

The geometry of numbers:  
an automorphic perspective  
Stephen D. Miller  
Rutgers University  
Spring 2020

February 7, 2021

## Contents

<b>I</b>	<b>2/14 Lecture</b>	<b>4</b>
1	Review: Minkowski's second theorem	4
2	Small exponent RSA	4
3	Coppersmith: An Overview	6
<b>II</b>	<b>2/18 Lecture</b>	<b>10</b>
4	The Siegel Integration Formula	10
5	Existence of dense packings	11
6	Lie theoretic formulation of Siegel's Integration Formula	12

7	Eisenstein series and Epstein zeta function	15
<b>III</b>	<b>2/21 Lecture</b>	<b>17</b>
8	Non-holomorphic Eisenstein series for $SL(2, \mathbb{Z})$	17
9	The Maass-Selberg Relations for $SL(2)$	18
10	Applications of Maass-Selberg	20
11	Proof of the Maass-Selberg relations for $n = 2$	21
<b>IV</b>	<b>2/25 Lecture</b>	<b>23</b>
12	Borel Eisenstein Series on $SL(n, \mathbb{R})$	24
	12.1 Borel Eisenstein Series . . . . .	25
	12.2 Langlands' constant term formula . . . . .	26
13	The Maass-Selberg relations for $SL(n)$	27
<b>V</b>	<b>2/28 Lecture</b>	<b>28</b>
14	Application of Maass-Selberg to $\text{vol}(\Gamma \backslash G)$	28
15	Second proof of the Siegel Integration Formula	30
<b>VI</b>	<b>3/3 Lecture</b>	<b>35</b>
<b>VII</b>	<b>3/6 Lecture</b>	<b>40</b>
16	Case (ii) of Harish-Chandra's Theorem	86
17	LLL Algorithm	90

These are notes from my graduate course on lattices at Rutgers University during the Spring 2020 semester. The first part of the course covered some standard topics in the geometry of numbers (such as Minkowski's theorems, which is where these notes start). The notes for the second part of the course (below) were taken and typed up by several students (Leonidas Daskalakis, Priyank Deshpande, Louis Gaudet, George Hauser, Sumeet Khandelwal, Alex Karlovitz, Doyon Kim, Nathan Mehlhop, and Forrest Thurman), with later edits and aggregation by myself. I wish to thank these students for this.

The notes are partly intended not just for mathematicians, but also for computer scientists (especially cryptographers) and physicists. Given the potential value they may have for scientists in other areas, I have decided to release the notes in a fairly unpolished state (hoping to return to them with future editing). It goes without saying that these rough notes are to be used at the reader's own risk, since there are surely typos and gaps etc. in the exposition. (Even more so, those typos and gaps should be attributed to me and *not* to the student scribes!)

–Stephen D. Miller, Rutgers University

## Part II

### 2/18 Lecture

#### 4 The Siegel Integration Formula

Let  $G = SL(n, \mathbb{R})$  and  $\Gamma = SL(n, \mathbb{Z})$ . As we have seen,  $\Gamma \backslash G$  is the moduli space of unimodular lattices  $\Lambda$  (unimodular meaning  $|\Lambda| = 1$ ). A matrix  $g \in G$  corresponds to the lattice  $\Lambda$  spanned by its rows  $v_1, \dots, v_n$ ,

$$\Lambda = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_n$$

$G$  is locally compact and so carries a Haar measure  $dg$  invariant under right translation (and unique up to a constant positive multiple). In fact,  $dg$  is necessarily also invariant under left translation, since for any  $h$ ,  $d(hg) = \chi(h)dg$  for some positive constant  $\chi(h)$ ; by composition clearly  $\chi$  is a character on  $G$  with values in  $\mathbb{R}_{>0}$ , but  $G = SL(n, \mathbb{R})$  does not have any nontrivial such characters, showing  $\chi \equiv 1$ . Thus  $dg$  gives a bi-invariant measure on the space of lattices, under which  $\Gamma \backslash G$  in fact has finite volume.

Given an even Schwartz function  $f \in \mathcal{S}(\mathbb{R}^n)$ , the sum of the function  $f$  over the lattice  $\Lambda$  corresponding to a matrix  $g \in G$  defines a function on  $\Gamma \backslash G$  by the formula

$$\mathcal{E}_f(g) = \sum_{\substack{\lambda \in \Lambda \\ \lambda \neq 0}} f(\lambda), \quad (1)$$

where the sum is over nonzero integral combinations of the rows of  $g$ . Then *Siegel's Integration Formula*

$$\frac{1}{\text{vol}(\Gamma \backslash G)} \int_{\Gamma \backslash G} \mathcal{E}_f(g) dg = \int_{\mathbb{R}^n} f(x) dx \quad (2)$$

says the mean of  $\mathcal{E}_f$  equals the total integral of  $f$ .

#### Remarks:

1. One can relax the conditions on  $f$  but – as is nearly always the case with summation formulas – the exact class of functions is not as important as the underlying algebraic identity (one proves it for a large range

of functions, and later attempts to extend to more general cases by limiting arguments).

2. Roughly speaking, formula (2) equates two different kind of averages. On the right-hand side there is the total integral of  $f$ . On the left-hand side, there is a type of iterated average: first  $f$  is summed over a lattice, then the value of that sum is averaged over all lattices. Siegel's proof of (2) first argues (purely on the grounds of invariance properties) that these averages must coincide up to a constant, and then shows the constant is in fact 1 by a limiting argument.
3. Both sides of Siegel's Integration Formula (2) are unchanged if  $f(x)$  is replaced by  $f(xk)$  for  $k \in K = \text{SO}(n)$ , so we may without loss of generality take  $f$  to be rotationally symmetric (by replacing  $f(x)$  with  $\int_K f(xk)dk$ ).

## 5 Existence of dense packings

Before giving the proof of Siegel's Integration Formula (2), we make a detour to see its famous application to sphere packing.

A domain  $S \subset \mathbb{R}^n$  is called *star-like* if  $ts \in S$  whenever  $s \in S$  and  $0 \leq t \leq 1$ . Suppose  $S$  is star-like, bounded, and measurable, and further satisfies the symmetry condition  $S = -S$ . Then Siegel's Integration Formula (2) (after being extended to a larger class of functions  $f$ ) can be applied to the characteristic function  $f = \chi_S$  of  $S$ . We know that

$$\sum_{\substack{\lambda \in \Lambda \\ \lambda \neq 0}} f(\lambda) = \sum_{\substack{\lambda \in \Lambda \\ \lambda \neq 0}} \chi_S(\lambda) = \#\{\lambda \in \Lambda \cap S \mid \lambda \neq 0\}$$

is an *even* non-negative integer  $\geq 0$ , owing to  $S = -S$ . Siegel's Integration formula then equates the mean value of this integer, taken over all unimodular lattices, with the volume of  $S$ .

The upshot is that there must exist some lattice  $\Lambda$  with  $|\Lambda| = 1$  such that

$$\#\{\lambda \in \Lambda \cap S \mid \lambda \neq 0\} \leq \text{vol}(S)$$

(by the mean value theorem); if we furthermore assume  $\text{vol}(S) < 2$ , then we must have  $S \cap \Lambda = \{0\}$ . That is, for quantifiably small  $S$  there always exists some unimodular lattice whose nonzero vectors completely avoid  $S$ .

The most natural such case to consider, of course, is when  $S$  is a ball. The radius  $r$  of a ball in  $\mathbb{R}^n$  of volume 2 is  $r = \left(\frac{n}{2\pi e}\right)^{1/2} (1 + O(1/n))$  (which is an easy exercise using Stirling's formula). It follows that there exists some unimodular lattice  $\Lambda$  such that

$$\lambda_1(\Lambda) \geq r \sim \sqrt{\frac{n}{2\pi e}}, \quad (3)$$

which gives the existence of dense lattice packings! Of course this is merely an existence result: direct constructions of such lattices are not known.

The bound (3) is basically the Minkowski-Hlawka Theorem. It gives a better estimate than simply taking *saturated* packings, in which one places points at least distance 2 apart until there is no further opportunity to do so (the packing of balls of radius 1 centered at these points has density at least  $2^{-n}$ , because doubling the radii would yield balls that cover all of  $\mathbb{R}^n$ ). The estimate (3) turns out yield twice as large a lower bound. Over the years there have been further improvements for lower bounds with better constants and in particular dimensions. For example,

- $n2^{-n}$  for lattices (Rogers, 1950s)
- $65963n2^{-n}$  (Venkatesh 2010) (and actually  $(\log \log n)n2^{-n}$  for special  $n$  – see below.) Also, the constant 65963 can actually be increased to any constant  $< 2 \sinh(\pi e)^2 / \pi^2 e^3$ .

## 6 Lie theoretic formulation of Siegel's Integration Formula

The traditional proof (due to Siegel) first uses the underlying symmetries to show that the left- and right-hand sides of (2) agree up to a constant. There are various ways to pin down that this constant equals 1. One convincing argument is to look at the special case that  $f$  is the characteristic function of a ball of a large radius  $r$  in  $\mathbb{R}^n$ . For fixed  $g$  and large  $r$  we have that

$$\mathcal{E}_f(g) = \#(\Lambda \cap \{\|\lambda\| \leq r\}) - 1 \sim \text{volume of ball of radius } r,$$

which is basically a restatement of the fact that the covolume  $|\Lambda| = 1$ . The volume on the right-hand side is of course the total integral  $\int_{\mathbb{R}^n} f(x)dx$  of  $f$ .

There is an equivalent statement of Siegel's theorem in terms of *primitive vectors* in  $\Lambda$ , i.e., those for which  $\lambda \in m\Lambda$  implies  $m = \pm 1$ . This is quite natural from the point of view of detecting short vectors, since imprimitive vectors are never the shortest in  $\Lambda$ . Let  $\Lambda'$  denote the set of primitive vectors in  $\Lambda$ , and define

$$\mathcal{E}'_f(g) := \sum_{\lambda \in \Lambda'} f(\lambda) \quad \text{and} \quad f^\Sigma(x) := \sum_{m \geq 1} f(mx). \quad (4)$$

Then  $\mathcal{E}_f(g) = \mathcal{E}'_{f^\Sigma}(g)$ , since  $\Lambda_{\neq 0} = \bigsqcup_{m \geq 1} m\Lambda'$ . Also,

$$\begin{aligned} \int_{\mathbb{R}^n} f^\Sigma(x) dx &= \int_{\mathbb{R}^n} \sum_{m \geq 1} f(mx) dx \\ &= \sum_{m \geq 1} m^{-n} \int_{\mathbb{R}^n} f(x) dx = \zeta(n) \int_{\mathbb{R}^n} f(x) dx. \end{aligned} \quad (5)$$

Therefore the Siegel integration formula (2) has the equivalent reformulation

$$\frac{1}{\text{vol}(\Gamma \backslash G)} \int_{\Gamma \backslash G} \mathcal{E}'_{f^\Sigma}(g) dg = \frac{1}{\zeta(n)} \int_{\mathbb{R}^n} f^\Sigma(x) dx. \quad (6)$$

However, this last equation is in terms of the function  $f^\Sigma$  from (4), but not  $f$  itself. However, it is actually *equivalent* to such a statement,

$$\frac{1}{\text{vol}(\Gamma \backslash G)} \int_{\Gamma \backslash G} \mathcal{E}'_f(g) dg = \frac{1}{\zeta(n)} \int_{\mathbb{R}^n} f(x) dx, \quad f \in \mathcal{S}(\mathbb{R}^n). \quad (7)$$

The reasoning behind the equivalence is as follows: (7) also holds for the functions  $f(m \cdot)$ ,  $m \in \mathbb{N}$ , and summing over  $m$  recovers (6). The other direction of the equivalence follows similarly using Möbius inversion.

Recall that  $\Lambda$  is the  $\mathbb{Z}$ -span of the rows  $v_j$  of the matrix  $g$ , and so  $\Lambda'$  consists of all vectors of the form  $\lambda = m_1 v_1 + \cdots + m_n v_n$  for coprime  $n$ -tuples of integers  $m_j$ . Every such coprime  $n$ -tuple  $[m_1 \ m_2 \ \cdots \ m_n]$  (written as a row vector) is the bottom row of some matrix  $\gamma \in \Gamma = \text{SL}(n, \mathbb{Z})$ . Letting  $e_n = [0 \ 0 \ \cdots \ 0 \ 1]$  denote the  $n$ -th standard basis vector,  $e_n \gamma = [m_1 \ m_2 \ \cdots \ m_n]$  and one recovers that  $\lambda = e_n \gamma g$  is the bottom row of  $\gamma g$ .

Of course, the  $\gamma$  here is not uniquely determined. To measure this, we introduce some notation. Let  $P$  denote the “mirabolic” subgroup of  $G$  consisting

of all matrices such that  $e_n p = z e_n$  for some  $z \neq 0$ . Thus  $P$  is the set of matrices in  $G = \mathrm{SL}(n, \mathbb{R})$  having bottom row equal to a nonzero multiple of  $e_n$ , and  $\{\text{bottom rows of matrices in } \Gamma g\}$  is in bijection with  $\{\text{elements of } (P_+ \cap \Gamma) \backslash \Gamma g\}$ , where  $P_+$  is defined as the subset of  $P$  for which the bottom right entry of the matrix is equal to 1.<sup>4</sup> This is because  $P_+ \cap \Gamma$  is the stabilizer of  $e_n$  in  $\Gamma$ .

Putting this together results in the formula

$$\mathcal{E}'_f(g) = \sum_{\lambda \in \Lambda'} f(\lambda) = \sum_{\gamma \in (\Gamma \cap P_+) \backslash \Gamma} f(e_n \gamma g),$$

and integrating over  $\Gamma \backslash G$  results in the equalities

$$\begin{aligned} \int_{\Gamma \backslash G} \mathcal{E}'_f(g) dg &= \int_{\Gamma \backslash G} \sum_{\gamma \in (\Gamma \cap P_+) \backslash \Gamma} f(e_n \gamma g) dg \\ &= \int_{(\Gamma \cap P_+) \backslash G} f(e_n g) dg && \text{(unfolding)} \\ &= \int_{P_+ \backslash G} \int_{(\Gamma \cap P_+) \backslash P_+} f(e_n p g) dp dg && \text{(folding)} \\ &= \int_{P_+ \backslash G} \int_{(\Gamma \cap P_+) \backslash P_+} f(e_n g) dp dg && \text{(since } e_n p = e_n) \\ &= \mathrm{vol}((\Gamma \cap P_+) \backslash P_+) \int_{P_+ \backslash G} f(e_n g) dg. \end{aligned}$$

The “folding” step involves a Haar measure for  $P_+$ , and to make this a proper argument one must compare the normalizations of the Haar measures on  $G$ ,  $P_+$ , and  $P_+ \backslash G$ . From above,  $P_+ \backslash G \cong \mathbb{R}^n - \{0\}$  and the measure  $dg$  on the quotient  $P_+ \backslash G$  corresponds to a scalar multiple of the usual Lebesgue measure on  $\mathbb{R}^n$ . Calculating the precise constant completes what amounts to a soft proof of the Siegel Integration Formula (which is basically Siegel’s original argument, just expressed more group-theoretically). This has a modern interpretation in terms of Tamagawa numbers, which gives a more general calculation these and many others measure factors.

---

<sup>4</sup>The mirabolic subgroup  $P$  is an example of a parabolic subgroup, a highly useful notion in linear algebraic groups. The name itself is a contraction of “miracle parabolic”.

## 7 Eisenstein series and Epstein zeta function

Our goal is to prove the equivalent formulation (7) of the Siegel integration formula. Most of the next several sections are devoted giving a proof of this using the theory of Eisenstein series. That such a proof exists is folklore due to the theory of the constant term. However, our proof seems to be new in the sense that it gives more precise information about the contribution of lattices coming from the cusps. In any event, by far and away the main purpose of this exposition is to explain how automorphic machinery can be used to prove Siegel's integration formula.

As mentioned above, there is no loss of generality in assuming that the function  $f \in \mathcal{S}(\mathbb{R}^n)$  is radially symmetric, meaning that  $f(x) = p(\|x\|)$  for some  $p \in \mathcal{S}(\mathbb{R})$  (necessarily even).<sup>5</sup>

We shall next see that formula (4),

$$\mathcal{E}'_f(g) = \sum_{\lambda \in \Lambda'} p(\|\lambda\|), \quad (8)$$

defines an *incomplete Eisenstein Series*.

Recall the *Epstein Zeta function*,

$$\text{Eps}(s, g) = \sum_{\substack{\lambda \in \Lambda \\ \lambda \neq 0}} \|\lambda\|^{-s},$$

which is absolutely convergent for  $\Re s > n$ . The *Mirabolic Eisenstein series* is defined as

$$\text{Eis}(s, g) = \sum_{\gamma \in (\Gamma \cap P) \backslash \Gamma} \|e_n \gamma g\|^{-s} = \frac{1}{2} \sum_{\lambda \in \Lambda'} \|\lambda\|^{-s} = \frac{1}{2\zeta(s)} \text{Eps}(s, g). \quad (9)$$

The factor of two corresponds to the fact that  $\pm I \in \Gamma \cap P$  (this is the difference between  $\Gamma \cap P$  and  $\Gamma \cap P_+$ ), and the factor of  $\zeta(s)$  comes from taking into account the multiples  $m\lambda$  of primitive  $\lambda$ , for  $m \in \mathbb{N}$  (just as in (5)).

---

<sup>5</sup>This correspondence induces an isomorphism of topological vectors spaces [?, Lemma 2.1].

Incomplete Eisenstein series are contour integrals of Eisenstein series, and we shall now demonstrate such a relation between  $\text{Eps}(s, g)$  and  $\text{Eis}(s, g)$ . Recall the *Mellin transform* of the even Schwartz function  $p$ ,

$$(Mp)(s) = \int_0^\infty p(x) x^s \frac{dx}{x},$$

which we recall is holomorphic for  $\Re s > 0$  and has a meromorphic continuation (using integration by parts) to  $\mathbb{C}$  whose poles are contained in  $\mathbb{Z}_{\leq 0}$ . It is a special case of the Fourier transform, but for the multiplicative group of positive reals (hence the Haar measure  $\frac{dx}{x}$ ). Just as with Fourier theory, there is the *Mellin Inversion formula*:

$$p(x) = \frac{1}{2\pi i} \int_{\Re s=2} (Mp)(s) x^{-s} ds.$$

The value of  $\Re s = 2$  here is not so important: we can replace the contour with  $\Re s = c$ , for any  $c > 0$  (using Cauchy's theorem and the fact that  $Mp(s)$  decays rapidly on vertical strips).

Applying Mellin inversion to the Eisenstein series and using (8)-(9), we arrive at the formulas

$$\begin{aligned} \mathcal{E}'_f(g) &= \frac{1}{2\pi i} \int_{\Re s=n+1} (Mp)(s) \cdot 2 \text{Eis}(s, g) ds \\ &= \frac{1}{2\pi i} \int_{\Re s=n+1} (Mp)(s) \zeta(s)^{-1} \text{Eps}(s, g) ds \end{aligned}$$

and

$$\mathcal{E}_f(g) = \frac{1}{2\pi i} \int_{\Re s=n+1} (Mp)(s) \text{Eps}(s, g) ds$$

( $n + 1$  can be replaced with any real number greater than  $n$ , which is the abscissa of absolute convergence of  $\text{Eis}(s, g)$  in  $s$ ).

We close with the following equivalent restatement of the Siegel integration formula (2) and its equivalent form (7):

$$\begin{aligned} \frac{1}{\text{vol}(\Gamma \backslash G)} \int_{\Gamma \backslash G} \frac{1}{2\pi i} \int_{\Re s=n+1} (Mp)(s) \text{Eis}(s, g) ds dg &= \\ \frac{1}{2\zeta(n)} \int_{\mathbb{R}^n} p(\|x\|) dx &= \frac{\sigma(n)}{2\zeta(n)} \int_0^\infty p(x) x^{n-1} dx = \frac{\sigma(n)}{2\zeta(n)} Mp(n), \end{aligned} \tag{10}$$

where  $\sigma(n)$  is the surface area of the  $n - 1$  sphere (coming from the use of radial coordinates in the second to last identity).

## Part III

### 2/21 Lecture

In this lecture we are going to specialize to the case of  $n = 2$ , and give a more analytic proof of Siegel's Integration Formula. The main tool will be the *Maass-Selberg relations*, which gives a formula for the inner product of two Eisenstein series. After seeing the details in this simplest case, we will later generalize to general  $n > 1$ .

Since we are in dimension  $n = 2$ , any unimodular lattice in  $\Lambda \subset \mathbb{R}^2$  (up to rotation) is generated by the two vectors  $y^{-1/2}(1, 0)$  and  $y^{-1/2}(x, y)$  for some  $x \in \mathbb{R}$  and  $y > 0$ . To see this, simply take any basis  $\{v_1, v_2\}$  of  $\mathbb{R}^2$ , ordered so that the counterclockwise angle from  $v_1$  to  $v_2$  lies in the interval  $(0, \pi)$ , and rotate so that  $v_1$  lies on the  $x$ -axis. Then the general lattice vector  $\lambda \in \Lambda$  has squared-length  $\|\lambda\|^2 = y^{-1}|m_1z + m_2|^2$  for some  $m_1, m_2 \in \mathbb{Z}$ , where  $z = x + iy$  lies in the complex upper half plane.

## 8 Non-holomorphic Eisenstein series for $SL(2, \mathbb{Z})$

With this notation, the Epstein Zeta function is

$$\text{Eps}(s, \Lambda) = 2\zeta(s) \text{Eis}(s, \Lambda) = \sum_{\substack{(m_1, m_2) \in \mathbb{Z}^2 \\ (m_1, m_2) \neq (0, 0)}} \frac{y^{s/2}}{|m_1z + m_2|^s}$$

(see (9)). This is a scalar multiple of Siegel's *nonholomorphic Eisenstein series*  $E_{s/2}(z)$ , where

$$E_s(z) := \text{Eis}(2s, \Lambda) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} \Im(\gamma z)^s, \quad (11)$$

where  $\Gamma_\infty$  is subgroup of upper triangular matrices in  $\Gamma = SL(2, \mathbb{Z})$ , i.e., its elements have the form  $\pm \begin{pmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{pmatrix}$ . The cosets in  $\Gamma_\infty \backslash \Gamma$  correspond to matrices with a common bottom row up to sign,  $\begin{pmatrix} * & * \\ c & d \end{pmatrix}$ , i.e.,  $(c, d)$  ranges over all coprime pairs of integers modulo  $\pm 1$ . To verify (11), simply observe that for  $\gamma \in \Gamma$  one has

$$\Im(\gamma z) = \frac{\Im z}{|cz + d|^2} = \frac{y}{|cz + d|^2}.$$

The rest of this lecture is devoted to the main properties of the nonholomorphic Eisenstein series  $E_s(z)$ . The sum (11) is absolutely convergent for  $\Re s > 1$ , and meromorphically continues to  $s \in \mathbb{C}$ . Although the series in (11) only converges for  $\Re s$  sufficiently large,  $E_s(z)$  has a meromorphic continuation to all of  $\mathbb{C}$ , and satisfies a functional equation relating  $s$  and  $1 - s$ . In the  $z$ -variable,  $E(s, z)$  is automorphic under  $\Gamma = \mathrm{SL}(2, \mathbb{Z})$ , and is an eigenfunction of the hyperbolic laplacian  $\Delta = -y^2(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2})$  with eigenvalue  $s(1 - s)$ .

The measure  $\frac{dx dy}{y^2}$  is unique measure (up to constants) on the complex upper half plane  $\mathbb{H}$  which is invariant under translation by  $G = \mathrm{SL}(2, \mathbb{R})$ . The stabilizer of the identity under this action is the maximal compact subgroup  $K = \mathrm{SO}(2) \subset G$ , and so  $\mathbb{H}$  may be identified with the quotient  $G/K$ . We normalize Haar measure on  $K$  to have total volume 1 on this compact group. Since the Eisenstein series are, by construction, right-invariant under  $K$  (this is because norms are rotation invariant), we may rewrite formula (10) as

$$\frac{1}{2\pi i} \int_{\Re s=3} (Mp)(s) \int_{\mathcal{F}} E_{s/2}(x + iy) \frac{dx dy}{y^2} ds = \frac{6}{\pi} \mathrm{vol}(\mathcal{F})(Mp)(2), \quad (12)$$

where  $\mathcal{F}$  is a fundamental domain for  $\Gamma \backslash \mathbb{H}$  and we have used the facts that  $\sigma(2) = 2\pi$  and  $\zeta(2) = \frac{\pi^2}{6}$ . In fact,  $\mathrm{vol}(\mathcal{F}) = \pi/3$  as we shall shortly see as an example of the following machinery we develop in order to prove (12).

## 9 The Maass-Selberg Relations for $SL(2)$

The inner product of two  $\Gamma$ -automorphic functions  $f$  and  $g$  on  $\mathbb{H}$  is given by

$$\int_{\Gamma \backslash \mathbb{H}} f \bar{g} \frac{dx dy}{y^2}. \quad (13)$$

Roughly speaking, the *Maass-Selberg relations* computes the inner product of two Eisenstein series  $E(s_1, z)$  and  $E(s_2, z)$ . The reason we say “roughly” is that when  $f$  and  $g$  are both Eisenstein series  $E_{s_1}$  and  $E_{s_2}$ , the integral in (13) actually diverges aside from certain highly-special cases (e.g., both  $s_1 = s_2 = 0$ ). One way to understand this is to write  $E(s, x + iy)$  as a Fourier series in  $x$ . The constant term in this expansion is

$$c(y, s) = \int_0^1 E_s(x + iy) dx = y^s + \varphi(s) y^{1-s}, \quad (14)$$

where  $\varphi(s) = \xi(2s - 1)/\xi(2s)$  and

$$\xi(s) = \pi^{-s/2} \Gamma(s/2) \zeta(s) = \xi(1 - s) \quad (15)$$

is the completed Riemann  $\zeta$ -function. The important facts about  $\varphi$  here are that it has a pole at  $s = 1$  and a zero at  $s = 0$ . We will not derive this formula, but we will explain its form: the  $y^s$  term comes from the identity coset in the sum (11), and the  $y^{1-s}$  term must be there as well because of the functional equation relating  $E(s, z)$  and  $E(1 - s, z)$ . The functions  $y^s$  and  $y^{1-s}$  are in fact the only two power functions of  $y$  which are eigenvalues of  $\Delta$  (aside from the degenerate case of  $s = 1/2$ , when the latter must be replaced by  $y^{1/2} \log(y)$ ).

Note that when  $s = 0$ , we have  $\phi(0) = 0$  and hence  $c(0, y) = 1$  – in fact  $E(0, z)$  is the constant function 1 (as it must be, since its eigenvalue under  $\Delta$  is 0, making it harmonic). Alternatively, the residue of  $E_s(z)$  at  $s = 1$  is constant. For values of  $s \neq 0$  it is not hard to see that the constant term does not decay fast enough as  $y \rightarrow \infty$  for the integral in (13) to converge (the Riemann-Lebesgue Lemma shows that the non-constant terms cannot compete with it in size, which is entirely analogous to the fact that cusp forms decay rapidly).

Because of the divergence in (13), a *truncation operator* defined as follows. Given a large parameter  $C > 1$ , decompose the fundamental domain  $\mathcal{F}$  for  $\Gamma \backslash \mathbb{H}$  as the union of

$$\mathcal{F}^{>C} = \{z \in \mathcal{F}, \Im z > C\} \quad \text{and} \quad \mathcal{F}^{\leq C} = \{z \in \mathcal{F}, \Im z \leq C\},$$

and define the truncation by subtracting the constant term when  $z \in \mathcal{F}^{>C}$ :

$$(\Lambda^C E_s)(z) = \begin{cases} E_s(z) & \text{if } \Im z \leq C \\ E_s(z) - c(y, s) & \text{if } \Im z > C \end{cases}, \quad (z \in \mathcal{F}).$$

The idea here is that the constant term  $c(s, y)$  is the reason (13) does not converge for  $y$  large, so we just subtract off that term when  $y$  is large. For this reason, Langlands titled his chapter on more-general truncation operators “ $L^2(\Gamma \backslash G)$  as the bed of Procrustes” (cf. p.109b of the Babylonian Talmud’s Tractate Sanhedrin).

The *Maass-Selberg relations* state

$$\begin{aligned} \int_{\mathcal{F}} (\Lambda^C E_{s_1})(z) (\Lambda^C E_{s_2})(z) \frac{dx dy}{y^2} &= \int_{\mathcal{F}} (\Lambda^C E_{s_1})(z) E_{s_2}(z) \frac{dx dy}{y^2} \quad (16) \\ &= \frac{C^{s_2+s_1-1}}{s_2+s_1-1} + \varphi(s_2) \frac{C^{s_1-s_2}}{s_1-s_2} + \varphi(s_1) \frac{C^{s_2-s_1}}{s_2-s_1} + \varphi(s_1)\varphi(s_2) \frac{C^{1-s_2-s_1}}{1-s_2-s_1}. \end{aligned} \quad (17)$$

Equation (16) says we only need to truncate one of the Eisenstein series (that is,  $\Lambda^C$  is a self-adjoint operator under the  $L^2$  inner product), and equation (17) evaluates both integrals in (16).

## 10 Applications of Maass-Selberg

Before proving the Maass-Selberg relations, we give two applications. The first is a warm-up, and the second is the proof of the Siegel Integral Formula (12) in dimension  $n = 2$ .

For our first application (alluded to after (12)) we derive that  $\text{vol}(\mathcal{F}) = \pi/3$  under the Haar measure  $\frac{dx dy}{y^2}$ . We take  $s_1 = s$  and  $s_2 = 0$ . Then  $E_{s_2} = 1$ ,  $\phi(s_2) = 0$ , and (17) tells us that

$$\int_{\mathcal{F}} (\Lambda^C E_s)(z) \frac{dx dy}{y^2} = \frac{C^{s-1}}{s-1} - \varphi(s) \frac{C^{-s}}{s}. \quad (18)$$

Next we take  $s \rightarrow 0$ . On the left side, the integrand approaches the characteristic function of  $\mathcal{F}^{\leq C}$ , while the right side approaches  $-C^{-1} + \pi/3$  using the facts that  $\xi(s) = \xi(1-s)$  has a simple pole with residue 1 at  $s = 1$ , and  $\xi(-1) = \xi(2) = \pi^{-1}\zeta(2) = \frac{\pi}{6}$ . Thus  $\text{vol}(\mathcal{F}^{\leq C}) = \frac{\pi}{3} - \frac{1}{C}$ , which is not hard to directly verify under the measure  $\frac{dx dy}{y^2}$  using a simple trigonometric substitution. Finally, taking  $C \rightarrow \infty$ , we derive that  $\text{vol}(\mathcal{F}) = \pi/3$ . This proof was generalized by Langlands in much wider generality.

For our second application, we use the Maass-Selberg relations to prove the dimension  $n = 2$  case of the Siegel Integration Formula (12). First, we truncate the Eisenstein Series:

$$\frac{1}{2\pi i} \int_{\Re s=3} \int_{\mathcal{F}} Mp(s)(\Lambda^C E_{s/2})(z) \frac{dx dy}{y^2} ds$$

If we reverse the order of integration – which is valid since we are in the range of absolute convergence – and then take the limit as  $C \rightarrow \infty$ , then we recover the left hand side of (12). On the other hand, inserting (18) gives

$$\frac{1}{2\pi i} \int_{\Re s=3} Mp(s) \left( \frac{C^{s/2-1}}{s/2-1} - \varphi(s/2) \frac{C^{-s/2}}{s/2} \right) ds.$$

The contribution of the second term (involving  $C^{-s/2}$ ) vanishes in the  $C \rightarrow \infty$  limit, hence we need only consider the first term. Shifting contours to the left picks up a residue of  $2Mp(2)$  from the pole at  $s = 2$  of the first term; if one moves the contour to  $\Re s = 3/2$ , say, the remaining integral contributes  $O(C^{-1/4})$  and tends to zero in the  $C \rightarrow \infty$  limit. By our first application computing  $\text{vol}(\mathcal{F}) = \frac{\pi}{3}$ , we see that  $2Mp(2)$  is also the right-hand side of (12) as was to be shown.

## 11 Proof of the Maass-Selberg relations for $n = 2$

This proof is taken from the exposition in Miller, 2001, “On the existence and temperedness of cusp forms for  $\text{SL}(3, \mathbb{Z})$ ,” page 16, and is Selberg’s proof of the Maass-Selberg’s relation. Maass’ proof used Green’s Theorem.

We demonstrate the first equality in the Maass-Selberg relation (16) by showing that

$$\int_{\mathcal{F}} (\Lambda^C E_{s_1})(z) \left( E_{s_2}(z) - (\Lambda^C E_{s_2})(z) \right) \frac{dx dy}{y^2} = 0,$$

that is,

$$\int_{\mathcal{F}^{\geq C}} (\Lambda^C E_{s_1})(z) c(y, s_2) \frac{dx dy}{y^2} = 0.$$

Now, since  $C$  is large  $\mathcal{F}^{\geq C}$  is a rectangle, and so we can integrate first in  $x$  to get

$$\int_C^\infty \left( \int_0^1 \Lambda^C E_{s_1}(z) dx \right) c(y, s_2) \frac{dy}{y^2} = \int_C^\infty (c(y, s_1) - c(y, s_1)) c(y, s_2) \frac{dy}{y^2} = 0.$$

This shows the power of the truncation definition. A more naive definition would have completely (*ala* Procrustes and Sdom) chopped off the function

to have zero support above  $\Im(z) = C$ . Instead, merely its constant term is subtracted. The result actually decays very quickly so is still integrable, and yet satisfies the above easy calculation. Put differently, the truncation operator  $\Lambda^C$  subtracts only what needs to be subtracted.

To prove the second equality (17), we first introduce the notation

$$\delta_C(z) = \begin{cases} 0 & \text{if } \Im z \leq C \\ 1 & \text{if } \Im z > C. \end{cases}$$

Now for  $z \in \mathcal{F}$  we may write

$$(\Lambda^C E_s)(z) = E_s(z) - \delta_C(z) c(y, s) = \sum_{\gamma \in \Gamma_\infty \setminus \Gamma} \left( \Im(\gamma z)^s - \underbrace{\delta_C(\gamma z) c(\Im(\gamma z), s)}_{\text{zero unless } \gamma \in \Gamma_\infty} \right)$$

since  $C \gg 1$ . Note that the formula on the right defines a  $\Gamma$ -automorphic function on  $\mathbb{H}$ , and is presented in a form which makes it useful to unfold. Since  $E_{s_2}(z)$  is automorphic in the  $z$ -variable, we find

$$(\Lambda^C E_{s_1})(z) E_{s_2}(z) = \sum_{\gamma \in \Gamma_\infty \setminus \Gamma} \left( \Im(\gamma z)^s - \delta_C(\gamma z) c(\Im(\gamma z), s) \right) E_{s_2}(\gamma z),$$

and this last function's integral over  $z = x + iy \in \Gamma \setminus \mathbb{H}$  is

$$\begin{aligned} & \int_{\Gamma_\infty \setminus \mathbb{H}} \left( \Im(z)^s - \delta_C(z) c(\Im(z), s) \right) E_{s_2}(z) \frac{dx dy}{y^2} \\ &= \int_0^\infty \left( y^{s_1} - \delta_C(y) c(y, s_1) \right) \int_0^1 E_{s_2}(z) dx \frac{dy}{y^2} \\ &= \int_0^\infty \left( y^{s_1} - \delta_C(y) c(y, s_1) \right) c(y, s_2) \frac{dy}{y^2} \\ &= \int_0^C y^{s_1} c(y, s_2) \frac{dy}{y^2} - \phi(s_1) \int_C^\infty y^{1-s_1} c(y, s_2) \frac{dy}{y^2} \end{aligned}$$

Now we plug in the formula for  $c(y, s)$  and integrate term-by-term. The desired formula pops out, but some care must be taken for which range of  $s_1$  and  $s_2$  the above argument is valid. For instance, it is sufficient to first assume that  $\Re(s_1) > \Re(s_2) > 1$ , and then derive the final formula by meromorphic continuation to  $\mathbb{C} \times \mathbb{C}$ .

## Part IV

### 2/25 Lecture

We now turn to proving the Siegel integration formula (10) for general  $n > 1$ , after having done the  $n = 2$  case as a warmup. We first start with the right-hand side, which is considerably easier. Until now we have not calculated the surface area  $\sigma(n)$  of the unit sphere in  $\mathbb{R}^n$ :

**Lemma.** *The unit ball in  $\mathbb{R}^n$  has volume  $\frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)}$  and surface area  $\sigma(n) = 2\frac{\pi^{n/2}}{\Gamma(\frac{n}{2})}$ .*

*Proof.* Let  $p(r) = e^{-\pi r^2}$ ,  $f(x) = p(\|x\|)$ , and  $I = \int_{\mathbb{R}^n} p(x) dx$ . Splitting variables and polar coordinates as in (10) shows that

$$I^n = \int_{\mathbb{R}^n} f(x) dx = \sigma(n) \int_0^\infty p(r) r^{n-1} dr.$$

When  $n = 2$ ,  $\sigma(2) = 2\pi$  and

$$I^2 = \int_0^\infty e^{-\pi r^2} \cdot 2\pi r dr = -e^{-\pi r^2} \Big|_0^\infty = 1,$$

which is the famous calculation of the Gaussian integral: that the positive constant  $I$  is equal to 1. For general  $n > 1$  the change of variables  $r = \sqrt{u}$  shows that

$$\sigma(n)^{-1} = \int_0^\infty e^{-\pi r^2} r^{n-1} dr = \frac{1}{2} \int_0^\infty e^{-\pi u} u^{n/2-1} du = \frac{\pi^{-n/2}}{2} \Gamma(n/2).$$

The volume of ball of radius  $r$  is  $r^n$  times the asserted formula for the unit ball, so that by differentiation the surface area of the unit ball  $\sigma(n)$  is  $n$  times the volume of the unit ball, completing the proof.  $\square$

Therefore the right-hand side of (10) is equal to

$$\text{RHS (10)} = \frac{1}{\xi(n)} Mp(n) \tag{19}$$

using (15). Note that  $\pi^{-n/2}\Gamma(n/2)$  is so-called “archimedean” contribution to this last formula (i.e., the part that comes from real analysis without any influence of the lattice itself) merges nicely with the “arithmetic” part (the value of  $\zeta(n)$ , which takes into account the relatively prime condition). We can now restate (10) as

$$\frac{1}{2\pi i} \int_{\Gamma \backslash G} \int_{\Re s = n+1} Mp(s) \text{Eis}(s, g) ds dg = \frac{\text{vol}(\Gamma \backslash G)}{\xi(n)} Mp(n). \quad (20)$$

Note that we haven’t specified the Haar measure  $dg$ , nor do we need to: it scales with the volume on the right-hand side.

## 12 Borel Eisenstein Series on $SL(n, \mathbb{R})$

In this section we will introduce a different type of Eisenstein series, which has the virtue of extra flexibility in computing inner products and fortunately subsumes  $\text{Eis}(\cdot)$  as a special case.

Let  $A$  be the set of diagonal matrices in  $SL(n, \mathbb{R})$ . Writing a matrix  $a \in A$  as  $\text{diag}(a_1, \dots, a_n)$ , with  $a_1 a_2 \cdots a_n = 1$ , let  $h$  denote the diagonal matrix  $\text{diag}(h_1, \dots, h_n)$ , with  $h_j = \log(a_j)$  and  $h_1 + \cdots + h_n = 0$ . Then  $a$  is equal to the matrix exponential  $\exp(h)$ , which provides an isomorphism between  $\mathfrak{a} := \{ \text{the hyperplane in } \mathbb{R}^n \text{ whose coordinates sum to zero} \}$  and  $A$ .

We introduce some notation from Lie theory, specialized to this situation. Let  $\mathfrak{a}^*$  denote the (real) linear dual of  $\mathfrak{a}$ , that is, its space of real-valued linear functionals. Each linear function  $\lambda \in \mathfrak{a}^*$  can be written as an  $n$ -tuple  $(\lambda_1, \dots, \lambda_n)$  so that its action on  $h \in \mathfrak{a}$  is given by  $\lambda_1 h_1 + \cdots + \lambda_n h_n$ . Since  $h_1 + \cdots + h_n = 0$ , adding a fixed constant to each coordinate of that  $n$ -tuple results in the same linear functional, so that  $\mathfrak{a}^*$  is in fact isomorphic to the quotient of  $\mathbb{R}^n$  by span of the vector  $(1, 1, \dots, 1)$ . A very important element of  $\mathfrak{a}^*$  is the linear functional

$$\rho = \text{the coset of } (n, n-1, \dots, 1) \text{ modulo } (1, 1, \dots, 1). \quad (21)$$

Linear functionals  $\lambda \in \mathfrak{a}^*$  of course give rise to characters of  $A$  by the formula

$$a^\lambda = \exp(h)^\lambda = \exp(\lambda(h)) = a_1^{\lambda_1} a_2^{\lambda_2} \cdots a_n^{\lambda_n},$$

where  $a = \exp(h)$ .

## 12.1 Borel Eisenstein Series

Let  $B$  denote the set of upper triangular matrices in  $GL(n, \mathbb{R})$ ,  $N$  the set of upper triangular matrices with diagonal entries 1, and  $K = SO(n)$ . We have the Iwasawa decomposition  $G = N \times A \times K$  with uniqueness of expression. Furthermore  $B$ 's connected component of the identity (i.e., upper triangular matrices with positive diagonal entries) is equal to  $N \times A$ , again with uniqueness of expression. Since  $A$  normalizes  $N$  the map  $a^\lambda$  defined above extends to a character of  $B$ , by defining it to be trivial on diagonal matrices in  $\Gamma = SL(n, \mathbb{Z})$  (which consists of diagonal matrices with  $\pm 1$  entries on the diagonal and determinant 1). Given an element of  $g$  we thus have the well-defined function  $a(g)^\lambda$ , where  $a(g)$  is its  $A$ -component in the Iwasawa decomposition

The Borel (or “minimal parabolic”) Eisenstein series is defined using a shift by  $\rho$  as

$$E(g, \lambda) = \sum_{\gamma \in (\Gamma \cap B) \backslash \Gamma} a(\gamma g)^{\lambda + \rho}. \quad (22)$$

The sum as written above is absolutely convergent if  $\lambda$  is “a little bit bigger” than  $\rho$ , in the sense we now make precise. Let  $\mu = \lambda - \rho$ , and write  $\mu = (\mu_1, \dots, \mu_n)$ . The condition for absolute convergence is that  $\mu_j > \mu_{j+1}$  for each  $j = 1, \dots, n - 1$ ; in this case one calls  $\mu$  *strictly dominant*. In terms of  $\lambda = (\lambda_1, \dots, \lambda_n)$ , this condition is that  $\lambda_j > \lambda_j + 1$  for each  $1 \leq j < n$ . In fact,  $\lambda$  can be taken to be complex (meaning that  $\lambda_j \in \mathbb{C}$ ), in which the convergence condition is that its real part satisfies this dominance condition:

$$\Re \lambda_j > \Re \lambda_{j+1} + 1, \quad 1 \leq j < n. \quad (23)$$

This range of absolute convergence is known as the *Godement range* and is very natural. For  $n = 2$  it specializes to the fact that  $E_s$  from (11) is absolutely convergent in the range  $\Re s > 1$ . This is best possible, for we shall see that  $E(g, \lambda)$  has a pole at  $\lambda = \rho$ .

We sketch a proof of Godement’s proof of the absolute convergence. First, one argues that if  $g$  is translated on the right by a tiny perturbation of the identity (so that  $g$  is replaced by matrices  $gh$  with  $h$  lying in a fixed open subset  $\mathcal{O}$  of the identity), then  $a(\gamma gh)a(\gamma g)^{-1}$  lies in a fixed neighborhood of the identity – independently of  $\gamma \in \Gamma$  and  $g \in G$ . To see this, write  $\gamma g = nak$  in Iwasawa form, where  $a = a(\gamma g)$ . The claim follows from the

fact that multiplication on the right by  $h$  is continuous on each of the three Iwasawa factors.

Therefore absolute convergence of the sum in (22) would follow from showing the absolute convergence of the combined sum and integral of  $a(\gamma gh)^{\lambda+\rho}$ , over all  $\gamma \in (\Gamma \cap B) \backslash \Gamma$  and  $h$  in a small open set. The latter integral is equivalently the integral of  $a(x)^{\lambda+\rho}$  over the  $(\Gamma \cap B) \backslash \Gamma$ -translates of  $g\mathcal{O}$ . By definition of  $\Gamma$  being a discrete group, these translates are disjoint (provided  $\mathcal{O}$  is sufficiently small); hence the integral is bounded above by that of  $a(x)^{\lambda+\rho}$  over all  $x \in (\Gamma \cap B) \backslash G$ , which itself reduces to the convergence of the integral of  $a^{\lambda+\rho}$  over  $A$ . This last integral is an easy calculation using explicit formulas for Haar measure.

## 12.2 Langlands' constant term formula

Let

$$c(s) = \phi\left(\frac{s}{2} + 1\right) = \frac{\xi(s)}{\xi(1+s)} = \frac{\xi(1-s)}{\xi(1+s)},$$

e.g.,  $c(s)$  vanishes to first order at  $s = 0$ . For each pair of distinct integers  $i$  and  $j$  from 1 to  $n$ , let  $\alpha_{i,j}$  denote the element of  $\mathfrak{a}^*$  defined by the difference of elementary basis vectors  $e_i - e_j$ . These are known as *roots*, and those with  $i < j$  are deemed *positive* roots. Let  $\Delta = \Delta_+ \sqcup \Delta_-$  denote the set of all roots, with  $\Delta_+$  denoting the positive roots and  $\Delta_- = -\Delta_+$  the negative roots. For brevity sometimes we use the notation  $\alpha > 0$  to indicate  $\alpha \in \Delta_+$ , and  $\alpha < 0$  to indicate  $\alpha \in \Delta_-$ . We write  $\langle \lambda, \alpha_{i,j} \rangle = \lambda_i - \lambda_j$  for  $\lambda = (\lambda_1, \dots, \lambda_n) \in \mathfrak{a}^*$ . Since  $\Delta$  spans  $\mathfrak{a}^*$  this extends to a pairing on  $\mathfrak{a}^* \times \mathfrak{a}^*$ .<sup>6</sup> Let  $\Sigma \subset \Delta_+$  denote the *simple roots*, which are those satisfying  $j - i = 1$ . Every positive root is a nonnegative integral combination of simple roots.

Langlands' constant term formula states that

$$\int_{(\Gamma \cap N) \backslash N} E(ng, \gamma) dn = \sum_{w \in W} a^{w\lambda+\rho} M(w, \lambda), \quad (24)$$

---

<sup>6</sup>If coset representatives  $\lambda = (\lambda_1, \dots, \lambda_n)$  and  $\mu = (\mu_1, \dots, \mu_n)$  have entries summing to zero, then this pairing is given by  $\langle \lambda, \mu \rangle = \lambda_1 \mu_1 + \dots + \lambda_n \mu_n$ . The formula remains valid if only one of  $\lambda$  or  $\mu$  has entries summing to zero.

where the Weyl group  $W$  is the permutation group on entries of  $\lambda$ , and

$$M(w, \lambda) = \prod_{\substack{\alpha > 0 \\ w\alpha < 0}} c(\langle \lambda, \alpha \rangle). \quad (25)$$

For example, if  $\lambda = -\rho = (-n, -n + 1, \dots, -2, -1)$  modulo  $(1, 1, \dots, 1)$ , then  $\langle \lambda, \alpha_{i,j} \rangle = i - j < 0$ . In particular none of the factors in (25) has a pole. If  $w\alpha_{i,j} < 0$  and  $j = i + 1$  (i.e.,  $\alpha_{i,j} \in \Sigma$ ), then  $c(\langle -\rho, \alpha_{i,j} \rangle) = c(-1) = 0$  and hence  $M(w, -\rho) = 0$ . Thus the contribution to the constant term vanishes for any  $w \in W$  which “flips“ the sign of a simple root  $\alpha_{i,i+1}$ . In fact every nontrivial  $w \in W$  flips some simple root, for otherwise  $w$  would flip the sign of no positive root and could only be trivial. We conclude that only  $w = e$  contributes to the sum  $\sum_{w \in W} a^{-w\rho + \rho} M(w, -\rho)$ : the constant term is simply  $a^{-\rho + \rho} = 1$ , and in fact the annihilated-by- $\Delta$ -hence-constant function  $E(\cdot, -\rho) \equiv 1$ .

### 13 The Maass-Selberg relations for $SL(n)$

Though it admittedly has a complicated description, there are truncation operators  $\Lambda^C$  for higher rank groups which were introduced by Langlands, indexed by matrices  $C \in A$  whose diagonal entries are in decreasing order. They are self-adjoint as in the  $n = 2$  case (16), and satisfy the following generalization of (17):

$$\int_{\Gamma \backslash G} (\Lambda^C E)(g, \lambda_1) E(g, \lambda_2) dg = \sum_{w_1, w_2 \in W} \frac{C^{w_1 \lambda_1 + w_2 \lambda_2}}{\prod_{\alpha \in \Sigma} \langle w_1 \lambda_1 + w_2 \lambda_2, \alpha \rangle} M(w_1, \lambda_1) M(w_2, \lambda_2), \quad (26)$$

where  $M(w, \lambda)$  is defined above in (25). Letting  $\lambda_2 = -\rho$  and using the fact above that  $M(w_2, -\rho)$  vanishes unless  $w_2 = e$ , it again implies

$$\int_{\Gamma \backslash G} (\Lambda^C E)(g, \lambda) dg = \sum_{w \in W} \frac{C^{w\lambda - \rho}}{\prod_{\alpha \in \Sigma} \langle w\lambda - \rho, \alpha \rangle} M(w, \lambda). \quad (27)$$

Applying the truncation operator  $\Lambda^C$  to the constant function results in the characteristic function of a truncated fundamental domain. By self-adjointness, (27) is also equal to the integral of  $E(g, \lambda)$  over a truncated fundamental domain for  $\Gamma \backslash G$ .

## Part V

### 2/28 Lecture

#### 14 Application of Maass-Selberg to $\text{vol}(\Gamma \backslash G)$

**Theorem.**  $\text{vol}(\Gamma \backslash G) = \xi(2)\xi(3)\cdots\xi(n)$ , where  $\xi(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$ .

This is classical; we will give a proof due to Langlands. To prove the theorem, we need a lemma.

**Lemma.**  $\lim_{\varepsilon \rightarrow 0} \frac{-c(-1+\varepsilon)}{\varepsilon} = \xi(2) = \frac{\pi}{6}$ .

*Proof of the lemma.* Note that  $c(s) = \frac{1}{c(-s)}$ . So

$$\lim_{\varepsilon \rightarrow 0} \frac{-c(-1+\varepsilon)}{\varepsilon} = \frac{1}{(-\varepsilon)c(1-\varepsilon)} = \lim_{\varepsilon \rightarrow 0} \frac{1}{\varepsilon c(1+\varepsilon)} = \lim_{\varepsilon \rightarrow 0} \frac{1}{\varepsilon} \frac{\xi(2+\varepsilon)}{\xi(1+\varepsilon)} = \xi(2),$$

since  $\zeta(s)$  has a simple pole with residue 1 at  $s = 1$ , hence so does  $\xi(s)$ .<sup>7</sup> The proof follows since  $\xi(2) = \pi^{-1} \cdot \frac{\pi^2}{6} = \frac{\pi}{6}$ .  $\square$

*Proof of the volume formula.* We start with (27) with  $\lambda = (\varepsilon - 1)\rho$ , with  $\varepsilon > 0$  small, and

$$C = \begin{pmatrix} T^{\frac{n-1}{2}} & & & 0 \\ & T^{\frac{n-3}{2}} & & \\ & & \ddots & \\ 0 & & & T^{\frac{1-n}{2}} \end{pmatrix}, \quad (28)$$

with  $T > 0$  large. Note that the powers of  $T$  here differ by  $\frac{n+1}{2}$  from the vector entries in (21). The proof will involve taking  $\varepsilon \rightarrow 0$  to get a formula for the volume of the truncated fundamental domain, and then taking  $T \rightarrow \infty$  to complete the calculation.

For  $\varepsilon$  sufficiently small and  $T$  sufficiently large, the right-hand side of (27) contains various powers of  $T$ . In more detail,  $C^{w\lambda-\rho} = T^{\langle \rho, w\lambda-\rho \rangle}$  in terms

---

<sup>7</sup>This uses the fact that  $\Gamma(\frac{1}{2}) = \sqrt{\pi}$ , which is the calculation of the Gaussian integral.

of the pairing  $\langle \cdot, \cdot \rangle$ . The numbers  $\langle \rho, w\lambda - \rho \rangle$  are small perturbations of the  $\varepsilon = 0$  case

$$-\langle \rho, w\rho + \rho \rangle = -\langle \rho, \rho \rangle - \langle \rho, w\rho \rangle.$$

By Cauchy-Schwarz this last expression is non-positive, and equals zero precisely when  $w = w_{\text{long}}$ , the permutation that reverses everything (since  $w_{\text{long}}\rho = -\rho$  is the only nontrivial Weyl translate of  $\rho$  collinear to  $\rho$ ). The upshot of this standard fact in Lie theory is that the  $w = w_{\text{long}}$  term dominates all the others on the right-hand side of (27); the other terms give (precise) sub-leading contributions (which are details not needed to prove the volume formula, and hence shall be disregarded).

Since  $w_{\text{long}}\rho = -\rho$  and  $w_{\text{long}}\lambda - \rho = -\varepsilon\rho$ , the main term in our application of (27) is

$$T^{-\varepsilon\langle \rho, \rho \rangle} \frac{M(w_{\text{long}}, (\varepsilon - 1)\rho)}{\prod_{\alpha \in \Sigma} \langle -\varepsilon\rho, \alpha \rangle} = T^{-\varepsilon\langle \rho, \rho \rangle} \frac{\prod_{1 \leq i < j \leq n} c((\varepsilon - 1)\langle \rho, \alpha_{i,j} \rangle)}{\prod_{1 \leq j < n} \langle -\varepsilon\rho, \alpha_{j,j+1} \rangle}.$$

The pairing  $\langle \rho, \alpha_{i,j} \rangle = j - i$ , so the power of  $T$  as well as the factors in the numerator with  $j > i + 1$  have well-defined limits as  $\varepsilon \rightarrow 0$ . The factors in the numerator with  $j = i + 1$  vanish at  $\varepsilon = 0$  to first order, as do each of the factors in the denominator. The limiting ratio of these two expressions is calculated in the above Lemma. Hence

$$\begin{aligned} \lim_{\varepsilon \rightarrow 0} T^{-\varepsilon\langle \rho, \rho \rangle} \frac{M(w_{\text{long}}, (\varepsilon - 1)\rho)}{\prod_{\alpha \in \Sigma} \langle -\varepsilon\rho, \alpha \rangle} &= \xi(2)^{n-1} \prod_{\substack{i,j \leq n \\ i < j-1}} \frac{\xi(i-j)}{\xi(i-j+1)} \\ &= \xi(2)^{n-1} \prod_{\substack{i,j \leq n \\ i < j-1}} \frac{\xi(1+j-i)}{\xi(j-i)} \\ &= \xi(2)^{n-1} \prod_{k=2}^{n-1} \left( \frac{\xi(k+1)}{\xi(k)} \right)^{n-k} \\ &= \xi(2) \xi(3) \cdots \xi(n), \end{aligned}$$

after collapsing the telescoping product. □

## 15 Second proof of the Siegel Integration Formula

We now return to our main theme, trying to prove Siegel's integration formulation via its equivalence

$$\begin{aligned} \frac{1}{2\pi i} \int_{\Gamma \backslash G} \int_{\Re s = n+1} Mp(s) \text{Eis}(s, g) ds dg &= \frac{\text{vol}(\Gamma \backslash G)}{\xi(n)} Mp(n) \\ &= \xi(2) \xi(3) \cdots \xi(n-1) Mp(n) \end{aligned} \tag{29}$$

(notice amidst the metamorphosis from (20) how cleanly the factor  $\zeta(n)$  from the relatively-prime condition, which became  $\xi(n)$  after the surface area calculation, fits with the volume formula.)

In order to use the Maass-Selberg relations for the Borel Eisenstein series (22), we will relate

$$\text{Eis}(s, g) = \sum_{\gamma \in (\Gamma \cap P) \backslash \Gamma} \|e_n \gamma g\|^{-s} \tag{30}$$

(see (9)) to

$$E(g, \lambda) = \sum_{\gamma \in (\Gamma \cap B) \backslash \Gamma} a(\gamma g)^{\lambda + \rho} \tag{31}$$

for certain  $\lambda$ . The summands are different, and the parabolics defining the ranges of summation are different (recall that  $P$  is the mirabolic subgroup of  $G = SL(n, \mathbb{R})$ , characterized by the first  $n-1$  entries of its bottom row vanishing).

Factor  $\gamma$  in (31) as  $\gamma = \gamma_1 \gamma_2$ , where  $\gamma_1$  ranges over coset representatives for  $(\Gamma \cap B) \backslash (\Gamma \cap P)$  and  $\gamma_2$  ranges over coset representatives for  $(\Gamma \cap P) \backslash \Gamma$  (noting that  $B \subset P$ ). Then in the range of absolute convergence (23) we may write

$$E(g, \lambda) = \sum_{\gamma_2 \in (\Gamma \cap P) \backslash \Gamma} E_{n-1}(\gamma_2 g, \lambda),$$

where

$$E_{n-1}(g, \lambda) = \sum_{\gamma_1 \in (\Gamma \cap B) \backslash (\Gamma \cap P)} a(\gamma_1 g)^{\lambda + \rho} \tag{32}$$

will be seen to essentially equal an  $SL(n-1)$  Borel Eisenstein series. Our strategy to match (30) to (31) will be to find a value of  $\lambda$  so that  $E_{n-1}(g, \lambda) = \|e_n \gamma g\|^{-s}$ . This  $\lambda$  will be outside the Godement range of absolute convergence, but nevertheless the equality will make sense by meromorphic continuation.

To wit, decompose

$$\lambda + \rho = (\lambda_1 + n, \lambda_2 + n - 1, \dots, \lambda_{n-1} + 2, 0) + (0, \dots, 0, \lambda_n + 1);$$

as before this represents a coset representative modulo multiples of the constant vector  $(1, 1, \dots, 1)$ . Let's consider  $a^{\lambda+\rho}$  for a diagonal matrix  $a$  with positive entries  $a_1, a_2, \dots, a_n$  which multiply to 1 (so that the failure of the entries of  $\lambda + \rho$  to sum to zero is not a problem):

$$a^{\lambda+\rho} = a_1^{\lambda_1+n} a_2^{\lambda_2+n-1} \dots a_{n-1}^{\lambda_{n-1}+2} a_n^{\lambda_n+1}.$$

The entry  $a_n$  is important to us, since if  $g$  is written in Iwasawa form as  $g = nak$ , then

$$\|e_n g\| = \|e_n n a k\| = \|e_n a k\| = \|e_n a\| = a_n$$

since the norm is invariant under rotation by elements  $k \in K = SO(n)$ . This motivates defining a particular choice of  $\lambda = \lambda(s)$  by setting  $\lambda_n = -s - 1$  and  $\lambda_j = -n - 1 + j$  for  $1 \leq j < n$ :

$$\lambda(s) = (-n, -n + 1, -n + 2, \dots, -3, -2, -s - 1). \quad (33)$$

Thus  $\lambda_j - \lambda_{j+1}$  is  $-1$  for  $1 \leq j < n - 1$ , and  $\lambda_{n-1} - \lambda_n = s - 1$ .

Next we use the results of the preceding paragraph to analyze  $a(\gamma_1 g)$  as  $\gamma_1$  ranges over cosets representatives for  $(\Gamma \cap B) \backslash (\Gamma \cap P)$ . The matrix  $\gamma_1$  lies in  $P$ , and so can be written as  $um$ , where  $u \in \Gamma$  is equal to  $I_n$  plus a matrix with nonzero entries only in the top  $n-1$  entries of its rightmost column, and  $m \in \Gamma$  has block form  $(n-1, 1)$ . The matrix  $u$  also belongs to  $\Gamma \cap B$ . Since  $\Gamma \cap B$  includes diagonal matrices with  $-1$  as their last entry, cosets for  $(\Gamma \cap B) \backslash (\Gamma \cap P)$  are in bijective correspondence with  $(\Gamma_{n-1} \cap B_{n-1}) \backslash \Gamma_{n-1}$ , where  $\Gamma_{n-1} = SL(n-1, \mathbb{Z})$  and  $B_{n-1} \subset SL(n-1, \mathbb{R})$  is the latter's subgroup of upper triangular matrices. Thus we may take the coset representative  $\gamma_1$

to have the form  $\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}$ , with  $\delta \in \Gamma_{n-1}$ . We may likewise factor  $g \in G$  in its Iwasawa form as

$$g = \begin{pmatrix} I_{n-1} & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} g_{n-1} & 0 \\ 0 & \Delta \end{pmatrix} k,$$

where  $u \in \mathbb{R}^{n-1}$ ,  $g_{n-1} \in GL(n-1, \mathbb{R})$ ,  $\Delta = \det(g_{n-1})^{-1}$ , and  $k \in SO(n)$ . Then

$$\begin{aligned} \gamma_1 g &= \begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} I_{n-1} & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} g_{n-1} & 0 \\ 0 & \Delta \end{pmatrix} k \\ &= \begin{pmatrix} I_{n-1} & \delta u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \delta g_{n-1} & 0 \\ 0 & \Delta \end{pmatrix} k. \end{aligned} \tag{34}$$

If  $a_{n-1}(\delta g_{n-1})$  denotes the  $A$ -component of the Iwasawa decomposition of  $\delta g_{n-1}$  for  $SL(n-1, \mathbb{R})$ , then  $a(\gamma_1 g) = \begin{pmatrix} a_{n-1}(\delta g_{n-1}) & 0 \\ 0 & \Delta \end{pmatrix}$  and we may write

$$a(\gamma_1 g)^{\lambda+\rho} = a_{n-1}(\delta g_{n-1})^{(\lambda_1+n, \lambda_2+n-1, \dots, \lambda_{n-1}+2, 0)} \Delta^{\lambda_{n+1}}.$$

The last factor is independent of  $\delta$ , and the key point of this calculation is that it is now apparent that (32) equals  $\Delta^{\lambda_{n+1}}$  times the sum over  $\delta$  of  $a_{n-1}(\delta g_{n-1})^{(\lambda_1+n, \lambda_2+n-1, \dots, \lambda_{n-1}+2, 0)}$ . Notice that this sum is a Borel Eisenstein series for  $SL(n-1, \mathbb{Z})$ , which at  $\lambda = \lambda(s)$  from (33) is the constant function (i.e., it is being evaluated at  $-\rho$  for  $SL(n-1)$ ). That proves that  $E_{n-1}(g, \lambda(s)) = \Delta^{\lambda_{n+1}} = \Delta^{-s}$ . It is clear from (34) that  $\|e_n \gamma_1 g\| = \|e_n \Delta k\| = \Delta$ , completing the proof that  $E_{n-1}(g, \lambda(s)) = \|e_n \gamma g\|^{-s}$  and hence of the equality between (30) and (31).

To finish this proof of the Siegel integration formula, we return to (29) and compute the left-hand side. Notice that the order of integration is crucial, since the  $s$ -integration combines several Eisenstein series (none of which are integrable over  $\Gamma \backslash G$ ) into an incomplete Eisenstein series which is. However, the correspond integrals of the truncated Eisenstein series do converge, allowing the order of integration to be switched. Taking  $C$  as in (28), the large  $T$  limit of

$$\frac{1}{2\pi i} \int_{\Re s = n+1} M p(s) \int_{\Gamma \backslash G} (\Lambda^C E)(g, \lambda(s)) dg ds \tag{35}$$

converges to the left-hand side of (29). By the Maass-Selberg relations (27) this last expression equals

$$\frac{1}{2\pi i} \int_{\Re s = n+1} Mp(s) \sum_{w \in W} \frac{C^{w\lambda(s)-\rho} M(w, \lambda(s))}{\prod_{\alpha \in \Sigma} \langle w\lambda(s) - \rho, \alpha \rangle} ds. \quad (36)$$

The right-hand side of (29) suggest taking a residue at  $s = n$ ; we will be done if we can show the leading term in (36) comes from a Weyl group element  $w \in W$  with residue  $\xi(2) \cdots \xi(n-1)$  at  $s = n$  (using a contour shift as in the proof of the  $n = 2$  case). There  $\lambda(n)$  from (33) is put into descending order by reversing the order of the first  $n-1$  entries. The leading term comes from  $C^{w\lambda(n)-\rho} = T^{(\rho, w\lambda(s)-\rho)}$  when  $w$  is this permutation, which we assume it is for the rest of this calculation. (The fact that this is the leading term is proven using the Cauchy-Schwartz analysis in the proof of the volume formula.)

By definition of  $\lambda(s)$ , one has

$$\langle \lambda(s), \alpha_{i,j} \rangle = \begin{cases} i - j, & i < j < n \\ s - n + i, & i < j = n. \end{cases} \quad (37)$$

The permutation  $w$  flips the signs of the first  $n-1$  entries, and so if performed naively one runs into the issue that  $M(w, \lambda)$  from (25) vanishes. However,  $w\lambda(n) = (-2, -3, \dots, -n+1, -n, -n-1) = \rho$ , so the denominators do also (just as in the volume formula) and one has to proceed more carefully by looking at the full contribution to the integral (36) for this  $w$ ,

$$\frac{1}{2\pi i} \int_{\Re s = n+1} Mp(s) \frac{C^{w\lambda(s)-\rho} M(w, \lambda(s))}{\prod_{\alpha \in \Sigma} \langle w\lambda(s) - \rho, \alpha \rangle} ds. \quad (38)$$

We perturb  $\lambda(s)$  slightly by adding  $\varepsilon\rho$  for  $\varepsilon$  small: let

$$\begin{aligned} \tilde{\lambda}(s) &= \lambda(s) + \varepsilon\rho \\ &= (n(-1+\varepsilon), (n-1)(-1+\varepsilon), \dots, 2(-1+\varepsilon), -s + (-1+\varepsilon)) \\ w\tilde{\lambda}(s) &= (2(-1+\varepsilon), 3(-1+\varepsilon), \dots, n(-1+\varepsilon), -s + (-1+\varepsilon)) \\ w\tilde{\lambda}(s) - \rho &= (2\varepsilon - 2 - n, 3\varepsilon - 2 - n, \dots, n\varepsilon - 2 - n, -s - 2 + \varepsilon) \\ &\equiv (2\varepsilon, 3\varepsilon, \dots, n\varepsilon, n - s + \varepsilon) \pmod{(1, 1, \dots, 1)}. \end{aligned}$$

Since the positive roots flipped by  $w$  are the  $\alpha_{i,j}$  with  $i < j < n$ ,

$$M(w, \tilde{\lambda}(s)) = \prod_{i < j < n} c((j-i)(-1+\varepsilon))$$

by (25); the  $\varepsilon$ -perturbation has kept this from vanishing. Also,

$$C^{w\lambda(s)-\rho} = T^{\langle \rho, w\lambda(s)-\rho \rangle} = T^{\varepsilon \sum_{j < n} (\frac{n+1}{2}-j)(j+1) - \frac{n-1}{2}(n-s+\varepsilon)} \quad (39)$$

and

$$\langle w\lambda(s) - \rho, \alpha_{j,j+1} \rangle = \begin{cases} -\varepsilon, & j < n-1 \\ s-n+(n-1)\varepsilon, & j = n-1. \end{cases}$$

We see that (38) has a  $n-2$  terms from  $M(w, \tilde{\lambda}(s))$  vanishing at  $\varepsilon = 0$ , each of which is compensated by a vanishing factor of  $-\varepsilon$  from the product in the denominator. As in the proof of the volume formula, we compute the  $\varepsilon \rightarrow 0$  limit of the integrand in (38) as

$$Mp(s) \frac{T^{-\frac{n-1}{2}(n-s)}}{s-n} \cdot \left[ \xi(2)^{n-2} \prod_{\substack{i < j < n \\ j-i > 1}} c(j-i) \right]$$

using the Lemma from the proof of the volume formula. The bracketed expression is the expression for the volume of  $SL(n-1, \mathbb{Z}) \backslash SL(n-1, \mathbb{R})$ . Therefore the contour shift to the left picks up the residue from the pole at  $s = n$  of

$$Mp(n) \xi(2) \xi(3) \cdots \xi(n-1),$$

which is precisely the right-hand side of (29).

## Index

- Boneh-Durfee attack, 5
- complex upper half plane, 18
- Constant term formula
  - $n=2$ , 18
- constant term formula, 26
- Coppersmith's method, 6
  - Howgrave-Graham estimate, 7
- covolume, 4
- dense packings
  - existence of, 11
  - Rogers bound, 12
  - saturated, 12
  - Venkatesh bound, 12
- Eisenstein series
  - absolute convergence, 25
  - Borel, 25
  - incomplete, 15
  - minimal parabolic, 25
  - nonholomorphic, 17
- Epstein Zeta function, 15
- fundamental domain
  - volume computation using Eisenstein series, 20
  - volume formula, 28
- Gaussian integral, 23
- Godement range, 25
- Godement, Roger, 25
- Haar measure, 10
- hyperbolic laplacian, 18
- Iwasawa decomposition, 25
- Langlands
  - Robert P., 19
- LLL algorithm, 4
  - applications, 4
- Maass-Selberg relations, 20
- maximal compact subgroup, 18
- Mellin inversion formula, 16
- Mellin transform, 16
- Minkowski's Second Theorem, 4
- Minkowski-Hlawka Theorem, 12
- mirabolic, 13
- pairing of roots, 26
- parabolic subgroup
  - mirabolic, 13
- primitive vector, 13
- Procrustes, 19, 21
- radius of constant volume ball, 12
- roots, 26
  - positive, 26
  - simple, 26
- RSA algorithm, 4
  - Wiener's attack, 5
- Schwartz function
  - radial, 15
- Sdom, 19, 21
- Siegel, 17
- Siegel integration formula, 10
  - soft proof, 14
- sphere packing density, 11
- star-like domain, 11
- strictly dominant, 25
- successive minima, 4

Tangawa number, [14](#)  
truncation operator, [19](#)  
    Langlands', [27](#)

unit ball  
    surface area, [23](#)  
    volume, [23](#)

Weyl group, [27](#)  
Wiener's attack on RSA, [5](#)