Part III — Modular Forms and L-functions
Definitions

Based on lectures by A. J. Scholl

Notes taken by Dexter Chua

Lent 2017

These notes are not endorsed by the lecturers, and I have modified them (often significantly) after lectures. They are nowhere near accurate representations of what was actually lectured, and in particular, all errors are almost surely mine.

Modular Forms are classical objects that appear in many areas of mathematics, from number theory to representation theory and mathematical physics. Most famous is, of course, the role they played in the proof of Fermat's Last Theorem, through the conjecture of Shimura-Taniyama-Weil that elliptic curves are modular. One connection between modular forms and arithmetic is through the medium of L-functions, the basic example of which is the Riemann ζ-function. We will discuss various types of L-function in this course and give arithmetic applications.

Pre-requisites

Prerequisites for the course are fairly modest; from number theory, apart from basic elementary notions, some knowledge of quadratic fields is desirable. A fair chunk of the course will involve (fairly 19th-century) analysis, so we will assume the basic theory of holomorphic functions in one complex variable, such as are found in a first course on complex analysis (e.g. the 2nd year Complex Analysis course of the Tripos).

Contents

0 Introduction

1 Some preliminary analysis

1.1 Characters of abelian groups

Definition (Character)**.** Let G be an abelian topological group. A (unitary) *character* of G is a continuous homomorphism $\chi : G \to \mathrm{U}(1)$, where $\mathrm{U}(1) = \{z \in \mathbb{C} \mid |z| = 1\}$.

Definition (Character group)**.** Let G be a group. The *character group* (or *Pontryagin dual*) $\hat{G}$ is the group of all characters of G.

1.2 Fourier transforms

Definition (Fourier transform)**.** Let $f : \mathbb{R} \to \mathbb{C}$ be an L^1 function, i.e. $\int |f| \;\mathrm{d}x < \infty$. The *Fourier transform* is

$$\hat{f}(y) = \int_{-\infty}^{\infty} e^{-2\pi i x y} f(x) \;\mathrm{d}x = \int_{-\infty}^{\infty} \chi_y(x)^{-1} f(x) \;\mathrm{d}x.$$

This is a bounded and continuous function on $\mathbb{R}$.

Definition (Schwarz space)**.** The *Schwarz space* is defined by

$$\mathcal{S}(\mathbb{R}) = \{f \in C^\infty(\mathbb{R}) : x^n f^{(k)}(x) \to 0 \text{ as } x \to \pm\infty \text{ for all } k, n \geq 0\}.$$

Definition (Discrete Fourier transform)**.** Given a function $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$, we define the *Fourier transform* $\hat{f} : \mu_N \to \mathbb{C}$ by

$$\hat{f}(\zeta) = \sum_{a \in \mathbb{Z}/N\mathbb{Z}} \zeta^{-a} f(a).$$

Definition (Haar measure)**.** Let G be a topological group. A *Haar measure* is a left translation-invariant Borel measure on G satisfying some regularity conditions (e.g. being finite on compact sets).

Definition (Fourier transform)**.** Let G be a locally compact abelian group with a Haar measure $\mathrm{d}g$, and let $f : G \to \mathbb{C}$ be a continuous L^1 function. The *Fourier transform* $\hat{f} : \hat{G} \to \mathbb{C}$ is given by

$$\hat{f}(\chi) = \int_G \chi(g)^{-1} f(g) \;\mathrm{d}g.$$

1.3 Mellin transform and Γ-function

Definition (Mellin transform)**.** Let $f : \mathbb{R}_{>0} \to \mathbb{C}$ be a function. We define

$$M(f, s) = \int_0^\infty y^s f(y) \;\frac{\mathrm{d}y}{y},$$

whenever this converges.

Definition (Γ function)**.** The Γ *function* is the Mellin transform of

$$f(y) = e^{-y}.$$

Explicitly, we have

$$\Gamma(s) = \int_0^\infty e^{-y} y^s \;\frac{\mathrm{d}y}{y}.$$

2 Riemann ζ-function

Definition (Riemann ζ-function)**.** The *Riemann ζ-function* is defined by

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}$$

for $\mathrm{Re}(s) > 1$.

Definition (Bernoulli numbers)**.** The *Bernoulli numbers* are defined by a generating function

$$\sum_{n=0}^{\infty} B_n \frac{t^n}{n!} = \frac{t}{e^t - 1} = \left(1 + \frac{t}{2!} + \frac{t^2}{3!} + \cdots\right)^{-1}.$$

Notation.

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2).$$
$$\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$$

These are the real/complex Γ-*factors*.

Notation.

$$Z(s) \equiv \Gamma_{\mathbb{R}}(s)\zeta(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

3 Dirichlet L-functions

Definition (Dirichlet characters)**.** Let $N \geq 1$. A *Dirichlet character mod* N is a character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$.

As before, we write $\widehat{(\mathbb{Z}/N\mathbb{Z})}^\times$ for the group of characters.

Definition (Primitive character)**.** We say a character $\chi \in \widehat{(\mathbb{Z}/n\mathbb{Z})}^\times$ is *primitive* if there is no $M < N$ with $M \mid N$ with $\chi' \in \widehat{(\mathbb{Z}/M\mathbb{Z})}^\times$ such that

$$\chi = \chi' \circ (\text{reduction mod } M).$$

Definition (Equivalent characters)**.** We say characters $\chi_1 \in \widehat{(\mathbb{Z}/N_1\mathbb{Z})}^\times$ and $\chi_2 \in \widehat{(\mathbb{Z}/N_2\mathbb{Z})}^\times$ are *equivalent* if for all $x \in \mathbb{Z}$ such that $(x, N_1 N_2) = 1$, we have

$$\chi_1(x \text{ mod } N_1) = \chi_2(x \text{ mod } N_2).$$

Definition (Conductor)**.** The *conductor* of a character χ is the unique $M \mid N$ such that there is a *primitive* $\chi_* \in \widehat{(\mathbb{Z}/M\mathbb{Z})}^\times$ that is equivalent to χ.

Definition (Dirichlet L-series)**.** Let $\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})}^\times$ be a Dirichlet character. The *Dirichlet L-series* of χ is

$$L(\chi, s) = \sum_{\substack{n \geq 1 \\ (n, N) = 1}} \chi(n) n^{-s}.$$

4 The modular group

Definition ($\mathrm{GL}_2(\mathbb{R})^+$)**.**

$$\mathrm{GL}_2(\mathbb{R})^+ = \{\gamma \in \mathrm{GL}_2(\mathbb{R}) : \det \gamma > 0\}.$$

Definition ($\mathrm{PGL}_2(\mathbb{R})^+$)**.**

$$\mathrm{PGL}_2(\mathbb{R})^+ = \frac{\mathrm{GL}_2(\mathbb{R})^+}{\mathbb{R}^\times \cdot I}.$$

Definition (Modular group)**.** The *modular group* is

$$\mathrm{PSL}_2(\mathbb{Z}) = \frac{\mathrm{SL}_2(\mathbb{Z})}{\{\pm I\}}.$$

Definition (Principal congruence subgroup)**.** For $N \geq 1$, the *principal congruence subgroup* of level N is

$$\Gamma(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv I \pmod N\} = \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})).$$

Any $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ containing some $\Gamma(N)$ is called a *congruence subgroup*, and its *level* is the smallest N such that $\Gamma \supseteq \Gamma(N)$

Definition ($\Gamma_0(N)$, $\Gamma_1(N)$)**.** We define

$$\Gamma_0(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod N\right\}$$

and

$$\Gamma_1(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0, d \equiv 1 \pmod N\right\}.$$

We similarly define $\Gamma^0(N)$ and $\Gamma^1(N)$ to be the transpose of $\Gamma_0(N)$ and $\Gamma_1(N)$ respectively.

5 Modular forms of level 1

5.1 Basic definitions

Definition (Modular form of level 1)**.** A holomorphic function $f : \mathcal{H} \to \mathbb{C}$ is a *modular form of weight* $k \in \mathbb{Z}$ *and level* 1 if

(i) For any
$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1),$$
we have
$$f(\gamma(z)) = (cz + d)^k f(z).$$

(ii) f is holomorphic at ∞ (to be defined precisely later).

Definition (Cusp form)**.** A modular form f is a *cusp form* if the constant term $a_0(f)$ is 0.

Definition (Weak modular form)**.** A *weak modular form* is a holomorphic form on $\mathcal{H}$ satisfying (i) which is *meromorphic* at ∞.

Definition (Eisenstein series)**.** Let $k \geq 4$ be even. We define

$$G_k(z) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(mz + n)^k} = \sideset{}{'}\sum_{(m,n) \in \mathbb{Z}^2} \frac{1}{(mz + n)^k}.$$

Definition (Normalized Eisenstein series)**.** We define

$$\begin{aligned} E_k(z) &= (2\zeta(k))^{-1} G_k(z) \\ &= 1 - \frac{2k}{B_k} \sum_{n \geq 1} \sigma_{k-1}(n) q^n \\ &= \frac{1}{2} \sum_{\substack{(m,n)=1 \\ m,n \in \mathbb{Z}}} \frac{1}{(mz + n)^k}. \end{aligned}$$

Definition (Slash operator)**.** Let

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \gamma \in \mathrm{GL}_2(\mathbb{R})^+, \quad z \in \mathcal{H},$$

and $f : \mathcal{H} \to \mathbb{C}$ any function. We write

$$j(\gamma, z) = cz + d.$$

We define the *slash operator* to be

$$(f \underset{k}{|} \gamma)(z) = (\det \gamma)^{k/2} j(\gamma, z)^{-k} f(\gamma(z)).$$

5.2 The space of modular forms

Definition (Δ and τ)**.**

$$\Delta = \frac{E_4^3 - E_6^2}{1728} = \sum_{n \geq 1} \tau(n) q^n \in S_{12}.$$

5.3 Arithmetic of Δ

6 Hecke operators

6.1 Hecke operators and algebras

Notation. For $g \in G$ and $m \in M^\Gamma$, we let

$$m|[\Gamma g \Gamma] = \sum_{i=1}^{n} m g_i, \qquad (*)$$

where

$$\Gamma g \Gamma = \coprod_{i=1}^{n} \Gamma g_i.$$

6.2 Hecke operators on modular forms

Definition (Hecke eigenform)**.** Let $f \in S_k \setminus \{0\}$. Then f is a *Hecke eigenform* if for all $n \geq 1$, we have

$$T_n f = \lambda_n f$$

for some $l_n \in \mathbb{C}$. It is *normalized* if $a_1(f) = 1$.

7 L-functions of eigenforms

Notation. We write $|a_n| = O(n^{k/2})$ if there exists $c \in \mathbb{R}$ such that for sufficiently large n, we have $|a_n| \leq cn^{k/2}$. We will also write this as

$$|a_n| \ll n^{k/2}.$$

8 Modular forms for subgroups of $\mathrm{SL}_2(\mathbb{Z})$

8.1 Definitions

Definition (Cusps)**.** The *cusps* of Γ (or $\bar{\Gamma}$) are the orbits of Γ on $\mathbb{P}^1(\mathbb{Q})$.

Definition (Width of cusp)**.** Let $\alpha \in \mathbb{Q} \cup \{\infty\}$ be a representation of a cusp of Γ. We pick $g \in \Gamma(1)$ with $g(\infty) = \alpha$. Then $\gamma(\alpha) = \alpha$ iff $g^{-1}\gamma g(\infty) = \infty$. So

$$g^{-1}\overline{\Gamma}_\alpha g = (\overline{g^{-1}\Gamma g})_\infty = \left\langle \pm \begin{pmatrix} 1 & m_\alpha \\ 0 & 1 \end{pmatrix} \right\rangle$$

for some $m_\alpha \geq 1$. This m_α is called the *width* of the cusp α (i.e. the cusp $\Gamma\alpha$).

Definition (Modular form)**.** Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be of finite index, and $k \in \mathbb{Z}$. A *modular form of weight k on* Γ is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ such that

(i) $f \underset{k}{|} \gamma = f$ for all $\gamma \in \Gamma$.

(ii) f is holomorphic at the cusps of Γ.

If moreover,

(iii) f vanishes at the cusps of Γ,

then we say f is a *cusp form*.

8.2 The Petersson inner product

8.3 Examples of modular forms

Definition ($G_{\mathbf{r},k}$)**.** Let $k \geq 3$. Pick any vector $\mathbf{r} = (r_1, r_2) \in \mathbb{Q}^2$. We define

$$G_{\mathbf{r},k}(z) = \sum_{\mathbf{m} \in \mathbb{Z}^2}{}' \frac{1}{((m_1 + r_1)z + m_2 + r_2)^k},$$

where $\sum'$ means we omit any $\mathbf{m}$ such that $\mathbf{m} + \mathbf{r} = \mathbf{0}$.

Definition (ϑ_2 and ϑ_4)**.**

$$\begin{aligned} \vartheta_2(z) &= \sum_{n \in \mathbb{Z}} e^{\pi i (n+1/2)^2 z} = q^{1/8} \sum_{n \in \mathbb{Z}} q^{n(n+1)/2} = 2q^{1/8} \sum_{n \geq 0} q^{n(n+1)/2} \\ \vartheta_4(z) &= \sum_{n \in \mathbb{Z}} (-1)^n e^{\pi i n^2 z} = 1 + 2 \sum_{n \geq 1} (-1)^n q^{n^2/2}. \end{aligned}$$

Notation. We write

$$W_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$$

9 Hecke theory for $\Gamma_0(N)$

Definition (Hecke operators on $\Gamma_0(N)$)**.** If $p \nmid N$, we define

$$T_p f = p^{\frac{k}{2}-1}\left(f\underset{k}{|}\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) + \sum_{k=0}^{p-1} f\underset{k}{|}\left(\begin{smallmatrix} 1 & b \\ 0 & p \end{smallmatrix}\right)\right)$$

which is the same as the case with $\Gamma(1)$.

When $p \mid N$, then we define

$$U_p f = p^{\frac{k}{2}-1}\sum_{n=0}^{p-1} f\underset{k}{|}\left(\begin{smallmatrix} 1 & b \\ 0 & p \end{smallmatrix}\right).$$

Some people call this T_p instead, and this is very confusing.

10 Modular forms and rep theory

Definition (Non-holomorphic modular forms)**.** We let $W_k(\Gamma(1))$ be the set of all C^∞ functions $\mathcal{H} \to \mathbb{C}$ such that

(ii) $f \underset{k}{|} \gamma = f$ for all $\gamma \in \Gamma(1)$

(iii) $f(x + iy) = O(y^R)$ as $y \to \infty$ for some $R > 0$, and the same holds for all derivatives.

Definition (Maass form)**.** A *Maass form* on $\mathrm{SL}_2(\mathbb{Z})$ is an $f \in W_0(\Gamma(1))$ such that

$$\Delta f = \lambda f$$

for some $\lambda \in \mathbb{C}$.

Definition (Cusp form)**.** A Maass form is a *cusp form* if $F_1 = 0$, i.e. $A = B = 0$.

Definition (R_k^*)**.** Define

$$R_k^* = 2i\frac{\partial}{\partial z} + \frac{1}{y}k.$$

Definition (Automorphic form)**.** An *automorphic form* on Γ is a C^∞ function $\Phi : \Gamma \backslash G \to \mathbb{C}$ such that $\Phi(g r_\theta) = e^{ik\theta}\Phi(g)$ for some $k \in \mathbb{Z}$ such that

$$\Omega\Phi = \lambda\Phi$$

for some $\lambda \in \mathbb{C}$, satisfying a growth condition given by

$$\Phi \begin{pmatrix} a & b \\ c & d \end{pmatrix} \leq \text{polynomial in } a, b, c, d.$$