *conjugate* if there exists an inner automorphism $\rho$ on $PGL(2, q)$ such that $\alpha = \rho\beta$. In [5], these actions, or conjugacy classes, have been parameterized with the elements $\theta \in F_q$. Corresponding to each root $\theta(\neq 0, 3)$ of $f(\theta) = 0$ in $F_p$ where $p \equiv \pm 1(mod\ k)$, we obtain a conjugacy class of actions of $PGL(2, Z)$ on $PL(F_p)$ each action evolving $\Delta(2, 3, k)$. By $D(\theta, q)$ we mean a coset diagram of the conjugacy class corresponding to parameter $\theta \in F_q$.

We need the following results proved in [4] and [5] .

**Theorem 1.** [4] *Given a fragment $\gamma$, where $\gamma$ is a non-simple fragment consisting of two connected, non-trivial circuits such that neither of them is periodic, there exists a polynomial $F(z)$ in $Z\left[z\right]$ such that*

(*i*) *if the fragment $\gamma$ occurs in $D\left(\theta, q\right)$, then* $F\left(\theta\right) = 0$, (*ii*) *if* $F(\theta) = 0$ *then the fragment, or a homomorphic image of it occurs in* $D(\theta, q)$ *or in* $D(\theta, \overline{q})$, *where* $D(\theta, \overline{q})$ *denotes the diagram with the vertices from the complement* $PL\left(F_{q^2}\right) \backslash PL\left(F_q\right)$.

**Theorem 2.** [5] *The conjugacy classes of a non-degenerate homomorphisms of* $PGL(2, Z)$ *into* $PGL(2, q)$ *are in one-to-one correspondence with the elements* $\theta \neq 0$, 3 *of* $F_q$. *under the correspondence which maps each class to its parameter.*

## 2. Appropriate fragments

By an *appropriate fragment* we shall mean a fragment composed of two non-trivial, connected circuits $C_1$ and $C_2$ such that neither of them is periodic and at least three vertices of this fragment are fixed by $(xy)^{11}$.

By Theorems 1 and 2, we can find conjugacy classes of non-degenerate homomorphisms corresponding to the elements $\theta(\neq 0, 3)$ in some finite field $F_p$, $p \equiv \pm 1(mod\ 11)$ obtained from the condition in the form of a polynomial. Each conjugacy class corresponds to a diagram. These coset diagrams will be such that every vertex in these diagrams will be a fixed point of $(\overline{x}\,\overline{y})^{11}$, and so by a well known fact that no non-trivial linear fractional transformation in $PGL(2, q)$ can fix more than two vertices in $F_q$, it will depict the triangle group $\alpha(\Delta(2, 3, 11))$.

**Theorem 3.** *Let* $\gamma$ *be an appropriate fragment of a coset diagram for* $PGL(2, Z)$ *with at least one of the three vertices as the common vertex of* $C_1$ *and* $C_2$. *Then there exists a coset diagram* $D(\theta,\ p)$ *containing* $\gamma$, *or its homomorphic image, representing* $\alpha(\Delta(2, 3, 11))$.

*Proof.* Consider $\gamma$ which is composed of two non-periodic circuits $C_1$ and $C_2$. Let $w_1$ and $w_2$ be two elements of $PSL(2, Z)$ induced by the circuits $C_1$ and $C_2$ respectively. That is $w_1 = xyxyxyyxyxy$ and $w_2 = xyyxyyxyxyy$. We can represent $w_1$ and $w_2$ as matrices $W_1 = XYXYXYYXYXY$ and $W_2 = XYYXYYXYXYY$ which are elements of $SL(2, Z)$, where $X$ and $Y$ are the matrices representing the elements $x$ and $y$ (of orders 2 and 3 respectively) of $PSL(2, Z)$. According to Mushtaq [4], we can express $W_1$ and $W_2$ as linear combinations of $I$, $X$, $Y$ and $XY$, that is,

$$W_1 = \lambda_0 I + \lambda_1 X + \lambda_2 Y + \lambda_3 XY$$

and

$$W_2 = \mu_0 I + \mu_1 X + \mu_2 Y + \mu_3 XY.$$

We take $X = \begin{bmatrix} a & kc \\ c & -a \end{bmatrix}$, $Y = \begin{bmatrix} d & kf \\ f & -d-1 \end{bmatrix}$, with $trace(X) = 0$ and $\det(X) = \Delta$. Then the characteristic equation of $X$ is $X^2 + \Delta I = O$, and since $trace(Y) = -1$ and $\det(Y) = 1$, the characteristic equation of $Y$ is $Y^2+Y+I = O$. Thus the characteristic equation of $XY$ is $(XY)^2-r(XY)+\Delta I = O$, where $r = trace(XY)$ and $\Delta = \det(XY)$. Also, $\Delta = -(a^2 + kc^2)$ and $d^2 + d + kf^2 + 1 = 0$. Using these equations, we obtain

$$\begin{aligned}(XY)^n &= \left\{\binom{n-1}{0}r^{n-1} - \binom{n-2}{1}r^{n-3}\triangle + ....\right\}XY \\ &\quad -\triangle\left\{\binom{n-2}{0}r^{n-2} - \binom{n-3}{1}r^{n-4}\triangle + ...\right\}I.\end{aligned}$$

After a suitable manipulation of the above equations, we get $XYX = rX + \triangle I + \triangle Y$, $YXY = rY + X$ and $YX = rI - X - XY$. Of course

$(XY)^3 = (r^2 - \Delta)XY - r\Delta I$,
$(XY)^4 = (r^3 - 2r\Delta)XY - (r^2\Delta - \Delta^2)I$,
$(XY^2)^2 = rXY + rX - \Delta I$,
$(XY^2)^3 = (r^2 - \Delta)XY + (r^2 - \Delta)X - r\Delta I$, and
$(XY^2)^4 = (r^3 - 2r\Delta)XY + (r^3 - 2r\Delta)X - (r^2\Delta - \Delta^2)I$.

Now,

$$\begin{aligned}W_1 &= XYXYXY^2XYXY \\ &= (XY)^3Y(XY)^2 \\ &= [(r^2 - \Delta)XY - r\Delta I]Y(rXY - \Delta I) \\ &= [(r^2 - \Delta)XY^2 - r\Delta Y][rXY - \Delta I] \\ &= [(r^2 - \Delta)(-XY - X) - r\Delta Y][rXY - \Delta I] \\ &= [(-r^2 + \Delta)XY + (-r^2 + \Delta)X - r\Delta Y][rXY - \Delta I] \\ &= [(-r^3 + r\Delta)(XY)^2 + (-r^3 + r\Delta)X^2Y - r^2\Delta YXY + (r^2\Delta - \Delta^2)XY \\ &\quad +(r^2\Delta - \Delta^2)X + r\Delta^2Y] \\ &= [(-r^3 + r\Delta)(rXY - \Delta I) + (-r^3 + r\Delta)\,(-\Delta I)\,Y - r^2\Delta(rY + X)+ \\ &\quad (r^2\Delta - \Delta^2)XY + (r^2\Delta - \Delta^2)X + r\Delta^2Y] \\ &= [(-r^4 + r^2\Delta)XY + (r^3\Delta - r\Delta^2)I + (r^3\Delta - r\Delta^2)Y - r^3\Delta Y - r^2\Delta X \\ &\quad +(r^2\Delta - \Delta^2)XY + (r^2\Delta - \Delta^2)X + r\Delta^2Y] \\ &= [(r^3\Delta - r\Delta^2)I - \Delta^2X + 0Y + (-r^4 + 2r^2\Delta - \Delta^2)XY\end{aligned}$$

and

$$\begin{aligned}W_2 &= XYYXYYXYXYY \\ &= \left(XY^2\right)^2\left(XY\right)^2Y \\ &= [rXY + rX - \Delta I][rXY - \Delta I]Y\end{aligned}$$

$$\begin{aligned}
&= [rXY + rX - \Delta I][rXY^2 - \Delta Y]\\
&= [rXY + rX - \Delta I][r(-XY - X) - \Delta Y]\\
&= [rXY + rX - \Delta I][-rXY - rX - \Delta Y]\\
&= [-r^2\,(XY)^2 - r^2XYX - r\Delta XY^2 - r^2XY - r^2X^2 - r\Delta XY + r\Delta XY +\\
&\quad r\Delta X + \Delta^2Y]\\
&= [-r^2\,(rXY - \Delta I) - r^2(rX + \Delta Y + \Delta I) + r\Delta(XY + X) + r^2\Delta Y +\\
&\quad r^2\Delta I - r\Delta XY + r\Delta XY + r\Delta X + \Delta^2Y]\\
&= r^2\Delta I + (-r^3 + 2r\Delta)X + \Delta^2Y + (-r^3 + r\Delta)XY.
\end{aligned}$$

Using equations

$$\begin{aligned}
W_1 &= \lambda_0 I + \lambda_1 X + \lambda_2 Y + \lambda_3 XY,\\
W_2 &= \mu_0 I + \mu_1 X + \mu_2 Y + \mu_3 XY,
\end{aligned}$$

we obtain $\lambda_1 = -\Delta^2$, $\lambda_2 = 0$ and $\lambda_3 = (-r^4 + 2r^2\Delta - \Delta^2)$, $\mu_1 = (-r^3 + 2r\Delta)$, $\mu_2 = \Delta^2$ and $\mu_3 = (-r^3 + r\Delta)$.

Now substituting these values in the equation

$$\begin{aligned}
&(\lambda_2\mu_3 - \mu_2\lambda_3)^2 + \triangle\,(\lambda_3\mu_1 - \mu_3\lambda_1)^2 + (\lambda_1\mu_2 - \mu_1\lambda_2)^2\\
&\qquad + r\,(\lambda_2\mu_3 - \mu_2\lambda_3)\,(\lambda_3\mu_1 - \mu_3\lambda_1) + (\lambda_2\mu_3 - \mu_2\lambda_3)\,(\lambda_1\mu_2 - \mu_1\lambda_2) = 0
\end{aligned}$$

we get:

$$\begin{aligned}
&[0 - \Delta^2(-r^4 + 2r^2\Delta - \Delta^2)]^2 + \Delta[(-r^3 + 2r\Delta)(-r^4 + 2r^2\Delta - \Delta^2)\\
&+\Delta^2(-r^3 + r\Delta)]^2 + [-\Delta^2.\Delta^2 - 0]^2 + r[0 - \Delta^2(-r^4 + 2r^2\Delta - \Delta^2)]\\
&[(-r^3 + 2r\Delta)(-r^4 + 2r^2\Delta - \Delta^2) + \Delta^2(-r^3 + r\Delta)] +\\
&[0 - \Delta^2(-r^4 + 2r^2\Delta - \Delta^2)][-\Delta^4 - 0] = 0,
\end{aligned}$$

$$\begin{aligned}
&[\Delta^4(r^4 - 2r^2\Delta + \Delta^2)^2 + \Delta(r^7 - 2r^5\Delta + \Delta^2r^3 - 2r^5\Delta + 4r^3\Delta^2 - 2r\Delta^3\\
&-r^3\Delta^2 + r\Delta^3) + \Delta^8 + r\Delta^2(r^4 - 2r^2\Delta + \Delta^2)(r^7 - 2r^5\Delta + r^3\Delta^2 - 2r^5\Delta\\
&+4r^3\Delta^2 - 2r\Delta^3 + r^3\Delta^2 + r\Delta^3) + \Delta^6[-r^4 + 2r^2\Delta - \Delta^2]] = 0,
\end{aligned}$$

$$\begin{aligned}
&\Delta^4[\Delta^2\theta^2 - 2\Delta^2\theta + \Delta^2]^2 + \Delta[r^7 - 4r^5\Delta + 4r^3\Delta^2 - r\Delta^3]^2 + \Delta^8\\
&+r\Delta^2[\Delta^2\theta^2 - 2\Delta^2\theta + \Delta^2][r^7 - 4r^5\Delta + 4r^3\Delta^2 - r\Delta^3]\\
&+\Delta^6[-\Delta^2\theta^2 + 2\Delta^2\theta - \Delta^2] = 0.
\end{aligned}$$

That is,

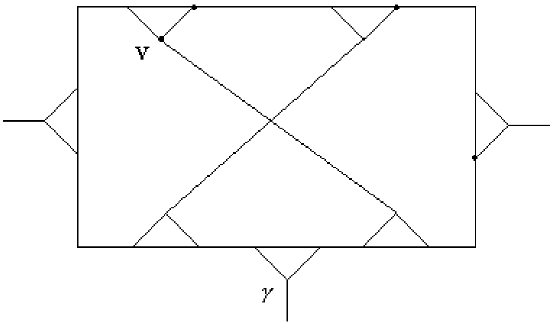
$$\begin{aligned}
\Delta^8[(\theta^2 - 2\theta + 1)^2 + \theta(\theta^3 - 4\theta^2 + 4\theta - 1)^2 + 1 +\\
\theta(\theta^2 - 2\theta + 1)(\theta^3 - 4\theta^2 + 4\theta - 1) + (-\theta^2 + 2\theta - 1)] = 0.
\end{aligned}$$

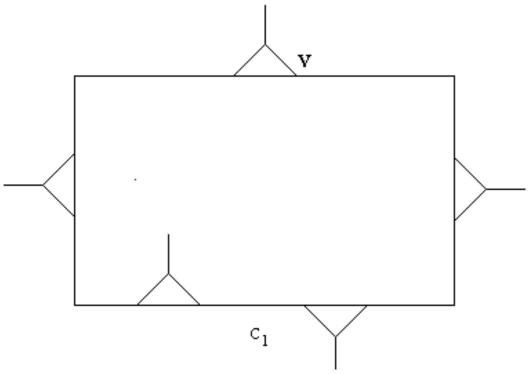
By Theorem 1 we obtain a polynomial $f(\theta) = \theta^7 - 7\theta^6 + 18\theta^5 - 20\theta^4 + 7\theta^3 + 3\theta^2 - 2\theta + 1$. If we let $f(\theta) = 0$, then $f(\theta_i) = 0$ where $\theta_i \in F_p$ and

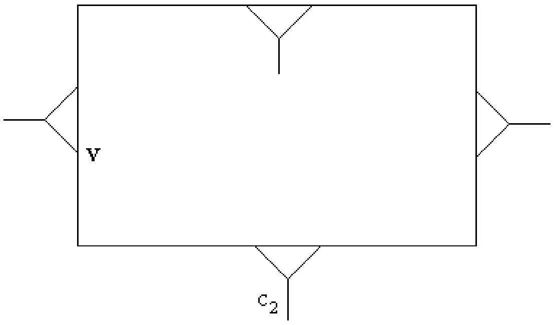
$p \equiv \pm 1 (\text{mod } 11)$, then according to our Theorem 2, $D(\theta_i, p)$ is such that it corresponds to a conjugacy class of non-degenerate homomorphisms $\alpha$ from $PGL(2, Z)$ into $PGL(2, p)$. This depicts an action of $PGL(2, Z)$ on $PL(F_p)$ and the diagram depicting the action is such that every vertex in the diagram is fixed by the element $(\overline{x}\,\overline{y})^{11}$. Since no non-trivial linear fractional transformation can fix more than two vertices in $PL(F_p)$, thus $(\overline{x}\,\overline{y})^{11} = 1$ and so the coset diagram represents the homomorphic image of the triangle group $\Delta(2, 3, 11)$, that is, $\alpha(\Delta(2, 3, 11))$. □

**Theorem 4.** *There exists only two coset diagrams* $D(19, 67)$ *and* $D(125, 199)$ *for the action of* $PGL(2, Z)$ *on* $PL(F_p)$ *depicting* $\alpha(\Delta(2, 3, 11))$*, where* $2 \leqslant p \leqslant 1033$*, and* $p$ *is a prime congruent to* $\pm 1$ *(mod* $11)$.

*Proof.* In order to obtain the required coset diagram first of all we take the following fragment $\gamma$ which is composed of two non-trivial, and non-periodic circuits $C_1$ and $C_2$ with the vertex $\mathbf{v}$ of $\gamma$ as the common vertex of $C_1$ and $C_2$ as shown in the fragment. Note that the fragment is required to contain at least three vertices, namely $\mathbf{v}_1$, $\mathbf{v}_2$ and $\mathbf{v}$ which are fixed by $(\overline{x}\,\overline{y})^{11}$. Let $w_1 = xyxyxyyxyxy$ and $w_2 = xyyxyyxyxyy$ be the elements induced by the circuits $C_1$ and $C_2$ respectively. Notice that $w_1$ and $w_2$ are the elements of $PSL(2, Z)$ and represent the matrices $W_1 = XYXYXYYXYXY$ and $W_2 = XYYXYYXYXYY$ belonging to $GL(2, Z)$, where $X$ and $Y$ are the matrices representing $x$ and $y$ of $PGL(2, Z)$, so $(185, 185)\,(0, \infty)(3, 198)(88, 156)$.







As in [4] ,

$$\begin{aligned} W_1 &= XYXYXY^2XYXY \\ &= [(r^3\Delta - r\Delta^2)I - \Delta^2X + 0Y + (-r^4 + 2r^2\Delta - \Delta^2)XY \end{aligned}$$

and

$$\begin{aligned} W_2 &= XYYXYYXYXYY \\ &= r^2\Delta I + (-r^3 + 2r\Delta)X + \Delta^2Y + (-r^3 + r\Delta)XY \end{aligned}$$

and by using Theorem 1, we can obtain a polynomial $f(\theta) = \theta^7 - 7\theta^6 + 18\theta^5 - 20\theta^4 + 7\theta^3 + 3\theta^2 - 2\theta + 1$. If we convert this polynomial into an equation $f(\theta) = 0$, and solve it in the field $F_{67}$, we obtain 19, 60 and 61 as its roots. By using theorem 2 for $\theta = 19$, we obtain the matrices $X = \begin{bmatrix} 9 & 38 \\ 19 & -9 \end{bmatrix}$, $Y = \begin{bmatrix} 0 & 20 \\ 10 & -1 \end{bmatrix}$ and $T = \begin{bmatrix} 0 & -2 \\ 1 & 0 \end{bmatrix}$. Therefore the corresponding transformations are, $\overline{x} : z \mapsto \frac{9z+38}{19z-9}$, $\overline{y} : z \mapsto \frac{20}{10z-1}$ and

$\bar{t} : z \mapsto \frac{-2}{z}$. So,

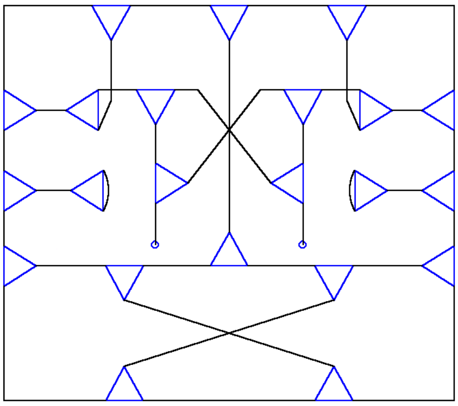
$$\begin{aligned}\bar{x} \ : \ & (33,0)(1,65)(62,2)(3,53)(4,\infty)(22,5)(6,13)(7,10)(8,42)(21,9)\\ & (11,64)(12,23)(14,46)(15,30)(39,16)(26,17)(18,34)(19,32)(20,47)\\ & (24,25)(31,27)(28,55)(61,29)(35,37)(36,59)(38,40)(41,57)(43,56)\\ & (44,48)(45,60)(49,58)(50,51)(52,63)(54,66),\end{aligned}$$

$$\begin{aligned}\bar{y} \ : \ & (0,47,\infty)(32,49,1)(65,15,46)(48,2,61)(45,66,53)(3,3,3)(44,44,44)\\ & (28,14,4)(33,19,43)(34,5,51)(42,13,63)(31,25,6)(22,16,41)(10,9,7)\\ & (38,37,40)(24,64,8)(50,23,39)(26,35,11)(12,21,36)(55,17,58)\\ & (30,59,56)(18,60,62)(54,29,52)(27,20,57),\end{aligned}$$

and

$$\begin{aligned}\bar{t} \ : \ & (0,\infty)\,(1,65)\,(2,66)\,(3,44)\,(4,33)\,(5,13)\,(6,22)\,(7,38)\,(8,50)\,(9,37)\\ & (10,40)\,(11,12)\,(14,19)\,(15,49)\,(16,25)\,(17,59)\,(18,52)\,(20,20)\,(21,35)\\ & (23,64)\,(24,39)\,(26,36)\,(27,57)\,(28,43)\,(29,60)\,(30,58)\,(31,41)\,(32,46)\\ & (33,4)\,(34,63)\,(55,56)\,(42,51)\,(54,62)\,(48,53)\,(61,45)\,(47,47)\,.\end{aligned}$$

Thus we have a coset diagram $D(19,67)$ in which each vertex of the diagram is fixed by $(\bar{x}\,\bar{y})^{11}$, and we have $(\bar{x}\,\bar{y})^{11} = 1$. Thus the diagram $D(19,67)$ is a representation of the triangle group $\alpha(\Delta\,(2,3,11))$.



Now solving the equation $f(\theta) = \theta^7 - 7\theta^6 + 18\theta^5 - 20\theta^4 + 7\theta^3 + 3\theta^2 - 2\theta + 1 = 0$ in $F_{199}$, we obtain 125, 159, and 193 as its roots.

For instance, if we consider $\theta = 125$, we obtain $X = \begin{bmatrix} 121 & 124 \\ 174 & -121 \end{bmatrix}$, $Y = \begin{bmatrix} 0 & 14 \\ 71 & -1 \end{bmatrix}$ and $T = \begin{bmatrix} 0 & -3 \\ 1 & 0 \end{bmatrix}$ as before. The corresponding transformations are: $\overline{x} : z \mapsto \frac{121z+124}{174z-121}$, $\overline{y} : z \mapsto \frac{14}{71z-1}$, and $\overline{t} : z \mapsto \frac{-3}{z}$. Thus,

$$
\begin{aligned}
\overline{x} \quad : \quad & (22,0)(106,1)(2,141)(96,3)(99,4)(5,48)(6,49)(7,70)(8,177) \\
& (9,119)(10,101)(31,11)(18,12)(13,60)(14,185)(165,15)(16,69) \\
& (113,17)(35,19)(93,20)(104,21)(43,23)(181,24)(59,25)(91,26) \\
& (27,\infty)(28,162)(194,29)(72,30)(32,54)(33,149)(160,34)(42,36) \\
& (140,37)(184,38)(39,88)(40,68)(41,193)(44,152)(45,134)(46,76) \\
& (183,47)(154,50)(51,157)(52,112)(53,147)(110,55)(114,56) \\
& (131,57)(58,179)(61,189)(62,173)(63,180)(64,192)(65,151) \\
& (66,107)(67,105)(71,116)(73,190)(195,74)(92,75)(77,169) \\
& (135,78)(79,87)(80,191)(81,129)(82,138)(83,168)(84,176) \\
& (85,170)(90,86)(89,103)(94,130)(95,108)(97,100)(98,127) \\
& (188,102)(109,133)(111,121)(115,171)(117,128)(118,175) \\
& (120,144)(122,196)(123,159)(124,172)(125,136)(126,155) \\
& (132,142)(137,182)(139,197)(143,198)(145,158)(146,187) \\
& (148,186)(150,164)(153,156)(161,178)(163,167)(166,174),
\end{aligned}
$$

$$
\begin{aligned}
\overline{y} \quad : \quad & (0,185,\infty)(1,40,188)(145,184,196)(137,87,2)(98,48,183) \\
& (3,47,186)(138,182,198)(166,136,4)(49,19,181)(106,5,63) \\
& (180,79,122)(86,6,30)(179,99,155)(7,57,157)(128,178,28) \\
& (172,61,8)(124,13,177)(9,78,119)(107,176,66)(46,10,25) \\
& (175,139,160)(131,11,24)(174,54,161)(69,36,12)(149,116,173) \\
& (171,14,192)(55,26,15)(159,130,170)(123,16,20)(169,62,165) \\
& (167,33,17)(152,18,168)(74,43,21)(142,111,164)(22,83,158) \\
& (102,163,27)(70,64,23)(121,115,162)(88,41,29)(144,97,156) \\
& (146,153,31)(32,39,154)(112,109,34)(76,73,151)(60,35,195)
\end{aligned}
$$

$$\begin{aligned}
&(150,125,189)(82,56,37)(129,103,148)(134,117,38)(68,51,147)\\
&(96,114,42)(71,89,143)(127,72,44)(113,58,141)(45,81,132)\\
&(104,140,53)(50,84,197)(101,135,187)(120,52,190)(133,65,194)\\
&(90,67,59)(118,95,126)(75,85,193)(100,110,191)(105,92,77)\\
&(93,80,108)(91,91,91)(94,94,94),
\end{aligned}$$

and

$$\begin{aligned}
\bar{t}\ :\ &(2,98)\,(4,49)\,(5,79)\,(6,99)\,(7,28)\,(8,124)\,(9,66)\,(10,139)\,(11,54)\\
&(12,149)\,(13,61)\,(14,14)\,(15,159)\,(16,62)\,(17,152)\,(18,33)\,(19,136)\\
&(20,169)\,(21,142)\,(22,27)\,(23,121)\,(24,174)\,(25,175)\,(26,130)\\
&(29,144)\,(30,179)\,(31,32)\,(34,76)\,(35,125)\,(36,116)\,(37,129)\\
&(38,68)\,(39,153)\,(40,184)\,(41,97)\,(42,71)\,(43,111)\,(44,113)\\
&(45,53)\,(46,160)\,(47,182)\,(48,87)\,(50,187)\,(51,117)\,(52,65)\\
&(55,170)\,(56,103)\,(57,178)\,(58,72)\,(59,118)\,(60,189)\,(63,180)\\
&(64,115)\,(67,95)\,(69,173)\,(70,162)\,(73,109)\,(74,164)\,(75,191)\\
&(77,93)\,(78,176)\,(80,92)\,(81,140)\,(82,148)\,(83,163)\,(84,135)\\
&(85,110)\,(86,155)\,(89,114)\,(90,126)\,(91,94)\,(96,143)\,(100,193)\\
&(101,197)\,(102,158)\,(104,132)\,(105,108)\,(106,122)\,(107,119)\\
&(112,151)\,(120,194)\,(123,165)\,(127,141)\,(128,157)\,(131,161)\\
&(133,190)\,(134,147)\,(137,183)\,(138,186)\,(145,188)\,(146,154)\\
&(150,195)\,(166,181)\,(1,196)\,(167,168)\,(171,192)\,(172,177)\\
&(185,185)\,(0,\infty)(3,198)(88,156).
\end{aligned}$$

Thus we have the coset diagram $D(125,199)$ (see the next page) in which each vertex is fixed by $(\overline{x}\,\overline{y})^{11}$ . We have therefore $(\overline{x}\,\overline{y})^{11}=1$.

Thus the diagram $D(125,199)$ is a representation of the triangle group $\alpha(\Delta\,(2,3,11))$. □

**Corollary 5.** *For prime $p$, $2\leqslant p\leqslant 1033$ such that $p\equiv\pm1(mod\ 11)$,*

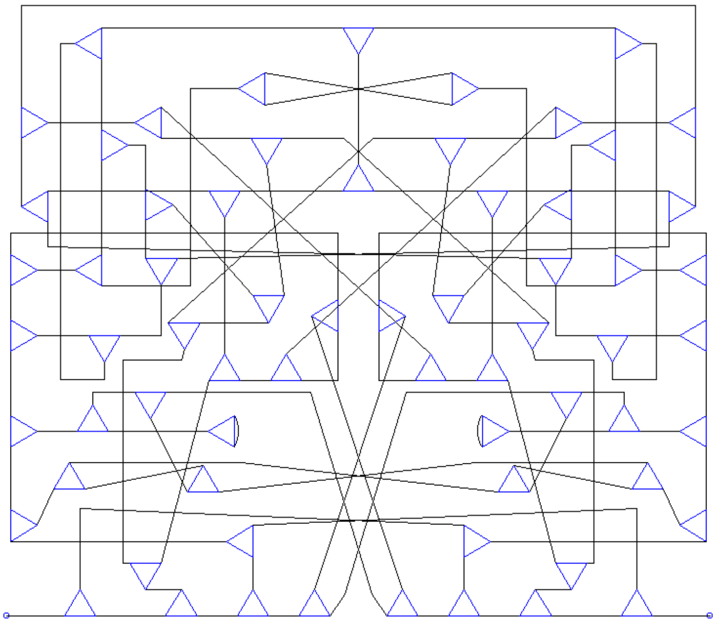
*$(i)$ the action of $PGL(2,Z)$ on $PL\,(F_p)$ is transitive,*

*$(ii)$ the diagram of $\alpha(\Delta\,(2,3,11))$ is connected.*

*Proof.* $(i)$ Consider the action of $PGL(2,Z)$ on $PL\,(F_{67})$. Of course, by Theorem 3, there is only one orbit $\Omega=\{\infty,0,1,2,\dots,66\}$ under this action. Thus the action of $PGL(2,Z)$ on $PL\,(F_{67})$ is transitive.

A similar argument shows that the action of $PGL(2,Z)$ on $PL(F_{199})$ is transitive.

(*ii*) The coset diagrams given in theorem 3 are the connected diagrams of $\alpha(\Delta(2,3,11))$. □



## References

[1] **M. D. E. Conder:** *Hurwitz groups: a brief survey*, Bull. Amer. Math. Soc. **23** (1990), 359 – 370.

[2] **B. Fine and G. Rosenberger:** *A note on generalized triangle groups*, Abh. Math. Sem. Univ. Hamburg **56** (1986), 233 – 244.

[3] **Q. Mushtaq and F. Shaheen:** *Coset diagrams for a homomorphic image of* $\triangle(2,3,6)$, Ars Combinatoria **23A** (1987), 187 – 193.

[4] **Q. Mushtaq:** *A condition for the existence of a fragment of a coset diagram*, Quart. J. Math. (Oxford) **2(39)** (1988), 81 – 95.

[5] **Q. Mushtaq:** *Parametrization of all homomorphisms from* $PGL(2,Z)$ *into* $PGL(2,q)$, Comm. algebra **20** (1992), 1023 – 1040.

[6] **J. S. Rose:** *A course on group theory*, Cambridge University Press, Cambridge, 1978.

Received October 17, 2005

Department of Mathematics
Quaid-i-Azam University
Islamabad 45320
Pakistan
e-mail: qmushtaq@apollo.net.pk

# Ideals in AG-band and AG$^*$-groupoid

*Qaiser Mushtaq and Madad Khan*

**Abstract**

We have shown that an ideal $I$ of an AG-band is prime iff ideal $(S)$ is totally ordered; it is prime iff it is strongly irreducible. The set of ideals of $S$ form a semilattice structure. We have proved that if $a$ belongs to the centre of $S$, then $S$ is zero-simple if and only if $(Sa)S = S$, for every $a$ in $S\backslash\{0\}$. Ideal structure in an AG$^*$-groupoid $S$ has also been investigated. It has been shown that if $I$ is a minimal right ideal of $S$ then $Ia$ is a minimal left ideal of $S$, for all $a$ in $S$. It has been shown also that every ideal of an AG$^*$-groupoid $S$ is prime if and only if it is idempotent and ideal $(S)$ is totally ordered.

## 1. Introduction

A groupoid $S$ is called an *Abel-Grassmann's groupoid*, abbreviated as an *AG-groupoid*, if its elements satisfy the left invertive law [4, 5], that is:

$$(ab)c = (cb)a \tag{1}$$

for all $a, b, c \in S$.

Several examples and interesting properties of AG-groupoids can be found in [5], [6], [7] and [8]. It has been shown in [5] that if an AG-groupoid contains a left identity then it is unique. It has been proved also that an AG-groupoid with right identity is a commutative monoid, that is, a semigroup with identity element.

It is also known [4] that in an AG-groupoid $S$, the *medial law*, that is,

$$(ab)(cd) = (ac)(bd) \tag{2}$$

for all $a, b, c, d \in S$ holds.

2000 Mathematics Subject Classification: 20M10, 20N990
Keywords: AG-groupoid, AG-band, AG$^*$-groupoid, minimal ideal, prime ideal, invertive law, medial law

## 2. AG-band

An AG-groupoid whose all elements are idempotents is called an *AG-band*. It is easy to see that in an AG-band $S$ for any $a, b, c \in S$, $(ab)a = a(ba)$ and $(ab)c = (ac)(bc)$, $(ab)b = ba$.

**Theorem 1.** *If an AG-band $S$ contains a left identity $e$ then $S$ becomes a semilattice with identity $e$.*

*Proof.* Let $x \in S$. Then

$$xe = (xx)e = (ex)x = xx = x$$

implies that $x$ is the right identity for $S$ and so by [5], the AG-band$S$ becomes a commutative monoid, that is, a semilattice with identity $e$. □

Due to Theorem 1, an AG-band with left identity becomes a semigroup with identity. So we cannot include automatically the left identity in an AG-band.

In an AG-band every congruence relation is trivially separative.

**Theorem 2.** *If $S$ is an AG-band and $a$ is a fixed element in $S$ then*

$$H(a) = \{x \in S : xa = x\}$$

*is a commutative subsemigroup with identity $a$.*

*Proof.* Since $a \in H(a)$ we conclude that $H(a)$ is non-empty.

Let $x, y, z \in H(a)$, then

$$xy = (xa)(ya) = (xy)(aa) = (xy)a$$

implies that $H(a)$ is a groupoid.

Now

$$xy = (xa)y = (ya)x = yx$$

shows that $H(a)$ is commutative and so it becomes associative. Also

$$ax = (aa)x = (xa)a \ = xa = x,$$

imply that $H(a)$ is a commutative subsemigroup of idempotents with identity $a$ in $S$. □

**Example 1.** Let $S = \{1, 2, 3, 4, 5, 6\}$ and a binary operation be defined in $S$ as follows:

| $\cdot$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 2 | 5 | 6 | 4 |
| 2 | 2 | 2 | 2 | 5 | 6 | 4 |
| 3 | 2 | 2 | 3 | 5 | 6 | 4 |
| 4 | 6 | 6 | 6 | 4 | 2 | 5 |
| 5 | 4 | 4 | 4 | 6 | 5 | 2 |
| 6 | 5 | 5 | 5 | 2 | 4 | 6 |

Then, as in [11] , $(S, \cdot)$ is an AG-band and $H(1) = \{1, 2\}$ is a semilattice with identity 1.

The following definitions are given in [10]. If $S$ is an AG-groupoid and $A, B \subseteq S$, then $A$ and $B$ are called *right connected sets* if $AS \subseteq B$ and $BS \subseteq A$. Similarly, if $S$ is an AG-groupoid and $A$, $B \subseteq S$, then $A$ and $B$ are called *left connected* if $SA \subseteq B$ and $SB \subseteq A$. Also $A$ and $B$ are called *connected sets* if they are both left and right connected.

A subset $I$ of an AG-groupoid $S$ is said to be *right* (*left*) *ideal* if $IS \subseteq I$ ($SI \subseteq I$). As usual $I$ is said to be an *ideal* if it is both right and left ideal.

**Proposition 1.** *If $A$ and $B$ are left connected sets of an AG-band $S$ and $A$ is an ideal, then $S(A \cup B) \subseteq A$.*

**Lemma 1.** *If $A$ and $B$ are ideals of an AG-band $S$, then $AB$ and $BA$ are right and left connected sets.*

*Proof.* Using identity (1), we get

$$(AB)S = (SB)A \subseteq BA.$$

Similarly

$$(BA)S \subseteq AB.$$

This shows that $AB$ and $BA$ are right connected. Using identity (1), we get

$$S(BA) = (SS)(BA) = ((BA)S)S = ((SA)B)S \subseteq AB.$$

Also

$$S(AB) \subseteq BA.$$

This implies that $AB$ and $BA$ are left connected. □

**Proposition 2.** *A proper subset $I$ of an AG-band $S$ is a right ideal if and only if it is left.*

*Proof.* Let $I$ be a right ideal of an AG-band $S$. Then $IS \subseteq S$, that is, $ix \in I$ for all $i \in I$ and $x \in S$. Hence

$$(xi) = (xx)i = (ix)x \in (IS)S \subseteq IS \subseteq I$$

shows that $SI \subseteq I$, that is, $I$ is a left ideal of $S$. The converse can be proved similarly. □

It can easily be seen from Proposition 2, that $SI \subseteq IS$.

An ideal $P$ of an AG-groupoid $S$ is *prime* (*semiprime*) if for any other ideals $A$, $B$ of $S$, $AB \subseteq P$ ($A^2 \subseteq P$) implies either $A \subseteq P$ or $B \subseteq P$ ($A \subseteq P$). A groupoid $S$ is called *fully semiprime* if every ideal of $S$ is semiprime. If $S$ is an AG-band then trivially $S$ is completely semiprime.

**Lemma 2.** *For every ideal $I$ of an AG-band $S$ we have*

$$\{x \in S \mid ax = x \; for \; a \in I\} \subseteq I \; and \; \{x \in S \mid ax = x \; for \; a \in I\} \subseteq I.$$

An AG-groupoid $S$ is called *totally ordered* if for all ideals $A$, $B$ of $S$ either $A \subseteq B$ or $B \subseteq A$.

**Theorem 3.** *Every ideal of an AG-band $S$ is prime if and only if the set of all ideals of $S$ is totally ordered.*

*Proof.* Assume that every ideal of an AG-band $S$ is prime. Let $P$, $Q$ be the ideals of $S$. Then $PQ \subseteq P$ and $PQ \subseteq Q$ imply that $PQ \subseteq P \cap Q$. Since $P \cap Q$ is prime, so $P \subseteq P \cap Q$ or $Q \subseteq P \cap Q$ imply that $P \subseteq Q$ or $Q \subseteq P$. Hence the set of all ideals of $S$ is totally ordered.

Conversely, let $I$, $J$ and $P$ be ideals of an AG-band $S$ such that $IJ \subseteq P$. Being ideals of $S$ they are totally ordered and that $I \subseteq J$. Thus $P$ is prime. □

**Theorem 4.** *If $I$ and $J$ are ideals of an AG-band $S$ then $IJ = I \cap J$.*

*Proof.* Let $I$ and $J$ be ideals of an AG-band $S$. Obviously, $IJ \subseteq I \cap J$. Since $I \cap J \subseteq I$, $I \cap J \subseteq J$, therefore $(I \cap J)^2 \subseteq IJ$. □

By Theorem 4, $IJ = JI$. Therefore the following Lemma is an easy consequence.

**Lemma 3.** *The set of ideals of an AG-band $S$ form a semilattice structure.*

An ideal $I$ of an AG-groupoid $S$ is said to be *strongly irreducible* if and only if for ideals $H$ and $K$ of $S$, $H \cap K \subseteq I$ implies that $H \subseteq I$ or $K \subseteq I$. This leads to the following important theorem with a rather straight forward proof.

**Theorem 5.** *In an AG-band every ideal is strongly irreducible if and only if it is a prime ideal.*

An AG-groupoid $S$ is (*left, right*) *simple*, if $S$ contains no proper (left, right) ideals. Left simple, right simple and simple AG-bands coincide. The AG-band from Example 1 is not simple because $\{2, 4, 5, 6\}$ is a proper ideal of $S$.

An AG-groupoid $S$ with zero is called *zero-simple* if $\{0\}$ and $S$ are its only ideals and $S^2 \neq \{0\}$.

**Example 2.** Let $S = \{1, 2, 3, 4\}$ and the operation be defined on $S$ as follows:

| $\cdot$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 4 | 2 | 3 |
| 2 | 3 | 2 | 4 | 1 |
| 3 | 4 | 1 | 3 | 2 |
| 4 | 2 | 3 | 1 | 4 |

Then, as in [11], $(S, \cdot)$ is a simple AG-band. If we adjoin 0 in $S$ then it become a zero-simple AG-band.

**Theorem 6.** *If $aS = Sa$ for all non-zero $a$ in an AG-band $S$, then $S$ is zero-simple if and only if $(Sa)S = S$.*

*Proof.* Clearly $S^2 \neq \{0\}$ and $S^3 = S$. Now for any $a$ in $S \backslash \{0\}$ the subset $(Sa)S$ of $S$ is an ideal of $S$. Therefore either $(Sa)S = S$ or $(Sa)S = \{0\}$. If $(Sa)S = \{0\}$, then the set $I = \{x \in S : (Sx)S = \{0\}\}$ contains an element other than zero, and $I$ becomes an ideal of $S$. As $S$ is zero-simple so by definition $I = S$, that is, $(Sx)S = \{0\}$ for every $x$ in $S$. This implies that $S^3 = \{0\}$. But this is a contradiction to the fact that $S = S^3$. Hence $(Sa)S = S$.

Conversely, assume that, $(Sa)S = S$ for every $a$ in $S \backslash \{0\}$. Also if $A$ is an ideal of $S$ containing $a$, then $(SA)S \subseteq A$ implies $(Sa)S \subseteq A$. □

**Corollary 1.** *$S$ is simple if and only if $(Sa)S = S$.*

*Proof.* If $S$ is a simple AG-band, then $(Sa)S$ is an ideal of $S$ and so $(Sa)S = S$. Conversely, if $(Sa)S = S$ for all $a \in S$, then we need to show that $S$ is simple. Let $A$ be an ideal of $S$ and $a \in A$. Then $(SA)S \subseteq A$ implies that $(Sa)S \subseteq A$. Now, if $0 \in S$, then $(S0)S = \{0\} \neq S$. As $(Sa)S = S$ holds for all $a \in S$, it means that $0 \notin S$. Hence $S$ without zero has no ideal except $S$ itself. □

An ideal $M$ in an AG-groupoid $S$ with zero is called *zero-minimal* if it is minimal in the set of all non-zero ideals.

**Proposition 3.** *If $M$ is a zero-minimal ideal of an AG-band $S$ such that $aS = Sa$ for all non-zero $a \in S$, then $M$ is a zero-simple AG-band.*

*Proof.* Clearly $M = M^3$ and if $a \in M\backslash\{0\}$, then $(Sa)S$ is an ideal of $S$ contained in $M$. It is non-zero, since it contains $a$, and so $(Sa)S = M$. Thus using (2) and (1) we get

$$(Ma)M \subseteq (Sa)S = M = M^3 = (M((Sa)S))M \subseteq (Ma)M,$$

which implies $(Ma)M = M$. By Theorem 6, $M$ is zero-simple. □

**Proposition 4.** *Let $S$ be an AG-band without zero. If $K$ is a minimal ideal of $S$, then $K$ is a simple AG-band.*

*Proof.* Note that $0 \notin S$ implies $0 \notin K$. As $K$ is uniquely minimum so it cannot contain any other ideal of $S$. Hence $K$ is a simple AG-band. □

## 3. Ideals in an AG$^*$-groupoid

An AG-groupoid $S$ is called an *AG$^*$-groupoid* if it satisfies one of the following equivalent weak associative laws [10]:

$$(ab)c = b(ac), \tag{3}$$

$$(ab)c = b(ca). \tag{4}$$

From (3) and (4), we obtain

$$b(ac) = b(ca) \tag{5}$$

for all $a, b, c \in S$.

If all elements of an AG$^*$-groupoid $S$ are idempotent, then $S = S^2$. This further implies that $S$ is a commutative semigroup [10].

If $S$ is an AG$^*$-groupoid and $a = a^2$ (for a fixed element $a \in S$) then, as it is proved in [10], $aS = Sa$ and $(xa)y = x(ay)$ for any $x, y \in S$. If $a$ belongs to $Sa = aS$, then $Sa = aS$ is a semilattice.

A non-associative left simple (right simple, simple) AG$^*$-groupoid does not exist [9]. $SA$ is a left ideal of an AG$^*$-groupoid $S$ for all subsets $A$ of $S$.

**Lemma 4.** *If $I$ is a right ideal of an $AG^*$-groupoid $S$ and $J$ is a subset of $S$ then $IJ$ is a left ideal of $S$ and it is a right ideal if $IJ = JI$, and $a(IJ)$ $\{(JI)a\}$ becomes a left (right) ideal of $S$.*

*Proof.* The proof is straight forward. □

By $\mathcal{K}$ we shall mean the set of all ideals of an AG$^*$-groupoid $S$.

**Proposition 5.** *In any $AG^*$-groupoid:*

(*i*) *$\mathcal{K}$ has associative powers,*

(*ii*) *$I^m I^n = I^{m+n}$, for all $I \in \mathcal{K}$,*

(*iii*) *$(I^m)^n = I^{mn}$, for all $I \in \mathcal{K}$ and all positive integers $m$, $n$,*

(*iv*) *$(AB)^n = A^n B^n$ for $n \geqslant 1$ and $(AB)^n = B^n A^n$ for $n \geqslant 2$, $\forall A, B \in \mathcal{K}$.*

*Proof.* The proof is obvious. □

**Lemma 5.** *If $I$ is an ideal of an $AG^*$-groupoid $S$ then so is $I^n$ for $n \geqslant 2$.*

*Proof.* Let $I$ be a right ideal of an AG$^*$-groupoid $S$ and $x = ij \in I^2$ where $i, j \in I$. Using identity (3), we get

$$\begin{aligned} s(ij) &= (is)j \subseteq II = I^2, \\ (ij)s &= j(is) \subseteq II = I^2, \end{aligned}$$

which shows that $I^2$ is an ideal of $S$. Now suppose that $I^{n-1}$ is an ideal. Then using (1), (3), and Proposition 5(*ii*), we get

$$\begin{aligned} I^n S &= (I^{n-1} I)S = (SI)I^{n-1} \subseteq II^{n-1} = I^n, \\ SI^n &= S(I^{n-1} I) = (IS)I^{n-1} \subseteq I^n, \end{aligned}$$

which completes the proof. □

**Lemma 6.** *If $I$ is an ideal of an $AG^*$-groupoid $S$ and $a = a^2$, then $aI^2$ is an ideal of $S$.*

*Proof.* Using Proposition $5(iv)$ and identity (3), we get $I^2a = aI^2$. Then it is not difficult to see that $aI^2$ is an ideal. □

An ideal $I$ of an AG-groupoid $S$ is called *minimal* if and only if it does not contain any ideal of $S$ other than itself.

**Theorem 7.** *If $I$ is a minimal right ideal of an $AG^*$-groupoid $S$ then for all $a \in S$ $Ia$ is a minimal left ideal of $S$.*

*Proof.* Let $I$ be the minimal right ideal of an AG$^*$-groupoid $S$ and $x = ia \in Ia$, where $i \in I$. Then using identity (3) we get $sx = s(ia) = (is)a \in Ia$ which shows that $Ia$ is a left ideal of $S$. Let $H$ be a non-empty left ideal of $S$ properly contained in $Ia$. Define $H' = \{r \in I : ra \in H\}$. If $y \in H'$, then $ya \in H$, and so $(ys)a = s(ya) \in SH \subseteq H$, imply that $H'$ is a right ideal of $S$ properly contained in $I$. This is a contradiction to the minimality of $I$. Hence $Ia$ is a minimal left ideal of $S$. □

**Theorem 8.** *If $I$ is a minimal left ideal of an $AG^*$-groupoid $S$ then $aI$ $(a^2 = a)$ is a minimal right ideal of $S$.*

*Proof.* Let $ai \in aI$ where $I$ is a minimal left ideal of an AG$^*$-groupoid $S$. Then using identities (3) and (2) we get

$$ia = i(aa) = (ai)a = (ai)(aa) = (aa)(ia) = a(ia) = (aa)i = ai.$$

Also $(ai)s = (ia)s = a(is) \in aI$, shows that $aI$ is a right ideal of $S$. Let $H$ be a non-empty right ideal of $S$ properly contained in $aI$. Define $H' = \{r : ar \in I\}$. Then $a(sy) = (sy)a = (ay)s \in HS \subseteq H$ imply that $H'$ is a left ideal of $S$ properly contained in $I$. But this is a contradiction to the minimality of $I$. Hence $aI$ is a minimal left ideal of $S$. □

**Theorem 9.** *Every ideal of an $AG^*$-groupoid $S$ is prime if and only if it is idempotent and the set of all ideals of $S$ is totally ordered.*

*Proof.* Let every ideal of $S$ be prime. Assume that $I$ is any ideal of $S$. Then $I^2$ is an ideal of $S$ by Lemma 5. Also $I^2 \subseteq I$ implies that $I \subseteq I^2$ or $I = I^2$. If $P$ and $Q$ are any ideals of $S$ then, $PS \subseteq P$ and $SQ \subseteq Q$ implies that $PQ \subseteq P$ and $PQ \subseteq Q$, and so $PQ \subseteq P \cap Q$. Since intersection of two prime ideals is prime. So, $P \subseteq P \cap Q$ or $Q \subseteq P \cap Q$. This implies that $P \subseteq Q$ or $Q \subseteq P$. Hence the set of all ideals of $S$ is totally ordered.

Conversely, assume that every ideal of $S$ is idempotent and the set of all ideals of $S$ is totally ordered. Let $I$, $J$ and $P$ be any ideals of $S$ such that $IJ \subseteq P$ with $I \subseteq J$. Then $I = I^2 = II \subseteq IJ \subseteq P$, implies that every ideal of $S$ is prime. □

## References

[1] **G. Birkhoff**: *Lattice Theory*, AMS Colloq. Publication, 1954.

[2] **J. S. Golan**: *The theory of semirings with applications in mathematics and theoretical computer science*, Pitman Monographs and Surveys in Pure and Appl. Math., 54, London, 1992.

[3] **P. Holgate**: *Groupoids satisfying a simple invertive law*, Math. Stud. **61** (1992), 101 – 106.

[4] **M. A. Kazim and M. Naseeruddin**: *On almost-semigroups*, Alig. Bull. Math. **2** (1972), 1 – 7.

[5] **Q. Mushtaq and S. M. Yusuf**: *On LA-semigroups*, Alig. Bull. Math. **8** (1978), 65 – 70.

[6] **Q. Mushtaq**: *Abelian groups defined by LA-semigroups*, Studia Scient. Math. Hungar. **18** (1983), 427 – 428.

[7] **Q. Mushtaq and Q. Iqbal**: *Decomposition of a locally associative LA-semigroup*, Semigroup Forum **41** (1990), 154 – 164.

[8] **Q. Mushtaq and M. Iqbal**: *On representation theorem for inverse LA-semigroups*, Proc. Pakistan Acad. Sci. **30** (1993), 247 – 253.

[9] **P. V. Protić and N. Stevanović**: *On Abel-Grassmann's groupoids*, Proc. Math. Conf. Pristina, 1994, 31 – 38.

[10] **P. V. Protić and N. Stevanović**: *AG-test and some general properties of Abel-Grassmann's groupoids*, PU. M. A, **6** (1995), 371 – 383.

[11] **P. V. Protić and N. Stevanović**: *Abel-Grassmann's bands*, Quasigroups and Related Systems **11** (2004), 95 – 101.

[12] **N. Stevanović and P. V. Protić**: *Some decomposition of Abel-Grassmann's groupoids*, PU. M. A. **8** (1997), 355 – 366.

Received October 17, 2005

Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
E-mail: qmushtaq@isb.apollo.net.pk

# Skew endomorphisms on n-ary groups

*Nikolay A. Shchuchkin*

**Abstract**

Let $\overline{x}^{(k)}$ denote this element of an $n$-ary group $G$ which is skew to $\overline{x}^{(k-1)}$, where $k \geqslant 1$ and $\overline{x}^{(0)} = x$. We find the identities defining the variety of all $n$-ary groups for which the operation $^{-(k)} : x \mapsto \overline{x}^{(k)}$ is an endomorphism.

## 1. Introduction

According to the general convention used in the theory of $n$-ary systems the sequence of elements $x_i, x_{i+1}, \ldots, x_j$ will be denoted by $x_i^j$. In the case $j < i$ it will be the empty symbol. If $x_{i+1} = x_{i+2} = \ldots = x_{i+t} = x$, then instead of $x_{i+1}^{i+t}$ we shall write $\overset{(t)}{x}$. In this convention $f(x_1, \ldots, x_n) = f(x_1^n)$ and

$$f(x_1, \ldots, x_i, \underbrace{x, \ldots, x}_{t}, x_{i+t+1}, \ldots, x_n) = f(x_1^i, \overset{(t)}{x}, x_{i+t+1}^n).$$

If $m = k(n-1)+1$, then the $m$-ary operation $g$ of the form

$$g(x_1^{k(n-1)+1}) := \underbrace{f(f(..., f(f}_{k}(x_1^n), x_{n+1}^{2n-1}), ...), x_{(k-1)(n-1)+2}^{k(n-1)+1})$$

will be denoted by $f_{(k)}$. In certain situations, when the arity of $g$ does not play a crucial role or when it will differ depending on additional assumptions, we will write $f_{(.)}$ to mean $f_{(k)}$ for some $k = 1, 2, ....$

For $n \geqslant 3$, there are several equivalent definitions of an $n$-ary group (see for example, [2], [6], [8], [10]). The definition given in [1] generalizes the definition of a binary group as follows:

The algebra $\langle G, f\rangle$ with the $n$-ary operation $f$ is called an *$n$-ary group* if for every $i = 1, 2, \ldots, n$ the following two conditions are satisfied:

2000 Mathematics Subject Classification: 20N15

Keywords: $n$-ary group, skew element, endomorphism.

1. the operation $f$ satisfies the general associative law:

$$f(f(x_1^n),x_{n+1}^{2n-1})=f(x_1^i,f(x_{i+1}^{i+n}),x_{i+n+1}^{2n-1}),\tag{1}$$

2. the equation $f(a_1^{i-1},x,a_{i+1}^n)=b$ has a unique solution $x\in G$ for all $a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n,b\in G^n$.

An algebra $\langle G,f\rangle$ satisfying (1) for all $i=1,2,\ldots,n$ is called an *$n$-ary semigroup*.

In an $n$-ary group $\langle G,f\rangle$ the solution $z$ of the equation

$$f(\overset{(n-1)}{x},z)=x,$$

is denoted by $\overline{x}$ and is called the *skew element* of $x$.

One can prove (see for example [1]) that

$$f(\overset{(i-1)}{x},\overline{x},\overset{(n-i)}{x})=x,\quad 1\leqslant i\leqslant n,$$

$$f(y\overset{(n-j-1)}{x},\overline{x},\overset{(j-1)}{x})=y,\quad 1\leqslant j\leqslant n-1\tag{2}$$

$$f(\overset{(i-1)}{x},\overline{x},\overset{(n-i-1)}{x},y)=y,\quad 1\leqslant i\leqslant n-1\tag{3}$$

for all $x,y\in G$.

Identities (1), (2) and (3) can be used as identities defining the variety of all $n$-ary groups (see [2], [6], [8], [10]).

For example, in [6] the following theorem is proved.

**Theorem 1.1.** *An $n$-ary $(n>2)$ semigroup $\langle G,f\rangle$ with the unary operation $^{-}:x\rightarrow\overline{x}$ is an $n$-ary group if and only if the identities* (2) *and* (3) *hold in $G$ for some $1\leqslant i,j\leqslant n-1$.*

Following Post [11], we say that two sequences $a_1^{n-1}$ and $b_1^{k(n-1)}$ of elements of $G$ are *equivalent* in an $n$-ary group $\langle G,f\rangle$ if the equation

$$f(x,a_1^{n-1})=f_{(k)}(x,b_1^{k(n-1)})\tag{4}$$

is valid for some $x\in G$.

**Lemma 1.2.** *If in an $n$-ary group $\langle G,f\rangle$ the sequences $a_1^{n-1}$ and $b_1^{k(n-1)}$ are equivalent, then the equation* (4) *is valid for all $x\in G$.*

*Proof.* Indeed, if this equality holds for some $x, a_1^{n-1}, b_1^{k(n-1)} \in G$, then

$$f(y, \overset{(n-3)}{x}, \overline{x}, f(x, a_1^{n-1})) = f(y, \overset{(n-3)}{x}, \overline{x}, f_{(k)}(x, b_1^{k(n-1)}))$$

is valid for all $y \in G$. Whence, according to the associativity of $f$, we obtain

$$f(f(y, \overset{(n-3)}{x}, \overline{x}, x), a_1^{n-1}) = f_{(k)}(f(y, \overset{(n-3)}{x}, \overline{x}, x), b_1^{k(n-1)}).$$

This, by (2), implies

$$f(y, a_1^{n-1}) = f_{(k)}(y, b_1^{k(n-1)}),$$

which completes the proof. □

## 2. Skew endomorphisms

W. A. Dudek posed in ([5]) several problems on the operation $\bar{}: x \to \overline{x}$ on $n$-ary groups. He asks (see also [4]) when this operation is an endomorphism, i.e., in which $n$-ary groups the identity

$$\overline{f(x_1^n)} = f(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n) \tag{5}$$

is satisfied.

The partial answer was given in [5]. Other answer is given in [13]. Namely, in [13] the following theorem is proved.

**Theorem 2.1.** *The operation* $\bar{}: x \to \overline{x}$ *is an endomorphism of an $n$-ary group $\langle G, f\rangle$ if and only if*

$$f(f(x, \overset{(n-1)}{u}, y), \ldots, f(x, \overset{(n-1)}{u}, y), \overset{(2)}{u}) = \\ f(\overset{(n-1)}{y}, f(u, f(x, \overset{(n)}{u}), \ldots, f(x, \overset{(n)}{u}), x, u), u)$$

*and*

$$f(\overset{n}{u}, f(\overset{n-1}{x}, u, u)) = f(f(\overset{n-1}{x}, u, u), \overset{n}{u})$$

*hold for all* $x, y, u \in G$.

It is clear that $\bar{}: x \to \overline{x}$ is an endomorphism in all commutative $n$-ary groups. Obviously, it is an endomorphism in all idempotent (also non-commutative) $n$-ary groups. Głazek and Gleichgewicht proved in [9] that it is an endomorphism in all *medial* $n$-ary groups, i.e., in $n$-ary groups satisfying the identity

$$f(\{f(x_{i1}^{in})\}_{i=1}^{i=n}) = f(\{f(x_{1i}^{ni})\}_{i=1}^{i=n}). \tag{6}$$

One can prove (see [2]) that an $n$-ary group $\langle G, f\rangle$ is medial if there exists an element $a \in G$ such that

$$f(x, \overset{(n-2)}{a}, y) = f(y, \overset{(n-2)}{a}, x) \tag{7}$$

holds for all $x, y \in G$.

Using (7) and the associativity of the operation $f$ it is not difficult to verify that the following theorem is true.

**Theorem 2.2.** *Each medial $n$-ary group satisfies the identity*

$$f_{(n-1)}(x_1, \overset{(n-2)}{x_2}, \overset{(n-2)}{x_3}, \ldots, \overset{(n-2)}{x_{n+1}}, x_{n+2}) = \\ f(x_1, \underbrace{f(x_{n+1}, x_n, ..., x_2), \ldots, f(x_{n+1}, x_n, ..., x_2)}_{n-2 \quad times}, x_{n+2}). \tag{8}$$

The identity (8) describes the class of $n$-ary groups for which $^{-} : x \to \overline{x}$ is an endomorphism.

**Theorem 2.3.** *The operation $^{-} : x \to \overline{x}$ is an endomorphism of an $n$-ary group $\langle G, f\rangle$ if and only if $\langle G, f\rangle$ satisfies* (8).

*Proof.* Let $^{-} : x \to \overline{x}$ be an endomorphism of an $n$-ary group $\langle G, f\rangle$, i.e., let (5) be satisfied. Then, according to (2) and (3), for any $x_2^{n+2} \in G$ we have

$$f_{(n-1)}(f(\overline{x}_{n+1}, \overline{x}_n, \ldots, \overline{x}_2), \overset{(n-2)}{x_2}, \overset{(n-2)}{x_3}, \ldots, \overset{(n-2)}{x_{n+1}}, x_{n+2}) = x_{n+2}$$

and

$$f(\overline{f(x_{n+1}, x_n, ..., x_2)}, \underbrace{f(x_{n+1}, x_n, ..., x_2), \ldots, f(x_{n+1}, x_n, ..., x_2)}_{n-2 \quad times}, x_{n+2}) = x_{n+2}$$

for all elements $x_2^{n+1} \in G$, which, by (5), means that the sequences $\overset{(n-2)}{x_2}, \overset{(n-2)}{x_3}, ..., \overset{(n-2)}{x_{n+1}}, x_{n+2}$ and $\underbrace{f(x_{n+1}, x_n, ..., x_2), ..., f(x_{n+1}, x_n, ..., x_2)}_{n-2 \quad times}, x_{n+2}$ are equivalent. So, in view of Lemma 1.1, the equality (8) is valid for all $x_1^{n+1} \in G$.

Conversely, let (8) be satisfied in an $n$-ary group $\langle G,f\rangle$. Then putting $x_1=f(\overline{y}_1,\overline{y}_2,\dots,\overline{y}_n)$, $x_{n+2}=\overline{f(y_1^n)}$ and $x_k=y_{n+2-k}$ for $2\leqslant k\leqslant n+1$ we see that the left hand side of (8) has the form

$$f_{(n-1)}(f(\overline{y}_1,\overline{y}_2,\dots,\overline{y}_n),\overset{(n-2)}{y_n},\overset{(n-2)}{y_{n-1}},\dots,\overset{(n-2)}{y_1},\overline{f(y_1^n)})=\overline{f(y_1^n)}.$$

On the right side of (8) we obtain

$$f(f(\overline{y}_1,\overline{y}_2,\dots,\overline{y}_n),\underbrace{f(y_1^n),\dots,f(y_1^n)}_{n-2\quad times},\overline{f(y_1^n)})=f(\overline{y}_1,\overline{y}_2,\dots,\overline{y}_n).$$

So, $\overline{f(y_1^n)}=f(\overline{y}_1,\overline{y}_2,\dots,\overline{y}_n)$ for all $y_1^n\in G$. This completes the proof. □

This theorem proves that the converse of Theorem 2.2 is not true. Indeed, in any idempotent $n$-ary group the operation $^{-}:x\to\overline{x}$ is the identity endomorphism but not any idempotent $n$-ary group is medial [11].

Let $\overline{x}^{(k)}$ be the skew element to $\overline{x}^{(k-1)}$, where $k\geqslant 1$ and $\overline{x}^{(0)}=x$, i.e., let $\overline{x}^{(1)}=\overline{x}$, $\overline{x}^{(2)}=\overline{\overline{x}}$, and so on. If $^{-}:x\to\overline{x}$ is an endomorphism of an $n$-ary group $\langle G,f\rangle$, then obviously $^{-(k)}:x\to\overline{x}^{(k)}$ is an endomorphism too. In some cases it is an automorphism (see [4] and [5]). However, the converse is not true. For example, in all ternary groups $\overline{\overline{x}}=x$, i.e., the operation $^{-(2)}:x\to\overline{\overline{x}}$ is the identity endomorphism, but in a ternary group $\langle S_3,f\rangle$ defined on the symmetric group $S_3$, where $f$ is the composition on three permutations, we have

$$\overline{f((12),(13),(123))}\neq(132)=f(\overline{(12)},\overline{(13)},\overline{(132)}).$$

Hence $^{-}:x\to\overline{x}$ is not an endomorphism of this group.

Since in ternary groups $\overline{\overline{x}}=x$ for all $x$, we have $\overline{x}^{(k)}=x$ if $k$ is even, and $\overline{x}^{(k)}=\overline{x}$ if $k$ is odd. Therefore, the operation $^{-(k)}:x\to\overline{x}^{(k)}$ is the identity endomorphism or coincides with the operation $^{-}:x\to\overline{x}$. From the last theorem it follows that $^{-}:x\to\overline{x}$ is an endomorphism of a ternary group if and only if this group is medial. In this case $^{-}:x\to\overline{x}$ is an automorphism.

Other important properties of operations $^{-(k)}:x\to\overline{x}^{(k)}$ in $n$-ary groups satisfying some additional properties are described in [3] and [4].

Following Post [11] an *$n$-ary power* of an element $x$ in an $n$-ary group $\langle G,f\rangle$ is defined as $x^{<0>}=x$ and $x^{<k+1>}=f(\overset{(n-1)}{x},x^{<k>})$ for all $k>0$.

In this convention $x^{<-k>}$ means $z \in G$ such that $f(x^{<k-1>}, \overset{(n-2)}{x}, z) = x^{<0>} = x$.

It is not difficult to verify that the following exponential laws hold

$$f(x^{<s_1>}, x^{<s_2>}, \ldots, x^{<s_n>}) = x^{<s_1+s_2+\ldots+s_n+1>},$$
$$(x^{<r>})^{<s>} = x^{<rs(n-1)+s+r>} = (x^{<s>})^{<r>}.$$

Using the above laws we can see that $\overline{x} = x^{<-1>}$ and, consequently

$$\overline{x}^{\,(2)} = (x^{<-1>})^{<-1>} = x^{<n-3>},$$
$$\overline{x}^{\,(3)} = ((x^{<-1>})^{<-1>})^{<-1>},$$

and so on. Generally: $\overline{x}^{\,(k)} = (\overline{x}^{\,(k-1)})^{<-1>}$ for all $k \geqslant 1$. This implies (see [3] or [4]) that $\overline{x}^{\,(k)} = x^{<S_k>}$ for

$$S_k = -\sum_{i=0}^{k-1}(2-n)^i = \frac{(2-n)^k - 1}{n-1}\,.$$

For even $k$ we have $S_k = \frac{(n-2)^k-1}{n-1}$. Hence

$$\overline{x}^{\,(k)} = f_{(\cdot)}(\overset{((n-2)^k)}{x}) \tag{9}$$

for even $k$. In particular $\overline{\overline{x}} = x^{<n-3>} = f_{(n-3)}(\overset{((n-2)^2)}{x})$. Thus the operation ${}^{-(k)} : x \to \overline{x}^{\,(k)}$ coincides with the operation ${}^{<S_k>} : x \to x^{<S_k>}$. So, the operation ${}^{-(k)} : x \to \overline{x}^{\,(k)}$ is an endomorphism if and only if

$$f(x_1^n)^{<S_k>} = f(x_1^{<S_k>}, x_2^{<S_k>}, \ldots, x_n^{<S_k>})$$

is valid for all $x_1^n \in G$. This implies

**Theorem 2.4.** *For even $k$ the operation ${}^{-(k)} : x \to \overline{x}^{\,(k)}$ is an endomorphism of an $n$-ary group $\langle G, f\rangle$ if and only if the identity*

$$f_{(\cdot)}(\underbrace{f(x_1^n), \ldots, f(x_1^n)}_{(n-2)^k}) = f_{(\cdot)}(\overset{((n-2)^k)}{x_1}, \overset{((n-2)^k)}{x_2}, \ldots, \overset{((n-2)^k)}{x_n})$$

*is satisfied.*

**Theorem 2.5.** *For odd $k$ the operation $^{-(k)} : x \to \overline{x}^{(k)}$ is an endomorphism of an $n$-ary group $\langle G, f\rangle$ if and only if the identity*

$$\begin{aligned} &f_{(\cdot)}(x_1, \overset{((n-2)^k)}{x_2}, \overset{((n-2)^k)}{x_3}, \ldots, \overset{((n-2)^k)}{x_{n+1}}, x_{n+2}) = \\ &\qquad f_{(\cdot)}(x_1, \underbrace{f(x_{n+1}, x_n, \ldots, x_2), \ldots, f(x_{n+1}, x_n, \ldots, x_2)}_{(n-2)^k}, x_{n+2}), \end{aligned} \tag{10}$$

*is satisfied.*

*Proof.* Let $k$ be odd and let $^{-(k)} : x \to \overline{x}^{(k)}$ be an endomorphism of an $n$-ary group $\langle G, f\rangle$. From (2), (3) we get

$$f_{(\cdot)}(y, \overset{((n-2)^k)}{x}, \overset{((n-2)^{k-1})}{\overline{x}}) = f_{(\cdot)}(y, \overset{(n-2)}{x}, \overline{x}, \ldots, \overset{(n-2)}{x}, \overline{x}) = y, \tag{11}$$

$$f_{(\cdot)}(\overset{((n-2)^{k-1})}{\overline{x}}, \overset{((n-2)^k)}{x}, y) = f_{(\cdot)}(\overline{x}, \overset{(n-2)}{x}, \ldots, \overline{x}, \overset{(n-2)}{x}, y) = y. \tag{12}$$

Consequently

$$f_{(\cdot)}(f_{(\cdot)}(\overset{((n-2)^{k-1})}{\overline{x}_{n+1}}, \overset{((n-2)^{k-1})}{\overline{x}_n}, \ldots, \overset{((n-2)^{k-1})}{\overline{x}_2}), \overset{((n-2)^k)}{x_2}, \ldots, \overset{((n-2)^k)}{x_{n+1}}, x_{n+2}) = x_{n+2}$$

and

$$\begin{aligned} &f_{(\cdot)}(\underbrace{\overline{f(x_{n+1}, x_n, \ldots, x_2)}, \ldots, \overline{f(x_{n+1}, x_n, \ldots, x_2)}}_{(n-2)^{k-1}}, \\ &\qquad\qquad \underbrace{f(x_{n+1}, x_n, \ldots, x_2), \ldots, f(x_{n+1}, x_n, \ldots, x_2)}_{(n-2)^k}, x_{n+2}) = x_{n+2}. \end{aligned}$$

Since $k-1$ is even, by (9) we have $\overline{x}^{(k)} = \overline{(\overline{x})}^{(k-1)} = f_{(\cdot)}(\overset{((n-2)^{k-1})}{\overline{x}})$ for all $x \in G$. Thus

$$\overline{f(x_{n+1}, x_n, \ldots, x_2)}^{(k)} = f_{(\cdot)}(\underbrace{\overline{f(x_{n+1}, x_n, \ldots, x_2)}, \ldots, \overline{f(x_{n+1}, x_n, \ldots, x_2)}}_{(n-2)^{k-1}})$$

and

$$f_{(\cdot)}(\overset{((n-2)^{k-1})}{\overline{x}_{n+1}}, \overset{((n-2)^{k-1})}{\overline{x}_n}, \ldots, \overset{((n-2)^{k-1})}{\overline{x}_2}) = f_{(\cdot)}(\overline{x}_{n+1}^{(k)}, \overline{x}_n^{(k)}, \ldots, \overline{x}_2^{(k)}),$$

whence

$$f_{(\cdot)}(\overset{((n-2)^{k-1})}{\overline{x}_{n+1}}, \overset{((n-2)^{k-1})}{\overline{x}_{n}}, \ldots, \overset{((n-2)^{k-1})}{\overline{x}_{2}}) =$$
$$f_{(\cdot)}(\underbrace{\overline{f(x_{n+1}, x_n, \ldots, x_2)}, \ldots, \overline{f(x_{n+1}, x_n, \ldots, x_2)}}_{(n-2)^{k-1}}).$$

This, together with the above two identities containing $x_{n+2}$, means that the sequences:

$$\overset{((n-2)^{k})}{x_2}, \overset{((n-2)^{k})}{x_3}, \ldots, \overset{((n-2)^{k})}{x_{n+1}}, x_{n+2}$$

and

$$\underbrace{f(x_{n+1}, x_n, \ldots, x_2), \ldots, f(x_{n+1}, x_n, \ldots, x_2)}_{(n-2)^{k}}, \; x_{n+2}$$

are equivalent. Hence, by Lemma 1.2, the equality (10) is valid for all $x_1^{n+2} \in G$.

On the other hand, if (10) is valid for all $x_1^{n+2} \in G$, then for

$$\begin{aligned} x_1 &= f_{(\cdot)}(\overset{((n-2)^{k-1})}{\overline{y}_1}, \overset{((n-2)^{k-1})}{\overline{y}_3}, \ldots, \overset{((n-2)^{k-1})}{\overline{y}_n}), \\ x_k &= y_{n+2-k}, \quad \text{for} \;\; k = 2, 3, \ldots, n+1, \\ x_{n+2} &= f_{(\cdot)}(\underbrace{\overline{f(y_1^n)}, \overline{f(y_1^n)}, \ldots, \overline{f(y_1^n)}}_{(n-2)^{k-1}}) = f_{(\cdot)}(\overset{((n-2)^{k-1})}{\overline{f(y_1^n)}}), \end{aligned}$$

it has the form

$$f_{(\cdot)}(f_{(\cdot)}(\overset{((n-2)^{k-1})}{\overline{y}_1}, \ldots, \overset{((n-2)^{k-1})}{\overline{y}_n}), \overset{((n-2)^{k})}{y_n}, \ldots, \overset{((n-2)^{k})}{y_2}, \overset{((n-2)^{k})}{y_1}, f_{(\cdot)}(\overset{((n-2)^{k-1})}{\overline{f(y_1^n)}}) =$$
$$f_{(\cdot)}(f_{(\cdot)}(\overset{((n-2)^{k-1})}{\overline{y}_1}, \ldots, \overset{((n-2)^{k-1})}{\overline{y}_n}), \overset{((n-2)^{k})}{f(y_1^n)}, f_{(\cdot)}(\overset{((n-2)^{k-1})}{\overline{f(y_1^n)}})).$$

Whence, applying (11) and (12), we obtain

$$f_{(\cdot)}(\overset{((n-2)^{k-1})}{\overline{f(y_1^n)}}) = f_{(\cdot)}(\overset{((n-2)^{k-1})}{\overline{y}_1}, \ldots, \overset{((n-2)^{k-1})}{\overline{y}_n}).$$

But, by (9), for all $y \in G$ we have $f_{(\cdot)}(\overset{((n-2)^{k-1})}{\overline{y}}) = \overline{(\overline{y})}^{(k-1)} = \overline{y}^{(k)}$. Thus, the last identity implies

$$\overline{f(y_1^n)}^{(k)} = f(\overline{y}_1^{(k)}, \overline{y}_2^{(k)}, \ldots, \overline{y}_n^{(k)}).$$

Therefore, ${}^{-(k)} : x \longrightarrow \overline{x}^{(k)}$ is an endomorphism. □

Note that for any finite $n$-ary group there exists a natural number $m$ such that $\overline{x}^{(m)} = x$ holds for all $x \in G$. The same holds also in some infinite $n$-ary groups (see for example [3]). In these groups endomorphisms ${}^{-(k)} : x \longrightarrow \overline{x}^{(k)}$ are automorphisms.

## References

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

[2] **W. A. Dudek:** *Remarks on n-groups*, Demonstratio Math. **13** (1980), 165 – 181.

[3] **W. A. Dudek:** *Autodistributive n-groups*, Commentationes Math. Annales Soc. Math. Polonae, Prace Matematyczne **23** (1983), 1 – 11.

[4] **W. A. Dudek:** *Medial n-groups and skew elements*, Proceedings of the V Universal Algebra Symposium "Universal and Applied Algebra", Turawa 1988, World Scientific, Singapore 1989, 55 – 80.

[5] **W. A. Dudek:** *On some old and new problems in n-ary groups*, Quasigroups and Related Systems **8** (2001), 15 – 36.

[6] **W. A. Dudek, K. Glazek and B. Gleichgewicht:** *A note on the axioms of n-groups*, Coll. Math. Soc. J. Bolyai **29** "Universal Algebra", Esztergom (Hungary) 1977, 195 – 202, North-Holland, Amsterdam, 1982.

[7] **A. M. Gal'mak:** *Remarks on polyadic groups*, Quasigroups and Related Systems **7** (2000), 67 – 71.

[8] **A. M. Gal'mak:** *n-ary Groups, I*, (Russian), Gomel State University, 2003.

[9] **K. Głazek and B. Gleichgewicht:** *Abelian n-groups*, Coll. Math. Soc. J. Bolyai **29** "Universal Algebra", Esztergom (Hungary) 1977, 321 – 329, North-Holland, Amsterdam, 1982.

[10] **A. G. Kurosh:** *General algebra. Lectures of* 1969 – 1970 *educational year*, (Russian), Moscow, Nauka, 1974.

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

[12] **N. A. Shchuchkin:** *Interconnection of $n$-groups and groups*, Chebyshevski Sbornik **4** (2003), 125 – 141.

[13] **F. M. Sokhatsky:** *On Dudek's problems on the skew operation in polyadic groups*, East Asian Math. J. **19** (2003), 63 – 71.

Received 11 November 2004
Revised November 30, 2006

Volgograd State Pedagogical University
Lenina prosp., 27
400131 Volgograd
Russia
e-mail: shchuchkin@fizmat.vspu.ru