JP Journal of Algebra, Number Theory and Applications
© 2013 Pushpa Publishing House, Allahabad, India
Published Online: February 2014
Available online at http://pphmj.com/journals/jpanta.htm
Volume 31, Number 2, 2013, Pages 143-149

SEMIHOMOMORPHISMS ON ABELIAN GROUPS

A. A. Abdelkarim

Jerash University
Jerash, Jordan

Abstract

In this note, we define an m-semihomomorphism f on an Abelian group as a function satisfying $f(x+y) = f(x) + f(y) + f(a)$, $f^{(m)}(a) = 0$ for some element a. We prove that the set of all m-semihomorphisms on Q, or Z_p, p is a prime, is a commutative inverse semigroup and compute its order in case of Z_p. Then we compute the semigroup of 2-semihomorphisms on a general Z_n.

Introduction

Let G be an Abelian group. Then the set of all group homomorphisms is a commutative semigroup under composition. For if f, g are homomorphisms, then $f \circ g(x+y) = f(g(x+y)) = f(g(x)+g(y)) = f(g(x)) + f(g(y))$. There is another special kind of functions on G. A function $f : G \to G$ is called an *m-semihomomorphism* (*m-semhom* for short) if there is an element $a \in G$ such that $f(x+y) = f(x) + f(y) + f(a)$ with $f^{(m)}(a) = 0$, where $f^{(m)}$ is the composition of m copies of f. For example a homomorphism $f : G \to G$ is a 1-semhom for it satisfies $f(x+y) = f(x) + f(y) + f(0)$, $f(0) = 0$. We notice that the composition of two 2-semhoms f, g, need not be a semhom.

Received: November 23, 2013; Accepted: December 31, 2013
2010 Mathematics Subject Classification: 20K30.
Keywords and phrases: m-semihomomorphism, Abelian group.
Communicated by Mitsuo Kanemitsu

For let f, g be two 2-semhoms on an Abelian group G. Thus $f(x+y) = f(x) + f(y) + f(a)$, $g(x+y) = g(x) + g(y) + g(b)$ such that $f(f(a)) = 0 = g(g(b))$. Then

$$f \circ g(x+y) = f(g(x+y)) = f(g(x) + g(y) + g(b))$$

$$= f(g(x)) + f(g(y)) + f(g(b)) + 2f(a),$$

$$f(f(g(b)) + f(a) + f(a)) = f(f(g(b))) + f(f(a)) + f(f(a)) + 2f(a)$$

$$= f(f(g(b))) + 2f(a)$$

need not be 0 as shown by Example 5. In this note, we discuss some cases in which the set of m-semhoms on an Abelian group is a commutative semigroup and sometimes it is an inverse semigroup.

The Results

The simplest Abelian groups are the additive group of a field. We first discuss the existence of semhoms on the group $(Q, +)$. This amounts to the following problem: Given a positive integer m find all functions $f : Q \to Q$ such that there exists $a \in Q$ for which it holds that $f(x+y) = f(x) + f(y) + f(a)$, $f^{(m)}(a) = 0$, for all $x, y \in Q$.

Proposition 1. *Let $a \in Q$ and let $f : Q \to Q$ be an m-semhom with a corresponding element $a \in Q$. Then for all $x \in Q$, $f(x) = (f(1) - f(0))x - f(a)$, $f(a) = -f(0)$. If $m = 2$, then $f(x) = x - a/2$. If $m > 2$, then $f(x) = f(1)x$.*

Proof. If we take $x, y = 0$, then $-f(0) = f(a)$. Thus for all $x, y \in Q$, $f(x+y) = f(x) + f(y) - f(0)$. If we put $x, y = 1$, then we get $f(2) = 2f(1) - f(0)$. Using induction, we can show that for all integers $m \in Z$, we have $f(m) = mf(1) + (1-m)f(0)$. Also, $f(1) = f(1/2 + 1/2) = f(1/2) + f(1/2) - f(0) = 2f(1/2) - f(0)$ and so $f(1/2) = (1/2)f(1) + (1-1/2)f(0)$. Using induction, we can show that for all nonzero integers n, we have $f(1/n) = (1/n)f(1) + (1 - 1/n)f(0)$ and in general we have for all rational numbers x, $f(x) = xf(1) + (1 - x)f(0)$. Thus

$$f(x) = (f(1) + f(a))x - f(a) = cx - f(a), \qquad c = f(1) + f(a). \qquad (1)$$

It follows that $f(f(a)) = cf(a) - f(a)$ and in general

$$f^{(m)}(a) = c^{m-1}f(a) - c^{m-2}f(a) - \cdots - cf(a) - f(a)$$

$$= f(a)(c^{m-1} - c^{m-2} - \cdots - c - 1). \qquad (2)$$

Let $m = 2$. Then we have $0 = f(f(a)) = cf(a) - f(a) = f(a)(c-1)$. If $f(a) = 0$, then $f(x) = f(1)x$. If $f(a) \neq 0$, then $c = 1$, $f(x) = x - f(a)$, $f(a) = a - f(a)$, $2f(a) = a$ and $f(x) = x - a/2$.

Let $m > 2$. From $f^{(m)}(a) = 0$ and from equation (2), we get

$$c^{m-1} - c^{m-2} - \cdots - c - 1 = 0. \qquad (3)$$

If this equation has a rational root, then it will be 1 or –1. Since $m - 1 > 1$, it follows that 1 cannot be a root. If –1 is a root, then

$$c^{m-1} = \frac{c^{m-1} - 1}{c - 1}. \qquad (4)$$

If $m - 1$ is even, then it follows that $1 = 0$ which is absurd. If $m - 1$ is odd, then it follows that $-1 = 1$ which is absurd. Thus equation (3) has no rational solutions. Thus $f(a) = 0$ and so $f(x) = f(1)x$ if $m > 2$. This completes the proof. □

Next we discuss the Abelian group $(Z_p, +)$ of the field $(Z_p, +, \cdot)$.

Proposition 2. *Let* $p > 2$ *be a prime number and let* $f : Z_p \to Z_p$ *be a* 2-*semhom*: $a \in Z_p$, $f(x + y) = f(x) + f(y) + f(a)$, $f(f(a)) = 0$. *Then either* $f(a) = 0$, $f(x) = f(1)x$ *or* $f(x) = x - a/2 = x + f(0)/2$ *for all* x. *If* *f is an m-semhom*, $m > 2$, *then either* $f(a) = 0$, $f(x) = f(1)x$ *or* $f(x) = (f(1) + f(a))x - f(a)$ *such that* $(f(1) - f(0))^m - (f(1) - f(0))^{m-1} + 1 = 0$.

Proof. The proof is similar to that of the preceding proposition. If we take $x, y = 0$, then $-f(0) = f(a)$ and so $f(x+y) = f(x) + f(y) - f(0)$. If we put $x, y = 1$, then we get $f(2) = 2f(1) - f(0)$. Using induction, we can show that for all integers $m \in Z_p$, we have $f(m) = mf(1) + (1-m)f(0)$. In general, we have for all x, $f(x) = xf(1) + (1-x)f(0)$. Thus

$$f(x) = (f(1) - f(0))x + f(0) = cx + f(0), \qquad c = f(1) - f(0). \tag{5}$$

Let $m = 2$. Thus $f(f(a)) = 0 = cf(a) - f(a) = f(a)(c-1)$. If $f(a) = 0$, then $f(x) = f(1)x$. While if $f(a) \neq 0$ and $f(a)$ is a unit, then $c = 1$. Thus $f(x) = x - f(a)$. Then $f(a) = a - f(a)$ and so $2f(a) = a$. If $m = 2$, then $a = 0$. Thus $f(x) = x - a/2$. Let $m > 2$. From $f^{(m)}(a) = 0$ and from equation (2), we get

$$c^{m-1}f(a) - c^{m-2}f(a) - \cdots - cf(a) - f(a) = 0.$$

If $f(a) = 0$, then $f(x) = f(1)x$. If $f(a) \neq 0$, then we get

$$c^{m-1} - c^{m-2} - \cdots - c - 1 = 0, \qquad c^{m-1} = 1 + c + \cdots + c^{m-2}.$$

We have three cases to consider: $m - 1 < p$, $m - 1 = p$, $m - 1 > p$. If $m - 1 < p$, then c cannot be 1 for this would imply $1 = m - 1 \bmod p$ and this is impossible. If $m - 1 = p$ and $c = 1$, then $1 = p - 1$ which is absurd. If $m - 1 > p$ and $m - 1 = kp + r$, $0 \leq r < p$, then if $c = 1$, we have $1 = kp + r = r \bmod p$ which is absurd even if $r = 0$. Thus we have $c^{m-1} = (c^{m-1} - 1)/(c - 1) \to c^m - 2c^{m-1} + 1 = 0$. Thus c is a solution of the equation $x^m - 2x^{m-1} + 1 = 0$, $x \neq 1$, $m > 2$. For example, $x^3 - 2x^2 + 1 = 0$, $x \neq 1$ has no solution in Z_3 but it has a solution $x = 3$ in Z_5. □

Proposition 3. *The set of* 2-*semhoms on the group* $(Q, +)$ *with the composition operator is a commutative inverse semigroup. The set of* 2-*semhoms on the group* $(Z_p, +)$ *with the composition operator is a finite commutative inverse semigroup.*

Proof. The proof is direct: $(x - a/2) \circ (x - b/2) = x - (a + b)/2$ which is a 2-semhom. Also, $(x - a/2) \circ (x + b) \circ (x - a/2) = x - a/2$ implies that $x - (a/2) + b - (a/2) = x - (a/2)$ and so $b = a/2$ and the inverse of $x - a/2$ is $x + a/2$. Since the idempotents commute, the commutative semigroup is an inverse semigroup. □

Now let us try to solve the following problem. Let $n > 2$ be a positive integer not necessarily a prime. Find all 2-semhoms on Z_n; i.e., all functions $f : Z_n \to Z_n$ such that there is $a \to Z_n$ which makes the following equation hold: $f(x + y) = f(x) + f(y) + f(a), \; ff(a) = 0.$

We first notice that $f(x) = (f(1) - f(0))x + f(0), \; f(0) = -f(a)$. From $f(f(a)) = 0$, it follows that $f(-f(0)) = 0 = (f(1) - f(0))(-f(0)) + f(0) = (f(0))^2 - f(0)f(1) + f(0) = f(0)(f(0) + 1 - f(1))$. Thus the 2-semhom f is completely determined by $f(0)$ and $f(1)$. If $f(0)$ is a unit, then $f(1) = f(0) + 1$. Let for all $m \in Z_n$, $\psi(m)$ denote the number of annihilators k of m in Z_n. Thus $km = 0 \bmod n$. This is the same as the number of annihilators of $\gcd(m, n)$ in Z_n and this is $\gcd(m, n)$. Thus for any $f(0)$, there are $\psi(f(0))$ of 2-semhoms corresponding to $f(0)$. Thus the total number of 2-semhoms is $\sum_{m=0}^{n-1} \gcd(m, n) = n + \sum_{k=1}^{n-1} \gcd(k, n)$.

We first notice that any 2-semhom is of the form $f(x) = (f(1) - f(0))x + f(0), \; f(0) = -f(a), \; f(0)(f(0) + 1 - f(1)) = 0$. Thus $f(x) = Mx + f(0)$, $f(0)(1 - M) = 0$.

Proposition 4. *The set of* 2-*semhoms on the Abelian group* $(Z_n, +)$

under the operation $(M_1x + f(0)) \circ (M_2x + g(0)) = M_1M_2x + f(0)g(0)$ *is a commutative semigroup of order* $n + \sum_{k=1}^{n-1} \gcd(k, n)$.

Proof. The first part of the proposition was proved earlier. The set of all 2-semhoms is not closed under composition as was noted earlier and as shown in Example 5. But this set is a commutative semigroup under the operation $(m_1x + k_1) \circ (m_2x + k_2) = m_1m_2x + k_1k_2$. For if $m_1x + k_1,\ m_2x + k_2$ are 2-semhoms, then

$$(m_1 - 1)k_1 = 0,\ (m_2 - 1)k_2 = 0 \Rightarrow m_1k_1 = k_1,\ m_2k_2 = k_2 \tag{6}$$

$$\Rightarrow m_1m_2k_1k_2 = k_1k_2 \Rightarrow (m_1m_2k_1k_2 - 1)k_1k_2 = 0. \tag{7}$$

Thus $(m_1x + k_1) \circ (m_2x + k_2) = m_1m_2x + k_1k_2$. This operation is well defined and commutative. □

Example 5. Let us find all 2-semhoms $f : Z_6 \to Z_6$. If $k = 0 = f(0)$, then $f(x) = Mx$, totalling to 6. If $k = 1 = f(0)$, then $M = 1$ and we have only one such function: $f(x) = x + 1$. If $k = 2$, then $M = 1, 4$ giving $x + 2$, $4x + 2$. If $k = 3$, then $M = 1, 3, 5$ giving $x + 3$, $3x + 3$, $5x + 3$. If $k = 4$, then $M = 1$, $M = 4$ giving $x + 4$, $4x + 4$. If $k = 5$, then $M = 1$ giving $x + 5$. Thus we have: $0, x, 2x, 3x, 4x, 5x$, $x + 1$, $x + 2$, $4x + 2$, $x + 3$, $3x + 3$, $5x + 3$, $x + 4$, $4x + 4$, $x + 5$ totalling 15 functions. We notice that $6 + \gcd(1, 6) + \gcd(2, 6) + \gcd(3, 6) + \gcd(4, 6) + \gcd(5, 6) = 6 + 1 + 2 + 3 + 2 + 1 = 15$ as claimed. For example, if we pick $f(x) = 4x + 4$, then $f(x + y) = 4x + 4y + 4$, $f(x) + f(y) = 4x + 4y + 8$ and we see that $f(x + y) = f(x) + f(y) - 4 = f(x) + f(y) = 2$, $2 = 4x_1 + 4$, $x_1 = 1$ and $2 = f(1)$, $f(f(1)) = f(2) = 4(2) + 4 = 0$. We notice that the composition of the two 2-semhoms: $x + 5$ after $4x + 4$ is $4x + 3$ which is not a 2-semhom. The resulting semigroup is a commutative semigroup of order 15. It is an inverse semigroup because it is commutative and the cube of every element is the element itself.

Example 6. Similarly we see that all such functions $f : Z_9 \to Z_9$ are $0, x, 2x, ..., 8x$ and $x+1$ and $x+2$ and $x+3$, $4x+3$, $7x+3$, $x+4$, $x+5$, $x+6$, $4x+6$, $7x+6$, $x+7$, $x+8$ totalling 21. We notice that $9+\sum_{n=1}^{8} \gcd(n, 9) = 9+1+1+3+1+1+3+1+1 = 21$ as expected. The resulting semigroup, although commutative, is not an inverse semigroup. $(x+3) \circ (mx+d) \circ (x+3) = mx$ for every mx and so $x+3$ is not a regular element in this semigroup.

Problem 7. Is it true that the semigroup of all 2-semhoms on Z_n, $n > 2$, n is not a prime, is an inverse semigroup if and only if n is square-free?

Problem 8. What is the structure of the set of all m-semhoms, $m > 2$, of the Abelian group $(Z_n, +)$?

Problem 9. What is the structure of the set of all semhoms on the Abelian group $(Z_p \times Z_p, +)$ or the like?

References

[1] J. M. Howe, An Introduction to Semigroup Theory, Academic Press, 1976.

[2] J. Rotman, The Theory of Groups, An Introduction, Allyn and Bacon, Inc., Boston, 1965.