5.3 Freiman homomorphisms

We now introduce the fundamental concept of a *Freiman homomorphism*, that allows us to transfer an additive problem in one group Z to another group Z' in a way which is more flexible than the usual algebraic notion of group homomorphism. Roughly speaking, the role of Freiman homomorphisms is to additive sets as group homomorphisms are to additive groups. To avoid confusion we shall often write additive sets A more fully as (A, Z), where Z is the ambient group of A.

Definition 5.21 (Freiman homomorphisms) Let $k \geq 1$, and let A, B be additive sets with ambient groups Z and W respectively. A *Freiman homomorphism* of order k ϕ from (A, Z) to (B, W) (or more succinctly from A to B) is a map $\phi : A \to B$ with the property that

$$a_1 + \cdots + a_k = a'_1 + \ldots + a'_k \implies \phi(a_1) + \cdots + \phi(a_k) = \phi(a'_1) + \cdots + \phi(a'_k)$$

for all $a_1, \ldots, a_k, a'_1, \ldots, a'_k$. If in addition there is an inverse map $\phi^{-1} : B \to A$ which is a Freiman homomorphism of order k from (B, W) to (A, Z), then we say that ϕ is a *Freiman isomorphism of order k*, and that (A, Z) and (B, W) are *Freiman isomorphic of order k*.

For an equivalent characterization of a Freiman isomorphism, see Exercise 5.3.1.

It is easy to verify that a Freiman homomorphism of order k will also be Freiman homomorphic of all orders $k' < k$. Of course it is the $k \geq 2$ cases that are interesting; any map from A to B will be Freiman homomorphic of order 1, and any bijection will be Freiman isomorphic of order 1. Also, the identity map id from (A, Z) to (A, Z) is always a Freiman isomorphism of any order, and the composition of two Freiman homomorphisms (resp. isomorphisms) of order k is another Freiman homomorphism (resp. isomorphism) of order k; in particular, the relation of being Freiman isomorphic of order k is an equivalence relation. Thus the class of additive sets, and the Freiman homomorphisms of a fixed order k between them, form a category.

Remark 5.22 We digress to give an analogy with the differential geometry of manifolds. Manifolds can either be viewed extrinsically (embedded inside an ambient space such as a Euclidean space $\mathbf{R}^d$) or intrinsically (as a set endowed with certain structures such as a topology, Riemannian metric, etc.). One can easily get from the former viewpoint to the latter by restricting certain structures of the ambient space to the embedded set; reversing this procedure and embedding an intrinsic manifold inside a given ambient space is often much harder. Throughout this book we have taken the extrinsic approach, embedding the additive set A inside an ambient group Z. However one could also take a purely intrinsic viewpoint,

fixing the order k of the Freiman homomorphism and viewing the additive set as $(A, \sim_k)$, where A is now thought of an abstract set (rather than a subset of an additive group) and $\sim_k$ is the equivalence relation on A^k defined (extrinsically) by setting $(a_1, \ldots, a_k) \sim_k (a'_1, \ldots, a'_k)$ if and only if $a_1 + \cdots + a_k = a'_1 + \cdots + a'_k$. This is still enough to develop the theory of Freiman homomorphism and isomorphisms, and one can define notions such as sum sets, additive energy, etc. in this intrinsic setting. However there do not appear to be any major advantages with this approach, especially since the embedding problem turns out to be relatively easy to solve (in contrast with the situation for, say, Riemannian manifolds). See Exercise 5.5.6 below.

We now give some examples of Freiman homomorphisms.

- If $\phi : Z \to Z'$ is a group homomorphism (resp. isomorphism) from one group Z to another Z', then it induces a Freiman homomorphism (resp. isomorphism) from (A, Z) to $(\phi(Z), Z')$ of arbitrary order. In particular, the reflection map $\phi : Z \to Z$ defined by $\phi(x) := -x$ is a Freiman isomorphism from (A, Z) to $(-A, Z)$ of arbitrary order.
- If (A, Z) and (B, W) are two additive sets such that $Z \subseteq W$ and $A \subseteq B$, then the inclusion map $\iota : A \to B$ is a (rather trivial) Freiman homomorphism of arbitrary order. Thus, if $\phi : (B, W) \to (B', W')$ is any Freiman homomorphism, then the restriction $\phi|_A : (A, Z) \to (B', W')$ will be a Freiman homomorphism of the same order.
- If $x \in Z$, then the translation map $\phi : Z \to Z$ defined by $\phi(y) := y + x$ is a Freiman isomorphism from (A, Z) to $(A + x, Z)$ of any order.
- Let $N, M \geq 1$ be integers. Let $\phi : \mathbf{Z} \to \mathbf{Z}_M$ be the canonical quotient homomorphism, and let $\psi : [0, N) \to \phi([0, N))$ be the restriction of ϕ to $[0, N)$. Then ψ is a Freiman homomorphism of any order. But ψ is only a Freiman isomorphism of order k when $M \geq kN$, in which case ψ^{-1} is also a Freiman isomorphism. Thus it is possible to have a Freiman isomorphism between a set in a torsion-free group and a set in a torsion group, which would be impossible if one were only considering group homomorphisms.
- Let a, r be elements of an additive group Z, and let $P := a + [0, N) \cdot r$ be the arithmetic progression $P = \{a, a + r, \ldots, a + (N - 1)r\}$. Then the map $\phi : [0, N) \to P$ defined by $\phi(n) := a + nr$ is a Freiman homomorphism from $([0, N), \mathbf{Z})$ to $(P, \mathbf{Z})$ of any order. It is a Freiman isomorphism of order k if and only if $\mathrm{ord}(r) \geq kN$. In particular, if r is non-zero and Z is torsion-free, then ϕ is a Freiman isomorphism of all orders.
- Let $N, M, d \geq 1$ be integers, and let $\phi : \mathbf{Z}^d \to \mathbf{Z}$ be the map $\phi(a_1, \ldots, a_d) := \sum_{j=1}^{d} a_j M^{j-1}$. Then the map ϕ is a Freiman homomorphism from $[0, N)^d$ to

$\phi([0, N)^d)$ of any order, and is a Freiman isomorphism of order k when $M \geq kN$.

- The sets $\{0, 1, 10, 11\}$ and $\{0, 1, 100, 101\}$ in $\mathbf{Z}$ are Freiman isomorphic of order k for any $k < 10$, but are not Freiman isomorphic of order k for any $k \geq 10$.

The relevance of Freiman homomorphisms to the theory of sum sets lies in the following lemma:

Lemma 5.23 *Let (A, G) be an additive set, and let $\phi : (A, G) \to (\phi(A), H)$ be a surjective Freiman homomorphism of order k. Then we have*

$$|\varepsilon_1\phi(A_1) + \cdots + \varepsilon_k\phi(A_k)| \leq |\varepsilon_1 A_1 + \cdots + \varepsilon_k A_k|$$

whenever $A_1, \ldots, A_k$ are non-empty subsets of A and $\varepsilon_1, \ldots, \varepsilon_k = \pm 1$. If ϕ is in fact a Freiman isomorphism of order k, then we may replace inequality with equality. In particular, if A and B are Freiman isomorphic of order k, then

$$|lB - mB| = |lA - mA| \text{ whenever } l, m \geq 0 \text{ and } l + m \leq k.$$

Proof Define an equivalence relation $\sim$ on $A_1 \times \cdots \times A_k$ by by declaring

$$(a_1, \ldots, a_k) \sim (a'_1, \ldots, a'_k) \iff \varepsilon_1 a_1 + \cdots + \varepsilon_k a_k = \varepsilon_1 a'_1 + \cdots + \varepsilon_k a'_k.$$

Observe that the number of equivalence classes in $A_1 \times \cdots \times A_k$ is precisely $|\varepsilon_1 A_1 + \cdots + \varepsilon_k A_k|$. Also observe that we can rewrite the above condition

$$\varepsilon_1 a_1 + \cdots + \varepsilon_k a_k = \varepsilon_1 a'_1 + \cdots + \varepsilon_k a'_k$$

in a positive form as

$$\sum_{j:\varepsilon_j=1} a_j + \sum_{j:\varepsilon_j=-1} a'_j = \sum_{j:\varepsilon_j=1} a'_j + \sum_{j:\varepsilon_j=-1} a_j.$$

From this it is clear that the equivalence relation is respected by any Freiman homomorphism of order k. Combining these observations yields the lemma. □

Thus Freiman isomorphisms will preserve the cardinality of iterated sum and difference sets (as well as related quantities such as the doubling constant, difference constant, and energy); see Exercise 5.3.5. Of course, in many applications one wants to take sum sets involving *two* additive sets A, B in an ambient group Z rather than one. One way to resolve this is to work with the union $A \cup B$, since Lemma 5.23 then shows that Freiman isomorphisms of $A \cup B$ will preserve the cardinality of sets such as $A + B$ or $A - B$ (if the order of the isomorphism is at least 2). But this has the slight drawback that one loses the freedom to translate A and B independently. One way to get around this is to define the *disjoint union* $A \uplus B$ of A and B, defined in the ambient group $Z \times \mathbf{Z}$ as

$$A \uplus B := (A \times \{0\}) \cup (B \times \{1\}).$$

Then any Freiman isomorphism of the disjoint union will preserve sum sets (see Exercise 5.3.7). Note that the obvious projection map from $A \uplus B$ to $A \cup B$ is a Freiman homomorphism of any order.

Freiman homomorphisms also preserve the property of being a progression:

Proposition 5.24 *Let $\phi : A \to B$ be a Freiman homomorphism of order at least 2, and let $P = a + [0, N] \cdot v$ be a progression in A. Then $\phi(P)$ is a progression in B with the same rank, dimensions, and volume as P. Furthermore, if ϕ is in fact a Freiman* isomorphism *of order at least 2, then $\phi(P)$ is proper if and only if P is proper.*

Proof We may assume that the components N_j of N are all strictly positive, since if one of the components N_j is zero then we can simply remove it and lower the rank by 1. By translation invariance we may suppose that the base point a is equal to 0, and that $\phi(0)$ is also zero. In particular P, and thus A, contains all the basis vectors $v_1, \ldots, v_d$.

Since ϕ is a Freiman homomorphism of order 2 and $\phi(0) = 0$, we see that $\phi(x + v_j) = \phi(x) + \phi(v_j)$ whenever x and $x + v_j$ both lie in A and $1 \leq j \leq d$. Iterating this we see from induction that $\phi(n \cdot v) = n \cdot \phi(v)$ for any $n \in [0, N]$, where $\phi(v) \in B^{\oplus d}$ is the d-tuple $\phi(v) := (\phi(v_1), \ldots, \phi(v_d))$. Thus $\phi(P) = [0, N] \cdot \phi(v)$ and is thus a progression with the same rank, dimensions, and volume as P. To prove the last part of the proposition, observe that if ϕ is a Freiman isomorphism then $|P| = |\phi(P)|$, and hence $|P| = |[0, N]|$ if and only if $|\phi(P)| = |[0, N]|$. □

We now show that torsion-free additive groups are no richer than the integers, for the purposes of understanding sums and differences of finite sets.

Lemma 5.25 *Let A be a finite subset of a torsion-free additive group Z. Then for any integer k, there is a Freiman isomorphism $\phi : A \to \phi(A)$ of order k to some finite subset $\phi(A)$ of the integers $\mathbf{Z}$. The same is true if we replace $\mathbf{Z}$ by $\mathbf{Z}_N$, if N is sufficiently large depending on A.*

Note that the converse is trivial: one can always embed the integers in any other torsion-free additive group, and hence any additive set in the integers can be embedded in any other torsion-free additive group such as $\mathbf{R}^d$. However, many of these embeddings are trivial, living in some subspace of $\mathbf{R}^d$. The question of the largest dimension one can "non-trivially" embed an additive set in will lead to the concept of *Freiman dimension*, which we shall study in Section 5.5.

Proof By Corollary 3.6 we may take $Z = \mathbf{Z}^n$ for some $n \geq 0$. By translating A we may assume that A in fact lives in $(\mathbf{Z}^+)^n$, i.e. all the coordinates are non-negative. Since A is finite, we see that A is a subset of $[0, M/k)^n$ for some large

integer M (a multiple of k). Now define the map $\phi : A \to \mathbf{Z}$ by

$$\phi(a_1, \ldots, a_n) := a_1 + a_2 M + a_3 M^2 + \cdots + a_n M^{n-1}.$$

In other words, we view elements of A as digit strings of integers base M. This is a Freiman isomorphism of order k (with ϕ_k being defined the same way as ϕ, but restricted to kA); the point is that if M is large enough we never have to "carry" a digit. This shows that we can map A to the integers via a Freiman isomorphism; the same argument shows that we can map to $\mathbf{Z}/(N \cdot \mathbf{Z})$ if $N \geq M^n$. □

As we shall see later, the machinery of Freiman homomorphisms and Freiman isomorphisms will also be very useful when dealing with torsion groups, for instance we can use it to pass from a problem on the integers to a problem on a cyclic group or vice versa. If one is willing to only work with a fixed fraction of an additive set A, then the following compression lemma allows one to work in a cyclic group whose order is only a little bit larger than that of A itself.

Lemma 5.26 *[295] Let A be an additive set whose ambient group Z is either torsion-free or a cyclic group of prime order, and let $n \geq 1$ be a positive integer. Let N be an integer such that*

$$2n|nA - nA| < N < |Z|$$

(note the condition $N < |Z|$ is vacuous if Z is torsion-free). Then there exists a subset $A' \subseteq A$ of cardinality $|A'| \geq |A|/n$ and a Freiman isomorphism $\pi : A' \to B$ from A' to a subset $B \subseteq \mathbf{Z}_N$ of order n.

Proof By Lemma 5.25 it suffices to consider the case where Z is a cyclic group $\mathbf{Z}_p$ of prime order.

We shall use the first moment method. Let $\lambda \in \mathbf{Z}_p \backslash \{0\}$ be an invertible element of $\mathbf{Z}_p$ chosen uniformly at random. The map $x \mapsto \lambda \cdot x$ is thus an additive group isomorphism on $\mathbf{Z}_p$, and is in particular a Freiman isomorphism on $\mathbf{Z}_p$ of all orders. This freedom to dilate A by an arbitrary amount will be needed to avoid a certain "collision" problem which will become apparent shortly.

We now define the projection $\pi : \mathbf{Z}_p \to \mathbf{Z}_N$ by setting

$$\pi(m) := \iota(m) \bmod N,$$

where $\iota : \mathbf{Z}_p \to [0, p)$ is the obvious map that sends the residue class $m + (p \cdot \mathbf{Z})$ to m for $m = 0, \ldots, p-1$.

The map π is not quite an additive homomorphism; however note, for $j = 0, 1, \ldots, n-1$, that π is a Freiman homomorphism of order n when restricted to the set $Z_j := (jp/n, (j+1)p/n]$, which is a set that occupies roughly $\frac{1}{n}$ of the original field $\mathbf{Z}_p$. By the pigeonhole principle, for each λ, there exists a $0 \leq j =$

$j(\lambda) < 8$ such that the set $A' := \lambda \cdot A \cap Z_j$ has cardinality $|A'| \geq |A|/n$. Thus if we set $B := \pi(A') \subseteq \mathbf{Z}_N$, then the map $\pi : A' \to B$ is a surjective Freiman homomorphism of order n.

We are almost done; however we have not established that π is a Freiman *iso*morphism. The only possible obstruction is that there may be collisions in nA', in the sense that

$$\pi(x_1) + \cdots + \pi(x_n) = \pi(x'_1) + \cdots + \pi(x'_n)$$

while $x_1 + \cdots + x_n \neq x'_1 + \cdots + x'_n$, for some $x_1, \ldots, x_n, x'_1, \ldots, x'_n \in A'$ Fortunately, this type of collision rarely occurs, if N is large enough and λ is chosen randomly. Indeed, if we do have the above collision, then we see that

$$\iota(x_1) + \cdots + \iota(x_n) - (\iota(x'_1) + \cdots + \iota(x'_n))$$

must be a non-zero multiple of N. Since $x_1, \ldots, x_n, x'_1, \ldots, x'_n$ lie in A', and hence in λA, we thus see that a collision can only occur if $n\iota(\lambda A) - n\iota(\lambda A)$ contains a non-zero multiple of N. However, we can compute the probability that this occurs:

$$\begin{aligned}
&\mathbf{P}(\exists k \in \mathbf{Z} \backslash 0 : kN \in n\iota(\lambda A) - n\iota(\lambda A)) \\
&\leq \sum_{|k| \leq np/N; k \neq 0} \mathbf{P}(kN \in n\iota(\lambda A) - n\iota(\lambda A)) \\
&\leq \sum_{|k| \leq np/N; k \neq 0} \mathbf{P}(kN + p \cdot \mathbf{Z} \in n\lambda A - n\lambda A) \\
&= \sum_{|k| \leq np/N; k \neq 0} \sum_{x \in nA - nA} \mathbf{P}(kN = \lambda x \bmod p) \\
&= \sum_{|k| \leq np/N; k \neq 0} \sum_{x \in nA - nA} \mathbf{P}(\lambda = (kN)^{-1} x \bmod p) \\
&\leq \sum_{|k| \leq np/N; k \neq 0} \sum_{x \in nA - nA} \frac{1}{p-1} \\
&\leq \frac{2np}{N} |nA - nA| \frac{1}{p-1},
\end{aligned}$$

where we have used the fact that p is prime (to invert kN modulo p). By our hypotheses on N we thus see that this probability is strictly less than 1. Thus we may choose λ so that $\pi : A' \to B$ will be a Freiman isomorphism of order n as claimed. □

The above argument should be compared with the proof of Theorem 1.3.

Exercises

5.3.1 Let $\phi : A \to B$ be a map between two additive sets, and let $k \geq 1$. Show that ϕ is a Freiman isomorphism of order k if and only if ϕ is surjective

and

$$a_1 + \cdots + a_k = a'_1 + \cdots + a'_k \iff \phi(a_1) + \cdots + \phi(a_k) = \phi(a'_1) + \cdots + \phi(a'_k)$$

for all $a_1, \ldots, a_k, a'_1, \ldots, a'_k \in A$.

5.3.2 [257] Let $n > 1$. Show that $\{0, 1, n+1\}$ is Freiman isomorphic to $\{0, 1, n\}$ of order n but not $n+1$.

5.3.3 Show that given any $k \geq 1$ and any additive set A, that A is Freiman isomorphic of order k to some subset of a finite abelian group.

5.3.4 Let (A, Z) and (B, W) be additive sets, and let $\phi : A \to B$ be a map which is a Freiman homomorphism of any order k. Suppose also that Z is the group generated by A. Show that there exists a unique group homomorphism $\psi : Z \to W$ and an element $c \in Z'$ such that $\phi(x) = \psi(x) + c$ for all $x \in A$.

5.3.5 Let (A, Z) and (B, W) be Freiman isomorphic of order at least 2. Show that $\sigma[A] = \sigma[B]$, that $\delta[A] = \delta[B]$, and that $E(A, A) = E(B, B)$. For any $\alpha \in \mathbf{R}$, show that $|\mathrm{Sym}_\alpha(A)| = |\mathrm{Sym}_\alpha(B)|$. (See Definitions 2.4, 2.8, 2.32 for the meanings of these terms.)

5.3.6 Let (A, Z) and (B, W) be additive sets which contain the origin 0, and let $\phi : (A, Z) \to (B, W)$ be a Freiman isomorphism of order at least 3 which fixes the origin, thus $\phi(0) = 0$. Show that for any $K \geq 1$, that A is a K-approximate group if and only if B is. Show that if one replaces "K-approximate group" by "translate of a K-approximate group" then one can drop the requirement that $\phi(0) = 0$ and that A, B contain 0.

5.3.7 Let $(A, Z), (B, Z), (A', Z'), (B', Z')$ be additive sets, and suppose that $\phi : A \uplus B \to A' \uplus B$ is a Freiman isomorphism of order k which maps A to A' and B to B'. Show that $|n_1 A - n_2 A + n_3 B - n_4 B| = |n_1 A' - n_2 A' + n_3 B' - n_4 B'|$ whenever $|n_1| + |n_2| + |n_3| + |n_4| \leq k$. If $k \geq 2$, show that $d(A, B) = d(A', B')$ and $E(A, B) = E(A', B')$. Also, show that A can be covered by K translates of B if and only if A' can be covered by K' translates of B'.

5.3.8 Suppose that two additive sets A and B are Freiman isomorphic of order k. If $n, m, k' \geq 0$ are such that $k'(n+m) \leq k$, show that $nA - mA$ and $nB - mB$ are Freiman isomorphic of order k'.

5.3.9 Show that all Sidon sets of a fixed cardinality N are Freiman isomorphic of order 2 to each other. More generally, for any $h \geq 2$, show that all B_h sets of cardinality N are Freiman isomorphic to each other of order h, and that the image of a B_h set under a Freiman isomorphism is still a B_h set. Thus one could work with a "standard" B_h set of order N, such as the basis $e_1, \ldots, e_N$ of $\mathbf{Z}^N$, and many additive results concerning that standard set would automatically transfer over to an arbitrary B_h set.