Chapter 1

Introduction

Zero-sum additive theory is an area of mathematics whose oldest roots trace back to Cauchy, but which has only recently begun experiencing rapid growth and development. In this chapter we shall give proof of the some of the theorems that we are going to use in the subsequent chapters of this thesis. And we shall give the references to the theorems which we are not proving in this chapter.

1.1 The Erdős-Ginzburg-Ziv Theorem

A familiar high school problem says that given any sequence of $n$ integers $a_1, a_2, \cdots, a_n$, there exists a non-empty subsequence, which sum up to 0 (mod $n$). In other words, \exists nonempty $I \subset \{1, 2, \cdots, n\}$ such that

$$\sum_{i \in I} a_i \equiv 0 \pmod{n}. \quad (1)$$

Indeed, if one considers the sums $s_1 = a_1, s_2 = a_1 + a_2, \cdots, s_n = a_1 + \cdots + a_n$, then either some $s_i$ is 0 (mod $n$) or by Pigeon Hole Principle at least two of the $s_i$’s are equal modulo $n$.

Weighted generalization of the above problem is an interesting question. We do not take up this question in the present chapter, but shall be dealing with this problem
Chapter 1. Introduction

in the last chapter.

We [23] take up generalization of the problem in another direction, where one asks about prescribing the size of $I$ (with introducing some weights) in (1). In this particular direction, a theorem of Erdős, Ginzburg and Ziv [32] (henceforth, referred to as the EGZ theorem) says the following,

**Theorem 1.1.1 (EGZ Theorem).** For any positive integer $n$, any sequence $a_1, a_2, \ldots, a_{2n-1}$ of $2n - 1$ integers has a subsequence of $n$ elements whose sum is 0 modulo $n$.

A prototype of zero-sum theorems, the EGZ theorem continues to play a central role in the development of this area of combinatorics. In the chapter, we survey this area, give references to some related questions and try to summarize some of the recent developments including the result of C. Reiher [71]. We shall also give a proof of Rónyai’s theorem at the end of Section 1.3.

Apart from the original paper of Erdős, Ginzburg and Ziv [32], there are many proofs of the above theorem available in the literature (see [1], [11], [17], [62], for instance). We shall present two proofs of EGZ theorem in this section.

The higher dimensional analogue of the EGZ theorem, which was considered initially by Harborth [49] and Kemnitz [51] has given rise to a very active area of combinatorics today. In Section 1.2, we shall take up this theme and mention some results of Alon, Dubiner [11], [10] and Reiher [71] in this direction along with other related questions. We shall end Section 1.3 with a Rónyai’s [72] proof of $f(p, 2) \leq 4p - 2$, where $p$ is a prime number. And in Chapter 3 we shall be dealing with results in this direction (see [60]).

Finally, in Section 1.4, we briefly describe the analogous questions related to general finite groups.

**Proof of Theorem 1.1.1** We observe that the essence of the EGZ theorem lies in
the case when \( n \) is a prime. For the case \( n = 1 \), there is nothing to prove and let us assume the result is true in the case when \( n \) is a prime. Now, we proceed by induction on the number of prime factors (counted with multiplicity) of \( n \). Therefore, if \( n > 1 \) is not a prime, we write \( n = mp \), where \( p \) is prime. Since number of prime factors of \( m \) (counted with multiplicity) is less than that of \( n \), by induction hypothesis theorem holds true for \( m \). We shall use this fact later.

By our assumption, each subsequence of \( 2p-1 \) members of the sequence \( a_1, a_2, \cdots, a_{2n-1} \) has a subsequence of \( p \) elements whose sum is 0 modulo \( p \). From the original sequence we go on repeatedly omitting such subsequences of \( p \) elements having sum equal to 0 modulo \( p \). Even after \( 2m - 2 \) such sequences are omitted, we are left with \( 2pm - 1 - (2m - 2)p = 2p - 1 \) elements and so we can extract at least one more subsequence of \( p \) elements with the property that sum of its elements is equal to 0 modulo \( p \).

Thus we have found \( 2m-1 \) pairwise disjoint subsets \( I_1, I_2, \cdots, I_{2m-1} \) of \( \{1, 2, \cdots, 2mp-1\} \) with \( |I_i| = p \) and \( \sum_{j \in I_i} a_j \equiv 0 \mod p \) for each \( i \in \{1, 2, \cdots, 2m - 1\} \). We now consider the sequence \( b_1, b_2, \cdots, b_{2m-1} \) where for \( i \in \{1, 2, \cdots, 2m - 1\} \), \( b_i \) is the integer \( \frac{1}{p} \sum_{j \in I_i} a_j \).

Now as we have just observed by the induction hypothesis, this new sequence has a subsequence of \( m \) elements whose sum is divisible by \( m \). The union of the corresponding sets \( I_i \) will supply the desired subsequence of \( mp = n \) elements of the original sequence such that the sum of the elements of this subsequence is divisible by \( n \).

Let us now proceed to establish the result in the case \( n = p \), a prime. For the first proof presented here, we shall need the following result (for a proof of which, one may look into [1] or [50], for instance).

**Theorem 1.1.2** (Chevalley-Warning). Let \( f_i(x_1, x_2, \cdots, x_n), i = 1, \cdots, r \), be \( r \) polynomials in \( \mathbb{F}_q[x_1, x_2, \cdots, x_n] \) such that the sum of the degrees of these polynomials is
less than $n$ and $f_i(0,0,\cdots,0) = 0$, $i = 1, \cdots, r$. Then there exists $(\alpha_1, \alpha_2, \cdots, \alpha_n) \in \mathbb{F}_q^n$ with not all $\alpha_i$’s zero, which is a common solution to the system $f_i(x_1, x_2, \cdots, x_n) = 0$, $i = 1, \cdots, r$.

Here and in what follows, for any prime power $q$, $\mathbb{F}_q$ will denote the finite field with $q$ elements and the symbol $\mathbb{F}_q^\ast$ will denote the multiplicative group of non-zero elements of $\mathbb{F}_q$.

Now we proceed to prove Theorem 1.1.1 for the case $n = p$, a prime, which will finish the proof of Theorem 1.1.1. Given a sequence $a_1, a_2, \cdots, a_{2p-1}$ of elements of $\mathbb{F}_p$, we consider the following system of two equations in $(2p - 1)$ variables over the finite field $\mathbb{F}_p$:

\[
\sum_{i=1}^{2p-1} a_ix_i^{p-1} = 0, \\
\sum_{i=1}^{2p-1} x_i^{p-1} = 0.
\]

Since $2(p - 1) < 2p - 1$ and $x_1 = x_2 = \cdots = x_{2p-1} = 0$ is a solution, by Theorem 1.1.2 above, there is a nontrivial solution $(y_1, \cdots, y_{2p-1})$ of the above system. By Fermat’s little theorem, writing $I = \{i : y_i \neq 0\}$, from the first equation it follows that $\sum_{i \in I} a_i = 0$ and from the second equation we have $|I| = p$.

For our second proof of the ‘prime case’ of EGZ theorem, we shall need the following generalized version of Cauchy-Davenport inequality ([20], [25], can also look into [58] or [62] for instance):

**Theorem 1.1.3** (Cauchy-Davenport). Let $A_1, A_2, \cdots, A_h$ be non-empty subsets of $\mathbb{F}_p$. Then

\[
\left| \sum_{i=1}^{h} A_i \right| \geq \min \left( p, \sum_{i=1}^{h} |A_i| - h + 1 \right).
\]
Chapter 1. Introduction

(Here \( \sum_{i=1}^h A_i \) is the set consisting of all elements of \( \mathbb{F}_p \) of the form \( \sum_{i=1}^h a_i \), where \( a_i \in A_i \).)

Now, for a prime \( p \), we consider representatives modulo \( p \) in the interval \( 0 \leq a_i \leq p-1 \) for the given elements and rearranging, if necessary, we assume that

\[
0 \leq a_1 \leq a_2 \leq \cdots \leq a_{2p-1} \leq p-1.
\]

We can now assume that

\[
a_j \neq a_{j+p-1}, \quad \text{for } j = 1, \ldots, p-1.
\]

For otherwise, the \( p \) elements \( a_j, a_{j+1}, \ldots, a_{j+p-1} \) being equal, the result holds trivially.

Now, applying Theorem 1.1.3 on the sets

\[
A_i := \{a_j, a_{j+p-1}\}, \quad \text{for } j = 1, \ldots, p-1,
\]

so that

\[
\left| \sum_{j=1}^{p-1} A_i \right| \geq \min \left( p, \sum_{i=1}^{p-1} |A_i| - (p-1) + 1 \right) = p,
\]

we have

\[
-a_{2p-1} \in \sum_{j=1}^{p-1} A_i
\]

and hence once again we have established EGZ theorem for the case when \( n \) is a prime. \( \square \)

**Remark 1.1.1.** The EGZ theorem as well as many other zero-sum results can also find their place in a larger class of results in combinatorics. More precisely, a result saying that a substructure can not avoid certain regularity properties of the original structure because the ‘size’ of the substructure is ‘large’ enough, or a structure which sufficiently ‘big’ has certain unavoidable regularities, is termed as a *Ramsey-type theorem* in combinatorics.
Remark 1.1.2. Let us now observe that in Theorem 1.1.1, the number $2n - 1$ is the smallest positive integer for which the theorem holds. In other words, if $f(n)$ denotes the smallest positive integer such that given a sequence $a_1, a_2, \ldots, a_{f(n)}$ of not necessarily distinct integers, there exists a set $I \subset \{1, 2, \ldots, f(n)\}$ with $|I| = n$ such that $\sum_{i \in I} a_i \equiv 0 \pmod{n}$, then $f(n) = 2n - 1$. This can be seen as follows. From Theorem 1.1.1, it follows that $f(n) \leq 2n - 1$. On the other hand, if we take a sequence of $2n - 2$ integers such that $n - 1$ among them are 0 modulo $n$ and the remaining $n - 1$ are 1 modulo $n$, then clearly, we do not have any subsequence of $n$ elements, sum of whose elements is 0 modulo $n$. The idea we have used to prove EGZ theorem will be used many times in this thesis.

1.2 Higher dimensional analogue of EGZ theorem

As in Remark 1.1.2, for any positive integer $d$, we define $f(n, d)$ to be the smallest positive integer such that given a sequence of $f(n, d)$ number of not necessarily distinct elements of $\mathbb{Z}^d$, there exists a subsequence $x_{i_1}, x_{i_2}, \ldots, x_{i_n}$ of length $n$ such that its centroid $(x_{i_1} + x_{i_2} + \cdots + x_{i_n})/n$ also belongs to $\mathbb{Z}^d$. In other words, $f(n, d)$ is the smallest positive integer $N$ such that every sequence of $N$ elements in $(\mathbb{Z}/n\mathbb{Z})^d$ has a subsequence of $n$ elements which add up to $(0, 0, \ldots, 0)$. We observe that $f(n, 1) = f(n)$ where $f(n)$ is as defined in Remark 1.1.2.

This higher dimensional analogue was first considered by Harborth [49]; he observed the following general bounds for $f(n, d)$.

Since the number of elements of $(\mathbb{Z}/n\mathbb{Z})^d$ having coordinates 0 or 1 is $2^d$, considering a sequence where each of these elements are repeated $(n - 1)$ times, one observes that

$$1 + 2^d(n - 1) \leq f(n, d). \quad (2)$$

Again, observing that in any sequence of $1 + n^d(n - 1)$ elements of $(\mathbb{Z}/n\mathbb{Z})^d$ there will
be at least one vector appearing at least \(n\) times, we have
\[
f(n, d) \leq 1 + n^d(n - 1).
\]
(3)

For \(d = 1\), the EGZ theorem gives the exact value
\[
f(n, 1) = 2n - 1.
\]

For the case \(d = 2\) also, the lower bound in (2) is expected to give the right magnitude of \(f(n, 2)\) and this expectation, which is known as Kemnitz Conjecture in the literature, has been recently established by Reiher (see [71]). In view of (2) and (4), to establish the Kemnitz’s conjecture, it is enough to prove \(f(p, 2) = 4p - 3\), for all primes \(p\), and that is what Reiher did. We shall state Reiher’s result in the next section.

Historically, the first result in this direction was contained in the above mentioned paper of Harborth [49] where he proved that \(f(3, 2) = 9\). Kemnitz [51] established this conjecture when \(n\) is of the form \(2^e3^f5^g7^h\). However, the lower bound given in (2) is known not to be tight in general. Harborth [49] proved that \(f(3, 3) = 19\); this is strictly greater than the lower bound 17 which one obtains from (2). Different proofs of the result \(f(3, 3) = 19\) appeared since then (see [18] and [2], for instance; see also [10] for some more references in this regard). However, Harborth’s result on \(f(3, 3)\) did not rule out the possibility that for a fixed dimension \(d\), for a sufficiently large prime \(p\) the lower bound in (2) might determine the exact value for \(f(p, d)\). But a recent result of Elsholtz [31] in this direction, rules out such possibilities. We shall come back to this theme very shortly.

Another important observation made by Harborth [49] was the following:
\[
f(mn, d) \leq \min(f(n, d) + n(f(m, d) - 1), f(m, d) + m(f(n, d) - 1)).
\]
(4)

This result follows by an elementary argument of the same nature as was adopted in deriving Theorem 1.1.1 from the result in the ‘prime case’. 
Harborth [49] observed that from (2), (3) and (4), one can easily derive the exact value for $f(2^r, d)$ for any $d \geq 2$. More precisely, for $n = 2$ the lower and upper bounds for $f(2,d)$, given respectively by (2) and (3), are both $2^d + 1$ and assuming $f(2^r, d) = (2^r - 1)2^d + 1$, $f(2^s, d) = (2^s - 1)2^d + 1$ for some particular $d$, by (2) and (4), it follows that $f(2^{r+s}, d) = (2^{r+s} - 1)2^d + 1$.

However, for all odd primes $p$ and $d \geq 3$, we have a long way to go regarding the exact values for $f(p, d)$.

Coming back to the cases $d \geq 3$, the lower bound in (2) is known not to be the exact value of $f(p, d)$ for all odd primes $p$. As mentioned earlier, a particular instance of this phenomenon was observed by Harborth [49] by proving that $f(3, 3) = 19$. The following general result in this direction was proved by Elsholtz [31].

**Theorem 1.2.1.** For an odd integer $n \geq 3$, the following inequality holds:

$$f(n, d) \geq \left(\frac{9}{8}\right)^{\left\lfloor \frac{n}{4}\right\rfloor} (n - 1)2^d + 1.$$  

Thus the lower bound in (2) is not the correct value of $f(n, d)$ for $d \geq 3$.

Now, one observes that the gap is quite large between the lower and the upper bounds given respectively in (2) and (3). A very important result of Alon and Dubiner [10] says that the growth of $f(n, d)$ is linear in $n$; when $d$ is fixed and $n$ is increasing, this is much better as compared to the upper bound given by (3). More precisely, Alon and Dubiner [10] proved the following.

**Theorem 1.2.2.** There is an absolute constant $c > 0$ so that for all $n$,

$$f(n, d) \leq (cd \log_2 d)^dn.$$  

The proof of Theorem 1.2.2 due to Alon and Dubiner combines techniques from additive number theory with results about the expansion properties of Cayley graphs with
given eigenvalues. In the same paper [10] the authors conjecture that the estimate in Theorem 1.2.2 can possibly be improved. More precisely, the existence of an absolute constant $c$ is predicted such that

$$f(n, d) \leq c^d n, \text{ for all } n \text{ and } d.$$ 

1.3 The two dimensional case

As have been mentioned, with Reiher’s [71] recent proof of Kemnitz’s conjecture the problem has been solved in the two dimensional case. We go through the historical development to some extent.

In the two dimensional case, in a very significant paper [11], Alon and Dubiner proved that

**Theorem 1.3.1.** We have

$$f(n, 2) \leq 6n - 5.$$ 

One can observe that by an argument similar to the one used in the proof of Theorem 1.1.1, the inequality $f(p, 2) \leq 6p - 5$, for every prime $p$, implies $f(n, 2) \leq 6n - 5$, for every $n$. The proof of the fact that $f(p, 2) \leq 6p - 5$, as given in this paper of Alon and Dubiner, is ingenious and uses algebraic tools such as the theorem of Chevalley and Warning (Theorem 1.1.2) and the algebra of permanents. It also uses the EGZ theorem, the result in the one dimensional case. It has been indicated in [11] that the proof can be modified to yield the stronger result that $f(p, 2) \leq 5p - 2$. A relatively simple proof of a slightly weaker version of Theorem 1.3.1 is also sketched in this paper.

We now state a sharper result due to Rónyai [72].
Theorem 1.3.2. For a prime \( p \), we have

\[
f(p, 2) \leq 4p - 2.
\]

Remark 1.3.1. As we have mentioned before, from the inequality \( f(p, 2) \leq 6p - 5 \), for every prime \( p \), by an argument similar to the one used in the proof of Theorem 1.1.1, one gets the result \( f(n, 2) \leq 6n - 5 \), for every \( n \). Such would be the case for the bound \( f(n, 2) \leq 4n - 3 \) of Kemnitz’s conjecture. However, this argument does not go through for the bound given by the above theorem. But, as mentioned in Rónyai [72], it is not difficult to observe that Theorem 1.3.2 along with (4) implies that

\[
f(n, 2) \leq \frac{41}{10} n.
\]

Since Kemnitz proved \( f(n, 2) = 4n - 3 \), whenever \( n \) is of the form \( 2^e 3^f 5^g 7^h \), and \( 4n - 3 \leq \frac{41}{10} n \). So \( f(n, 2) \leq \frac{41}{10} n \) for all positive integers \( n \) which does not have a prime factor greater than 7.

Indeed, if we write \( n = mp \), where \( p \geq 11 \) is a prime and assume \( f(m, 2) \leq \frac{41}{10} m \), then using \( f(p, 2) \leq 4p - 2 \) and (4), we get

\[
f(mp, 2) \leq (f(p, 2) - 1)m + f(m, 2) \leq (4p - 3)m + \frac{41}{10} m \leq \frac{41}{10} m + 4mp \leq \frac{mp}{10} + 4mp = \frac{41}{10} n.
\]

Gao [34] obtained the following generalization of the result (Theorem 1.3.2) of Rónyai [72] mentioned before.

Theorem 1.3.3. For an odd prime \( p \) and a positive integer \( r \), we have

\[
f(p^r, 2) \leq 4p^r - 2.
\]

Following Gao [34], we now sketch a proof of Theorem 1.3.3. We note that this proof proceeds along a line which is quite different from the proof of Theorem 1.3.2 as given by Rónyai [72].
The proof uses the following special case of a very elegant result of Olson [64]. Apart from being interesting in its own right, it has several important results as its immediate corollaries.

**Lemma 1.3.4 (Olson).** For a prime \( p \), let \( s_1, s_2, \ldots, s_k \) be a sequence \( S \) of elements of \( (\mathbb{Z}/p^r\mathbb{Z})^d \) such that \( k \geq 1 + d(p^r - 1) \). Then, writing \( f_e(S) \) for the number of subsequences of even length of \( S \) which sum up to zero and \( f_o(S) \) for the number of subsequences of odd length which sum up to zero, we have

\[
f_e(S) - f_o(S) \equiv -1 \pmod{p}.
\]

First we note the following two corollaries to Lemma 1.3.4; these will be used to prove Theorem 1.3.3. Later we shall remark about few more consequences of the above lemma of Olson.

**Lemma 1.3.5.** If \( S \) is a zero-sum sequence of \( 3p^r \) elements in \( (\mathbb{Z}/p^r\mathbb{Z})^2 \), then \( S \) contains a zero-sum subsequence of length \( p^r \).

For any sequence \( S \) of elements of \( (\mathbb{Z}/p^r\mathbb{Z})^2 \), if \( r(S) \) denotes the number of zero-sum subsequences \( W \) of \( S \) with \( |W| = 2p^r \), one has the following.

**Lemma 1.3.6.** Let \( T \) be a sequence of elements of \( (\mathbb{Z}/p^r\mathbb{Z})^2 \) with \( 3p^r - 2 \leq |T| \leq 4p^r - 1 \). Suppose that \( T \) contains no zero-sum subsequence of length \( p^r \). Then

\[
r(T) \equiv -1 \pmod{p}.
\]

Both the above lemmas follow easily from Lemma 1.3.4 by appending 1 as the third coordinate to each of the elements in \( S \) and \( T \) respectively. For instance, if \( S \) in Lemma 1.3.5 is \( (a_1, b_1), (a_2, b_2), \ldots, (a_m, b_m) \), where \( m = 3p^r \), one considers the sequence
$S' = (a_1, b_1, 1), (a_2, b_2, 1), \cdots, (a_l, b_l, 1)$ with $l = 3p^r - 2$. Now, by Lemma 1.3.4, $S'$ and hence $S_1 = (a_1, b_1), (a_2, b_2), \cdots, (a_l, b_l)$ must have a zero-sum subsequence, length of which must be $p^r$ or $2p^r$. If there is a zero-sum subsequence $S_2$ of $S_1$ of length $2p^r$, then its complement in $S$ provides us with one such with length $p^r$. Hence Lemma 1.3.5 follows. Let $T'$ be the sequence corresponding to $T$ with the length same as that of $T$. Since $T$ does not have a zero sum subsequence of length $p^r$, by Lemma 1.3.5 it does not have a zero sum subsequence of length $3p^r$. So $f_e(T') - f_o(T') = r(T') = r(T)$. Therefore, by Lemma 1.3.4, we get Lemma 1.3.6.

**Proof of Theorem 1.3.3.** If possible, suppose that there is a sequence $S$ of elements of $(\mathbb{Z}/p^r\mathbb{Z})^2$ such that $S$ is of length $4p^r - 2$ and $S$ has no zero-sum subsequence of length $p^r$.

By Lemma 1.3.6,

$$r(T) \equiv -1 \pmod{p},$$

for every subsequence $T$ of $S$ with $|T| \geq 3p^r - 2$.

We have

$$\sum_{T \subset S, \ |T| = 3p^r - 2} r(T) = \binom{4p^r - 2 - 2p^r}{3p^r - 2 - 2p^r} r(S).$$

Hence

$$\sum_{T \subset S, \ |T| = 3p^r - 2} (-1) \equiv \binom{2p^r - 2}{p^r - 2} (-1) \pmod{p}.$$

Thus

$$\binom{4p^r - 2}{3p^r - 2} \equiv \binom{2p^r - 2}{p^r - 2} \pmod{p},$$

which would imply that

$$3 \equiv \binom{4p^r - 2}{3p^r - 2} \equiv \binom{2p^r - 2}{p^r - 2} \equiv 1 \pmod{p}$$

- a contradiction. \(\Box\)

**Remark 1.3.2.** As was observed by Alon and Dubiner [11], the EGZ theorem follows almost immediately from Lemma 1.3.4. More precisely, for any prime $p$, given any
sequence $a_1, a_2, \cdots, a_{2p-1}$ of elements of $(\mathbb{Z}/p\mathbb{Z})$, we just consider the sequence

$$(a_1, 1), (a_2, 1), \cdots, (a_{2p-1}, 1)$$

in $(\mathbb{Z}/p\mathbb{Z})^2$.

**Remark 1.3.3.** Regarding implications of Lemma 1.3.4 we must mention that in the original paper of Olson [64], the lemma was used to find the value of Davenport’s constant $D(G)$ for a finite abelian $p$-group $G$. For any finite abelian group $G$, the important combinatorial invariant *Davenport’s constant* $D(G)$ is defined to be the smallest positive integer $s$ such that for any sequence $g_1, g_2, \cdots, g_s$ of (not necessarily distinct) elements of $G$, there is a nonempty $I \subset \{1, \cdots, s\}$ such that $\sum_{i \in I} g_i = 0$. For relations between Kemnitz’s conjecture and a conjecture involving the Davenport’s constant and some other conjectures related to zero-sum problems, one may look into some papers of Thangadurai [77] and Gao and Geroldinger [40]. In Section 1.4, we shall have an occasion to state an important relation (due to Gao [35]) between the Davenport’s constant and another constant emerging out from a natural generalization of the EGZ theorem for finite abelian groups.

**Theorem 1.3.7** (Reiher). For an odd prime $p$, we have

$$f(p, 2) = 4p - 3.$$ 

We now consider a generalization of $f(n, d)$ as defined in the beginning of Section 1.2. Let $f_r(n, d)$ denote the smallest positive integer such that given any sequence of $f_r(n, d)$ elements in $(\mathbb{Z}/n\mathbb{Z})^d$, there exists a subsequence of $(rn)$ elements whose sum is zero in $(\mathbb{Z}/n\mathbb{Z})^d$. Thus $f_1(n, d) = f(n, d)$.

As has been mentioned in a paper of Gao and Thangadurai [43], one can derive (as in [40]) that

$$f_r(n, 2) = (r + 2)n - 2, \text{ for integers } r \geq 2 \quad (5)$$
from the known results about the Davenport’s constant for finite abelian $p$-groups and by using Reiher’s result on the exact value of $f_1(n, 2)$. Indeed we shall use following result of Gao [34] and Reiher’s Theorem [71] to conclude (5).

**Theorem 1.3.8.** Let $q$ be a prime power. Then we have $f(q, 2) \leq 4q - 2$ and $f_2(q, 2) \leq 4q - 2$.

Exact values of $f_r(n, 1)$ for $r \geq 1$ can be easily obtained from the EGZ theorem. We shall be dealing with case $r = 1$ in Chapter 3 (See [60]).

As had been mentioned in the introduction, we shall conclude this section with a sketch of Rónyai’s recent proof of Kemnitz’s conjecture. We mention that some interesting partial results towards the conjecture of Kemnitz and some related results had been obtained by Gao [41], Thangadurai [76] and Sury and Thangadurai [74]. We shall need following lemma before giving the proof of Rónyai’s theorem [72] (see also [1]).

**Lemma 1.3.9.** Let $F$ be a field and $m$ a positive integer. Then the (multilinear) monomials $\prod_{i \in I} x_i$, $I \subset \{1, 2, \cdots, m\}$ constitute a basis of the $F$-linear space of all functions from $\{0, 1\}^m$ to $F$ (Here 0 and 1 are viewed as elements of $F$).

**Proof.** The monomials $\prod_{i \in I} x_i$, $I \subset \{1, 2, \cdots, m\}$ span a linear space of dimension $2^m$ over $F$. This is also the dimension of the space of functions from $\{0, 1\}^m$ to $F$, therefore it suffices to verify that every function from the latter set can be expressed as an $F$-linear combination of the monomials $\prod_{i \in I} x_i$. The space of functions is clearly spanned by the characteristic functions $\chi_u$, $u \in \{0, 1\}^m$, where $\chi_u(u) = 1$ and $\chi_u(v) = 0$ if $v \neq u$, hence it is enough to establish the required representation for characteristic functions. Write $u = (u_1, u_2, \cdots, u_m)$ and let $U \subset \{1, 2, \cdots, m\}$ be the set of coordinate positions $j$ where $u_j = 1$ and $U'$ be the set of indices $j$ with $u_j = 0$.

Then we have

$$\chi_u(x_1, x_2, \cdots, x_m) = \prod_{i \in U} x_i \prod_{i \in U'} (1 - x_i)$$
as functions on \( \{0, 1\}^m \). By expanding the right hand side we obtain an expression of the desired form. This proves the lemma.

Now, we shall give the proof of the Rónyai’s theorem.

**Proof of Theorem 1.3.2.** The assertion is obvious for \( p = 2 \), hence we may assume that \( p \) is an odd prime. Put \( m = 4p - 2 \).

Let

\[
v_1 = (a_1, b_1), v_2 = (a_2, b_2), \ldots, v_m = (a_m, b_m)
\]

be a sequence of terms from \( \mathbb{Z}_p \oplus \mathbb{Z}_p \). We have to prove that there exists an \( I \subset \{1, 2, \ldots, m\} \), \( |I| = p \) such that \( \sum_{i \in I} v_i = (0, 0) \).

Let \( \sigma(x_1, x_2, \ldots, x_m) := \sum_{I \subset \{1, 2, \ldots, m\}, |I| = p} \prod_{i \in I} x_i \) denote the \( p \)-th elementary symmetric polynomial of the variable \( x_1, x_2, \ldots, x_m \). By Lemma 1.3.5 it is enough to prove that there is a subset \( J \) of \( \{1, 2, \ldots, m\} \), with \( |J| = p \) or \( |J| = 3p \) such that \( \sum_{i \in J} v_i = (0, 0) \).

Assume on the contrary that, there does not exist such \( J \). Consider the polynomial \( P \) over the prime field \( \mathbb{F}_p \),

\[
P := \left( \left( \sum_{i=1}^{m} a_i x_i \right)^{p-1} - 1 \right) \left( \left( \sum_{i=1}^{m} b_i x_i \right)^{p-1} - 1 \right) \left( \left( \sum_{i=1}^{m} x_i \right)^{p-1} - 1 \right) A,
\]

where \( A = (\sigma(x_1, x_2, \ldots, x_m) - 2) \). We claim that \( P \) vanishes on all vectors \( u \in \{0, 1\}^m \), except on the all 0 vector \( \mathbf{0} \), where \( P(\mathbf{0}) = 2 \). Indeed, the third factor vanishes on \( u \) unless it has Hamming weight (the number of ones) multiple of \( p \). If the Hamming weight of \( u \) is \( 2p \) then one can easily see that, \( \sigma(u) = \binom{2p}{p} = 2 \) in \( \mathbb{F}_p \), hence the last factor vanishes on \( u \). Finally if the Hamming weight of \( u \) is \( p \) or \( 3p \) then

\[
\left( \left( \sum_{i=1}^{m} a_i x_i \right)^{p-1} - 1 \right) \left( \left( \sum_{i=1}^{m} b_i x_i \right)^{p-1} - 1 \right)
\]

is 0 on \( u \) by the indirect hypothesis. We obtained that \( P = 2\chi_0 \) as function on \( \{0, 1\}^m \).

Note also that \( \deg P \leq 3(p-1) + p = 4p - 3 \). Now, reduce \( P \) into a linear combination of multilinear monomials by using the relations \( x_i^2 = x_i \) (which are valid on \( \{0, 1\}^m \))
and let $Q$ denote the resulting expression. Clearly, we have $Q = 2\chi_0$ as a function on $\{0,1\}^m$ and $\deg Q \leq 4p - 3$, because reduction can not increase the degree. But this is in contradiction with the uniqueness part of Lemma 1.3.9, form the multilinear representative of $2\chi_0 = 2(1 - x_1)(1 - x_2)\cdots(1 - x_m)$ has degree $m = 4p - 2$. Hence theorem is proved. 

\section*{1.4 EGZ theorem for finite groups}

It is not difficult to see that following the method employed in deriving Theorem 1.1.1 from the ‘prime case’, and appealing to the structure theorem for finite abelian groups, one can derive Theorem 1.4.1 from the EGZ theorem.

**Theorem 1.4.1.** Let $G$ be an abelian group of order $n$. Then given any sequence $g_1, g_2, \cdots, g_{2n-1}$ of $2n - 1$ elements of $G$, there exists a subsequence of $n$ elements whose sum is the identity element $0$ of $G$.

We note that for the cyclic group of order $n$, $2n - 1$ is the smallest number satisfying the above property. That is, if for any abelian group $G$ of order $n$, if $ZS(G)$ is the smallest integer $t$ such that for any sequence of $t$ elements of $G$, there exists a subsequence of $n$ elements whose sum is the identity element $0$ of $G$, then we have

$$ZS(\mathbb{Z}/n\mathbb{Z}) = 2n - 1.$$ 

Sometimes the notation $E(G)$ is also used instead of $ZS(G)$ in the literature. By Theorem 1.4.1, $ZS(G) \leq 2n - 1$, for any abelian group $G$ of order $n$. However, for a non-cyclic abelian group $G$ of order $n$, $ZS(G)$ need not be equal to $2n - 1$. In this direction, a result of Alon, Bialostocki and Caro \cite{9} says that for a non-cyclic abelian group $G$ of order $n$, $ZS(G) \leq \frac{3n}{2}$ and the bound $\frac{3n}{2}$ is realized only by groups of the form $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$. Subsequently, Caro \cite{19} showed that if a non-cyclic abelian group $G$ of order $n$ is not of the form $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$, then $ZS(G) \leq \frac{4n}{3} + 1$ and this
Chapter 1. Introduction

Bound is realized only by groups of the form \( \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z} \). Further generalization of the same nature have been obtained by Ordaz and Quiroz [68] rather recently stating that apart from the groups \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} \) and \( \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z} \) which appear in the last statement, for any non-cyclic abelian group \( G \) of order \( n \), \( ZS(G) \leq \frac{5n}{4} + 2 \) and equality holds only for groups of the form \( \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4m\mathbb{Z} \). Further generalization of these results describing the situation with abelian groups \( G \) having smaller values of \( ZS(G) \) may involve groups other than \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} \), \( \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z} \), \( \ldots \), \( \mathbb{Z}/r\mathbb{Z} \oplus \mathbb{Z}/rm\mathbb{Z} \), for positive integers \( r \). One should mention that the method of Ordaz and Quiroz [68] involves obtaining an upper bound for the Davenport’s constant \( D(G) \) (as defined in Remark 1.3.3) of the relevant groups \( G \) and using the following beautiful result of Gao [35] which links \( ZS(G) \) with \( D(G) \).

**Theorem 1.4.2.** If \( G \) is a finite abelian group of order \( n \), then \( ZS(G) = D(G) + n - 1 \).

One would also like to know the validity of the statement of Theorem 1.4.1 for general finite groups.

For a finite solvable group \( G \), by induction on the length \( k \) of a minimal abelian tower \( (0) = G_k \subset G_{k-1} \subset \cdots \subset G_0 = G \) and using the result in Theorem 1.4.1, one can easily derive (see [67],[73], for instance) the following result employing the same argument as employed in the proof of Theorem 1.1.1 in deriving the general case from the ‘prime case’.

**Theorem 1.4.3.** Let \( G \) be a finite solvable group (written additively) of order \( n \). Then given any sequence \( g_1, g_2, \ldots, g_{2n-1} \) of \( 2n - 1 \) elements of \( G \), there exist \( n \) distinct indices \( i_1, \ldots, i_n \) such that

\[
g_{i_1} + g_{i_2} + \cdots + g_{i_n} = 0.
\]

The above result holds without the assumption that the group \( G \) is solvable. This follows from the following general result of Olson [66].
Theorem 1.4.4. Let $G$ be a finite group (written additively) of order $n > 1$. Let $S$ be a sequence $g_1, g_2, \cdots, g_{2n-1}$ of elements of $G$ in which no element appears more than $n$ times. Then $G$ has a subgroup $K$ of order $k > 1$ and $S$ has a subsequence $T = a_1, \cdots, a_{n+k-1}$ such that

i) $K$ is a normal subgroup of the subgroup $H$ of $G$ generated by the elements $\{a_1, a_2, \cdots, a_{n+k-1}\}$,

ii) there exists an $a \in H$ such that $a_i \in a + K = K + a$ for $1 \leq i \leq n + k - 1$, and

iii) $K$ is the set of all sums $a_{i_1} + \cdots + a_{i_n}$ where $i_1, \cdots, i_n$ are $n$ distinct indices (in any order) in $\{1, \cdots, n + k - 1\}$.

We note that for a non-abelian group $G$ of order $n$, given a sequence of $2n-1$ elements of $G$, we are not ensured that there is a subsequence of $n$ elements which adds up to the identity, rather a permutation of a subsequence of length $n$ will do so. However, it is conjectured [66] that there must be a subsequence of $n$ elements which adds up to the identity. This is not known even for solvable groups.

1.5 Kneser’s Addition Theorem

A beautiful theorem of Kneser is about sums of finite subsets of an abelian group $G$. We need the following definitions to state the theorem.

For a non-empty subset $A$ of an abelian group $G$. The stabilizer of $A$, denoted by $Stab(A)$, is defined as the following set,

$$Stab(A) = \{x \in G : x + A = A\}.$$

One can easily see that $0 \in Stab(A)$ and $Stab(A)$ is a subgroup of $G$. Moreover, $Stab(A)$ is a largest subgroup of $G$ such that,

$$Stab(A) + A = A.$$

In particular, $Stab(A) = G$ if and only if $A = G$. An element $g \in Stab(A)$ is called a period of $A$, and $A$ is called a periodic set if $Stab(A) \neq \{0\}$ and $A$ is called an aperiodic
set if $\text{Stab}(A) = 0$. For example, if $A$ is an infinite arithmetic progression in $\mathbb{Z}$ with
difference $d$, then $\text{Stab}(A) = d\mathbb{Z}$.

Kneser proved that if $A$ and $B$ are non-empty, finite subsets of an abelian group $G$,
then either $|A + B| \geq |A| + |B|$ or

$$|A + B| = |A + H| + |B + H| - |H|,$$

where $H = \text{Stab}(A + B)$ is the stabilizer of $A + B$.

Note that, if $\phi : G \to G/H$ is the natural group homomorphism, where $H = \text{Stab}(A)$,
then $\text{Stab}(\phi(A)) = \{H\} \subset G/H$. In other words, $\phi(A)$ is an aperiodic subset of $G/H$.

Next, we shall state Kneser’s Theorem.

**Theorem 1.5.1** (Kneser’s Addition Theorem). Let $G$ be an abelian group, and let $A$
and $B$ be finite, non-empty subsets of $G$. Let $H = \text{Stab}(A + B)$. Then

$$|A + B| \geq |A + H| + |B + H| - |H|.$$

Following theorem is a consequence of the above theorem, which is also referred as
Kneser’s Addition Theorem sometimes.

**Theorem 1.5.2.** Let $G$ be an abelian group, and let $A_1, A_2, \ldots, A_k$
be $k$ finite, non-empty subsets of $G$. Let $H = \text{Stab}(A_1 + A_2 + \cdots + A_k)$. Then

$$|A_1 + A_2 + \cdots + A_k| \geq |A_1 + H| + |A_2 + H| + \cdots + |A_k + H| - (k - 1)|H|.$$

**Theorem 1.5.3** (I. Chowla). Let $m \geq 2$, and let $A$ and $B$ be non-empty subsets of
$\mathbb{Z}/m\mathbb{Z}$. If $0 \in B$ and $\gcd(b, m) = 1$ for all $b \in B \setminus \{0\}$, then

$$|A + B| \geq \min(m, |A| + |B| - 1).$$

In the special case when $G$ is a finite cyclic group, Kneser’s theorem implies the theo-
rems of Cauchy-Davenport (Theorem 1.1.3) and I. Chowla (Theorem 1.5.3). Theorem
1.5.3 follows from Kneser’s theorem in following way,
Let $A$ and $B$ be non-empty subsets of $\mathbb{Z}/m\mathbb{Z}$ such that $0 \in B$ and $\gcd(n, m) = 1$, for any $n \in B \setminus \{0\}$. If $A + B = \mathbb{Z}/m\mathbb{Z}$, then we are through. Suppose $A + B \neq \mathbb{Z}/m\mathbb{Z}$. Kneser’s Theorem implies $|A + B| \geq |A + H| + |B + H| - |H|$, where $H = \text{Stab}(A + B)$. Since $\gcd(n, m) = 1$, for any $n \in B \setminus \{0\}$, $H \neq n + H$. Therefore $|B + H| = |B' + H| + |H|$, where $B' = B \setminus \{0\}$. So $|A + B| \geq |A + H| + |B' + H| \geq |A| + |B'| = |A| + |B| - 1$. So we have Chowla’s theorem. Clearly Cauchy-Davenport theorem (Theorem 1.1.3) follows from Chowla’s theorem.

1.6 Weighted EGZ Theorem

If $n$ is a positive integer, we will identify $\mathbb{Z}_n$ with the set of integers $\{0, 1, 2, \cdots, n-1\}$. Adhikari et. al. [3, 7, 4, 5] generalized well known constants $\text{ZS}(G)$ and $\text{D}(G)$ to $\text{E}_A(G)$ and $\text{D}_A(G)$ respectively. Sometimes the notation $\text{E}(G)$ is used instead of $\text{ZS}(G)$, in literature. Let $G$ be an additive finite abelian group of order $n$ with additive identity 0. Let $A$ be a non-empty subset of integers. The weighted EGZ constant, denoted by $\text{E}_A(G)$, is defined as the least $t \in \mathbb{N}$ such that for every sequences $x_1, x_2, \cdots, x_t$ of elements of $G$, there exist indices $j_1, j_2, \cdots, j_n \in \mathbb{N}$, $1 \leq j_1 < j_2 < \cdots < j_n \leq t$ and $(a_1, a_2, \cdots, a_n) \in A^n$ with $\sum_{i=1}^{n} a_i x_{j_i} = 0$. And the weighted Davenport’s constant $\text{D}_A(G)$, is defined as the least $t \in \mathbb{N}$ such that for all sequences $x_1, x_2, \cdots, x_t$ of elements of $G$, there exist indices $j_1, j_2, \cdots, j_k \in \mathbb{N}$, $1 \leq j_1 < j_2 < \cdots < j_k \leq t$ and $(a_1, a_2, \cdots, a_k) \in A^k$ with $\sum_{i=1}^{k} a_i x_{j_i} = 0$. For obvious reasons we take $A \subset \{1, 2, \cdots, \exp(G) - 1\}$. When $G$ is a cyclic group $\mathbb{Z}_n$, we denote $\text{E}_A(G)$ and $\text{D}_A(G)$ by $\text{E}_A(n)$ and $\text{D}_A(n)$ respectively.

For several sets $A \subset \mathbb{Z}_n \setminus \{0\}$ of weights, exact value of $\text{E}_A(n)$ and $\text{D}_A(n)$ have been determined (see [4, 5, 7]. The case $A = \{1\}$ is covered by the well known EGZ theorem. In [23] we shall be extending the results of [5]. And in [22] we shall be giving an upper bound on the Davenport constant $\text{D}(G)$. The case $A = \{\pm 1\} = \{1, -1\}$ was done in [4], where it has been shown that, $\text{E}_A(n) = n + \lfloor \log_2 n \rfloor$. Moreover, by the
Chapter 1. Introduction

pigeonhole principle one can easily see, \( D_A(n) \leq \lceil \log_2 n \rceil + 1 \) (See [4]). And by considering the sequence 1, 2, 2^2, \cdots, 2^r, where \( r \) is defined by \( 2^{r+1} \leq n < 2^{r+2} \), it follows that, \( D_A(n) \geq \lfloor \log_2 n \rfloor + 1 \). Hence, \( D_A(n) = \lfloor \log_2 n \rfloor + 1 \). It has also been observed in [4] that for \( A = \{1, 2, 3, \cdots, n-1\} \), we have \( E_A(n) = n + 1 \). In this case it is very clear that, \( D_A(n) = 2 \). So for \( A = \{1, 2, 3, \cdots, n-1\} \) and \( A = \{\pm 1\} \) we have \( E_A(n) = D_A(n) + n - 1 \). In [4] it has been conjectured that \( E_A(n) = n + \Omega(n) \), where \( A = \{a \in \{1, 2, 3, \cdots, n-1\} : \gcd(a, n) = 1\} \) and \( \Omega(n) \) is the number of prime factors of \( n \), counted with multiplicity. This conjecture was independently established by F. Luca [55] and S. Griffiths [47]. It has been expected by Adhikari and conjectured by R. Thangadurai [75] that, \( E_A(G) = D_A(G) + |G| - 1 \). This conjecture has been established recently by Grynkiewicz, Marchan and Ordaz [48]. Before this the following partial results had been obtained by Adhikari and Chen [3], Yuan and Zeng [79].

**Theorem 1.6.1** (Adhikari, Chen). Let \( G \) be a finite abelian group of order \( n \) and \( A = \{a_1, a_2, \cdots, a_r\} \) be a non-empty subset of \( \mathbb{Z} \) and \( r \geq 2 \). If \( \gcd(a_2 - a_1, a_3 - a_1, \cdots, a_r - a_1, n) = 1 \), then \( E_A(G) = D_A(G) + n - 1 \).

**Theorem 1.6.2** (Yuan, Zeng). Let \( A \) be any non-empty subset of \( \mathbb{Z} \). Then \( E_A(n) = D_A(n) + n - 1 \).

Now we give the plan of the remaining chapters. In Chapter 2 we shall be giving an upper bound on a Davenport constant of a finite abelian group of rank \( r \). In Chapter 3 we shall give a conditional result in the direction of higher dimensional analogue of Erdős-Ginzburg-Ziv Theorem. In Chapter 4 we shall be giving an upper bound on weighted Erdős-Ginzburg-Ziv constant for one particular weight, \( A = \{\pm 1\} \).