for some proper subgroup H of G. Since, by Lagrange's theorem, the order $|H|$ of any subgroup H of G divides the order $|G|$ of the group G, we have $|H| \le |G|/p$. Therefore,

$$3|A| \le |G| + |H| \le (1 + 1/p)|G|,$$

and the desired result follows. □

What about the lower bounds for $\alpha(G)$?

We have already seen that for $G = \mathbb{Z}_n$ with even n, we have an equality $\alpha(G) = |G|/2$. If $G = \mathbb{Z}$ is the group of integers, then

$$\alpha(S) > |S|/3$$

for any finite subset $S \subseteq \mathbb{Z} \setminus \{0\}$ (we have proved this fact in Sect. 18.2 using the probabilistic argument). For other Abelian groups the situation is not so clear.

The following naive argument shows that in this case also

$$\alpha(G) \ge \sqrt{|G|} - 1.$$

To show this, let A be a maximal sum-free subset. If $a \notin A$, then $A \cup \{a\}$ is not sum-free by the assumption, so we can write $a = s_1 + s_2$ for some $s_1, s_2 \in A$. Therefore $|G \setminus A| \le |A|^2$, from which the desired inequality $|A| \ge \sqrt{|G|} - 1$ follows.

Better lower bounds can be derived using an improvement of Theorem 25.10, also due to Kneser, which states that with the same hypotheses, either $|A + B| \ge |A| + |B|$ or $|A + B| \ge |A| + |B| - |H|$ for some proper subgroup H such that $H + A + B = A + H$ (see, for example, Street (1972) for the proof). Here we only mention that the best know lower bound for an arbitrary finite Abelian group G is $\alpha(G) \ge 2|G|/7$. More information about the properties of sum-free sets can be found, for example, in Nathanson (1996).

25.4 Sum-product sets

For every $A \subset \mathbb{R}$ we let $A+A = \{a+b : a, b \in A\}$ and $A \cdot A = \{ab : a, b \in A\}$. An old conjecture of Erdős states that, for every $\epsilon > 0$, every sufficiently large finite set $A \subset \mathbb{R}$ satisfies

$$\max\{|A + A|, |A \cdot A|\} \ge |A|^{2-\epsilon}.$$

That is, this conjecture asserts that every set of numbers A must have either a large sum-set $A + A$ or a large product set $A \cdot A$. The conjecture is central to our understanding of the interplay between the additive and multiplicative properties of a set of numbers.

Erdős and Szemerédi (1983) were the first to prove that there exists $\delta > 0$ so that $\max\{|A+A|, |A\cdot A|\} \geq |A|^{1+\delta}$ for all sufficiently large sets A. This parameter δ has been steadily improved by a number of authors. One highlight in this sequence is a proof by Elekes (1997) that δ may be taken arbitrarily close to $1/4$. His argument utilizes a clever application of the Szemerédi–Trotter theorem on point-line incidences (see Theorem 18.7).

Recall that the Szemerédi–Trotter theorem asserts the following: If $2 \leq k \leq \sqrt{N}$ and if we take any set of N points in the plane, then it is not possible to draw more than $O(N^2/k^3)$ lines so that each of them contains at least k of the points.

Theorem 25.13 (Elekes 1997)**.** *There is an absolute constant $\epsilon > 0$ such that, for every set A of non-negative real numbers,*

$$\max\{|A+A|, |A\cdot A|\} \geq \epsilon |A|^{5/4}\,.$$

Proof. Let $n = |A|$, and consider the following n^2 straight lines

$$f_{a,b}(x) := a(x-b) = ax - ab \qquad \text{for } a, b \in A.$$

Observe that, for every $a, b \in A$, the function maps at least n elements $b + c$ with $c \in A$ to some elements $f_{a,b}(b+c) = a \cdot c$ of $A \cdot A$. From a geometric point of view, this means that the graph of each of these $m = n^2$ lines $f_{a,b}(x)$ contains $k = n$ or more points of $P := (A+A) \times (A \cdot A)$. By applying the Szemerédi–Trotter theorem to P with $k = n$ and $N = |P|$, we get $n^2 = O(|P|^2/n^3)$, that is

$$|A+A| \cdot |A \cdot A| = |P| = \Omega(n^{5/2})\,. \qquad \square$$

In the case of *finite* fields we have the following result.

Theorem 25.14 (Garaev 2007)**.** *Let p be a prime number, and $A \subseteq \mathbb{F}_p \setminus \{0\}$. Then the number of elements in at least one of the sets $A+A$ or $A \cdot A$ is at least an absolute constant times*

$$\min\left\{\sqrt{p|A|},\ \frac{|A|^2}{\sqrt{p}}\right\}.$$

In particular, if $|A| \approx p^{2/3}$ then this minimum is about $|A|^{5/4}$.

Proof (due to Solymosi 2009). His idea is a very clever application of the expander mixing lemma (Lemma 15.5). As in Sect. 15.2.1, consider a graph G whose vertices are $n = p(p-1)$ pairs (a, b) of elements of a finite field $\mathbb{Z}_p$ with $a \neq 0$, and two vertices (a, b) and (c, d) are joined by an edge iff $ac = b + d$ (all operations modulo p). We already know that this graph is $(p-1)$-regular and that the second largest eigenvalue λ of its incidence matrix is smaller than $\sqrt{3p}$ (see Lemma 15.6). So, if we define $S, T \subseteq V$ by

$$S = (A \cdot A) \times (-A) \quad \text{and} \quad T = (A^{-1}) \times (A + A)$$

then the expander mixing lemma (Lemma 15.2) tells us that

$$\begin{aligned} e(S,T) &\leq \frac{(p-1)|S||T|}{p(p-1)} + \lambda\sqrt{|S||T|} = \frac{|S||T|}{p} + \lambda\sqrt{|S||T|} \\ &< \frac{|A \cdot A||A + A||A|^2}{p} + \sqrt{3p|A \cdot A||A + A||A|^2}\,, \end{aligned}$$

where the second inequality used $\lambda < \sqrt{3p}$. But for every $a, b, c \in A$ there is an edge between vertices $(ab, -c) \in S$ and $(b^{-1}, a+c) \in T$, so that $e(S,T) \geq |A|^3$. Thus, if we set $N := |A + A||A \cdot A|$, then rearranging the resulting inequality

$$\begin{aligned} |A|^3 \leq e(S,T) &\leq \frac{N|A|^2}{p} + |A|\sqrt{3pN} \\ &= \sqrt{N}\left(\frac{\sqrt{N}|A|^2}{p} + |A|\sqrt{3p}\right) \end{aligned}$$

gives

$$\sqrt{N} > \left(\frac{\sqrt{N}}{p|A|} + \frac{\sqrt{3p}}{|A|^2}\right)^{-1}.$$

Now, since $(x+y)^{-1} \geq \frac{1}{2}\min\{x^{-1}, y^{-1}\}$ for positive x and y, we find that

$$\sqrt{N} \geq \epsilon \cdot \min\left\{\frac{p|A|}{\sqrt{N}},\ \frac{|A|^2}{p^{1/2}}\right\}$$

with $\epsilon = 1/2\sqrt{3}$, which in turn implies

$$\sqrt{N} \geq \epsilon \cdot \min\left\{\sqrt{p|A|},\ \frac{|A|^2}{\sqrt{p}}\right\}.$$

To finish the proof, we need only use the two-term arithmetic-geometric mean inequality:

$$\max\{|A + A|, |A \cdot A|\} \geq \frac{|A \cdot A| + |A + A|}{2} \geq \sqrt{|A \cdot A||A + A|} = \sqrt{N}\,.$$

□