Combinatorial Number Theory

the roots of unity in $K$, then by (2.8.b)

by the above, they all have the same

in $\mathcal{O}$ consists of $z \in (\mathbb{R}^s \times \mathbb{C}^t)^*$ such that

$< N(z) < 1$

$l(z) = \sum_{k=1}^{s+t} \xi_k l_k$

Restriction of automorphisms gives rise

$Gal(L/\mathbb{Q}[k]) \cong Gal(\mathbb{Q}[k])$
Contents

1 Basics and Cardinality Inequalities 1
2 Structure of Sets with Few Sums 9
3 Location and Sumsets 15
4 Density 21
5 Measure and Topology 27
Chapter 1

Basics and Cardinality Inequalities

**Definition 1.0.1.** Let $A$ and $B$ be sets in a (mostly commutative) group. We call the group operation addition and use additive notation. The **sumset** of these sets is

$$A + B = \{a + b : a \in A, b \in B\}.$$  

Similarly, the **difference set**

$$A - B = \{a - b : a \in A, b \in B\} = \{a + (-b)\}.$$

For repeated addition we write

$$kA = A + \cdots + A, \ k \text{ times;}$$

in particular, $1A = A$, $0A = \{0\}$. Also, $k \cdot A = \{ka : a \in A\}$.

**Theorem 1.0.2.** (Trivial sumset estimates) Let $A, B$ be additive sets with common ambient group $\mathbb{Z}$, and let $x \in \mathbb{Z}$. Then we have the identities $|A + x| = |-A| = |A|$, the inequalities

$$\max(|A|, |B|) \leq |A + B|, |A - B| \leq |A||B|$$

and

$$|A| \leq |A + A| \leq \frac{|A|(|A| + 1)}{2}.$$  

More generally, for any integer $n \geq 1$, we have $|(n + 1)A| \geq |nA|$ and

$$|nA| \leq \left( \frac{|A| + n - 1}{n} \right).$$

**Proposition 1.0.3.** Suppose that $A, B$ are additive sets with common ambient group $\mathbb{Z}$. Then the following are equivalent:

i) $|A + B| = |A|$;
ii) \(|A - B| = |A|\);
iii) \(|A + nB - mB| = |A|\) for at least one pair of integers \((n, m) \neq (0, 0)\);
iv) \(|A + nB - mB| = |A|\) for all integers \(n, m\);
v) there exists a finite subgroup \(G\) of \(Z\) such that \(B\) is contained in a coset of \(G\), and \(A\) is a union of cosets of \(G\).

**Proposition 1.0.4.** Suppose that \(A, B\) are additive sets with common ambient group \(Z\). Then the following are equivalent:
i) \(|A + B| = |A| |B|\);
ii) \(|A - B| = |A| |B|\);
iii) \(|\{(a, a', b, b') \in A \times A \times B \times B : a + b = a' + b'\}| = |A| |B|\);
iv) \(|\{(a, a', b, b') \in A \times A \times B \times B : a - b = a' - b'\}| = |A| |B|\);
v) \(|A \cap (x - B)| = 1\) for all \(x \in A + B\);
vi) \(|A \cap (B + y)| = 1\) for all \(y \in A - B\);
vi) \((A - A) \cap (B - B) = \{0\}\).

**Definition 1.0.5.** For an additive set \(A\), the **doubling constant** \(\sigma[A]\) is defined to be the quantity
\[
\sigma[A] = \frac{|2A|}{|A|} = \frac{|A + A|}{|A|}.
\]
Similarly we define the **difference constant** \(\delta[A]\) as
\[
\delta[A] = \frac{|A - A|}{|A|}.
\]
We have that
\[
1 \leq \sigma[A] \leq \frac{|A| + 1}{2} \text{ and } 1 \leq \delta[A] \leq |A| - 1 + \frac{1}{|A|}.
\]

**Definition 1.0.6.** An additive set \(A\) with the maximal value of doubling constant (or equivalently, with maximal difference constant, is known as a **Sidon set**. This means that all the pairwise sums of \(A\) are distinct, excluding the trivial equalities coming from the identity \(a + b = b + a\).

**Definition 1.0.7.** Let \(A\) and \(B\) be two additive sets with a common ambient group \(Z\). We define the **Ruzsa distance** \(d(A, B)\) between these two sets to be the quantity
\[
d(A, B) = \log \frac{|A - B|}{|A|^{1/2} |B|^{1/2}}.
\]

**Lemma 1.0.8.** (Ruzsa triangle inequality) The Ruzsa distance \(d(A, B)\) is non-negative, symmetric, and obeys the triangle inequality
\[
d(A, C) \leq d(A, B) + d(B, C)
\]
for all additive sets \(A, B, C\) with common ambient group \(Z\).
Proposition 1.0.9. Suppose that \((A, Z)\) is an additive set. Then the following are equivalent:

i) \(\sigma([A]) = 1\) (i.e. \(|A + A| = |A|\));

ii) \(\delta([A]) = 1\) (i.e. \(|A - A| = |A|\), or \(d(A, A) = 0\));

iii) \(d(A, B) = 0\) for at least one additive set \(B\);

iv) \(|nA - mA| = |A|\) for at least one pair of non-negative integers \(n, m\) with \(n + m \geq 2\);

v) \(|nA - mA| = |A|\) for all non-negative integers \(n, m\);

vi) \(A\) is a coset of a finite subgroup \(G\) of \(Z\).

Definition 1.0.10. If \(A\) and \(B\) are two additive sets with ambient group \(Z\), we define the additive energy \(E(A, B)\) between \(A\) and \(B\) to be

\[
E(A, B) = |\{(a, a', b, b') \in A \times A \times B \times B : a + b = a' + b'\}|.
\]

Lemma 1.0.11. (Ruzsa’s covering lemma) For any additive sets \(A, B\) with common ambient group \(Z\), there exists an additive set \(X_+ \subset B\) with

\[
B \subset A - A + X_+; \quad |X_+| \leq \frac{|A + B|}{|A|}; \quad |A + X_+| = |A||X_+|
\]

and similarly there exists an additive set \(X_- \subset B\) with

\[
B \subset A - A + X_-; \quad |X_-| \leq \frac{|A - B|}{|A|}; \quad |A - X_-| = |A||X_-|.
\]

In particular, \(B\) can be covered by \(\min(\frac{|A + B|}{|A|}, \frac{|A - B|}{|A|})\) translates of \(A - A\).

Definition 1.0.12. For nonempty subsets \(A, B\) of an abelian group \(G\), then for \(e \in G\), the e-transform of the pair \((A, B)\) is the pair \((A(e), B(e))\) of subsets of \(G\) defined by

\[
A(e) = A \cup (B + e) \quad \text{and} \quad B(e) = B \cap (A - e).
\]

Lemma 1.0.13. Let \((A(e), B(e))\) be the e-transform of the pair \((A, B)\). Then

\[
A(e) + B(e) \subset A + B
\]

and

\[
A(e) \setminus A = e + (B \setminus B(e)).
\]

If \(A\) and \(B\) are finite sets, then

\[
|A(e)| + |B(e)| = |A| + |B|.
\]

If \(e \in A\), and \(0 \in B\), then \(e \in A(e)\) and \(0 \in B(e)\).

Theorem 1.0.14. Let \(A, B\) be finite sets in a commutative group and write \(|A| = m\), \(|A + B| = \alpha m\). For arbitrary non-negative integers \(k, l\) we have

\[
|kB - lB| \leq \alpha^{k+l}m.
\]
CHAPTER 1. BASICS AND CARDINALITY INEQUALITIES

Definition 1.0.15. A directed graph \( G = (V(G), E(G)) \) is a graph of level \( h \) if the vertex set \( V(G) \) is the union of \( h + 1 \) pairwise disjoint nonempty sets \( V_0, V_1, \ldots, V_h \) and if every edge of \( G \) is of the form \((v, v')\), where \( v \in V_{i-1} \) and \( v' \in V_i \) for some \( i = 1, \ldots, h \).

Definition 1.0.16. A directed graph \( G \) of level \( h \) is a Plünnecke graph of level \( h \) if it is commutative i.e. it satisfies the following two conditions:

i) Let \( 1 \leq i \leq h - 1 \) and \( k \geq 2 \). Let \( u \in V_{i-1}, v \in V_i, \) and \( w_1, \ldots, w_k \in V_{i+1} \) be \( k + 2 \) distinct vertices of \( G \) such that \((u, v) \in E(G)\) and \((v, w_j) \in E(G)\) for \( j = 1, \ldots, k \). Then there exist distinct vertices \( v_1, \ldots, v_k \in V_i \) such that \((u, v_j) \in E(G)\) and \((v_j, w_j) \in E(G)\) for \( j = 1, \ldots, k \).

ii) Let \( 1 \leq i \leq h - 1 \) and \( k \geq 2 \). Let \( u_1, \ldots, u_k \in V_{i-1}, v \in V_i, \) and \( w \in V_{i+1} \) be \( k + 2 \) distinct vertices of \( G \) such that \((u_j, v) \in E(G)\) for \( j = 1, \ldots, k \), and \((v, w) \in E(G)\). Then there exist distinct vertices \( v_1, \ldots, v_k \in V_i \) such that \((u_j, v_j) \in E(G)\) and \((v_j, w) \in E(G)\) for \( j = 1, \ldots, k \).

Definition 1.0.17. Let \( A, B \) be nonempty, finite subsets of an abelian group. The addition graph is a Plünnecke graph of level \( h \), whose \( i \)th vertex set is the sumset \( A + iB \) and whose edges are the ordered pairs of group elements of the form \((v, v + b)\), where \( b \in B \) and \( v \in A + (i - 1)B \) for some \( i = 1, \ldots, h \).

Definition 1.0.18. For \( X, Y \subset V \), we define the image of \( X \) in \( Y \) as
\[
\text{im}(X, Y) = \{y \in Y: \text{there is a directed path from some } x \in X \text{ to } y\}.
\]

The magnification ratio is defined by
\[
\mu(X, Y) = \min \left\{ \frac{|\text{im}(Z, Y)|}{|Z|} : Z \subset X, Z \neq \emptyset \right\}.
\]

Theorem 1.0.19. (Plünnecke). In a commutative layered graph, \( \mu_j^{1/j} \) is decreasing.

An obvious (and typically the only available) upper estimate for \( \mu_j \) is \(|V_j|/|V_0|\).

Theorem 1.0.20. Let \( j < h \) be integers and \( G \) a commutative layered graph on the layers \( V_0, \ldots, V_h \). Write \(|V_0| = m, |V_j| = s. \) There is an \( X \subset V_0, X \neq \emptyset, \) such that
\[
|\text{im}(X, V_h)| \leq (s/m)^{0/h} |X|.
\]

Theorem 1.0.21. Let \( j < h \) be integers, \( A, B \) sets in a commutative group and write \(|A| = m, |A + jB| = \alpha m. \) There is an \( X \subset A, X \neq \emptyset, \) such that
\[
|X + hB| \leq \alpha^{0/h} |X|.
\]

Corollary 1.0.22. Let \( j < h \) be integers and \( A, B \) be sets in a torsion-free commutative group with \(|A| = m, |A + jB| = \alpha m. \) We have
\[
|hB| \leq (\alpha^{0/h} - 1) m + 1.
\]
Lemma 1.0.23. The restricted addition graph is commutative.

Theorem 1.0.24. Let \( j < h \) be integers, \( A, B, C \) sets in a commutative group and write \( |A| = m, |(A+jB)\setminus(C+(j-1)B)| = \alpha m \). There is an \( X \subset A, X \neq \emptyset \), such that
\[ |(X+hB)\setminus(C+(h-1)B)| \leq \alpha^{h/j}|X|. \]

Theorem 1.0.25. Let \( G \) be a commutative layered graph with layers \( V_0, \ldots, V_h, |V_0| = m \). If \( \mu_h \geq 1 \), then there are \( m \) (vertex)-disjoint paths from \( V_0 \) to \( V_h \).

Definition 1.0.26. The \textit{outdegree} and \textit{indegree} of a vertex \( x \) will be denoted by
\[ d^+(x) = d^+ (x, G) = |\{ y : x \rightarrow y \}|, \]
\[ d^-(x) = d^- (x, G) = |\{ y : y \rightarrow x \}|. \]

Corollary 1.0.27. In a commutative graph if \( \mu_h \geq 1 \), then \( \mu_j \geq 1 \) for \( 1 \leq j \leq h \).

Definition 1.0.28. Let \( G' = (V', E') \) and \( G'' = (V'', E'') \) be \( h \)-layered graphs with layers \( V' \) and \( V'' \). Their \textit{layered product} is the \( h \)-layered graph on the \( h \)-th magnification ratio of this graph is clearly
\[ \mu_j(I_{nh}) = |V_j| = |jB|. \]

Theorem 1.0.29. Let \( A, B_1, \ldots, B_h \) be sets in a commutative group \( G \) and write \( |A| = m, |A + B_i| = \alpha_i m \). There is an \( X \subset A, X \neq \emptyset \), such that
\[ |X + B_1 + \cdots + B_h| \leq \alpha_1 \alpha_2 \cdots \alpha_h |X|. \]

Theorem 1.0.30. Let \( j < h \) be integers, and let \( A, B_1, \ldots, B_h \) be finite sets in a commutative group \( G \). Let \( K = \{1, 2, \ldots, h\} \), and for any \( I \subset K \) put
\[ B_I = \sum_{i \in I} B_i, \quad \text{and} \quad |A| = m, |A + B_I| = \alpha_I m. \]

Write
\[ \beta = \left( \prod_{L \subseteq K, |L| = j} \alpha_L \right)^{(j-1)!/(h-j)!/(h-1)!} \]

There exists an \( X \subset A, X \neq \emptyset \), such that
\[ |X + B_K| \leq \beta |X|. \]
Theorem 1.0.33. Let \( j < h \) be integers, \( G \) a commutative layered graph on the layers \( V_0, \ldots, V_h \). Write \( |V_0| = m, |V_j| = s, \gamma = h/j \). Let an integer \( k \) be given, \( 1 \leq k \leq m \). There is an \( X \subset V_0, |X| \geq k \), such that

\[
|\text{im}(X, V_h)| \leq \left( \frac{s}{m} \right)^\gamma + \left( \frac{s}{m-1} \right)^\gamma + \cdots + \left( \frac{s}{m-k+1} \right)^\gamma + (|X|-k) \left( \frac{s}{m-k+1} \right)^\gamma.
\]

Theorem 1.0.34. With similar notation as above, let a real number \( t \) be given, \( 0 \leq t < m \). There is an \( X \subset V_0, |X| > t \), such that

\[
|\text{im}(X, V_h)| \leq \frac{s^\gamma}{\gamma} \left( \frac{1}{(m-t)^{\gamma-1}} - \frac{1}{m^{\gamma-1}} \right) + (|X|-t) \left( \frac{s}{m-t} \right)^\gamma.
\]

Theorem 1.0.35. Let \( j < h \) be integers, \( A, B \) sets in a commutative group, and write \( |A| = m, |A+jB| = s, \gamma = h/j \). Let a real number \( t \) be given, \( 0 \leq t < m \). There is an \( X \subset A, |X| > t \), such that

\[
|X + hB| \leq \frac{s^\gamma}{\gamma} \left( \frac{1}{(m-t)^{\gamma-1}} - \frac{1}{m^{\gamma-1}} \right) + (|X|-t) \left( \frac{s}{m-t} \right)^\gamma.
\]

Theorem 1.0.36. Let \( j < h \) be integers, \( A, B, C \) sets in a commutative group, and write \( |A| = m, |(A+jB) \setminus (C+(j-1)B)| = s, \gamma = h/j \). Let a real number \( t \) be given, \( 0 \leq t < m \). There is an \( X \subset A, |X| > t \), such that

\[
|(X+hB) \setminus (C+(h-1)B)| \leq \frac{s^\gamma}{\gamma} \left( \frac{1}{(m-t)^{\gamma-1}} - \frac{1}{m^{\gamma-1}} \right) + (|X|-t) \left( \frac{s}{m-t} \right)^\gamma.
\]

The case \( j = 1, h = 2 \) is as follows:

Corollary 1.0.37. Let \( A, B \) be sets in a commutative group and write \( |A| = m, |A+iB| = s \). Let a real number \( t \) be given, \( 0 \leq t < m \). There is an \( X \subset A, |X| > t \), such that

\[
|X + 2B| \leq \frac{s^2}{(m-t)^2} \left( |X| - \frac{t(t+m)}{2m} \right).
\]

Theorem 1.0.38. Let \( A, B_1, \ldots, B_h \) be sets in a commutative group \( G \) and write \( |A| = m, |A+B_i| = \alpha_i m \). Let a real number \( t \) be given, \( 0 \leq t < m \). There is an \( X \subset A, X \neq \emptyset \), such that

\[
|X+B_1+\cdots+B_h| \leq \alpha_1 \alpha_2 \cdots \alpha_h m^h \left( \frac{1}{h} \left( \frac{1}{(m-t)^{h-1}} - \frac{1}{m^{h-1}} \right) + \frac{|X|-t}{(m-t)^{h-1}} \right).
\]

Theorem 1.0.39. Let \( A, Y, Z \) be finite sets in a (not necessarily commutative) group. We have

\[
\]
Corollary 1.0.40. If $|A| = m$, $|2A| \leq \alpha m$, then $|-A + A| \leq \alpha^2 m$ and $|A - A| \leq \alpha^2 m$.

Corollary 1.0.41. If $|A| = m$, $|3A| \leq \alpha m$, then $|-2A + 2A| \leq \alpha^2 m$.

Theorem 1.0.42. Let $\alpha > 2$. Then for any $c < \frac{\sqrt{2\log 2}}{\sqrt{3}}$ and infinitely many $m$, there exist two sets $A$ and $B$ such that $|A| = m, |A + B| \leq \alpha m$ and for any nonempty $X \subset A$, one has
\[
\frac{|X - B|}{|X|} \geq \exp \left( c \sqrt{\log(\alpha/2)} \left( \log m \right) (\log \log m)^{-1} \right).
\]

Theorem 1.0.43. Let $A$ and $B$ be nonempty and finite subsets of some abelian group such that $|A| = m, |A + B| \leq \alpha m$. Then there exists some nonempty subset $X$ of $A$ such that
\[
\frac{|X - B|}{|X|} \leq \alpha \exp \left( 2 \sqrt{\log \alpha} (\log m) \right).
\]

Theorem 1.0.44. In any commutative group we have
\[
|A||Y + Z| \leq |A + Y||A + Z|.
\]

Theorem 1.0.45. Let $X, Y, Z$ be finite sets in a commutative group. We have
\[
|X + Y + Z|^2 \leq |X + Y||Y + Z||X + Z|.
\]

Theorem 1.0.46. Let $X, Y, Z$ be finite sets in a not necessarily commutative group. We have
\[
|X + Y + Z|^2 \leq |X + Y||Y + Z| \max_{y \in Y} |X + y + Z|.
\]

Theorem 1.0.47. Let $A_1, \ldots, A_k$ be finite, nonempty sets in an arbitrary commutative semigroup. Put
\[
S = A_1 + \cdots + A_k,
\]
\[
S_i = A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_k.
\]
We have
\[
|S| \leq \left( \prod_{i=1}^{k} |S_i| \right)^{1/(k-1)}.
\]

Theorem 1.0.48. Let $m, n$ be positive integers, satisfying $m \leq n \leq m^2$. There is a set $A$ of integers such that $|A| \asymp m, |2A| \asymp n$ and
\[
|3A| \asymp \min \left( n^3/m^2, n^{3/2} \right).
\]
Theorem 1.0.49. Let $A, B$ be finite sets in a commutative group $G$, $|A| = m, |A + B| = \alpha m, 1 < \alpha \leq 2$. We have

$$|A + 2B| \leq \alpha m + \frac{3}{2} (\alpha - 1)m\sqrt{|2B|},$$

consequently

$$|A + 2B| \leq \alpha m + 3(\alpha - 1)m^{3/2};$$

if $G$ is torsion-free, then

$$|A + 2B| \leq \alpha m + 3(\alpha - 1)^{3/2}m^{3/2}.$$

Theorem 1.0.50. Let $A, B_1, B_2$ be sets in a (typically non-commutative group) $G$ and write $|A| = m, |B_1 + A| = \alpha_1 m, |A + B_2| = \alpha_2 m$. There is an $X \subset A, X \neq \emptyset$, such that

$$|B_1 + X + B_2| \leq \alpha_1 \alpha_2 |X|.$$

Definition 1.0.51. A collection of sets $B_1, \ldots, B_k$ in a (non-commutative) group is exocommutative, if for all $x \in B_i, y \in B_j$ with $i \neq j$ we have $x + y = y + x$.

Theorem 1.0.52. Let $A, B_1, B_2, \ldots, B_k, C_1, C_2, \ldots, C_l$ be sets in a (typically non-commutative group) $G$ and write $|A| = m, |B_i + A| = \alpha_i m, i = 1, \ldots, h, |A + C_j| = \beta_j m, j = 1, \ldots, l$. Assume that both $B_1, \ldots, B_k$ and $C_1, \ldots, C_l$ are exocommutative. Then there is an $X \subset A, X \neq \emptyset$, such that

$$|B_1 + \cdots + B_k + X + C_i + \cdots + C_l| \leq \alpha_1 \ldots \alpha_k \beta_1 \ldots \beta_l |X|.$$
Chapter 2

Structure of Sets with Few Sums

Theorem 2.0.1. (Freiman) If $A \subset \mathbb{N}, |A| = m, |A + A| \leq 3m - 4$, then $A$ is contained in an arithmetic progression of length $\leq |A + A| - m + 1 \leq 2m - 3$.

Definition 2.0.2. Let $q_1, \ldots, q_d$ and $a$ be elements of an arbitrary commutative group, $l_1, \ldots, l_d$ positive integers. A $d$-dimensional generalized arithmetic progression is a set of the form

$$P = P(q_1, \ldots, q_d; l_1, \ldots, l_d; a) = \{a + x_1q_1 + \cdots + x_dq_d : 0 \leq x_i \leq l_i\}.$$  

We call $d$ the dimension of $P$, and its size to be

$$||P|| = \prod_{i=1}^{d} (l_i + 1),$$

which is the same as the number of elements if all the above sums are distinct, and in that case, we say that $P$ is proper.

Theorem 2.0.3. (Freiman’s Theorem) If $A \subset \mathbb{Z}, |A| = n, |A + A| \leq \alpha n$, then $A$ is contained in a generalized arithmetic progression of dimension $\leq d(\alpha)$ and size $\leq s(\alpha)n$.

Recall that the exponent of a group $G$ is the smallest positive integer $r$ such that $rg = 0$ for every $g \in G$.

Theorem 2.0.4. Let $G$ be a commutative group of exponent $r, A \subset G, |A| = m, |A + A| \leq \alpha m$. $A$ is contained in a coset of a subgroup of size $\leq \alpha^2 r^4 m$. 

Theorem 2.0.5. (Green-Ruzsa) Let $G$ be a commutative group, $A \subseteq G$, $|A| = m$, $|A + A| \leq \alpha m$. $A$ is contained in a set of the form $H + P$, where $H$ is a subgroup, $P$ is a generalized arithmetic progression, the dimension of $P$ is $\leq d(\alpha)$ and $|H||P| \leq s(\alpha)m$.

For the quantities $d, s$ we have the following bounds: $d(\alpha) \ll \alpha^c, s(\alpha) \ll e^{\alpha^c}$.

Theorem 2.0.6. Let $r \geq 2$ be an integer, and let $G$ be a commutative group of exponent $r$. Let $A \subseteq G$ be a finite set, $|A| = m$. If there is another set $A' \subseteq G$ such that $|A'| = m$ and $|A + A'| \leq \alpha m$ (in particular, if $|A + A| \leq \alpha m$ or $|A - A| \leq \alpha m$), then $A$ is contained in a subgroup $H$ of $G$ such that

$$|H| \leq f(r, \alpha)m, \quad \text{where} \quad f(r, \alpha) = \alpha^2 r^{\alpha^4}.$$

Definition 2.0.7. Let $G_1, G_2$ be commutative groups, $A_1 \subseteq G_1, A_2 \subseteq G_2$. We say that a mapping $\phi : A_1 \to A_2$ is a homomorphism of order $r$ in the sense of Freiman, or an $F_r$-homomorphism for short, if for every $x_1, \ldots, x_r, y_1, \ldots, y_r \in A_1$ (not necessarily distinct), the equation

$$x_1 + x_2 + \cdots + x_r = y_1 + y_2 + \cdots + y_r$$

implies

$$\phi(x_1) + \phi(x_2) + \cdots + \phi(x_r) = \phi(y_1) + \phi(y_2) + \cdots + \phi(y_r).$$

We call $\phi$ an $F_r$-isomorphism if it is one-to-one, and its inverse is a homomorphism as well, that is, the above implication is if-and-only-if. If we say Freiman isomorphism without specifying $r$, then the first nontrivial case $r = 2$ is meant.

Lemma 2.0.8. Let $G, G'$ be commutative groups. If a set $P' \subseteq G'$ is the homomorphic image of a generalized arithmetical progression $P(q_1, \ldots, q_d; l_1, \ldots, l_d; a) \subseteq G$, then there are elements $q'_1, \ldots, q'_d, a' \in G'$ such that

$$P' = P(q'_1, \ldots, q'_d; l_1, \ldots, l_d; a')$$

and the homomorphism is given by

$$\phi(a + x_1 q_1 + \cdots + x_d q_d) = a' + x_1 q'_1 + \cdots + x_d q'_d.$$

Lemma 2.0.9. Let $G, G'$ be commutative groups, and let $A \subseteq G, A' \subseteq G'$ be $F_r$-isomorphic sets. Assume that $r = r'(k + l)$ with non-negative integers $r', k, l$. The sets $kA - lA$ and $kA' - lA'$ are $F_{r'}$-isomorphic.

Lemma 2.0.10. Let $A$ be a finite set in a torsion-free commutative group, and let $r$ be any positive integer. There is a set $A' \subseteq \mathbb{Z}$ which is $F_r$-isomorphic to $A$.

Definition 2.0.11. We define the Freiman dimension of a set $A \subseteq \mathbb{R}^k$ as the largest $d$ for which there is an isomorphic properly $d$-dimensional set.
Theorem 2.0.12. Let $A$ be a finite set in a torsion-free commutative group, $|A| = m$, $r \geq 2$ an integer and $|rA - rA| = n$.

i) For every $q \geq n$ there exists a set $A' \subset A$, $|A'| \geq m/r$ which is $F_r$-isomorphic to a set $T'$ of residues modulo $q$.

ii) There is a set $A^* \subset A$, $|A^*| \geq m/r^2$, which is $F_r$-isomorphic to a set $T^*$ of integers.

$$T^* \subset [0, n/r].$$

Here, a group will be commutative. Recall that a character is a homomorphism $\gamma : G \rightarrow \mathbb{C}_1$. We have $\gamma(x + y) = \gamma(x)\gamma(y)$. The characters of $G$ form a group (under pointwise multiplication) which we denote $\Gamma$. Its unity is the principal character $\gamma_0 \equiv 1$, and the inverse of $\gamma(g)$ is $\overline{\gamma(g)} = \gamma(g)$, which is the complex conjugate. If $\gamma$ is a character on a cyclic group $\mathbb{Z}_q$ and $\gamma(1) = \omega$, then $\gamma(n) = \omega^n$. Since $\gamma(q) = \gamma(0) = 1$, we see that $\omega$ must be a $q$-th root of unity, say $\omega = e^{2\pi ik/q}$ with some $k$, consequently

$$\gamma(n) = e^{2\pi i kn/q}.$$

Definition 2.0.13. Let $\phi : G \rightarrow \mathbb{C}$ be a function on the group $G$. Its Fourier transformation is the function $f : \Gamma \rightarrow \mathbb{C}$ defined by

$$f(\gamma) = \sum_{g \in G} \phi(g)\gamma(g).$$

The Fourier transform is often denoted by $f = \hat{\phi}$.

For a cyclic group $G = \mathbb{Z}_q$ the characters are the functions

$$\gamma_k(n) = e^{2\pi ik/n}, \quad k = 0, 1, \ldots, q - 1.$$ 

Consequently, the Fourier transform of a function $\phi$ is given by

$$f(\gamma_k) = \sum_n e^{2\pi i kn/q}\phi(n).$$

If we identify this character $\gamma_k$ with its subscript $k \in \mathbb{Z}_q$, we can also say that the Fourier transform is

$$f(k)\sum_n e^{2\pi i kn/q}\phi(n).$$

Given the Fourier transform of a function, we can reconstruct the function from it as follows.
Theorem 2.0.14. (Fourier inversion formula) Let $\phi$ be a function on $G$ and $f = \hat{\phi}$ its Fourier transform. We have

$$\phi(x) = \frac{1}{|G|} \sum_{\gamma \in \Gamma} f(\gamma) \overline{\gamma}(x).$$

Theorem 2.0.15. (Parseval formula) Let $\phi$ be a function on $G$ and $f = \hat{\phi}$ its Fourier transform. We have

$$\sum_{\gamma \in \Gamma} |f(\gamma)|^2 = |G| \sum_{x \in G} |\phi(x)|^2.$$

The Fourier transform of the set $A \subset G$ will be denoted $\hat{A}(\gamma)$. For $\phi$ its indicator function, we have

$$\hat{A}(\gamma) = f(\gamma) = \sum_{a \in A} \gamma(a).$$

Let now $A_1, A_2$ be sets in $G$ with Fourier transforms $f_1, f_2$. We see that

$$f_1(\gamma) f_2(\gamma) = \sum_{x \in G} r(x)$$

where $r(x) = |\{(a_1, a_2) : a_i \in A_i, a_1 + a_2 = x\}|$ is the number of representations of $x$ as a sum with summands from our sets. The inversion formula now gives

$$r(x) = \frac{1}{|G|} \sum_{\gamma \in \Gamma} f_1(\gamma) f_2(\gamma) \overline{\gamma}(x).$$

Definition 2.0.16. If $G$ is a commutative group, $\gamma_1, \ldots, \gamma_k$ are characters of $G$ and $\epsilon_j > 0$, we write

$$B(\gamma_1, \ldots, \gamma_k; \epsilon_1, \ldots, \epsilon_k) = \{g \in G : \text{arg}\gamma_j(g) \leq 2\pi \epsilon_j \text{ for } j = 1, \ldots, k\}$$

and we call these sets Bohr sets. In particular, if $\epsilon_1 = \cdots = \epsilon_k = \epsilon$, we shall speak of a Bohr $(k, \epsilon)$-set. (We take the branch of arg that lies in $[-\pi, \pi)$).

We work mainly in $\mathbb{Z}_q$. A typical character is of the form

$$\gamma(x) = e^{2\pi iux/q}, u \in \mathbb{Z}_q,$$

so $\text{arg}\gamma(x) = 2\pi ||ux/q||$, where $||t||$ denotes the absolute fractional part of $t$ (its distance to the nearest integer). Hence a Bohr set in $\mathbb{Z}_q$ can be written as

$$B(u_1, \ldots, u_k; \epsilon_1, \ldots, \epsilon_k) = \{x \in \mathbb{Z}_q : ||u_j x/q|| \leq \epsilon_j \text{ for } j = 1, \ldots, k\}.$$
Lemma 2.0.17. Let $G$ be a finite commutative group, $|G| = q$. Let $A$ be a nonempty subset of $G$ and write $|A| = m = \beta q$. The set $D = 2A - 2A$ contains a Bohr $(k, \epsilon)$-set with some integer $k < \beta^{-2}$ and $\epsilon = 1/4$.

Theorem 2.0.18. If $A_1, A_2, A_3$ are subsets of $G$, a commutative group with $|G| = q$ and $|A_i| \geq \beta_i q$, then, for some $t$, $A_1 + A_2 + A_3 \supset t + B(\gamma_1, \ldots, \gamma_k, \eta)$, where $k$ and $\eta$ depend only on the densities $\beta_i$.

Definition 2.0.19. A set $L \subseteq \mathbb{R}^d$ is a lattice if it is a discrete subgroup and it is not contained in any smaller dimensional subspace. Any such lattice is isomorphic to $\mathbb{Z}^d$; that is, there are linearly independent vectors $e_1, \ldots, e_d \in \mathbb{R}^d$ such that $L = \{x_1 e_1 + \cdots + x_d e_d : x_i \in \mathbb{Z}\}$.

Definition 2.0.20. A set $F \subseteq \mathbb{R}^d$ is a fundamental domain if the sets $F + x, x \in L$, cover $\mathbb{R}^d$ without overlap.

An example is $F = \{x_1 e_1 + \cdots + x_d e_d : 0 \leq x_i < 1\}$.

Definition 2.0.21. The common value of volumes of fundamental domains and absolute value of determinants of matrices formed by integral bases is called the determinant of the lattice.

Definition 2.0.22. Let $Q$ be a closed neighborhood of 0, and let $L$ be a lattice in $\mathbb{R}^d$. The successive minima of $Q$ with respect to the lattice are the smallest positive numbers $0 < \lambda_1 \leq \cdots \leq \lambda_d$ such that there are linearly independent vectors $a_1, \ldots, a_d \in L, a_i \in \lambda_i Q$.

Lemma 2.0.23. (Minkowski’s inequality for successive minima) Let $Q$ be a closed neighborhood of 0, and let $L$ be a lattice in $\mathbb{R}^d$. Let $0 < \lambda_1 \leq \cdots \leq \lambda_d$ be the successive minima of $Q$ with respect to $L$. We have

$$\lambda_1 \cdots \lambda_d \leq 2^d \frac{\det L}{\text{vol} Q}.$$ 

Theorem 2.0.24. Let $q$ be a positive integer, $u_1, \ldots, u_d$ residues modulo $q$ such that $(u_1, u_2, \ldots, u_d, q) = 1$, $\epsilon_1, \ldots, \epsilon_d$ real numbers satisfying $0 < \epsilon_j < 1/2$. Write

$$\delta = \frac{\epsilon_1 \cdots \epsilon_d}{d^d}.$$ 

There are residues $v_1, \ldots, v_d$ and non-negative integers $l_1, \ldots, l_d$ such that the set

$$P = \{v_1 x_1 + \cdots + v_d x_d : |x_i| \leq l_i\}$$

satisfies

$$P \subset B(u_1, \ldots, u_d; \epsilon_1, \ldots, \epsilon_d),$$

the previous sums are all distinct and

$$|P| = ||P|| = \prod (2l_j + 1) \geq \prod (l_j + 1) > \delta q.$$
Lemma 2.0.25. Let $q$ be a prime, and let $A$ be a nonempty set of residues modulo $q$ with $|A| = \beta q$. There are residues $v_1, \ldots, v_d$ and non-negative integers $l_1, \ldots, l_d$ such that the set

$$P = \{v_1x_1 + \cdots + v_dx_d : |x_i| \leq l_i\}$$

satisfies $P \subset D = 2A - 2A$, the previous sums are all distinct and

$$||P|| = \prod (2l_j + 1) \geq \prod (l_j + 1) > \delta q,$$

where $d \leq \beta^2$ and

$$\delta(4d)^{-d} \leq (\beta^2/4)^{1/\beta^2}.$$

Theorem 2.0.26. Let $A, B$ be finite sets in a torsion-free commutative group satisfying $|A| = |B| = m$, $|A + B| \leq \alpha m$. There are numbers $d, s$ depending only on $\alpha$ such that $A$ is contained in a generalized arithmetical progression of dimension at most $d$ and size at most $sm$.

Theorem 2.0.27. Let $r_k(n)$ denote the maximal number of integers that can be selected from the interval $[1, n]$ without including a $k$-term arithmetical progression and write $\omega_k(n) = n/r_k(n)$.

Assume that $|A| = n$ and $A$ does not contain any $k$-term arithmetic progression. We have

$$|A + A - A - A| \geq \frac{1}{4} \omega_k(n)n,$$

$$|A + B| \geq \frac{1}{\sqrt{2}} \omega_k(n)^{1/4} n^{1/4} |B|^{3/4}$$

for every set $B$,

$$|A + B| \geq \frac{1}{\sqrt{2}} \omega_k(n)^{1/4} n$$

for every set $B$ such that $|B| = n$,

$$|A + A| \geq \frac{1}{\sqrt{2}} \omega_k(n)^{1/4} n,$$

$$|A - A| \geq \frac{1}{\sqrt{2}} \omega_k(n)^{1/4} n.$$

Corollary 2.0.28. Assume that $|A| = n$ and $A$ does not contain any three-term arithmetical progression. For every constant $c < 1/8$ and $n > n_0(c)$ we have

$$|A + B| \geq \frac{1}{2} n (\log n)^c$$

for every set $B$ such that $|B| = n$, in particular

$$|A + A| \geq \frac{1}{2} n (\log n)^c,$$

$$|A - A| \geq \frac{1}{2} n (\log n)^c.$$
Chapter 3

Location and Sumsets

Theorem 3.0.1. (Cauchy-Davenport inequality) Let $p$ be a prime, $A, B \subset \mathbb{Z}_p$ nonempty sets. We have

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

Proposition 3.0.2. Let $A, B$ be additive sets in $\mathbb{Z}$ such that $|A|, |B| \geq 2$. Then $|A + B| = |A| + |B| - 1$ if and only if $A, B$ are arithmetic progressions of the same step.

Theorem 3.0.3. (Vosper’s Theorem) Let $p$ be a prime, and let $A, B$ be additive sets in $\mathbb{Z}_p$ such that $|A|, |B| \geq 2$ and $|A + B| \leq p - 2$. Then $|A + B| = |A| + |B| - 1$ if and only if $A$ and $B$ are arithmetic progressions with the same step.

Definition 3.0.4. The reduced diameter $\text{diam} A$ of a set $A \subset \mathbb{Z}$ is the smallest $u$ such that $A$ is contained in an arithmetic progression $\{b, b + q, \ldots, b + uq\}$.

Theorem 3.0.5. For any set $A \subset \mathbb{Z}$ with $|A| = m$ and $\text{diam} A = u$ we have

$$|2A| \geq \min(m + u, 3m - 3).$$

Definition 3.0.6. A set is sumfree if it has no three elements such that $x + y = z$ (so we exclude $2x = z$ too).

Definition 3.0.7. Let $S$ be a nonempty set in a commutative group $G$. The stabilizer or group of periods of $S$ is the set

$$\text{stab} S = \{x \in G : x + S = S\}.$$

This is a subgroup of $G$.

Theorem 3.0.8. (Kneser’s Theorem) Let $A, B$ be finite sets in a commutative group $G$, $S = A + B$ and $H = \text{stab} S$. We have

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

If this holds with strict inequality, then

$$|A + B| \geq |A + H| + |B + H| \geq |A| + |B|.$$
Lemma 3.0.9. Let $S$ be a finite set in a group, $S = S_1 \cup S_2$. We have

$$|S| + |\text{stab } S| \geq \min(|S_1| + |\text{stab } S_1|).$$

Lemma 3.0.10. Let $S$ be a finite set in a group, $S = S_1 \cup S_2 \cup \cdots \cup S_k$. We have

$$|S| + |\text{stab } S| \geq \min(|S_i| + |\text{stab } S_i|).$$

If we translate a set $A$ so that its minimal element is 0, and divide each element by their gcd, then we can write $A$ as $A = \{a_1, \ldots, a_m\}, a_1 = 0, a_m = u$ with $\gcd(a_1, \ldots, a_m) = 1$.

Theorem 3.0.11. (Freiman) Let $A, B \subset \mathbb{Z}$, $A = \{0 = a_1 < \cdots < a_m = u\}, B = \{0 = b_1 < \cdots < b_n = v\}$. If $\gcd(a_1, \ldots, a_m, b_1, \ldots, b_n) = 1$ and $u \leq v$, then

$$|A + B| \geq \min(m + v, m + n + \min(m, n) - 3).$$

Theorem 3.0.12. (Lev and Smeliansky) If $\gcd(b_1, \ldots, b_n) = 1$ and $u \leq v$, then

$$|A + B| \geq \min(m + v, n + 2m - 2 - \delta),$$

where $\delta = 1$ if $u = v$ and $\delta = 0$ if $u < v$.

Definition 3.0.13. Let $G$ be a semigroup (usually a commutative group). For a fixed finite set $B \subset G$ we define its impact function by

$$\xi_B(m) = \xi_B(m, G) = \min\{|A + B| : A \subset G, |A| = m\}.$$

This is defined for all positive integers if $G$ is infinite, and for $m \leq |G|$ if $G$ is finite.

Theorem 3.0.14. Let $G'$ be a commutative group, $G$ a subgroup of $G'$, and let $B \subset G$ be a finite set. If $G$ is infinite, we have

$$\xi_B(m, G') = \xi_B(m, G)$$

for all $m$. If $G$ is finite, say $|G| = q$, then for $m = kq + r, 0 \leq r \leq q - 1$, we have

$$\xi_B(m, G') = \xi_B(r, G) + kq.$$

Definition 3.0.15. Let $G$ be a torsion-free group. Take a finite $B \subset G$, and let $G'$ be the subgroup generated by $B - B$, that is, the smallest subgroup such that $B$ is contained in a single coset. Let $B' = B - a$ with some $a \in B$, so that $B' \subset G'$. The group $G'$, as any finitely generated torsion-free group, is isomorphic to $\mathbb{Z}^d$ for some $d$. We call this $d$, the dimension of $B$, denoted $\dim B$. 

16
Observe that this dimension is not necessarily equal to the geometrical dimension. In this case $B \subset \mathbb{R}^k$, this is its dimension over the field of rationals. The reduced diameter makes sense exactly for one-dimensional sets.

**Theorem 3.0.16.** Let $B$ be a one-dimensional set in a torsion-free commutative group, $\text{diam } B = v \geq 3$.

i) For 
\[ m > \frac{(v-1)(v-2)}{2} \]
we have $\xi_B(m) = m + v$.

ii) If 
\[ \frac{(k-1)(k-2)}{2} < m \leq \frac{k(k-1)}{2} \]
with some integer $2 \leq k < v$, then $\xi_B(m) \geq m + k$. Equality holds for the set $B = \{0, 1, v\} \subset \mathbb{Z}$.

**Theorem 3.0.17.** Let $B$ be a one-dimensional set in a torsion-free commutative group, $\text{diam } B = v \geq 3$, $|B| = n$. Define $w$ by

\[ w = \min_{d\mid v, d \leq n-2} \left[ \frac{n-2}{d} \right] \]

For every $m$ we have

\[ \xi_B(m) \geq m + \min \left( v, \frac{w}{2} + \min_{t \in \mathbb{N}} \left( \frac{m}{t} + \frac{tw}{2} \right) \right) \]

**Lemma 3.0.18.** Let $B'$ be the set of residues of elements of $B$ modulo $v$. For every nonempty $X \subset \mathbb{Z}_v$, we have

\[ |X + B'| \geq \min(|X| + w, v) \]

**Corollary 3.0.19.** Using the assumptions and notations of above, we have

\[ \xi_B(m) \geq \min \left( m + v, \left( \sqrt{m} + \sqrt{w/2} \right)^2 \right) \]

**Theorem 3.0.20.** (Freiman) Let $A \subset \mathbb{R}^d$ be a finite set, $|A| = m$. Assume that $A$ is proper $d$-dimensional, that is, it is not contained in any affine hyperplane. Then

\[ |A + A| \geq (d+1)m - \frac{d(d+1)}{2} \]

**Definition 3.0.21.** A long simplex is a set of the form

\[ L_{dm} = \{0, e_1, 2e_1, \ldots, (m - d)e_1, e_2, e_3, \ldots, e_d\} \]
CHAPTER 3. LOCATION AND SUMSETS

Note that the above theorem has equality when $A$ is a long simplex.

**Theorem 3.0.22.** If $A, B \subset \mathbb{R}^d$, $|A| \leq |B|$ and $\text{diam}(A + B) = d$, then we have

$$|A + B| \geq |B| + d|A| - \frac{d(d + 1)}{2}.$$  

We now consider finite sets in a Euclidean space $\mathbb{R}^d$. Put

$$F_d(m, n) = \min\{ |A + B| : |A| = m, |B| = n, \dim(A + B) = d \},$$

$$F'_d(m, n) = \min\{ |A + B| : |A| = m, |B| = n, \dim B = d \},$$

$$F''_d(m, n) = \min\{ |A + B| : |A| = m, |B| = n, \dim A = \dim B = d \}.$$

To describe $F_d$ define another function $G_d$ as follows:

$$G_d(m, n) = n + \sum_{j=1}^{m-1} \min(d, n-j), \ n \geq m \geq 1,$$

and for $m > n$ extend it symmetrically, putting $G_d(m, n) = G_d(n, m)$.

**Theorem 3.0.23.** For all positive integers $m, n$ and $d$ satisfying $m + n \geq d + 2$ we have

$$F_d(m, n) \geq G_d(m, n).$$

**Theorem 3.0.24.** Assume $1 \leq m \leq n$. We have

$$F_d(m, n) = F'_d(m, n) = G_d(m, n)$$

unless either $n < d + 1$ or $m \leq n - m \leq d$ (in this case $n \leq 2d$).

For a fixed value of $n$, define the weight of a point $x = (x_1, \ldots, x_d)$ as

$$w(x) = \frac{x_1}{n-d} + x_2 + \cdots + x_d.$$  

This defines an ordering by writing $x < y$ if either $w(x) < w(y)$ or $w(x) = w(y)$ and for some $j$ we have $x_j > y_j$ and $x_i = y_i$ for $i < j$. Let $D_{dnn}$ be the collection of the first $m$ vectors with non-negative integer coordinates in this ordering. We have $D_{dnn} = L_{dn} = B$, and, more generally $D_{dnn} = rB$ for any integers $m$ satisfying some things.
Theorem 3.0.25. (Gardner and Gronchi) If \( A, B \subset \mathbb{R}^d, |A| = m, |B| = n \) and \( \dim B = d \), then we have
\[
|A + B| \geq |D_{d,mn} + L_{dn}|.
\]

Corollary 3.0.26. For \( m \geq n > d \) we have
\[
F''_d(m, n) = F'_d(m, n) = |D_{d,mn} + L_{dn}|.
\]

Theorem 3.0.27. If \( A, B \subset \mathbb{R}^d, |A| = m \geq |B| = n \) and \( \dim B = d \), then we have
\[
|A + B| \geq m + (d - 1)n + (n - d)^{1 - 1/d}(m - d)^{1/d} - \frac{d(d - 1)}{2}.
\]

Theorem 3.0.28. If \( A, B \subset \mathbb{R}^d, |A| = m, |B| = n \) and \( \dim B = d \), then we have
\[
|A + B|^{1/d} \geq m^{1/d} + \left( \frac{n - d}{d!} \right)^{1/d}.
\]

Definition 3.0.29. For \( G \) a torsion-free group, and finite \( B \subset G \), then like before, let \( G' \) be the subgroup generated by \( B - B \) and \( B' = B - a \) with some \( a \in B \), so that \( B' \subset G' \). So we have an isomorphism \( \phi : G' \rightarrow \mathbb{Z}^d \) and let \( B'' = \phi(B') \). The hull volume of \( B \) is the volume of the convex hull of the set \( B'' \), denoted \( hv B \).

Theorem 3.0.30. Let \( B \) be a finite set in a torsion-free group \( G, d = \dim B, v = hv B \). We have
\[
\lim |kB| = v.
\]

Theorem 3.0.31. Let \( B \) be a finite set in a torsion-free commutative group \( G, d = \dim B, v = hv B \). We have
\[
\lim \xi_B(m)^{1/d} - m^{1/d} = v^{1/d}.
\]

Theorem 3.0.32. With the notations of the previous theorem, if \( d \geq 2 \) and \( m \geq v \), we have
\[
\xi_B(m) \leq m + dv^{1/d}m^{1 - 1/d} + c_1v^{2/d}m^{1 - 2/d},
\]
\[
\xi_B(m)^{1/d} - m^{1/d} \leq v^{1/d} + c_2v^{2/d}m^{1 - 1/d}
\]
\((c_1, c_2 \text{ depend on } d)\). With \( n = |B| \) for large \( m \) we have
\[
\xi_B(m) \geq m + dv^{1/d}m^{1 - 1/d} - c_3v^{d+2/d}n^{-1/2}m^{1 - 3/d},
\]
\[
\xi_B(m)^{1/d} - m^{1/d} \geq v^{1/d} - c_4v^{d+3/d}n^{-1/2}m^{-1/(2d)}.
\]

Theorem 3.0.33. The impact function of the set \( B = \{0, e_1, e_2\} \subset \mathbb{Z}^2 \) satisfies
\[
\sqrt[3]{\xi_B(m)} - \sqrt[12]{m} > \sqrt[20]{v}
\]
for all \(m\).

The impact function of the set \(B = \{0, e_1, e_2, -(e_1 + e_2)\} \subset \mathbb{Z}^2\) satisfies

\[
\sqrt{\xi_B(m)} - \sqrt{m} < \sqrt{v}
\]

for infinitely many \(m\).

**Definition 3.0.34.** The \(d\)-dimensional impact volume of a set \(B\) (in an arbitrary commutative group) is the quantity

\[
iv_d(B) = \inf_{m \in \mathbb{N}} (\xi_B(m)^{1/d} - m^{1/d})^d.
\]

**Theorem 3.0.35.** Let \(B\) be a finite set in a commutative torsion-free group, \(\dim B = d, |B| = n\). We have

\[
\left(\frac{n - d}{d!}\right) \leq iv_d(B) \leq hv_B,
\]

with equality in both places if \(B\) is a long simplex.

**Theorem 3.0.36.** Let \(n_1, \ldots, n_d\) be positive integers and let

\[B = \{(x_1, \ldots, x_d) \in \mathbb{Z}^d : 0 \leq x_i \leq n_i\}\]

We have

\[iv_d(B) = hv_B = v = n_1 \cdots n_d.
\]

**Theorem 3.0.37.** Let \(G = G_1 \times G_2\) be a commutative group represented as the direct product of the groups \(G_1\) and \(G_2\). Let \(B = B_1 \times B_2 \subset G\) be a finite set with \(B_1 \subset G_1, B_2 \subset G_2\). We have

\[iv_d(B) \geq iv_{d-1}(B_1)iv_1(B_2).
\]

**Definition 3.0.38.** The thickness \(\theta(B)\) of a set \(B \subset \mathbb{R}^d\) is the smallest integer \(k\) with the property that there is a hyperplane \(P\) of \(\mathbb{R}^d\) and \(x_1, \ldots, x_k \in \mathbb{R}^d\) such that \(B \subset \bigcup_{i=1}^{k} P + x_i\).

**Theorem 3.0.39.** (Hovanskii’s theorem) Let \(A\) be a finite set in a commutative semigroup \(G\). There is a polynomial \(f\) and an integer \(n_0\) such that for \(n > n_0\) we have

\[|nA| = f(n).
\]

**Definition 3.0.40.** Let \(B\) be a finite set in a commutative semigroup, and let \(vk^d\) be the leading term of the polynomial which coincides with \(|kB|\) for large \(k\). By the dimension of \(B\) we mean the degree \(d\) of this polynomial, and by the hull volume we mean the leading coefficient \(v\).
Chapter 4

Density

**Definition 4.0.1.** For a set $A$ of integers we shall use the same letter to denote its counting function

$$A(x) = |A \cap [1, x]|.$$  

We allow $A$ to contain 0 or negative numbers, but they are not taken into account in the function.

**Definition 4.0.2.** The asymptotic density of a set $A$ of integers is defined by

$$d(A) = \lim_{x \to \infty} \frac{A(x)}{x},$$

if this limit exists. The lower and upper (asymptotic) densities are the corresponding lower and upper limits, respectively:

$$d(A) = \lim_{x \to \infty} \inf A(x)/x, \quad \overline{d}(A) = \lim_{x \to \infty} \sup A(x)/x.$$  

**Definition 4.0.3.** A set $A \subset \mathbb{N}_0$ is an additive basis of order $h$ if $hA = \mathbb{N}_0$, that is, every positive integer can be expressed as a sum of $h$ integers from $A$.

A set $A \subset \mathbb{N}_0$ is an asymptotic basis of order $h$, if every sufficiently large integer can be expressed as a sum of $h$ integers from $A$, that is, $\mathbb{N}_0 \setminus hA$ is finite.

The smallest such integer $h$ is called the exact order or exact asymptotic order of $A$, respectively.

So the proper wording is that the set $P$ of primes forms an asymptotic basis. To be a basis, a set must contain 0 and 1. Schnirelmann established that integers that can be written as a sum of two primes have positive density, that is $\underline{d}(2P) > 0$, and that every set having positive density is a basis.
Definition 4.0.4. The Schnirelmann density of a set $A$ of integers is the number
\[ \sigma(A) = \inf_{n \in \mathbb{N}} \frac{A(n)}{n}. \]

Asymptotic density is translation invariant and it is invariant under the exclusion or inclusion of finitely many elements; Schnirelmann density does not have either property, in fact, $\sigma(A) = 0$ if $1 \notin A$.

Theorem 4.0.5. If $0 \in A$ and $\sigma(A) > 0$, then $A$ is a basis.

Theorem 4.0.6. Let $A$ and $B$ be sets of non-negative integers with positive Schnirelmann densities $\sigma(A) = \alpha$ and $\sigma(B) = \beta$, respectively. If $0 \in A \cup B$, then
\[ \sigma(A + B) \geq \alpha + \beta - \alpha \beta. \]

Theorem 4.0.7. Let $A$ and $B$ be sets of non-negative integers with positive Schnirelmann densities $\sigma(A) = \alpha$ and $\sigma(B) = \beta$, respectively. If $\alpha + \beta \geq 1$ and $0 \in A \cup B$, then $A + B \supset \mathbb{N}$.

Theorem 4.0.8. (Mann) If $0 \in A \cap B$, then
\[ \sigma(A + B) \geq \min(1, \sigma(A) + \sigma(B)). \]

Corollary 4.0.9. If $0 \in A$ and $\sigma A = \alpha > 0$, then $A$ is a basis of order $\leq 1/\alpha$.

Definition 4.0.10. The joint (Schnirelmann) density of the sets $A_1, \ldots, A_k$ is defined by
\[ \sigma(A_1, \ldots, A_k) = \inf_n \frac{A_1(n) + \cdots + A_k(n)}{n}. \]

Theorem 4.0.11. If $0 \in A \cap B$, then
\[ \sigma(A + B) \geq \min(1, \sigma(A, B)). \]

Theorem 4.0.12. Let $0 \leq \gamma \leq 1$, let $n$ be a positive integer and let $A, B$ be sets such that $0 \in A \cap B$. Put $C = A + B$. If
\[ A(k) + B(k) \geq \gamma k \text{ for } 1 \leq k \leq n, \]
then
\[ C(k) \geq \gamma k \text{ for } 1 \leq k \leq n. \]

Theorem 4.0.13. Let $0 \leq \gamma \leq 1$, $0 \leq \delta \leq 1 - \gamma$, let $n$ be a positive integer and let $A, B$ be sets such that $0 \in A \cap B$. Put $C = A + B$. If
\[ A(k) + B(k) \geq \gamma k - \delta \text{ for } 1 \leq k \leq n, \]
then
\[ C(k) \geq \gamma k - \delta \text{ for } 1 \leq k \leq n. \]
Theorem 4.0.14. (Van der Corput) Let $0 \leq \gamma \leq 1$, let $n$ be a positive integer and let $A, B$ be sets such that $0 \in A \cap B$. Put $C = A + B$. If 

$$1 + A(k) + B(k) \geq \gamma(k + 1) \text{ for } 1 \leq k \leq n,$$

then 

$$1 + C(k) \geq \gamma(k + 1) \text{ for } 1 \leq k \leq n.$$

By writing 

$$S(\alpha, \beta) = \inf \{\sigma(A + B) : \sigma(A) = \alpha, \sigma(B) = \beta, 0 \in A\}$$

and 

$$M(\alpha, \beta) = \inf \{\sigma(A + B) : \sigma(A) = \alpha, \sigma(B) = \beta, 0 \in A \cap B\},$$

we can restate Schnirelmann’s, Mann’s and Lepson’s results as 

$$\alpha + \beta - \alpha \beta \leq S(\alpha, \beta) \leq M(\alpha, \beta) = \min(\alpha + \beta, 1).$$

Theorem 4.0.15. For all $\alpha, \beta$ we have 

$$S(\alpha, \beta) = \inf_{n \geq 0} \frac{[\alpha n] + [\beta(n + 1)]}{n + 1}.$$

Definition 4.0.16. Let $\alpha, \beta$ be positive real numbers satisfying $\alpha + \beta \leq 1$. We call $(\alpha, \beta)$ a Schnirelmann pair if $S(\alpha, \beta) = \alpha + \beta - \alpha \beta$, and a Mann pair if $S(\alpha, \beta) = \alpha + \beta$.

Theorem 4.0.17. The numbers $(\alpha, \beta)$ form a Schnirelmann pair if and only if they can be expressed as 

$$\alpha = \frac{k}{n}, \quad \beta = \frac{1}{n + 1}$$

with certain integers $n \geq 2$ and $1 \leq k \leq n - 1$.

Theorem 4.0.18. If $\alpha$ and $\beta$ form a Mann pair, then they are either both rational or both irrational. A pair of rational numbers, say $\alpha = p/q, \beta = r/s$, is a Mann pair if and only if they satisfy 

$$\{\alpha(1 - n)\} + \{-\beta n\} \geq \alpha$$

for every integer $1 \leq n \leq \text{lcm}[q, s]$. A pair of irrational numbers is a Mann pair if and only if there are integers $k, l, m$ such that 

$$\alpha k + \beta l = m \quad 0 < k < 1/\alpha, 0 \leq l < 1/\alpha.$$
Theorem 4.0.19. \textit{(Kneser)} Let $A$ and $B$ be sets of positive integers. Either
\[
d(A + B) \geq d(A) + d(B),
\]
or there exists positive integers $q, k, l$ such that $q \geq k + l - 1$ and
i) $A$ is contained in $k$ residue classes modulo $q$,
ii) $B$ is contained in $l$ residue classes modulo $q$,
iii) $A + B$ is equal to $k + l - 1$ residue classes modulo $q$ except a finite set.

Sometimes a density increment occurs also when we add a set of density 0. Hinchin proved that for the set $Q$ of non-negative squares we have $\sigma(A + Q) > \sigma(A)$ whenever $0 < \sigma(A) < 1$. Later, Erdős proved that every basis has this property.

Theorem 4.0.20. Let $B \subset \mathbb{Z}$ be a basis of order $k$ and let $A \subset \mathbb{Z}$. Then
\[
\sigma(A + B) \geq \sigma(A) + \frac{\sigma(A)(1 - \sigma(A))}{2k}.
\]

Theorem 4.0.21. Let $B \subset \mathbb{Z}$ be an asymptotic basis of order $k$ and let $A \subset \mathbb{Z}$. Then
\[
d(A + B) \geq d(A) + \frac{d(A)(1 - d(A))}{2k}.
\]

Theorem 4.0.22. If $A, B \subset \mathbb{N}_0, 0 \in B$, then
\[
\sigma(A + B) \geq \sigma(A)^{1 - \frac{1}{k}} \sigma(kB)^\frac{1}{k}
\]In particular, if $kB = \mathbb{N}_0$, then $\sigma(A + B) \geq \sigma(A)^{1 - \frac{1}{k}}$.

Theorem 4.0.23. Let $A, B \subset \mathbb{Z}$ and let $k$ be a positive integer. We have
\[
d(A + B) \geq d(A)^{1 - \frac{1}{k}} \sigma(kB)^\frac{1}{k}.
\]

Let $Q$ be the set of squares: $Q = \{n^2, n \in \mathbb{N}_0\}$. They form a basis of order 4, that is, $4Q = \mathbb{N}_0$. We also know that $3Q$ contains all numbers except those of the form $4^a(8b - 1)$, for some $a$ and $b$. This implies that the Schnirelmann density of the set of threefold sums of squares is positive: $\sigma(3Q) > 0$.

Theorem 4.0.24. \textit{(Plünnecke)} Let $A$ be a subset of the integers with $\sigma(A) = \alpha$, and $Q$ the set of squares. We have
\[
\sigma(A + Q) \geq c\alpha^{1/2}
\]for some absolute constant $c > 0$. 24
Theorem 4.0.25. For every $\epsilon > 0$ there exists a constant $c_\epsilon$ depending on $\epsilon$ such that if $d(A) = \alpha$, then

$$d(A + Q) \geq c_\epsilon \alpha^\epsilon.$$ 

Theorem 4.0.26. Let $A$ be a subset of integers. There is a positive constant $c$ with the following properties (valid for $q$ sufficiently large).

i) If $\sigma(A) = 1/q$, then $\sigma(A + P') \geq \frac{c}{\log q}$.

ii) If $d(A) = 1/q$, then $d(A + P) \geq \frac{c}{\log \log q}$.

Definition 4.0.27. We say that $B$ is an **essential component** if $B$ is such that $\sigma(A + B) > \sigma(A)$ for every $0 < \sigma(A) < 1$.

Some examples are sets of positive density, and bases. Clearly if $B$ is a basis of order $k$, it must satisfy $B(x) > x^{1/k}$, hence a set such that $B(x) = O(x^\epsilon)$ for every positive $\epsilon$ cannot be a basis.

Theorem 4.0.28. i) For every $\epsilon > 0$ there exists an essential component with $B(n) < c(\log n)^{1+\epsilon}$.

ii) There is no essential component $B$ with $B(n) < c(\log n)^{1+o(1)}$. 


Chapter 5

Measure and Topology

Measure is a close analogue of cardinality, the same questions asked for finite sets can be formulated for measures of sets of reals or in $\mathbb{R}^d$. The following is an analogue of the Cauchy-Davenport inequality. We consider subsets of $[0, 1)$, addition is meant modulo 1. Assume every set mentioned is compact or open, with Lebesgue measure denoted by $\mu$.

Theorem 5.0.1. For $A, B \subset [0, 1)$ we have

$$\mu(A + B) \geq \min(1, \mu(A) + \mu(B)).$$

Let $G$ be a locally compact topological group. If $G$ is compact, or commutative, it has an invariant measure $\mu$, called Haar measure. Invariance means that we have

$$\mu(A + x) = \mu(x + A) = \mu(A)$$

for every measurable set and every $x \in G$. If an invariant Haar measure exists, the group is called unimodular.

Theorem 5.0.2. Let $G$ be a compact, connected group, $A, B \subset G$ measurable sets such that $A + B$ is also measurable. We have

$$\mu(A + B) \geq \min(\mu(A) + \mu(B), \mu(G)).$$

Theorem 5.0.3. Let $G$ be a locally compact, non-compact group which does not have any proper compact-open subgroup. Let $A, B \subset G$ be measurable sets such that $A + B$ is also measurable. We have

$$\mu(A + B) \geq \mu(A) + \mu(B).$$
Definition 5.0.4. Let $G$ be a group with a Haar measure $\mu$, and $B \subset G$ a measurable set. We define the impact function of $B$ analogously to the finite situation
\[ \xi_A(x) = \inf \{ \mu(A + B) : B \subset G, \mu(B) = x \}. \]

Theorem 5.0.5. If $G$ does not have any proper compact-open subgroup, then $\xi$ is a continuous concave function on its whole domain.

Another curious property of the impact function is its symmetry. To avoid an exception we redefine the impact function at 0 by continuity: $\xi(0) = \lim_{x \to 0^+} \xi(x)$.

Theorem 5.0.6. Assume that $G$ is compact, commutative and connected. The smallest value of $x$ for which $\xi(x) = \mu(G)$ is $x = \mu(G) - \xi(0)$. The graph of $\xi(x)$ on the interval $[0, \mu(G) - \xi(0)]$ is symmetric to the line $x + y = \mu(G)$.

Let $A, B$ be Borel sets in $\mathbb{R}^d$. The Brunn-Minkowski inequality estimates $\mu(A + B)$ in a natural way, with equality if $A$ and $B$ are homothetic convex sets. This can be expressed in terms of the impact function as
\[ \xi_B(a) \geq (a^{1/d} + \mu(B)^{1/d})^d, \]
and this is the best possible estimate in terms of $\mu(B)$ only. To measure the degree of non-convexity, one can try to use the measure of the convex hull beside the measure of the set. This is analogous to the hull volume, and it is sufficient to describe the asymptotic behavior of $\xi$.

Theorem 5.0.7. For every bounded Borel set $B \subset \mathbb{R}^d$ of positive measure we have
\[ \lim_{a \to \infty} \xi_B(a)^{1/d} - a^{1/d} = \mu(\text{conv } B)^{1/d}. \]

Theorem 5.0.8. Let $\mu(B) = b, \mu(\text{conv } B) = v$. We have
\[ \xi_B(a)^{1/d} \geq a^{1/d} + v^{1/d} \left(1 - c(v/b)^{1/2}(v/a)^{1/(2d)}\right), \]
\[ \xi_B(a) \geq a + dv^{1/d}a^{-1/d} \left(1 - c(v/b)^{1/2}(v/a)^{1/(2d)}\right) \]
with a suitable positive constant $c$ depending on $d$.

Theorem 5.0.9. Let $B \subset \mathbb{R}$, and write $\mu(B) = b, \mu(\text{conv } B) = v$. If
\[ a \geq \frac{v(v - b)}{2b} + \frac{b(v/b)(1 - \{v/b\})}{2}, \]
then \( \xi_B(a) = a + v \). If the above inequality does not hold, then let \( k \) be the unique positive integer satisfying

\[
\frac{k(k-1)}{2} \leq \frac{a}{b} < \frac{k(k+1)}{2},
\]

and define \( \delta \) by

\[
\frac{a}{b} = \frac{k(k-1)}{2} + \delta k.
\]

We have

\[
\xi_B(a) \geq a + \frac{(k + \delta)}{b},
\]

and equality holds if \( B = [0, b] \cup \{v\} \).

**Theorem 5.0.10.** Let \( B \subset \mathbb{R} \), and write \( \mu(B) = b, \mu(\text{conv} B) = v \). We have

\[
\xi_B(a) \geq \min\left(a + v, (\sqrt{a} + \sqrt{b/2})^2\right).
\]

**Corollary 5.0.11.** If \( a \leq b \), then we have

\[
\mu(A + B) \geq \min(2a + b, a + v).
\]

**Definition 5.0.12.** Let \( G \) be a group and \( T \) a topology on it. We say that \( (G, T) \) is a **topological group**, if addition and subtraction are continuous in \( T \); that is, \( f(x, y) = x - y \) is jointly continuous in both variables. It is a **semitopological group**, if \( x - y \) is continuous in each variable separately.

**Definition 5.0.13.** A set \( A \) in a group \( G \) is **syndetic**, if there are finitely many elements \( x_1, \ldots, x_\kappa \in G \) such that

\[
\bigcup (A + x_i) = G.
\]

**Theorem 5.0.14.** (Bogolyubov) If \( A \subset \mathbb{Z} \) is a syndetic set, then \( 2A - 2A \) contains a Bohr set (in other words, it is a neighborhood of 0 in the Bohr topology).

**Definition 5.0.15.** The **lower** and **upper Banach densities** of a set \( A \) of integers are defined by

\[
d_\ast(A) = \lim_{n \to \infty} \min_x \frac{|A \cup [x+1, x+n]|}{n},
\]

\[
d^\ast(A) = \lim_{n \to \infty} \max_x \frac{|A \cup [x+1, x+n]|}{n}.
\]

**Theorem 5.0.16.** (Bogolyubov) If \( d^\ast(A) > 0 \), then there exist \( \alpha_1, \ldots, \alpha_\kappa \) and \( \epsilon > 0 \), with \( \kappa \) and \( \epsilon \) depending only on \( d^\ast(A) > 0 \), such that \( B(\alpha_1, \ldots, \alpha_\kappa, \epsilon) \subset 2A - 2A \).

**Theorem 5.0.17.** Let \( A \) be a set of integers with \( d^\ast(A) > 0 \), and let \( r, s, t \) be integers such that \( r + s + t = 0 \). The set \( r \cdot A + r \cdot A + t \cdot A \) is a Bohr neighborhood of 0. In particular, the set \( 2A - 2 \cdot A = A + A - 2 \cdot A \) is a Bohr neighborhood of 0.
Theorem 5.0.18. Assume $d^*(A) > 0$. Then there is an $A' \subset \mathbb{N}$ such that $d(A') > 0$ and $A' - A' \subset A - A$.

Theorem 5.0.19. There exists an $A$ with $d(A) > 0$ such that there is no $A'$, with $d_*(A) > 0$ and $A' - A' \subset A - A$. Consequently, $A - A$ is not a Bohr neighborhood of 0.

Theorem 5.0.20. If $d^*(A) > 0$, then there exists a $B = B(\alpha_1, \ldots, \alpha_k, \epsilon)$ such that $d((A - A) \setminus B) = 0$.

Definition 5.0.21. We say that $V \subset \mathbb{Z}$ is a neighborhood of 0 in the difference set topology if there exists a set $A$ with $d^*(A) > 0$ such that $A - A \subset V$. $V'$ is said to be a neighborhood of $n \in \mathbb{Z}$ if $V = V' - n$ is a neighborhood of 0.

Definition 5.0.22. The **syndetic difference topology** is defined similarly to the difference set topology, but now we say that $V \subset \mathbb{Z}$ is a neighborhood of 0 if there exists an $A$ with $d_*(A) > 0$ such that $A - A \subset V$.

Definition 5.0.23. The **combinatorial difference topology** is defined as follows. Let $A_1, \ldots, A_k$ be subsets of the integers such that $\mathbb{Z} = \bigcup_{i=1}^n A_i$, then $\bigcup_i (A_i - A_i)$ is a neighborhood of 0.