Bulletin of the Iranian Mathematical Society Vol. 38 *No. 4* (*2012*), *pp 1063-1077.*

SMARANDACHE ALGEBRAS AND THEIR SUBGROUPS

P. J. ALLEN, H. S. KIM* AND J. NEGGERS

Communicated by Jamshid Moori

Abstract. In this paper we define Smarandache algebras and show that every finite group can be found in some Smarandache algebra. We define and study the Smarandache degree of a finite group and determine the Smarandache degree of several classes of finite groups such as cyclic groups, elementary abelian p-groups, and dihedral groups D_p.

1. Introduction

The notion of Smarandache was introduced by Smarandache, and Kandasamy [6] studied the concept of Smarandache groupoids, Smarandache Bol groupoids and obtained several interesting results. Padilla [7] discussed Smarandache algebraic structures. Jun [5] studied a Smarandache structure on BCC-algebras, and introduced the notion of Smarandache BCC-ideals and obtained some conditions for a (special) subset to be a Smarandache BCC-ideal. The present authors [1, 2] discussed Smarandache disjointness in BCK/d-algebras. Hummadi and Muhammad [4] studied tripotent elements and Smarandache triple tripotnents in the ring of integers modulo n and in some group ring. Recently, .

MSC(2010): Primary: 20D99; Secondary: 20F99
Keywords: Smarandache algebras and groups.
Received: 16 November 2009, Accepted: 10 May 2010.
∗Corresponding author
© 2012 Iranian Mathematical Society.

Saeid [7] discussed Smarandache weak BE-algebras. For more information on the notion of Smarandache we refer to [6].

In this paper we define Smarandache algebras and show that every finite group can be found in some Smarandache algebra. We define and study the Smarandache degree of a finite group and determine the Smarandache degree of several classes of finite groups such as cyclic groups, elementary abelian p-groups, and dihedral groups D_p.

2. Smarandache algebras

Let $P(x, y) \in K[x, y]$ denote a polynomial in two variables having coefficients in the field K. We define the binary operation $* : K \times K \to K$ by $a * b = P(a, b)$; that is, $a * b$ is the value of the polynomial at (a, b). When the polynomial $P(x, y)$ has degree n, the binary system $(K, *)$ will be called a *polynomial algebra of degree n*. The binary system $(K, *)$ will be called a *Smarandache algebra* provided K contains a subset G with more than one element such that $(G, *)$ is a group. Whenever the binary system $(K, *)$ has a non-trivial subgroup under the induced multiplication $*$, we will call $P(x, y)$ a *Smarandache polynomial*. We begin with several instructive examples.

Example 2.1. Let $K = Z_5 = \{0, 1, 2, 3, 4\}$ be the field of integers modulo 5 and define $P(x, y) = x + y + xy + x^2y^2 \in K[x, y]$. The product $2 * 4$ is illustrated

$$2 * 4 = P(2, 4) = 2 + 4 + 2 \cdot 4 + 2^2 \cdot 4^2 = 78 = 3 \pmod 5$$

Since $P(x, y)$ has degree 4, it follows that $(K, *)$ is a polynomial algebra of degree 4 and has its complete multiplication table given below:

$*$	0	1	4	2	3
0	0	1	4	2	3
1	1	4	0	4	1
4	4	0	1	3	3
2	2	4	3	4	2
3	3	1	3	2	1

The elements of K were arranged in the multiplication table to emphasize that $G = \{0, 1, 4\}$ is a subgroup of $(K, *)$. Clearly, G is the familiar cyclic group of order 3 with identity 0. Consequently, $(K, *)$ is a Smarandache algebra of degree 4. It is also clear that elements outside the subgroup G may not satisfy the associative law. For example, $(2*1)*3 \neq 2*(1*3)$.

Example 2.2. Let $P(x,y) = x^2 + y^2$ be a polynomial of degree 2 over the field $K = Z_3$ of integers modulo 3. The polynomial algebra $(K,*)$ of degree 2 has the following multiplication table:

$*$	0	1	2
0	0	1	1
1	1	2	2
2	1	2	2

Although $(K,*)$ is an associative binary system, it does not contain a non-trivial subgroup. Consequently, $(K,*)$ is not a Smarandache algebra, or equivalently, $P(x,y)$ is not a Smarandache polynomial over the field Z_3.

Our first theorem will demonstrate that any finite algebraic system can be found within an appropriately chosen polynomial algebra.

Theorem 2.3. *Let $A = \{a_1, a_2, \cdots, a_n\}$ be a finite set with n elements and suppose that $\circ : A \times A \to A$ is a binary operation on A; that is, $(A, \circ)$ is a finite binary system with n elements. If K is any field containing at least n elements, then there exists a polynomial $P(x,y)$ of degree at most $2n$ with coefficients in K such that the polynomial algebra $(K,*)$ contains a subalgebra $(S,*)$ that is isomorphic to $(A,\circ)$.*

Proof. Since K has at least n elements, we can select any n distinct elements $z_1, z_2, \cdots, z_n$ from K. Define a map $\varphi : A \to S$ by $\varphi(a_i) = z_i$. Since $(A,\circ)$ is a binary system, it is clear that $a_i \circ a_j = a_k$ for some k and we take $z_k = \varphi(a_k)$. Given $i, j \in \{1, 2, \cdots, n\}$ we define

$$P_{ij}(x,y) = z_k(xy - z_i z_j + 1)\frac{\prod_{t\neq i}(x - z_t)\prod_{s\neq j}(y - z_s)}{\prod_{t\neq i}(z_i - z_t)\prod_{s\neq j}(z_j - z_s)}.$$

It is clear that $P_{ij}(x,y) \in K[x,y]$ and has degree $2 + 2(n-1) = 2n$. From direct substitution, it follows that

$$P_{ij}(z_u, z_v) = \begin{cases} z_k, & \text{if } u = i \text{ and } v = j, \\ 0, & \text{otherwise.} \end{cases}$$

Define

$$P(x,y) = \sum_{1 \le i,j \le n} P_{ij}(x,y). \tag{2.1}$$

Then $P(z_i, z_j) = z_k$ and it follows that

$$\varphi(a_i \circ a_j) = \varphi(a_k) = z_k = P(z_i, z_j) = z_i * z_j = \varphi(a_i) \circ \varphi(a_j).$$

That is, φ is an isomorphism mapping the algebra $(A, \circ)$ onto the algebra $(S, *)$. Cancellation of terms in the sum (1) is always possible. Consequently, the degree of the polynomial $P(x,y)$ is at most $2n$. □

Corollary 2.4. *If G is a finite group of order n, then there exists a field K and a polynomial $P(x,y)$ of degree at most $2n$ such that the Smarandache algebra $(K,*)$ contains a subalgebra $(B,*)$ that is isomorphic to G.*

The finite group G has *Smarandache degree m*, denoted by $sd(G) = m$, provided G can be found within a polynomial algebra $(K,*)$ of degree m but is not contained within any polynomial algebra of degree less than m. In view of Corollary 2.4, a finite group G of order n has Smarandache degree less than or equal $2n$. In this article, we will investigate the Smarandache degree of several classes of finite groups.

Whenever $P(x,y)$ and $Q(x,y)$ are different polynomials in $K[x,y]$, each polynomial could be used to determine a polynomial algebra. We will denote their binary operations by $a *_p b = P(a,b)$ and $a *_q b = Q(a,b)$, respectively. Our next example will illustrate the argument given in the proof of Lemma 2.6 below.

Example 2.5. Let $K = Z_3 = \{0,1,2\}$ be the field of integers modulo 3, and let $P(x,y) = xy$. The polynomial algebra $(K, *_p)$ of degree 2 has multiplication table:

$*_p$	1	2	0
1	1	2	0
2	2	1	0
0	0	0	0

The cyclic group $G = \{1,2\}$ is clearly a subgroup of the polynomial algebra $(K, *_p)$. Unlike Example 1, where the identity of the subgroup was 0, this example now has identity $e = 1$. However, we can use $P(x, y)$ to define a new polynomial $Q(x, y) \in K[x, y]$ by

$$\begin{aligned} Q(x,y) &= P(x+1, y+1) - 1 \\ &= (x+1)(y+1) - 1 \\ &= x + xy + y. \end{aligned}$$

Clearly $Q(x, y)$ has the same degree as $P(x, y)$ and gives the polynomial algebra $(K, *_q)$ with multiplication table:

$*_q$	0	1	2
0	0	1	2
1	1	0	2
2	2	2	2

Observe that the cyclic group with two elements can now be found in the Smarandache algebra $(K, *_q)$ as $H = \{0, 1\}$ with identity $e = 0$.

Lemma 2.6. *Suppose that the group G can be found within the Smarandache algebra $(K, *_p)$ generated by a polynomial $P(x, y)$ of degree m. If G has the identity $e \in K$, then there exists an isomorphic algebra $(K, *_q)$ generated by a polynomial $Q(x, y)$ of degree m that contains a subgroup H isomorphic to G, and H has the identity $0 \in K$.*

Proof. Let $k \in K$. We use $P(x, y)$ to define a polynomial

$$Q(x, y) = P(x + k, y + k) - k$$

Moreover, define $\varphi : (K, *_p) \to (K, *_q)$ by $\varphi(g) = g - k$ for $g \in K$. Then

$$\begin{aligned} \varphi(a) *_q \varphi(b) &= (a-k) *_q (b-k) \\ &= Q(a-k, b-k) \\ &= P((a-k)+k, (b-k)+k) - k \\ &= P(a, b) - k \\ &= a *_p b - k \\ &= \varphi(a *_p b) \end{aligned}$$

and it follows that $\varphi : (K, *_p) \to (K, *_q)$ is an isomorphism. In particular, if we choose $k = e$, the above isomorphism gives $H = \varphi(G)$ as a subgroup of $(K, *_q)$ that is isomorphic to G, and H has the identity $\varphi(e) = e - e = 0$. $\square$

Throughout the remainder of this article, we will not distinguish between the group G and an isomorphic copy of it.

Lemma 2.7. *Suppose that G is a non-trivial finite group having Smarandache degree* 1. *Then G is contained in a Smarandache algebra $(K, *)$ constructed from the polynomial $P(x, y) = x + y$.*

Proof. In view of Lemma 2.6, we know that G is contained in an algebra $(K, *)$ of degree 1 where G has identity $0 \in K$. The polynomial $P(x, y)$ of degree 1 must have the form $P(x, y) = A + Bx + Cy$ where A, B and C are elements of the field K. Since 0 is the identity of G, $g = g*0 = A + Bg$ for every $g \in G$. Thus, $0 = A + (B - 1)g$ for every $g \in G \subset K$ immediately forces $A = 0$ and $B = 1$. Starting with $g = 0 * g$ will likewise give $C = 1$. Consequently, $P(x, y) = x + y$. □

The following basic results from the theory of fields can be found in Herstein [3]. There is a unique field, denoted by $GF(p^n)$, with p^n elements for every prime p and every positive integer n. The fields $GF(p^n)$ account for all finite fields. The additive group $(GF(p^n), +)$ is the direct sum of n copies of the additive cyclic group $(Z_p, +)$ of integers modulo p; that is,

$$GF(p^n) \cong Z_p \oplus Z_p \oplus \cdots \oplus Z_p.$$

Therefore, every non-zero element in $GF(p^n)$ has order p under addition. Consequently, $(GF(p^n), +)$ is an elementary abelian p-group.

Theorem 2.8. *Let G be a non-trivial finite group. Then G has Smarandache degree 1 if and only if G is an elementary abelian p-group.*

Proof. Suppose G has Smarandache degree 1. Lemma 2.7 implies that G can be found in the polynomial algebra $(K, *)$ where $P(x, y) = x + y$. Clearly, $a*b = a+b$ is addition in the field K. Since fields of characteristic 0 do not contain non-zero elements of finite order under addition, it follows that the non-trivial finite group G is a subset of K where K has prime characteristic p. Without loss of generality, we know that $G \subset GF(p^n) \subset K$ for some positive integer n. Thus,

$$G \subset GF(p^n) \cong Z_p \oplus Z_p \oplus \cdots \oplus Z_p$$

and it follows that G is an abelian p-group.

Suppose that G is an elementary abelian p-group. It is well-known that

$$G \cong Z_p \oplus Z_p \oplus \cdots \oplus Z_p$$

for some number, say n, copies of Z_p. Then G is clearly a subgroup of the polynomial algebra $(K, *)$ of degree 1, where $K = GF(p^n)$ and $P(x, y) = x + y$. It follows that the finite elementary abelian p-group has $sd(G) = 1$, and the proof is complete. $\square$

Theorem 2.9. *Let G be a non-trivial finite cyclic group.*

(i) *G has prime order p if and only if $sd(G) = 1$,*
(ii) *G has composite order if and only if $sd(G) = 2$.*

Proof. (i) Suppose that G has Smarandache degree 1. Theorem 2.8 immediately implies that G is a finite elementary abelian p-group. Since G is cyclic, it follows that G must be a cyclic group of order p. On the other hand, if G is a cyclic group of order p it is clear that G is isomorphic to the additive group Z_p. Consequently, G can be found in the polynomial algebra $(K, *)$ of degree 1 where $K = GF(p^1) \approx Z_p$ and $P(x, y) = x + y$.

(ii) Let K denote the field of complex numbers. Then the Smarandache algebra $(K, *)$ induced by the Smarandache polynomial $P(x, y) = xy$ is just the group of non-zero complex numbers under the usual complex multiplication. Obviously, $(K, *)$ contains many non-trivial subgroups. In particular, when $n > 1$ is an integer

$$G = \{e^{2\pi ik/n} \mid k = 0, 1, 2, \cdots, n - 1\}$$

is a finite cyclic subgroup of order n. Consequently, any finite cyclic group can be found as a subgroup of some Smarandache algebra $(K, *)$ that is induced by a Smarandache polynomial $P(x, y)$ with degree not greater than 2. In view of part (i), it is clear that a finite cyclic group of composite order must have Smarandache degree 2. $\square$

3. **Polynomial algebras**

Our next result demonstrates that polynomial algebras of degree less than four can not contain any non-abelian groups.

Theorem 3.1. *If G is a subgroup of the polynomial algebra $(K, *)$ of degree less than or equal to 3, then G is abelian.*

Proof. Assume that there exists a polynomial algebra of degree less than or equal to 3 that contains a non-abelian group G. Without loss of generality, we may in view of Lemma 2.6 suppose that the identity of G is $e = 0$ and that the polynomial algebra $(K, *)$ of degree less than or equal to 3 is generated by the polynomial

$$P(x, y) = A + Bx + Cy + Dx^2 + Exy + Fy^2 + Gx^3 + Hx^2y + Ixy^2 + Jy^3$$

where the coefficients $A, B, \cdots, J$ are elements of the field K. The elements of G will be denoted by

$$G = \{e = 0, g_1, g_2, \cdots, g_r\} \subset K$$

where each $g_i \neq 0$. Since G is non-abelian, G must contain at least 6 elements. Therefore, $r \geq 5$. Clearly, for each $g_i \in G$

$$g_i = g_i * 0 = P(g_i, 0) = A + Bg_i + Dg_i^2 + Gg_i^3 \tag{3.1}$$

and

$$g_i = 0 * g_i = P(0, g_i) = A + Cg_i + Fg_i^2 + Jg_i^3. \tag{3.2}$$

After subtracting (3.2) from (3.1) we obtain

$$0 = (B - C)g_i + (D - F)g_i^2 + (G - J)g_i^3. \tag{3.3}$$

Equation (3.3) shows that the polynomial

$$f(x) = (B - C)x + (D - F)x^2 + (G - J)x^3 \in K[x]$$

has at least 5 roots in the field K. Therefore, the polynomial $f(x)$ must be the zero polynomial; i.e., $B - C = 0, D - F = 0$, and $G - J = 0$. Consequently, $B = C, D = F, G = J$ and we can write $P(x, y)$ as

$$P(x, y) = A + B(x + y) + D(x^2 + y^2) + Exy + Hx^2y + Ixy^2 + G(x^3 + y^3)$$

After rewriting equation (3.1) above as $0 = A + (B - 1)g_i + Dg_i^2 + Gg_i^3$, it is also clear that the polynomial $h(x) = A + (B - 1)x + Dx^2 + Gx^3$ has at least 5 roots in K. Consequently, $h(x)$ must be the zero polynomial with $A = 0, B = 1, D = 0$ and $G = 0$. It now follows that

$$P(x, y) = (x + y) + xy(E + Hx + Iy). \tag{3.4}$$

If $I = H$, then it must follow that $a * b = P(a, b) = P(b, a) = b * a$ for every $a, b \in G$, a contradiction since G is non-abelian. Therefore, $I \neq H$. Since $e = 0$ and each $g_i \in G$ has an inverse, we may suppose that $g_j \in G$ is such that $g_i * g_j = g_j * g_i = 0$. Using equation (3.4) we have

$$0 = g_i + g_j + g_i g_j (E + H g_i + I g_j), \tag{3.5}$$

and

$$0 = g_j + g_i + g_j g_i (E + H g_j + I g_i). \tag{3.6}$$

Subtracting (3.6) from (3.5) gives

$$0 = (g_i g_j)(H - I)(g_i - g_j).$$

The product of elements in a field K can not be zero unless one of the factors is zero. Since $g_i g_j \neq 0$ and $H - I \neq 0$ it follows that $g_i - g_j = 0$. Consequently, $g_i = g_j$ and we have shown that each element of G is its own inverse. This immediately implies that G is abelian, a contradiction. □

Let Z_p denote the field of integers modulo the prime $p > 2$. Since the multiplicative group of any finite field is cyclic, it is clear that

$$G = \{g \in Z_p \,|\, g \neq 0\}$$

is multiplicatively a cyclic group of order $p - 1$. The elements of G can be written as

$$1, 2, 3, \cdots, \frac{p-1}{2}, -\frac{p-1}{2}, \cdots, -3, -2, -1$$

and consequently, $G^2 = \{1^2, 2^2, 3^2, \cdots, [\frac{p-1}{2}]^2\}$ since $g^2 = (-g)^2$ in any field. It is easy to see that the subgroup G^2 has order $\frac{p-1}{2}$. We will need the well known results in the next lemma. The proof is provided for the sake of completeness.

Lemma 3.2. *Let p be a prime, $p > 2$, and let Z_p denote the field of integers modulo p. Then*

(i) *The polynomial $x^2 + r \in Z_p[x]$, where $r \neq 0$, is irreducible over Z_p if and only if $-r \notin G^2$.*

(ii) *If $r \in G$ and $-r \notin G^2$, then $(-r)^{\frac{p-1}{2}} = -1$.*

Proof. (i) It is obvious that the quadratic $x^2 + r \in Z_p$ is irreducible if and only if it has no roots in Z_p. Part(i) follows immediately.

(ii) Since $p - 1$ is an even integer, we can write $p - 1 = 2^n q$ where q is an odd integer (note that q may be 1). A cyclic group has one and only one subgroup of order k for every positive divisor k of its order. Consequently, G contains a subgroup T of order 2^n and a subgroup H of order q. Since $\gcd(2^n, q) = 1$, it is clear that $T \cap H =< 1 >$. Moreover, $G = TH$. Clearly, $H =< h >= \{1, h, h^2, h^3, \cdots, h^{q-1}\}$ is a cyclic group of odd order q, since G is cyclic and any subgroup of a cyclic group must be cyclic. We know that h^s is a generator of H if and only if $\gcd(s, q) = 1$. Consequently, h^2 is a generator of H and it follows that $H^2 = H$. Therefore,

$$G^2 = (TH)^2 = T^2H^2 = T^2H.$$

We have already observed that G^2 has $\frac{p-1}{2}$ elements. It follows immediately that T^2 must have 2^{n-1} elements.

Next, suppose that $t \in T$ where $t \notin T^2$. Since T has order 2^n, it is clear that t has order 2^k where $1 \leq k \leq n$. Assume that $k < n$. Since T^2 is a cyclic group of order 2^{n-1}, and 2^k divides the order T^2, it follows that T^2 contains one and only one subgroup, say J, of order 2^k. However, we now have two distinct subgroups, J and $< t >$, of the cyclic group G with the same order, which is a contradiction. We have proven that if $t \in T$ where $t \notin T^2$, then t is a generator of T. So $t^{2^n} = 1$. Since -1 is the unique element of order 2 in G, and since the cyclic subgroup T must contain an element of order 2, it follows that $t^{2^{n-1}} = -1$.

Finally, let $r \in G$ where $-r \notin G^2$. We can write $r = th$ where $t \in T$ and $h \in H$. Clearly, $-r = -(th) = (-t)h$. Since $-r \notin G^2 = T^2H$, it follows that $-t \notin T^2$. We now have

$$\begin{aligned}
(-r)^{\frac{p-1}{2}} &= (-t)^{\frac{p-1}{2}} h^{\frac{p-1}{2}} \\
&= (-t)^{2^{n-1}q} h^{2^{n-1}q} \\
&= [(-t)^{2^{n-1}}]^q [h^q]^{2^{n-1}} \\
&= [-1]^q [1]^{2^{n-1}}, \qquad \text{since } -t \notin T^2 \text{ and } |H| = q \\
&= -1, \qquad \text{since } q \text{ is an odd integer.}
\end{aligned}$$

This completes the proof of part (ii). □

The field $K = GF(p^2)$ is constructed from the quotient ring

$$K \cong Z_p[x]/(x^2 + r)$$

where $x^2 + r$ is an irreducible quadratic in Z_p. In view of Lemma 3.2, we may use any $r \in G$ where $-r \notin G^2$. The elements of K, modulo the ideal $(x^2 + r)$, are the polynomials of the form

$$K = \{ux + v \,|\, u, v \in Z_p\}$$

We of course add and multiply as in any quotient ring and use the fact that $x^2 + r = 0$, or equivalently, $x^2 = -r$, to reduce products to the form $ux + v$.

Lemma 3.3. *If $ux + v \in K = GF(p^2)$ where $x^2 + r$ is irreducible, then*

$$(ux + v)^p = -ux + v.$$

Proof. It follows that

$$\begin{aligned}
(ux + v)^p &= (ux)^p + v^p \\
&= u^p x^p + v^p \\
&= ux(x^2)^{\frac{p-1}{2}} + v \\
&= ux(-r)^{\frac{p-1}{2}} + v \\
&= ux(-1) + v \qquad \text{by Lemma 3.2} \\
&= -ux + v.
\end{aligned}$$

□

Lemma 3.4. *Let $P(x, y) = x + y + xy(1 + y^{p-1})$ be a polynomial in $Z_p[x, y]$. If $mx + n$ and $ux + v$ are elements in the field $K = GF(p^2)$, then*

$$(mx + n) * (ux + v) = (m + u + 2mv)x + (n + v + 2nv).$$

Proof. It will be convenient to rewrite the polynomial $P(x, y)$ as

$$P(x, y) = x + y + x(y + y^p).$$

Then

$$\begin{aligned}
&(mx + n) * (ux + v) \\
= \;& (mx + n) + (ux + v) + (mx + n)[(ux + v) + (ux + v)^p] \\
= \;& (mx + n) + (ux + v) + (mx + n)[(ux + v) + (-ux + v)] \\
= \;& (mx + n) + (ux + v) + (mx + n)[2v] \\
= \;& (m + u + 2mv)x + (n + v + 2nv).
\end{aligned}$$

□

Let $p > 2$ be a prime, and let

$$D_p =< a, b \mid a^p = 1, b^2 = 1, \text{and } ba = a^{-1}b >$$

be the dihedral group of order $2p$. We will show, in the next two theorems, that D_p has Smarandache degree $p + 1$.

Theorem 3.5. *Let $p > 2$ be a prime. The dihedral group D_p of order $2p$ can be found within the polynomial algebra $(K, *)$ where $K = GF(p^2)$ and $P(x, y) = x + y + xy(1 + y^{p-1})$.*

Proof. We know that $K = GF(p^2) = \{ux + v \mid u, v \in Z_p\}$. Let G denote the following set of elements in K:

$$0, x, 2x, 3x, \cdots, (p-1)x, -1, -1x-1, -2x-1, -3x-1, \cdots, -(p-1)x-1.$$

It is clear that G contains $2p$ distinct elements of K. Define a map $\eta : D_p \to G$ by

$$\eta(a^i b^j) = \begin{cases} ix, & \text{if } j = 0, \\ -ix - 1, & \text{if } j = 1 \end{cases}.$$

It follows that η is a one-to-one map from D_p onto G. The following four cases will show that $\eta(g_1 \cdot g_2) = \eta(g_1) * \eta(g_2)$ for every $g_1, g_2 \in D_p$ and it will have been proven that $(G, *)$ is a group isomorphic to D_p.
Case 1: $g_1 = a^i$ and $g_2 = a^j$.

$$\begin{aligned} \eta(a^i) * \eta(a^j) &= (ix) * (jx) \\ &= (i + j)x, \qquad \text{by Lemma 3.4} \\ &= \eta(a^{i+j}) \\ &= \eta(a^i \cdot a^j). \end{aligned}$$

Case 2: $g_1 = a^i b$ and $g_2 = a^j$.

$$\begin{aligned} \eta(a^i b) * \eta(a^j) &= (-ix - 1) * (jx) \\ &= -(i - j)x - 1, \qquad \text{by Lemma 3.4} \\ &= \eta(a^{i-j} b) \\ &= \eta(a^i b \cdot a^j). \end{aligned}$$

Case 3: $g_1 = a^i b$ and $g_2 = a^j b$.

$$\begin{aligned} \eta(a^i b) * \eta(a^j b) &= (-ix-1)*(-jx-1) \\ &= (i-j)x, \qquad \text{by Lemma 3.4} \\ &= \eta(a^{i-j}) \\ &= \eta(a^i b \cdot a^j b). \end{aligned}$$

Case 4: $g_1 = a^i$ and $g_2 = a^j b$.

$$\begin{aligned} \eta(a^i) * \eta(a^j b) &= (ix)*(-jx-1) \\ &= -(i+j)x-1, \qquad \text{by Lemma 3.4} \\ &= \eta(a^{i+j} b) \\ &= \eta(a^i \cdot a^j b). \end{aligned}$$

□

Theorem 3.6. *The dihedral group D_p of order $2p$ where $p > 2$ is prime and has $sd(D_p) = p+1$.*

Proof. Assume that D_p can be found within a polynomial algebra $(K, *)$ generated by the polynomial $P(x,y)$ having degree $k \le p$. Lemma 2.6 implies that we may consider $e = 0$ is the identity of D_p. If we write $P(x,y) = \sum a_{ij} x^i y^j$, then $g * 0 = g$ for every $g \in D_p$ implies that

$$g = P(g,0) = a_{00} + a_{10} g + a_{20} g^2 + \cdots + a_{k0} g^k.$$

Consequently, the polynomial $f(x) = a_{00} + (a_{10}-1)x + a_{20}x^2 + \cdots + a_{k0}x^k$ has every element in D_p for a root; i.e., $f(g) = 0$ for every $g \in D_p$. It follows that $f(x)$ must be the zero polynomial. Thus, $a_{00} = a_{20} = a_{30} = \cdots = a_{k0} = 0$ and $a_{10} = 1$. By a symmetric argument, the fact that $0 * g = g$ for every $g \in D_p$ will imply that $a_{00} = a_{02} = a_{03} = \cdots = a_{0k} = 0$ and $a_{01} = 1$. Therefore,

$$P(x,y) = x + y + xyQ(x,y)$$

for some polynomial $Q(x,y)$ having degree $k-2$.

The dihedral group D_p contains p elements of order 2 each having the form

$$b_0 = a^0 b,\ b_1 = a^1 b,\ b_2 = a^2 b,\ \cdots,\ b_{p-1} = a^{p-1} b.$$

Thus,

$$\begin{aligned} 0 = b_i * b_i = P(b_i, b_i) &= b_i + b_i + b_i b_i Q(b_i, b_i) \\ &= 2b_i + b_i b_i Q(b_i, b_i) \\ &= (2 + b_i Q(b_i, b_i))b_i. \end{aligned}$$

Since $b_i \neq 0$ in the field K, it must follow that $2 + b_i Q(b_i, b_i) = 0$. Consequently, the polynomial $h(x) = 2 + xQ(x, x)$ has degree at most $p - 1$ and has p elements $b_0, b_1, \cdots, b_{p-1}$ that are roots and it follows that $h(x)$ must be the zero polynomial. Therefore, $2 = 0$ in the field K, and $Q(x, x)$ is also the zero polynomial. Since $2 = 0$, it is clear that K has characteristic 2. The generator $a \in D_p$ must have order $p > 2$. However,

$$\begin{aligned} a * a = P(a, a) &= a + a + a^2 Q(a, a) \\ &= 2a + a^2 \cdot 0 \quad \text{since } Q(x, x) \text{ is the zero polynomial} \\ &= 0 + a^2 \cdot 0 \\ &= 0. \end{aligned}$$

We have established that a has order 2, a contradiction. □

Acknowledgments

The authors are deeply grateful to referee's helpful suggestions and help for completing the paper.

References

[1] P. J. Allen, H. S. Kim and J. Neggers, Smarandache disjoint in BCK/d-algebras, *Sci. Math. Jpn.* **61** (2005), no. 3, 447–449.

[2] P. J. Allen, H. S. Kim and J. Neggers, Super commutative d-algebras and BCK-algebras in the Smarandache setting, *Sci. Math. Jpn.* **62** (2005), no. 1, 131–135.

[3] I. N. Herstein, Topics in Algebra, Xerox College Publishing, Lexington, Mass.-Toronto, Ont., 1975.

[4] P. A. Hummadi and A. K. Muhammad, Smarandache triple tripotents in Z_n and in group ring Z_2G, *Int. J. Algebra* **4** (2010), no. 25-28, 1219–1229.

[5] Y. B. Jun, Smarandache BCC-algebras, *Int. J. Math. Math. Sci.* **2005** (2005), no. 18, 2855–2861.

[6] W. B. V. Kandasamy, Groupoids and Smarandache Groupoids, American Research Press, Rehoboth, 2002.

[7] R. Padilla, Smarandache algebraic structures, *Bull. Pure & Appl. Sci.* **17** (1988), 119–121.

[8] A. B. Saeid, Smarandache weak BE-algebras, *Commun. Korean Math. Soc.* **27** (2012), no. 3, 489–496.

P. J. Allen
Department of Mathematics, University of Alabama, Tuscaloosa, AL 35487-0350, USA
Email: pallen@as.ua.edu

Hee Sik Kim
Department of Mathematics, Hanyang University and Research Institute for Natural Sciences, Seoul, 133-791, Korea
Email: heekim@hanyang.ac.kr

J. Neggers
Department of Mathematics, University of Alabama, Tuscaloosa, AL 35487-0350, USA
Email: jneggers@as.ua.edu