CHAPTER II

GENERAL PROPERTIES

In this chapter, general properties of skew-semifields are given, and we also characterize cyclic groups admitting skew-semifield structure.

Theorem 2.1. Let S be a skew-semifield. Then either S is a skew-field or every nonzero element of S has no additive inverse.

Proof : Suppose that there is an element $x \in S\setminus\{0\}$ such that x has an additive inverse, say z. To show that every element in S has an additive inverse, let $y \in S$. Since $x + z = 0$, $yx^{-1}(x + z) = 0$. Then $y + yx^{-1}z = 0$, so $yx^{-1}z$ is an additive inverse of y. Therefore we have that S is an abelian group under addition. Hence S is a skew-field.

#

The following corollary follows directly from Theorem 2.1.

Corollary 2.2. Let S be a skew-semifield. If S is not a skew-field, then $a + b \neq 0$ for all $a,b \in S\setminus\{0\}$.

Theorem 2.3. Let S be a skew-semifield. If S contains more than two elements, then S has no additive zero.

Proof : Suppose that S has an additive zero, say a. Then $x + a = a$ for all $x \in S$. Since $|S| > 1$, $a \neq 0$. Then $a^{-1}x + 1 = 1$ for all $x \in S$. If follows that for each $x \in S$, $x + 1 = a^{-1}(ax) + 1 = 1$.

If $x \in S \smallsetminus \{0\}$, then $1 + x = 1 = 1 + x^{-1}$ and hence $x = x1 = x(1 + x^{-1}) = x + 1 = 1$. Thus $S \smallsetminus \{0\} = \{1\}$ which implies that $|S| = 2$. This proves that if $|S| > 2$, then S has no additive zero, as required.

#

Theorem 2.4. Let S be a finite skew-semifield. Then S is not a skew-field if and only if $x + x = x$ for all $x \in S$.

Proof : Assume that S is not a skew-field. By Corollary 2.2, $(S \smallsetminus \{0\},+)$ is a finite semigroup. Then there exists an element $a \in S \smallsetminus \{0\}$ such that $a + a = a$ (see [8], page 20). Then $1 = a^{-1}a = a^{-1}(a + a) = 1 + 1$. This implies that $x + x = x$ for all $x \in S$.

Conversely, assume that $x + x = x$ for all $x \in S$. Then $(S,+)$ is not a group since $|S| > 1$. Hence S is not a skew-field.

#

Theorem 2.5. A finite skew-semifield containing more than two elements is a field.

Proof : Let $S = (S,+,\cdot)$ be a finite skew-semifield and $|S| > 2$. Suppose that S is not a skew-field. By Theorem 2.4, $x + x = x$ for all $x \in S$. It follows that $nx = x$ for all $x \in S$ and for all positive integer n where $nx = x + x + \ldots + x$ (n times). Let $y \in S \smallsetminus \{0,1\}$. Since $(S \smallsetminus \{0\},\cdot)$ is a finite group, $(1 + y)^m = 1$ for some positive integer m. Since $(S,+)$ is commutative and 1 and y commute under multiplication, it follows that

$$1 = (1 + y)^m = 1 + \binom{m}{1}y + \binom{m}{2}y^2 + \ldots + \binom{m}{m-1}y^{m-1} + y^m.$$

But $\binom{m}{i} y^i = y^i$ for all $i = 1,2,\ldots,m-1$, so we have that $1 = 1 + y + y^2 + \ldots + y^m$. Thus

$$\begin{aligned} 1 + y &= (1 + y + y^2 + \ldots + y^m) + y \\ &= 1 + (y + y) + y^2 + \ldots + y^m \\ &= 1 + y + y^2 + \ldots + y^m \\ &= 1. \end{aligned}$$

This proves that $1 + y = 1$ for all $y \varepsilon S\smallsetminus\{0,1\}$. Let $t \varepsilon S\smallsetminus\{0,1\}$. Then $1 + t = 1$,so $t^{-1} + 1 = t^{-1}$. Since $t^{-1} \varepsilon S\smallsetminus\{0,1\}$, $1 + t^{-1} = 1$. Then $t^{-1} = 1$. Therefore $t = 1$, a contradiction. Hence S is a skew-field. Since S is finite, S is a field.

#

Note that if S is a skew-semifield such that $|S| = 2$ and S is not a field, then $1 + 1 = 1$ (Theorem 2.4), and hence S is the Boolean algebra of 2 elements.

Theorem 2.6. Let $S = (S,+,\cdot)$ be a skew-semifield. Then the following statements hold :

(i) If there exists an element $a \in S$ such that $a \neq 1$ and $a^2 = 1$, then $1 + a = 0$, and hence S is a skew-field.

(ii) There exists at most one element $a \varepsilon S$ such that $a \neq 1$ and $a^2 = 1$.

Proof : (i) Since $(S\smallsetminus\{0\},\cdot)$ is a group, $a(1 + a) = a + 1 = 1 + a$ and $a \neq 1$, it follows that $1 + a = 0$, and hence S is a skew-field.

(ii) Suppose that $a,b \varepsilon S$ are such that $a \neq 1$, $a^2 = 1$, $b \neq 1$ and $b^2 = 1$. By (i), $(S,+)$ is an abelian group and a and b are inverses of 1 in $(S,+)$. Then $a = b$.

#

In the last part of this chapter, we characterize cyclic groups admitting skew-semifield structure (that is, cyclic groups admitting semifield structure).

Let G be an infinite cyclic group with a generator a. Then $G = \{a^n | n \in \mathbb{Z}\}$ and $a^i \neq a^j$ if $i \neq j$ where $\mathbb{Z}$ is the set of all integers. Let $\cdot$ denote the operation on G^o. Define the operation + on G^o by

$$a^i + a^j = a^{\max\{i,j\}}$$

and

$$a^i + 0 = 0 + a^i = a^i$$

for all $i,j \in \mathbb{Z}$. Then $x + y = y + x$ for all $x,y \in G^o$. Claim that $(G^o,+,\cdot)$ is a semifield. To show that + is associative and $\cdot$ is distributive over + in G^o, let $x,y,z \in G^o$. If $x = 0$, $y = 0$ or $z = 0$, it is easy to see that $x + (y + z) = (x + y) + z$ and $x\cdot(y + z) = (x\cdot y) + (x\cdot z)$. Assume that $x \neq 0$, $y \neq 0$ and $z \neq 0$. Then $x = a^i$, $y = a^j$ and $z = a^k$ for some $i,j,k \in \mathbb{Z}$. Then $(x + y) + z = (a^i + a^j) + a^k = a^{\max\{i,j,k\}} = a^i + (a^j + a^k) = x + (y + z)$ and $x\cdot(y + z) = a^i.\ (a^j + a^k) = a^{i+\max\{j,k\}} = a^{\max\{i+j,i+k\}} = a^{i+j} + a^{i+k} = (a^i.\ a^j) + (a^i.\ a^k) = (x\cdot y) + (x\cdot z)$. Hence we have the claim, so we have

<u>Theorem 2.7</u>. An infinite cyclic group admits a semifield structure.

Theorem 2.7 and the next theorem show that an infinite cyclic group is an example of a group which admits a semifield structure but does not admit a field structure.

<u>Theorem 2.8</u>. An infinite cyclic group does not admit a field structure.

<u>Proof</u> : Let G be an infinite cyclic group with a generator a. Then $G = \{a^n | n \varepsilon \mathbb{Z}\}$ and $a^i \neq a^j$ if $i \neq j$. Suppose that G admits a field structure under an addition $+$. Then $a + x = 0$ for some $x \varepsilon G^{\circ}$. Since $a \neq 0$, $x \neq 0$. Then $x = a^k$ for some $k \varepsilon \mathbb{Z}$. Therefore $a + a^k = 0$.

<u>Case 1</u> : $k \neq 1$. Then

$$a^k + a^{2k-1} = a^{k-1}(a + a^k) = 0$$

which implies that

$$a = a + (a^k + a^{2k-1}) = (a + a^k) + a^{2k-1} = a^{2k-1}.$$

It is a contradiction since $2k - 1 \neq 1$.

<u>Case 2</u> : $k = 1$. Then $a + a = 0$ which implies that $1 + 1 = a^{-1}a + a^{-1}a = a^{-1}(a + a) = 0$. Hence $x + x = 0$ for all $x \varepsilon G^{\circ}$. Therefore we have $(x + y)^2 = x^2 + y^2$ for all $x, y \varepsilon G^{\circ}$. Since a is a generator of G, $a \neq 1$. Then $1 + a \neq 0$, so $1 + a = a^m$ for some $m \varepsilon \mathbb{Z}$. Since $x + x = 0$ for every $x \varepsilon G$, $1 + a^m = a$. From $a \neq 0$ and $1 \neq 0$, it follows that $m \neq 0$ and $m \neq 1$.

<u>Subcase 2.1</u> : m is even. Then $\frac{m}{2} \varepsilon \mathbb{Z}$ and $a = 1 + a^m = (1 + a^{\frac{m}{2}})^2 \neq 0$. Let $j \varepsilon \mathbb{Z}$ be such that $1 + a^{\frac{m}{2}} = a^j$. Then $a = a^{2j}$, a contradiction.

<u>Subcase 2.2</u> : m is odd. Then $\frac{m+1}{2} \varepsilon \mathbb{Z}$ and $a^2 = a(1 + a^m) = a + a^{m+1}$ since $1 + a^m = a$. Thus $a = a^2 + a^{m+1} = (a + a^{\frac{m+1}{2}})^2 \neq 0$. Then $a + a^{\frac{m+1}{2}} = a^r$ for some $r \varepsilon \mathbb{Z}$. Then $a = a^{2r}$, a contradiction.

Hence G does not admit a field structure.

#

In the last theorem of this chapter, we give a characterization of finite cyclic groups admitting semifield structure.

Theorem 2.9. A finite cyclic group of order n admits a semifield structure if and only if $n = p^m - 1$ for some prime p and positive integer m.

Proof : Let G be a finite cyclic group of order n. It follows from Theorem 1.1 that if $n = p^m - 1$ for some prime p and positive integer m, then G admits a field structure and hence G admits a semifield structure.

Conversely, assume that G admits a semifield structure. Let $\cdot$ be the operation on G^o. Then there exists an operation + on G^o such that $(G^o,+,\cdot)$ is a semifield. If $n = 1$, then $n = 1 = 2^1 - 1$, so we are done. Assume that $n > 1$. Then $|G^o| > 2$. By Theorem 2.5, $(G^o,+,\cdot)$ is a field. Let p be the characteristic of the field $(G^o,+,\cdot)$. Then p is a prime and $n + 1 = |G^o| = p^m$ for some positive integer m. Hence $n = p^m - 1$. #

Corollary 2.10. A finite cyclic group of order n admits a field structure if and only if $n = p^m - 1$ for some prime p and positive integer m.

Proof : The "only if" part follows directly from Theorem 2.9. The "if" part follows from Theorem 1.1. #