0

Duality and Fourier analysis

The notion of duality and its action in analytic number theory informs this entire work. Emphasis is given to the interplay between the arithmetic and analytic meaning of inequalities. The following remarks place ideas employed in the present work within a broader framework.

1. Conics. By duality the notion of a point conic gives rise to the notion of a line conic. The members of the line conic comprise the tangents to the point conic. Slightly surrealistically we may regard a conic to be a geometric object, defined from the inside by a point locus, and from the outside by a line envelope.

2. Dual spaces. Let V be a finite dimensional vector space over a field F. The dual of V is the vector space of linear maps of V into F. The space V and its dual, V', are isomorphic.

To every linear map $T : V \to W$ between spaces, there corresponds a dual map $T' : W' \to V'$. In standard notation, the action $f(x)$ of a function f upon x is written $\langle x, f \rangle$. The dual map T' is defined by $\langle Tx, y' \rangle = \langle x, T'y' \rangle$ where x, y' denote typical elements of V, W' respectively.

Let $V = F^n$, $W = F^m$. We may identify W' with the set of maps $W \to F$ given by $k \mapsto k^t y'$, where y' is a vector in W, t denotes transposition. If we employ a similar identification for V', then T is represented by an m-by-n matrix with entries in F, T' by the transpose of the same matrix. The defining relation of the dual map may be expressed in the form $(Ha)^t b = a^t(H^t b)$, where $H = (h_{ij})$, $1 \le i \le m$, $1 \le j \le n$, represents T. In other terms

(i)
$$\sum_{i=1}^{m} \sum_{j=1}^{n} h_{ij} a_j b_i = \sum_{j=1}^{n} a_j \sum_{i=1}^{m} h_{ij} b_i .$$

If we set $a_i = 1 = b_j$ for every i, j, then we may view the interchange of two summations as a 'computation through the dual'.

A non-zero vector x is an eigenvector of an operator $T : V \to V$, and λ is the corresponding (scalar) eigenvalue, if $Tx = \lambda x$. The set of all such x corresponding to a fixed eigenvalue comprises an eigenspace of T.

3. Spectral decomposition. On a finite dimensional vector space V over the complex numbers an inner product $(\ ,\ )$ can be defined. Riesz' representation theorem asserts that each linear map of V into $\mathbb{C}$ has the form $x \mapsto (x, w)$ for a unique vector w in V. To each linear operator T from V to itself there corresponds an adjoint operator T^*, also from V into itself, and defined by $(Tx, y) = (x, T^*y)$ for all x, y in V.

The operator T is self-adjoint with respect to the inner product if $T = T^*$. The spectral theorem then asserts the existence of a basis for V, orthogonal with respect to the inner product and comprised of eigenvectors of T.

An operator S which commutes with T takes each eigenspace of T into itself. If S is self-adjoint with respect to the same inner product, then we may spectrally decompose each eigenspace by S. Continuing in this manner we see that the basis vectors in the spectral decomposition of V by T may be chosen simultaneous eigenvectors of any (mutually) commuting family of self-adjoint operators which contains T.

The notion of an eigenvector has a meaning for any finite dimensional vector space over a field F, but complications occur. Let $T : F^n \to F^n$ be represented by the matrix H, and let I denote the n-by-n unit matrix. Then λ is (formally) an eigenvalue of T if and only if $\det(H - \lambda I) = 0$. It is clear that the solutions λ to this polynomial equation need not belong to the ground field F. In order to employ all the eigenfunctions, it is apparently necessary to work in a space on which the associated operator is not initially defined. The simplest groundfield analogue of $\mathbb{C}$ would be an algebraically closed field; but that abandons structural advantages attached to fields that are not algebraically closed. For example, over the reals a linear combination of self-adjoint operators is again self-adjoint. Over the complex numbers it need not be.

The Riesz representation allows an inner product space V to be identified with its dual. The identification is not quite a linear map since for a scalar λ, $(x, \lambda w) = \bar{\lambda}(x, w)$; a complex conjugation appears. However, with an appropriate interpolation of this identification and its inverse, to each linear map $T : V \to W$ between inner product spaces, there corresponds an adjoint linear map $T^* : W \to V$, formally defined by $(Tx, y) = (x, T^*y)$, the inner products evaluated in their respective spaces.

On $\mathbb{C}^n$, the standard inner product is given by $(u, v) = \sum_{j=1}^{n} u_j \bar{v}_j$. If the operator $T : \mathbb{C}^n \to \mathbb{C}^m$ is represented by the matrix H, then T^* is represented by $\bar{H}^t$, the complex conjugate transpose of H. There is an analogue of the identity (i), with every b_i replaced by $\bar{b}_i$, and we may correspondingly speak of 'computation through the adjoint'.

4. Banach spaces. The dual of a Banach space over $\mathbb{C}$ is the space of bounded linear operators into $\mathbb{C}$. Two Banach spaces are isometric if there is an isomorphism between them in which the norms of corresponding elements have the same value. Whilst a Banach space is isometric to a subspace of its second dual, neither the first nor second dual of a Banach space need be isometric to the original space. The formalism of **2** carries over, moreover $\|T\| = \|T'\|$.

Hilbert spaces are the Banach spaces whose norm is induced by an inner product. The definition of the adjoint operator between Hilbert spaces slightly extends that for finite dimensional vector spaces, and $\|T\| = \|T^*\|$. For each self-adjoint operator there is a corresponding spectral decomposition of the space on which it acts. However, the spectrum of an operator may contain a continuous component, and the corresponding decomposition of an arbitrary vector in the Hilbert space will then employ projection valued measures.

I assume the spectral decomposition theorem for Hilbert spaces only in the background discussion of Chapter 21. However, the interpretation of finite dimensional vector spaces as Banach spaces with respect to various norms is a notion central to the present work. Moreover, estimates of the spectra of operators on an appropriate inner product space are explicitly or implicitly important. The methods are elementary, the viewpoint perhaps sophisticated.

5. Duality principle. Let h_{ij}, $1 \le i \le m$, $1 \le j \le n$, be mn complex numbers. Narrowly interpreted, the *principle of duality*, as it is often called, asserts that

$$\text{(ii)} \qquad \sum_{i=1}^{m} \left| \sum_{j=1}^{n} a_j h_{ij} \right|^2 \le \lambda \sum_{j=1}^{n} |a_j|^2$$

is valid for all complex a_j, if and only if

$$\text{(iii)} \qquad \sum_{j=1}^{n} \left| \sum_{i=1}^{m} b_i h_{ij} \right|^2 \le \lambda \sum_{i=1}^{m} |b_i|^2$$

is valid for all complex b_i. A simple proof of this particular assertion is given in Chapter 3. The principle may be employed to give a unifying interpretation of inequalities of Large Sieve type, [30].

Let H denote the matrix (h_{ij}). Inequality (ii) asserts that the operator $T : \mathbb{C}^n \to \mathbb{C}^m$, given by $a \mapsto Ha$, in terms of the standard euclidean norms on $\mathbb{C}^n$ and $\mathbb{C}^m$ satisfies $\|T\| \le \lambda^{1/2}$. The companion inequality asserts that the dual operator $T' : \mathbb{C}^m \to \mathbb{C}^n$ given by $b \mapsto H^t b$ satisfies $\|T'\| \le \lambda^{1/2}$. The principle of duality follows from the assertion $\|T\| = \|T'\|$ of **4**.

In terms of norms

$$|a|_\alpha = \left(\sum_{j=1}^{n} |a_j|^\alpha \right)^{1/\alpha}, \quad |b|_{\alpha'} = \left(\sum_{i=1}^{m} |b_i|^{\alpha'} \right)^{1/\alpha'}, \quad \frac{1}{\alpha} + \frac{1}{\alpha'} = 1,$$

a similar application of functional analysis shows that

$$\sup_{a \ne 0} |a|_\alpha^{-1} \left(\sum_{i=1}^{m} \left| \sum_{j=1}^{n} a_j h_{ij} \right|^\alpha \right)^{1/\alpha}$$

$$\sup_{b \ne 0} |b|_{\alpha'}^{-1} \left(\sum_{j=1}^{n} \left| \sum_{i=1}^{m} b_i h_{ij} \right|^{\alpha'} \right)^{1/\alpha'}$$

have identical values. Applications of Hölder's inequality show that each of these expressions has the same value as

$$\sup_{\substack{a,b \\ \text{non null}}} (|a|_\alpha |b|_{\alpha'})^{-1} \left| \sum_{i=1}^{m} \sum_{j=1}^{n} b_i a_j h_{ij} \right|.$$

From the case $\alpha = \alpha' = 2$, we see that in this setting the duality principle is equivalent to estimating a bilinear form universally.

The left hand side of (ii) has the representations $(Ha, Ha) = (a, \bar{H}^t Ha)$ by the standard inner product on $\mathbb{C}^n$. The best value of λ is the spectral radius of the self-adjoint operator on $\mathbb{C}^n$ represented by $\bar{H}^t H$. This same value is the spectral radius of the self-adjoint operator on $\mathbb{C}^m$ represented by $H\bar{H}^t$.

More generally, the duality principle asserts that certain inequalities come in pairs, and that each pair is equivalent to an estimate for the (equal) spectral radii of a corresponding pair of self-adjoint operators, [30].

Over the last twenty years the duality principle has been increasingly applied in analytic number theory. A main difficulty is the conceptualisation of the problem to hand in terms which allow interpretations of a universal nature. For example, many problems may be reduced to the estimation of sums

$$\sum_{i=1}^{m} \left| \sum_{j=1}^{n} a_j h_{ij} \right|^2$$

or similar. Typically, the a_j are known only in some weak sense, their individual values difficult to obtain. In such circumstances it is often advantageous to allow the a_j to vary freely and seek estimates of the type (ii) through the agency of an appropriate dual, such as (iii). To aid this process we may modify the h_{ij}, for example, by introducing convenience factors, so that the spectral radius of the underlying operator may be readily approached. Amongst many objects, the unlikely may serve as a variable, for example a chain of characters defined on differing groups but possessing a common property.

Variations on the duality principle are employed throughout the present volume. When the h_{ij} are values of characters, this principle has something of the nature of a reciprocity theorem. An illustrative example in the estimation of a character sum using duality is given at the end of Chapter 23. An example applied to the study of the global distribution of the class number of imaginary quadratic fields occurs in [41] Chapter 22.

Several applications of the duality principle, one involving the use of prime numbers as a support set, are vital to the characterisation of differences of additive functions made in [39]. A typical application of the principle to the estimation of character sums appears in Heath-Brown, [97], Lemma 11.1, p. 319, in the course of his proof that for all sufficiently large moduli q, every reduced residue class (mod q) contains a prime not exceeding $q^{11/2}$. I indicate other examples as this volume proceeds.

6. Fourier analysis (mod 1). Fourier analysis arose historically from the practice of constructing general solutions to partial differential equations important in physics by using the superposition of simpler solutions. Dirichlet was the first to provide a wide class of functions of finite period which are equal to convergent sums of their corresponding formal Fourier series. Such complex valued functions f, of period 1, have an expansion

$$f(x) = \sum_{k=-\infty}^{\infty} a_k e^{2\pi i k x},$$

where

$$a_k = \int_0^1 f(x) e^{-2\pi i k x} dx.$$

Fourier series have been embraced within general disciplines.

7. Locally compact groups. The dual of a locally compact abelian group is the group of its continuous homomorphisms into the unit circle in the complex plane with topology induced by the standard topology on $\mathbb{C}^2$. These homomorphisms are called the characters of the group. G will denote a typical group, $\widehat{G}$ its dual and U the unit circle in $\mathbb{C}^2$. Pontryagin and van

Kampen showed that with a suitable topology $\widehat{G}$ becomes locally compact, and $\widehat{\widehat{G}}$ is isomorphic to G.

G has a translation invariant Haar measure, unique up to renormalisation. If $d\mu$ denotes this measure, and χ a typical character on G, then a formal Fourier transform of a function $f : G \to \mathbb{C}$ is the function $\hat{f} : \widehat{G} \to \mathbb{C}$ given by

$$\chi \mapsto \int_G f\bar{\chi}d\mu.$$

Under favourable circumstances there is an inverse transform relating f to the function

$$g \mapsto \int_{\widehat{G}} \hat{f}(\chi)\chi(g)d\nu,$$

where g denotes a typical element of G, and $d\nu$ the Haar measure on $\widehat{G}$.

G is discrete if and only if its dual group is compact. We may then renormalise the Haar measure to give the dual space measure 1, and regard the elements of G as random variables on $\widehat{G}$. To effect this view in general we may condition the measure on $\widehat{G}$.

To an extent, analytic number theory is the study of certain discrete groups by means of their (compact) duals.

8. Fourier analysis (mod 1) revisited. In remark **6**, f is defined on the quotient of additive groups $\mathbb{R}/\mathbb{Z}$. The characters on this group are $x \mapsto e^{2\pi ikx}$, one for each integer k. $\mathbb{R}/\mathbb{Z}$ has dual group $\mathbb{Z}$.

We can define an inner product on the Lebesgue class $L^2(0,1)$ and so on $L^2(\mathbb{R}/\mathbb{Z})$ by

$$(f,g) = \int_0^1 f(x)\overline{g(x)}dx.$$

With this definition $L^2(\mathbb{R}/\mathbb{Z})$ becomes a Hilbert space. In an abuse of notation, the classical orthogonality of exponentials may be expressed:

$$(e^{2\pi ikx}, e^{2\pi imx}) = 0 \quad \text{if} \quad k \neq m.$$

The exponentials $e^{2\pi ikx}$ are eigenfunctions of the differential operator $\frac{d^2}{dx^2}$. It is tempting to try and derive a Fourier expansion from the spectral decomposition theorem. However, this differential operator, although formally self-adjoint on the space of L^2 functions, does not take $L^2(\mathbb{R}/\mathbb{Z})$ into itself. If we cut $L^2(\mathbb{R}/\mathbb{Z})$ down to $\mathbb{C}^\infty(\mathbb{R}/\mathbb{Z})$, the subspace of functions infinitely differentiable, then $\frac{d^2}{dx^2}$ is indeed self-adjoint; but the space $C^\infty(\mathbb{R}/\mathbb{Z})$ is not complete with respect to the norm induced by the inner product. This difficulty is the topological analogue of the algebraic field-of-definition problem attached to the eigenvalues of operators on a finite dimensional space.

Again we wish to extend an operator to a more comprehensive space. Since $\mathbb{C}^\infty(\mathbb{R}/\mathbb{Z})$ is dense in $L^2(\mathbb{R}/\mathbb{Z})$ and $(-g'', g) = (g', g') \geq 0$ there, a theorem of Friedrichs ensures a self-adjoint extension of $-\frac{d^2}{dx^2}$ to $L^2(\mathbb{R}/\mathbb{Z})$. The rôle of $\mathbb{C}^\infty(\mathbb{R}/\mathbb{Z})$ may also be played by the polynomials in $\exp(2\pi i x)$. The subtleties of Fourier analysis begin to reveal themselves.

From the orthogonality of the exponential characters we derive Parseval's relation:

$$\int_0^1 \left| \sum_{|k|\leq n} a_k e^{2\pi i k x} \right|^2 dx = \sum_{|k|\leq n} |a_k|^2,$$

valid for all a_k in $\mathbb{C}$. If we regard this equality as a bound for a mean square norm, then by duality the functions f in $L^2(\mathbb{R}/\mathbb{Z})$ satisfy

$$\sum_{|k|\leq n} \left| \int_0^1 f(x) e^{2\pi i k x} dx \right|^2 \leq \int_0^1 |f(x)|^2 dx,$$

Bessel's inequality. Moreover, there is a function f, not essentially zero, which gives equality. The Hardy–Littlewood circle method amounts to estimating asymptotically the Fourier coefficients of a given periodic function $f(x)$. The interval $[0, 1)$ is covered by smaller intervals around rational numbers a/q, $1 \leq a \leq q$, $(a, q) = 1$, for varying q, and in part $f(x)$ is treated by reduction to $f(a/q)$.

With the reversal of this method Linnik devised (his inequality of) the Large Sieve, [120].

9. Fourier analysis on $\mathbb{R}$. A typical character of the additive group of reals is given by $x \mapsto e^{itx}$, for some real t. $\widehat{\mathbb{R}}$ is isomorphic to $\mathbb{R}$. The Haar measures on $\mathbb{R}, \widehat{\mathbb{R}}$ are renormalised Lebesgue measure. The choice of renormalisation may vary to effect elegance in the presentation of results.

Control of a function around the origin is equivalent to control of its Fourier transform at infinity (far from the origin). That a function and its Fourier transform cannot both be small at infinity was pointed out by Wiener. As a severe example, let the measurable f and its transform $\hat{f}$ vanish outside a compact set I. Then

$$\hat{f}(t) = \frac{1}{\sqrt{2\pi}} \int_I f(x) e^{-itx} dx$$

defines an everywhere analytic function of complex t. Since $\hat{f}(t)$ vanishes on a half-line $\mathrm{Re}\,(t) > t_0$, $\mathrm{Im}\,(t) = 0$, by analytic continuation $\hat{f} = 0$ identically. For functions belonging to $L^2(\mathbb{R})$, Plancherel's relation asserts that

$$\int_{\mathbb{R}} |\hat{f}(t)|^2 dt = \int_{\mathbb{R}} |f(x)|^2 dx;$$

and here $f = 0$ almost surely.

The property of changing ends through Fourier analysis is much exploited in the theory of probability. To each distribution function $F(u)$ on the line corresponds the Fourier–Stieltjes transform

$$\phi(t) = \int_{\mathbb{R}} e^{itu} dF(u),$$

otherwise known as the characteristic function. Asymptotic properties of the tail $1 - F(z) + F(-z)$, as $|z| \to \infty$, are then equivalent to properties of $\phi(t)$ as $t \to 0$.

Wiener's phenomenon may be compared with the reciprocating action of duality.

Applications of Fourier analysis on $\mathbb{R}$, with and without integration, appear in Chapters 14, 15, 16. Notions from the theory of probability, including that of independent random variables, are explicitly utilised in Chapters 25, 26 and 28.

For functions f supported on a half-line, it is often possible to view $\sqrt{2\pi}\ \hat{f}(-is)$ as a function of the complex variable s. This function is then called the Laplace transform of f. A series of exercises demonstrating the Laplace transform is given in Chapter 7.

10. Poisson summation. In Remark **9** the Fourier transform on $\mathbb{R}$ was renormalised to identify Plancherel's identity within an isometry between the space $L^2(\mathbb{R})$ and its dual. In the present remark it is appropriate to define

$$\hat{f}(t) = \int_{\mathbb{R}} f(x) e^{-2\pi itx} dx, \quad t \text{ in } \mathbb{R}.$$

$\mathbb{Z}$ is a subgroup of $\mathbb{R}$. Under favourable circumstances the function f, defined on $\mathbb{R}$, may be summed over the representatives of a coset to generate a function $\sum_{n=-\infty}^{\infty} f(n+x)$ defined on $\mathbb{R}/\mathbb{Z}$. Expanding this as a Fourier series and reassembling formally gives

$$\sum_{n=-\infty}^{\infty} f(n+x) = \sum_{k=-\infty}^{\infty} e^{2\pi ikx} \hat{f}(n).$$

In particular,

$$\sum_{n=-\infty}^{\infty} f(n) = \sum_{n=-\infty}^{\infty} \hat{f}(n).$$

This last is Poisson summation. The choice of Fourier transform $\hat{f}$ on $\mathbb{R}$ ensures consistency between the Haar measures on $\mathbb{R}$ $(= \widehat{\mathbb{R}})$ and $\mathbb{R}/\mathbb{Z}$ $(= \widehat{\mathbb{Z}})$.

An example is furnished by $f(x) = \exp(-\pi x^2 y)$, $y > 0$. Then $\hat{f}(t) = y^{-1/2}\exp(-\pi t^2 y^{-1})$ and

$$\sum_{n=-\infty}^{\infty} e^{-\pi n^2 y} = \frac{1}{\sqrt{y}} \sum_{n=-\infty}^{\infty} e^{-\pi n^2/y}.$$

The left side representation gives precise asymptotic behaviour as $y \to \infty$, the right as $y \to 0+$. We can change ends.

Once the formula is established, we may extend it to hold for $y = -iz$, z complex, with the complex z-plane cut to guarantee a single valued meaning to $(-iz)^{1/2}$. Evaluating the resulting expressions at suitable rational points, Cauchy could give a proof of the quadratic reciprocity law through the agency of Gauss sums.

A derivation of standard Large Sieve inequalities as an application of the duality principle, implemented by a Poisson summation, is given in [56], Chapter 6, and in the exercises of the present Chapter 4. A sophisticated application of this methodology may be found in a recent paper of Duke and Iwaniec, [24].

11. Dirichlet characters. If we give a finite abelian group the discrete topology, then the dual group is isomorphic to the original group. This process was begun by Dirichlet, who explicitly constructed the characters of the groups of reduced residue classes $(\bmod\, m) : (\mathbb{Z}/m\mathbb{Z})^*$, in the course of his celebrated proof that each such class contains infinitely many primes.

12. Characters on Q^*. Dirichlet characters are readily extended to the multiplicative positive rationals prime to m. We endow Q^*, the multiplicative group of all positive rationals, with the discrete topology. Let Γ_m denote the subgroup of Q^* generated by the primes dividing m. Then there is a canonical homomorphism $Q^* \to Q^*/\Gamma_m$, and

$$Q^* \to Q^*/\Gamma_m \to (\mathbb{Z}/m\mathbb{Z})^* \to U$$

gives a character on Q^*. This is not quite the generalisation favoured in Analytic Number Theory, which extends a Dirichlet character to be zero on the integers that have a prime in common with m.

Since Q^* is a direct sum of the cyclic groups generated by the prime numbers, the dual of Q^* is isomorphic to the direct product of denumerably many copies of $\mathbb{R}/\mathbb{Z}$. A study of the characters of Q^* obtained by factoring by a suitable subgroup,

$$Q^* \to Q^*/\Gamma \to U,$$

can be brought to bear upon the problem of representing rationals as products of given rationals, [48], [51], [52], [56], [78]. To this end the method of the stable dual, including the principle of duality, may in particular be applied. This may be viewed as the beginning of a systematic study of Harmonic Analysis on Q^*.

13. Fourier analysis on $\mathbb{R}^*$. Let $\mathbb{R}^*$ denote the multiplicative group of positive reals. The map $u \mapsto \log u$ renders $\mathbb{R}^*$ isomorphic to the additive group of reals, and induces a topology on $\mathbb{R}^*$ from that on $\mathbb{R}$. Likewise the Haar measure on $\mathbb{R}^*$ is induced by Lebesgue measure on $\mathbb{R}$. The characters on $\mathbb{R}^*$ have the form $x \mapsto x^{it}$, t real. The dual of $\mathbb{R}^*$ is isomorphic to $\mathbb{R}$. Corresponding to the Fourier transform is the Mellin transform. The inversion of a Mellin transform takes place naturally along a line in the complex plane. Using substitution, appropriate formulae may be formally derived from those for Fourier analysis on $\mathbb{R}$.

It was Riemann, in his celebrated paper of 1860, who introduced Mellin transforms into analytic number theory, and with them the accompanying problem of providing analytic continuation for certain Dirichlet series.

Inspired by a method of Euler, Dirichlet based his investigation of the distribution of primes in residue classes upon the study of the L-series $\sum_{n=1}^{\infty} \chi(n)n^{-s}$ associated with the characters χ on $(\mathbb{Z}/m\mathbb{Z})^*$. His s is real, $s > 1$. Both the characters and the series of the form $\sum_{n=1}^{\infty} a_n n^{-s}$ are now named after him. It is clear that a Dirichlet series is a Mellin–Stieltjes transform

$$\int_{1-}^{\infty} y^{-s} d\left(\sum_{n\le y} a_n\right).$$

In its half-plane of absolute convergence, a Dirichlet series has the representation

$$\sum_{n=1}^{\infty} a_n n^{-s} = s\int_1^{\infty} y^{-s} \sum_{n\le y} a_n y^{-1} dy,$$

with $y^{-1}dy$ the Haar measure on $\mathbb{R}^*$. Under the property of changing ends, to investigate the asymptotic distribution of prime numbers requires knowledge of appropriate Dirichlet series as s approaches 1, their abscissa of absolute convergence. Note that for $\operatorname{Re}(s) > 1$, $d\left(\sum_{n\le x} a_n n^{-s}\right)$ assigns a finite measure to $\mathbb{R}$. As s approaches 1, $y^{-(s-1)}$ approaches the identity (origin) of the group $(\mathbb{R}^*)^\wedge$.

Plancherel's relation and a Mellin analogue occur in Chapters 14 and 15. In Chapter 28 I employ the Mellin transform of a Dirichlet series to estimate the norm of a composition of operators.