2.1 Sum sets

We now systematically study the sum sets $A+B$ and difference sets $A-B$ of two additive sets A, B in an ambient group Z as defined in Definition 0.1, as well as the iterated sum sets nA. We should caution the reader that the iterated sum set nA is in general not the same as the dilate $n \cdot A := \{n \cdot a : a \in A\}$ though we do have the inclusion $n \cdot A \subseteq nA$. Similarly the difference set $A-B$ should not be confused with the set-theoretic difference $A \backslash B := \{x \in A : x \notin B\}$. We also write $A+x = A+\{x\}$ for the translate of A by an element $x \in Z$.

Since addition of group elements is associative and commutative, one can easily verify the same is true for addition of sets. We should caution however that the sum set operation is not invertible: for instance, $A+B-B$ contains A but is generally not equal to A. Similarly, when $n > m$, then $nA - mA$ will contain $(n-m)A$ but will generally be larger.

A very fundamental question in this topic is the following: under what conditions is $A+B$ "small", and under what conditions is it "large"? More precisely, we will be interested in the cardinality $|A+B|$ of the sum set $A+B$. We have the following trivial estimates:

Lemma 2.1 (Trivial sum set estimates) *Let A, B be additive sets with common ambient group Z, and let $x \in Z$. Then we have the identities $|A+x| = |-A| = |A|$, the inequalities*

$$\max(|A|, |B|) \leq |A+B|, |A-B| \leq |A||B| \tag{2.1}$$

and the inequalities

$$|A| \leq |A+A| \leq \frac{|A|(|A|+1)}{2}. \tag{2.2}$$

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

$$|nA| \leq \binom{|A|+n-1}{n} = \frac{|A|(|A|+1)\cdots(|A|+n-1)}{n!}. \tag{2.3}$$

We remark that the lower bound in (2.1) can be improved for specific groups Z, or when A and B have large "dimension"; see Theorem 3.16, Lemma 5.3, Theorem 5.17, Corollary 5.13, Theorem 5.4.

Proof We shall just prove (2.3), as all the other inequalities either follow from this inequality or are trivial. We argue by induction on $|A|$. If $|A| = 1$ then both sides of (2.3) are equal to 1. If $|A| > 1$, then we can write $A = B \cup \{x\}$ where B is a non-empty set with $|B| = |A| - 1$. Then

$$nA = \bigcup_{j=0}^{n} (jB + (n-j) \cdot x)$$

and hence by the induction hypothesis and Pascal's triangle identity

$$|nA| \leq \sum_{j=0}^{n} |jB| \leq \sum_{j=0}^{n} \binom{|A|-1+j-1}{j} = \binom{|A|+n-1}{n}$$

as claimed. (We adopt the convention that $0B = \{0\}$.) □

Observe from the above facts that the magnitude of sum sets such as $A+B$, $A-B$, kA are unaffected if one translates A or B by an arbitrary amount. This gives much of the theory of sum sets a "translation-invariant" or "affine" flavor. We will sometimes take advantage of this translation invariance to normalize one of the sets, for instance to contain the origin 0.

For "generic" additive sets A and B, the cardinalities of the sum sets considered in Lemma 2.1 are much more likely to be closer to the upper bounds listed above than the lower bounds; see for instance Exercise 2.1.1. This suggests that the lower bounds are only attainable, or close to being attainable, when the sets A and B have a considerable amount of structure; we shall develop this theme in the remainder of this chapter, by introducing tools such as doubling and difference constants, Ruzsa distance, additive energy, and K-approximate groups to quantify some of these notions of "structure". For now, we at least settle the question of when the lower bound in (2.1) is attained.

Proposition 2.2 (Exact inverse sum set theorem) *Suppose that A, B are additive sets with common ambient group Z. Then the following are equivalent:*

- $|A+B| = |A|$;
- $|A-B| = |A|$;
- $|A+nB-mB| = |A|$ *for at least one pair of integers* $(n,m) \neq (0,0)$;
- $|A+nB-mB| = |A|$ *for all integers* n, m;
- *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.*

Proof We shall just show that the first claim implies the fifth; the remaining claims are either similar or easy and are left to the exercises. By translating B if necessary we may assume that B contains 0. Then $A+B \supset \{0\}+A = A$, but since $|A+B| = |A|$ we have $A+B = A$. In particular $A+b = A$ for all $b \in B$. Thus if we define the *symmetry group* $\mathrm{Sym}_1(A)$ (also known as the *period* of A) to be the set $\mathrm{Sym}_1(A) := \{h \in Z : A+h = A\}$, then we have $B \subseteq \mathrm{Sym}_1(A)$. We leave as an exercise for the reader the verification that $\mathrm{Sym}_1(A)$ is a finite group, and A is the union of cosets of $\mathrm{Sym}_1(A)$; the claim then follows by setting $G := \mathrm{Sym}_1(A)$. □

We shall study the symmetry group $\mathrm{Sym}_1(A)$, as well as the more general symmetry sets $\mathrm{Sym}_\alpha(A)$, more systematically in Section 2.6.

As to when the upper bound is attained, we do not have as explicit a description, but we can give a number of equivalent formulations of the condition.

Proposition 2.3 *Suppose that A, B are additive sets with common ambient group Z. Then the following are equivalent:*

- $|A+B| = |A||B|$;
- $|A-B| = |A||B|$;
- $|\{(a,a',b,b') \in A\times A\times B\times B : a+b = a'+b'\}| = |A||B|$;
- $|\{(a,a',b,b') \in A\times A\times B\times B : a-b = a'-b'\}| = |A||B|$;
- $|A\cap(x-B)| = 1$ *for all* $x \in A+B$;
- $|A\cap(B+y)| = 1$ *for all* $y \in A-B$;
- $(A-A)\cap(B-B) = \{0\}$.

We leave the easy proof of this proposition to the exercises. For a partial generalization of it, see Corollary 2.10 below.

In Proposition 2.2 and Proposition 2.3, the sets $A+B$ and $A-B$ have the same size (see also Exercise 2.1.6). However, this is not true in general. A basic example is the set $A = \{0,1,3\} \subset \mathbf{Z}$; then $A+A = \{0,1,2,3,4,6\}$ has six elements and $A-A = \{-3,-2,-1,0,1,2,3\}$ has seven elements. More generally, if $A = \{0,1,3\}^d \subset \mathbf{Z}^d$, then $A+A$ has 6^d elements and $A-A$ has 7^d. Thus $A-A$ can be larger than $A+A$ by an arbitrarily large amount. In the converse direction, the set $A := \{(0,0),(1,0),(2,0),(3,1),(4,0),(5,1),(6,1),(7,0),(8,1),(9,1)\} \in \mathbf{Z}_{10}\times\mathbf{Z}_2$ is such that $A+A = \mathbf{Z}_{10}\times\mathbf{Z}_2$ has 20 elements, but $A-A = \mathbf{Z}_{10}\times\mathbf{Z}_2\backslash\{(0,1)\}$ has only 19 elements; one can amplify this example as before by raising to the power d. Despite these examples, however, there are still several relationships between the size of $|A+A|$ and $|A-A|$; see in particular (2.11) below.

Exercises

2.1.1 Let $N, M \geq 1$ be integers, and let A and B be sets of cardinality N and M respectively chosen uniformly at random from the real interval $\{x \in \mathbf{R} : 0 \leq x \leq 1\}$. Show that with probability 1 we have $|A+B| = |A||B|$ and $|nA| = \binom{|A|+n-1}{n}$ for all $n \geq 1$.

2.1.2 Prove the remaining claims in Proposition 2.2.

2.1.3 Let A be an additive set. Show that A is a group if and only if $2A = A$.

2.1.4 Prove Proposition 2.3.

2.1.5 [289] Find an additive set A of integers such that $|A-A| < |A+A|$. (Hint: there are several ways to proceed. One way is to tile the lattice $\mathbf{Z}^2$ with the $\mathbf{Z}_{10}\times\mathbf{Z}_2$ example given above, and somehow truncate and then project this back to $\mathbf{Z}$.)