Chapter 2
Introduction to Sumsets

This chapter introduces the first main branch of study in this course: sumsets.

2.1 Sumsets

In this course, we study the structure theory for 'additive' objects. Our first principal objects of study are subsets A and B of an abelian group G and their *sumset*:

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

Our summands $A,\ B \subseteq G$ will generally be finite and nonempty, though we will expand our interests to include infinite summands at times. When there are more than two summands, we denote the sumset of $A_1, \ldots, A_n \subseteq G$ by

$$\sum_{i=1}^{n} A_i = A_1 + A_2 + \cdots + A_n = \left\{ \sum_{i=1}^{n} a_i : a_i \in A_i \right\},$$

and for multiple summands of the same set, we use the abbreviation

$$kA = \underbrace{A + A + \cdots + A}_{k}.$$

This should not be confused with the dilation of a set, which is instead denoted

$$k \cdot A = \{ka : a \in A\}.$$

More generally, if g is an element and A is a set such that ag is defined for all $a \in A$, then we set

$$A \cdot g = \{ag : a \in A\}.$$

For purposes of notational simplicity, we often associate a single element $g \in G$ with the singleton set $\{g\}$; thus, for example, the translation of a set is denoted $b + B = \{b\} + B$. Likewise, when we need to talk about subtracting sets, we use

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

D.J. Grynkiewicz, *Structural Additive Theory*, Developments in Mathematics 30,
DOI 10.1007/978-3-319-00416-7_2, © Springer International Publishing Switzerland 2013

to denote the *difference set* of A and B, which is the same as adding A and $-B := \{-b : b \in B\}$. Of related interest is what is sometimes known as the *restricted sumset*

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

We adopt the convention that both the setminus and intersection operations take precedence over addition, so

$$A + B \setminus C = A + (B \setminus C) \text{ and } A + B \cap C = A + (B \cap C).$$

Generally, we will be very interested in the cardinality $|A+B|$, which is translation invariant:

$$|x + A| = |A|$$
$$|x + A + B| = |A + B|.$$

Most of our problems will be translation invariant, i.e., there will no difference between considering the set A or the set $x + A$, and so we will often w.l.o.g. (without loss of generality) translate the sets as is convenient. To emphasize this, we use the abbreviation

$$\langle A\rangle_* := \langle A - A\rangle = \langle -a_0 + A\rangle, \qquad \text{where } a_0 \in A,$$

for the *translation invariant subgroup generated* by A, alternatively described as *the subgroup generated up to translation by* A. Note that

$$a_0 + \langle -a_0 + A\rangle = a_0 + \langle A\rangle_* \quad \text{is the minimal coset containing } A, \quad \text{for any } a_0 \in A,$$

so that it does not matter which $a_0 \in A$ is chosen above. Of course, we will usually be able to translate our sets so that they contain zero, in which case $\langle A\rangle_* = \langle A\rangle$ (when $0 \in A$). Likewise we write $\gcd^*(A) := \gcd(A - A) = \gcd(A - a_0)$, where $a_0 \in A$ and gcd is the greatest common divisor, for the *translation invariant gcd* of $A \subseteq \mathbb{Z}$. Note the definition of $\gcd^*$ is independent of $a_0 \in A$.

The most common reoccurring theme is the idea that if $|A + B|$ is 'small', then A, B and $A + B$ must have 'structure'. We will throughout the course see many different theorems that exemplify this general philosophy.

2.2 Infinite Summands

Though our main interest is the study of sumsets of *finite* sets, it will often be very convenient to extend our theory to include *infinite* sets as well; we will later see some simple examples showing the importance of this added flexibility. If $|A| = \infty$, then $|A + B| = \infty$, which might at first appear to be a very large cardinality and so not subject to the above paradigm regarding small sumsets. However, in such case, we can instead consider $|(A + B) \setminus (A + b)|$ for $b \in B$, which can be finite even when $|A|$ is infinite. Indeed, if $B = \{b_1, \ldots, b_n\}$, then one can view the sumset $A + B$ as being constructed by taking the translate $A + b_1$, which contributes $|A|$ elements to $|A + B|$, and then seeing how many new elements, outside $A + b_1$, can be obtained from among the remaining translates $A + b_i$, for $i \in [2, n]$. Under this view, we can interpret the bound $|A + B| \geq |A| + |B| - 1$ as saying that each element of B contributes one element to $|A + B|$ except for the first, which is instead used up translating the elements from A to $A + B$. Viewed in this way, the finiteness of the first set A seems less consequential, and in many cases not necessary for formulating a sumset question.

The following notational convention, regarding how certain infinities should cancel, will allow us to simultaneously phrase a result in the natural way for the case when both sets are finite, while at the same time including the important extension allowing infinite sets:

$$|A+B|-|A| := \sup\{|(A+B)\setminus(A+b)| : b \in B\} \in \mathbb{N}_0 \cup \{\infty\}. \tag{2.1}$$

We allow both A and B to be infinite in the above definition, though will we soon see that most of the sumset questions we are interested in are rather degenerate when more than one subset is infinite. As a consequence of this definition, if $|A| = \infty$, $|B| < \infty$ and $r \in \mathbb{Z} \cup \{\infty\}$, then

$$|A+B| \le |A| + r \quad \text{implies} \quad |(A+B)\setminus(b+A)| \le r \quad \text{for all } b \in B, \quad \text{and}$$
$$|A+B| \ge |A| + r \quad \text{implies} \quad |(A+B)\setminus(b_0+A)| \ge r \quad \text{for some } b_0 \in B,$$

where $b_0 \in B$ can be any element attaining the maximum in the definition of $|A+B|-|A|$. Note that

$$|A+B|-|A| = \infty \quad \text{when } |A| < \infty \text{ and } |B| = \infty.$$

Since $A + b \subseteq A + B$ for $b \in B$, the definition in (2.1) agrees with the usual interpretation of $|A+B|-|A|$ when both sets are finite. In general, we can have

$$|(A+B)\setminus(b+A)| \ne |(A+B)\setminus(b'+A)| \quad \text{for distinct } b, b' \in B.$$

However, the prototypical sets A motivating our partial extension to the infinite will be *cofinite*, meaning $|(a_0 + \langle A\rangle_*)\setminus A| < \infty$, where $a_0 \in A$. If we translate A to include zero, this condition takes the simpler form $|\langle A\rangle \setminus A| < \infty$. For such sets, we will later see that it does not matter which $b \in B$ is used to define $|A+B|-|A|$. Of course, the above conventions also apply to collections of more than two sets $A_1, \dots, A_n$ simply by interpreting $|\sum_{i=1}^n A_i| - |A_j|$ as $|A_j + (\sum_{\substack{i=1\\ i\ne j}}^n A_i)| - |A_j|$.

Finally, as a matter of convention, if we write $|\sum_{i=1}^n A_i| \ge \sum_{i=1}^n |A_i| + r$, where $r \in \mathbb{Z} \cup \{\infty\}$, then we mean

$$\left|\sum_{i=1}^n A_i\right| - |A_j| \ge \sum_{\substack{i=1\\ i\ne j}}^n |A_i| + r \quad \text{for all } j \in [1,n],$$

i.e., a lower bound on the sumset holds under any interpretation of how to cancel infinite quantities. However, for upper bounds $|\sum_{i=1}^n A_i| \le \sum_{i=1}^n |A_i| + r$, we assume only that

$$\left|\sum_{i=1}^n A_i\right| - |A_j| \le \sum_{\substack{i=1\\ i\ne j}}^n |A_i| + r \quad \text{for some } j \in [1,n],$$

so that $|\sum_{i=1}^n A_i| \ge \sum_{i=1}^n |A_i| + r$ failing to hold is equivalent to $|\sum_{i=1}^n A_i| < \sum_{i=1}^n |A_i| + r$ holding. Since we will soon reduce consideration to when only one A_i is infinite, the $j \in [1,n]$ for which this holds will then be the unique A_j with $|A_j| = \infty$.

2.3 Multiplicity of Representation in a Sumset

At times, it will be important to consider how many representations an element $x \in A + B$ has as a sum $x = a + b$ with $a \in A$ and $b \in B$. We let

$$\mathsf{r}_{A,B}(x) = |\{(a,b) \in A \times B : a + b = x\}|$$

denote the number of such representations, so that $\mathsf{r}_{A,B}(x) \geq 1$ if and only if $x \in A + B$. If $A = B$, then 'most' elements $x \in 2A$ have $\mathsf{r}_{A,A}(x) \geq 2$, since $x + y = y + x$ provides two representations of the same element any time x, $y \in A$ are distinct; thus only elements from $2 \cdot A$ are possible candidates to be unique expression elements in $2A$. The representation number can be alternatively defined by

$$\mathsf{r}_{A,B}(x) = |(x - A) \cap B| = |(x - B) \cap A|.$$

Just note that if $a + b = x$, where $a \in A$ and $b \in B$, then $b = x - a$ is an element of $(x - A) \cap B$, and likewise any element $b = x - a \in (x - A) \cap B$ gives rise to an expression $a + b = x$. Thus $(x - A) \cap B$ is precisely the subset of all $b \in B$ for which there is some $a \in A$ that can be added to b to obtain x, and likewise for $(x - B) \cap A$. Note, for each $b \in G$, there is precisely one element $g \in G$ such that $g + b = x$; thus there is at most one way to represent x as a sum using $b \in B$, and the question is whether this one particular element does or does not live in A.

2.4 X-Component Decompositions

Let $X \subseteq G$ be a nonempty subset. If $A' \subseteq G$ cannot be written as the disjoint union $A' = A'_1 \uplus A'_2$ of two nonempty subsets A'_1 and A'_2 such that $A'_1 + X$ and $A'_2 + X$ are also disjoint, then A' is called *X-connected*. Any subset A has a unique decomposition $A = \biguplus_{i=1}^{n} A_i$ with $A_i + X$ and $A_j + X$ disjoint for $i \neq j$ and each A_i a nonempty X-connected subset of A. Indeed, one can simply define a graph whose vertices are the elements of A with an edge between two elements a, $a' \in A$ when $(a + X) \cap (a' + X) \neq \emptyset$, and then the A_i are simply the vertices of A from the same connected component in this graph. We call this the *X-component decomposition of A*, and the individuals subsets A_i are then each *X-components*. Note that the X-component decomposition of A is unaffected by translating X, so we generally assume $0 \in X$. The two most typical sets X considered are taking $X = H$ to be a subgroup of G and taking $X = \{0, d\}$ with $d \neq 0$. We discuss these in detail below.

2.5 Arithmetic Progressions

An *arithmetic progression* with *difference* d, in a abelian group G, is just a set of the form $A = \{a_0 + id : i \in I\}$, where a_0, $d \in G$, d is nonzero, and $I \subseteq \mathbb{Z}$ is either an interval in $\mathbb{Z}$ or the *complement of an interval* in $\mathbb{Z}$, so $I = [a, b]$, $I = (-\infty, b]$, $I = [a, \infty)$ or $I = (-\infty, a] \cup [b, \infty)$, where a, $b \in \mathbb{Z}$ with $a \leq b$ and $|I| \in [1, \infty]$. It is extremely important to note that, under this definition, $I = (-\infty, a] \cup [b, \infty) \subseteq \mathbb{Z}$ is an arithmetic progression in $\mathbb{Z}$. These sets can be thought of as arithmetic progressions which pass through the point at infinity. We include them as arithmetic progressions since, from an additive point of view, they exhibit much of the same behavior as more conventional arithmetic progressions, and since excluding them from being arithmetic progressions would needlessly complicate the statement of several theorems. This definition also ensures that the complement of an arithmetic progression inside the minimal coset containing it is again an arithmetic progression (or the empty set).

As we will later see, arithmetic progressions play an extremely important role in describing the structure of sets with small sumset, so important that we will spend some time exploring their basic additive properties. Note that, by our definition, any H-coset, where $H = \langle d \rangle$, is an example of an arithmetic progression A with difference d. If $a \in A$ but $a - d \notin A$, then a is the *first term* in the progression, and if $a \in A$ but $a + d \notin A$, then a is the *last term* in the progression; observe there is at most one first term and at most one last term in an arith-

metic progression with difference d. The *length* of the progression is just the number of distinct terms. Note that if B is also an arithmetic progression with difference d, then $A+B$ will be another arithmetic progression with difference d and length $|A+B| = \min\{|\langle d\rangle|,\ |A|+|B|-1\}$; of course, the length of an arithmetic progression with difference d cannot exceed $|\langle d\rangle|$. If $|A|+|B|-1 \le |\langle d\rangle|,\ |B| \le |A| < \infty$ and we arrange the terms of $A+B = \{c_1, \ldots, c_{|A|+|B|-1}\}$ in the order given by d, starting with the first term c_1 of the arithmetic progression and ending with the last term $c_{|A|+|B|-1}$, then the corresponding sequence of representation numbers, $\mathsf{r}_{A,B}(c_1), \ldots, \mathsf{r}_{A,B}(c_{|A|+|B|-1})$, takes the form

$$1, 2, \ldots, |B|-1, \underbrace{|B|, |B|, \ldots, |B|}_{|A|-|B|+1}, |B|-1, \ldots, 2, 1. \tag{2.2}$$

Naturally, any arithmetic progression with difference d is also an arithmetic progression with difference $-d$, the only difference being that first and last terms swap position.

If $X = \{0, d\}$, and $A = \biguplus_{i\in I} A'_i$ is the X-component decomposition of A, then each finite A'_i is a maximal arithmetic progression with difference d contained in A which will have a first and last term if $|A'_i| < \mathrm{ord}(d)$, and each infinite A'_i is simply an arithmetic progression with difference d. However, for each $a \in A$, there can be at most two sets A'_i and A'_j that are infinite and contained in the same $\langle d\rangle$-coset. By our convention above concerning infinite arithmetic progressions, their union is then still an arithmetic progression. Thus, replacing any such pairs of infinite A'_i and A'_j from the same $\langle d\rangle$-coset with $A'_i \cup A'_j$, we obtain a decomposition

$$A = \biguplus_{i\in I} A_i, \quad \text{with each } A_i \text{ a maximal arithmetic progression of difference } d \text{ contained in } A,$$

where the maximal refers to containment in A. We call this the *d-progression decomposition* of A.

2.6 H-Coset Decompositions

When $X = H$ is a subgroup of G, then the X-component decomposition of a set $A \subseteq G$,

$$A = \biguplus_{\beta\in I} A_\beta, \qquad \text{where } A_\beta = (\beta + H) \cap A \neq \emptyset \text{ and } H \le G,$$

will be called the *H-coset decomposition* of A. Each set A_β is referred to as an *H-coset slice*. Note that if $\langle d\rangle \le H$, where $d \in G$ is nonzero, then every A_i from the d-progression decomposition of A lies wholly inside some H-coset, and thus wholly inside some A_β from the H-coset decomposition of A. Also, $|\phi_H(A)| = |I|$.

2.7 Induction on Well-Ordered Sets

Next we pause to say a few words about induction, which will be a common feature of many proofs in this course. However, the inductive arguments encountered may be slightly more sophisticated than those found in many other parts of mathematics. Indeed, so called double—even triple—inductions will be fairly commonplace. Now recall that induction can be performed on any well-ordered set X, that is, so long as any nonempty subset of X has a minimal element, then we can proceed by induction using the order on X. To be concrete, let us

describe the framework for a typical triple induction, from which the workings of higher order inductions can be readily extrapolated. For this simplified setup, we have three parameters, say α, β and γ, which take integer values or may be equal to $\pm\infty$; for instance, the cardinality of a set we are trying to prove something about could be one of these parameters. Now the triple (α, β, γ) lies in the cartesian product $(\mathbb{Z} \cup \{\pm\infty\})^3$, which can be ordered using the lexicographic (dictionary) order, that is, $(x, y, z) \le (x', y', z')$ when either $x < x'$, or $x = x'$ and $y < y'$, or $x = x'$, $y = y'$ and $z \le z'$. Thus, when we proceed by induction on the triple of parameters (α, β, γ), we first (at least typically) verify what we desire to prove for various "base cases", namely, special values of the parameter triple (α, β, γ), then consider an arbitrary situation with parameters (α, β, γ) outside any base case, and finally assume the theorem or statement true whenever we have parameters $(\alpha', \beta', \gamma') < (\alpha, \beta, \gamma)$ (the inductive step). Once the theorem is proved under this setup for (α, β, γ), the theorem follows by induction, though usually there cannot be any possible parameter triple (α, β, γ) strictly less than the triple of a base case except that of another base case, i.e., the base cases need to cover all minimal values of the parameter triple. This is because the argument from the inductive step, showing the statement is true for (α, β, γ) provided it is true for all parameters $(\alpha', \beta', \gamma') < (\alpha, \beta, \gamma)$, usually (though not always) requires that there actually *exist* some parameter $(\alpha', \beta', \gamma') < (\alpha, \beta, \gamma)$. In essence, an inductive argument describes a recursive process by which one iteratively reduces the problem from an arbitrary situation to a special situation which can be solved directly (i.e., a base case). To see that an inductive setup is actually valid, it can be helpful to visualize an arbitrary point (α, β, γ) and trace in one's mind the recursive path leading back to one of the base cases. On the rare occasion that the argument establishing the inductive step also works for the base case, in which case doing the base case separately is not needed, we will instead structure the proof by considering a minimal counterexample, which is logically equivalent but without the expectation of a separate base case. Note, if the parameters are known to satisfy (say) $\alpha \ge \alpha_0$, $\beta \ge f(\alpha)$ and $\gamma \ge g(\alpha, \beta)$, for some constant α_0, integer valued function f dependent only on α, and integer valued function g dependent only on α and β, then it is sufficient to handle only the case when $\alpha = \alpha_0$ as base case, as the only minimal point under these circumstances is $(\alpha_0,\ f(\alpha_0),\ g(\alpha_0,\ f(\alpha_0)))$.

2.8 Freiman Homomorphisms

When studying the behavior of sumsets $A + B$ with $A,\ B \subseteq G$, we are really only concerned with the additive structure and relationship between A and B, and such structure may be identical to that of a pair of subsets $A',\ B' \subseteq G'$ of a completely different abelian group G'. Thus it is useful to have a notion of additive isomorphism. As such, we define a *Freiman isomorphism* to be a pair of maps $\psi_A : A \to A' \subseteq G'$ and $\psi_B : B \to B' \subseteq G'$ such that

$$\psi_A(a) + \psi_B(b) = \psi_A(a') + \psi_B(b') \quad \text{if and only if} \quad a + b = a' + b',$$

for $a,\ a' \in A$ and $b,\ b' \in B$. Note that the above condition forces the maps to both be bijective (as otherwise we obtain a contradiction of the form $\psi_A(a) + \psi_B(b) = \psi_A(a') + \psi_B(b)$ but $a + b \ne a' + b$). If only $a + b = a' + b'$ implies $\psi_A(a) + \psi_B(b) = \psi_A(a') + \psi_B(b')$, then we call the pair of maps (ψ_A, ψ_B) a *Freiman homomorphism*.

Suppose $\psi_A : A \to G'$ and $\psi_B : B \to G'$ form a Freiman homomorphism of the pair $A,\ B \subseteq G$. Then, for any $x \in A + B$, say $x = a + b$ with $a \in A$ and $b \in B$, we can define

$$\psi_{A+B}(x) = \psi_{A+B}(a + b) := \psi_A(a) + \psi_B(b),$$

which, by the definition of a Freiman homomorphism, is well-defined and independent of the choice of $a \in A$ and $b \in B$ summing to x. Thus a Freiman homomorphism gives rise to an additive map $\psi_{A+B} : A + B \to G'$ on the sumset $A + B$ and not just the individual sets A and B.

In fact, the requirement $\psi_{A+B} = \psi_A + \psi_B$, where the lack of inputs is taken to mean this holds true for all values for which this is defined, is easily seen to be an equivalent restatement of the definition of a Freiman homomorphism, with the case of isomorphism corresponding to when $\psi_{A+B} : A + B \to G'$ is injective. We will usually drop the subset subscripts on ψ when the domain is clear, thus associating the collection of maps forming the Freiman homomorphism with the single object ψ.

More generally, if we have a collections of nonempty subsets $A_1, \dots, A_n \subseteq G$ and G' is another abelian group, then a Freiman homomorphism ψ of $A_1 + \cdots + A_n$ is a collection of maps (subscripts often suppressed) $\psi_I : \sum_{i\in I} A_i \to G'$, one for each of the $2^n - 1$ nonempty subsets $I \subseteq [1, n]$, such that

$$\psi_{I\uplus J}\left(\sum_{i\in I} a_i + \sum_{j\in J} a_j\right) = \psi_I\left(\sum_{i\in I} a_i\right) + \psi_J\left(\sum_{j\in J} a_j\right), \text{ where } a_i \in A_i \text{ and } a_j \in A_j,$$

whenever $I, J \subseteq [1, n]$ are disjoint and nonempty. It is an isomorphism when $\psi_{[1,n]}$ is injective on $A_1 + \cdots + A_n$, which, as in the 2-summands case, implies ψ_I is injective for all smaller subsets $I \subseteq [1, n]$, including each A_i. From the definition, it is immediate that each $\psi_I : \sum_{i\in I} A_i \to G'$ is a Freiman homomorphism, for $I \subseteq [1, n]$, which must be injective if $\psi_{[1,n]}$ is injective.

Iterating the additive property of a Freiman isomorphism (and suppressing subscripts), it follows that

$$\psi(a_1 + \cdots + a_n) = \psi(a_1) + \cdots + \psi(a_n), \quad \text{where } a_i \in A_i,$$

for a Freiman homomorphism ψ of $A_1 + \cdots + A_n$. Moreover, we have

$$\psi(a_1) + \cdots + \psi(a_n) = \psi(a_1 + \cdots + a_n) = \psi(a'_1 + \cdots + a'_n) = \psi(a'_1) + \cdots + \psi(a'_n) \quad (2.3)$$

whenever $a_1 + \cdots + a_n = a'_1 + \cdots + a'_n$ with $a_i, a'_i \in A_i$. If ψ is injective on $A_1 + \cdots + A_n$, then (2.3) can only hold if $a_1 + \cdots + a_n = a'_1 + \cdots + a'_n$. Conversely, analogous to the case of 2-summands, it is readily shown that if one has maps $\psi_i : A_i \to G'$ such that

$$\sum_{i=1}^{n} \psi_i(a_i) = \sum_{i=1}^{n} \psi_i(a'_i) \quad \text{if and only if} \quad \sum_{i=1}^{n} a_i = \sum_{i=1}^{n} a'_i,$$

for $a_i, a'_i \in A_i$, then the maps ψ_i induce a Freiman isomorphism of $A_1 + \cdots + A_n$ by setting $\psi_I(\sum_{i\in I} a_i) = \sum_{i\in I} \psi_i(a_i)$, where $a_i \in A_i$ and $I \subseteq [1, n]$ (details left to Exercise 2.9); likewise for Freiman homomorphisms. Thus our definition of Freiman homomorphism and isomorphism for multiple sets, as given above, is really only a more abstract way of defining an additive homomorphism and one that agrees with our previous one. When we have no need to specify the image of a Freiman isomorphism, we will simply say that $\psi : A_1 + \cdots + A_n \to G'$ is an injective Freiman homomorphism, in which case $A_1 + \cdots + A_n$ is isomorphic with its image $\psi(A_1 + \cdots + A_n) = \psi(A_1) + \cdots + \psi(A_n)$. Hence, by injective, we mean that $\psi_{[1,n]}$ is injective, for which it is generally *not* sufficient that each ψ_i be injective (see Exercise 2.10).

The following basic lemma shows, in particular, that the property of a pair of sets A and B being translates of one another is invariant of isomorphism on the sumset $A + B$.

Lemma 2.1. *Let G and G' be abelian groups and let $\psi : A + B \to G'$ be a Freiman homomorphism of the sumset of the nonempty sets $A, B \subseteq G$. Then $\psi_A - \psi_B$ is constant on $A \cap B$ and*

$$\sup\{|\psi_A(A \cap (x + B))| : x \in G\} \le \sup\{|\psi_A(A) \cap (y + \psi_B(B))| : y \in G'\}. \quad (2.4)$$

In particular, $\sup\{|A \cap (x + B)| : x \in G\}$ *is invariant of Freiman isomorphism.*

Proof. Let $x \in G$ be arbitrary. Consider arbitrary elements $c,\ c' \in A \cap (x + B)$. Then

$$c + (c' - x) = c' + (c - x) \in A + B$$

implies $\psi_A(c) + \psi_B(c' - x) = \psi_A(c') + \psi_B(c - x)$. Consequently, $\psi_A(c) - \psi_B(c - x) = \psi_A(c') - \psi_B(c' - x)$. Since $c,\ c' \in A \cap (x + B)$ were arbitrary, this shows that $\psi_A(c) - \psi_B(c - x)$ is constant for $c \in A \cap (x + B)$, say

$$\psi_A(c) - \psi_B(c - x) = f(x) \in G' \quad \text{for } c \in A \cap (x + B).$$

Taking $x = 0$ shows $\psi_A - \psi_B$ is constant on $A \cap B$.

Now, each $\psi_A(c) \in \psi_A(A \cap (f(x) + B))$ has $\psi_A(c) = f(x) + \psi_B(c - x)$ with $c - x \in B$. Hence

$$|\psi_A(A \cap (x + B))| \le |\psi_A(A) \cap (f(x) + \psi_B(B))| \le \sup\{|\psi_A(A) \cap (x + \psi_B(B))| :\ y \in G'\},$$

and as the above inequality holds for all $x \in G$, we see that (2.4) follows. For the final statement of the lemma, recall that Freiman isomorphisms must be bijective, so that $|\psi_A(A \cap (x + B))| = |A \cap (x + B)|$ in the above inequality, whence

$$\sup\{|A \cap (x + B)| :\ x \in G\} \le \sup\{|\psi_A(A) \cap (y + \psi_B(B))| :\ y \in G'\}$$

follows. Swapping the roles of $A + B$ and $\psi(A + B)$ in this argument, which is possible since Freiman isomorphism is a symmetric relation, yields the reverse inequality, completing the proof. □

We next show how—by appropriately translating the maps ψ_i in a Freiman homomorphism ψ (cf. Exercise 2.4)—the individual maps ψ_I can always be assumed to agree on their common domains. This is slightly reminiscent of the behavior of certain systems of maps in Algebraic Geometry. Since most of our problems are generally translation invariant, the assumption $0 \in A_i$ and $\psi_i(0) = 0$ for all $i \in [1, n]$ is just a normalization hypothesis, and a Freiman homomorphism ψ translated so the hypothesis of Proposition 2.1 holds (namely, so that $\psi_i(0) = 0$ for all i) will be called a *normalized Freiman homomorphism*. Of course, we must have $0 \in \bigcap_{i=1}^n A_i$ to speak of normalized Freiman homomorphisms of $\sum_{i=1}^n A_i$. However, note that the normalization is with respect to the particular translates of the sets A_i originally chosen, and choosing different translates of the A_i would result in different possible normalized homomorphisms.

Proposition 2.1 below simply states that $\psi_I = \psi_{[1,n]}|_I$ for all nonempty $I \subseteq [1, n]$, so that all the individual maps ψ_I are simply restrictions of the map $\psi_{[1,n]} : \sum_{i=1}^n A_i \to G'$. Thus, once we have normalized our Freiman homomorphism ψ per Proposition 2.1, we have $\psi_I(x) = \psi_J(x)$ for all nonempty $I,\ J \subseteq [1, n]$ with $x \in \sum_{i\in I} A_i \cap \sum_{j\in J} A_j$, i.e., the value $\psi(x)$ is unaffected by which set $\sum_{i\in I} A_i$ the element x is considered to live in, which helps explain why we will often drop the subscripts from ψ. In particular, for a normalized Freiman isomorphism ψ, we have $|\bigcup_{i=1}^n A_i| = |\bigcup_{i=1}^n \psi(A_i)|$ (Exercise 2.5). The assumption $0 \in \bigcap_{i=1}^n A_i$ can be thought of as fixing a base point in $A_1 \times \cdots \times A_n$, used for fixing which translates of the sets A_i we should consider, and, by changing this base point, we effect a change in the size of $|\bigcup_{i=1}^n A_i|$.

Essentially, Proposition 2.1 means that an equivalent definition of a normalized Freiman homomorphism of $\sum_{i=1}^n A_i$, where $0 \in \bigcap_{i=1}^n A_i$, is simply a single map $\psi : \sum_{i=1}^n A_i \to G'$, where G' is another abelian group, such that

$$\psi(0) = 0 \quad \text{and} \quad \psi\left(\sum_{i=1}^n a_i\right) = \sum_{i=1}^n \psi(a_i) \ \text{ for } a_i \in A_i.$$

Thus a Freiman homomorphism, once translated so that it is normalized, may be viewed as a kind of 'local' group homomorphism, with the Freiman homomorphism ψ being an isomorphism (with its image $\sum_{i=1}^n \psi(A_i) \subseteq G'$) when ψ is injective on $\sum_{i=1}^n A_i$.

Proposition 2.1. *Let G and G' be abelian groups, let $A_1, \dots, A_n \subseteq G$ be nonempty subsets translated so that $0 \in \bigcap_{i=1}^n A_i$, and let $\psi : A_1 + \cdots + A_n \to G'$ be a Freiman homomorphism such that $\psi_i(0) = 0$ for all $i \in [1,n]$. Then, for all nonempty subsets $I \subseteq [1,n]$, we have*

$$\psi_I(x) = \psi_{[1,n]}(x) \quad \text{for all } x \in \sum_{i\in I} A_i \subseteq \sum_{i=1}^n A_i.$$

Proof. If $I = [1,n]$, then the statement is clear, so assume $J := [1,n] \setminus I$ is nonempty. Then the additive properties of Freiman homomorphisms and our normalization hypotheses together imply

$$\psi_{[1,n]}(x) = \psi_{[1,n]}\left(x + \sum_{j\in J} 0\right) = \psi_I(x) + \psi_J\left(\sum_{j\in J} 0\right) = \psi_I(x) + \sum_{j\in J} \psi_j(0) = \psi_I(x)$$

for all $x \in \sum_{i\in I} A_i$. □

2.9 Exercises

Exercise 2.1. Give examples of an arithmetic progression with a first but no last term, with a last but no first term, and with neither a first nor last term.

Exercise 2.2. Give an example of a set A having some A_i from its $\{0,d\}$-component decomposition $A = \biguplus_{i\in I} A_i$ that is not a maximal (by containment in A) arithmetic progression.

Exercise 2.3. Let A and B be finite, nonempty subsets of an abelian group G. Show that there exists an injective Freiman isomorphism $\psi : A + B \to G'$ with G' a *finite* abelian group.

Exercise 2.4. Let $A_1, \dots, A_n \subseteq G$ be nonempty subsets of the abelian group G. If $\psi : \sum_{i=1}^n A_i \to G'$ is a Freiman homomorphism and $c_1, \dots, c_n \in G'$, then show that the translated maps $\psi_i + c_i$, for $i \in [1,n]$, also induce a Freiman homomorphism of $\sum_{i=1}^n A_i$.

Exercise 2.5. Let G be an abelian group and $A_1, \dots, A_n \subseteq G$ be nonempty subsets translated so that $0 \in \bigcap_{i=1}^n A_i$. If $\psi : \sum_{i=1}^n A_i \to G'$ is an injective normalized Freiman homomorphism, then

$$\left|\bigcup_{i=1}^n A_i\right| = \left|\bigcup_{i=1}^n \psi(A_i)\right|.$$

Exercise 2.6. Find a pair of nonempty (possibly infinite) subsets A and B of an abelian group such that

$$|A+B| - |A| \neq \sum_{\beta\in I} (|A_\beta + B| - |A_\beta|),$$

where $A = \biguplus_{\beta\in I} A_\beta$ is the $\langle B\rangle_*$-coset decomposition of A.

Exercise 2.7. Let G be an abelian group and let $A \subseteq G$ be an arithmetic progression with difference $d \in G \setminus \{0\}$. If $2 \leq |A| \leq \mathrm{ord}(d) - 2$ and A is also an arithmetic progression with difference $d' \in G \setminus \{0\}$, then $d = \pm d'$.

The following basic calculus min/max problem is remarkable for how often we will need to use it, so often in fact, that we will always do so implicitly without further reference.

Exercise 2.8. Let $M \in \mathbb{Z}^+$, let $X \subseteq \mathbb{R}^+$ be compact and define the function $f : X \to \mathbb{R}^+$ by $f(x) = \frac{M}{x} + x$. Show that f achieves its maximum value at either $\max X$ or $\min X$. Also, calculate the minimum value of f over $X = \mathbb{R}^+$.

Exercise 2.9. Let G and G' be abelian groups and let $A_1, \ldots, A_n \subseteq G$ be nonempty subsets. Suppose there are maps $\psi_i : A_i \to G'$ such that

$$\sum_{i=1}^{n} \psi_i(a_i) = \sum_{i=1}^{n} \psi_i(a_i') \quad \text{if and only if} \quad \sum_{i=1}^{n} a_i = \sum_{i=1}^{n} a_i',$$

for $a_i, a_i' \in A_i$. Show that the maps ψ_i induce a Freiman isomorphism of $A_1 + \cdots + A_n$ by setting $\psi_I(\sum_{i \in I} a_i) = \sum_{i \in I} \psi_i(a_i)$, where $a_i \in A_i$ and $I \subseteq [1, n]$. If one instead only has

$$\sum_{i=1}^{n} \psi_i(a_i) = \sum_{i=1}^{n} \psi_i(a_i') \quad \text{when} \quad \sum_{i=1}^{n} a_i = \sum_{i=1}^{n} a_i',$$

for $a_i, a_i' \in A_i$, show that the induced map defined by $\psi_I(\sum_{i \in I} a_i) = \sum_{i \in I} \psi_i(a_i)$ is simply a Freiman homomorphism.

Exercise 2.10. Give an example of a Freiman homomorphism $\psi : A_1 + \cdots + A_n \to G'$ such that each $\psi_i : A_i \to G'$ is injective, for $i \in [1, n]$, but $\psi_{[1,n]} : A_1 + \cdots + A_n \to G'$ is not.

Exercise 2.11. Show that if $\psi : A_1 + \cdots + A_n \to G'$ is an n-summand Freiman homomorphism, then $\psi' : B_1 + \cdots + B_j \to G'$, where $B_j = A_j + \cdots + A_n$, $\psi_j' = \psi_{[j,n]}$, and $B_i = A_i$ and $\psi_i' = \psi_i$ for $i \in [1, j-1]$, gives a j-summand Freiman homomorphism, which is injective if $\psi_{[1,n]}$ is injective.

Exercise 2.12. Give an example of a pair of finite, nonempty subsets A and B of an abelian group G with $\langle A + B \rangle_* = G$, $A + B \neq G$ and $\mathsf{r}_{A,B}(x) \geq 2$ for all $x \in A + B$.

Exercise 2.13. Use the sumset notation from this chapter to describe the set of midpoints of a set $A \subseteq \mathbb{R}^n$.

Notes

The study of sumsets, particularly bounds and inverse problems, dates back to Cauchy (1813) [37], though the more modern notation introduced in this chapter only arose in the latter part of the 20th century, in part popularized by the text [171]. The field lay mostly dormant throughout the 1800s and early 20th century, resurfacing when Davenport reproved the result of Cauchy [43]. Interest revived, and afterwards, particularly during the late 1950s onwards, many of the now classical results from the field were derived. However, it was only after the seminal work of Freiman [62] was more fully expounded, explained and put to great use—with the help of Bilu [30], Nathanson [171] and Gowers [92, 93], among others—that the field began to receive greater attention. The analytic and ergodic aspects of Additive Combinatorics have since been

developed to new dizzying heights—with the recent culmination being Green and Tao's proof of arbitrarily long arithmetic progression in the primes [97]—and the reader interested in this related branch of Additive Theory is directed to Tao and Vu's recent text [208].

All of the above concerns the study of finite sumsets. Sumsets with infinite summands have generally been studied in the context of various notions of density; see, e.g., [90, 117]. The idea to extend finite sumset results to allow certain infinite summands per the definition (2.1) is introduced here, though it bears certain resemblance with the ideas behind Hamidoune's Isoperimetric Method (see Chapter 21). Indeed, it was inspired by the Isoperimetric Method, and a precursor to this idea appears to be contained in [119], as remarked in [122], though its seems it was never further pursued. Correspondingly, the infinite summand case in results from subsequent chapters is not found elsewhere in the current literature. Freiman homomorphisms are so called to honor Freiman, whose idea it was to view an additive set as independent from the group in which it lives [62]. For whatever reason, the definition is often only given for the symmetric h-fold sumset hA, though the analogous definition for distinct summands is natural enough.

http://www.springer.com/978-3-319-00415-0

Structural Additive Theory
Grynkiewicz, D.
2013, XII, 426 p., Hardcover
ISBN: 978-3-319-00415-0