2.1.6 Let A, B be additive sets in a *finite* additive group Z, such that $|A| + |B| > |Z|$. Prove that $A + B = A - B = Z$. Give an example to show that the condition $|A| + |B| > |Z|$ cannot be improved.

2.1.7 Show that for any additive set A, the symmetry group $\mathrm{Sym}_1(A)$ of A as defined in the proof of Proposition 2.2 is a finite group contained in $A - A$, obeys the identity $A = A + \mathrm{Sym}_1(A)$, and that A is a union of cosets of $\mathrm{Sym}_1(A)$. (We shall define a more general notion of *symmetry sets* $\mathrm{Sym}_\alpha(A)$ of an additive set in Section 2.6.)

2.1.8 Let $d \geq 1$. Give an example of an additive set A of *integers* such that $|A + A| = 6^d$ and $|A - A| = 7^d$. (see also Lemma 5.25.)

2.2 Doubling constants

The traditional way to measure the additive structure inside an additive set A is via *doubling constants* $\sigma[A]$, which we now define. We will shortly develop two other measures of additive structure, namely the *additive energy* $E(A, A)$, and the concept of a *K-approximate group*, which are also useful, and are closely related to the doubling constant.

Definition 2.4 (Doubling constant) For an additive set A, the *doubling constant* $\sigma[A]$ is defined to be the quantity

$$\sigma[A] := \frac{|2A|}{|A|} = \frac{|A + A|}{|A|}.$$

Similarly we define the *difference constant* $\delta[A]$ as

$$\delta[A] := \frac{|A - A|}{|A|}.$$

From (2.2) we thus have the bounds

$$1 \leq \sigma[A] \leq \frac{|A| + 1}{2} \text{ and } 1 \leq \delta[A] \leq \frac{|A| - 1}{2} + \frac{1}{|A|}.$$

The upper bound here is quite easy to attain; for instance if $A = 2^\wedge[0, N) = \{1, 2, 2^2, \ldots, 2^{N-1}\} \subset \mathbf{Z}$, then $|A| = N$, $|A + A| = \frac{N(N+1)}{2}$, and $|A - A| = \frac{N(N-1)}{2} + 1$, hence $\sigma[A] = \frac{N+1}{2}$ and $\delta[A] = \frac{N-1}{2} + \frac{1}{N}$. In the converse direction, Proposition 2.2 shows that $\sigma[A] = 1$ (or $\delta[A] = 1$) if and only if A is a coset of a group; we shall elaborate upon this in Proposition 2.7 below.

An additive set A with the maximal value of doubling constant $\sigma[A] = (|A| + 1)/2$ (or equivalently, with maximal difference constant $\delta[A] = \frac{|A|-1}{2} + \frac{1}{|A|}$) is known as a *Sidon set* or a *B_2 set*. Informally, this means that all the pairwise sums of A are distinct, excluding the trivial equalities coming from the identity $a + b = b + a$; see Exercise 2.2.1. We will revisit Sidon sets in Section 4.5.

There are various senses in which this behavior is "generic"; for instance, if A is a set of N real numbers chosen uniformly at random from the unit interval $\{x \in \mathbf{R} : 0 \leq x \leq 1\}$, then we see from Exercise 2.1.1 that A is a Sidon set with probability 1, and so $|A+A| = \frac{N(N+1)}{2}$; the point is that if $\{a,b\} \neq \{c,d\}$ then $a+b$ and $c+d$ will "generically" be distinct. A more interesting question is to understand the conditions under which the doubling constant $\sigma[A]$ (or difference constant $\delta[A]$) can be *small*.

As mentioned earlier, $\sigma[A] = 1$ if and only if A is the coset of a finite subgroup G of Z. We thus expect that if A has a doubling constant which is small, but not actually equal to 1, then it should behave "approximately" like a group (up to translations); we shall see several manifestations of this heuristic throughout this book, when we develop more tools with which to analyze the doubling constant. Indeed, the study of sets of small doubling constant can be thought of as a kind of "approximate group theory", with the inverse sum set theorems of Chapter 5 then being analogous to a classification theorem for groups.

The study of sets with close to maximal doubling appears to be hopeless at present. A probabilistic construction of Ruzsa [291] shows that there exist large additive sets A with $|A-A|$ very close to the maximal value of $|A|^2$, but $|A+A| < |A|^{2-c}$ for some explicit absolute constant $c > 0$; and similarly with the roles of $A-A$ and $A+A$ reversed.

Exercises

2.2.1 Let A be an additive set. Show that A is a Sidon set if and only if, for any $a,b,c,d \in A$, we have $a+b \neq c+d$ unless $\{a,b\} = \{c,d\}$.

2.2.2 Let Z be an additive group, let $a, r \in Z$, and let $N \geq 1$ be an integer. Let $P = \{a, a+r, \ldots, a+(N-1)r\}$ be an arithmetic progression in Z. Show that $\sigma[P] \leq 2 - \frac{1}{N}$, with equality if and only if $\mathrm{ord}(r) \geq 2N-1$, where $\mathrm{ord}(r)$ is the order of the group element r in Z.

2.2.3 If $\phi : Z' \to Z$ is a surjective group homomorphism whose kernel $\ker(\phi) := \phi^{-1}(\{0\})$ is finite, and A is an additive set in Z, show that $\sigma[\phi^{-1}(A)] = \sigma[A]$.

2.2.4 If A, A' are additive sets in Z, Z' respectively, show that $\sigma[A \times A'] = \sigma[A]\sigma[A']$. In particular $\sigma[A^{\oplus d}] = \sigma[A]^d$ for all $d \geq 1$.

2.2.5 Let A be any additive set. Show that a non-empty subset of A can have doubling constant at most $\sqrt{\sigma[A]|A|/2}$. Give examples that show that this bound cannot be improved except by an absolute constant. What is the analogous statement for the difference constant?

2.2.6 [100] Let A be any additive set. Show that a Sidon set contained in A can have cardinality at most $\sqrt{2\sigma[A]|A|}$. (Thus sets with small doubling