Chapter 4 Fourier Series and Integrals on Groups

4.1 GROUPS

Up to now, you have studied Fourier series and integrals for assorted classes of functions, mostly on the circle and the line. Both of these spaces are commutative groups (under addition). The purpose of this chapter is, first, to take a new look at the old series and integrals from the point of view of groups, and second, to develop similar ways of expressing functions on other important (commutative and noncommutative) groups. The knowledge of groups that you will need is prepared in the present section and at appropriate places later. Birkhoff and MacLane [1965] is recommended for additional information; for a fascinating elementary account of finite groups and symmetry, see Weyl [1952].

1. Groups as Such

A *group* G is a class of objects g which is equipped with a *multiplication*, that is, a map of $(g_1, g_2) \in G \times G$ into G expressed as a (formal) product "$g_1 g_2$," in such a way that

(a) the multiplication is associative: $g_1(g_2g_3) = (g_1g_2)g_3$,
(b) there is an identity 1: $1g = g1 = g$.
(c) every $g \in G$ has an inverse g^{-1}: $g^{-1}g = gg^{-1} = 1$.

G is *commutative* if g_2g_1 is always the same as g_1g_2; in this circumstance, it is customary to use addition $[g_1 + g_2]$ in place of multiplication $[g_1g_2]$ and to denote the identity by 0 instead of by 1.

EXAMPLES

(1) S^1: the circle $[0, 1)$ under addition modulo 1.

(2) R^1: the line under addition.

(3) R^{1+}: the positive real numbers under multiplication.

(4) Z^1: the integers under addition.

(5) Z_m^{+}: the integers $0, 1, ..., m-1$ under addition modulo a positive integer m.

(6) $Z_p^{\times}$: the positive integers $1, 2, ..., p-1$ under multiplication modulo a prime p.

(7) the permutation of $n \geqslant 2$ letters under composition of permutations.

(8) the symmetries of the square: counterclockwise rotation by 0°, 90°, 180°, 270°, reflection in either diagonal, horizontal and vertical reflection, under composition.

(9) $SO(3)$: the special orthogonal group of 3×3 real orthogonal matrices [transpose = inverse] with determinant $+1$, under the conventional multiplication of matrices.

(10) $M(2)$: the rigid motions of the plane, i.e., translations and rotations, *alias* the Euclidean congruences.

EXERCISE 1. Example 6 is an actual group only if p is prime. *Hint:* If p is prime, then $0 < n < p$ and p are relatively prime, so $in + jp = 1$ for some integral i and j.

EXERCISE 2. Example 7 is noncommutative if $n \geqslant 3$.

EXERCISE 3. Examples 8–10 are noncommutative groups.

2. Subgroups and Homomorphisms

Let G be a group. Then $H \subset G$ is a *subgroup* if it is a group in its own right. G/H stands for the family of *cosets* $gH = (gh\colon h \in H)$ as g runs over G. A *homomorphism* j of G is a map of G into a second group, which preserves the multiplication $[j(g_1g_2) = j(g_1)j(g_2)]$; j is an *isomorphism* if it is also 1:1 and onto.

EXERCISE 4. Check that two cosets are either identical or disjoint, i.e., the nonidentical cosets cover G simply (no overlapping).

EXERCISE 5. Check that G/H is a group under the multiplication $(g_1 H)(g_2 H) = (g_1 g_2)H$ iff $g^{-1}Hg \subset H$ for every $g \in G$, and that in that case the natural map j: $g \to gH$ of G into G/H is a homomorphism. *Hint:* Check first that the proposed rule for multiplication makes sense, i.e., if $g_1 H = g_3 H$ and $g_2 H = g_4 H$, then $g_1 g_2 H = g_3 g_4 H$.

EXERCISE 6. Every homomorphism j of G arises as in Exercise 5: Namely, if j is a homomorphism of G into a second group G', then $j(G)$ is a subgroup of G', $H = j^{-1}(1') = (g \in G\colon j(g) = 1')$ is a subgroup of G, and $j(G)$ is isomorphic to G/H. Here, $1'$ stands for the identity of G'. Check all these claims.

EXERCISE 7. The symmetries of the square [Example 8] which leave the upper left-hand corner fixed form a subgroup H. Show that G/H can be identified with the corners of the square, but is *not* a group. *Hint:* Identify $g \in G$ with the place to which it sends the upper left-hand corner.

EXERCISE 8. Check that the groups of Examples 2 and 3 are isomorphic.

EXERCISE 9. Check that any finite group is isomorphic to a subgroup of the permutations of n letters for sufficiently large n. *Hint:* Pick $k \in G$. Then you can identify the map $g \to kg$ with a permutation of the "letters" $g \in G$.

EXERCISE 10. Check that R^1/Z^1 is isomorphic to S^1.

3. Characters

A *character* of a group G is a homomorphism e of G into the (multiplicative) group of complex numbers of modulus 1:

(a) $\quad |e(g)| = 1, \qquad g \in G,$

(b) $\quad e(g_1 g_2) = e(g_1)e(g_2);$

in the case of continuous groups, such as Examples 1, 2, and 3, it is customary to insist that e be a continuous function on G.

EXERCISE 11. Check that $e(1) = 1$.

EXERCISE 12. Check that $e(g^{-1}) = e(g)^{-1} = e(g)^*$.

$\hat{G}$ stands for the class of characters of the group G.

EXERCISE 13. Check that $\hat{G}$ is a commutative group under the multiplication $(e_1 e_2)(g) = e_1(g) e_2(g)$. What is the identity of $\hat{G}$? $\hat{G}$ is the so-called *dual group* of G.

EXERCISE 14. Compute the dual group of $Z_m{}^+$. *Hint:* $Z_m{}^+$ may be identified with the integers $0 \leqslant n < m$. Check that $(Z_m{}^+)^\wedge = Z_m{}^+$.

EXERCISE 15. The "signature" of a permutation is $(-1)^\sharp$ in which $\sharp$ is the number of transposition $ij \rightarrow ji$ figuring in the permutation. Check that this signature is a character of the group of permutations of $n = 3$ letters. *Hint:* Every permutation is a product of transpositions but can be so expressed in many ways. The point is that the *parity* of the number of transpositions involved is an attribute of the permutation itself.

EXERCISE 16. The only character of the group of permutations of $n \geqslant 2$ letters besides the signature is $e \equiv 1$. The moral is that characters are probably not much use for *noncommutative* groups; see Subsection 4.8.4 for a proof that $e \equiv 1$ is the *only* character of the group $SO(3)$ of Example 9. *Hint:* $e(ij) = \pm 1$ for any transposition ij. Why? Besides, $(ik)(ij)(ik) = kj$, and so $e(ij)$ is either always $+1$ or always -1 for every ij.

4.2 FOURIER SERIES ON THE CIRCLE

The purpose of this section is to "explain" the exponentials

$$e_n(x) = e^{2\pi i n x}$$

figuring in the standard Fourier series

$$f = \sum \hat{f}(n)\, e_n$$

from the point of view of the circle group $S^1 = R^1/Z^1$.

1. Characters

e_n: $n \in Z^1$ is a complete list of the characters of the circle group.

PROOF. e_n is a character for every integer n: Namely, $|e_n| = 1$ and $e_n(x+y) = e_n(x) e_n(y)$. Now let e be any character and think of it as a character of R^1 of period 1 by putting $e(x+n) = e(x)$ for $0 \leqslant x < 1$ and integral n. Because $|e| = 1$,

$$e(x) = e^{i\varphi(x)}$$

with a real phase φ, and since e is multiplicative $[e(x+y) = e(x)e(y)]$, φ is additive $[\varphi(x+y) = \varphi(x) + \varphi(y)$, modulo $2\pi]$. But then $\varphi(jx) = j\varphi(x)$, modulo 2π, for any integral j, so $\varphi(x) = x\varphi(1)$, modulo 2π, for rational $x = k/j$, and

$$e(x) = e^{ix\varphi(1)},$$

first for rational $x = k/j$, and then for every real x, by continuity. To finish the proof, you infer from

$$1 = e(0) = e(1) = e^{i\varphi(1)}$$

that $\varphi(1)$ can only be an integral multiple of 2π, i.e., $e = e_n$ for some $n \in Z^1$.

EXERCISE 1. The map $e_n \to n \in Z^1$ is an isomorphism between the dual group $(S^1)^\wedge$ and Z^1. Check that $(S^1)^{\wedge\wedge}$ [the dual group of $(S^1)^\wedge$] is isomorphic to S^1 $[(Z^1)^\wedge$ up to isomorphism]. This is a simple instance of the so-called "Pontrjagin duality"; see also Exercises 4.1.10 and 4.1.14, and Section 4.5, especially the comment on the Poisson summation formula.

2. Invariant Subspaces

A second group-theoretical way of getting at the exponentials e_n is via translation invariant subspaces of $\mathsf{L}^2(S^1)$. A closed subspace M is translation invariant if it is closed under translations, i.e., if

$$f_y(x) = f(x+y)$$

belongs to M for every $f \in \mathsf{M}$ and every $y \in S^1$. A simple example is provided by the class M_n of complex multiples of e_n.

Warning: In this book invariant subspaces are *always* closed subspaces.

EXERCISE 2. Check that $e_n \circ f = e_n \hat{f}(n)$ belongs to M for any $f \in \mathsf{M}$. *Hint:* $e_n \circ f$ may be approximated in $\mathsf{L}^2(S^1)$ by the Riemann sum

$$\sum_{k=0}^{m-1} f\left(x - \frac{k}{m}\right) \int_{k/m}^{(k+1)/m} e_n(y)\, dy.$$

EXERCISE 3. The "spectrum" of M is the class of integers n such that $\hat{f}(n) \neq 0$ for some $f \in \mathsf{M}$. Check that M is the (perpendicular) sum $\oplus \mathsf{M}_n$, n running over the spectrum of M.

The content of Exercise 3 is that M_n: *$n \in Z^1$ is a complete list of minimal invariant subspaces of* $\mathsf{L}^2(S^1)$. The self-evident perpendicular splitting

$$\mathsf{L}^2(S^1) = \bigoplus_{|n| < \infty} \mathsf{M}_n$$

is a special case; you may regard it as a new statement of the Plancherel identity.

EXERCISE 4. Check that the family f_y: $0 \leqslant y < 1$ spans $\mathsf{L}^2(S^1)$ iff $\hat{f}(n)$ never vanishes.

EXERCISE 5. Check that as n runs over Z^1, $\mathsf{M}^n = (f \in \mathsf{L}^2(S^1) : \hat{f}(n) = 0)$ runs through the maximal invariant subspaces of $\mathsf{L}^2(S^1)$. The adjective "maximal" means that there are no other invariant subspaces between M^n and $\mathsf{L}^2(S^1)$.

3. Eigenfunctions

Additional interest attaches to the exponentials e_n as eigenfunctions of the differential operator $Kf = f''$. What is not self-evident beforehand is that the minimal invariant subspaces should be eigenspaces of such a nice differential operator! A link is provided by

EXERCISE 6. Check that any linear operator K acting on $\mathsf{C}^\infty(S^1)$ and commuting with translations $[x \to x+y]$ and reflection $[x \to -x]$ acts like multiplication by a constant on $\mathsf{M}_n \oplus \mathsf{M}_{-n}$, i.e., $\mathsf{M}_n \oplus \mathsf{M}_{-n}$ is an eigenspace of K. Check that if $K = c_0(x) + c_1(x)D + \cdots + c_n(x)D^n$ is a differential operator with coefficients from $\mathsf{C}^\infty(S^1)$ which commutes with translations and reflections, then it must be a polynomial in D^2.

4. Homomorphisms

Think of summable functions on the circle as an algebra under the customary product

$$f_1 \circ f_2(x) = \int_0^1 f_1(x-y) f_2(y)\, dy.$$

A homomorphism of this algebra is a mapping $j \neq 0$ into the complex numbers which respects

(a) complex multiplication: $j(\text{constant} \times f) = \text{constant} \times j(f)$,
(b) addition: $j(f_1 + f_2) = j(f_1) + j(f_2)$, and
(c) multiplication: $j(f_1 \circ f_2) = j(f_1)\, j(f_2)$,
subject to the technical condition
(d) $|j(f)| \leqslant \text{constant} \times \|f\|_1$, with a constant independent of f.

A simple example is provided by the nth Fourier coefficient:

$$j_n(f) = \hat{f}(n) = \int_0^1 f e_n{}^*.$$

EXERCISE 7. Check that if j is a homomorphism then there is an integer n such that $j(e_m) = 1$ or 0 according as $m = n$ or not. *Hint:* $e_n \circ f = e_n \hat{f}(n)$; now apply j to both sides.

Any summable function f can be well-approximated by sums of exponentials, so by (d) and Exercise 7, either $j(f) = \hat{f}(n)$ for some n, or $j(f) \equiv 0$, which is not allowed; in short, j_n: $n \in Z^1$ *is a complete list of the homomorphisms of* $\mathsf{L}^1(S^1)$.

EXERCISE 8. Give a second proof that $j_n(f) = \hat{f}(n)$ is a complete list of homomorphisms using Exercise 1.5.6 to represent $j(f)$ as $\int_0^1 f(x)\, e^*(x)\, dx$ with a bounded function e. *Hint:* Think of e and f as periodic functions on R^1. Then $j(f_1 \circ f_2) = j(f_1)\, j(f_2)$ implies $e(x+y) = e(x)\, e(y)$ a.e. on the plane, and therefore

$$e(x) \int_a^b e(y)\, dy = \int_a^b e(x+y)\, dy = \int_{a+x}^{b+x} e(y)\, dy$$

for almost all x and any a and b. Conclude that $e \in \mathsf{C}^1(S^1)$ is a solution of $e'(x) = e'(0)\, e(x)$.

5. Summary

To sum up, the exponentials e_n: $n \in Z^1$ play four different roles: (a) They are the characters of the circle group; (b) they span the minimal invariant subspaces; (c) they are eigenfunctions of $Kf = f''$; (d) they can be identified with the homomorphisms of the algebra of summable functions.

This is the simplest statement of the four principal themes of the present chapter. You will see that, with appropriate modifications, they recur for (samples of) a wide class of important groups, and provide you with a powerful and flexible arsenal of Fourier methods, specially adapted to group-allied problems.

EXERCISE 9. Redo Subsections 1–4 for the standard $(n \geqslant 2)$-dimensional torus $T^n = R^n/Z^n$ of Subsection 1.10.1.

4.3 FOURIER INTEGRALS ON THE LINE

A group-theoretical interpretation is also available for Fourier integrals on the line, but with technical complications.

1. Characters

The exponentials

$$e_\gamma(x) = e^{2\pi i\gamma x}$$

are the characters of R^1, and the map $e_\gamma \to \gamma \in R^1$ is an isomorphism between the dual group $(R^1)^\wedge$ and R^1 itself, that is to say, R^1 is self-dual. The proof is made as before; the only difference is that no restriction is placed upon the phrase $\varphi(1) = 2\pi\gamma$.

2. Invariant Subspaces

The business of invariant subspaces is complicated by the fact that nonzero minimal closed subspaces do not exist. But there *is* a perfectly satisfactory analogue of Exercise 4.2.3.

EXERCISE 1. Any invariant subspace M of $\mathsf{L}^2(R^1)$ can be expressed as

$$\mathsf{M} = \mathsf{L}^2(Q)^\wedge = (f \in \mathsf{L}^2(R^1) : \hat{f} = 0 \text{ off } Q)$$

for some measurable set $Q \subset R^1$. *Hint:* By Exercise 1.3.13, M is separable. Pick $f_n : n \geqslant 1$ dense in M and let $Q = \bigcup_{n=1}^\infty (\gamma : \hat{f}_n(\gamma) \neq 0)$. Check that $\mathsf{M}^\wedge \subset \mathsf{L}^2(Q)$. The fact that $\mathsf{M}^\wedge = \mathsf{L}^2(Q)$ is now verified by picking k from the annihilator of $\mathsf{M}^\wedge$ in $\mathsf{L}^2(Q)$ and concluding that $k = 0$ from

$$0 = \int e^{2\pi i\gamma y}\hat{f}(\gamma)\, k^*(\gamma)\, d\gamma$$

for every $y \in R^1$ and $f \in \mathsf{M}$.

The content of Exercise 1 can be expressed in a formal but suggestive way. The class M_γ of complex multiples of e_γ is closed under translations, and while it is *not* a subspace of $\mathsf{L}^2(R^1)$, it is only "a little way out": namely,

$$\int_\alpha^\beta e_\gamma(x)\, d\gamma = \frac{e_\beta(x) - e_\alpha(x)}{2\pi i x}$$

belongs to $\mathsf{L}^2(R^1)$ for any small interval $[\alpha,\beta]$ so you may think of $M_\gamma d\gamma$ as a "thin slice" of $\mathsf{L}^2(R^1)$. The content of Exercise 1 is that any closed invariant subspace M is the (perpendicular) sum (or better, the integral) of the "slices" in its "spectrum":

$$\mathsf{M} = \bigoplus_Q \mathsf{M}_\gamma\, d\gamma = \int_Q \mathsf{M}_\gamma\, d\gamma.$$

A special case of Exercise 1 is the fact that the translates of $f \in \mathsf{L}^2(R^1)$ span $\mathsf{L}^2(R^1)$ iff $(\gamma : \hat{f}(\gamma) = 0)$ is of measure 0; see Exercise 2.5.11 for an application to Hermite functions, and Exercise 4.2.4 for the analogue for the circle. The present statement is known as "Wiener's Tauberian theorem."

EXERCISE 2.[1] The translates of a summable function f span $\mathsf{L}^1(R^1)$ iff $\hat{f}(\gamma) \neq 0$ for *any* $\gamma \in R^1$. Check this for rapidly decreasing f. The general fact is known as "Wiener's Tauberian theorem for $\mathsf{L}^1(R^1)$." *Hint:* Any compact function of class $\mathsf{C}^\infty(R^1)$ can be expressed as $\hat{f}\hat{k}$ for some compact $\hat{k} \in \mathsf{C}^\infty(R^1)$. Why? Now look at $(\hat{f}\hat{k})^\vee = f \circ k$. The rest should be plain sailing.

3. Eigenfunctions

As before, it is very satisfactory to notice that the exponentials

$$e^{2\pi i y x}$$

are (bounded) eigenfunctions of the differential operator $Kf = f''$. As for the circle, any nice differential operator commuting with translations and reflection is a polynomial in $K = D^2$.

4. Homomorphisms

The business of homomorphisms of $L^1(R^1)$ is technically more complicated, too. A homomorphism is defined as before, and $e_\gamma \circ f = e_\gamma \hat{f}(\gamma)$, but e_γ is not summable, so the old proof fails. But the *fact* is still true:

$$j_\gamma(f) = \hat{f}(\gamma) = \int f e_\gamma{}^*, \qquad \gamma \in R^1,$$

is a complete list of the homomorphisms of $\mathsf{L}^1(R^1)$.

PROOF. The map $f \to f_y$ interacts with the homomorphism j as follows:

$$j(f_y)\, j(k) = j(f_y \circ k) = j(f \circ k_y) = j(f)\, j(k_y)$$

for summable f and k. Pick k so as to make $j(k) = 1$. Then

$$j(f_y) = e(y)\, j(f)$$

for every summable f, with a universal function

$$e(y) = j(k_y).$$

This function is a character. To begin with,

$$e(x+y)\, j(f) = j(f_{x+y}) = e(x)\, j(f_y) = e(x)\, e(y)\, j(f)$$

[1] Adapted from Kac [1965].

so e is multiplicative. It is also bounded:

$$|e(y)| = |j(k_y)| \leqslant \text{constant} \times \|k\|_1 .$$

$|e| \equiv 1$ follows readily, and from $e(0) = 1$, you conclude that

$$e(y) = e^{2\pi i \gamma y} = e_\gamma(y)$$

for some real γ. Now $j(f)$ may actually be evaluated as

$$\begin{aligned} j(f) = j(k) j(f) &= j(k \circ f) \\ &= j\left(\int k_{-y} f(y)\, dy\right) \\ &= \int j(k_{-y}) f(y)\, dy \\ &= \int f(y)\, e^{-2\pi i \gamma y}\, dy \\ &= \hat{f}(\gamma) . \end{aligned}$$

The only point at issue is the passage from line 2 to line 3 which may be justified by picking $k \in \mathrm{C}_\downarrow^\infty(R^1)$, still with $j(k) = 1$, and noting that the length

$$\left\| k \circ f - \sum_{|i| \leqslant ln} k_{-i/n} \int_{i/n}^{(i+1)/n} f(y)\, dy \right\|_1$$

tends to 0 as $n \uparrow \infty$ and $l \uparrow \infty$, in that order, for then

$$j(k \circ f) - \sum_{|i| \leqslant ln} j(k_{-i/n}) \int_{i/n}^{(i+1)/n} f(y)\, dy ,$$

which is bounded by a constant multiple of this length, also tends to 0, and therefore

$$j(f) = \lim_{l \uparrow \infty} \lim_{n \uparrow \infty} \sum_{|i| \leqslant ln} e_\gamma{}^*(i/n) \int_{i/n}^{(i+1)/n} f(y)\, dy = \int f e_\gamma{}^* .$$

The proof is finished.

EXERCISE 3. Give a second proof that $j_\gamma(f) = \hat{f}(\gamma)$ is a complete list of homomorphisms in the style of Exercise 4.2.8.

EXERCISE 4. Redo Subsections 1–4 for R^n $(n \geqslant 2)$.

EXERCISE 5. $\mathrm{L}^1[0, \infty)$ inherits from $\mathrm{L}^1(R^1)$ the product

$$f_1 \circ f_2(x) = \int_0^x f_1(x-y) f_2(y)\, dy .$$

Check that

$$j_\gamma(f) = \hat{f}(\gamma) = \int_0^\infty f(x)\, e^{-\gamma x}\, dx$$

is a homomorphism for any $\gamma \geqslant 0$. What is the most general homomorphism?

EXERCISE 6. Check that the "Laplace transform" $f \to \hat{f}$, as defined in Exercise 5, is 1:1 for $f \in \mathrm{L}^2[0, \infty)$ ($\gamma = 0$ is now excluded). How do you actually compute f from $\hat{f}$? *Answer:*

$$f(x) = \lim_{a \downarrow 0} \frac{1}{2\pi} \int_{-\infty}^{\infty} \hat{f}(a+ib)\, e^{ibx}\, db\,.$$

Compute $[(1+x^2)^{-1}]^\wedge$, $[\sin x]^\wedge$, $[x^4]^\wedge$. Can you apply your inversion formula to these special cases?

This kind of transform is specially well-suited to problems of electrical circuits as in Subsection 2.7.4, for instance. Heaviside introduced it for that purpose about the turn of the century, though the idea is much older; for additional information and applications, see Doetsch [1958].

EXERCISE 7.[2] Define a new product for summable functions on the line by the recipe

$$f_1 \square f_2(x) = f_1(x) \int_{-\infty}^{x} f_2(y)\, dy + f_2(x) \int_{-\infty}^{x} f_1(y)\, dy\,.$$

Check that

(a) $\square$ is commutative and associative;

(b) $\|f_1 \square f_2\|_1 \leqslant \|f_1\|_1\, \|f_2\|_1$;

(c) every nontrivial homomorphism for the $\square$-product can be expressed as

$$j(f) = \int_{-\infty}^{y} f$$

for some $-\infty < y \leqslant \infty$, *Hint for* (*c*): The $\square$-product of the indicator functions 1_I and 1_J of intervals I and J of length $|I|$ and $|J| < \infty$ can be expressed $1_I \square 1_J = |I|\, 1_J$ if I lies to the left of J, so $j(1_I)\, j(1_J) = |I|\, j(1_J)$, and if $j(1_J) \neq 0$, then $j(f) = \int f$ for every f that lives to the left of J. Try a second proof using Exercise 1.5.6 in the style of Exercise 4.2.8.

By (c), the inversion formula for the $\square$-product is simply the "fundamental theorem of calculus": namely, the transform $\hat{f}(y) = \int_{-\infty}^{y} f$ is inverted by

[2] Adapted from Lardy [1966].

differentiation $f^{\vee}=f'$! This kind of transform has been systematically exploited for solving combinatorial problems by Rota [1964]. A typical example is the "Möbius inversion formula" of number theory. This has to do with functions on the positive integers: the transform is

$$\hat{f}(n)=\sum_{d\ \text{dividing}\ n} f(d),$$

and you invert by use of

$$f(n)=\sum_{d\ \text{dividing}\ n} e(n/d)\hat{f}(d),$$

in which e is the "Möbius function":

$$e(n)=\begin{cases}1 & \text{if } n=1,\\ (-1)^m & \text{if } n>1 \text{ is the product}\\ & \text{of } m \text{ unequal primes},\\ 0 & \text{if } n>1 \text{ is not a product}\\ & \text{of unequal primes}.\end{cases}$$

EXERCISE 8. Check the Möbius inversion formula. *Hint:* The binomial identity $\sum_{k=0}^{n}\binom{n}{k}(-1)^k=(1-1)^n=0$ implies that $\sum_{k\,\text{dividing}\,d}e(k)=0$ if $d>1$.

EXERCISE 9. Check that $f\rightarrow\hat{f}(n)$ is a homomorphism for the product

$$f_1\circ f_2(n)=\sum_{(i,j)=n} f_1(i)f_2(j),$$

(i,j) being the least common multiple of i and j.

4.4 FINITE COMMUTATIVE GROUPS

The Fourier idea is seen in its simplest form on a finite commutative group. The purpose of this section is to develop the necessary facts about such groups. The Fourier series themselves occupy Section 4.5; an application to number theory will be found in Section 4.6.

Let G be a finite commutative group, and let H be a subgroup. The coset space G/H is always a group [see Exercise 4.1.5]: the so-called *factor group* $\sharp(G)$ is the cardinality of G. For $g\in G$, $\sharp_G(g)=\sharp(g)$ is the smallest integer $n\geqslant 1$ such that $g^n=1$. The following exercises have to do with these notions.

EXERCISE 1. Check that $\sharp(G)=\sharp(G/H)\sharp(H)$. *Hint:* Two cosets gH are either identical or disjoint.

EXERCISE 2. Check the following facts: $\sharp(g)$ divides $\sharp(G)$ for every $g \in G$. $g^n = 1$ iff n is an integral multiple of $\sharp(g)$. $\sharp_{G/H}(gH)$ divides $\sharp_G(g)$. *Hint:* Use Exercise 1 with $H = (g^k\colon\ 0 \leqslant k < \sharp(g))$ to prove the first assertion.

The "product" $G_1 \times G_2$ of the groups G_1 and G_2 is the set-theoretical product, made into a group by use of componentwise multiplication: If $g = (g_1, g_2)$ and $h = (h_1, h_2)$, then $gh = (g_1 h_1, g_2 h_2)$. A simple [infinite] example is provided by Z^2 [the lattice of integral points in the plane] which is the direct product of two copies of Z^1: $Z^2 = Z^1 \times Z^1$.

BASIS THEOREM. *Any finite commutative group G is isomorphic to a direct product of "counters"*

$$Z_m^{\ +} = \textit{the integers under addition modulo } m, \quad \textit{alias the multiplicative group of } m\textit{th roots of unity } e^{2\pi i k/m}\colon 0 \leqslant k < m,$$

i.e., G is isomorphic to

$$Z_{m_1}^+ \times \cdots \times Z_{m_n}^+$$

for some $1 \leqslant n < \infty$ *and some integral* $m_i\colon i \leqslant n$.

The m_i's need not be primes, but you can choose them to be powers of a prime. You may take this on faith if you like and pass directly on to Section 4.5. The proposition goes back to Gauss; the proof presented below is adapted from Speiser [1945, pp. 46–49].

Step 1: Check that G is isomorphic to $Z_p^{\ +} \times \cdots \times Z_p^{\ +}$ if $\sharp(g)$ is a fixed prime p for every $g \in G$, excepting $g = 1$.

PROOF. Pick $g_i\colon i \leqslant n$ from G such that

$$g_1^{e_1} \cdots g_n^{e_n} \neq 1$$

for any $0 \leqslant e_i < p$, excepting $e_i \equiv 0$, and make n as big as possible subject to this condition. These products fill out a subgroup H of G which is isomorphic to $Z_p^{\ +} \times \cdots \times Z_p^{\ +}$ (n-fold), and the statement is that $H = G$; if not, you could find $g \notin H$, and you could augment n (against the assumption), as follows from the fact that $\sharp_{G/H}(g) > 1$, since gH is not the identity in G/H, and therefore $\sharp_{G/H}(g) = p$, since it divides $\sharp_G(g) = p$ [see Exercise 2].

Step 2: Check that G is isomorphic to a product of counters if $\sharp(g)$ is a power of a fixed prime p for every $g \in G$.

PROOF. Put

$$\max_G \#(g) = p^m.$$

The proposition is proved by induction on m; Step 1 is the case $m = 1$, and you assume that everything works for any integer less than m for $m \geqslant 2$. Now $G' = (g^p : g \in G)$ is a subgroup of G, and

$$\max_{G'} \#(g') = p^{m-1},$$

so G' is a product of counters. Therefore, you can pick $n \geqslant 1$ and g_i': $i \leqslant n$ out of G' so that every $g' \in G'$ can be expressed in precisely one way as

$$g' = (g_1')^{e_1'} \cdots (g_n')^{e_n'}, \qquad 0 \leqslant e_i' < \#(g_i') = p^{f_i}.$$

Because $g_i' \in G'$, it is a pth power of some $g_i \in G$, and

$$\#(g_i) = p\#(g_i') = p^{f_i+1}.$$

The claim is that

$$g_1^{e_1} \cdots g_n^{e_n} \neq 1$$

for any $0 \leqslant e_i < p^{f_i+1}$, excepting $e_i \equiv 0$. In the opposite case,

$$g_1^{a_1} \cdots g_n^{a_n} = 1$$

for some $0 \leqslant a_i < p^{f_i+1}$, and a_1 would have to be an integral multiple of $\#_{G/K}(g_1 K)$, K being the subgroup

$$(g_2^{b_2} \cdots g_n^{b_n} : 0 \leqslant b_i < p^{f_i+1}).$$

But $\#_{G/K}(g_1 K)$ divides $\#_G(g_1)$ and is therefore a power of p, so that a_1 (and likewise every one of the other exponents a_i) is a power of p, and the offending identity $g_1^{a_1} \cdots g_n^{a_n} = 1$ can be expressed in the forbidden form

$$(g_1')^{e_1'} \cdots (g_n')^{e_n'} = 1, \qquad 0 \leqslant e_i' < p^{f_i}!$$

This contradiction shows that the subgroup

$$H = (g_1^{e_1} \cdots g_n^{e_n} : 0 \leqslant e_i < p^{f_i+1})$$

is isomorphic to

$$Z^+_{p^{f_1+1}} \times \cdots \times Z^+_{p^{f_n+1}}.$$

Now if $H = G$, you are finished. If not, pick $g \notin H$. Then $g^{-p} \in G'$; as such it is the pth power of some $h \in H$, and $\#(gh) = p$ since $(gh)^p = 1$ but $gh \neq 1$. By the now familiar argument

$$g_1^{e_1} \cdots g_n^{e_n} (gh)^{e_{n+1}} \neq 1$$

for any $0 \leqslant e_i < p^{f_i+1}$ and $e_{n+1} < p$, excepting $e_i \equiv 0$. Put $g_{n+1} = gh$ and $f_{n+1} = 0$. Then the subgroup

$$H_1 = (g_1^{e_1} \cdots g_{n+1}^{e_{n+1}} \colon 0 \leqslant e_i < p^{f_i+1})$$

is isomorphic to $H \times Z_p{}^+$, it contains g, and if you have not already exhausted (either yourself or) the whole of G, you can go on in this way adjoining factors $Z_p{}^+$ until you have done so. The bulk of the proof is finished.

Step 3: You have only to check that G splits into a direct product of groups of the kind disposed of in Step 2.

PROOF. Pick a prime p dividing $\sharp(g)$ for some $g \neq 1$ from G. Both

$$G_1 = (g_1 \colon \sharp(g_1) \quad \text{is a power of} \quad p) \qquad .$$

and

$$G' = (g' \colon \sharp(g_1') \quad \text{is not divisible by} \quad p)$$

are subgroups of G, as is plain from the fact that $\sharp(g_1 g_2)$ divides $\sharp(g_1)\sharp(g_2)$. Also, G_1 contains a nontrivial power of g so that $\sharp(G_1) \geqslant 2$, and if you now grant that G is isomorphic to $G_1 \times G'$, the rest will follow by induction: G' splits into $G_2 \times G''$ so as to make $\sharp(g_2)$ a power of a fixed prime p_2 for every $g_2 \in G_2$ and $\sharp(G_2) \geqslant 2$, and so on. The point at issue is whether or not every $g \in G$ can be expressed as a product $g = g_1 g'$ in precisely one way. The fact that you can have at most one such splitting is self-evident from $G_1 \cap G' = 1$. To prove the existence of such a splitting, put $\sharp(g) = p^f q$ with q not divisible by p and pick integers i and j so that $ip^f + jq = 1$. Then

$$g = g^{ip^f} g^{jq}$$

is the desired splitting: Namely, for the second factor,

$$(g^{jq})^{p^f} = (g^{p^f q})^j = 1 ,$$

so that $\sharp(g^{jq})$ divides p^f and is therefore a power of p, which is to say that $g^{jq} \in G_1$, while, for the first factor,

$$(g^{ip^f})^q = (g^{p^f q})^i = 1 ,$$

so that $\sharp(g^{ip^f})$ divides q and is therefore not divisible by p, which is to say that $g^{ip^f} \in G'$. The proof is finished.

4.5 FOURIER SERIES ON A FINITE COMMUTATIVE GROUP

By Section 4.4, you may as well suppose that the group in question is a product of counters:

$$G = Z_{m_1}^+ \times \cdots \times Z_{m_n}^+ .$$

The usefulness of this splitting may now be seen in the following computation of the dual group $\hat{G}$.

Z_m^+ is identified with the integers $0 \leqslant k < m$ under addition modulo m, and $g \in G$ is identified with a point $k = (k_1, \cdots, k_n)$ of the additive group $Z_{m_1}^+ \times \cdots \times Z_{m_n}^+$, that is to say, you identify g with $k_1 g_1 + \cdots + k_n g_n$, in which $g_l = (0, \cdots, 1, \cdots, 0)$ contains a 1 in the lth place and 0's elsewhere. A character $e \in \hat{G}$ is now seen to split as

$$e(g) = e(g_1)^{k_1} \cdots e(g_n)^{k_n},$$

and since

$$e(g_l)^{m_l} = e(g_l^{m_l}) = e(1) = 1,$$

you see that the numbers $e(g_l)$ are m_lth roots of unity:

$$e(g_l) = e^{2\pi i j_l/m_l}$$

for some $0 \leqslant j_l < m_l$. But then the character e is completely specified by

$$j = (j_1, \cdots, j_n) \in Z_{m_1}^+ \times \cdots \times Z_{m_n}^+,$$

and the map $e \to j$ establishes an isomorphism between the dual group $\hat{G}$ and the group $Z_{m_1}^+ \times \cdots \times Z_{m_n}^+$; in particular, G is self-dual!

A function f on G may be expanded into a sum of characters, or "Fourier series." The chief point is that under the inner product

$$(f_1, f_2) = \sum_{g \in G} f_1(g) f_2(g)^*,$$

the characters form a perpendicular family:

$$(e_1, e_2) = \sharp(G) \quad \textit{or} \quad 0 \qquad \textit{according as } e_1 = e_2 \textit{ or not.}$$

PROOF.

$$\begin{aligned} e_1(g_0)(e_1, e_2) &= \sum_G e_1(g_0) e_1(g) e_2(g)^* \\ &= \sum_G e_1(g_0 g) e_2(g)^* \\ &= \sum_G e_1(g) e_2(g_0^{-1} g)^* \\ &= \sum_G e_1(g) e_2(g_0^{-1})^* e_2(g)^* \\ &= e_2(g_0)(e_1, e_2), \end{aligned}$$

for any $g_0 \in G$, so either $e_1 \equiv e_2$ or else $(e_1, e_2) = 0$. The evaluation

$$\|e\|^2 = (e, e) = \sum_G |e(g)|^2 = \sharp(G)$$

is automatic from $|e(g)| = 1$. The proof is finished.

EXERCISE 1. Check that if H is a subgroup of G, then

$$\sum_H e(h) = \#(H) \quad \text{or} \quad 0 \qquad \text{according as } e \equiv 1 \text{ on } H \text{ or not.}$$

Hint: Think of the sum as the inner product of e with the identity of $\hat{H}$.

Every $g \in G$ can be viewed as a character on $\hat{G}$, i.e., as an element in $G^{\wedge\wedge}$, by defining

$$g(e) \equiv e(g).$$

Clearly g is multiplicative:

$$g(e_1 e_2) \equiv (e_1 e_2)(g) = e_1(g)e_2(g) = g(e_1)g(e_2),$$

and of modulus 1. Moreover in the present circumstances [G isomorphic to $\hat{G}$] distinct elements in G give rise to distinct elements in $G^{\wedge\wedge}$ and therefore you see that

$$\sum_{\hat{G}} e(g_1)e(g_2)^* = \#(\hat{G}) \quad \text{or} \quad 0 \qquad \text{according as } g_1 = g_2 \text{ or not.}$$

This leads at once to the

PLANCHEREL THEOREM. *Any function f on G can be expanded into a Fourier series*

$$f = \sum_{\hat{G}} \hat{f}(e)\, e$$

with coefficients

$$\hat{f}(e) = \#(G)^{-1}(f, e) = \#(G)^{-1} \sum_G f(g)e(g)^*,$$

and there is a Plancherel identity:

$$\|f\|^2 = \sum_G |f(g)|^2 = \#(G) \sum_{\hat{G}} |\hat{f}(e)|^2 = \#(G)\|\hat{f}\|^2.$$

PROOF. To see that $f = \sum \hat{f}(e)e$, just compute the sum as follows:

$$\begin{aligned}\sum_{\hat{G}} \hat{f}(e)e(g_0) &= \sum_{\hat{G}} e(g_0)\#(G)^{-1} \sum_G f(g)e(g)^* \\ &= \sum_G f(g)\#(G)^{-1} \sum_{\hat{G}} e(g_0)e(g)^* \\ &= f(g_0).\end{aligned}$$

The proof of the Plancherel identity is just as easy.

The next topic is the Poisson summation formula, but first a brief aside. Given a subgroup H of G, let $(G/H)'$ be the class of characters e of G which are trivial on H: $e(h) \equiv 1$. A character of this kind is a function of cosets gH and so can be thought of as a character of the factor group G/H. This correspondence goes the other way too: any character e' of G/H can be lifted up to G by the rule $e(g) = e'(gH)$ and so can be thought of as belonging to $(G/H)'$. To sum up, $(G/H)'$ and $(G/H)^\wedge$ are isomorphic, and you may take the liberty of confusing the two. The Poisson summation formula may now be stated as

$$\sum_H f(h) = \sharp(H) \sum_{(G/H)^\wedge} \hat{f}(e).$$

PROOF. Bring in the function

$$f^0(g) = \sum_H f(gh)$$

and compute

$$\begin{aligned}\sharp(G) f^{0\wedge}(e) &= \sum_G f^0(g) e(g)^* \\ &= \sum_G \sum_H f(gh) e(g)^* \\ &= \sum_H \sum_G f(g) e(gh^{-1})^* \\ &= \sum_H e(h) \sum_G f(g) e(g)^* \\ &= \sharp(H)\sharp(G)\hat{f}(e)\end{aligned}$$

if $e \equiv 1$ on H, and 0 otherwise, in accordance with Exercise 1. But then

$$\begin{aligned}f^0(g) &= \sum_{\hat{G}} f^{0\wedge}(e) e(g) \\ &= \sharp(H) \sum_{(G/H)^\wedge} \hat{f}(e) e(g),\end{aligned}$$

and Poisson's formula drops out upon putting $g = 1$.

This formula should be compared with the Poisson summation formula for functions on the line:

$$\sum_{Z^1} f(n) = \sum_{Z^1} \hat{f}(n)$$

[see Subsection 2.7.5]. The similarity is plain; in fact, if G is the additive group R^1 and if H is the subgroup Z^1, then G/H is the circle group $S^1 = [0, 1)$, and $(G/H)^\wedge = (S^1)^\wedge$ is a copy of Z^1 [see Exercise 4.1.10]. Therefore, apart from the factor $\sharp(H)$, the formula has the same group-theoretical flavor in both cases.

*EXERCISE 2**.[1] Find the solution of

$$x_0^2 - x_1 x_2 = y_0, \qquad x_1^2 - x_2 x_0 = y_1, \qquad x_2^2 - x_0 x_1 = y_2,$$

for known y. Think of x and y as functions on the additive group Z_3. The dual group $Z_3^\wedge$ can be identified with the multiplicative group of cube roots of unity:

$$\omega = 1, \quad e^{2\pi i/3}, \quad e^{4\pi i/3},$$

via the formula $e(k) = \omega^k$. Check the identity

$$\hat{x}(e^{2\pi i/3}\omega)\,\hat{x}(e^{4\pi i/3}\omega) = \tfrac{1}{3}\hat{y}(\omega^2)$$

and obtain the *Answer:*

$$\hat{x}(\omega) = \pm[\hat{y}(\omega^2)]^{-1}\{\tfrac{1}{27}\hat{y}(1)\,\hat{y}(e^{2\pi i/3})\,\hat{y}(e^{4\pi i/3})\}^{1/2},$$

assuming $\hat{y} \neq 0$.

EXERCISE 3.[2] Check that for any function f on G, the determinant of the $\#(G) \times \#(G)$ matrix $[f(g_1 g_2^{-1})]$ can be expressed as

$$\det[f(g_1 g_2^{-1})] = \prod_{\hat{G}} \#(G)\hat{f}(e)$$

and use this to prove a primitive variant of Exercise 4.2.4. *Hint:*

$$f(g_1 g_2^{-1}) = \sum_{\hat{G}} \hat{f}(e)\, e(g_1)\, e(g_2)^*.$$

EXERCISE 4.[3] Check the following variant of the Poisson summation formula:

$$\sum_{G/H}\left|\sum_{H} f(gh)\right|^2 = \#(G)\#(H)\sum_{(G/H)^\wedge} |\hat{f}(e)|^2$$

with the previous convention about $(G/H)^\wedge$. *Hint:* Apply the Plancherel identity to $f^0(g) = \sum_H f(gh)$.

EXERCISE 5.[3] The group $G = Z_2^+ \times \cdots \times Z_2^+$ (n-fold) is placed in 1:1 correspondence with the set $Q = 0, 1, \cdots, 2^n - 1$ by mapping

$$g = (k_0, \cdots, k_{n-1}) \to \sum_{i=0}^{n-1} k_i 2^i,$$

[1] K. Itô, private communication.

[2] Adapted from W. N. Anderson, Jr., private communication.

[3] After Crimmins *et al.* [1969].

in which $k_i = 0$ or 1 for $0 \leqslant i < n$. This permits you to think of Q as a group isomorphic to G. Prove that $j\colon G \to Q$ is an isomorphism iff

$$j(g) = \sum_{i=0}^{n=1} [1 - e_i(g)]\, 2^{i-1},$$

in which $e_i\colon 0 \leqslant i < n$ is a basis of the dual group $\hat{G}$, that is to say, every character e can be expressed in precisely one way as a product $e = e_0^{k_0} \cdots e_{n-1}^{k_{n-1}}$ with $0 \leqslant k_i < 2$.

EXERCISE 6. The *infinite* product $G = Z_2{}^+ \times Z_2{}^+ \times \cdots$ is a commutative group; it may be put into correspondence with the interval $0 \leqslant x < 1$ by means of the map

$$j\colon g = (k_1, k_2, \cdots) \to x = \sum_{i=1}^{\infty} k_i 2^{-i}.$$

The correspondence is not 1:1 owing to the fact that rational numbers x have ambiguous binary expansions, but they fill up a set of measure 0, only. Check that the action of G on $[0, 1]$ defined by the recipe $gx = j[gj^{-1}(x)]$ preserves the lengths of intervals and therefore the measure of nice sets, also. The so-called "Rademacher function" $e_n(x) = 1 - 2k_n$ is a character of G, as is the "Walsh function"

$$e^i(x) = e_1^{i_1}(x) e_2^{i_2}(x) \cdots$$

for any "tame" $i = (i_1, i_2, \cdots) \in G$, i.e., any string of 0's and 1's with only 0's from some point on. Draw pictures of the first few Rademacher functions. Prove that the family of Walsh functions is a unit-perpendicular basis of $\mathrm{L}^2[0, 1]$.

4.6★ GAUSS' LAW OF QUADRATIC RECIPROCITY

Fourier series on a finite commutative group *look* very simple, but the applications can be both complicated and deep. Applications to number theory can be found in Chandrasekharan [1968], Hardy and Wright [1954], and Rademacher [1956]; to statistical mechanics in Ginibre [1970], and McKean [1964]; to coding in Crimmins *et al.* [1969]; and this is only a tiny sample. The present application is to number theory.

Gauss' law of quadratic reciprocity has to do with a problem of arithmetic: *for which integers $0 < n < p$ is it possible to solve the quadratic congruence $x^2 = n$, modulo p, for a fixed prime $p > 2$*, or, what is the same, which of the integers $0 < n < p$ are "quadratic residues" modulo p? To study this problem, bring in the "Legendre symbol"

$$e(n) = \left(\frac{n}{p}\right) = \begin{cases} +1 & \text{if } n \text{ is a quadratic residue modulo} p, \\ -1 & \text{otherwise}. \end{cases}$$

Gauss' law states that for any odd primes p and q

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(1/2)(p-1)(1/2)(q-1)}.$$

The purpose of this section is to prove this fact by Fourier methods via the so-called *Gaussian sum* defined by the recipe

$$G_q(e^{2\pi in/q}) = \sum_{k=0}^{q-1} e^{2\pi ik^2n/q}$$

for $0 \leqslant n < q$ and any odd integer q, prime or not. This is one of the simpler though not the most elementary proofs of the law of quadratic reciprocity. Gauss himself gave eight different proofs; see Nagell [1951, p. 144], and, for additional information on this beautiful circle of ideas, Bachmann [1907] and/or Rademacher [1964]. The first steps of the proof are contained in Exercises 1 and 2. $Z_p{}^\times$ is the group of integers $0 < n < p$ under multiplication modulo$p$ [see Exercise 4.1.1]. Q is the class of quadratic residues $0 < n < p$, and Q' the complementary class of quadratic nonresidues.

EXERCISE 1. Check that the integers $1^2, 2^2, \cdots, (p-1)^2$, considered modulo$p$, provide a twofold list of Q; in particular, both Q and Q' contain $\frac{1}{2}(p-1)$ integers, each.

EXERCISE 2. Check that the Legendre symbol $e(n) = (n/p)$ is a character of Z_p, that is to say, $Q \cdot Q \subset Q$, $Q' \cdot Q \subset Q'$, and $Q' \cdot Q' \subset Q$. *Hint:* Check $Q \cdot Q \subset Q$ first; the rest follows by counting with the help of Exercise 1.

Here, the proof takes a peculiar twist: You take e, which is a character of $Z_p{}^\times$, extend it to the additive group $Z_p{}^+$ by putting $e(0) = 0$, and expand it into a Fourier series on the latter. This is how the Gaussian sums come in. To begin with,

$$\begin{aligned} e^\vee(n) &= \sum_{k=0}^{p-1} e(k)\, e^{2\pi ink/p} \\ &= \sum_Q e^{2\pi ink/p} - \sum_{Q'} e^{2\pi ink/p} \end{aligned}$$

for $0 \leqslant n < p$, in which $Z_p^{+\wedge}$ is identified with the multiplicative group of pth roots of unity. The elementary identity

$$0 = \sum_{k=0}^{p-1} e^{2\pi ink/p} = 1 + \sum_Q e^{2\pi ink/p} + \sum_{Q'} e^{2\pi ink/p}$$

and Exercise 1 are now applied to identify $e^\vee$ as a Gaussian sum:

$$\begin{aligned} e^\vee(n) &= 1 + 2 \sum_Q e^{2\pi ink/p} \\ &= \sum_{k=0}^{p-1} e^{2\pi ink^2/p} \\ &= G_p(e^{2\pi in/p}). \end{aligned}$$

This leads at once to a useful formula: For $0 < n < p$, nk runs through Z_p^+ once (modulo$p$) as k runs from 0 to $p-1$, so by Exercise 2,

$$\begin{aligned} G_p(e^{2\pi in/p}) = e^\vee(n) &= \sum_{k=0}^{p-1} e(nk)\, e^{2\pi ink/p} e(n) \\ &= \sum_{k=0}^{p-1} e(k)\, e^{2\pi ik/p} e(n) \\ &= G_p(e^{2\pi i/p})\, e(n), \end{aligned}$$

permitting you to express the Legendre symbol for $0 < n < p$ as a ratio of Gaussian sums:

$$e(n) = \frac{G_p(e^{2\pi in/p})}{G_p(e^{2\pi i/p})}.$$

The latter is nothing but an odd way of writing the Z_p^+ Fourier series for e, modified at $n = 0$ so as to make $e(0) = G_p(e^{2\pi i/p})^{-1}$.

EXERCISE 3. Deduce that $G_p(e^{2\pi i/p}) = \sqrt{p}$ times a power of i; no computations are needed! *Hint:* $e^{\vee\vee} = G_p(e^{2\pi i/p})^2 e = pe(-\ \cdot)$, and this implies $G_p^2 = \pm p$.

EXERCISE 4.

$$G_{pq}(e^{2\pi i/pq}) = G_p(e^{2\pi iq/p})\, G_q(e^{2\pi ip/q})$$

for any odd primes p and q. *Hint:* Compute the left-hand side from the definition, using the fact that as $k[j]$ runs once from 0 to $p-1$ $[q-1]$, $kq+jp$ runs once over $0 \leqslant n < pq-1$, modulopq.

The law of quadratic reciprocity can now be stated entirely in terms of Gaussian sums:

$$\begin{aligned} (-1)^{(1/2)(p-1)(1/2)(q-1)} &= \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \\ &= \frac{G_q(e^{2\pi ip/q})\, G_p(e^{2\pi iq/p})}{G_q(e^{2\pi i/q})\, G_p(e^{2\pi i/p})} \\ &= \frac{G_{pq}(e^{2\pi i/pq})}{G_p(e^{2\pi i/p})\, G_q(e^{2\pi i/q})}. \end{aligned}$$

EXERCISE 5. Check that the law of quadratic reciprocity follows from the evaluation of the Gaussian sum:

$$G_p(e^{2\pi i/p}) = \sqrt{p}(i)^{[(p-1)/2]^2}$$

for *any* odd integral p, prime or not. *Hint:* The elementary congruence

$$\left(\frac{pq-1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2 - \left(\frac{q-1}{2}\right)^2 = \frac{(p-1)(q-1)}{2} \text{ modulo } 4$$

is helpful.

The proof is finished by the actual evaluation of the Gaussian sum, based upon the deeper formula of Landsberg and Schaar:

$$\frac{1}{\sqrt{p}}\sum_{n=0}^{p-1} e^{2\pi i n^2 q/p} = \frac{e^{\pi i/4}}{\sqrt{2q}}\sum_{n=0}^{2q-1}\exp\left(\frac{-\pi i n^2 p}{2q}\right)$$

for any integral p and $q \geqslant 1$.

PROOF.[1] The proof is based upon the Jacobi identity for the theta-function:

$$\sum_{n=-\infty}^{\infty} \exp(-\pi n^2 t) = t^{-1/2} \sum_{n=-\infty}^{\infty} \exp(-\pi n^2/t)$$

[see Subsection 1.7.5], which was proved for $t > 0$, but is actually valid in the open right-hand half-plane, both sides being analytic in that region. Replace $t > 0$ by $t - 2iq/p$ and make $t \downarrow 0$. The left-hand side of Jacobi's identity is

$$\sum e^{-\pi n^2 t}\exp(2\pi i n^2 q/p) = t^{-1/2}\left[(1/p)\sum_{n=0}^{p-1}\exp(2\pi i n^2 q/p) + o(1)\right],$$

since $\exp(2\pi i n^2 q/p)$, as a function of n, is of period p, and

$$\sum \exp(-\pi n^2 t) = t^{-1/2}[1 + o(1)].$$

Besides, the right-hand side is

$$\frac{1}{(t-2iq/p)^{1/2}}\sum \exp\left(-\frac{\pi n^2 t}{t^2+4q^2/p^2}\right)\exp\left(-\frac{2\pi i n^2 q/p}{t^2+4q^2/p^2}\right)$$

$$= \frac{1}{(-2iq/p)^{1/2}}\left(\frac{4q^2}{tp^2}\right)^{1/2}\left[\frac{1}{2q}\sum_{n=0}^{2q-1}\exp\left(\frac{-\pi i n^2 p}{2q}\right) + o(1)\right]$$

for similar reasons. A comparison of the two expressions produces the Landsberg–Schaar identity.

[1] Adapted from Bellman [1961].

The evaluation of the Gaussian sum is now achieved by putting $q = 1$:

$$G_p(e^{2\pi i/p}) = \left(\frac{p}{2}\right)^{\frac{1}{2}} e^{\pi i/4}[1+e^{-\pi i p/2}]$$
$$= \sqrt{p}(i)^{[(p-1)/2]^2},$$

as you can easily check by looking at the cases $p = 1$ modulo 4 and $p = 3$ modulo 4, separately.

EXERCISE 6. Use the Landsberg–Schaar identity to prove the so-called "supplementary theorems":

(a) $\left(\dfrac{-1}{p}\right) = (-1)^{[(p-1)/2]^2}$

(b) $\left(\dfrac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Hint: (b) is proved by putting $q = 2$; as to (a), look at

$$\left(\frac{-1}{p}\right)G_p(e^{2\pi i/p}) = G_p(e^{-2\pi i/p}) = G_p(e^{2\pi i/p})^*.$$

EXERCISE 7. Check that the Möbius function of Exercise 4.3.8 can be expressed as

$$e(n) = \sum_{\substack{1 \leqslant k < n \\ (k,n)=1}} e^{2\pi i k/n}.$$

$(k, n) = 1$ signifies that k and n have no common primes. *Hint:* Prove first that the sum $[f(n)]$ is "multiplicative" $[f(ij) = f(i)f(j)$ if $(i,j) = 1]$ with the help of the trick suggested for use in Exercise 4. Then evaluate $f(n)$ for n a prime power.

4.7 NONCOMMUTATIVE GROUPS

The rest of this chapter is devoted to a number of special but important noncommutative groups.

A finite noncommutative group G cannot have enough characters to do Fourier series: If it did, then every function f on G could be expanded as a sum

$$f(g) = \sum_{\hat{G}} \hat{f}(e)e(g),$$