41159

NAME OF AUTHOR/*NOM DE L'AUTEUR* MURRAY MARTIN

TITLE OF THESIS/*TITRE DE LA THÈSE* THE MAJOR ADDITIVITY THEOREMS FOR SCHNIRELMANN AND ASYMPTOTIC DENSITY

UNIVERSITY/*UNIVERSITÉ* SIMON FRASER

DEGREE FOR WHICH THESIS WAS PRESENTED/ *GRADE POUR LEQUEL CETTE THÈSE FUT PRÉSENTÉE* MASTER OF SCIENCE

YEAR THIS DEGREE CONFERRED/*ANNÉE D'OBTENTION DE CE DEGRÉ* 1978

NAME OF SUPERVISOR/*NOM DU DIRECTEUR DE THÈSE* DR. A. R. FREEDMAN

DATED/*DATÉ* Sept 7/78 SIGNED/*SIGNÉ*

PERMANENT ADDRESS/*RÉSIDENCE FIXE* [redacted]

THE MAJOR ADDITIVITY THEOREMS
FOR SCHNIRELMANN AND ASYMPTOTIC DENSITY

by

Murray Martin

B.Sc.(Hons), Simon Fraser University, 1972

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in the Department

of

Mathematics

SIMON FRASER UNIVERSITY

September 1978

Approval

Name: Murray Martin

Degree: Master of Science

Title of Thesis: THE MAJOR ADDITIVITY THEOREMS FOR SCHNIRELMANN AND ASYMPTOTIC DENSITY

Examining Committee:

Chairperson: A.H. Lachlan

A.R. Freedman
Senior Supervisor

J.L. Berggren

D. Sharma

J.J. Sember
External Examiner

Date Approved: September 6, 1978

Abstract

In this thesis we give the major additive results for Schnirelmann and asymptotic density. A concise proof of the $\alpha + \beta$ Theorem (Mann's Theorem), which deals with finding a lower bound for the Schnirelmann density of the sum of two sets, appears in Chapter 2. However, the majority of the thesis is devoted to the development and proof of the theorem of M. Kneser. Kneser's result deals with finding a lower bound for the asymptotic density of the sum of two sets. In both the proof of the $\alpha + \beta$ Theorem and Kneser's Theorem we rely heavily on the use of τ-transformations. The τ-transformations are similar to the transformations used by F. Dyson. They are used to modify the sets being added in such a way that certain additive and density properties remain invariant.

Acknowledgments

The author would like to express his appreciation to Dr. A.R. Freedman, of the Mathematics Department at Simon Fraser University, for choosing the topic of the thesis and for all his ideas and suggestions, without which this thesis would not have been written.

He would like to thank his wife Janette, for the hours spent proofreading the thesis for spelling and punctuation mistakes. Also, he wishes to acknowledge Kathy Bootle for an excellent job in typing the thesis. Finally, he would like to thank those associated with the Mathematics Department at Simon Fraser University who have made his years of training in mathematics so memorable.

Table of Contents

Introduction

In this thesis we will present the major additivity theorems for Schnirelmann and asymptotic density.

Let I denote the set of all integers and I_0 denote the set of all nonnegative integers. The sum $A + B$ of two sets A and B is the set of all integers of the form $a + b$, where $a \in A$ and $b \in B$. $A(n)$ will denote the number of positive integers belonging to A which are less than or equal to n.

The Schnirelmann density, $d(A)$, of A is defined by

$$d(A) = \operatorname*{glb}_{n \geq 1} \frac{A(n)}{n} .$$

In 1931, E. Landau and L. Schnirelmann (see [5]) conjectured that for any $A,B \subset I_0$, if $0 \in A \cap B$ and $d(A) + d(B) \leq 1$, then

$$d(A+B) \geq d(A) + d(B),$$

but were unable to prove the conjecture. Early in 1932, A. Khintchin [6] proved the conjecture true for the special case when $d(A) = d(B)$. This problem attained the stature of a famous unsolved problem known as the $\alpha + \beta$ conjecture. Finally, in 1942, H.B. Mann [8] proved the conjecture was true for all sets A and B which satisfy the hypothesis. Later, Dyson [2] was able to give a simpler and clearer proof than H.B. Mann [8], which leant itself more readily to generalizations.

The asymptotic density, $\delta(A)$, of A is defined by

$$\delta(A) = \liminf_{n\to\infty} \frac{A(n)}{n} .$$

For asymptotic density $\delta(A+B) \geq \delta(A) + \delta(B)$ is not necessarily true. For example, if $A = B = \{0,2,4,\ldots\}$, then $\delta(A+B) = \frac{1}{2}$, while $\delta(A) + \delta(B) = 1$. However, M. Kneser [7] in 1953 proved what might be called the analog to the $\alpha + \beta$ Theorem for asymptotic density. Kneser proved that if $A,B \subset I$ and $\delta(A) + \delta(B) \leq 1$, then $\delta(A+B) \geq \delta(A) + \delta(B)$, except that, when A and B are associated with a union of residue classes modulo g, in a way that will be described in detail in Chapter 3, we get the following weaker inequality holding,

$$\delta(A+B) \geq \delta(A) + \delta(B) - \frac{1}{g} .$$

In the above example $g = 2$ and $\delta(A+B) = \frac{1}{2}$, $\delta(A) + \delta(B) - \frac{1}{g} = \frac{1}{2}$.

In Chapter 1 we state and prove some of the elementary properties of Schnirelmann and asymptotic density for subsets of I_0. Many of these elementary properties will be useful in later chapters. In Chapter 2 we define τ-transformations and state and prove their useful properties. The τ-transformations are used extensively in the proof of the $\alpha + \beta$ Theorem and Kneser's Theorem. We conclude Chapter 2 with an elegant proof of the $\alpha + \beta$ Theorem using τ-transformations. In Chapter 3 we prove Kneser's remarkable theorem. Although the proof is 40 pages long, each step is of an elementary nature. I have attempted and, I believe, succeeded in giving a clearer proof than any found in the literature. In Chapter 4 we show that Kneser's Theorem implies the previous results concerned with finding lower bounds for the asymptotic density of the sum of two sets of integers.

We introduce the following notation and definitions which we will use extensively throughout this thesis. In the first two chapters, the letters $A,B,C,\ldots$ denote subset of I_0; the letters $a,b,c,\ldots$ denote the elements of $A,B,C,\ldots$ respectively. However in Chapter 3, we allow $A,B,C,\ldots$ to be subsets of I. For any set A and integer t,

$$t + A = \{t+a \mid a \in A\} ,$$

is referred to as the <u>translation of A by t</u>. For any subsets A,B of I, A is said to be <u>equivalent</u> to B (denoted by $A \sim B$), if there exists an integer N such that

$$A \cap \{n \mid n \geq N\} = B \cap \{n \mid n \geq N\} .$$

If m,n are nonnegative integers such that $m \leq n$, we denote by $A[m,n]$, the number of elements a of A satisfying $m \leq a \leq n$. Then $A[1,n] = A(n)$, and

$$A[1,n] = A[1,m] + A[m+1,n], \text{ if } 1 \leq m < n.$$

For convenience we will redefine both Schnirelmann and asymptotic density in Chapter 1.

Chapter 1.

Schnirelmann and Asymptotic Density

§1. Schnirelmann Density

Let $A(n)$ denote the counting function of the positive part of A, that is,

$$A(n) = \sum_{1 \le a \le n} 1,$$

is the number of positive integers in A not exceeding n.

We define the Schnirelmann density, $d(A)$, of A by $d(A) = \operatorname{glb}_n \{ \frac{A(n)}{n} \mid n=1,2,3,\ldots \}$. To help familiarize the reader with Schnirelmann density we shall state and prove a few of the elementary properties of this definition.

1.1.1 Proposition. If $A \subset I_0$, then $0 \le d(A) \le 1$.

Proof. Follows clearly from the fact that $0 \le \frac{A(n)}{n} \le 1$ for all n.

1.1.2 Proposition. If $\alpha = d(A)$, then $A(n) \ge \alpha n$ for all n $(n=1,2,3,\ldots)$.

Proof. This result follows from the fact that $\alpha \le \frac{A(n)}{n}$ for all n.

1.1.3 Proposition. If $1 \notin A$, then $d(A) = 0$.

Proof. If $1 \notin A$, then $\frac{A(1)}{1} = 0$, so that $d(A) = \operatorname{glb}_{n \ge 1} \{ \frac{A(n)}{n} \} = 0$.

1.1.4 Proposition. If $\alpha = d(A)$, then $\alpha = 1$ if and only if $A = I_0$ or $A = I_0 \setminus \{0\}$.

Proof. Assume $\alpha = 1$, then $\frac{A(n)}{n} = 1$ for all n, which implies that $A = I_0$ or $A = I_0 \setminus \{0\}$. Assume $A = I_0$ or $A = I_0 \setminus \{0\}$, then $\frac{A(n)}{n} = 1$ for all n and therefore $\alpha = 1$.

The counting function plays an important role in the theory of density. The following result about counting functions is very useful in that it gives a bound of the sum of the counting functions at n, of two sets if the integer n does not belong to the sum of the two sets.

1.1.5 Proposition. If $0 \in A \cap B$ and $n \notin A + B$, then $A(n) + B(n) \leq n - 1$.

Proof. Since $n \notin A + B$ and $0 \in A \cap B$, then $n \notin A$ and $n \notin B$. Let $0 < a_1 < a_2 < \ldots < a_k \leq n$ be all the elements belonging to A which are less than or equal to n, so that $A(n) = k$. For each i, $(i=1,2,\ldots,k)$ $n - a_i \in \{1,2,\ldots,n-1\}$ and $n - a_i \notin B$, for if $n - a_i \in B$, then $a_i + (n-a_i) = n \in A + B$, contradicting our hypothesis. Since there are k elements of the form $n - a_i$ and since $n \notin B$, then $B(n) = n - (k+1)$. So it follows that $A(n) + B(n) \leq k + n - (k+1) = n - 1$.

The following proposition is an early result in the development of the theory of density.

1.1.6 Proposition. If $A, B \subset I_0$, $0 \in A \cap B$ and $d(A) + d(B) \geq 1$, then $A + B = I_0$.

Proof. Let $\alpha = d(A)$ and $\beta = d(B)$. Assume that $A + B \neq I_0$, then there exists an $n \in I_0$ such that $n \notin A + B$. Then by Propositions 1.1.2 and 1.1.5 we have the following

$$1 \leq \alpha + \beta \leq \frac{A(n)}{n} + \frac{B(n)}{n} = \frac{A(n) + B(n)}{n} < \frac{n - 1}{n} < 1 ,$$

which is a contradiction. Therefore $A + B = I_0$.

L. Schnirelmann (see [5]) asked the question: To what extent is the density of the sum of several sequences determined solely by the density of the summands, irrespective of their arithmetical nature. We shall be interested in this question as it pertains to two sets only. E. Landau and L. Schnirelmann (see [5]) proved the following remarkable inequality:

If $0 \in A \cap B$, then $d(A+B) \geq d(A) + d(B) - d(A)d(B)$.

This was the first tool for estimating the density of a sum of two sets from the densities of the summands. A.S. Besicovitch [1], defining $d'(B) = \operatorname{glb}_n \left\{ \frac{B(n)}{n + 1} \right\}$ $(n=1,2,\ldots)$ was able to prove the following:

If $1 \in A$ and $0 \in B$, then $d(A+B) \geq d(A) + d'(B)$.

P. Erdös [3] was able to improve on this result when he was able to show that:

If $1 \in A$ and $0 \in B$, then $d(A+B) \geq d(A) + d^*(B)$,

where $d^*(B) = \operatorname{glb}_{n>k} \{ \frac{B(n)}{n+1} \}$, $\{1,2,\ldots,k\} \subset B$, but $k+1 \notin B$.
It is clear from the definitions that for any set B, $d^*(B) \geq d'(B)$.

As mentioned in the introduction, E. Landau and L. Schnirelmann conjectured that:

if $0 \in A \cap B$, $d(A) + d(B) \leq 1$, then $d(A+B) \geq d(A) + d(B)$,

but it was not until eleven years later that the conjecture was proven true by H.B. Mann [8]. However, the result by A.S. Besicovitch is not superseded by the $\alpha + \beta$ Theorem, since $0 \in A$ is not stipulated.

§2. Asymptotic Density

We define the asymptotic density, $\delta(A)$, of A by $\delta(A) = \liminf_{n\to\infty} \frac{A(n)}{n}$ $(n=1,2,\ldots)$. Thus, by contrast with Schnirelmann density, the early elements of A do not have a disproportionately important effect on the value of $\delta(A)$. We shall now state a few elementary results about asymptotic density.

1.2.1 Proposition. If $A \subset I_0$, then $0 \le \delta(A) \le 1$.

Proof. The result follows clearly from the fact that $0 \le \frac{A(n)}{n} \le 1$ for all n.

1.2.2 Proposition. If $A \subset I_0$, then $d(A) \le \delta(A)$.

Proof. Let $g_k = \text{glb}\{ \frac{A(n)}{n} \mid n \ge k\}$ $(k=1,2,\ldots)$. Since $g_1 \le g_2 \le g_3 \le \ldots \le g_k \le \ldots$, we have that,

$$d(A) = g_1 \le \lim_{k\to\infty} g_k = \liminf_{n\to\infty} \frac{A(n)}{n} = \delta(A).$$

1.2.3 Proposition. If $A,B \subset I_0$ with $A \subset B$, then $\delta(A) \le \delta(B)$.

Proof. Since $A \subset B$, then $A(n) \le B(n)$ for all n $(n=1,2,\ldots)$. So that $\frac{A(n)}{n} \le \frac{B(n)}{n}$, and $\delta(A) = \liminf_{n\to\infty} \frac{A(n)}{n} \le \liminf_{n\to\infty} \frac{B(n)}{n} = \delta(B)$.

1.2.4 Proposition. Let $A \subset I_0$ and x be any positive integer,

i) if $B = A + x$, then $\delta(A) = \delta(B)$,

ii) if $B = A - x$, then $\delta(A) = \delta(B)$.

Proof. Let $\alpha = \delta(A)$ and $0 < a_1 < a_2 < \ldots < a_k \le n < a_{k+1} < \ldots < a_{k+x}$ be the first $k + x$ positive integers belonging to A.

Proof of (i). Since $B = A + x$, then $A(n) - x \leq A(n-x) = B(n) \leq A(n)$. Result (i) follows from the fact that,

$$\alpha = \liminf_{n\to\infty} \frac{A(n) - x}{n} \leq \liminf_{n\to\infty} \frac{B(n)}{n} \leq \liminf_{n\to\infty} \frac{A(n)}{n} = \alpha.$$

Proof of (ii). Since $B = A - x$, $a_x \leq x$ and $a_{k+x} \leq n + x$, then

$$A(n) - x \leq B(n) \leq A(n+x) \leq A(n) + x.$$

Our result follows again from the fact that,

$$\alpha = \liminf_{n\to\infty} \frac{A(n) - x}{n} \leq \liminf_{n\to\infty} \frac{B(n)}{n} \leq \liminf_{n\to\infty} \frac{A(n) + x}{n} = \alpha.$$

1.2.5 Proposition. If $A,B \subset I_0$, $0 \in A \cap B$ and $\delta(A) + \delta(B) > 1$, then $A + B \sim I_0$.

Proof. Let $\varepsilon = \delta(A) + \delta(B) - 1$. By the definition of lim inf there exists an N such that $n \geq N$ implies $\frac{A(n)}{n} \geq \delta(A) - \frac{\varepsilon}{4}$ and $\frac{B(n)}{n} \geq \delta(B) - \frac{\varepsilon}{4}$. Now suppose $n \geq N$ and $n \notin A + B$, then by Proposition 1.1.5, $1 + \frac{\varepsilon}{2} = \delta(A) + \delta(B) - \frac{\varepsilon}{2} \leq \frac{A(n)}{n} + \frac{B(n)}{n} < \frac{n-1}{n} < 1$ which is a contradiction. Therefore $(A + B) \cap \{n \mid n \geq N\} = I \cap \{n \mid n \geq N\}$, or $A + B \sim I_0$.

The strict inequality in the hypothesis of Proposition 1.2.5 is necessary. Consider the case when $A = B = \{0,2,4,6,\ldots\}$, then $\delta(A) = \delta(B) = \frac{1}{2}$ and therefore $\delta(A) + \delta(B) = 1$, but $A + B = \{0,2,4,6,\ldots\}$. So when Proposition 1.2.5 is compared with Proposition 1.1.6, we find that the hypothesis and conclusions are both weaker in

Proposition 1.2.5.

1.2.6 Proposition. If $A, B \subset I_0$ and $A \sim B$, then $\delta(A) = \delta(B)$.

Proof. Since $A \sim B$ then there exists a $k \in I_0$ such that $A \cap \{n \mid n \geq k\} = B \cap \{n \mid n \geq k\}$. From this we can conclude that $A(n) - k \leq B(n) \leq A(n) + k$. Thus $\frac{A(n)-k}{n} \leq \frac{B(n)}{n} \leq \frac{A(n)+k}{n}$ and our result follows from

$$\liminf_{n\to\infty} \frac{A(n)-k}{n} \leq \liminf_{n\to\infty} \frac{B(n)}{n} \leq \liminf_{n\to\infty} \frac{A(n)+k}{n}$$

and the fact that

$$\liminf_{n\to\infty} \frac{A(n)-k}{n} = \liminf_{n\to\infty} \frac{A(n)+k}{n} = \delta(A).$$

1.2.7 Proposition. If $A \subset I_0$ and n is any positive fixed integer and

$$\delta'(A) = \liminf_{k\to\infty} \frac{A(kn)}{kn}, \quad \text{then} \quad \delta(A) = \delta'(A).$$

Proof. For $x \in I_0$ there exists a $k \in I_0$ such that $kn \leq x < (k+1)n$ and $A(kn) \leq A(x) < A((k+1)n)$. Thus $\frac{A(kn)}{(k+1)n} \leq \frac{A(x)}{x} < \frac{A((k+1)n)}{kn}$, so that $\frac{k}{k} \cdot \frac{A(kn)}{(k+1)n} \leq \frac{A(x)}{x} < \frac{A((k+1)n)}{kn} \cdot \frac{(k+1)}{(k+1)}$ which implies that

$$\frac{k}{k+1} \cdot \frac{A(kn)}{kn} \leq \frac{A(x)}{x} < \frac{k+1}{k} \cdot \frac{A((k+1)n)}{(k+1)n} .$$

Therefore, $\liminf_{k\to\infty} \frac{k}{k+1} \cdot \frac{A(kn)}{kn} \leq \liminf_{x\to\infty} \frac{A(x)}{x} \leq \liminf_{k\to\infty} \frac{k+1}{k} \cdot \frac{A((k+1)n)}{(k+1)n}$, and we get that $\delta'(A) \leq \delta(A) \leq \delta'(A)$.

1.2.8 Proposition. If $0 \le a_1 < a_2 < \dots < a_k$ are incongruent modulo g and $A = \{a_i + ng \mid i = 1,2,\dots,k,\ n \in I_0\}$, then $\delta(A) = \frac{k}{g}$.

Proof. The result follows from the fact that $\frac{k\cdot[\frac{n}{g}]-C}{n} \le \frac{A(n)}{n} \le \frac{k\cdot[\frac{n}{g}]+k}{n}$ for all $n \in I_0$, where $C = \max_{1\le i\le k}\{a_i\}$. Thus

$$\frac{k}{g} = \liminf_{n\to\infty} \frac{k\cdot[\frac{n}{g}]-C}{n} \le \liminf_{n\to\infty} \frac{A(n)}{n} \le \liminf \frac{k\cdot[\frac{n}{g}]+k}{n} = \frac{k}{g}.$$

The reader should note that if we allow A to contain the negative part of each congruence class, the conclusion will still remain the same since $A(n)$ only counts the positive integers of A that are less than or equal to n.

In Chapter 1 we have presented the definitions and some of the elementary properties of both Schnirelmann and asymptotic density. The reader should now be better prepared to understand the development and proof of the $\alpha + \beta$ Theorem and Kneser's Theorem.

Chapter 2.

τ-transformations and the $\alpha + \beta$ Theorem.

The major result used in the proof of Kneser's theorem requires the systematic use of τ-transformations. Given two sets A and B, we shall construct two new sets A' and B', the τ-transforms of A and B, by removing certain positive elements from B giving B' and placing additional elements into A giving A'. The transformation τ will depend only on the choice of a particular element a_o of A.

2.1.1 Definition. The strong union $A \vee B$ of two sets A and B each containing 0, is defined to be the aggregate of the elements of A and B; each element being counted according to its multiplicity, except that 0 is counted only once.

The distinction between union and strong union is required for counting purposes only; we may regard the two as identical except in the one respect that the elements of the latter are weighted for counting purposes. If $A = \{0,1,2,4,6,10\}$ and $B = \{0,2,4,7,8,10\}$, then $A \vee B = \{0,1,2,2,4,4,6,7,8,10,10\}$. From the example it becomes clear that $(A \vee B)(n) = A(n) + B(n)$, and in particular if $0 \in A$, then $(A \vee B)[0,n] = A[0,n] + B[1,n]$. With this in mind we define

$$\delta(A \vee B) = \liminf_{n\to\infty} \frac{(A \vee B)(n)}{n}.$$

2.1.2 Definition. Let $\langle A,B\rangle$ be a given system of sets. If $a_o \in A$, then we define the new system $\langle A,B\rangle^\tau = \langle A^\tau, B^\tau\rangle$, where

$\tau = \tau(a_o)$ by;

$$A^\tau = A \cup (a_o+B) \ ,$$
$$B^\tau = B \cap (A-a_o) \ ,$$

and we define

$$C = A + B \ , \qquad C^\tau = A^\tau + B^\tau \ ,$$

and
$$V = A \vee B \ , \qquad V^\tau = A^\tau \vee B^\tau \ .$$

2.1.3 Theorem. The transformation τ has the following properties:

i) $A \subset A^\tau$, $B^\tau \subset B$,

ii) $C^\tau \subset C$,

iii) $a_o + B^\tau \subset A \subset A^\tau$,

iv) If $0 \in A$, then $0 \in A^\tau$ and if $0 \in B$, then $0 \in B^\tau$,

v) $\delta(V^\tau) = \delta(V)$.

The proofs of (i), (iii) and (iv) are obvious.

Proof of (ii). We need to show that $A^\tau + B^\tau \subset A + B$. Let $y \in A^\tau + B^\tau$, then $y = x + b^\tau$ where $x \in A^\tau$ and $b^\tau \in B^\tau$. First consider the case where $x = a \in A$, so that $y = x + b^\tau = a + b^\tau \subset A + B$ by (i). Now consider the case where $x = a_o + b$, $a_o \in A$ and $b \in B$, so that $y = x + b^\tau = (a_o+b) + b^\tau = (a_o+b^\tau) + b \subset A + B$ by (iii).

Proof of (v). Since $A^\tau = A \cup (a_o+B)$ and $B^\tau = B \cap (A-a_o)$, we define $B' = \{b \mid b \in B \text{ and } b \neq a - a_o \text{ for any } a \in A\}$. The system $\langle A,B\rangle^\tau$ can be described by: the set B' has been removed from B leaving B^τ and $a_o + B'$ has been included in A, thus making up A^{τ}. Therefore $V(n)$ and $V^{\tau}(n)$ differ at most by the number of integers of B' lying in the interval $[n-a_o+1,n]$, that is, $V(n) - |a_o| \leq V^{\tau}(n) \leq V(n)$ for all n and therefore $\delta(V) = \delta(V^{\tau})$.

When we write $\langle A,B\rangle^{\tau_1\tau_2} = \langle A^{\tau_1},B^{\tau_1}\rangle^{\tau_2}$ we shall mean that $\langle A,B\rangle^{\tau_1\tau_2}$ is derived from $\langle A,B\rangle$ by first applying τ_1 to $\langle A,B\rangle$ by means of some element $a_o \in A$ and then by applying τ_2 to $\langle A^{\tau_1},B^{\tau_1}\rangle$ by means of some element $a_1 \in A^{\tau_1}$. We shall represent a finite sequence of τ-transformations by T, and write $\langle A,B\rangle^{T}$ for $\langle A,B\rangle^{\tau_1\tau_2\ldots\tau_r}$ if $\langle A,B\rangle^{T}$ is the result of applying τ_1 to $\langle A,B\rangle$, τ_2 to $\langle A^{\tau_1},B^{\tau_1}\rangle$, ..., and finally, τ_r to $\langle A^{\tau_1\tau_2\ldots\tau_{r-1}}, B^{\tau_1\tau_2\ldots\tau_{r-1}}\rangle$. We shall refer to $\langle A,B\rangle^{T}$ as a system derived from $\langle A,B\rangle$, or as a derivation of $\langle A,B\rangle$. A derivation $\langle A^{T},B^{T}\rangle^{T'}$ of $\langle A^{T},B^{T}\rangle$ is also a derivation $\langle A,B\rangle^{TT'}$ of $\langle A,B\rangle$.

2.1.4 <u>Theorem</u>. Any derived system $\langle A,B\rangle^{T}$ of $\langle A,B\rangle$ has the following properties:

i) $A \subset A^{T}$, $B^{T} \subset B$,

ii) $C^{T} \subset C$,

iii) If $0 \in A$, then $0 \in A^{T}$ and if $0 \in B$, then $0 \in B^{T}$,

iv) $\delta(V^{T}) = \delta(V)$.

All of these properties are obvious consequences of Theorem 2.1.3.

We are now in a position to use τ-transformations to prove a theorem, which is a combination of a theorem by Dyson [2] and a theorem by van der Corput [10]. From this theorem, with very little difficulty we shall be able to prove the $\alpha + \beta$ Theorem, and later we shall use this theorem in the proof of Kneser's result.

2.1.5 Theorem. Let $0 < \gamma \leq 1$ and n be any positive integer. Also let A and B be two sets, each containing 0 and lying entirely within the interval $[0,n]$. Denote by V and C the strong union and sum, respectively, of A and B. If $\theta = 0$ or 1, then

$$\text{i)} \quad V[\theta,m] \geq \gamma(m-\theta+1) \qquad (m=\theta,\theta+1,\ldots,n) ,$$

implies

$$\text{ii)} \quad C[\theta,m] \geq \gamma(m-\theta+1) \qquad (m=\theta,\theta+1,\ldots,n) .$$

Proof. We suppose on the contrary that the result is false, and that n is the least positive integer for which there exists a pair of sets contained in $[0,n]$ for which (i) is true and (ii) is false. Among all such pairs of sets we choose A and B with the additional property that $B[0,n]$ is minimal. We may suppose that B contains at least one positive element, for if 0 is the only element of B, the statements (i) and (ii) are identical.

We shall obtain a contradiction in the following manner. We shall construct two new sets A' and B', by using τ-transformations, with the following properties:

iii) $V'[\theta,m] \geq \gamma(m-\theta+1)$ $(m=\theta,\theta+1,\ldots,n)$,

iv) $C' \subset C$,

v) $B'[0,n] < B[0,n]$.

Properties (iii) and (iv) imply that the pair A' and B' satisfy (i) but not (ii) and property (v) contradicts the minimal property of $B[0,n]$.

Let a^* be the least among the elements $a \in A$ for which $a + B \not\subset A$. The element a^* exists, for since B contains a positive element, the largest element of $A + B$ is certainly not in A. We will show that, if $a^* > 0$ and r is any integer satisfying $0 \leq r < a^*$, then

vi) $b + (A \cap [0,r]) \subset A$ for every $b \in B$,

from which it immediately follows that,

vii) if $A[0,r] \geq \gamma(r+1)$, then $A[b,b+r] \geq A[0,r] \geq \gamma(r+1)$ for every $b \in B$.

Proof of (vi). Let $x \in b + (A \cap [0,r])$. Then $x = b + a$ for some $a \in A$ and $b + a \leq r < a^*$ which implies that $a < a^*$. By the definition of a^*, $a + B \subset A$ and hence $x = a + b \in A$.

We shall require the following fact:

2.1.6 If $a^* > 0$, then for every r satisfying $0 \leq r < a^*$, $A[0,r] \geq \gamma(r+1)$.

Proof of 2.1.6. Suppose there exist r satisfying $0 \le r < a^*$ for which $A[0,r] < \gamma(r+1)$, and let r' be the least such r. Since $0 \in A$ and $\gamma \le 1$, it follows that $r' \ge 1$ and so $A[1,r'] < \gamma r'$. Therefore $A[\theta,r'] < \gamma(r'-\theta+1)$. However, by (i), $V[\theta,r'] \ge \gamma(r'-\theta+1)$, and therefore $[\theta,r']$ must contain a positive element $b_o \in B$ since $V[\theta,r'] = A[\theta,r'] + B[1,r']$. Now, by the minimal property of r', $A[0,b_o-1] \ge \gamma b_o$ while $A[0,r'] < \gamma(r'+1)$. Thus $A[b_o,r'] < \gamma(r'-b_o+1)$ and, by (vii) (with $r = r' - b_o$), $A[0,r'-b_o] < \gamma(r'-b_o+1)$. Since b_o is positive, this contradicts the definition of r' and 2.1.6 is proved.

Recall that $a^* \in A$. Define $B'' = \{b \mid b \in B,\ a^* + b \notin A\}$. B'' is nonempty, since a^* satisfied the condition that $a^* + B \not\subset A$. Let $\tau = \tau(a^*)$ and thus

$$A^\tau = A \cup (a^*+B) = A \cup (a^*+B''),$$

and

$$B^\tau = B \cap (A-a^*) = B \setminus B''.$$

The set B^τ satisfies property (v) since $B^\tau = B \setminus B''$ and B'' is nonempty. Property (iv) is true by (ii) of Theorem 2.1.3.

It remains to confirm (iii). If $a^* = 0$, then V' and V are identical (since the difference between A^τ, B^τ and A, B is that some of the elements of B have been placed in A). In this case (i) and (iii) are the same.

We may assume that $a^* > 0$. Considering (iii) for a particular $m \le n$, the translation of B'' causes only those elements b of B''

in the interval $[m-a^*+1,m]$ to fall outside of $[\theta,m]$. Hence $V'[\theta,m] = V[\theta,m] - B[m-a^*+1,m]$ for all $m \le n$. Therefore to confirm (iii), it will be sufficient to prove that, for each m, $V[\theta,m] - B[m-a^*+1,m] \ge \gamma(m-\theta+1)$.

Let b_1 be the least positive $b \in B$ in the interval $[m-a^*+1,m]$ (if there is no such b_1 there is nothing to prove). Let $m = b_1 + r$ so that $0 \le r < a^*$. Then $V[\theta,b_1-1] \ge \gamma(b_1-\theta)$. Since $V[\theta,m] - B[m-a^*+1,m] = V[\theta,b_1-1] + A[b_1 m]$, then $A[b_1,m] \ge \gamma(m-b_1+1)$ is all that remains to be proved. $A[0,r] \ge \gamma(r+1)$ is true by 2.1.6 and therefore $A[b_1,m] = A[b_1,b_1+r] \ge \gamma(r+1)$ is true by (vii). This establishes (iii), and so the proof of Theorem 2.1.5 is complete.

The restriction, in Theorem 2.1.5, that both A and B be contained in the interval $[0,n]$ is made only for the purpose of simplifying the notation in the proof. The following corollary is an immediate consequence of Theorem 2.1.5.

2.1.7 <u>Corollary</u>. Let $0 < \gamma \le 1$. If $\theta = 0$ or 1 and $0 \in A \cap B$, then

$$V[\theta,m] \ge \gamma(m-\theta+1) \quad (m=\theta,\theta+1,\ldots),$$

implies

$$C[\theta,m] \ge \gamma(m-\theta+1) \quad (m=\theta,\theta+1,\ldots).$$

The $\alpha + \beta$ Theorem is one of the most outstanding results in the theory of density. The original proof by H.B. Mann [8] in 1942 was very complicated. We are now in a position to give a quick proof using Corollary 2.1.7 with $\theta = 1$.

2.1.8 $\alpha + \beta$ Theorem. If $A, B \subset I_0$ and $0 \in A \cap B$, then $d(A+B) \geq \min(1, d(A)+d(B))$.

Proof. Let $\alpha = d(A)$ and $\beta = d(B)$.

Case 1. Assume $\alpha + \beta \geq 1$, then by Proposition 1.1.6, $A + B = I_0$ and the result follows immediately.

Case 2. Assume $\alpha + \beta < 1$. $V[1,n] = V(n) = A(n) + B(n) \geq (\alpha+\beta)n$ for $n = 1,2,3,\ldots$ by Proposition 1.1.2. By Corollary 2.1.7, with $\theta = 1$ and $\gamma = \alpha + \beta$, we have that $C(n) \geq \gamma n = (\alpha+\beta)n$ $(n=1,2,3,\ldots)$. This completes the proof of the $\alpha + \beta$ Theorem.

Chapter 3.

Kneser's Theorem

§1. Kneser's Theorem

Kneser's theorem deals with the problem of, given a system of two sets <A,B>, obtaining a lower bound for $\delta(A+B)$ in terms of $\liminf_{n\to\infty} \frac{A(n) + B(n)}{n}$.

It will be convenient to permit A and B to contain negative integers. This allowance makes no essential difference in finding a lower bound for $\delta(A+B)$, since only the positive integers are counted in $A(n)$ and $B(n)$.

We shall begin with some preparatory remarks and definitions. The sum and strong union of the system <A,B> will be denoted respectively by C and V. Since $V(n) = A(n) + B(n)$, our problem now will be to obtain a lower bound for $\delta(C)$ in terms of $\delta(V)$. We will be able to replace, as will be clear later, the system <A,B> by any system <A',B'> which satisfies the following two conditions:

i) $A \subset A'$ and $B \subset B'$,

ii) $C' \sim C$.

3.1.1 Definition. If two systems <A,B> and <A',B'> satisfy conditions (i) and (ii), we say that <A',B'> is a worse system than <A,B>.

3.1.2 Lemma. Let a, b be any integers. If we define a new system $\langle A',B'\rangle$ from the system $\langle A,B\rangle$ by,

$$A' = A - a,$$

and

$$B' = B - b,$$

then $\delta(C) = \delta(C')$ and $\delta(V) = \delta(V')$.

Proof. Both results are obvious consequences of Proposition 1.2.4.

3.1.3 Definition. Let $0 \leq r_1 < r_2 < \ldots < r_k < g$ and $0 \leq s_1 < s_2 < \ldots < s_\ell < g$. If $A = \bigcup_{i=1}^{k} \{ng + r_i \mid n \in I\}$ and $B = \bigcup_{i=1}^{\ell} \{ng + s_i \mid n \in I\}$, then we say that the system $\langle A,B\rangle$ is degenerate modulo g.

The reader will note that A and B are the union of entire congruence classes modulo g. If we say that the system $\langle A,B\rangle$ is degenerate, we mean that it is degenerate modulo g, for some g.

The following example will show that the inequality $\delta(C) \geq \min(1,\delta(V))$ suggested by a direct analogy to the $\alpha + \beta$ Theorem is false; and that, for systems $\langle A,B\rangle$ which are degenerate modulo g, we cannot prove more than

iii) $\delta(C) \geq \delta(V) - \frac{1}{g}$.

If $A = B = \{n \mid n \equiv 0,1 \text{ modulo } g\}$, then $\delta(C) = \frac{3}{g}$ and $\delta(V) = \frac{4}{g}$.

The inequality (iii) does not hold in general, unless g is minimal in some sense. For if $\langle A,B\rangle$ is degenerate modulo g, it is also degenerate modulo mg for any integer $m > 1$; and if <A,B> is chosen to satisfy $\delta(C) = \delta(V) - \frac{1}{g}$, then (iii) is false when g is replaced by mg. We will find that the minimal condition for g is that there are no systems <A',B'> worse than <A,B> that are degenerate to a modulus less than g. We shall eventually prove the following theorem due to M. Kneser [7].

3.1.4 Theorem. If the system <A,B> is degenerate modulo g, then there exists a divisor g' of g and a system <A',B'>, degenerate modulo g', such that <A',B'> is worse than <A,B> and

$$\delta(C') \geq \delta(V') - \frac{1}{g'} .$$

By Proposition 1.2.6 and Proposition 1.2.3, it follows that $\delta(C) = \delta(C') \geq \delta(V') - \frac{1}{g'} \geq \delta(V) - \frac{1}{g'}$ and Theorem 3.1.4 gives an answer to our problem in the case when <A,B> is degenerate modulo g. The following theorem gives an answer to our problem in the case when <A,B> is any system such that there exists a system <A',B'> degenerate modulo g' which is worse than <A,B>.

3.1.5 Theorem. Let <A,B> be any system. If there exists a system <A',B'> degenerate modulo g' and worse than <A,B>, then there exists a divisor g" of g' and a system <A",B"> such that <A",B"> is worse than <A',B'> and

$$\delta(C) \geq \delta(V) - \frac{1}{g''} .$$

Proof. By Theorem 3.1.4, $\delta(C'') \geq \delta(V'') - \frac{1}{g''}$. Since $\delta(C) = \delta(C') = \delta(C'')$ and $\delta(V'') \geq \delta(V') \geq \delta(V)$ (by Proposition 1.2.3 and Proposition 1.2.6) we have that $\delta(C) \geq \delta(V) - \frac{1}{g''}$.

A degenerate system $\langle A,B \rangle$ may become non-degenerate when some of the elements are removed from A and/or B. This will happen when a single element is removed, which clearly has no effect on our degenerate case. As a result of Theorem 3.1.5, we include in the degenerate case systems $\langle A,B \rangle$ which are not degenerate themselves, but corresponding to which there is a worse system which is degenerate.

For the remaining systems not covered by Theorem 3.1.5, we will eventually prove the following remarkable theorem also due to M. Kneser [7].

3.1.6 <u>Theorem</u>. If no system worse than $\langle A,B \rangle$ is degenerate, then $\delta(C) \geq \delta(V)$.

If the conclusion of Theorem 3.1.6 is false for a given system $\langle A,B \rangle$, then there must exist a natural number g' and a system $\langle A',B' \rangle$ degenerate modulo g', such that $\langle A',B' \rangle$ is worse than $\langle A,B \rangle$. Then by Theorem 3.1.4, there exists a natural number g'' and a system $\langle A'',B'' \rangle$ degenerate modulo g'', such that $\langle A'',B'' \rangle$ is worse than $\langle A',B' \rangle$ (also worse than $\langle A,B \rangle$) and $\delta(C'') \geq \delta(V'') - \frac{1}{g''}$.

We may therefore combine Theorem 3.1.5 and Theorem 3.1.6 to give Kneser's theorem.

3.1.7 <u>Theorem</u> (M. Kneser [7]). For any given system <A,B>, either $\delta(C) \geq \delta(V)$ or there exists a natural number g' and a system <A',B'> degenerate modulo g' such that <A',B'> is worse than <A,B> and $\delta(C') \geq \delta(V') - \frac{1}{g'}$.

To help the reader follow the proof of Kneser's Theorem we have added a flowchart following the bibliography, in Appendix II.

§2. Intermediate Results

As we mentioned in Chapter 2, τ-transformations play an important role in the proof of Kneser's theorem. In this section we present a lemma and a theorem, both requiring τ-transformations, that we will use in proving Theorem 3.2.4. Theorem 3.2.4 is the major step used in proving Kneser's theorem 3.1.7 and uses in its proof the principal ideas of Kneser's argument.

3.2.1 <u>Lemma</u>. If F is a finite subset of A and $0 \in B$, then there exists a derivation $\langle A,B\rangle^T$ of $\langle A,B\rangle$ such that

$$F + B^T \subset A^T .$$

Proof. Suppose that $F = \{a_1, a_2, \ldots, a_n\}$. If $\tau_1 = \tau_1(a_1)$ is a τ-transformation applied to $\langle A,B\rangle$, then by (iii) of Theorem 2.1.3,

$$a_1 + B^{\tau_1} \subset A^{\tau_1} .$$

If $\tau_2 = \tau_2(a_2)$ is applied to $\langle A^{\tau_1}, B^{\tau_1}\rangle$, then by (iii) of Theorem 2.1.3 again, $a_2 + B^{\tau_1\tau_2} \subset A^{\tau_1\tau_2}$. Since by (i) of Theorem 2.1.3 $B^{\tau_1\tau_2} \subset B^{\tau_1}$ and $A^{\tau_1} \subset A^{\tau_1\tau_2}$, we have that $a_1 + B^{\tau_1\tau_2} \subset a_1 + B^{\tau_1} \subset A^{\tau_1} \subset A^{\tau_1\tau_2}$ and hence

$$\{a_1, a_2\} + B^{\tau_1\tau_2} \subset A^{\tau_1\tau_2} .$$

At the r^{th} stage of this process, we show in the same way that if

$\tau_r = \tau_r(a^r)$ is applied to $\langle A^{\tau_1\cdots\tau_{r-1}}, B^{\tau_1\cdots\tau_{r-1}}\rangle$, then $a^r + B^{\tau_1\cdots\tau_r}$ and $\{a_1,\ldots,a_{r-1}\} + B^{\tau_1\cdots\tau_r}$ each are contained in $A^{\tau_1\cdots\tau_r}$, and hence

$$\{a_1,a_2,\ldots,a_r\} + B^{\tau_1\cdots\tau_r} \subset A^{\tau_1\cdots\tau_r}.$$

Writing $T = \tau_1\tau_2\cdots\tau_n$, we arrive after n steps at a derivation $\langle A,B\rangle^T$ of $\langle A,B\rangle$ for which $F + B^T \subset A^T$.

3.2.2 Theorem. If $0 \in A \cap B$, if A contains m consecutive integers, and if $\delta(C) < \frac{m}{m+1}\,\delta(V)$, then $C \sim I$.

This Theorem is remarkable in that the hypothesis $\delta(C) < \frac{m}{m+1}\,\delta(V)$ requires that C be small and yet the conclusion of the theorem is that C is large.

Proof. Suppose A contains the m consecutive integers $a, a+1, \ldots, a+m-1$. We define the system $\langle A',B'\rangle$ by $A' = A - a$ and $B' = B$. Then $0 \in A' \cap B'$ and by Lemma 3.1.2, $\delta(C) = \delta(C')$ and $\delta(V) = \delta(V')$. Since the system $\langle A',B'\rangle$ satisfies the hypothesis of Theorem 3.2.2, we may assume without loss of generality that $\{0,1,2,\ldots,m-1\} \subseteq A$. We may even suppose that

i) $\{0,1,2,\ldots,m-1\} + B \subset A$.

For by Lemma 3.2.1, (i) is certainly true for some derivation of $\langle A,B\rangle$, and the hypothesis of Theorem 3.2.2 holds for every derivation of $\langle A,B\rangle$ by Theorem 2.1.4.

If we can prove, for some derivation T, that $C^T \sim I$, then since $C^T \subset C$, we have that $C \sim I$. Note by hypothesis of Theorem 3.2.2 that $\delta(V) > 0$.

Let γ be a positive number satisfying

ii) $\gamma < \delta(V)$,

such that

iii) $\gamma = \frac{m+1}{m}$ if $\frac{m}{m+1}\,\delta(V) > 1$.

We have then, in any case,

iv) $\frac{m}{m+1}\gamma \leq 1$.

Inequality (ii) implies the existence of a positive integer $x_o = x_o(\gamma)$ such that

v) $A(x) + B(x) > \gamma x \quad (x \geq x_o)$,

and we choose x_o to be the least positive integer for which (v) is true. Our choice of x_o implies that

vi) $A(x_o-1) + B(x_o-1) \leq \gamma(x_o-1)$,

and if we subtract this inequality from (v) and replace x by $x + x_o$, we arrive at

vii) $A[x_o,x_o+x] + B[x_o,x_o+x] \geq \gamma(x+1) \quad (x=0,1,2,\ldots)$.

Letting $x = 0$ in (vii) we have that $A[x_o,x_o] + B[x_o,x_o] \geq \gamma$, which implies that $x_o \in A$ or $x_o \in B$. By (i), $B \subset A$ and therefore $x_o \in A$. Let x_1 be the least element of B greater than or equal to x_o. Define the new system $\langle A',B' \rangle$ by

$$A' = (A-x_o) \cap [0,\infty) ,$$

and
$$B' = (B-x_1) \cap [0,\infty) ,$$

so that $0 \in A' \cap B'$. We shall prove that

viii) $$V'[0,x] \geq \frac{m}{m+1}\gamma(x+1) \qquad (x=0,1,2,\ldots) .$$

By the definition of x_0, x_1, the intervals $[x_o,x_o]$, $[x_o,x_1]$ contain exactly one element respectively of A and B, so that

$$A'(x) = A[x_o+1,x_o+x] = A[x_o,x_o+x] - 1 ,$$

and
$$B'(x) = B[x_1+1,x_1+x] = B[x_1,x_1+x] - 1 \geq B[x_o,x_o+x] - 1.$$

It now follows using (vii) that

$$\begin{aligned} V'[0,x] &= A'[0,x] + B'[1,x] \\ &= 1 + A'(x) + B'(x) \\ &\geq 1 + A[x_o,x_o+x] + B[x_o,x_o+x] - 2 \\ &\geq \gamma(x+1) - 1 \\ &\geq \frac{m}{m+1}\gamma(x+1) \quad \text{provided} \quad x \geq \frac{m+1}{\gamma} - 1 . \end{aligned}$$

So, if $x \geq \frac{m+1}{\gamma} - 1$, we have that $V'[0,x] \geq \frac{m}{m+1}\gamma(x+1)$. To complete the proof of (viii) it is sufficient to show that (viii) is true for $x < \frac{m+1}{\gamma} - 1$.

If $0 \leq x < x_1 - x_o$, then the interval $[x_o, x_o+x]$ contains no elements of B so that, by (vii)

ix) $V'[0,x] \geq A'[0,x] = A[x_o,x_o+x] = A[x_o,x_o+x] + B[x_o,x_o+x] \geq \gamma(x+1)$,

and therefore $V'[0,x] \geq \frac{m}{m+1}\gamma(x+1)$.

If $x_1 - x_o \leq x < x_1 - x_o + m$, then since $x_1 \in B$ we have by (i), that $x_1 + \{0,1,2,\ldots,m-1\} \subset A$. Thus the interval $[x_1-x_o,x]$ is entirely contained in A' and we have by (ix), that

$$
\begin{aligned}
V'[0,x] \geq A'[0,x] &= A'[0,x_1-x_o-1] + A'[x_1-x_o,x] \\
&\geq \gamma(x_1-x_o) + (x-x_1+x_o+1) \\
&\geq \frac{m}{m+1}\gamma(x_1-x_o) + \frac{m}{m+1}\gamma(x-x_1+x_o+1) \quad \text{since } \frac{m}{m+1}\gamma \leq 1 \\
&= \frac{m}{m+1}\gamma(x+1) .
\end{aligned}
$$

Next suppose that $x_1 - x_o + m \leq x < \frac{m+1}{\gamma} - 1$. The interval $[0,x]$ contains m elements of A' and $m > \frac{\gamma}{m+1}\gamma(x+1)$ since $x < \frac{m+1}{\gamma} - 1$. Therefore $V'[0,x] \geq A'[0,x] \geq m > \frac{m}{m+1}\gamma(x+1)$ and this completes the proof of (viii).

Since $V'[0,x] \geq \frac{m}{m+1}\gamma(x+1)$ for $x = 0,1,2,\ldots$, then by Corollary 2.1.7 with $\theta = 0$ we have that

x) $C'[0,x] \geq \frac{m}{m+1}\gamma(x+1)$ for $x = 0,1,2,\ldots$.

We will now show that the conclusion of Theorem 3.2.2 follows from (x). We may suppose that $\frac{m}{m+1}\delta(V) > 1$. For if $\frac{m}{m+1}\delta(V) \leq 1$, then (x) implies that $\delta(C) = \delta(C') \geq \frac{m}{m+1}\gamma$ for any γ less than $\delta(V)$, and therefore $\delta(C) \geq \frac{m}{m+1}\delta(V)$ which contradicts our hypothesis.

Suppose then, that $\frac{m}{m+1}\delta(V) > 1$. By (iii), $\frac{m}{m+1}\gamma = 1$ and by (x), we have that $C'[0,x] \geq x + 1$. Therefore for each $x = 0,1,2,\ldots$, all the integers of $[0,x]$ lie in C'; in other words $C' = I_0$. But

$$C = A + B \supset (A'+x_o) + (B'+x_1) = C' + (x_o+x_1) ,$$

so that $C \sim I$.

We now state and prove the following very useful corollary.

3.2.3 Corollary. Let the system $\langle A,B\rangle$ be such that $0 \in A \cap B$ and $\delta(C) < \delta(V)$. Then if there exists an infinite sequence of natural numbers $m_1, m_2, \ldots$ such that

1) $m_i \to \infty$ as $i \to \infty$,

and a sequence of corresponding derivations $\langle A,B\rangle^{T_1}$, $\langle A,B\rangle^{T_2}, \ldots$ of $\langle A,B\rangle$ such that

2) A^{T_i} contains m_i consecutive integers $(i=1,2,\ldots)$, then $C \sim I$.

Proof. Since $\frac{m_i}{m+1} \to 1$ as $i \to \infty$ and $\delta(C) < \delta(V)$, there exists an integer r such that $\delta(C) < \frac{m_r}{m_r + 1}\delta(V)$. Then by (ii) and (iv) of Theorem 2.1.4, we have

$$\delta(C^{T_r}) \leq \delta(C) < \frac{m_r}{m_r + 1}\delta(V) = \frac{m_r}{m_r + 1}\delta(V^{T_r}) ,$$

and by Theorem 3.2.2, $C^{T_r} \sim I$. Since $C^{T_r} \subset C$ we have that $C \sim I$.

To prove Theorem 3.1.7 it will be sufficient to prove Theorem 3.1.5 and Theorem 3.1.6. Both of these theorems will be seen later to follow from Theorem 3.2.5. Before stating Theorem 3.2.5 we need the following important definition.

3.2.4 <u>Definition</u>. For a given set A and a given natural number g, we denote by A^g the set of all numbers of the form $a + gn$ where $a \in A$ and $n \in I$.

The reader will note that A^g is the smallest set containing A which is degenerate modulo g.

3.2.5 <u>Theorem</u>. If $\langle A,B \rangle$ is such that $0 \in A \cap B$ and $\delta(C) < \delta(V)$, there exists a subset E of C, containing 0, and a natural number g, such that

i) $E \sim E^g$,

and

ii) $\delta(E) \geq \delta(V) - \frac{1}{g}$.

We will not prove Theorem 3.2.5 directly, but prove Theorem 3.3.7 which in turn implies Theorem 3.3.9, which we will show implies Theorem 3.2.5.

§3. Proof of Theorem 3.2.5

Throughout this section we will assume

$$0 \in A \cap B ,$$

and

$$\delta(C) \leq \delta(V) .$$

The proof of Theorem 3.2.5 is very long and in places is rather involved. The reader is reminded of the flow chart following the bibliography. I have attempted to present the proof as clearly as possible. It will be helpful to introduce the following two set functions and their useful properties.

3.3.1 Definition. Let A be any set. We define $f(A)$ to be the least element of the set of positive differences of pairs of elements of A;

$$f(A) = \min_{\substack{a,a' \\ a \neq a'}} |a-a'| .$$

3.3.2 Definition. For any given set A, let $g(A)$ denote the highest common factor of the elements of A.

Clearly $g(A)$ is a divisor of $f(A)$ and, in particular,

$$g(A) \leq f(A) .$$

The values $f(B^T)$, $g(B^T)$ corresponding to the derivation $\langle A,B\rangle^T$ of $\langle A,B\rangle$ play a vital part in the following argument.

3.3.3 <u>Lemma</u>. If each set of the system $\langle A,B\rangle$ contains 0, then for every derivation $\langle A,B\rangle^T$,

$$\text{i)} \quad \delta(C) \geq \delta(V) - \frac{1}{f(B^T)},$$

and

$$\text{ii)} \quad \delta(C^T) \geq \delta(V^T) - \frac{1}{g(B^T)}.$$

Proof. For every derivation $\langle A,B\rangle^T$, $0 \in B^T$ by (iii) of Theorem 2.1.4. Put $b_o = 0$ and let b_r be the r^{th} positive element of B^T, $b_o < b_1 < \ldots < b_r < \ldots$. Then $b_r = \sum_{n=1}^{r} (b_n - b_{n-1}) \geq rf(B^T)$ and, taking b_r to be the largest element of B^T not exceeding x, we obtain $B^T(x) \leq \frac{x}{f(B^T)}$. This follows from the fact that $rf(B^T) \leq b_r \leq x$ and $B^T(x) = r$. Since $B^T(x) - \frac{x}{f(B^T)} \leq 0$, we therefore have

$$\delta(C^T) \geq \delta(A^T) \geq \liminf_{\to\infty} \frac{1}{x} \{A^T(x) + B^T(x) - \frac{x}{f(B^T)}\}$$

$$= \delta(V^T) - \frac{1}{f(B^T)},$$

so that (i) follows from the fact that $C^T \subset C$ and $\delta(V^T) = \delta(V)$, and (ii) follows from the fact that $f(B^T) \geq g(B^T)$.

If the set of numbers $f(B^T)$ corresponding to all possible derivations $\langle A,B\rangle^T$ is unbounded, (i) implies that $\delta(C) \geq \delta(V)$. But this is not consistent with our hypothesis for this section, so that we may assume from now on:

1) the set $\{f(B^T) | \langle A,B\rangle^T$ is a derivation of $\langle A,B\rangle\}$,

3.3.4 is bounded,

2) the set $\{g(B^T) | \langle A,B\rangle^T$ is a derivation of $\langle A,B\rangle\}$ is bounded,

(where (2) follows from (1) and the fact that $g(B^T) \leq f(B^T)$). Let

3.3.5
$$g = \max_{\langle A,B\rangle^T} g(B^T) ,$$

where the max is taken over all derivations of $\langle A,B\rangle$.

3.3.6 Lemma. If $\langle A^T, B^T\rangle$ is a derivation of $\langle A,B\rangle$, then $f(B^T) \geq f(B)$ and $g(B^T) \geq g(B)$.

Proof. If $\langle A,B\rangle^T$ is a derivation of $\langle A,B\rangle$, we have, by (i) of Theorem 2.1.4, that $B^T \subset B$, and the lemma follows from the Definitions 3.3.1 and 3.3.2.

Let $\langle A,B\rangle^T$ be any derivation such that $g = g(B^T)$ is maximal. By Lemma 3.3.6, if $(\langle A,B\rangle^T)^{T'}$ is any derivation of $\langle A,B\rangle^T$, (and therefore also of $\langle A,B\rangle$), then $g(B^{TT'}) = g(B^T) = g$. If for the system $\langle A,B\rangle$, $g(B) = g$ is maximal, then for any derivation $\langle A,B\rangle^T$ of $\langle A,B\rangle$, $g(B^T) = g$.

With the properties of the set functions f and g in mind, we begin our proof of Theorem 3.2.5 by first proving the following theorem which later we will show implies Theorem 3.2.5.

3.3.7 Theorem. Let $\langle A,B\rangle$ be a system with the following properties;

i) $0 \in A \cap B$,

ii) $\delta(C) < \delta(V)$,

iii) $g(B^T) = g(B) = g$ for every derivation $\langle A,B\rangle^T$,

iv) A contains g consecutive integers.

Then $C \sim I$.

The proof of Theorem 3.3.7 requires the following lemma.

3.3.8 <u>Lemma</u>. Let $\langle A,B\rangle$ satisfy conditions (i) and (iii) of Theorem 3.3.7. If F is a finite subset of A, then there exists an integer y and a derivation $\langle A,B\rangle^T$ of $\langle A,B\rangle$ such that

1) $(y+F) \cup (y+g+F) \subset A^T$.

Before giving the proof, we shall use Lemma 3.3.8 to prove Theorem 3.3.7. Let $= \{a_o, a_o+1, \ldots, a_o+g-1\}$ be the set of g consecutive integers of A. Applying Lemma 3.3.8, (1) states that A^T contains the set

$$L_T = \{a_o+y, a_o+y+1, \ldots, a_o+y+g-1, a_o+y+g, a_o+y+g+1, \ldots, a_o+y+2g-1\}$$

consisting of $2g$ consecutive integers. By (iii) of Theorem 2.1.4 and Lemma 3.3.6, the system $\langle A^T, B^T\rangle$ satisfy the hypothesis of our lemma. Therefore applying the lemma to $\langle A^T, B^T\rangle$, there exists a further derivation $\langle A^T, B^T\rangle^{T_1}$ for which A^{TT_1} contains $3g$ consecutive integers, and so on. Therefore we have an infinite sequence of derivations of $\langle A,B\rangle$ satisfying the hypothesis of Corollary 3.2.3 with $m_i = ig$, $(i=1,2,3,\ldots)$, and Theorem 3.3.7 follows from this corollary.

Proof of Lemma 3.3.8. Let $f = \max_{\langle A,B\rangle^T} f(B^T)$ and let $P = \{\langle A,B\rangle^T \mid f(B^T) = f\}$. It follows from the definition of f and Lemma 3.3.6 that P is closed under the operation of derivations. We choose from the set P of all derivations of $\langle A,B\rangle$ one system, call it $\langle A,B\rangle^{T_1}$, for which the number of residue classes modulo f with representatives in B^{T_1} is minimal. Let $p_1,p_2,\ldots,p_k \pmod f$ be these residue classes. Also let Q be the set of all derivations of $\langle A,B\rangle^{T_1}$. Thus for every derivation $(\langle A,B\rangle^{T_1})^T$ of $\langle A,B\rangle^{T_1}$, $B^{T_1 T}$ is represented by the same residue classes $p_1,p_2,\ldots,p_k \pmod f$. Otherwise, by (i) of Theorem 2.1.4, $B^{T_1 T} \subset B^T$ and any fewer residue classes would contradict our choice of $\langle A,B\rangle^{T_1}$. All elements $\langle A,B\rangle^T$ of Q satisfy the following properties:

a) $g(B^T) = g(B) = g$,

b) $f(B^T) = f$ and B^T contains at least two elements whose difference is f,

c) B^T intersects exactly the residue classes $p_1,p_2,\ldots,p_k \pmod f$,

d) Q is closed under derivations.

By the definition of g and property (a), g can be expressed as a linear combination of a finite number of elements of B^T. By property (c), there exist integers $n_1,n_2,\ldots,n_k$ such that $g = \sum_{i=1}^{k} n_i p_i \pmod f$. This congruence can be expressed in the following more convenient form

$$2)\quad g = \sum_{j=1}^{k'} \sigma_j \pmod f ,$$

where $k' = n_1+n_2+\ldots+n_k$ and $\sigma_1,\sigma_2,\ldots \sigma_{k'}$ consists of the integers $p_1,p_2,\ldots,p_k$, each p_i occurring with multiplicity n_i for $i=1,2,\ldots,k$.

We can now prove (1). Let $<A,B>^T \in Q$. Since $F \subset A$, then $F \subset A^T$. Thus, applying Lemma 3.2.1 to $<A,B>^T$ and using property (d), there exists a derivation $<A,B>^{T_1}$ of $<A,B>^T$ such that $F + B^{T_1} \subset A^{T_1}$ and $<A,B>^{T_1} \in Q$. B^{T_1} contains an element $x_1 \equiv \sigma_1 \pmod f$, by property (c) so that $F + x_1 \subset A^{T_1}$. Since the system $<A,B>^{T_1}$ satisfies the hypothesis of our lemma, then applying the same procedure with $<A,B>^{T_1}$ in place of $<A,B>^T$ and $F_1 = F + x_1$ in place of F, we arrive at a derivation $<A,B>^{T_2} \in Q$ of $<A,B>^{T_1}$, such that

$$(x_1+x_2) + F = x_2 + F_1 \subset A^{T_2} , \quad x_2 \equiv \sigma_2 \pmod f.$$

Continuing in this manner, we arrive at a derivation $<A,B>^{T_{k'}} \in Q$ such that

$$(x_1+x_2+\ldots+x_{k'}) + F \subset A^{T_{k'}} , \quad x_j \equiv \sigma_j \pmod f \quad (j=1,2,\ldots,k').$$

By (2), $x_1+x_2+\ldots+x_{k'} = g + nf$ for some integer n, and since $F \subset A \subset A^{T_{k'}}$, we have that

$$3)\quad F \cup (F+g+nf) \subset A^{T_{k'}} .$$

If $n = 0$, (3) implies (1) with $y = 0$ and we are done.

Assume that $n \neq 0$. Since $0 \in A^{T_{k'}} \cap B^{T_{k'}}$, we can apply Lemma 3.2.1 with $F \cup (F+g+nf)$ in place of F, and obtain a derivation $\langle A,B\rangle^{T'}$ of $\langle A,B\rangle^{T_{k'}}$ such that

$$4) \quad \{F \cup (F+g+nf)\} + B^{T'} \subset A^{T'} .$$

$\langle A,B\rangle^{T'} \in Q$ by property (d) and there exist elements $u', u' + f \in B^{T'}$ by property (b). Since $u', u' + f \in B^{T'}$, then (4) implies the following two conditions:

$$i) \quad (F+u') \cup (F+u'+g+nf) \subset A^{T'} ,$$

and

$$ii) \quad (F+u'+f) \cup (F+u'+g'(n+1)f) \subset A^{T'} .$$

If $n < 0$, we let $F' = F + u'$, and by the first part of condition (i) and the second part of condition (ii) we get the following condition that

$$iii) \quad F' \cup (F'+g+(n+1)f) \subset A^{T'} .$$

If $n > 0$, we let $F' = F + u' + f$ and by the second half of (i) and the first half of (ii) we get the following condition that

$$iv) \quad F' \cup (F'+g+(n-1)f) \subset A^{T'} .$$

Depending on whether $n < 0$ or $n > 0$ conditions (iii) and (iv) are similar to (3) with F' in place of F, T' in place of $T_{k'}$

and the coefficient of f diminished by 1 in absolute value. Repeating this procedure $|n|$ times, we arrive at a system $\langle A,B\rangle^{T^*} \in Q$, a set F^* and an integer y such that $F^* = F + y$ and

$$F^* \cup (F^*+g) \subset A^{T^*} .$$

This completes the proof of (1) and Lemma 3.3.8 as well as Theorem 3.3.7.

To show that Theorem 3.3.7 implies Theorem 3.2.5, we will show that Theorem 3.3.7 implies Theorem 3.3.9 (below) which in turn we show implies Theorem 3.2.5.

3.3.9 Theorem. Given the system $\langle A,B\rangle$ with $0 \in A \cap B$, if $\delta(C) < \delta(V)$ and if $g(B^T) = g(B) = g$ for every derivation $\langle A,B\rangle^T$ of $\langle A,B\rangle$, then $C \sim C^g$. (cf. definition 3.2.4).

The only difference between Theorem 3.3.7 and Theorem 3.3.9 is that in Theorem 3.3.7 the system $\langle A,B\rangle$ has the additional property that A contains g consecutive integers. If A contains g consecutive integers, then $C^g \sim I$ and therefore we note that Theorem 3.3.9 implies Theorem 3.3.7.

Before beginning our proof that Theorem 3.3.7 implies Theorem 3.3.9, we will devote the next several pages to defining a mapping F, which maps a union of k entire congruence classes modulo n, to a union of k entire congruence classes modulo n^*. Then we shall state and prove those relevant properties of F which we will use in proving Theorem 3.3.7 implies Theorem 3.3.9.

Let n be any natural number and let $p_o, p_1, \ldots, p_{k-1}$ be k incongruent integers modulo n. We define the set

$$P_n(p_o, p_1, \ldots, p_{k-1}) = \{p_0, p_1, \ldots p_{k-1}\}^n .$$

The reader will recall that $\{p_o, p_1, \ldots, p_k\}^n$ is the smallest set containing the integers $p_o, p_1, \ldots, p_k$ which is degenerate modulo n. (Definition 3.2.4).

Given the two sets $P_n(p_o, p_1, \ldots, p_{k-1})$, $P_{n^*}(p_o^*, p_1^*, \ldots, p_{k-1}^*)$ such that $p_o = p_o^* = 0$, we defined a mapping, F, of $P_n(p_o, p_1, \ldots, p_{k-1})$ onto $P_{n^*}(p_o^*, p_1^*, \ldots, p_{k-1}^*)$ by

$$F(p_i + tn) = p_i^* + tn^* .$$

In particular, $F(p_i) = p_i^*$ and since $p_o = p_o^* = 0$, $F(n) = n^*$ so that we may adopt, without inconsistency, the notation

$$F(x) = x^*$$

where $x \in P_n(p_o, p_1, \ldots, p_{k-1})$ and $x^* \in P_{n^*}(p_o^*, p_1^*, \ldots, p_{k-1}^*)$. If $X \subset P_n(p_o, p_1, \ldots p_{k-1})$, then $F(X) = \bigcup_{x \in X} \{F(x)\} = X^*$ so that $X^* \subset P_{n^*}(p_o^*, p_1^*, \ldots, p_{k-1}^*)$. Since F is a one to one and onto, the inverse mapping F^{-1} of $P_{n^*}(p_o^*, p_1^*, \ldots, p_{k-1}^*)$ onto $P_n(p_o, p_1, \ldots, p_{k-1})$ exists.

The mapping F has the following properties:

1) If $X \subset P_n(0)$, then $n^{-1}g(X) = (n^*)^{-1}g(X^*)$.

Proof. Since $X \subset P_n(0)$, then $X^* \subset P_{n^*}(0)$. Let $g(X) = tn$ and $g(X^*) = t'n^*$ for $t,t' \in I_0$. Since $tn^* \in X^*$, then by the definition of $t'n^*$, $t'n^* \mid tn^*$ and thus $t' \mid t$. Also since $t'n \in X$, then by the definition of tn, $tn \mid t'n$ and thus $t \mid t'$. Therefore $g(X) = tn$, $g(X^*) = tn^*$ and $n^{-1}g(X) = n^{-1}(tn) = (n^*)^{-1}(tn^*)$ $= (n^*)^{-1}g(X^*)$.

2) If a^* is defined and $x \in P_n(0)$, then $(a+x)^* = a^* + x^*$.

Proof. Let $a = p_i + tn$ for some i, $i = 0,1,\ldots,h-1$ and integer t. Since $x \in P_n(0)$, $x = t'n$ for some integer t'. So we have that

$$(a+x)^* = [p_i+(t+t')n]^* = p_i^* + (t+t')n^* = (p_i^*+tn^*) + t'n^* = a^* + x^*.$$

3) If $a,x \in P_n(p_i)$ for some i, $i=0,1,\ldots,h-1$, then $(x-a)^* = x^* - a^*$.

Proof. Let $x = p_i + tn$ for some integer t and let $a = p_i + t'n$ for some integer t'. So that

$$(x-a^*) = [(t-t')n]^* = (t-t')n^* = (p_i^*+tn^*) - (p_i^*+t'n^*) = x^* - a^*.$$

Suppose now that a system $\langle A,B\rangle$ satisfies $A \subset P_n(p_o,p_1,\ldots,p_{k-1})$ and $B \subset P_n(0)$. We consider $\langle A,B\rangle^\tau$ arising from the transformation $\tau = \tau(a_o)$, arising from Definition 2.1.2. We shall show that

$$(\langle A,B\rangle^{\tau})^* = \langle A^*,B^*\rangle^{\tau^*} \quad \text{where} \quad \tau^* = \tau(a_o^*) .$$

By property (2)

$$(A^{\tau})^* = [A \cup (a_o+B)]^* = A^* \cup (a_o+B)^* = A^* \cup (a_o^*+B^*) = (A^*)^{\tau^*},$$

and by property (3)

$$(B^{\tau})^* = [B \cap (A-a_o)]^* = B^* \cap (A-a_o)^* = B^* \cap (A^*-a_o^*) = (B^*)^{\tau^*},$$

since every element $x \in A$ satisfying $x - a_o \in B \subset P_n(0)$ must satisfy $x \in P_n(p_j)$ where j is defined by $a_o \in P_n(p_j)$.

3.3.10 <u>Lemma</u>. If $\langle A,B\rangle$ is any system such that $A \subset P_n\,(p_o,p_1,\ldots,p_{h-1})$ and $B \subset P_n(0)$, then F maps $\langle A,B\rangle^T$ onto $\langle A^*,B^*\rangle^{T^*}$ where $\langle A,B\rangle^T$ is a derivation of $\langle A,B\rangle$ and $\langle A^*,B^*\rangle^{T^*}$ is a derivation of $\langle A^*,B^*\rangle$. Also, it is clear that as T ranges over all derivations of $\langle A,B\rangle$, T^* ranges over all derivations of $\langle A^*,B^*\rangle$.

Proof. Let $T = \tau_1\tau_2\ldots\tau_k$. If $k = 1$, then the lemma is true by our preceeding discussion. Assume the lemma is true for $n = k - 1$. By our induction hypothesis we have that

$$(\langle A,B\rangle^{\tau_1\tau_2\ldots\tau_{k-1}})^* = \langle A^*,B^*\rangle^{\tau_1^*\tau_2^*\ldots\tau_{k-1}^*} .$$

We shall now show that the lemma holds when $n = k$.

$$(\langle A,B\rangle^{\tau_1\tau_2\cdots\tau_k})^* = (\langle A^{\tau_1\tau_2\cdots\tau_{k-1}}, B^{\tau_1\tau_2\cdots\tau_{k-1}}\rangle^{\tau_k})^*$$

$$= \langle (A^{\tau_1\tau_2\cdots\tau_{k-1}})^*, (B^{\tau_1\tau_2\cdots\tau_{k-1}})^*\rangle^{\tau_k^*}$$

$$= \langle A^{*\tau_1^*\tau_2^*\cdots\tau_{k-1}^*}, B^{*\tau_1^*\tau_2^*\cdots\tau_{k-1}^*}\rangle^{\tau_k^*}$$

$$= \langle A^*,B^*\rangle^{\tau_1^*\tau_2^*\cdots\tau_k^*} .$$

Since $B \subset P_n(0)$ we have by property (2) that

$$C^* = (A+B)^* = A^* + B^* ,$$

and it is clear that $V^* = A^* \vee B^*$.

3.3.11 <u>Lemma</u>. If $\langle A,B\rangle$ is any system such that $A \subset P_n(p_o,p_1,\ldots,p_{h-1})$ and $B \subset P_n(0)$, and $\langle A,B\rangle^T$ is any derivation of $\langle A,B\rangle$, then

i) $n\delta(C) = n^*\delta(C^*)$,

ii) $n\delta(V) = n^*\delta(V^*)$,

iii) $n^{-1}g(B^T) = (n^*)^{-1}g(B^{*T^*})$.

Proof of (i). If $x \in C$, then there exists an i, $i=0,1,2,\ldots,h-1$ and $t \in I$ such that $x = p_i + t_n$. Thus $\left|\frac{x}{n} - \frac{x^*}{n^*}\right| =$ $\left|\frac{p_i+t_n}{n} - \frac{p_i^*+t_n^*}{n^*}\right| = \left|\frac{p_i}{n} - \frac{p_n^*}{n^*}\right| \le \max_{0\le i\le h-1}\left|\frac{p_i}{n} - \frac{p_i^*}{n^*}\right| = k_o$. Since $\left|\frac{x}{n} - \frac{x^*}{n^*}\right| \le k_o$, for all $x \in C \cap [1,tn]$, we have that, (for suitable constants k_j), $1 \le x \le \frac{n}{n^*}x^* + k_1 \Rightarrow \frac{n^*}{n} \le x^* + k_2 \Rightarrow$

$\frac{n^*}{n} - k_2 \le x^* \Rightarrow k_3 \le x^*$. On the other hand $\frac{n}{n^*} x^* - k_1 \le x \le tn \Rightarrow$ $x^* \le tn^* + k_2$. Therefore we have that $x \in [1,tn]$ implies that $x^* \in [k_3, tn^*+k_2]$. From this we conclude that

$$C(tn) \le C^*(tn^*) + |k_3| + k_2 = C^*(tn^*) + k' .$$

Using the same argument and F^{-1} we can show that

$$C^*(tn^*) \le C(tn) + k".$$

Since $C^*(tn^*) - k" \le C(tn) \le C^*(tn^*) + k'$, we have that

$$\frac{C^*(tn)-k"}{tnn^*} \le \frac{C(tn)}{tnn^*} \le \frac{C^*(tn^*)+k'}{tnn^*} ,$$

and therefore

$$\frac{1}{n} \liminf_{t\to\infty} \frac{C^*(tn^*)-k"}{tn^*} \le \frac{1}{n^*} \liminf_{t\to\infty} \frac{C(tn)}{tn} \le \frac{1}{n} \liminf_{t\to\infty} \frac{C^*(tn^*)+k'}{tn^*} .$$

By Proposition 1.2.7 we have that $\frac{1}{n}\delta(C^*) \le \frac{1}{n^*}\delta(C) \le \frac{1}{n}\delta(C^*)$ and therefore $n\delta(C) = n^*\delta(C^*)$ follows immediately.

The proof of (ii) is similar to the proof of (i), and (iii) follows from property (1) of the mapping F and Lemma 3.3.10.

Proof that Theorem 3.3.7 implies Theorem 3.3.9.

Suppose that a given system <A,B> satisfies the hypothesis of Theorem 3.3.9. Let h be the maximum number of elements that can be chosen from A so as to be incongruent modulo g. It is possible to choose elements $p_o, p_1, \ldots, p_{h-1}$ of A so that

$$A \subset P_g(p_o, p_1, \ldots, p_{h-1}) \, ,$$

(actually $P_g(p_o, p_1, \ldots, p_{h-1}) = A^g$) and since $0 \in A$, we may take $p_o = 0$. Since $g(B^T) = g(B) = g$ (a hypothesis of Theorem 3.3.9), then $B^T \subset B \subset P_g(0)$.

We now take F to be the mapping of $P_g(p_o, p_1, \ldots, p_{h-1})$ onto $P_h(0,1,2,\ldots,h-1) = I$. The set A^* contains the h consecutive integers $0,1,2,\ldots,h-1$ and hence the system $\langle A^*, B^* \rangle$ satisfies the hypothesis of Theorem 3.3.7, with h in place of g, by Lemma 3.3.11. Therefore the conclusion of Theorem 3.3.7 holds, that is, $C^* \sim I = P_h(0,1,2,\ldots,h-1)$. On applying F^{-1} to C^* we get C and applying F^{-1} to $P_h(0,1,2,\ldots,h-1) = I$ we get $P_g(p_o, p_1, \ldots, p_{h-1}) = C^g$, since $C^g = A^g + B^g = A^g$. Now it remains for us to show that $C \sim C^g$.

Since $C^* \sim I$, then there exists an N such that $N = t_o h$ for some $t_o \in I_0$ and $C^* \cap [N,\infty) = [N,\infty)$. Let $p_j = \max\limits_{0 \le i \le h-1} p_i$. We claim that $C \cap [p_j + t_o g, \infty) = C^g \cap [p_j + t_o g, \infty)$. Since $C \subset C^g$, then $C \cap [p_j + t_o g, \infty) \subset C^g \cap [p_j + t_o g, \infty)$. Let $x \in C^g \cap [p_j + t_o g, \infty)$, thus $x = p_i + tg \ge p_j + t_o g$ and $t \ge t_o$. We have that $x^* = F(x) = i + th \ge 0 + t_o h$ and hence $x^* \in C^*$. Since the mapping F is one-to-one and onto and F maps C to C^*, then $x \in C$ and hence $C^g \cap [p_j + t_o g, \infty) \subset C \cap [p_j + t_o g, \infty)$. Therefore $C \sim C^g$ and this completes the proof that Theorem 3.3.7 implies Theorem 3.3.9.

Having shown that Theorem 3.3.7 implies Theorem 3.3.9, it remains for us to show that Theorem 3.3.9 implies Theorem 3.2.5.

Theorem 3.2.5 says that if the system <A,B> is such that $0 \in A \cap B$ and $\delta(C) < \delta(V)$, there exists a subset E, containing 0, of C and a natural number g, such that $E \sim E^g$ and $\delta(V) \geq \delta(V) - \frac{1}{g}$. It is clear from (ii), (iii) and (iv) of Theorem 2.1.4 that every derivation of <A,B> satisfies the hypothesis of Theorem 3.2.5, and if the conclusions of Theorem 3.2.5 hold for some derivation of <A,B>, they also hold for the system <A,B>.

3.3.12. <u>Theorem</u>. If each set of <A,B> contains 0, if $\delta(C) < \delta(V)$, then there exists an integer g and a derivation $\langle A,B\rangle^T$ of <A,B> with $g(B^T) = g$ such that $C^T \sim (C^T)^g$.

Proof. Let $g = \max_{\langle A,B\rangle^T} g(B^T)$, and hence there exists a derivation $\langle A,B\rangle^T$ of <A,B> with $g(B^T) = g$. By (ii), (iii) of Theorem 2.1.4 and Lemma 3.3.5, the hypotheses of Theorem 3.3.9 are satisfied by $\langle A,B\rangle^T$ and thus $C^T \sim (C^T)^g$.

Theorem 3.2.5 follows immediately from Theorem 3.3.12. If we let $g = \max_{\langle A,B\rangle^T} g(B^T)$ and $E = C^T$ where $\langle A,B\rangle^T$ is a derivation of <A,B> for which $g(B^T) = g$. By Lemma 3.3.3, $\delta(C^T) \geq \delta(V^T) - \frac{1}{g}$. By Theorem 2.1.4, $E = C^T \subset C$, $0 \in A^T \cap B^T$ and $\delta(V^T) = \delta(V)$ and this proves Theorem 3.2.5 for a particular derivation of <A,B> and by our previous remarks, Theorem 3.2.5 is also true for <A,B>.

§4. Proof of Theorem 3.1.6.

The hypothesis $0 \in A \cap B$ of Theorem 3.2.5 is necessary for the effective use of τ-transformations. However, for us to prove Theorem 3.1.6 we need a theorem similar to Theorem 3.2.5 in which the hypothesis $0 \in A \cap B$ does not necessarily hold. Before we state and prove this theorem we need the following lemma.

3.4.1 Lemma. Let E be a set. If $E \sim E^g$ and c is any integer, then $E + c \sim (E+c)^g$.

Proof. By Definition 3.2.4, $E + c \subset (E+c)^g$. For all large $x + c + mg \in (E+c)^g$, we have $x + mg \in E^g$ is large and so by hypothesis, $x + mg \in E$ and hence $x + c + mg \in E + c$. Therefore $E + c \sim (E+c)^g$.

3.4.2 Theorem. If the system $\langle A,B\rangle$ is such that $\delta(C) < \delta(V)$, there exists, corresponding to each element c of C, a subset E_c of C which contains c, and a natural number g_c, such that

$$(E_c)^{g_c} \sim E_c ,$$

and

$$\delta(E_c) \geq \delta(V) - \frac{1}{g_c} .$$

Proof. The given element c of C can be expressed in the form $c = a + b$ where $a \in A$ and $b \in B$. Let $\langle A',B'\rangle$ be the system defined by $A' = A - a$ and $B' = B - b$, so that $C' = C - c$, $0 \in A' \cap B'$ and, by Lemma 3.1.2

$$\delta(C') = \delta(C) \quad \text{and} \quad \delta(V') = \delta(V).$$

We can now apply Theorem 3.2.5 to <A',B'>, so that there exists a subset E' of C' containing 0, and a natural number $g = g_c$, such that $E' \sim (E')^{g_c}$ and $\delta(E') \geq \delta(V') - \frac{1}{g^c}$. By Lemma 3.4.1 and Proposition 1.2.4, the set $E_c = E' + c$ satisfies the requirements of Theorem 3.4.2.

Using Theorem 3.4.2 we will prove Theorem 3.4.3 (below) which in turn, we will show implies Theorem 3.1.6.

3.4.3 Theorem. If the system <A,B> satisfies $\delta(C) < \delta(V)$, there exists a natural number g such that $C \sim C^g$.

Proof. The set of numbers g_c, whose existence is established by Theorem 3.4.2, is bounded. For if they are not, then the inequality $\delta(E_c) \geq \delta(V) - \frac{1}{g_c}$ holds for arbitrarily large g_c and therefore, combined with the fact that $C \supset E_c$ for all c, implies that $\delta(C) \geq \delta(V)$, which contradicts our hypothesis.

Let g be the least common multiple of the finite set of values taken by g_c. By Theorem 3.4.2, C contains, with each element c, all integers of the form $c + mg_c$ from some point onward, and since g_c/g, C contains also all sufficiently large integers of the form $c + ng$. Therefore all large $c + ng$ in C^g are in C. Since $C \subset C^g$, we have $C \sim C^g$.

We proceed to show that Theorem 3.4.3 implies Theorem 3.1.6. We first require the following lemma.

3.4.4 Lemma. If $C = A + B$, then $C^g = A^g + B^g$.

Proof. Let $x \in C^g$, then

$$x = c + gn$$
$$= (a+b) + gn \quad \text{where} \quad a \in A, \quad b \in B$$
$$= a + (b+gn) .$$

Since $a \in A^g$ and $b + gn \in B^g$, we have $x \in A^g + B^g$ and $C^g \subset A^g + B^g$. Let $x \in A^g + B^g$ and a, b, n, n' be defined appropriately, then

$$x = (a+gn) + (b+gn')$$
$$= (a+b) + g(n+n')$$
$$= c + gm .$$

Thus $x \in C^g$, $C^g \supset A^g + B^g$ and therefore $C^g = A^g + B^g$.

We are now able to prove Theorem 3.1.6, namely, that if no system worse than $\langle A,B \rangle$ is degenerate, then $\delta(C) \geq \delta(V)$.

Proof. It will be sufficient to show that if $\delta(C) < \delta(V)$ there exists a system $\langle A',B' \rangle$ degenerate g', such that $\langle A',B' \rangle$ is worse than $\langle A,B \rangle$. By Lemma 3.4.4 and Theorem 3.4.3, the system $\langle A^g,B^g \rangle$ is degenerate modulo g and is worse than $\langle A,B \rangle$ where g is defined by Theorem 3.4.3. This completes the proof of Theorem 3.1.6.

§5. Proof of Theorem 3.1.4.

We shall begin our final section of Chapter 3 by proving Theorem 3.5.1 which is a generalization of Theorem 3.4.2. Then we shall use Theorem 3.5.1 in proving Theorem 3.1.4.

3.5.1 Theorem. If the system <A,B> is such that $\delta(C) < \delta(V)$, then there exists, corresponding to each finite subset $\{c_1,c_2,\ldots,c_n\}$ of C, a subset E of C containing $c_1,c_2,\ldots,c_n$, and a natural number g, such that

$$E^g \sim E$$

and

$$\delta(E) \geq \delta(V) - \frac{1}{g}.$$

Proof. The proof is by induction on n. If $n = 1$, the theorem is the same as Theorem 3.4.2 and is therefore true. Suppose then that $n > 1$, and assume the theorem is true for the subset $\{c_1,c_2,\ldots,c_{n-1}\}$ of C. Then by our induction hypothesis, there exists a $E_1 \subset C$ and a natural number g_1 such that $\{c_1,c_2,\ldots,c_{n-1}\} \subset E_1$, $E_1 \sim E_1^{g_1}$ and $\delta(E_1) \geq \delta(V) - \frac{1}{g_1}$. By Theorem 3.4.2, there exists a set E_2 and a natural number g_2 such that $c_n \in E_2 \subset C$, $E_2 \sim E_2^{g_2}$ and $\delta(E_2) \geq \delta(V) - \frac{1}{g_2}$. Let $E = E_1 \cup E_2$, then $\{c_1,c_2,\ldots,c_n\} \subset E \subset C$.

Case 1. If $E_1 \subset E_2^{g_2}$, we choose $g = g_2$ and we have that

$$E^g = (E_1 \cup E_2)^{g_2} = E_2^{g_2} \sim E_2 \subset E,$$

and since $E \subset E^g$ it follows that

$$E^g \sim E \quad \text{and} \quad \delta(E) \geq \delta(E_2) \geq \delta(V) - \frac{1}{g} .$$

Case 2. If $E_2 \subset E_1^{g_1}$, we choose $g = g_1$ and in the same manner we can show that

$$E^g \sim E \quad \text{and} \quad \delta(E) \geq \delta(V) - \frac{1}{g} .$$

Case 3. We assume that E_1 contains an element not in $E_2^{g_2}$ and E_2 contains an element not in $E_1^{g_1}$. Thus $E_1^{g_1} \cap E_2^{g_2}$ is a proper subset of both $E_1^{g_1}$ and $E_2^{g_2}$. The proof of Case 3 is several pages long. Let $g = \operatorname{lcm}\{g_1, g_2\}$, then

$$E \subset E^g = (E_1 \cup E_2)^g \subset (E_1^{g_1} \cup E_2^{g_2}) \sim (E_1 \cup E_2) = E$$

so that $E^g \sim E$, and all that remains to be proven is $\delta(E) \geq \delta(V) - \frac{1}{g}$.

To simplify notation we let $X = E_1^{g_1}$ and $Y = E_2^{g_2}$. In terms of X and Y we have that

i) $E \sim (X \cup Y)$,

ii) $\delta(X) \geq \delta(V) - \frac{1}{g_1}$, $\delta(Y) \geq \delta(V) - \frac{1}{g_2}$,

iii) $X \cap Y$ is a proper subset of X and Y.

Since $E \sim (X \cup Y)$, it is sufficient to prove that (ii) and (iii) imply

1) $\delta(X \cup Y) \geq \delta(V) - \frac{1}{g}$.

Let X be the union of the complete residue classes $x_1, x_2, \ldots, x_r$ (mod g_1) and Y the union of the complete residue classes $y_1, y_2, \ldots, y_s$ (mod g_2). Since $X \cap Y$ is a proper subset of X and of Y, $1 \leq r \leq g_1 - 1$, $1 \leq s \leq g_2 - 1$ and by Proposition 1.2.8,

$$\delta(X) = \frac{r}{g_1}, \quad \delta(Y) = \frac{s}{g_2}.$$

It is clear that $\delta(X \cup Y) = \delta(X) + \delta(Y) - \delta(X \cap Y)$ and if $\delta(X \cap Y) = 0$ we have, by (ii), that

$$\begin{aligned}
\delta(X \cup Y) &= \delta(X) + \delta(Y) \\
&\geq \max\left(\delta(V) - \frac{1}{g_1} + \frac{s}{g_2}, \ \delta(V) - \frac{1}{g_2} + \frac{r}{g_1}\right) \\
&\geq \delta(V) + \max\left(\frac{1}{g_2} - \frac{1}{g_1}, \frac{1}{g_1} - \frac{1}{g_2}\right) \\
&\geq \delta(V).
\end{aligned}$$

$\delta(X \cup Y) \geq \delta(V)$ implies $\delta(X \cup Y) \geq \delta(V) - \frac{1}{g}$ and we are done. We now suppose that

$$\delta(X \cap Y) > 0.$$

Define $d = \gcd\{g_1, g_2\}$ and let $g_1 = \ell_1 d$, $g_2 = m_1 d$ so that $g = \ell_1 g_2 = g_1 m_1$, where $g = \text{lcm}\{g_1, g_2\}$. Let $R_j = \{x_j + ng_1 \mid n \in I\}$ where $j = 1, 2, \ldots, r$ and $S_k = \{y_k + ng_2 \mid n \in I\}$ where $k = 1, 2, \ldots, s$. We partition both X and Y into d mutually exclusive sets in the following way:

$$X = \bigcup_{i=1}^{d} X_i \quad \text{where} \quad X_i = \bigcup_{\substack{j \\ x_j \equiv i \bmod d}} R_j \, ,$$

and

$$Y = \bigcup_{j=1}^{d} Y_j \quad \text{where} \quad Y_j = \bigcup_{\substack{k \\ y_k \equiv j \bmod d}} S_k \, .$$

Let r_i denote the number of congruence classes R_j of X in X_i and similarly let s_j denote the number of congruence classes S_k of Y in Y_j. Since $g_1 = \ell_1 d$, then $0 \le r_i \le \ell_1$ and since $g_2 = m_1 d$, then $0 \le s_j \le m_1$. If $r_i = \ell_1$ we say that X_i is full and similarly, if $s_j = m_1$ we say that Y_j is full. From elementary congruence theory, $X_i \cap Y_j$ is empty unless $i = j$, and $\delta(X_i \cap Y_i) = \frac{r_i s_i}{g}$ (a proof of these results will be found in Appendix I). Thus, since we are dealing with entire congruence classes,

$$2) \quad \delta(X \cap Y) = \sum_{i=1}^{d} \frac{r_i s_i}{g} \, ,$$

and therefore, since $\delta(X \cup Y) = \delta(X) + \delta(Y) - \delta(X \cap Y)$, $\delta(x) = \frac{r}{g_1}$ and $\delta(Y) = \frac{s}{g_2}$,

$$3) \quad \delta(X \cup Y) = \delta(X) + \frac{1}{g} \sum_{i=1}^{d} s_i(\ell_1 - r_i) = \delta(Y) + \frac{1}{g} \sum_{i=1}^{d} r_i(m_1 - s_i) \, .$$

We shall show that it is alright to assume that

iv) X_i, Y_i are not both full for any i, $1 \le i \le d$.

Suppose that $X \cap Y$ contains exactly t entire congruence classes modulo d. Let $X' = X \setminus \{ \bigcup_{\substack{i \\ r_i = \ell_1}} X_i \}$ and $Y' = Y \setminus \{ \bigcup_{\substack{j \\ s_j = m_1}} Y_j \}$. Now it is clear that $\delta(\bigcup_{\substack{i \\ r_i=\ell_1}} X_i) = \delta(\bigcup_{\substack{j \\ s_j=m_1}} Y_j) = \frac{t}{d}$ and X', Y' satisfy conditions (ii) (with $\delta(V') = \delta(V) - \frac{t}{d}$ in place of $\delta(V)$), (iii) and also (iv). Clearly, to prove (1) it is sufficient to prove that $\delta(X' \cup Y') \geq \delta(V') - \frac{1}{g}$.

Since $\delta(X \cap Y) = \sum_{i=1}^{d} \frac{r_i s_i}{g} > 0$, there exists i_o , $1 \leq i_o \leq d$ such that $r_{i_o} s_{i_o} \geq 1$, that is, $r_{i_o} \geq 1$ and $s_{i_o} \geq 1$, and by condition (iv), either

a) one of X_{i_o}, Y_{i_o} (but not both) is full,

or

b) neither X_{i_o} or Y_{i_o} is full.

Considering alternative (a) first, suppose that $r_{i_o} = \ell_1$ and $1 \leq s_{i_o} < m_1$. By (3) and condition (ii),

$$\delta(X \cup Y) \geq \delta(V) - \frac{1}{g_2} + \frac{1}{g} r_{i_o} (m_1 - s_{i_o}) \geq \delta(V) - \frac{1}{g_2} + \frac{\ell_1}{g} = \delta(V),$$

which implies inequality (1). The case when $s_{i_o} = m_1$ and $1 \leq r_{i_o} < \ell_1$ also implies inequality (1) in a similar manner.

Considering alternative (b), we have that $1 \leq r_{i_o} < \ell_1$ and $1 \leq s_{i_o} < m_1$. By (3),

$$\delta(X \cup Y) \geq \delta(V) - \frac{1}{g} + \max\left(\frac{1}{g} - \frac{1}{g_1} + \frac{s_{i_o}}{g}(\ell_1 - r_{i_o}), \frac{1}{g} - \frac{1}{g_2} + \frac{r_{i_o}}{g}(m_1 - s_{i_o})\right),$$

and inequality (1) follows if we can show that

$$4) \quad \left(\frac{1}{g} - \frac{1}{g_1} + \frac{s_{i_o}}{g}(\ell_1 - r_{i_o})\right) + \left(\frac{1}{g} - \frac{1}{g_2} + \frac{r_{i_o}}{g}(m_1 - s_{i_o})\right) \geq 0 .$$

After multiplying through by g, the left-hand side of (4) becomes

$$1 - \frac{g}{g_1} + s_{i_o}(\ell_1 - r_{i_o}) + 1 - \frac{g}{g_2} + r_{i_o}(m_1 - s_{i_o})$$

$$= s_{i_o}(\ell_1 - r_{i_o}) + r_{i_o}(m_1 - s_{i_o}) - \ell_1 - m_1 + 2$$

$$= \ell_1(s_{i_o} - 1) + m_1(r_{i_o} - 1) - 2r_{i_o}s_{i_o} + 2$$

$$\geq (r_{i_o} + 1)(s_{i_o} + 1) + (s_{i_o} + 1)(r_{i_o} - 1) - 2r_{i_o}s_{i_o} + 2$$

$$= 0$$

so that (4) is true. This completes the proof that $\delta(X \cup Y) \geq \delta(V) - \frac{1}{g}$ and of Theorem 3.5.1.

We shall use Theorem3.5.1 to prove Theorem 3.5.4 which we shall show implies Theorem 3.1.4. However, before stating and proving Theorem 3.5.4, we require the following two simple lemmas.

3.5.2 Lemma. If $A \subset I$ and g, h natural numbers, then $(A^g)^h = A^d$ where $d = \gcd\{g,h\}$.

Proof. Since $d = \gcd\{g,h\}$ then, from elementary divisibility theory, there exist integers r, s such that $d = rg + sh$. Let $x \in A^d$, then

$$x = a + dn \quad \text{where} \quad a \in A$$
$$= a + (rng + snh)$$
$$= (a + rng) + snh$$

so that $a + rng \in A^g$, $x \in (A^g)^h$ and hence $A^d \subset (A^g)^h$. Let $x \in (A^g)^h$, then

$$x = a' + hn \quad \text{where} \quad a' \in A^g$$
$$= (a + gn') + hn$$
$$= a + (gn' + hn)$$
$$= a + dn''$$

so that $x \in A^d$ which implies $(A^g)^h \subset A^d$ and thus $(A^g)^h = A^d$.

3.5.3 <u>Lemma</u>. If $A^{g_1} = A^{g_2} = \ldots = A^{g_k}$, then each set is equal to A^d where $d = \gcd\{g_1, g_2, \ldots, g_k\}$.

Proof. Proof is by induction on k. If $k = 2$, the result is true by Lemma 3.5.2 since $A^d = (A^{g_1})^{g_2} = (A^{g_2})^{g_2} = A^{g_2}$ and $A^d = (A^{g_2})^{g_1} = (A^{g_1})^{g_1} = A^{g_1}$. Suppose for $k > 2$ that each set $A^{g_1}, A^{g_2}, \ldots, A^{g_{k-1}}$ is equal to $A^{d'}$ where $d' = \gcd\{g_1, g_2, \ldots, g_{k-1}\}$. Thus $d = \gcd\{d', g_k\}$ and if $A^{d'} = A^{g_k}$, then applying the case $k = 2$, we obtain $A^{d'} = A^{g_k} = A^d$ and our proof is complete.

3.5.4 Theorem. If the system $\langle A,B\rangle$ is degenerate modulo g, then there exists a divisor g' of g such that $C^{g'} \sim C$ and

$$\delta(C^{g'}) \geq \delta(A^{g'} \vee B^{g'}) - \frac{1}{g'} .$$

Proof. Since $\langle A,B\rangle$ is degenerate modulo g, then $C = C^g$. Let g' be the least natural number such that $C = C^{g'}$, by Lemma 3.5.3, g' is a factor of g and by Lemma 3.4.4, $C^{g'} = A^{g'} + B^{g'}$. We may assume that $\delta(C^{g'}) < \delta(A^{g'} \vee B^{g'})$, otherwise there is nothing to prove.

Let $c_1, c_2, \ldots, c_n$ be a set of representatives of all the distinct residue classes (mod g') which occur in $C^{g'}$, and apply Theorem 3.5.1 to the system $\langle A^{g'}, B^{g'}\rangle$. By Theorem 3.5.1, there exists a subset E of $C^{g'}$ which contains $c_1, c_2, \ldots, c_n$, so that $E^{g'} = C^{g'}$, and a natural number $g"$, such that $E^{g"} \sim E$ and $\delta(E) \geq \delta(A^{g'} \vee B^{g'}) - \frac{1}{g"}$. Let $d = \gcd\{g', g"\}$. By Lemma 3.5.2,

$$C^d = (C^{g'})^{g"} = (E^{g'})^{g"} = (E^{g"})^{g'} = E^{g'} = C^{g'} ,$$

so that by the minimal property of g', $d = g'$. Hence $g" \geq g'$ and therefore

$$\delta(C^{g'}) = \delta(E^{g'}) \geq \delta(E) \geq \delta(A^{g'} \vee B^{g'}) - \frac{1}{g"} \geq \delta(A^{g'} \vee B^{g'}) - \frac{1}{g'} ,$$

proving Theorem 3.5.4.

We are now able to prove Theorem 3.1.4; namely, that if the system $\langle A,B\rangle$ is degenerate modulo g, there exists a divisor g' of g

and a system $\langle A',B'\rangle$, degenerate modulo g', such that $\langle A',B'\rangle$ is worse than $\langle A,B\rangle$ and $\delta(C') \geq \delta(V') - \frac{1}{g'}$.

Proof. The system $\langle A^{g'},B^{g'}\rangle$ by Theorem 3.5.4 is worse than $\langle A,B\rangle$ since $A \subset A^{g'}$; $B \subset B^{g'}$ and $C = C^{g'}$, and $\langle A^{g'},B^{g'}\rangle$ satisfies the conclusion of Theorem 3.1.4.

Thus we have proven Theorem 3.1.4, Theorem 3.1.6 and have shown that Theorem 3.1.4 implies Theorem 3.1.5 and hence have finally proven Kneser's Theorem.

Chapter 4

Conclusion

In this chapter we shall show that Kneser's result implies the earlier results concerned with finding a lower bound for the asymptotic density of the sum of two sets. In 1941, P. Erdös [3] proved,

1) if $0 \in A$, $0,1 \in B$, $\delta(B) \le \delta(A)$, $\delta(A) + \delta(B) \le 1$,

$$\text{then} \quad \delta(A+B) \ge \delta(A) + \frac{1}{2}\delta(B) .$$

By Lemma 3.1.2, the hypothesis that $0 \in A$, $0,1 \in B$ can be replaced by, "if B contains 2 consecutive integers". Then (1) can be restated to say that, if B contains 2 consecutive integers, $\delta(B) \le \delta(A)$, $\delta(A) + \delta(B) \le 1$, then $\delta(A+B) \ge \delta(A) + \frac{1}{2}\delta(B)$. This result was generalized by H. Ostmann [9] in 1949 when he proved that, if B contains m consecutive integers and $\delta(A \vee B) \le 1$, then $\delta(A+B) \ge \delta(A) + \frac{m-1}{m}\delta(B)$.

Given the system $\langle A,B \rangle$, if there does not exist a system worse than $\langle A,B \rangle$ which is degenerate, and B contains m consecutive integers, then Kneser proved that $\delta(C) \ge \delta(V) \ge \delta(A) + \delta(B)$. It is clear that $\delta(A) + \delta(B) \ge \delta(A) + \frac{m+1}{m}\delta(B)$ and, in this case, Kneser's result implies Ostmann's result.

Now assume there exists a system $\langle A',B' \rangle$ degenerate modulo g which is worse than $\langle A,B \rangle$, where B contains m consecutive integers.

By Definition 3.1.1, $B \subset B'$ and B' is the union of, say, k entire congruence classes modulo g. In this case, Kneser proved that $\delta(C) \geq \delta(A') + \delta(B') - \frac{1}{g}$. To show that Kneser's result implies Ostmann's result, we will consider the following two cases.

Case 1. Assume $g < m$.

The fact that $g < m$ implies $B' = I$. Thus $A' + B' = A' + I \sim C$ and $\delta(C) = 1$. Therefore $\delta(C) = 1 \geq \delta(A) + \delta(B) \geq \delta(A) + \frac{m-1}{m}\delta(B)$ since $\delta(A) + \delta(B) \leq 1$ by hypothesis.

Case 2. Assume that $g \geq m$.

We have that $k \geq m$ and $\delta(B') = \frac{k}{g}$ by Proposition 1.2.8. Therefore,

$$\begin{aligned}
\delta(C) &\geq \delta(A') + \delta(B') - \frac{1}{g} \\
&\geq \delta(A) + \frac{k-1}{g} \\
&= \delta(A) + \frac{k-1}{k} \cdot \frac{k}{g} \\
&\geq \delta(A) + \frac{m-1}{m}\delta(B),
\end{aligned}$$

and this completes the proof.

We conclude by giving an example of a non-degenerate system $\langle A,B\rangle$ such that there does not exist a degenerate system $\langle A',B'\rangle$ which is worse than $\langle A,B\rangle$. By Kneser, we have that $\delta(C) \geq \delta(V) \geq \delta(A) + \delta(B)$.

We partition the positive integers into the following intervals $[n!, (n+1)!-1]$ for $n = 1,2,3,\ldots$. Let $A = B = \bigcup_{n=1}^{\infty} [n!, \frac{1}{4} n!n]$ where $n!n$ is the number of integers in the interval $[n!, (n+1)!-1]$. Thus for any $k \in I_0$, $A = B$ will eventually contain k consecutive integers since the number of integers in the interval $[n!, \frac{1}{4} n!n] \to \infty$ as $n \to \infty$. Since for all $n \in I_0$, $\frac{1}{4} n \le A(n)$ and $\lim_{n\to\infty} \frac{A(n!)}{n!} = \frac{1}{4}$, we have that $\delta(A) = \delta(B) = \frac{1}{4}$.

We shall proceed to show that there does not exist a system $\langle A',B'\rangle$ degenerate modulo g which is worse than $\langle A,B\rangle$.

Assume there exists a system $\langle A',B'\rangle$ degenerate modulo g which is worse than $\langle A,B\rangle$, then $A' + B' = I$ since A and B contain g consecutive integers. For all $n > 4$, $(n+1)! - 1 \notin A$, $(n+1)! - 1 \notin B$ and $(n+1)! - 1 \notin A + B$. It is clear from the definition of A and B that $(n+1)! - \notin A$ and B. Since the largest integer belonging to A and B less than $(n+1)! - 1$ is $n! + \frac{1}{4} n!n$ and the fact that $2(n! + \frac{1}{4} n!n) < (n+1)! - 1$ shows that $(n+1)! - 1 \notin A + B$. Thus $A + B \not\sim I$, and since $\langle A',B'\rangle$ is worse than $\langle A,B\rangle$, we have

$$I = A' + B' \sim A + B \not\sim I ,$$

which is a contradiction. We therefore conclude that there does not exist a system $\langle A',B'\rangle$ degenerate modulo g which is worse than $\langle A,B\rangle$. Thus by Kneser we have that

$$\delta(C) \ge \delta(V) \ge \delta(A) + \delta(B) = \frac{1}{2} .$$

An example of a degenerate system is given in Chapter 3 page 21.

Bibliography

[1] Besicovitch, A.S., On the density of the sum of two sequences of integers, J. Lond. Math. Soc. 10 (1935) 246-248.

[2] Dyson, F., A theorem on the densities of sets of integers, J. Lond. Math. Soc. 20 (1945) 8-14.

[3] Erdos, P., On the asymptotic density of the sum of two sequences, Ann. of Math. 43 (1942) 65-68.

[4] Halberstam, H. and Roth, K.F., Sequences, Vol. 1, Oxford Univ. Press, 1966.

[5] Khintchin, A., Three pearls of number theory, Graylock Press, Rochester, N.Y. 1956.

[6] Knintchin, A., Zur additiven zahlentheorie, Mat. Sb. N.S. 39 (1932) 27-34.

[7] Kneser, M., Abschatzungen der asymptotischen dichte von summenmengen, Math. Z 58 (1953) 459-484.

[8] Mann, H.B., A proof of the fundamental theorem on the density of sums of sets of positive integers, Ann. of Math. (2) 43 (1942) 523-527.

[9] Ostmann, H., Additive zahlentheorie I,II (Ergenbnisse Series, Springer, 1956).

[10] van der Corput, J., On the sets of integers, I, II, III, Proc. Sect. Sci. K. ned. Akad. Wet. 50 (1947) 252-261, 340-350, 429-435.

Appendix I

In Chapter 3, section 5 we omitted the proof of a problem from elementary congruence theory so as not to disrupt our trend of thought in the proof of Theorem 3.5.1. Before presenting the proof, we shall restate the problem.

Let $x_1, x_2, \ldots, x_r$ be incongruent modulo g_1 and $y_1, y_2, \ldots, y_s$ be incongruent modulo g_2. Let $R_j = \{x_j + ng_1 \mid n \in I\}$ for $j = 1,2,\ldots,r$ and let $S_k = \{y_k + mg_2 \mid m \in I\}$ for $k = 1,2,\ldots,s$. We define

$$X = \bigcup_{j=1}^{r} R_j$$

and

$$Y = \bigcup_{k=1}^{s} S_k .$$

We partition both X and Y into $d = \gcd\{g_1, g_2\}$ mutually exclusive sets in the following manner:

$$X = \bigcup_{i=1}^{d} X_i \quad \text{where} \quad X_i = \bigcup_{\substack{j \\ x_j \equiv i \pmod{d}}} R_j$$

and

$$Y = \bigcup_{j=1}^{d} Y_j \quad \text{where} \quad Y_j = \bigcup_{\substack{k \\ y_k \equiv j \pmod{d}}} S_k .$$

Let r_i denote the number of congruence classes R_j of X in X_i and similarly let s_j denote the number of congruence classes S_k of Y in Y_j.

Lemma 1. If $i \neq j$, then $X_i \cap Y_j = \phi$.

Proof. Let $x \in X_i \cap Y_j$. Since $x \in X_i$, $x \equiv i \pmod d$ and since $x \in Y_j$, $x \equiv j \pmod d$ which is a contradiction since $i \neq j \pmod d$. Therefore $X_i \cap Y_j = \phi$.

We have that $X_i \cap Y_i = \bigcup_{\substack{j,k \\ x_j \equiv y_k \equiv i \pmod d}} R_j \cap S_k$. If $(j,k) \neq (j,k')$ then $(R_j \cap S_k) \cap (R_{j'} \cap S_{k'}) = \phi$ and hence $X_i \cap Y_i$ is a union of the $r_i s_i$ disjoint sets $R_i \cap S_k$. The fact that $\delta(X_i \cap Y_i) = \frac{r_i s_i}{g}$ where $g = \text{lcm}\,\{g_1, g_2\}$ follows immediately from Proposition 1.2.8 and Lemma 2 (below), since this shows that $R_j \cap S_k$ is an entire congruence class modulo g.

Lemma 2. Let $A = \{a + ng_1 \mid n \in I\}$ and $B = \{b + mg_2 \mid m \in I\}$. If $a \equiv b \pmod d$ where $d = \gcd\{g_1, g_2\}$, then there exists an integer c such that $A \cap B = \{c + ng \mid n \in I\}$ where $g = \text{lcm}\{g_1, g_2\}$.

Proof. Since $a \equiv b \pmod d$, there exists $k \in I$ such that $a = b + kd$. Thus, $A = \{b + kd + ng_1 \mid n \in I\}$ and $B = \{b + mg_2 \mid m \in I\}$. If there exists $n, m \in I$ such that $kd + ng_1 = mg_2$, then there exists an integer c such that $c \in A \cap B$. Let $\frac{g_1}{d} = \ell_1$, $\frac{g_2}{d} = m_1$ and from elementary number theory $\gcd\{\ell_1, m_1\} = 1$, and so there exists integers p, q such that $p\ell_1 + qm_1 = 1$. Thus,

$$kdpl_1 + kdqm_1 = kd$$

$$kpq_1 + kqg_2 = kd$$

$$kd + kpg_1 = -kqg_2 .$$

Letting $n = kp$, $m = -kq$ we have a solution to $kd + ng_1 = mg_2$. Therefore there exists a $c \in A \cap B$ and we have that $\{c + ng \mid n \in I\} \subset A \cap B$. (Proof. $c + ng = a + n_1g_1 + ng = a + (n_1+nm_1)g_1 \in A$ and similarly $c + ng \in B$.)

To show that $A \cap B = \{c + ng \mid n \in I\}$ it is sufficient to show that if $r,s \in A \cap B$ then $r \equiv s \pmod g$.

Assume $r,s \in A \cap B$, then

$$r = b + kd + i_1g_1 = b + j_1g_1 \quad \text{for some} \quad i_1,j_1 \in I$$

and

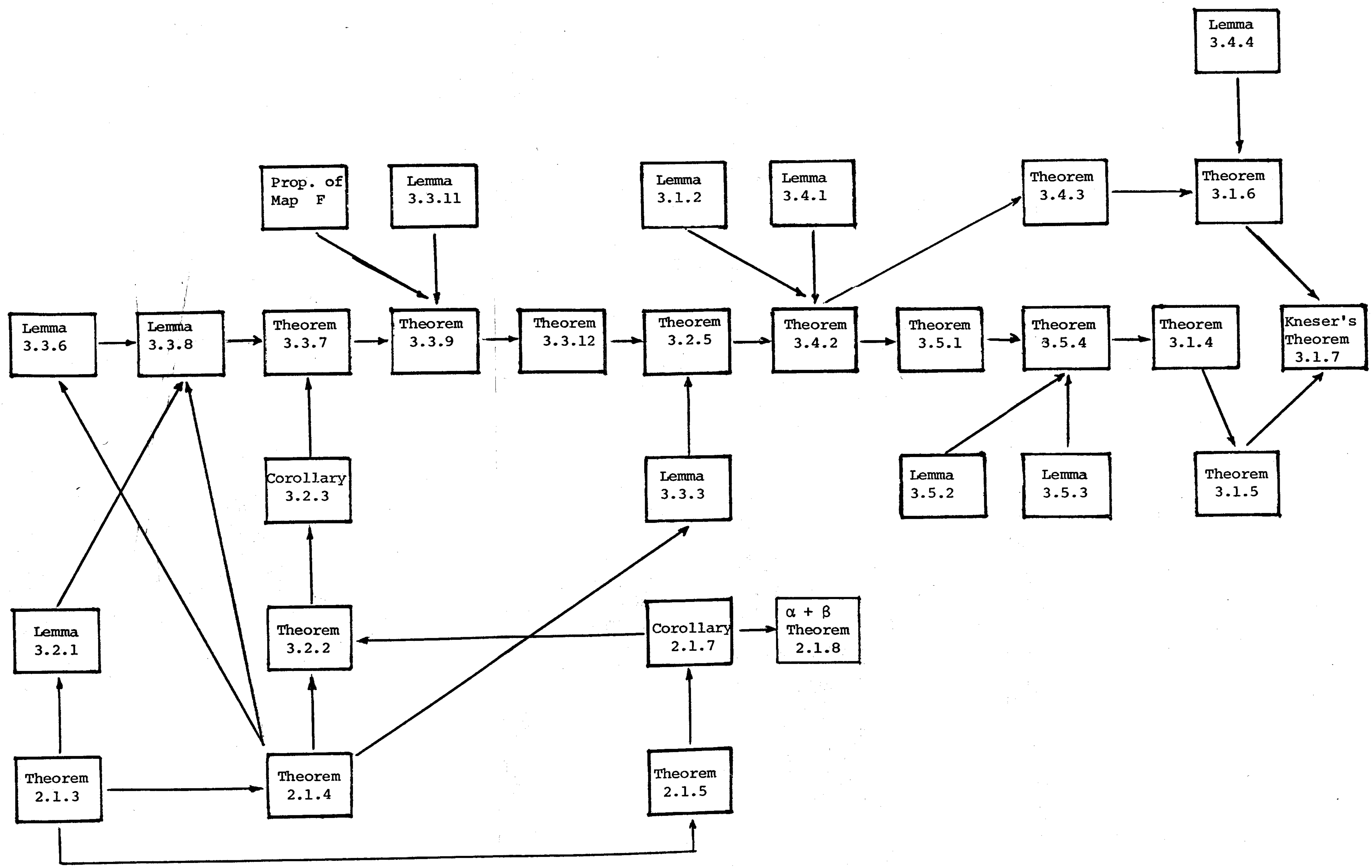
$$s = b + kd + i_2g_1 = b + j_2g_2 \quad \text{for some} \quad i_2,j_2 \in I.$$

Therefore $r - s = (i_1-i_2)g_1 = (j_1-j_2)g_2$ and so both g_1,g_2 are factors of $r - s$, whence $g = \text{lcm}\{g_1,g_2\}$ is also a factor of $r - s$. Hence $r \equiv s \pmod g$ and we are done.

Appendix II

Flowchart of Kneser's Theorem and the $\alpha + \beta$ Theorem.

1 oF


Lemma
3.4.4
Prop. of
Map F
Lemma
3.3.11
Lemma
3.1.2
Lemma
3.4.1
Theorem
3.4.3
Theorem
3.1.6
Lemma
3.3.6
Lemma
3.3.8
Theorem
3.3.7
Theorem
3.3.9
Theorem
3.3.12
Theorem
3.2.5
Theorem
3.4.2
Theorem
3.5.1
Theorem
3.5.4
Theorem
3.1.4
Kneser's
Theorem
3.1.7
Corollary
3.2.3
Lemma
3.3.3
Lemma
3.5.2
Lemma
3.5.3
Theorem
3.1.5
Lemma
3.2.1
Theorem
3.2.2
Corollary
2.1.7
α + β
Theorem
2.1.8
Theorem
2.1.3
Theorem
2.1.4
Theorem
2.1.5