Chapter II

DEFINITIONS AND SOME PROPERTIES OF STEINER TRIPLE SYSTEMS

2.0 Introduction

In this chapter Steiner triple systems and related concepts are introduced. A few examples of Steiner triple systems are also provided. Elementary properties concerning the structure of Steiner triple systems are derived for later uses.

2.1 Definitions and Examples

By a p-subset of a set A we mean any subset of A that contains exactly p elements.

2.1.1 Definition. A Steiner triple system, abbreviated as STS, is an ordered pair (A,S(A)), where A is a non-empty finite set, S(A) is a family of 3-subsets of A such that for any pair of distinct elements a,b in A there exists a unique element c in A such that $\{a, b, c\} \in S(A)$.

Any element of S(A) will be called a triple of (A,S(A) and any 3-subset of A which is not in S(A) will be called a triangle of (A,S(A)). If A contains n element we say that (A,S(A)) is a STS of order n.

The followingsare examples of STS of orders 1,3,7.

Example (i). Let $A = \{1\}$, $S(A) = \emptyset$.

Example (ii). Let $A = \{1, 2, 3\}$, $S(A) = \{\{1, 2, 3\}\}$.

Example (iii). Let $A = \{1, 2, \ldots, 7\}$ and $S(A)$ consists of the following 3-subsets of A :

$\{1,2,3\}$ $\{2,4,6\}$ $\{3,4,7\}$

$\{1,4,5\}$ $\{2,5,7\}$ $\{3,5,6\}$

$\{1,6,7\}$

2.1.2 Definition. By a subsystem of a STS $(A,S(A))$ we mean any STS $(B,S(B))$ such that $B \subseteq A$ and $S(B) \subseteq S(A)$.

The condition $S(B) \subset S(A)$ implies that $B \subset A$. Therefore, in order to verify that a STS $(B,S(B))$ is a subsystem of $(A,S(A))$ it suffices to show that $S(B) \subset S(A)$.

2.1.3 Definition. Let $(A,S(A))$ and $(A',S(A'))$ be STS. Any one to one mapping f from A onto A' such that $\{a, b, c\}$ is a triple of $(A,S(A))$ if and only if $\{f(a), f(b), f(c)\}$ is a triple of $(A',S(A'))$ is called an isomorphism from $(A,S(A))$ on to $(A',S(A'))$.

2.1.4 Definition. Steiner triple systems $(A,S(A))$ and $(A',S(A'))$ are said to be isomorphic if there exists an isomorphism from $(A,S(A))$ onto $(A',S(A'))$.

2.2 Elementary Properties of STS

2.2.1 Proposition. Let $(A,S(A))$, $(B,S(B))$ and $(C,S(C))$ be STS. If $(C,S(C))$, is a subsystem of $(B,S(B))$ and $(B,S(B))$ is a subsystem of $(A,S(A))$, then $(C,S(C))$ is also a subsystem of $(A,S(A))$.

Proof : From the hypothesis we have $S(C) \subset S(B)$ and $S(B) \subset S(A)$. Hence $S(C) \subset S(A)$. Therefore $(C,S(C))$ is a subsystem of $(A,S(A))$.

2.2.2 Proposition. Let $(A,S(A))$ be a STS. For any non-empty subset B of A let $S(B)$ denote the family of all triples of $(A,S(A))$ which are subsets of B. If for any distinct elements x,y in B there exists an element z in B such that $\{x, y, z\}$ is a triple of $(A,S(A))$, then $(B,S(B))$ is a subsystem of $(A,S(A))$.

Proof : By definition of $S(B)$ we see that $S(B)$ is a family of 3-subsets of B such that $S(B) \subset S(A)$. It is left to be shown that $(B,S(B))$ is a STS. Let x, y be any distinct elements of B. By the hypothesis there exists an element z in B such that $\{x, y, z\} \in S(A)$. Hence $\{x, y, z\}$ is a triple of $(A,S(A))$ which is a subset of B. Therefore $\{x, y, z\} \in S(B)$. Suppose that there exists an element t in B such that $\{x, y, t\} \in S(B)$. By definition of $S(B)$ we have $\{x, y, t\} \in S(A)$. Since $(A,S(A))$ is a STS, it follows that $t = z$. Therefore $(B,S(B))$ is a STS.

2.2.3 Proposition. Let $(B,S(B))$ be any subsystem of a STS $(A,S(A))$. If x and y are elements in $A - B$ and B respectively, then the element z in the triple $\{x, y, z\}$ of $(A,S(A))$ belongs to $A - B$.

Proof : Suppose $z \in B$. Then y and z are distinct elements of B so that there exists a unique element t in B such that $\{y,z,t\} \in S(B)$. Since $S(B) \subset S(A)$, it follows that $\{y,z,t\} \in S(A)$ and thus $t = x$. Therefore $x \in B$ which contradicts the assumption that $x \in A - B$. Hence $z \notin B$. Therefore $z \in A - B$.

2.2.4 Definition. Let $\mathcal{F}$ be a family of STS. By the intersection of the family $\mathcal{F}$ we mean the ordered pair (I,S), where

$$I = \bigcap \left\{ A \,/\, (A,S(A)) \in \mathcal{F} \right\}$$
$$S = \bigcap \left\{ S(A) \,/\, (A,S(A)) \in \mathcal{F} \right\}$$

Observe that elements in S are triples that belong to every S(A) of the STS in $\mathcal{F}$. Hence triples in S are subsets of every A such that $(A,S(A)) \in \mathcal{F}$. Therefore S is a family of 3-subsets of I. From now on we shall write S(I) to stand for S. In general, an intersection of a family of STS need not be a STS.

2.2.5 Proposition. Let C be any non-empty subset[1] of a STS (A,S(A)). Then the intersection (I,S(I)) of all subsystems of (A,S(A)) that contain[1] C is a subsystem of (A,S(A)). Furthermore, (I,S(I)) is the smallest subsystem of (A,S(A)) that contains C.

Proof : Let $\mathcal{F}$ be the family of all subsystems of (A,S(A)) that contain C. Since each STS in $\mathcal{F}$ contains C, hence $C \subset I$ and $S(I) \subset S(A)$. We have to show that (I,S(I)), is a STS. Let x,y be distinct elements of I. Since (A,S(A)) is a STS and $x, y \in A$, it follows that there exists a unique element z in A such that $\{x, y, z\} \in S(A)$. Let (B,S(B)) be any element of $\mathcal{F}$. Therefore $I \subset B$. Thus x, y are distinct elements of B so that there exists a unique element z(B) in B such that $\{x,y,z(B)\} \in S(B)$. Since

---

[1] When we say that a subsystem (B,S(B)) contains C or C is a subset of (B,S(B)) we mean that $C \subset B$.

$S(B) \subset S(A)$, it follows that $\{x,y,z(B)\} \in S(A)$ so that $z = z(B)$. Hence $z \in B$ and $\{x,y,z\} \in S(B)$. But B is arbitrary. Hence $\{x,y,z\} \in S(I)$. Suppose that t is an element of I such that $\{x,y,t\} \in S(I)$. Since $S(I) \subset S(A)$, hence $\{x,y,t\} \in S(A)$ so that $t = z$. Therefore $(I,S(I))$ is a subsystem of $(A,S(A))$.

Let $(A_1,S(A_1))$ be any subsystem of $(A,S(A))$ that contains C. Thus $(A_1,S(A_1)) \in \mathcal{F}$, and hence, $I \subset A_1$ and $S(I) \subset S(A_1)$. Therefore $(I,S(I))$ is the smallest subsystem of $(A,S(A))$ that contains C.

2.2.6 <u>Proposition.</u> Let f be an isomorphism from a STS $(A,S(A))$ onto a STS $(A',S(A'))$. For any subsystem $(R,S(R))$ of $(A,S(A))$, let R' be the image of R under f and $S(R')$ be the set of all images of triples of $(R,S(R))$ under f ; i.e.

$$R' = \{ f(x) \,/\, x \in R \}$$

and

$$S(R') = \{ \{f(x),f(y),f(z)\} \,/\, \{x,y,z\} \in S(R) \}$$

Then $(R',S(R'))$ is a subsystem of $(A',S(A'))$.

<u>Proof</u> : By definition $S(R') \subset S(A')$ and $S(R')$ is a family of 3-subsets of R'. To show that $(R',S(R'))$ is a STS, let x,y be any distinct elements of R'. Since $f(R) = R'$, it follows that there exists a, b in R such that $f(a) = x$, $f(b) = y$. But f is one to one and $x \neq y$. Hence a, b are distinct elements of R so that there exists a unique element c in R such that $\{a,b,c\} \in S(R)$. From $R' = f(R)$, we have $f(c) \in R'$. By definition of $S(R')$ it follows that $\{f(a),f(b),f(c)\} \in S(R')$. Therefore $\{x,y,f(c)\} \in S(R')$. Suppose that

u is an element of R' such that $\{x,y,u\} \in S(R')$. Since $f(R) = R'$, hence there exists an element d in R such that $f(d) = u$. Consequently $\{a,b,d\} \in S(R)$. As a result we have $d = c$ so that $u = f(c)$. Hence $(R', S(R'))$ is a STS. Therefore $(R', S(R'))$ is a subsystem of $(A', S(A'))$.

As a consequence of the above proposition, we have

2.2.7 Corollary. If $(A,S(A))$ and $(A',S(A'))$ are isomorphic STS such that $(A,S(A))$ contains a subsystem of order n, then $(A',S(A'))$ also contains a subsystem of order n.

2.2.8 Proposition. Let $(A,S(A))$ be a STS of order n. Then every element of A is contained in $\frac{n-1}{2}$ triples of $(A,S(A))$.

Proof : Let x be any element of A and let

$$T_x = \{ T \in S(A) \ / \ x \in T \}$$

Hence x is contained in $|T_x|$ triples of $(A,S(A))$. For any $T = \{x,y,z\} \in T_x$ we can form two 2-subsets of A that contain x; namely $\{x,y\}$ and $\{x,z\}$. Furthermore, any two triples in T_x have x as only their common elements. Therefore different triples give rise to entirely different 2-subsets of A that contain x. Hence the total number of 2-subsets of A that contain x formed from the triples in T_x is exactly $2|T_x|$. On the other hand, the total number of 2-subsets of A that contain x is $n - 1$. But for any 2-subset B of A that contains x there must exists a unique $T \in T_x$ such that $B \subseteq T$. Hence $2|T_x| = n - 1$ so that $|T_x| = \frac{n-1}{2}$. Since x is arbitrary, it follows that every element of A is contained in $\frac{n-1}{2}$ triples.

2.2.9 Proposition. The total number of triples in any STS of order n is $\frac{1}{6}n(n-1)$.

Proof : Let (A,S(A)) be any STS of order n. Assume that S(A) contains exactly k triples. Let $S(A) = \{A_1, A_2, \ldots, A_k\}$. For any A_i, the total number of 2-subsets of A_i is 3. Since any 2-subset of A is a subset of one and only one A_i, it follows that the total number of 2-subsets of $\bigcup_{i=1}^{k} A_i = A$ is 3k. On the other hand the total number of 2-subset of A is $\frac{1}{2}n(n-1)$. Hence $3k = \frac{1}{2}n(n-1)$ so that $k = \frac{1}{6}n(n-1)$.

2.3 Necessary Condition for the Existence of STS

When a positive integer n is given, we would like to know whether we can construct a STS of order n. It turns out that STS of order n do not exist for infinitely many values of n. A necessary condition for the existence of STS of order n is given in the following theorem.

2.3.1 Theorem. If a STS of order n exists, then

(2.3.1) $n \equiv 1$ or 3 (mod 6)

Proof : Since $\frac{n(n-1)}{6}$ is a positive integer, hence $n(n-1)$ is divisible by 3. Therefore n or n - 1 must be divisible by 3.

First , let us suppose that n is divisible by 3. In this case we have n = 3m for some positive integer m. Since $\frac{n-1}{2}$ is a positive integer, it follows that n - 1 = 2t for some positive integer t. Therefore $3m - 1 = 2t$. From this it follows that m must be odd. Let $m = 2s + 1$, where s is a positive integer. Hence $n = 3m = 3(2s + 1) = 6s + 3$. Therefore we have $n \equiv 3 \pmod 6$.

Next, we suppose that $n - 1$ is divisible by 3. Then $n - 1 = 3m$ for some positive integer m. Since $\frac{n-1}{2}$ is a positive integer, hence $n - 1 = 2t$ for some positive integer t. Therefore $3m = 2t$. From this it follows that m must be even. Let $m = 2s$ where s is a positive integer. Hence $n = 3m + 1 = 3(2s) + 1 = 6s + 1$. Thus we have $n \equiv 1 \pmod 6$.

Therefore $n \equiv 1$ or $3 \pmod 6$

In fact this necessary condition is also sufficient. This will be proved in Chapter IV.