4.1.14 Let G, H be two subgroups of Z and let x be an element of Z chosen randomly. Show that the indicators $\mathbf{I}(x \in G)$ and $\mathbf{I}(x \in H)$ have non-negative correlation, i.e. $\mathbf{Cov}(\mathbf{I}(x \in G), \mathbf{I}(x \in H)) \geq 0$; establish this both by Fourier-analytic means and by direct computation. Show that equality occurs if and only if $G + H = Z$.

4.1.15 Show that for any subgroup G of Z, we have $(G^\perp)^\perp = G$, and for any random variable f, we have $\widehat{\hat{f}}(x) = |Z|^{-1} f(-x)$. More generally, for any $A \subset Z$, we have $\langle A \rangle = (A^\perp)^\perp$, where $\langle A \rangle$ is the group generated by A.

4.1.16 If Z and Z' are finite groups, formulate a rigorous version of the statement that the Fourier transform on $Z \times Z'$ is the composition of the Fourier transform on Z and the Fourier transform on Z'.

4.2 L^p theory

We now turn to the analytic theory of the Fourier transform and of convolutions, starting with the L^p theory, and then apply it to the problem of locating arithmetic progressions inside sum sets.

If $f \in \mathbf{C}^Z$ and $0 < p < \infty$, we define the $L^p(Z)$ *norm* of f to be the quantity

$$\|f\|_{L^p(Z)} := (\mathbf{E}_Z |f|^p)^{1/p} = (\mathbf{E}_{x \in Z} |f(x)|^p)^{1/p}.$$

Thus for instance $\|f\|_{L^2(Z)}$ is just the Hilbert space magnitude of f. We also define

$$\|f\|_{L^\infty(Z)} = \sup_{x \in Z} |f(x)|.$$

Similarly we define

$$\|f\|_{l^p(Z)} := \left(\sum_{\xi \in Z} |f(\xi)|^p \right)^{1/p}$$

for $0 < p < \infty$ and

$$\|f\|_{l^\infty(Z)} := \sup_{\xi \in Z} |f(\xi)|.$$

We have the following two basic L^p estimates on the Fourier transform and on convolution.

Theorem 4.8 *Let $f, g : Z \to \mathbf{C}$ be functions on an additive group Z. Then for any $1 \leq p \leq 2$ we have the* Hausdorff–Young inequality

$$\|\hat{f}\|_{l^{p'}(Z)} \leq \|f\|_{L^p(Z)} \tag{4.12}$$

where the dual exponent p' to p is defined by $\frac{1}{p} + \frac{1}{p'} = 1$. Also, whenever $1 \leq p, q, r \leq \infty$ are such that $\frac{1}{p} + \frac{1}{q} = \frac{1}{r} + 1$, we have the Young inequality

$$\|f * g\|_{L^r(Z)} \leq \|f\|_{L^p(Z)} \|g\|_{L^q(Z)}. \tag{4.13}$$

Both inequalities follow easily from Riesz–Thorin complex interpolation theorem. With this theorem, one only needs to verify the extremal (and easy) cases. The Riesz–Thorin theorem, however, is beyond the scope of this book. On the other hand, one can also have an elementary proof, using combinatorial arguments (see Exercise 4.2.3).

Recall the additive energy $E(A, B)$ between two additive sets A, B in Z, defined in Definition 2.8. From that definition one can easily check that

$$E(A, B) = |Z|^3 \|1_A * 1_B\|^2_{L^2(Z)}.$$

By (4.2) and (4.9) we obtain the fundamental identity

$$E(A, B) = |Z|^3 E(1_A, 1_B) = |Z|^3 \sum_{\xi \in Z} |\hat{1}_A(\xi)|^2 |\hat{1}_B(\xi)|^2. \tag{4.14}$$

This formula may illuminate some of the properties of the additive energy that were obtained in Section 2.3, such as the symmetries $E(A, B) = E(B, A) = E(A, -B)$ and the Cauchy–Schwarz inequality (2.9); see Exercise 4.2.7.

For the purposes of additive combinatorics, the Fourier transform is most useful when applied to characteristic functions $f = 1_A$, and in this case one can say quite a bit about the Fourier transform and its relation to the additive energy $E(A, A)$.

Lemma 4.9 *Let A be a subset of a finite additive group Z, and let $\widehat{1_A} : Z \to \mathbf{C}$ be the Fourier transform of the characteristic function of A. Then we have the identities:*

$$\|\widehat{1_A}\|_{l^\infty(Z)} = \sup_{\xi \in Z} |\widehat{1_A}(\xi)| = \widehat{1_A}(0) = \mathbf{P}_Z(A); \tag{4.15}$$

$$\|\widehat{1_A}\|^2_{l^2(Z)} = \sum_{\xi \in Z} |\widehat{1_A}(\xi)|^2 = \mathbf{P}_Z(A); \tag{4.16}$$

$$\widehat{1_A}(\xi) = \overline{\widehat{1_A}(-\xi)}; \tag{4.17}$$

$$\|\widehat{1_A}\|^4_{l^4(Z)} = \sum_{\xi \in Z} |\widehat{1_A}(\xi)|^4 = \frac{E(A, A)}{|Z|^3}; \tag{4.18}$$

$$\widehat{1_A}(\xi) = \sum_{\eta \in Z} \widehat{1_A}(\eta) \widehat{1_A}(\xi - \eta). \tag{4.19}$$

This lemma follows easily from the estimates that have already been established; see Exercise 4.2.4.

We now present a simple application of the Fourier transform in the setting of a finite field F.

Lemma 4.10 *[41] Let F be a finite field, and let A be a subset of $F\backslash\{0\}$ such that $|A| > |F|^{3/4}$. Then*

$$3(A \cdot A) = A \cdot A + A \cdot A + A \cdot A = F.$$

Proof We give F a symmetric non-degenerate bilinear form of the type in Example 4.2. Let $f : F \to \mathbf{R}$ denote the non-negative function

$$f := \mathbf{E}_{a \in A} 1_{a \cdot A}.$$

Observe that $\operatorname{supp}(f) = A \cdot A$ and $\hat{f}(0) = \mathbf{E}_F f = \mathbf{P}_F(A)$. Taking Fourier transforms we obtain

$$\hat{f}(\xi) = \mathbf{E}_{a \in A} \widehat{1_A}(\xi/a)$$

for any $\xi \in F$. If $\xi \neq 0$, then we observe that the frequencies ξ/a are all distinct as a varies. Using Cauchy–Schwarz and then (4.16), we then obtain

$$|\hat{f}(\xi)| \leq \frac{1}{|A|}|A|^{1/2}\mathbf{P}_F(A)^{1/2} = 1/|F|^{1/2} \text{ for } \xi \neq 0.$$

Now let $x \in F$ be arbitrary. We use (4.4) and (4.9) to compute

$$\begin{aligned} f * f * f(x) &= \operatorname{Re} f * f * f(x) \\ &= \operatorname{Re} \sum_{\xi \in F} \hat{f}(\xi)^3 e(\xi \cdot x) \\ &\geq \operatorname{Re} \hat{f}(0)^3 - \sum_{\xi \in F\backslash\{0\}} |\hat{f}(\xi)|^3 \\ &\geq \mathbf{P}_F(A)^3 - \sum_{\xi \in F} |F|^{-1/2}|\hat{f}(\xi)|^2 \\ &= \mathbf{P}_F(A)^3 - |F|^{-1/2}\mathbf{P}_F(A) \\ &> 0 \end{aligned}$$

since $\mathbf{P}_F(A) > |F|^{-1/4}$ by hypothesis. Since $\operatorname{supp}(f * f * f) = 3(A \cdot A)$ and x was arbitrary, we are done. □

Remark 4.11 Lemma 4.10 is a simple example of a *sum-product estimate* – an assertion that a combination of a sum and product of a set A is necessarily much larger than A itself. It can be viewed as a quantitative reflection of the fact that a set A of cardinality greater than $|F|^{3/4}$ has difficulty behaving like a subfield of F. It should be compared with the results in Section 2.8.

Exercises

4.2.1 Let $1 \leq p < \infty$. By exploiting the convexity of the function $x \mapsto |x|^p$, establish the convexity of the set $\{f \in \mathbf{C}^Z : \|f\|_{L^p(Z)} \leq 1\}$, and conclude the *triangle inequality*

$$\|f + g\|_{L^p(Z)} \leq \|f\|_{L^p(Z)} + \|g\|_{L^p(Z)}.$$

Argue similarly for the $p = \infty$ case and with L^p replaced by l^p.

4.2.2 Let $1 < p < \infty$, and let p' the dual exponent, thus $1/p + 1/p' = 1$. By exploiting the convexity of the function $x \mapsto e^x$, establish the preliminary inequality

$$\mathbf{E}_{x\in Z}|f(x)||g(x)| \leq 1 \text{ whenever } \|f\|_{L^p(Z)}, \|g\|_{L^{p'}(Z)} \leq 1,$$

and then conclude *Hölder's inequality*

$$\|fg\|_{L^r(Z)} \leq \|f\|_{L^p(Z)}\|g\|_{L^q(Z)}$$

whenever $0 < p, q, r \leq \infty$ are such that $\frac{1}{p} + \frac{1}{q} = \frac{1}{r}$. Similarly with the L^p norms replaced by l^p norms.

4.2.3 The purpose of this exercise is to give a proof of Theorem 4.8 that does not require complex interpolation. First use (4.2), the trivial bound

$$\|\hat{f}\|_{l^\infty(\mathbf{Z})} \leq \|f\|_{L^1(\mathbf{Z})}, \tag{4.20}$$

and Hölder's inequality to establish the weaker estimate

$$\|\hat{f}\|_{l^{p'}(Z)} = O_p(\|f\|_{L^p(Z)})$$

whenever $f \in \mathbf{C}^Z$ is supported on a set A and obeys an estimate of the form $|f(x)| = \Theta(\lambda)$ for all $x \in A$ and some threshold λ. Then, prove the even weaker estimate

$$\|\hat{f}\|_{l^{p'}(Z)} = O_p(\|f\|_{L^p(Z)} \log(1 + |Z|))$$

for arbitrary $f \in \mathbf{C}^Z$ by applying the previous inequality to a dyadic decomposition of f, followed by the triangle inequality. Finally, remove the $O_p(\log(1 + |Z|))$ factor to establish (4.12) by replacing Z with a large power Z^M of Z, and similarly replacing f with a large tensor power (as in Corollary 2.19) and letting $M \to \infty$. Argue similarly to establish (4.13).

4.2.4 Prove Lemma 4.9.

4.2.5 Let A be an additive set in a finite additive group Z. Show that $\hat{1}_A$ is real-valued if and only if A is symmetric.

4.2.6 (Law of large numbers for finite groups) Let $f : Z \to \mathbf{R}_{\geq 0}$ be such that $\mathbf{E}_Z f = 1$ and $f(0) \neq 0$, and let H be the subgroup of Z generated by $\text{supp}(f)$. Show that $|\hat{f}(\xi)| \leq 1$, with equality if and only if $\xi \in H^\perp$.