torsion-free if and only if $Z$ contains no finite subgroups other than the trivial subgroup $\{0\}$.

3.1.5 Let $Z = Z_1 \oplus Z_2$ be a direct sum of additive groups and $r \geq 1$. Show that $Z$ is torsion-free (resp. $r$-torsion) if and only if $Z_1$ and $Z_2$ are torsion-free (resp. $r$-torsion).

3.1.6 Prove that $\mathbf{Q}$ and $\mathbf{R}$ are not finitely generated.

3.1.7 If $x, y$ are elements of an additive group $Z$ with finite order, show that $x + y$ also has finite order, and that $\mathrm{ord}(x + y)$ divides the least common multiple of $\mathrm{ord}(x)$ and $\mathrm{ord}(y)$. Conclude that the set $\mathrm{tor}(Z) := \{x \in Z : \mathrm{ord}(x) < \infty\}$ is a torsion group; we refer to it as the *torsion subgroup* of $Z$. It is clearly the largest subgroup of $Z$ which is a torsion group. Show that the quotient group $Z/\mathrm{tor}(Z)$ is torsion-free, and is in fact the largest quotient which is torsion-free (in the sense that all other torsion-free quotients are quotients of $Z/\mathrm{tor}(Z)$).

3.1.8 Show that Corollary 3.5 fails whenever $v$ is not irreducible.

## 3.2 Progressions

We now study a basic example of an additive set, namely that of a *generalized arithmetic progression* (or *progression* for short), as defined in Definition 0.2. These will be model examples of additive sets with large amounts of additive structure; they can be viewed as a hybrid between a lattice and a convex set. (For a more quantitative realization of this heuristic, see Lemma 3.36 below.)

Note that progressions with the same set of basis vectors add very easily

$$(a + [0, N] \cdot v) + (a' + [0, N'] \cdot v) = (a + a') + [0, N + N'] \cdot v \tag{3.1}$$

(so in particular the rank and basis vectors do not change), whereas progressions with different basis vectors add via the formula

$$(a + [0, N] \cdot v) + (a' + [0, N'] \cdot v') = (a + a') + [0, N \oplus N'] \cdot (v \oplus v'). \tag{3.2}$$

Note the progression on the right-hand side of (3.2) is likely to be highly improper if $v$ and $v'$ share some basis vectors in common. Also one can replace the box $[0, N]$ by another one and also obtain a progression:

$$a + [N, M] \cdot v = (a + N \cdot v) + [0, M - N] \cdot v.$$

Similarly if one uses boxes such as $[N, M)$, etc. In particular, the negation of a progression is also a progression:

$$-(a + [0, N] \cdot v) = (-a) + [0, N] \cdot (-v) = (-a - N \cdot v) + [0, N] \cdot v. \tag{3.3}$$

From this and (3.2) we see that the sum or difference of two progressions is again a progression. Finally, we make the easy observation that the Cartesian product of two progressions is again a progression.

We now show that, up to errors of $O(1)^d$, that progressions of rank $d$ are essentially closed under addition.

**Lemma 3.10** *Let $P = a + [0, N] \cdot v$ be a progression of rank $d$ in an additive group $Z$; we do not require that $P$ be proper (see Definition 0.2). Then for any integers $n < m$ and any $b \in Z$, we can cover $b + [nN, mN] \cdot v$ by $(m-n)^d$ translates of $P$. In particular for any $n, m \geq 0$ with $(n, m) \neq (0, 0)$, we can cover $nP - mP$ by $(n+m)^d$ translates of $P$, and in particular*

$$|nP - mP| \leq (n+m)^d |P|.$$

*Furthermore, $nP - mP$ is also a progression of rank $d$ and volume at most* $\mathrm{vol}(nP - mP) \leq (n+m)^d \mathrm{vol}(P)$.

*Proof* The first claim is clear since

$$[n \cdot N, m \cdot N] \cdot v = [0, N] \cdot v + [(n, \ldots, n), (m, \ldots, m)] \cdot (N_1 v_1, \ldots, N_d v_d).$$

From (3.1) we have

$$nP - mP = (na - ma - mN \cdot v) + [0, (n+m)N] \cdot v$$

from which the remaining claims follow. □

From this lemma we see in particular that if $P$ is a symmetric progression of rank $d$ and contains the origin (e.g. if $P = [-N, N] \cdot v$), then $P$ is a $2^d$-approximate group in the sense of Definition 2.25. Indeed one can think of (symmetric) progressions of small rank as substitutes for subgroups in torsion-free settings (since torsion-free groups cannot contain finite subgroups). They also are the arithmetic analogue of boxes (or more generally, parallelepipeds) in Euclidean space, and in fact many of the results from real-variable harmonic analysis regarding covering by boxes (in physical space, Fourier space, or both) will have analogues for progressions.

In the special case when the rank $d$ is equal to 1, a generalized arithmetic progression is the same as an *ordinary arithmetic progression* (or *arithmetic progression* for short)

$$P = a + [0, N] \cdot v = \{a + nv : 0 \leq n \leq N\}$$

with base point $a \in Z$, basis vector or *step* $v \in Z$, and length $N + 1$. Note again that the cardinality of $P$ may be less than $N + 1$ if $P$ is not proper, though in a torsion-free group this is only possible if the step $v$ is zero.

We record a trivial lemma that asserts that the sum set of a progression and a small set can be contained (somewhat inefficiently) in another progression.

**Lemma 3.11** *If $P$ is a progression of rank $d$, and $P + w_1, \ldots, P + w_K$ are translates of $P$, then all the translates $P + w_1, \ldots, P + w_K$ can be contained inside a single progression of rank $d + K - 1$ and volume $2^{K-1}\mathrm{vol}(P)$.*

*Proof* Write $P = a + [0, N] \cdot v$. By translation invariance we may set $w_K = 0$. Then the claim follows by using the progression $a + [0, N] \cdot v + [0, 1]^{K-1} \cdot (w_1, \ldots, w_{K-1})$. □

Thus if one adds a small number of elements to an progression, one can still place the combined set inside a progression of slightly larger rank and volume, although the volume can grow exponentially in $|A|$. This is unavoidable: see Exercise 3.2.2. Because of this exponential loss, it is sometimes better not to invoke this lemma, and deal with multiple shifts of a single progression rather than trying to contain everything inside a single progression. Note that we have not guaranteed that the progressions in Lemma 3.11 are proper; we will return to this point in Section 3.6.

## Exercises

3.2.1 Let $N = (N_1, \ldots, N_d)$ be a collection of non-negative integers. Show that every proper ordinary arithmetic progression of length $(N_1 + 1) \cdots (N_d + 1)$ is equal (as a set) to a proper generalized arithmetic progression of dimension $N$. (This example shows that the rank of a progression cannot be uniquely determined from the set of its elements, even if we restrict the progression to be proper.)

3.2.2 Let $K \geq 1$ and $d \geq 0$ be integers, and $P = a + [0, N] \cdot v$ be a rank $d$ progression in an additive group $Z$ for some basis vectors $v = (v_1, \ldots, v_d)$, and let $X = \{e_1, \ldots, e_K\}$ be a set of $K$ elements in $Z$. Suppose that the elements $v_1, \ldots, v_d, e_1, \ldots, e_K$ are linearly independent over $\mathbf{Z}$. Show that any progression which contains $P + X$ must necessarily have rank at least $d + K - 1$ and volume at least $2^{K-1}\mathrm{vol}(P)$, which shows that Lemma 3.11 is sharp.

3.2.3 Show that in a torsion-free additive group, the intersection of two ordinary arithmetic progressions is again an ordinary arithmetic progression. What happens if the torsion-free hypothesis is removed? What happens if one or both of the progressions is allowed to have rank greater than one?

3.2.4 Show that every finite additive group is also a proper progression.

3.2.5 Let $P$ be a progression of rank $d$. Show that $P$ contains an arithmetic progression $Q$ with $|Q| \geq |P|^{1/d}$, and furthermore that $Q$ is proper if $P$ is, and $Q$ can be chosen to be symmetric around the origin if $P$ is.