5.3.10 Let (A, Z) and (A', Z') be additive sets in finite additive groups Z, Z' which are Freiman isomorphic of order h for some $h \geq 1$. Show that $\|A\|_{\Lambda(2h)} = \|A'\|_{\Lambda(2h)}$, where the $\Lambda(p)$ constants are as in Definition 4.26.

5.3.11 [29] Let p be a prime, let $k \geq 1$, and let $(A, \mathbf{Z}_p)$ be an additive set in $\mathbf{Z}_p$ such that $|A| \leq \log_{2k} p$. Show that there exists an additive set $(A', \mathbf{Z})$ such that the canonical projection map from $\mathbf{Z}$ to $\mathbf{Z}_p$ is a Freiman isomorphism of order k from A' to A. (Hint: the claim is obvious if A is contained in the arithmetic progression $[-p/2k, p/2k] \cdot 1$ in $\mathbf{Z}_p$. For the general case, use the Kronecker approximation theorem (Corollary 3.25) to locate an integer n coprime to p such that $n \cdot A$ lies in this progression $[-p/2k, p/2k] \cdot 1$, and then find an integer m with $nm = 1 \pmod p$ to "invert" the dilation $x \mapsto n \cdot x$.)

5.3.12 [29] Let p be a prime, written in binary as $p = 2^{n_1} + \cdots + 2^{n_r}$ where $n_1 < \cdots < n_r$. Let $(A, \mathbf{Z}_p)$ be the additive set

$$A := \{0\} \cup \{1, 2^1, \ldots, 2^{n_r+1}\} \cup \{2^{n_1} + \cdots + 2^{n_j} : 1 \leq j \leq r\}.$$

Show that $|A| \leq 2 \log_2 p + 1$, but there does not exist any set of integers A' which is Freiman isomorphic of order 2 to A. This shows that the estimate $|A| \leq \log_{2k} p$ in Exercise 5.3.11 is very close to being sharp.

5.3.13 Let $(A, Z), (B, Z)$ be additive sets such that $A + B$ can be covered by K translates of A for some $K \geq 1$, and let $\phi : A \uplus B \to C$ be a Freiman homomorphism of order 4. Show that $\phi(A) + \phi(B)$ can be covered by K translates of $\phi(A)$.

5.3.14 Let Q be a progression of rank d, let $k \geq 1$, and let $N \geq k^d |Q|$. Show that there exists an additive set $(Q', \mathbf{Z}_N)$ in the cyclic group $\mathbf{Z}_N$ and a surjective Freiman homomorphism $\phi : Q' \to Q$ of order k. If Q is proper, one can also ensure that ϕ is injective. This fact is useful for viewing progressions as dense subsets of cyclic groups.

5.4 Torsion and torsion-free inverse theorems

We can now use all the machinery developed thus far to prove two inverse sum set theorems, one in the setting of r-torsion groups and one in the setting of torsion-free groups. The two arguments are quite different, but they will be combined to obtain an inverse sum set theorem for an arbitrary group in Section 5.6.

We begin with the r-torsion case.

Theorem 5.27 (Freiman theorem for r-torsion groups) *[300], [154] Suppose A is an additive set in an r-torsion group Z such that $|A + A| \leq K|A|$ or*

$|A - A| \leq K|A|$. *Then there exists a subgroup H of Z of cardinality $|A| \leq |H| \leq r^{K^{O(1)}}|A|$ such that A is contained in a translate of H.*

Proof By Proposition 2.26 we can find a $K^{O(1)}$-approximate group H such that A is contained in a translate of H. But then $H \pm H \subseteq H + X$ for some additive set X of cardinality at most $K^{O(1)}$. We conclude that the set $G := H + \langle X \rangle$ is a genuine group, where $\langle X \rangle$ is the group generated by X. But from the r-torsion hypothesis we have $|\langle X \rangle| \leq r^{|X|} \leq r^{K^{O(1)}}$, and the claim follows. □

Remark 5.28 The upper bound on $|G|$ has been improved to r^{2K^2-1} in [154], using the Green–Ruzsa covering lemma and the Plünnecke inequalities; see Exercise 5.4.1. The exponential dependence in K here is necessary, as the example $Z = \mathbf{Z}_r^K$, $A = \{e_1, \ldots, e_K\}$ shows. However if one relaxes the claim that A is completely contained in a translate of H then one should do better. For instance, it is conjectured by Marton [300] that in the above setting we can in fact find a group $H \subseteq Z$ of cardinality at most $|A|$ such that A can be covered by $O(K^{O_r(1)})$ translates of H. This would be sharp up to polynomial losses, since in that case one can easily verify that $|A + A|, |A - A| = O(K^{O_r(1)}|A|)$.

As a corollary we can also obtain a Chang-type theorem in the r-torsion case.

Corollary 5.29 (Chang theorem for r-torsion groups) *Suppose A is an additive set in an r-torsion group Z such that $E(A, A) \geq |A|^3/K$. Then $2A - 2A$ contains a subgroup of Z of cardinality at least $r^{-O(K^{O(1)})}|A|$.*

Proof We may take $r \geq 2$ as the case $r = 1$ is trivial. Using the Balog–Szemerédi–Gowers theorem (Theorem 2.31) and translating A if necessary, we may find a subset A' of A with $|A'| = \Omega(K^{-O(1)}|A|)$ which is contained in a $K^{O(1)}$-approximate group G of size $|G| = O(K^{O(1)}|A|)$. Using Theorem 5.27 we may place the approximate group G inside a genuine group H of cardinality at most $r^{K^{O(1)}}|A|$; thus $\mathbf{P}_H(A') \geq r^{-K^{O(1)}}$. By Proposition 4.39, we thus see that $2A' - 2A'$ contains a Bohr set $\mathrm{Bohr}_H(\mathrm{Spec}_\alpha(A'), \frac{1}{6})$ for some $\alpha = \Omega(K^{-O(1)})$. Using Lemma 4.36 as in the proof of Theorem 4.42, we conclude that $2A' - 2A'$ (and hence $2A - 2A$) contains a Bohr set $\mathrm{Bohr}_H(S, \frac{1}{6|S|})$ for some set of frequencies $S \subset H$ with $|S| = O(K^{O(1)})$. In particular, it contains the subgroup $\mathrm{Bohr}_H(S, 0)$. But as H is an r-torsion group, $\mathrm{Bohr}_H(S, 0) = \mathrm{Bohr}_H(S, 1/r)$, and so from (4.25) we see that

$$\begin{aligned} |\mathrm{Bohr}_H(S, 0)| &\geq r^{-O(K^{O(1)})}|H| \\ &\geq r^{-O(K^{O(1)})}|A'| \\ &= \Omega\big(r^{-O(K^{O(1)})}K^{-O(1)}|A|\big) \end{aligned}$$

and the claim follows (using the hypothesis $r \geq 2$ to absorb the lower order terms). □

We now turn to the torsion-free case. We begin with two preliminary results of interest in their own right. The first exploits all the above machinery of Freiman homomorphisms, as well as the powerful techniques of harmonic analysis from Chapter 4 and the additive geometry results in Chapter 3 (as encapsulated in Theorem 4.42), to show that if A has small doubling, then $2A - 2A$ contains a large proper progression.

Theorem 5.30 (Ruzsa–Chang theorem) *[295], [48] Let A be an additive set in a torsion-free additive group Z such that $|A + A| \leq K|A|$ for some $K \geq 1$. Then $2A - 2A$ contains a proper symmetric progression P of rank $O(K(1 + \log K))$ such that $|P| \geq e^{-O(K(1+\log^2 K))}|A|$.*

Proof Let p be the first prime number larger than $16|8A - 8A|$. By Corollary 2.23 and Bertrand's postulate (Exercise 1.10.3) one can then find a subset A' of A of cardinality $|A'| \geq |A|/8$, which is Freiman isomorphic of order 8 to an additive set B in $\mathbf{Z}_p$. Observe that

$$|B + B| = |A' + A'| \leq |A + A| \leq K|A| \leq 8K|B|$$

so B has doubling constant at most $8K$. Applying Theorem 4.42 we then obtain a proper symmetric progression Q inside $2B - 2B$ of rank at most $O(K(1 + \log K))$ and cardinality at least $O(K(1 + \log K))^{-O(K(1+\log K))}|B|$. In particular we have

$$|Q| \geq e^{-O(K \log^2 K)}|B|.$$

Since A' is Freiman isomorphic to B of order 8, $2A' - 2A'$ is Freiman isomorphic to $2B - 2B$ of order 2 (see Exercise 5.3.8). $2A - 2A$, contains a symmetric progression P which is Freiman isomorphic to P, and the claim follows. □

The second result is a variant of the Ruzsa covering lemma which gives good constants when the doubling constant is small.

Lemma 5.31 (Chang's covering lemma) *[48] Let $K, K' \geq 1$, and let A, B be additive sets in an ambient group Z such that $|nA| \leq K^n|A|$ for all $n \geq 1$, and such that $|A + B| \leq K'|B|$. Then, for any $a_0 \in A$, there exists elements $v_1, \ldots, v_d$ in $A - A$ with $d = 2K(1 + \log_2(KK'))$ such that $A \subseteq B - B + [0, 1]^d \cdot (v_1, \ldots, v_d) + a_0$.*

Proof Without loss of generality we may take K to be an integer. By translation we may take $a_0 = 0$. We construct a sequence of enlargements $B = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_N$ by iterating the argument of Lemma 2.14 as follows. Set $B_0 := B$. Now suppose inductively that $n \geq 0$ and B_n has already been constructed. Consider the collection $\{a + B_n : a \in A\}$ of translates of B_n by elements of A. If we can find at least $2K$ such translates which are disjoint, we set B_{n+1} to be the union of these $2K$

translates; thus $B_{n+1} = B_n + A_n$ for some subset A_n of A of cardinality $2K$, and $|B_{n+1}| = 2K|B_n|$, and then continue the algorithm. If we cannot find $2K$ disjoint translates, we select a family of disjoint translates of maximal cardinality, set B_{n+1} to be the union of these translates, and then halt the algorithm setting $N := n + 1$. Thus in the terminating case we have $B_{n+1} = B_n + A_n$, where A_n is a subset of A of cardinality less than $2K$.

Let us first see why this algorithm even terminates. By induction we see that $B_n \subseteq B + nA$ for all $0 \leq n < N$, but we also have $|B_n| = (2K)^n|B|$. On the other hand, from Lemma 2.6, we have

$$|B + nA| \leq \frac{|B - A||A + nA|}{|A|} \leq K'K^{n+1}.$$

Thus the algorithm must terminate by the time $(2K)^n$ exceeds $K'K^{n+1}$, and we therefore have the bound $N \leq 1 + \log_2(KK')$.

Now let a be any element of A. Observe that $B_{N-1} + a$ cannot be disjoint from B_N, since otherwise we could have added it to the collection of disjoint translates comprising B_N. Thus $a \in B_N - B_{N-1}$ for all $a \in A$, and hence

$$A \subseteq B_N - B_{N-1} = B - B + A_0 - A_0 + A_1 - A_1 + \cdots + A_{N-1} - A_{N_1} + A_N.$$

By Lemma 3.11, we see that each of the A_j (or $-A_j$) can be contained in a progression of the form $[0, 1]^{d_j} \cdot v$ for some $d_j \leq 2K$, where the components of v lie in A_j and hence in $A - A$ (since $0 \in A$ and $A_j \subseteq A$). The claim then follows from several applications of (3.2). □

As a consequence of these two results we obtain an inverse theorem in the torsion-free case.

Theorem 5.32 (Freiman's theorem for torsion-free groups) *[116], [295], [48] Let A be an additive set in a torsion-free group Z such that $|A + A| \leq K|A|$. Let $a_0 \in A$. Then there exists a proper progression P contained in $2A - 2A$ of rank at most $O(K(1 + \log K))$ and cardinality at most $|P| \leq |2A - 2A| \leq K^{O(1)}|A|$, and vectors $v_1, \ldots, v_d$ in $4A - 4A$ with $d = O(K^{O(1)})$, such that $A \subseteq P + [0, 1]^d \cdot (v_1, \ldots, v_d) + a_0$.*

Proof By translation we may assume that $a = 0$, so $0 \in A$. Applying Theorem 5.30 we see that $2A - 2A$ contains a proper progression P of rank at most $CK(1 + \log K)$ and cardinality at least $e^{-O(K(1+\log^2 K))}|A|$. Note from Corollary 2.23 that $|P| \leq |2A - 2A| \leq K^{O(1)}|A|$. Now we use Lemma 5.31 to cover A by $P - P$. First from Corollary 2.23 note that

$$|A + P| \leq |3A - 2A| \leq K^{O(1)}|A| \leq e^{O(K(1+\log^2 K))}|P|$$

and that $|nA| \leq K^{O(n)}|A|$ for all $n \geq 1$. Thus by Lemma 5.31 (and the remarks immediately following that lemma) we have

$$A \subseteq P - P + [0,1]^d \cdot (v_1, \ldots, v_d)$$

for some $v_1, \ldots, v_d \in A - A$ and $d = O(K^{O(1)})$. Also, from Lemma 3.10 we have $P - P \subseteq P + [0,1]^{d'} \cdot (w_1, \ldots, w_{d'})$ where $d' = O(K(1 + \log K))$ is the rank of P and $w_1, \ldots, w'_d \in P - P \subseteq 4A - 4A$. Combining these facts using (3.2) we obtain the result. □

One can reduce the rank of the containing progression to $K - 1$, at the cost of worsening the size of $|P|$:

Theorem 5.33 *[48] Let A be an additive set in a torsion-free group Z such that $|A + A| \leq K|A|$. Then there exists a proper progression P of rank at most $K - 1$ which contains A such that $|P| \leq \exp(O(K^{O(1)}))|A|$.*

Proof We may assume that $|A| \leq 100K^2$ (for instance) since the claim follows from Lemma 3.11 and Theorem 3.40 otherwise.

Without loss of generality we may assume that A contains the origin, and then we may assume that Z is generated by A otherwise we could pass from Z to the group $\langle A \rangle$ generated by A. From Theorem 5.32 and (3.2) we can contain A inside a progression Q of rank $d = O(K^{O(1)})$ and cardinality at most $\exp(O(K^{O(1)}))|A|$. Now consider the progression $2Q - 2Q$, which has the same rank as Q and essentially the same bounds on the cardinality. By Theorem 3.40 we can find a symmetric proper progression $R = [-N, N] \cdot v$ of some rank $d' \leq d$ containing $2Q - 2Q$ such that $|R| \leq \exp(O(K^{O(1)}))|A|$. In particular, the set A (which is contained inside $Q - Q$) is Freiman isomorphic of order 2 to a subset $\tilde{A}$ of $[-N, N] \subset \mathbf{Z}^{d'}$; thus $\tilde{A}$ has doubling constant at most K. By Freiman's lemma (Lemma 5.13) we may place $\tilde{A}$ in a subspace V of $\mathbf{Z}^{d'}$ of dimension at most $K - 1$.

We now use the "rank reduction argument". If $d' \leq K - 1$ then we are done (by setting $P = R$), so suppose $d' > K - 1$. The intersection of $[-N, N] \subset \mathbf{Z}^{d'}$ with V is the intersection of a convex subset with a lattice of rank strictly less than d' with cardinality at most $\exp(O(K^{O(1)}))|A|$, so by Lemma 3.36 we may contain it in a progression of rank strictly less than d' and cardinality at most $\exp(O(K^{O(1)}))|A|$, with steps inside $[-N, N]$. Using the Freiman isomorphism, this allows us to contain A in a progression Q' of rank strictly less than d and cardinality at most $\exp(O(K^{O(1)}))|A|$. We then iterate the above argument (replacing Q by Q') at most d times until one can contain A in a progression P of length $K - 1$. As the rank decreases at each stage it is easy to see that the final progression P will have size at most $\exp(O(K^{O(1)}))$. □

The exponential factors in Theorem 5.33 cannot be removed directly, as can be seen by considering the additive set $Z = \{e_1, \ldots, e_K\}$ in $\mathbf{Z}^K$. However it is conjectured that if one weakens the containment $A \subseteq P$ then one can do better, for instance

Conjecture 5.34 (Polynomial Freiman–Ruzsa conjecture) *Let A be an additive set in a torsion-free group Z such that $|A + A| \leq K|A|$. Then there exists a progression P of rank at most $O(K^{O(1)})$ such that $|P| = O(K^{O(1)}|A|)$ and $|A \cap P| = \Omega(K^{-O(1)}|A|)$.*

This would be the analog of Marton's conjecture mentioned earlier in this section. Such a conjecture, if true, would allow one to obtain substantially better bounds on many results whose proof involves Freiman's theorem. See [151], [152] for further discussion.

By combining Theorem 5.33 with Theorem 5.20 one can show

Proposition 5.35 *[28] Let A be an additive set in a torsion-free group Z such that $|A + A| \leq K|A|$ for some $K < 2^d$. Then there exists a proper progression P of rank at most d and size $|P| = \Theta_{K,d}(|A|)$ such that $|A \cap P| = \Theta_{K,d}(|A|)$.*

We leave the deduction of this proposition from the previous results to Exercise 5.4.5. Recently, a more quantitative version of this proposition was obtained:

Proposition 5.36 *[162] Let A be an additive set in a torsion-free group Z such that $|A + A| \leq K|A|$. Then for any $0 < \varepsilon \leq 1$ there exists a proper progression P of rank at most $\lfloor \log_2 K + \varepsilon \rfloor$ and size at most $|A|$ such that A is covered by $\exp(O(K^3 \log^3 K))/\varepsilon^{O(K)}$ translates of P.*

Exercises

5.4.1 [154] Using Lemma 2.17 and Corollary 6.28, improve the factor of $r^{K^{O(1)}}$ in Theorem 5.27 to r^{2K^2-1}.

5.4.2 Show that the term $(d+1)|A| - \frac{d(d+1)}{2}$ in Corollary 5.13 cannot be replaced by any smaller quantity.

5.4.3 Using Corollary 6.28, improve the bounds in Theorem 5.32 and Theorem 5.33 as much as you can.

5.4.4 [300], [151] Let Z, Z' be two r-torsion groups, let $K \geq 1$, and let $f : Z \to Z'$ be a function which is a "K-almost homomorphism" in the sense that the set $\{f(x+y) - f(x) - f(y) : x, y \in Z\}$ has cardinality at most K. Show that there exists a genuine group homomorphism $g : Z \to Z'$ such at $\{f(x) - g(x) : x \in Z\}$ has cardinality at most r^K. It is conjectured that one can improve r^K to $O_r(K^{O_r(1)})$; this would essentially imply Marton's conjecture. See [151], [152] for further discussion.