A study on the coefficients of Eisenstein elements of prime square level

Arkabrata Das

under the supervision of

Dr. Narasimha Kumar

A Thesis Submitted to

Indian Institute of Technology Hyderabad

In Partial Fulfillment of the Requirements for

The Degree of Master of Science

Department of Mathematics

Indian Institute of Technology, Hyderabad

Telangana-502285

MAY 2019

Declaration

This thesis entitled **A study on the coefficients of Eisenstein elements of prime square level** submitted by me to the Indian Institute of Technology, Hyderabad for the award of the degree in Master of Science in Mathematics contains a literature review of the article, *A note on the Eisenstein elements of prime square level* by Dr. Debargha Banerjee. The work presented in this thesis has been carried out under the supervision of **Dr. Narasimha Kumar**, Department of Mathematics, Indian Institute of Technology Hyderabad, Telangana.

I declare that this written submission represents my ideas in my own words, and where ideas or words of others have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be a cause for disciplinary action by the Institute and can also evoke penal action from the sources that have thus not been properly cited, or from whom proper permission has not been taken when needed.

Arkabrata Das

(Signature)

ARKABRATA DAS

(Arkabrata Das)

MA17MSCST11001

(Roll No.)

Approval Sheet

This Thesis entitled **A study on the coefficients of Eisenstein elements of prime square level by Arkabrata Das is approved for the degree in Master of Science from IIT Hyderabad**

CH.V.G.N.Kumar 26/05/19.

(Dr. Narasimha Kumar) Adviser
Dept. of Mathematics
IITH

Acknowledgements

I would like to express my deep sense of gratitude to my supervisor **Dr. Narasimha Kumar** for his valuable and constructive suggestions during the development of this project. I am thankful for his willingness to give his time so generously and for his support, encouragement, co-operation and invaluable guidance throughout this project. Due to his motivation and expert guidance, I was able to achieve much knowledge in number theory.

I hope that I have incorporated all the corrections suggested by my advisor. I will be solely held responsible for any mistake found in this thesis, if any, and not my advisor.

I would also like to thank all the teachers of the department of Mathematics for their constant support and encouragement and imparting knowledge.

Last but not the least, I would like to thank my family for believing in me and giving me an opportunity to study in IIT Hyderabad. Above all I thank The Almighty, Lord Shiva for all his blessings.

Arkabrata Das

Abstract

The Manin-Drinfeld theorem is an important result of the theory of modular forms on the existing of an isomorphism between the space of Eisenstein series $E_2(\Gamma_0(N))$ and a first homology group $\mathbb{H}_1(X_0(N), \mathbb{Z})$ of a modular curve $X_0(N)$. Explicitly such an isomorphism was first constructed in [1] in the case when $N = p$ is prime. In the thesis we review the structure of an isomorphism in the case when $N = p^2$ and $p \geq 3$ is prime.

Contents

Chapter 1

Introduction

The description of the structure of spaces $\mathcal{M}_k(\Gamma)$ is the main objective of the theory of modular forms. The theory had already found many applications, e.g. in number theory where a version of Modularity Theorem was used to prove the Fermat's Theorem. There are still a number of open problems and conjectures around modular forms such as the conjecture by Birch and Swinnerton-Dyer. The structure of the space $\mathcal{M}_2(\Gamma_0(N))$ was described by Manin and Drinfeld [2, 3]. They proved that the Eisenstein element corresponding to the Eisenstein series $E \in E_2(\Gamma_0(N))$ is a combination of certain modular symbols. Explicitly such representation was first found in [1] for the case when $N = p$ is prime. Below we review [4] where the analogous representation is obtained for numbers $N = p^2$, $p \geq 3$ is prime.

1.1 Modular group

By $\mathrm{SL}_2(\mathbb{Z})$ we denote the set of all 2×2 matrices with integer entries and determinant 1, that is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

if and only if $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$. The inverse of a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ is the matrix $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Every element $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ acts on the compactified complex plane $\mathbb{C} \cup \{\infty\}$ by the following rule.

- If $c = 0$, then

$$\gamma(z) = \begin{cases} \frac{az+b}{d}, \ z \in \mathbb{C} \\ \infty, \ z = \infty \end{cases}$$

(action is well-defined since $ad - bc = 1 = ad$ and $d = \pm 1$.

- If $c \neq 0$, then

$$\gamma(z) = \begin{cases} \frac{az+b}{cz+d}, \ z \in \mathbb{C}, \ z \neq -d/c \\ \infty, \ z = -d/c \\ a/c, \ z = \infty \end{cases}$$

$\gamma : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$ is a group action, as the composition $\gamma_1 \circ \gamma_2$ of actions coincides with the action of the product $\gamma_1 \gamma_2$.

The upper half-plane is $\mathbb{H} = \{z \in \mathbb{C} : Im(z) > 0\}$. For every $z \in \mathbb{H}$

$$\gamma(z) = \frac{az+b}{cz+d} = \frac{(az+b)(c\bar{z}+d)}{|cz+d|^2} = \frac{ac|z|^2 + bd + (ad+bc)Re(z) + i(ad-bc)Im(z)}{|cz+d|^2}$$

Hence $Im(\gamma(z)) = \frac{Im(z)}{|cz+d|^2} > 0$ and $\mathrm{SL}_2(\mathbb{Z})$ acts on the upper half-plane $\mathbb{H}$. By definition, $\mathrm{SL}_2(\mathbb{Z})$ also acts on $\mathbb{Q} \cup \{\infty\}$ which can be viewed as a projective space $\mathbb{P}^1(\mathbb{Q})$ (see section 1.6 about projective lines). With the usual topology $\mathbb{H}$ is a noncompact Riemann surface. The union $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ can be given a topology which defined a compact Riemann surface that compactifies $\mathbb{H}$.

1.2 Congruence subgroups

For a fixed integer $N \geq 1$, $\Gamma(N)$ denotes the set of all matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that $a \equiv d \equiv 1 \pmod N$ and $c \equiv b \equiv 0 \pmod N$. $\Gamma(N)$ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$, since sums and products commute with taking resides modulo N. Moreover, $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$:

if $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, then for every $\gamma \in \Gamma(N)$

$$\alpha^{-1}\gamma\alpha \equiv \alpha^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod N,$$

i.e. $\alpha^{-1}\Gamma(N)\alpha = \Gamma(N)$.

The index of $\Gamma(N)$ in $\mathrm{SL}_2(\mathbb{Z})$ is finite:

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$$

where the product is taken over all prime divisors of N.

$\Gamma(N)$ is a principle congruence subgroup. A subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup, if it contains $\Gamma(N)$ for some level N. Two important examples of congruence subgroups are

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

and

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

1.3 Modular curves

The quotient of the upper half-plane by the action of $\Gamma_0(N)$ is genoted by $Y_0(N)$:

$$Y_0(N) = \Gamma_0(N) \setminus \mathbb{H}$$

The quotient of the compactified upper half-plane by the action of $\Gamma_0(N)$ is genoted by $X_0(N)$:

$$X_0(N) = \Gamma_0(N) \setminus \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$$

These modular curves are sets of orbits of $\Gamma_0(N)$: $Y_0(N) = \{\Gamma_0(N)z, z \in \mathbb{H}\}$, $X_0(N) = \{\Gamma_0(N)z, z \in \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})\}$. With the quotient topology they are Riemann surfaces, $X_0(N)$ is a compact Riemann surface. The image $\Gamma_0(N) \setminus \mathbb{P}^1(\mathbb{Q})$ will be denoted as cusps (it is called the set of cusps of $X_0(N)$). More generally, $Y(\Gamma)$ and $X(\Gamma)$ denoted non-compactified and compactified modular curves with respect to a congruence subgroup Γ.

The topology on a modular curve is a quotient topology, so we need to introduce a proper topology on $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. For every point $\tau \in \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ we define the fundamental system of neighborhoods $\mathfrak{U}_\tau$ as follows.

1. If $\tau \in \mathbb{H}$ (i.e. $\tau = x + iy$, $y > 0$), then

   $$\mathfrak{U}_\tau = \{B(\tau, \epsilon) : \epsilon \in (0, y)\}.$$

   Here $B(\tau, \epsilon) = \{z \in \mathbb{C} : |z - \tau| < \epsilon\}$ – a usual disk of center τ and radius ϵ. Condition $\epsilon < y$ is needed to assure that the disk is in $\mathbb{H}$. In other words, fundamental system of neighborhoods of a (non-cuspidal) point $\tau \in \mathbb{H}$ is the same as on the complex plane.

2. If $\tau = \infty$, then

   $$\mathfrak{U}_\infty = \{\{\infty\} \cup \mathcal{N}_M : M > 0\},$$

where $\mathcal{N}_M = \{z \in \mathbb{H} : Im(z) > M\}$. It means that a neighborhood of ∞ contains all points of the upper half plane with large enough imaginary part.

3. If $\tau = p \in \mathbb{Q}$, then
$$\mathfrak{U}_p = \{\{p\} \cup B(p + i\epsilon, \epsilon) : \epsilon > 0\},$$
i.e. a neighborhood of $p \in \mathbb{Q}$ contains a disk in $\mathbb{H}$ that is tangent to real axis at a point p.

After we defined fundamental systems of neighborhoods, we can define the topology on $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$: a set $G \subset \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ is open if and only if for every $\tau \in G$ there is a neighborhood $B \in \mathfrak{U}_\tau$ such that $B \subset G$.

In such a way a true topology is defined.

1. Assume that $\{G_\alpha\}_{\alpha \in A}$ is a family of open sets. We will show that the union $G = \cup_{\alpha \in A} G_\alpha$ is open. Indeed, if $\tau \in G$, then $\tau \in G_\alpha$ for some $\alpha \in A$. By definition of open sets there is $B \in \mathfrak{U}_\tau$ such that $B \subset G_\alpha \subset G$. So, G is open.

2. Assume that G_1, G_2 are open sets. We will show that the intersection $G = G_1 \cap G_2$ is open. Indeed, if $\tau \in G$, then $\tau \in G_1$ and $\tau \in G_2$. By definition of open sets, there are $B_1, B_2 \in \mathfrak{U}_\tau$ such that $B_1 \subset G_1$, $B_2 \subset G_2$. As $B_1 \cap B_2 \subset G$, it remains to observe that $B_1 \cap B_2 \in \mathfrak{U}_\tau$. For $\tau \in \mathbb{H}$ and $\tau = \infty$ it is obvious, for $\tau = p$ we have
$$B_1 = \{p\} \cup B(p + i\epsilon_1, \epsilon_1), B_2 = \{p\} \cup B(p + i\epsilon_2, \epsilon_2).$$
Assume that $\epsilon_1 \leq \epsilon_2$. If $z = x + iy \in B_1$, then $|z - p - i\epsilon_1| < \epsilon_1$,
$$(x - p)^2 + (y - \epsilon_1)^2 < \epsilon_1^2,$$
and
$$|z - p - i\epsilon_2|^2 = (x - p)^2 + (y - \epsilon_2)^2 <$$
$$< \epsilon_1^2 - (y - \epsilon_1)^2 + (y - \epsilon_2)^2 =$$

$$= \epsilon_2^2 - 2y(\epsilon_2 - \epsilon_1) \leq \epsilon_2^2.$$

It means that $B_1 \subset B_2$ and $B_1 \cap B_2 = B_1 \in \mathfrak{U}_\tau$.

Now, $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ is a topological space. Moreover, every set $B \in \mathfrak{U}_\tau$ is open in $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. Indeed, consider $z \in B$. If $z \in \mathbb{H}$, then either $B \cap \mathbb{H}$ is a disk, or $B \cap \mathbb{H}$ is a strip $\mathcal{N}_M$. In any case one finds a disk around z that belongs to B. If $z \notin \mathbb{H}$ then either $z = \infty$ or $z = p \in \mathbb{Q}$. But if $z = \infty$, then $\infty \in B$ and necessarily $B \in \mathfrak{U}_\infty$. Similarly, if $z = p$, then $p \in B$ and necessarily $B \in \mathfrak{U}_p$.

As a conclusion, the space $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ is equipped with a topology by specifying fundamental system of neighborhoods of every its point. For this topology to be properly transferred to the modular curve, we check that every element $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ is a homeomorphism of $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$.

Consider $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $c \neq 0$. We recall that

$$\gamma(\tau) = \begin{cases} \frac{a\tau+b}{c\tau+d}, \tau \neq \infty, -\frac{d}{c} \\ \frac{a}{c}, \ \tau = \infty \\ \infty, \ \tau = -\frac{d}{c} \end{cases}$$

Then γ is a bijection of $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. Continuity at every $\tau \in \mathbb{H}$ follow from the relation $\gamma(\mathbb{H}) \subset \mathbb{H}$ and the fact that $\mathbb{H}$ is equipped with the usual topology of a upper half plane.

We check continuity at ∞. Now

$$\gamma(\infty) = p = \frac{a}{c}.$$

Consider a neighborhood of $p = \frac{a}{c}$. It is of the form $\{p\} \cup B(p + i\epsilon, \epsilon)$. We must find a negihborhood $\{\infty\} \cup \mathcal{N}_M$ of ∞, such that $\gamma(\mathcal{N}_M) \subset B(p + i\epsilon, \epsilon)$. Take $M = \frac{1}{2\epsilon c^2}$. Let

$z \in \mathcal{N}_M$, i.e. $Im(z) > M$. Then

$$|\gamma(z) - p - i\epsilon| = \left|\frac{az+b}{cz+d} - \frac{a}{c} - i\epsilon\right| = \frac{c(az+b) - a(cz+d) - i\epsilon c(cz+d)}{|c||cz+d|} =$$

from condition $ad - bc = 1$

$$= \frac{|1 + i\epsilon c(cz+d)|}{|c||cz+d|}$$

So, the condition to be verified is

$$|1 + i\epsilon c(cz+d)| < \epsilon|c||cz+d|$$

Equivalently,

$$(1 + i\epsilon c(cz+d))(1 - i\epsilon c(c\bar{z}+d)) < \epsilon^2 c^2 |cz+d|^2$$

$$1 + i\epsilon c(cz + d - c\bar{z} - d) < 0$$

$$1 - 2\epsilon c^2 Im(z) < 0$$

which is true by $Im(z) > M$. Continuity at $\tau = \infty$ is verified.

We check continuity at $p = -\frac{d}{c}$. Now

$$\gamma(p) = \infty.$$

Consider a neighborhood of ∞. It is of the form $\{\infty\} \cup \mathcal{N}_M$. We must find a negihborhood $\{p\} \cup B(p + i\epsilon, \epsilon)$ of p, such that $\gamma(B(p + i\epsilon, \epsilon)) \subset M$. Take $\epsilon = \frac{1}{2Mc^2}$. Let $z \in B(p + i\epsilon, \epsilon)$. Then

$$|z - p - i\epsilon| < \epsilon.$$

Equivalently,

$$\left|z + \frac{d}{c} - i\epsilon\right| < \epsilon$$

$$|cz + d - ic\epsilon| < \epsilon|c|$$

Taking squares we get

$$(cz + d - ic\epsilon)(c\bar{z} + d + ic\epsilon) < \epsilon^2 c^2$$

$$|cz + d|^2 + ic\epsilon(cz + d - c\bar{z} - d) < 0$$

$$|cz + d|^2 - 2c^2\epsilon Im(z) < 0.$$

So,

$$Im(\gamma(z)) = \frac{Im(z)}{|cz + d|^2} > \frac{1}{2c^2\epsilon} = M.$$

Continuity at $\tau = -\frac{d}{c}$ is verified.

We check continuity at $\tau = p \neq -\frac{d}{c}$. Now we have

$$\gamma(p) = \frac{ap + b}{cp + d} \in \mathbb{Q}.$$

Consider a neighborhood of $\gamma(p)$. It is of the form $\{\gamma(p)\} \cup B(\gamma(p) + i\epsilon, \epsilon)$. We must find a negihborhood $\{p\} \cup B(p + i\delta, \delta)$ of p, such that $\gamma(B(p + i\delta, \delta)) \subset B(\gamma(p) + i\epsilon, \epsilon)$. We observe from previous calculations that the relation

$$|z - p - i\delta| < \delta$$

is equivalent to

$$\frac{Im(z)}{|z - p|^2} > \frac{1}{2\delta}.$$

Hence, the relation $|\gamma(z) - \gamma(p) - i\epsilon| < \epsilon$ is equivalent to

$$\frac{Im(\gamma(z))}{|\gamma(z) - \gamma(p)|^2} > \frac{1}{2\epsilon}.$$

Further

$$|\gamma(z) - \gamma(p)| = \left| \frac{az + b}{cz + d} - \frac{ap + b}{cp + d} \right| =$$

$$= \frac{|acpz + adz + bcp + bd - acpz - bcz - adp - bd|}{|cz + d||cp + d|} = \frac{|z - p|}{|cz + d||cp + d|}.$$

So,

$$\frac{Im(\gamma(z))}{|\gamma(z)-\gamma(p)|^2} = \frac{Im(z)}{|z-p|^2}|cp+d|^2 > \frac{|cp+d|^2}{2\delta}$$

and it is enough to take $\delta = \frac{\epsilon}{|cp+d|^2}$. Continuity of $\gamma : \mathbb{H}^* \to \mathbb{H}^*$ is verified.

It remains to consider the case $c = 0$. From the relation $ad - bc = 1$ it follows that $|a| = |d| = 1$. Now

$$\gamma(\tau) = \begin{cases} \frac{a\tau+b}{d}, \tau \neq \infty \\ \infty, \ \tau = \infty \end{cases}$$

Again, continuity at $\tau \in \mathbb{H}$ is immediate. Let us check continuity at ∞. The relation for imaginary part takes the form

$$Im(\gamma(\tau)) = \frac{1}{|d|^2} Im(z) = Im(z),$$

so $Im(z) > M$ implies $Im(\gamma(z)) > M$. Continuity at ∞ is verified. Let us check continuity at $p \in \mathbb{Q}$. But again we have $|\gamma(z) - \gamma(p)| = |z - p|$, so if $|z - p - i\epsilon| < \epsilon$, then

$$\frac{Im(z)}{|z-p|} > \frac{1}{2\epsilon},$$

$$\frac{Im(\gamma(z))}{|\gamma(z)-\gamma(p)|} > \frac{1}{2\epsilon},$$

and finally $|\gamma(z) - \gamma(p) - i\epsilon| < \epsilon$. In the case $c = 0$ function γ simply shifts neighborhood of p onto a neighborhood of $\gamma(p)$.

With the quotient topology $X(\Gamma)$ is a Riemann surface with the local coordinates about a cusp $s \in \mathbb{P}^1(\mathbb{Q}) \cup \{\infty\}$ given by a composition of a straightening map $\delta \in \mathrm{SL}_2(\mathbb{Z})$, where $\delta(s)\infty$ and the wrapping map $\rho(z) = e^{2\pi i z/h}$ with width h equal to the index of a subgroup Γ_s that fixes a point s [5, §2.4.].

1.4 Modular forms

Let $k \in \mathbb{Z}$. We will consider holomorphic functions $f : \mathbb{H} \to \mathbb{C}$. For every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ define the factor of automorphy

$$j(\gamma, \tau) = c\tau + d.$$

The wight-k operator is defined by

$$f[\gamma]_k(\tau) := j(\gamma, \tau)^{-k} f(\gamma(\tau)).$$

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. A function f is weakly modular of weight k with respect to Γ, if the relation

$$f[\gamma]_k = f$$

holds for every $\gamma \in \Gamma$. Every weight-k weakly modular form admits a Laurent expansion in the following sense.

Since $\Gamma(N) \subset \Gamma$, it follows that $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma$. Let h be minimal positive integer such that $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \Gamma$. Then for every integer $m \in \mathbb{Z}$ we have $\gamma_{mh} = \begin{pmatrix} 1 & mh \\ 0 & 1 \end{pmatrix} \in \Gamma$. and

$$f(\tau + mh) = f[\gamma_{mh}]_k(\tau) = f(\tau).$$

The mapping $q_h(\tau) = e^{\frac{2\pi i \tau}{h}}$ sends $\mathbb{H}$ onto the punctured unit disk $D' = \{q \in \mathbb{C} : 0 < |q| < 1\}$. Define the function $g : D' \to \mathbb{C}$ by

$$g(q_h) = f(\tau), \; q_h = e^{\frac{2\pi i \tau}{h}}.$$

The definition is correct: if $e^{\frac{2\pi i \tau}{h}} = e^{\frac{2\pi i \tau'}{h}}$, then $\tau - \tau' = mh$ for some integer m and $f(\tau) = f(\tau' + mh) = f(\tau')$. Further, g is holomorphic in D' and hence can be written as a Laurent series:

$$f(\tau) = g(q_h) = \sum_{n \in \mathbb{Z}} a_n q_h^n.$$

f is called holomorphic at ∞, if $a_n = 0$ for all $n < 0$, i.e.

$$f(\tau) = g(q_h) = \sum_{n=0}^{\infty} a_n q_h^n.$$

In this case the series expansion in powers of q_h is called the Fourier expansion of $f[\alpha]_k$.

If f is weight-k weakly modular with respect to Γ, then for any $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ function $f[\alpha]_k$ is weight-k weakly modular with respect to $\alpha^{-1}\Gamma\alpha$. Since, $\Gamma(N)$ is normal, the subgroup $\alpha^{-1}\Gamma\alpha$ is a congruence subgroup and the property to be holomorphic at ∞ makes sense for $f[\alpha]_k$ as well.

Definition. A weight-k modular form with respect to a congruence subgroup Γ is a function $f : \mathbb{H} \to \mathbb{C}$ such that

- f is holomorphic
- f is weight-k weakly modular with respect to Γ
- for every $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ $f[\alpha]_k$ is holomorphic at ∞.

The space of all such forms is denoted $\mathcal{M}_k(\Gamma)$. It is a complex vector space. If, additionally, for every $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ the zero term in the Fourier expansion of $f[\alpha]_k$ is zero, then f is called a cusp form. The space of cusp forms is denoted by $\mathcal{S}_k(\Gamma)$, it is a subspace of $\mathcal{M}_k(\Gamma)$. The qoutient $\mathcal{M}_k(\Gamma)/\mathcal{S}_k(\Gamma)$ is called the space of Eisenstein series and is denoted by $E_k(\Gamma)$. In the chapter 3 we will specify representatives for elements of $E_k(\Gamma)$ that are true series. By definition, every Eisenstein series E is represented up to a cusp form by some $f \in \mathcal{M}_k(\Gamma)$. For every $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ the zero Fourier coefficient of $f[\alpha]_k$ is called the Fourier coefficient at ∞ and it is independent on the choice of f. It is assumed that all Fourier coefficients at ∞ of an Eisenstein series E belong to some number filed K, i.e. a finite dimensional field extension of the field of rational numbers $\mathbb{Q}$.

1.5 Homology and cohomology groups

1.5.1 General definitions

Denote by Δ^n the standard $n-$simplex in $\mathbb{R}^{n+1}$, that is

$$\Delta^n = \{(t_0, t_1, \dots, t_n) \in \mathbb{R}^{n+1} | t_0, \dots, t_n \geq 0, \sum_{i=0}^{n} t_i = 1\}.$$

A singular $n-$simplex in a topological space X is a continuous mapping $\sigma : \Delta^n \to X(\Gamma)$.

Let $v_0 = (1, 0, 0, \dots, 0)$, $v_1 = (0, 1, 0, \dots, 0), \dots,$ $v_n = (0, 0, 0, \dots, 1)$ be vertices of the simplex Δ^n. By $[v_0, \dots, \hat{v}_i, \dots, v_n]$ we will understand the set

$$\{(t_0, t_1, \dots, t_n) \in \Delta^n | t_i = 0\}$$

and we will identify it with Δ^{n-1} by the correspondence

$$(t_0, t_1, \dots, t_n) \to (t_0, t_1, \dots, t_{i-1}, t_{i+1}, \dots, t_n) \in \Delta^{n-1}$$

This correspondence is a natural identification of $i-$th $(n-1)-$dimensional facet of Δ^n with Δ^{n-1}. Respectively, the restriction

$$\sigma|_{[v_0, \dots, \hat{v}_i, \dots, v_n]}$$

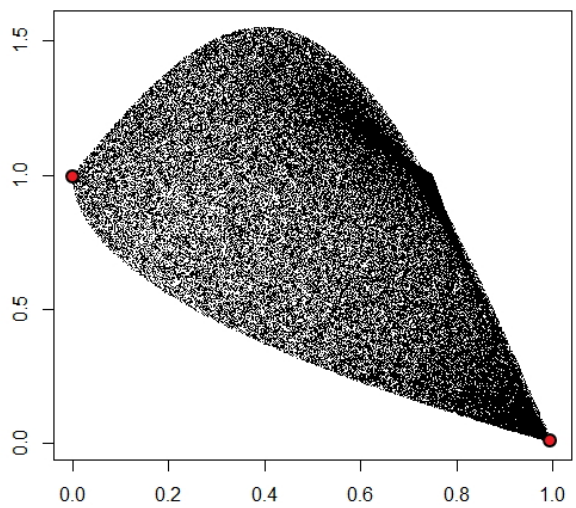
is a singular $(n-1)-$dimensional simplex. Precisely,

$$\sigma|_{[v_0, \dots, \hat{v}_i, \dots, v_n]}((t_0, t_1, \dots, t_{n-1})) = \sigma((t_0, \dots, t_{i-1}, 0, t_i, \dots, t_n))$$

Example 1.5.1. *Let $X = \mathbb{R}^2$ and*

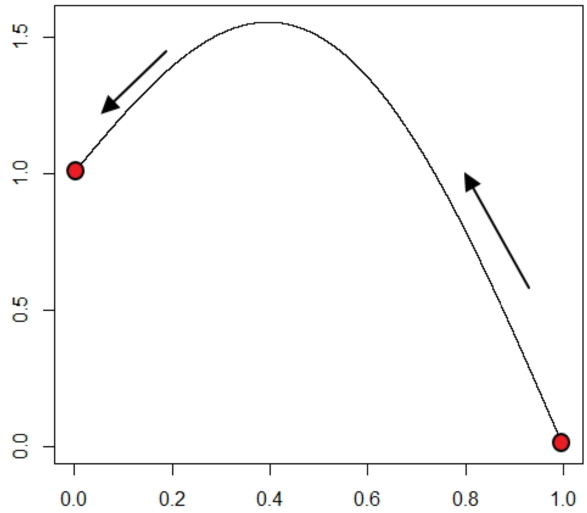
$$\sigma((t_0, t_1, t_2)) = (t_0^2 + t_1, \sin(\pi t_1) + t_2)$$

be a singular $2-$simplex in $\mathbb{R}^2$. Its vertices are $v_0 = (1,0)$, $v_1 = (1,0)$, $v_2 = (0,1)$. Vertices are $0-$dimensional facets. Observe that two of them coincide. Form of the simplex can be seen from the picture below. Vertices are represented by red points.

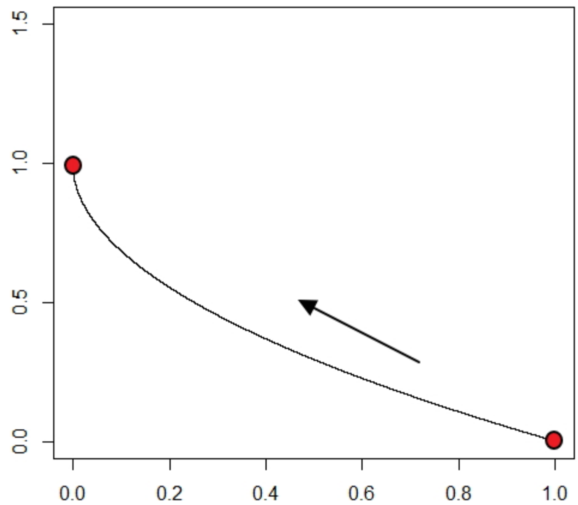


This simplex has three $1-$dimensional facets (actually, curves on the plane) that can be written in a parametrization $t = t_1 = 1 - t_0$, $0 \leq t \leq 1$, in the following way (the choice of parametrization is dictated by the fact that the order of vertices in the sub-simplex must be the same)

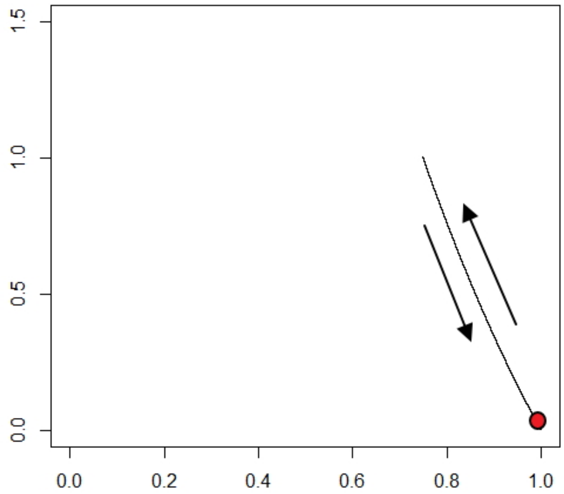
$$\sigma|_{[\hat{v}_0, v_1, v_2]} = \{(1 - t, \sin(\pi(1 - t)) + t) : 0 \leq t \leq 1\};$$



$$\sigma|_{[v_0,\hat{v}_1,v_2]} = \{((1-t)^2, t) : 0 \le t \le 1\};$$



$$\sigma|_{[v_0,v_1,\hat{v}_2]} = \{((1-t)^2 + t, \sin(\pi t)) : 0 \le t \le 1\}.$$



Let $C_n(X)$ be a free abelian group with basis the set of all singular $n-$simplices in X. Precisely,

$$C_n(X) = \{\sum_{i=1}^{m} n_i\sigma_i | m \geq 0, n_1, \ldots, n_m \in \mathbb{Z}, \sigma_1, \ldots, \sigma_m \text{ are singular n-simplices in } X\}.$$

It is called the set of $n-$chains in X.

Consider the (boundary) mapping $\partial_n : C_n(X) \to C_{n-1}(X)$, defined as a group homomorphism such that

$$\partial_n(\sigma) = \sum_{i=0}^{n} (-1)^i \sigma|_{[v_0,\ldots,\hat{v}_i,\ldots,v_n]}.$$

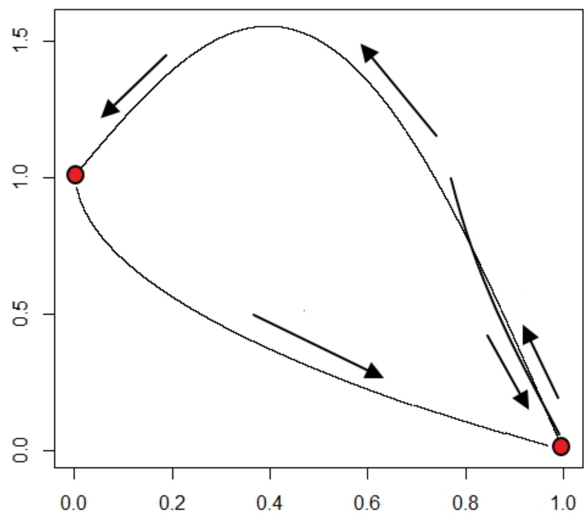
The homomorphism property implies that ∂_n is defined on all $C_n(X)$ by the rule

$$\partial_n(\sum_{i=1}^{m} n_i\sigma_i) = \sum_{i=1}^{m} n_i\partial_n(\sigma_i)$$

Example 1.5.2. *We use* $2-$*dimensional simplex in* $\mathbb{R}^2$ *defined in the example 1.5.1. We find that*

$$\partial_2(\sigma) = \sigma|_{[\hat{v}_0,v_1,v_2]} - \sigma|_{[v_0,\hat{v}_1,v_2]} + \sigma|_{[v_0,v_1,\hat{v}_2]}$$

These three curves are given on the plot below.



Observe that the arrow in $\sigma|_{[v_0,\hat{v}_1,v_2]}$ *is reversed, which corresponds to minus sign.* $\partial_2(\sigma)$ *is the cycle around the boundary of a singular simplex.*

Above constructions generalize to any field K. Let $C_n(X(\Gamma), K)$ be a set of all formal sums

$$\sum_{i=1}^{m} k_i \sigma_i,$$

where $m \geq 0$, $k_1, \dots, k_m \in K$ and $\sigma_1, \dots, \sigma_m$ are singular $n-$simplices. The space $C_n(X(\Gamma), K)$ is an abelian group. The boundary map $\partial_n : C_n(X(\Gamma), K) \to C_{n-1}(X(\Gamma), K)$ is defined as a group homomorphism such that

$$\partial_n(k\sigma) = \sum_{i=0}^{n} (-1)^i k\sigma|_{[v_0,\dots,\hat{v}_i,\dots,v_n]}$$

(here $(-1)k$ means the additive inverse of an element $k \in K$).

We check that $\partial_n \circ \partial_{n+1} = 0$.

Indeed, given any $(n+1)-$chain $k\sigma$ we have

$$\partial_{n+1}(k\sigma) = \sum_{i=0}^{n+1} (-1)^i k\sigma|_{[v_0,\dots,\hat{v}_i,\dots,v_{n+1}]}$$

and

$$\partial_n(\partial_{n+1}(\sigma)) = \sum_{i=0}^{n+1} \partial_n((-1)^i k\sigma|_{[v_0,\dots,\hat{v}_i,\dots,v_{n+1}]}) =$$

$$= \sum_{i=0}^{n+1} \left(\sum_{j=0}^{i-1} (-1)^{i+j} k\sigma|_{[v_0,\dots,\hat{v}_j,\dots,\hat{v}_i,\dots,v_{n+1}]} - \sum_{j=i+1}^{n+1} (-1)^{i+j} k\sigma|_{[v_0,\dots,\hat{v}_i,\dots,\hat{v}_j,\dots,v_{n+1}]} \right) =$$

$$= \sum_{0\le j<i\le n+1} (-1)^{i+j} k\sigma|_{[v_0,\dots,\hat{v}_j,\dots,\hat{v}_i,\dots,v_{n+1}]} - \sum_{0\le i<j\le n+1} (-1)^{i+j} k\sigma|_{[v_0,\dots,\hat{v}_i,\dots,\hat{v}_j,\dots,v_{n+1}]} = 0$$

The property $\partial_n \circ \partial_{n+1} = 0$ implies that one can define homology with coefficients

$$H_n(X(\Gamma), K) = \text{Ker } \partial_n/\text{Im } \partial_{n+1}$$

If A is a subspace of $X(\Gamma)$, then we define relative $n-$chains with coefficients as a quotient group

$$C_n(X(\Gamma), A, K) = C_n(X(\Gamma), K)/C_n(A, K).$$

If j_n is the quotient map:

$$j_n : C_n(X(\Gamma), K) \to C_n(X(\Gamma), A, K),$$

then the map $j_{n-1} \circ \partial_n : C_n(X(\Gamma), K) \to C_{n-1}(X(\Gamma), A, K)$ factors through $C_n(A, K)$. It defines a factored boundary map

$$\partial_n : C_n(X(\Gamma), A, K) \to C_{n-1}(X(\Gamma), A, K)$$

by the property

$$\partial_n \circ j_n = j_{n-1} \circ \partial_n.$$

For factored boundary maps relation $\partial_n \circ \partial_{n+1} = 0$ is preserved and the relative homology groups

$$H_n(X(\Gamma), A, K) = \text{Ker } \partial_n/\text{Im } \partial_{n+1}$$

are defined. In particular, $H_1(Y_0(N), K)$ is a group of cycles modulo boundaries of

2−chains in $Y_0(N)$ and $H_1(X_0(N), \text{cusps}, K)$ is a group of continuous curves in $X_0(N)$ with endpoints in cusps.

Homology groups were defined starting from the chain

$$\ldots \xrightarrow{\partial_3} C_2(X) \xrightarrow{\partial_2} C_1(X) \xrightarrow{\partial_1} C_0(X).$$

To define cohomology groups at first we consider dual chain. Let $C^n(X)$ be the group $\mathrm{Hom}(C_n(X); \mathbb{Z})$ of all homomorphisms from $C_n(X)$ to $\mathbb{Z}$, i.e. $C^n(X)$ consists of mappings

$$\phi : C_n(X) \to \mathbb{Z}$$

such that $\phi(\sum_{i=1}^m n_i\sigma_i) = \sum_{i=1}^m n_i\phi(\sigma_i)$. Elements of spaces $C^n(X)$ are called cochains. Coboundary map $\delta^n : C^{n-1}(X) \to C^n(X)$ is defined dually to boundary maps ∂_n :

if $\phi^{n-1} \in C^{n-1}(X)$, then

$$(\delta^n(\phi^{n-1}))(\sigma) = \phi^{n-1}(\partial_n(\sigma)),\ \sigma \in C_n(X).$$

The definition is correct,as $\partial_n(\sigma) \in C_{n-1}(X)$. We obtain a chain

$$\ldots \xleftarrow{\delta^3} C^2(X) \xleftarrow{\delta^2} C^1(X) \xleftarrow{\delta^1} C^0(X).$$

Coboundary maps stasify the relation

$$\delta^{n+1} \circ \delta^n = 0.$$

Indeed, for every $\phi \in C^{n-1}(X)$ and any $\sigma \in C_{n+1}(X)$ we have

$$(\delta^{n+1} \circ \delta^n(\phi))(\sigma) = (\delta^n(\phi))(\partial_{n+1}(\sigma)) =$$

$$= \phi(\partial_n \circ \partial_{n+1}(\sigma)) = \phi(0) = 0.$$

Cohomology groups are defined as factor groups

$$H^n(X) = \text{Ker } \delta^{n+1}/\text{Im } \delta^n.$$

One of the advantages of a cohomology is that it is clear how to define the product of cohomologies. Given cochains $\phi \in C^k(X)$, $\psi \in C^l(X)$ we define a cochain $\phi \cup \psi \in C^{k+l}(X)$ by the following rule:

for any $\sigma : \Delta^{k+l} \to X$

$$(\phi \cup \psi)(\sigma) = \phi(\sigma|_{[v_0,\ldots,v_k]})\psi(\sigma|_{[v_k,\ldots,v_{k+l}]})$$

The coboundary map satisfies the following relation

$$\delta^{k+l+1}(\phi \cup \psi) = \delta^{k+1}\phi \cup \psi + (-1)^k \phi \cup \delta^{l+1}\psi.$$

Indeed, for any simplex $\sigma : \Delta^{k+l+1} \to X$ we have

$$\delta^{k+1}\phi \cup \psi(\sigma) + (-1)^k \phi \cup \delta^{l+1}\psi(\sigma) =$$

$$= \phi(\partial_{k+1}\sigma|_{[v_0,\ldots,v_{k+1}]})\psi(\sigma|_{[v_{k+1},\ldots,v_{l+1}]}) + (-1)^k \phi(\sigma|_{[v_0,\ldots,v_k]})\psi(\partial_{l+1}\sigma|_{[v_k,\ldots,v_{k+l+1}]}) =$$

$$= \sum_{i=0}^{k+1}(-1)^i \phi(\sigma|_{[v_0,\ldots,\hat{v}_i,\ldots,v_{k+1}]})\psi(\sigma|_{[v_{k+1},\ldots,v_{l+1}]}) +$$

$$+ \sum_{j=0}^{l+1}(-1)^{k+j}\phi(\sigma|_{[v_0,\ldots,v_k]})\psi(\sigma|_{[v_k,\ldots,\hat{v}_{k+j},\ldots,v_{k+l+1}]}) = (\phi \cup \psi)(\partial_{k+l+1}\sigma)$$

As a consequence of this formula, the cup product factorizes through coboundary maps, and gives the cup product of cohomologies.

$$\cup : H^k(X) \times H^l(X) \to H^{k+l}(X).$$

Relative cup products

$$\cup : H^k(X,A) \times H^l(X) \to H^{k+l}(X,A),$$

$$\cup : H^k(X) \times H^l(X,A) \to H^{k+l}(X,A),$$

$$\cup : H^k(X,A) \times H^l(X,A) \to H^{k+l}(X,A)$$

are also defined by the product formula.

The cap product is defined similarly to the cup product:

$$\cap : C_k(X) \times C^l(X) \to C_{k-l}(X)$$

for any $\sigma : \Delta^k \to X$ and $\phi \in C^l(X)$ we define

$$\sigma \cap \phi = \phi(\sigma|_{[v_0,\ldots,v_l]})\sigma|_{[v_l,\ldots,v_k]}.$$

From the formula

$$\partial(\sigma \cap \phi) = (-1)^l(\partial\sigma \cap \phi - \sigma \cap \delta\phi)$$

it follows that the cap product is defined for homologies

$$\cap : H_k(X) \times H^l(X) \to H_{k-l}(X).$$

For the n-dimensional manifold M, there is a natural homomorphism

$$D : H^k(M) \to H_{n-k}(M)$$

which is called duality. It allows to define cap product for homologies,

$$\cap : H_k(M) \times H_{n-l}(M) \to H_{k-l}(X).$$

For example, on a two-dimensional manifold M a cap product

$$\cap : H_1(M) \times H_1(M) \to H_0(M)$$

is defined. If a manifold is path-connected, then $H_0(M) \sim \mathbb{Z}$ and we have a mapping (intersection pairing)

$$\circ : H_1(M) \times H_1(M) \to \mathbb{Z}$$

1.5.2 Group $H_1(X_0(N), \mathbf{cusps}, \mathbb{Z})$ and Eisenstein elements

As it was defined in the general case, $H_1(X_0(N), \text{cusps}, \mathbb{Z})$ is a relative homology group. To examine its structure we consider following objects. $C_n(X_0(N))$ is a group of formal linear combinations $\sum_{i=1}^m n_i\sigma_i^{(n)}$, where each $\sigma_i^{(n)}$ is a continuous mapping of $n-$simplex into $X_0(N)$; $C_n(\text{cusps})$ is a group of formal linear combinations $\sum_{i=1}^m n_i\sigma_i^{(n)}$, where each $\sigma_i^{(n)}$ is a continuous mapping of a simplex into the set of cusps. As the set of cusps is finite (hence discrete), a continuous mapping $\sigma_i^{(n)} : \Delta^n \to \text{cusps}$ reduces to a constant mapping. So we identify each $\sigma_i^{(n)}$ with a cusp. With this identification all groups $C_n(\text{cusps})$ become isomorphic to $C_0(\text{cusps})$ – a group of formal linear combinations of cusps.

$C_n(X_0(N), \text{cusps}) = C_n(X_0(N)/C_0(\text{cusps})$ is a quotient group, where two $n-$chains are identified if they differ by an element of $C_0(\text{cusps})$ its elements are formal linear combinations $\sum_{i=1}^m n_i\sigma_i^{(n)} + C_0(\text{cusps})$ where each $\sigma_i^{(n)}; \Delta^n \to X_0(N)$.

Following general theory we introduce two boundary operators

$$\partial_1(\sum_{i=1}^m n_i\sigma_i^{(1)} + C_0(\text{cusps})) = \sum_{i=1}^m n_i(\sigma_i^{(1)}(1) - \sigma_i^{(1)}(0)) + C_0(\text{cusps})$$

$$\partial_2(\sum_{i=1}^m n_i\sigma_i^{(2)} + C_0(\text{cusps})) = \sum_{i=1}^m n_i(\sigma_i^{(2)}(1,2) - \sigma_i^{(2)}(0,2) + \sigma_i^{(2)}(0,1)) + C_0(\text{cusps})$$

It was checked that $\partial_1 \circ \partial_2 = 0$, so we can define the quotient group

$$H_1(X_0(N), \text{cusps}, \mathbb{Z}) = \text{Ker } \partial_1 / \text{Im } \partial_2.$$

Below are two examples

Example 1.5.3. *A continuous path $\sigma : \Delta^1 \to X_0(N)$ such that $\sigma(0)$ and $\sigma(1)$ are cusps, is an element of $H_1(X_0(N), cusps, \mathbb{Z})$. Indeed, applying boundary operator we get*

$$\partial_1(\sigma) = \sigma(1) - \sigma(0) \in C_0(cusps)$$

So, relative homology group contains not only cycles in $X_0(N)$ but also paths between cusps.

Example 1.5.4. *Consider two paths $\sigma_1 : \Delta^1 \to X_0(N)$ and $\sigma_2 : \Delta_2 \to X_0(N)$ that connect two cusps, i.e. $\sigma_1(0,1) = \sigma_2(0,1) = \alpha$, $\sigma_1(1,0) = \sigma_2(1,0) = \beta$. Assume that these paths are homotopic in $X_0(N)$, i.e. there exists continuous mapping*

$$\phi : \Delta^1 \times [0,1] \to X_0(N)$$

such that $\phi(0,1;s) = \alpha$, $\phi(1,0;s) = \beta$, $\phi(t_0,t_1;0) = \sigma_1(t_0,t_1)$ and $\phi(t_0,t_1;1) = \sigma_2(t_0,t_1)$. Then relative homological calsses of σ_1 and σ_2 coincide. Indeed, consider $2-$simplex

$$\sigma^{(2)}(t_0,t_1,t_2) = \begin{cases} \phi(t_0, t_1+t_2; \frac{t_2}{t_1+t_2}), \ t_0 < 1 \\ \beta, \ t_0 = 1 \end{cases}$$

Its continuity follows from continuity of ϕ. We compute its boundary:

$$\partial_2 \sigma^{(2)}(t_0,t_1) = \sigma^{(2)}(0,t_0,t_1) - \sigma^{(2)}(t_0,0,t_1) + \sigma^{(2)}(t_0,t_1,0) =$$

$$= \phi(0,1;t_1) - \phi(t_0,t_1;1) + \phi(t_0,t_1;0) = \alpha - \sigma_2 + \sigma_1$$

It follows that $\sigma_1 - \sigma_2 \in C_0(cusps)$ and $\sigma_1 = \sigma_2$ in H_1.

Let $f \in \mathcal{M}_2(\Gamma)$. For any $z_0 \in \mathbb{H}$ and $\gamma \in \Gamma$ let $c(\gamma)$ be the class in $H_1(Y(\Gamma), \mathbb{Z})$ of the image in $Y(\Gamma)$ of the geodesic in $\mathbb{H}$ joining z_0 and $\gamma(z_0)$. The integral

$$\pi_f(\gamma) = \int_{c(\gamma)} f(z)dz \in \mathbb{C}.$$

is called the period homomorphism of the form f. The integral is independent on the choice of z_0 since for $z_1 = \alpha(z_0)$, $\alpha \in \Gamma$, one has

$$\int_{\alpha(z_0)}^{\gamma(\alpha)(z_0)} f(z)dz = \int_{z_0}^{\gamma(z_0)} f(\alpha(z))\frac{dz}{j(\alpha, z)^2} = \int_{z_0}^{\gamma(z_0)} f(z)dz.$$

If all coefficients at ∞ of the corresponding Eisenstein series E belong to K, we obtain the homomorphsim

$$\pi_E : H_1(Y(\Gamma), K) \to K.$$

Assume for two cycles $\sigma_1 \in H_1(X_0(N), \mathrm{cusps}, K)$ and $\sigma_2 \in H_1(Y_0(N), K)$ and a point $p \in \sigma_1 \cap \sigma_2$ the intersection of cycles at p is transversal – tangent spaces $T_p(\sigma_1)$ and $T_p(\sigma_2)$ generate the two-dimensional tangent space $T_p(X_0(N))$. Then there is a basis for $T_p(X_0(N))$ which consists of basises of $T_p(\sigma_1)$ and $T_p(\sigma_2)$. If this basis preserves orientation, define the intersection index to be $i_p(\sigma_1, \sigma_2) = 1$, otherwise $i_p(\sigma_1, \sigma_2) = -1$. Finally, the intersetion number for two cycles is defined as

$$\sigma_1 \circ \sigma_2 = \sum_{p \in \sigma_1 \cap \sigma_2} i_p(\sigma_1, \sigma_2)$$

(here we assume that cycles intersect transversally at every point). The definition depends only on the homological classes and thus gives the pairing of homological groups H_1 [6, Ch. 0, §4].

The Poincare duality theorem [6, Ch.0, §4] states that the pairing is perfect, that is every linear functional on $H_1(Y_0(N), K)$ is given by pairing with some element of

$H_1(X_0(N), \text{cusps}, K)$. Then there is an element $\mathcal{E} \in H_1(X_0(\Gamma), \text{cusps}, K)$ such that

$$\pi_E(\sigma) = \mathcal{E} \circ \sigma$$

1.5.3 Modular symbols

The mapping $\zeta : \mathrm{SL}_2(\mathbb{Z}) \to H_1(X_0(N), \text{cusps}, \mathbb{Z})$ is defined as follows. Given any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ consider cusps $\gamma(0), \gamma(\infty) \in \mathbb{P}^1(\mathbb{Q})$. Let $\zeta(\gamma)$ be the homological class of a path in $X_0(N)$ joining these two cusps.

Given elements $\alpha, \beta \in \mathbb{H}^*$ we denote by $\{\alpha, \beta\}$ the homology class of the geodesics in $X_0(N)$ connecting $\alpha.z_0$ to $\beta.z_0$. As homologies are defined up to boundaries of $2-$simplices it follows that

$$\{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \alpha\} = 0. \tag{1.1}$$

As $\{\alpha, \alpha\} = 0$, it follows that

$$\{\alpha, \beta\} = -\{\beta, \alpha\}.$$

Also, as $X_0(N)$ is the quotient under the action of $\Gamma_0(N)$ it follows that

$$\{\alpha, \beta\} = \{\gamma(\alpha), \gamma(\beta)\}$$

for all $\gamma \in \Gamma_0(N)$.

Proposition 1.5.1. *Consider any $\alpha \in \mathbb{H}^*$ and a mapping*

$$\gamma \to \{\alpha, \gamma(\alpha)\},\ \gamma \in \Gamma_0(N).$$

This mapping is a surjective homomorphism, independent of α.

Proof. 1. The mapping is a homomorphism. Indeed, consider $\gamma_1, \gamma_2 \in \Gamma_0(N)$. Then by (1.1)

$$\{\alpha, \gamma_1\gamma_2(\alpha)\} = \{\alpha, \gamma_1(\alpha)\} + \{\gamma_1(\alpha), \gamma_1\gamma_2(\alpha)\} =$$

from group invariance

$$= \{\alpha, \gamma_1(\alpha)\} + \{\alpha, \gamma_2(\alpha)\}.$$

2. The mapping is independent of α.

   For any β we have

$$\{\alpha, \beta\} = \{\gamma(\alpha), \gamma(\beta)\}$$

   Or

$$\{\alpha, \gamma(\alpha)\} + \{\gamma(\alpha), \beta\} = \{\gamma(\alpha), \beta\} + \{\beta, \gamma(\beta)\}$$

   So,

$$\{\alpha, \gamma(\alpha)\} = \{\beta, \gamma(\beta)\}$$

3. Surjectivity of the mapping follows from surjectivity of the canonical mapping

$$\pi_1 : (X_0(N), \phi(\alpha)) \to H_1(X_0(N), \mathbb{Z})$$

   (where π_1 is the fundamental group and α is a parabolic point for $\Gamma_0(N)$) [2, Prop. 1.4]

□

The mapping ζ sends $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ into $\{\gamma(0), \gamma(\infty)\} \in H_1(X_0(N), \mathrm{cusps}, \mathbb{Z})$. A generic element of $H_1(X_0(N), \mathrm{cusps}, \mathbb{Z})$ is of the form $\{0, \gamma(0)\}$ for some $\gamma \in \Gamma_0(N)$. Surjectivity of ζ will follow once proved that any element $\{0, \gamma(0)\}$ is a linear combination of elements $\{r(0), r(\infty)\}$, where $r \in \mathrm{SL}_2(\mathbb{Z})$.

If $\gamma(0) = \infty$ then we are representing the element $\{0, \infty\}$ and r can be taken as identity matrix. So, we assume that $\gamma(0) = \frac{b}{d} \neq \infty$. Also we assume that the rational number $\frac{b}{d}$ is given in the lowest terms and $b, d > 0$.

Fix right coset representatives for $\Gamma_0(N)$, i.e. fix matrices $r_0, \ldots, r_m$ such that

$$\mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(N)r_0 \cup \ldots \cup \Gamma_0(N)r_m$$

and the union is disjoint. Write the number $\frac{b}{d}$ as a continued fraction

$$\frac{b}{d} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ldots + \frac{1}{a_n}}}}$$

Then successive approximations $a_0 = \frac{p_0}{q_0}$, $a_0 + \frac{1}{a_1} = \frac{p_1}{q_1}$, $\ldots$, $\frac{b}{d} = \frac{p_n}{q_n}$ satisfy

$$p_j q_{j-1} - q_j p_{j-1} = (-1)^{j-1}, -1 \leq j \leq n$$

(additionally we put $\frac{p_{-1}}{q_{-1}} = \frac{1}{0}$, $\frac{p_{-2}}{q_{-2}} = \frac{0}{1}$).

It follows that

$$\gamma_j = \begin{bmatrix} (-1)^{j-1}p_j & p_{j-1} \\ (-1)^{j-1}q_j & q_{j-1} \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Now

$$\{0, \frac{b}{d}\} = \{\frac{p_{-2}}{q_{-2}}, \frac{p_n}{q_n}\} =$$

$$= \sum_{j=-1}^{n} \left\{ \frac{p_{j-1}}{q_{j-1}}, \frac{p_j}{q_j} \right\} = \sum_{j=-1}^{n} \{\gamma_j(0), \gamma_j(\infty)\}.$$

As a consequence, the group $H_1(X_0(N), \text{cusps}, \mathbb{Z})$ is generated by a finite set of homologies $\{r_j(0), r_j(\infty)\}$, where $r_0, \ldots, r_m$ are right coset representatives of the group $\Gamma_0(N)$. ζ is a surjective mapping.

1.6 Projective line over the ring

1.6.1 General construction and a projective line over $\mathbb{Z}/N\mathbb{Z}$

Let R be a commutative unital ring. Denote by U the set of unities in R, i.e. U is the set of invertible elements of R. Let

$$\mathbb{P}(R) = \{(a, b) \in R^2 : aR + bR = R\}.$$

On $\mathbb{P}(R)$ we introduce equivalence relation

$$(a, b) \sim (c, d) \Leftrightarrow \exists \lambda \in U : \ c = \lambda a, d = \lambda b.$$

The projective line over R is the quotient set

$$\mathbb{P}^1(R) = \mathbb{P}(R)/\sim .$$

Let us consider an example that was already met above.

Example 1.6.1. *If R is a field, then $U = R - \{0\}$ and $\mathbb{P}(R) = R^2 - \{(0, 0)\}$. Each pair $(a, b) \in \mathbb{P}(R)$ with $b \neq 0$ is equivalent to $(\frac{a}{b}, 1)$ and such points can be identified with $\frac{a}{b} \in R$. If $b = 0$, then $a \neq 0$ and a point $(a, 0)$ is equivalent to a point $(1, 0)$ which is identified with ∞. So, a projective line over a field is a one-point extension of a field. In particular, $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$.*

Next we discuss projective lines over rings $\mathbb{Z}/N\mathbb{Z}$. Below $\bar{a}$ denotes the residue modulo N of an integer $a \in \mathbb{Z}$.

Proposition 1.6.1.

$$\mathbb{P}(\mathbb{Z}/N\mathbb{Z}) = \{(\bar{a}, \bar{b}) \in (\mathbb{Z}/N\mathbb{Z})^2 : gcd(a, b, N) = 1\}.$$

Proof. The equality $\gcd(a, b, N) = 1$ means that the only common divisors of a, b and N are ± 1. Since an integer d divides a and N if and only if it divides $a + kN$ and N, the property $\gcd(a, b, N) = 1$ depends only on the residue classes of a and b modulo N and is well-defined for $\bar{a}, \bar{b} \in \mathbb{Z}/N\mathbb{Z}$. If $(\bar{a}, \bar{b}) \in \mathbb{P}(\mathbb{Z}/N\mathbb{Z})$, then

$$\bar{1} \in \mathbb{Z}/N\mathbb{Z} = \bar{a}\mathbb{Z}/N\mathbb{Z} + \bar{b}\mathbb{Z}/N\mathbb{Z}$$

So, there is $(\bar{u}, \bar{v}) \in (\mathbb{Z}/N\mathbb{Z})^2$ such that

$$\overline{au + bv} = \bar{1}$$

It means that N divides $au + bv - 1$, i.e.

$$1 = au + bv + kN = (\bar{a} + lN)u + (\bar{b} + mN)v + kN = \bar{a}u + \bar{b}v + (lu + mv + k)N$$

for some integers k, l, m. Then every common multiple of $\bar{a}, \bar{b}$ and N divides 1. This proves that $\gcd(\bar{a}, \bar{b}, N) = 1$.

Conversely, let $\gcd(\bar{a}, \bar{b}, N) = 1$. Then

$$\bar{a}u + \bar{b}v + kN = 1$$

for some integers u, v, k. Then for every integer c

$$\bar{c} = \overline{c \cdot 1} = \overline{c(au + bv)} = \overline{a(uc) + b(vc)} \in \bar{a}\mathbb{Z}/N\mathbb{Z} + \bar{b}\mathbb{Z}/N\mathbb{Z}$$

So,

$$\bar{a}\mathbb{Z}/N\mathbb{Z} + \bar{b}\mathbb{Z}/N\mathbb{Z} = \mathbb{Z}/N\mathbb{Z}$$

and $(\bar{a}, \bar{b}) \in \mathbb{P}(\mathbb{Z}/N\mathbb{Z})$.

□

Following general approach, we define the projective line $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ as the quotient set

$$\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) = \mathbb{P}(\mathbb{Z}/N\mathbb{Z})/ \sim,$$

where the equivalence relation $\sim$ is defined on $\mathbb{P}(\mathbb{Z}/N\mathbb{Z})$ by

$$(\bar{a}_1, \bar{b}_1) \sim (\bar{a}_2, \bar{b}_2)$$

if and only if there exists a unit $\bar{\lambda} \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that

$$\bar{a}_2 = \overline{\lambda a_1},\ \bar{b}_2 = \overline{\lambda b_1},$$

$(\mathbb{Z}/N\mathbb{Z})^\times = \{\bar{\lambda} \in \mathbb{Z}/N\mathbb{Z} : \gcd(\bar{\lambda}, N) = 1\}$ is the group of units in $\mathbb{Z}/N\mathbb{Z}$.

The mapping of $SL_2(\mathbb{Z})$ into $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \to (\bar{c}, \bar{d})$$

factors through $\Gamma_0(N)$ and defines a bijection $\Gamma_0(N) \setminus SL_2(\mathbb{Z}) \to \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$

1.6.2 Structure of $\mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})$

p is a prime ≥ 3. In this subsection $\bar{a}$ denotes the residue modulo p^2 of an integer a. The full set of coset representatives for $\mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})$ is given by $p(p+1)$ pairs

$$(\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1}), \ldots, (\bar{1}, \overline{p^2 - 1}),$$

$$(\bar{p}, \bar{1}), (\overline{2p}, \bar{1}), \ldots, (\overline{(p-1)p}, \bar{1}).$$

Proposition 1.6.2. *Every $x \in \mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})$ not of the form $(\bar{1}, \overline{kp \pm 1})$, $0 \leq k \leq p^2$ can be represented in the form $x = (r \bar{-} 1, r \bar{+} 1)$ for an integer r such that p does not divide r and 4 divides $r - 1$.*

Proof. • Let $x = (\bar{0}, \bar{1})$. Since $p \geq 3$, then $\gcd(2, p^2) = 1$ and $\bar{2}$ is a unit in $\mathbb{Z}/p^2\mathbb{Z}$. $(\bar{0}, \bar{1})$ is equivalent to $(\overline{2 \cdot 0}, \overline{2 \cdot 1})$, i.e.

$$x = (\bar{0}, \bar{2}) = (\overline{r - 1}, \overline{r + 1})$$

for $r = 1$.

- Let $x = (\bar{1}, \bar{t})$ and $\bar{t} \neq \overline{kp \pm 1}$. If p divides $t-1$, then $t = kp+1$ which is not the case, so $t-1$ is a unit in $\mathbb{Z}/p^2\mathbb{Z}$. Let $v \in \mathbb{Z}$ be such that $\overline{v(t-1)} = \bar{1}$. Since $\overline{(v+p^2)(t-1)} = \overline{v(t-1)} = 1$, we can take v even (if v is odd change it to even $v+p^2$ with same property). Let $r = 1+2v$. v is even, so 4 divides $r-1$. $\overline{2v} = \overline{r-1}$ is a unit in $\mathbb{Z}/p^2\mathbb{Z}$, so

$$(\bar{1}, \bar{t}) \sim (\overline{r-1}, \overline{t(r-1)}) = (\overline{r-1}, \overline{2vt}) = (\overline{r-1}, \overline{2(v+1)}) =$$

$$= (\overline{r-1}, \overline{2v+2}) = (\overline{r-1}, \overline{r+1})$$

It remains to check that p does not divide r. If it is not the case, then $r = kp$ and

$$kp = r = 1+2v, \;\; 2v = kp-1$$

$$\bar{2} = \overline{2v(t-1)} = \overline{(kp-1)(t-1)}$$

So, p^2 divides $(kp-1)(t-1)-2 = kp(t-1)-(t+1)$. Then p divides $t+1$ and $t = kp-1$, which is impossible. p does not divide r.

- Let $x = (\overline{kp}, \bar{1})$, where $1 \leq k \leq p-1$. Since $kp-1$ is not divisible by p, $\overline{kp-1}$ is a unit in $\mathbb{Z}/p^2\mathbb{Z}$. Let $v \in \mathbb{Z}$ be such that $\overline{v(kp-1)} = \bar{1}$. We can assume that v is odd (as we can change v to $v+p^2$). Let $r = -2v-1$. From representation $r = -2(v+1)+1$ and the fact that $v+1$ is even, it follows that 4 divides $r-1$. $\overline{r+1} = \overline{-2v}$ is a unit, so

$$(\overline{kp}, \bar{1}) \sim (\overline{kp(r+1)}, \overline{r+1}) = (\overline{-2vkp}, \overline{r+1}) = (\overline{-2(v+1)}, \overline{r+1}) =$$

$$= (\overline{-2v-2}, \overline{r+1}) = (\overline{r-1}, \overline{r+1}).$$

It remains to check that p does not divide r. If it is not the case, then $r = lp$ and

$$lp = r = -1 - 2v,\ 2v = -lp - 1$$

$$\bar{2} = \overline{2v(kp-1)} = \overline{(-lp-1)(kp-1)}$$

So, p^2 divides $(-lp-1)(kp-1) - 2 = -1 + p(l - k - lkp)$. Then p divides -1 which is impossible. p does not divide r.

$\square$

Several special matrices are introduced

$$\alpha_r = \begin{pmatrix} 1 & -r \\ 0 & 2p^2 \end{pmatrix}, \beta_r = \begin{pmatrix} 1 & -r \\ 0 & p^2 \end{pmatrix}$$

$$\nabla_k = \begin{pmatrix} 1 & 1 \\ s_k p & s_k p + 2 \end{pmatrix}, \kappa_k = \begin{pmatrix} 1 + s_k p & s_k p + 3 \\ 2 s_k p & 2(s_k p + 2) \end{pmatrix}$$

where $\delta_k = \begin{cases} 1, & k\ odd \\ 0, & k\ even \end{cases}$, $s_k = k + (\delta_k - 1)p = \begin{cases} k, & k\ odd \\ k - p, & k\ even \end{cases}$.

1.7 Special values of L-functions and the function F_E

Let $f \in \mathcal{M}_2(\Gamma)$. In [5, Proposition 5.9.1] the growth of coefficients is estimated: there is a constant $C > 0$ such that for all $n \geq 1$

$$|a_n| \leq Cn \tag{1.2}$$

From this the following estimate

$$\forall \epsilon > 0 \exists C > 0 : |f(iy)| \leq C y^{-2-\epsilon} \text{ for } 0 < y < 1 \tag{1.3}$$

is derived in [7, Proposition 1].

Also, if we write $\tilde{f}(z) = f(z) - a_0(f)$, then [8, Lemma 2.1.1]

$$\exists C > 0 : |f(iy)| \le Ce^{-y/N} \text{ for } y > 1 \tag{1.4}$$

Using these estimates we can define the L-function as a series

$$L(f,s) = N^s \sum_{n=1}^{\infty} a_n(f) n^{-s}. \tag{1.5}$$

Proposition 1.7.1. *$s \to L(f,s)$ is a holomorphic function in the region $\{s : Re(s) > 2\}$.*

Proof. We must check that for $Re(s) > 2$ the series in the definition of $L(f,s)$ converges absolutely and that the convergence is uniform on compact subsets of $\{s : Re(s) > 2\}$. From (1.2) we estimate

$$\sum_{n=1}^{\infty} |a_n(f)n^{-s}| \le C \sum_{n=1}^{\infty} n|n^{-s}| = C \sum_{n=1}^{\infty} n^{1-Re(s)}$$

If $s \in K$ where K is a compact in $\{s : Re(s) > 2\}$, then we can estimate $Re(s) > c$ for some $c > 2$ and all $s \in K$. So,

$$\sum_{n=1}^{\infty} \sup_{s \in K} \left(n^{1-Re(s)} \right) \le \sum_{n=1}^{\infty} n^{1-c} < \infty$$

The latter convergence follows from $1 - c < -1$.

$\square$

By the expression (1.5) function L is defined only in the half-plane $Re(s) > 2$. We will show that it can be extended to a meromorphic function in $\mathbb{C}$ with possible poles only at $s = 0$ or $s = 2$. To do this we use the Mellin transform of the function f.

Consider the infinite vertical line $\zeta(y) = iy$, $y \ge 0$. The Mellin trasform is the integral along ζ

$$D(f,s) = \int_{\zeta} \tilde{f}(z)(Im(z))^{s-1} dz.$$

Equivalently,

$$D(f,s) = i \int_0^\infty \tilde{f}(iy) y^{s-1} dy.$$

Proposition 1.7.2. *$s \to D(f,s)$ is a holomorphic function in the region $\{s : Re(s) > 2\}$.*

Proof. We must check that for $Re(s) > 2$ the integral in the definition of $D(f,s)$ converges absolutely and that the convergence is uniform on compact subsets of $\{s : Re(s) > 2\}$. At first we observe that the integral

$$\int_1^\infty \tilde{f}(iy) y^{s-1} dy$$

converges absolutely for all values of s. Indeed, using (1.4) we estimate the integrand as

$$|\tilde{f}(iy) y^{s-1}| \leq C y^{Re(s)-1} e^{-y/N}$$

If $s \in K$ where K is a compact, then we can estimate $Re(s) \leq c$ for some $c > 0$ and all $s \in K$. So, the integrand is estimated uniformly as

$$C y^{a-1} e^{-y/N}$$

which is integrable on $(1, \infty)$.

To prove convergence of the integral

$$\int_0^1 \tilde{f}(iy) y^{s-1} dy$$

we use (1.3):

$$|\tilde{f}(iy) y^{s-1}| \leq C y^{-2-\epsilon+Re(s)-1}$$

If $Re(s) > 2 + \epsilon$, then the estimate has the form $C y^\beta$, $\beta > -1$ and the result follows from convergence of the integral

$$\int_0^1 y^\beta dy = \frac{1}{1+\beta} < \infty.$$

□

The next proposition establishes a relation between L-function attached to f and a Mellin transform of f.

Proposition 1.7.3. *For all s with $Re(s) > 2$*

$$D(f,s) = i\Gamma(s)(2\pi)^{-s}L(f,s)$$

Proof. We use the Fourier transform of f :

$$D(f,s) = i\int_0^\infty \left(\sum_{n=1}^\infty a_n(f)e^{-\frac{2\pi n}{N}y}\right)y^{s-1}dy =$$

$$= i\sum_{n=1}^\infty a_n(f)\int_0^\infty e^{-\frac{2\pi n}{N}y}y^{s-1}dy =$$

change variables $t = \frac{2\pi n}{N}y$

$$= i\sum_{n=1}^\infty a_n(f)\frac{N^s}{(2\pi n)^s}\int_0^\infty t^{s-1}e^{-t}dt = i\Gamma(s)(2\pi)^{-s}L(f,s)$$

□

Rewrite obtained relation as

$$L(f,s) = -i(2\pi)^s\frac{1}{\Gamma(s)}D(f,s).$$

The function $\frac{1}{\Gamma(s)}$ is holomorphic on $\mathbb{C}$ [9, Chapter VII, §7]. So, if we extend $D(f,s)$ to a meromorphic function with possible poles at $s=0$ and $s=2$ then we will get the needed extension of $L(f,s)$.

Consider the matrix $\sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

Proposition 1.7.4. *For all s with $Re(s) > 2$*

$$D(f,s) = -i\frac{a_0(f)}{s} + i\frac{a_0(f[\sigma]_2)}{2-s} + i\int_1^\infty \tilde{f}(iy)y^{s-1}ds - i\int_1^\infty \tilde{f}[\sigma]_2(iy)y^{1-s}dy$$

Remark 1.7.1. *Proposition 1.4 establishes the needed extensions of $D(f,s)$ as both integrals in the right side are holomorphic on $\mathbb{C}$ (proved in proposition 1.2).*

Proof. By definition of the Mellin transform

$$D(f,s) = i\int_0^\infty \tilde{f}(iy)y^{s-1}dy = i\int_1^\infty \tilde{f}(iy)y^{s-1}dy + i\int_0^1 \tilde{f}(iy)y^{s-1}dy.$$

We have to transform the second summand.

$$i\int_0^1 \tilde{f}(iy)y^{s-1}dy = i\int_0^1 (f(iy) - a_0(f))y^{s-1}dy =$$

$$= i\int_0^1 f(iy)y^{s-1}dy - ia_0(f)\int_0^1 y^{s-1}dy =$$

$$= i\int_0^1 f(iy)y^{s-1}dy - i\frac{a_0(f)}{s} =$$

change variables $u = 1/y$

$$= i\int_1^\infty f(i/u)u^{-(s+1)}du - i\frac{a_0(f)}{s} =$$

observe that $f[\sigma]_2(z) = z^{-2}f(-1/z)$ so that $f(i/u) = f(-\frac{1}{iu}) = -u^2 f[\sigma]_2(iu)$

$$= -i\int_1^\infty f[\sigma]_2(iu)u^{1-s}du - i\frac{a_0(f)}{s} =$$

$$= -i\int_1^\infty \tilde{f}[\sigma]_2(iu) - ia_0(f[\sigma]_2)\int_1^\infty u^{1-s}du - i\frac{a_0(f)}{s} =$$

$$= -i\int_1^\infty \tilde{f}[\sigma]_2(iu) + i\frac{a_0(f[\sigma]_2)}{2-s} - i\frac{a_0(f)}{s}.$$

□

Extend the defintion of a weight-2 operator to any matrix $\alpha \in GL_2(\mathbb{Q})$ with positive determinant as follows:

$$f[\alpha](z) = \det(\alpha) j(\alpha, z)^{-2} f(\alpha(z)).$$

The function $f[\alpha]$ is a weight-2 modular form with respect to a congruence subgroup $\alpha^{-1}\Gamma\alpha$. For an Eisenstein series $E \in E_2(\Gamma_0(p^2))$ the function F_E is defined in terms special values of associated L-functions:

$$F_E : \mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z}) \to K$$

$$F_E(x) = \begin{cases} \frac{1}{2\pi i}(2L(E[\alpha_r], 1) - L(E[\beta_r, 1])), \quad x = (r-1, r+1) \\ \int_0^\infty 2(2E[\nabla_k] - E[\kappa_k])dz, \quad x = (1+kp, 1) \\ -F_E((1+kp, 1)), \quad x = (kp-1, 1) \\ 0, \ x = (\pm 1, 1) \end{cases}$$

In the main result of the paper [4], the Eisenstein element $\mathcal{E}$ is found as a linear combination of modular symbols $\zeta(g)$, $g \in \mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})$ with explicit coefficients:

$$\mathcal{E} = \sum_{g \in \mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})} F_E(g)\zeta(g),$$

if E is an element of a basis for $E_2(\Gamma_0(p^2))$ given in Lemma 3.1. Though $\zeta(\gamma)$ was defined for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, it factors through $\Gamma_0(p^2)$ (orbits in $X_0(p^2)$ are $\Gamma_0(p^2)$-invariant), so ζ is defined on $\Gamma_0(p^2) \setminus \mathrm{SL}_2(\mathbb{Z}) \sim \mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})$.

Chapter 2

Intersection with $\Gamma(2)$

2.1 Cusps of $\Gamma_0(p^2)$

To describe cusps of the group $\Gamma_0(p^2)$ we find the index of $\Gamma_0(p^2)$ in $\mathrm{SL}_2(\mathbb{Z})$ and relate this subgroup to $\mathrm{SL}_2(\mathbb{Z}/p^2\mathbb{Z})$.

Let $N > 1$ be an integer. The group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is defined similarly to the modular group $\mathrm{SL}_2(\mathbb{Z})$ but with all operations taken modulo N.

Definition 2.1.1. $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ *is the set of all matrices* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, *such that* $a, b, c, d \in \mathbb{Z}/N\mathbb{Z}$ *and* $ad - bc \equiv 1 (mod\ N)$.

$\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is a group as the relation $ad - bc \equiv 1(\mathrm{mod}\ N)$ implies that $ad - bc$ and N are coprime and there is a multiplicative inverse $(ad - bc)^{-1} \in \mathbb{Z}/N\mathbb{Z}$. Then

$$\gamma^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Example 2.1.1. *For* $N = 2$ *the group* $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ *consists of* 6 *elements:*

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Proposition 2.1.1. *The mapping*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} a(mod\ N) & b(mod\ N) \\ c(mod\ N) & d(mod\ N) \end{pmatrix}$$

is a surjective homomorphism of a group $\mathrm{SL}_2(\mathbb{Z})$ *onto a group* $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Proof. The mapping is a homomorphism since addition, subtraction and multiplication commute with taking residue modulo N. Only surjectivity must be proved. Assume that

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

We will find the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$a(\text{mod } N) = a', b(\text{mod } N) = b', c(\text{mod } N) = c', d(\text{mod } N) = d'.$$

Consider several cases.

- Let $c' \neq 0$, $d' \neq 0$. Denote by g the greatest common divisor of c' and d'. From the relation $a'd' - b'c' \equiv 1(\text{ mod } N)$ it follows that g has a multiplicative inverse modulo N and thus $(g, N) = 1$. Let $P(c')$ be the set of all distinct prime multiples of c'. Every two elements of $P(c')$ are coprime and the Chinese Remainder Theorem applies: there is an integer t such that for every $p \in P(c')$, $p|g$

  $$t \equiv 1(\text{ mod } p)$$

  and for every $p \in P(c')$, $p \not| g$

  $$t \equiv 0(\text{ mod } p).$$

  Integers c' and $d' + tN$ are coprime. Indeed, assume that there is a prime number

$p > 1$ such that $p|c'$ and $p|(d' + tN)$. Then $p \in P(c')$. There are two possibilities.

If $p|g$, then $p|d'$. So, $p|(tN)$. But $(g, N) = 1$ hence $p \not| N$ and $p|t$ which is impossible as $t \equiv 1(\mod p)$.

The second possibility is $p \not| g$. Then $p|t$ and $p|d'$. From $p|c'$ and $p|d'$ it follows that $p|g$ which is not the case.

- Let $c' \neq 0$, $d' = 0$. We repeat considerations of previous case substituting g with c'. From the relation $-b'c' \equiv 1(\mod N)$ it follows that $(c', N) = 1$. Let $P(c')$ be the set of all distinct prime multiples of c'. By the Chinese Remainder Theorem there is an integer t such that for every $p \in P(c')$,

$$t \equiv 1(\mod p).$$

Integers c' and $tN(= d' + tN)$ are coprime. Indeed, assume that there is a prime number $p > 1$ such that $p|c'$ and $p|tN$. Then $p \in P(c')$ and $p \not| t$. But from $(c', N) = 1$ it follows that $p \not| N$ which is impossible.

- If $c' = 0$, $d' \neq 0$, then we interchange roles of c' and d' and obtain coprime integers $sN(= c' + sN)$ and d'.

In any case, there are coprime integers $c' + sN$ and $d' + tN$. There are integers k, l such that

$$k(c' + sN) + l(d' + tN) = 1$$

On the other hand the condition $a'd' - b'c' \equiv 1(\mod N)$ implies $a'(d' + tN) - b'(c' + sN) \equiv 1(\mod N)$ and the existence of an integer m such that

$$a'(d' + tN) - b'(c' + sN) + mN = 1.$$

Then

$$(a' + lmN)(d' + tN) - (b' - kmN)(c' + sN) =$$

$$= a'(d' + tN) - b'(c' + sN) + mN(l(d' + tN) + k(c' + sN)) = 1 - mN + mN = 1$$

and

$$\begin{pmatrix} a' + lmN & b' - kmN \\ c' + sN & d' + tN \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

is the needed matrix.

□

Corollary 2.1.1. *If N_1 divides N_2 then the mapping*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} a(mod\ N_1) & b(mod\ N_1) \\ c(mod\ N_1) & d(mod\ N_1) \end{pmatrix}$$

is a surjective homomorphism of a group $\mathrm{SL}_2(\mathbb{Z}/N_2\mathbb{Z})$ onto a group $\mathrm{SL}_2(\mathbb{Z}/N_1\mathbb{Z})$.

When $N = p$ is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field. Consider the group $GL_2(\mathbb{Z}/p\mathbb{Z})$ of all 2×2 invertible matrices over $\mathbb{Z}/p\mathbb{Z}$. As $\mathbb{Z}/p\mathbb{Z}$ is a field, invertibility of a matrix γ is equivalent to the condition $\det \gamma \neq 0$.

Proposition 2.1.2. *The order of $GL_2(\mathbb{Z}/p\mathbb{Z})$ is $p(p-1)(p^2-1)$.*

Proof. We will construct all matrices $GL_2(\mathbb{Z}/p\mathbb{Z})$. There are p^2 possible 2-rows from elements of $\mathbb{Z}/p\mathbb{Z}$. The first row can be any nonzero row, i.e. there are $p^2 - 1$ possibilities for the first row. The second row can be any row but the multiple of the first row, i.e. given the first row there are $p^2 - p$ possibilities for the second row and

$$|GL_2(\mathbb{Z}/p\mathbb{Z})| = (p^2 - 1)(p^2 - p) = p(p-1)(p^2 - p)$$

□

Proposition 2.1.3. *The order of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is $p^3(1 - \frac{1}{p^2})$.*

Proof. The mapping

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to ad - bc$$

is a homomorphism of the group $GL_2(\mathbb{Z}/p\mathbb{Z})$ onto the multiplicative group $(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\} = \{1, 2, \ldots, p-1\}$. Its kernel consists of matrices with determinant 1, i.e. $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. It follows that the quotient $GL_2(\mathbb{Z}/p\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ and

$$|GL_2(\mathbb{Z}/p\mathbb{Z})| = |\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})| \cdot (p-1)$$

We find that the order of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is $\frac{p(p-1)(p^2-1)}{p-1} = p^3(1-\frac{1}{p^2})$. □

Consider the mapping

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} a(\text{mod } p) & b(\text{mod } p) \\ c(\text{mod } p) & d(\text{mod } p) \end{pmatrix}$$

of the group $\mathrm{SL}_2(\mathbb{Z}/p^2\mathbb{Z})$ onto the group $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ (it is defined in corollary 1.1). The kernel of this mapping consists of matrices that are equivalent to the identity matrix modulo p, i.e. it consists of matrices of the form

$$\begin{pmatrix} 1+pa & pb \\ pc & 1+pd \end{pmatrix}$$

where $a, b, c, d \in \mathbb{Z}/p\mathbb{Z}$ and $a + d \equiv 0$ modulo p. Moreover, such representation is unique. Now, for (a, b, c) there are p^3 choices and d is determined from $a + d \equiv 0$. So, the kernel consists of p^3 elements, and the order of $\mathrm{SL}_2(\mathbb{Z}/p^2\mathbb{Z})$ is

$$p^3 \cdot p^3(1-p^{-2}) = p^6\left(1-\frac{1}{p^2}\right)$$

Remark 2.1.1. *Obtained result is generalized to all N as follows. The order of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is*

$$N^3 \prod_{p|N, p \ prime} \left(1-\frac{1}{p^2}\right)$$

By $\Gamma_0(p^2) \setminus \mathrm{SL}_2(\mathbb{Z})$ we denote the family of right cosests $\{\Gamma_0(p^2)\gamma : \gamma \in \mathrm{SL}_2(\mathbb{Z})\}$.

Two cosets are either disjoint or equal and

$$\Gamma_0(p^2)\alpha = \Gamma_0(p^2)\beta \Leftrightarrow \alpha\beta^{-1} \in \Gamma_0(p^2).$$

We compute the order of $\Gamma_0(p^2) \setminus \mathrm{SL}_2(\mathbb{Z})$ in three steps.

1. Denote by $\Gamma(p^2)$ the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ that are equivalent to identity modulo p^2 (principal congruence subgroup). Then

$$|\Gamma(p^2) \setminus \mathrm{SL}_2(\mathbb{Z})| = p^6\left(1 - \frac{1}{p^2}\right)$$

   Indeed, two matrices α, β have the same cosets if and only if $\alpha(\bmod p^2) = \beta(\bmod p^2)$ (where taking residue is understood element-wise). So, the quotient $\Gamma(p^2) \setminus \mathrm{SL}_2(\mathbb{Z})$ is naturally isomorphic to $\mathrm{SL}_2(\mathbb{Z}/p^2\mathbb{Z})$.

2. Denote by $\Gamma_1(p^2)$ the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ that are equivalent to the matrix $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ modulo p^2. Then

$$|\Gamma_1(p^2) \setminus \mathrm{SL}_2(\mathbb{Z})| = p^6\left(1 - \frac{1}{p^2}\right)$$

   Indeed, the mapping

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to b$$

   is a homomorphic surjection of $\Gamma_1(p^2)$ to the additive group $\mathbb{Z}/p^2\mathbb{Z}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} \to$$

$$\to ab' + bd' \equiv b + b' (\bmod p^2)$$

Its kernel is $\Gamma(p^2)$ as $a \equiv d \equiv 1$ and $c \equiv 0$ by definition of $\Gamma_1(p^2)$. So, the index of $\Gamma(p^2)$ in $\Gamma_1(p^2)$ is p^2 and

$$|\Gamma_1(p^2) \setminus \mathrm{SL}_2(\mathbb{Z})| = \frac{|\Gamma(p^2) \setminus \mathrm{SL}_2(\mathbb{Z})|}{p^2} = p^4\left(1 - \frac{1}{p^2}\right)$$

3. The mapping

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to d$$

is a homomorphic surjection of $\Gamma_0(p^2)$ to the multiplicative group $(\mathbb{Z}/p^2\mathbb{Z}) \setminus \{0\}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} \to$$

$$\to cb' + dd' \equiv dd' (\mod p^2)$$

Its kernel is $\Gamma_1(p^2)$, so the index of $\Gamma_1(p^2)$ in $\Gamma_0(p^2)$ is $p^2 - p$.

$$|\Gamma_0(p^2) \setminus \mathrm{SL}_2(\mathbb{Z})| = \frac{|\Gamma_1(p^2) \setminus \mathrm{SL}_2(\mathbb{Z})|}{p^2 - p} = p^4 \frac{p^2 - 1}{p^2(p^2 - p)} = p^2 + p.$$

$$[\Gamma_0(N) : \mathrm{SL}_2(\mathbb{Z})] = N \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

In the case $N = p^2$, the index is

$$p^2\left(1 + \frac{1}{p}\right) = p(p+1).$$

Now we can find a complete set of representatives for $\Gamma_0(p^2)$ in $\mathrm{SL}_2(\mathbb{Z})$.

Lemma 2.1.1. *[4, Lemma 2.1] Matrices*

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \alpha_t = \begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}, 0 \le t \le p^2 - 1,$$

$$\beta_{kp} = \begin{pmatrix} 1 & 0 \\ kp & 1 \end{pmatrix}, 1 \leq k \leq p-1$$

form a complete set of representatives for $\mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})$.

Proof. There are

$$1 + p^2 + p - 1 = p(p+1)$$

matrices listed, so one only must check that neither two of them are equivalent modulo $\Gamma_0(p^2)$. But if $0 \leq t < s \leq p^2 - 1$, then

$$\alpha_t \alpha_s^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix} \begin{pmatrix} s & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ s-t & 1 \end{pmatrix} \notin \Gamma_0(p^2)$$

as $1 \leq s - t < p^2$.

If $0 \leq t \leq p^2 - 1$ and $1 \leq k \leq p - 1$, then

$$\alpha_t \beta_{kp}^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -kp & 1 \end{pmatrix} = \begin{pmatrix} kp & -1 \\ 1 - tkp & t \end{pmatrix} \notin \Gamma_0(p^2)$$

as $p \not| 1$

If $1 \leq k < l \leq p - 1$, then

$$\beta_{lp} \beta_{kp}^{-1} = \begin{pmatrix} 1 & 0 \\ lp & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -kp & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ (l-k)p & 1 \end{pmatrix} \notin \Gamma_0(p^2)$$

as $p \not| (l - k)$.

□

Lemma 2.1.2. *[4, Lemma 2.2] Cusps of* $\Gamma_0(p^2)$ *are* $\{0, \infty, \frac{1}{p}, \ldots, \frac{1}{(p-1)p}\}$.

Proof. Let P be the parabolic subgroup of $\mathrm{SL}_2(\mathbb{Z})$,

$$P = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \middle| \, n \in \mathbb{Z} \right\}.$$

By [5, Prop. 3.8.5] there is a bijection between the double coset space $\{\Gamma_0(p^2)\gamma P | \gamma \in \mathrm{SL}_2(\mathbb{Z})\}$ and the set of cusps of $\Gamma_0(p^2)$, given by

$$\Gamma_0(p^2)\gamma P \to \Gamma_0(p^2)\gamma(\infty).$$

We compute this mapping for a complete set of representatives found in Lemma 2.1.

For identity matrix:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}(\infty) = \frac{z}{1}\bigg|_{z=\infty} = \infty$$

For α_t, $0 \leq t \leq p^2 - 1$:

$$\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}(\infty) = \frac{-1}{z+t}\bigg|_{z=\infty} = 0$$

For β_{kp}, $1 \leq k \leq p - 1$:

$$\begin{pmatrix} 1 & 0 \\ kp & 1 \end{pmatrix}(\infty) = \frac{z}{kpz+1}\bigg|_{z=\infty} = \frac{1}{kp}$$

□

2.2 Subgroup Γ

A subgroup Γ is defined as the intersection of two congruence subgroups

$$\Gamma = \Gamma_0(p^2) \cap \Gamma(2)$$

It is a congruence subgroup as it contains, e.g. $\Gamma(2p^2)$. X_Γ is the corresponding modular curve and $\pi_\Gamma(z) = \Gamma z$ is the canonical surjection $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) \to X_\Gamma$.

Lemma 2.2.1. *[4, Lemma 2.3] Matrices*

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \gamma_k = \begin{pmatrix} (s_k p)^3 & -1 + s_k^2 p^2 \\ 1 + s_k^2 p^2 & p s_k \end{pmatrix}, 1 \leq k \leq p-1,$$

$$\beta_{t+\delta_t p^2} = \begin{pmatrix} 1 & 0 \\ (t+\delta_t p^2)p & 1 \end{pmatrix}, 0 \leq t \leq p^2 - 1$$

form a complete set of representatives for $\mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})$.

Proof. There are $1 + p - 1 + p^2 = p(p+1)$ matrices listed, neither two of them are congruent modulo $\Gamma_0(p^2)$. Indeed,

$$\gamma_k \gamma_l^{-1} = \begin{pmatrix} (s_k p)^3 & -1 + s_k^2 p^2 \\ 1 + s^2 k p^2 & p s_k \end{pmatrix} \begin{pmatrix} p s_l & 1 - s_l^2 p^2 \\ -1 - s_l^2 p^2 & (s_l p)^3 \end{pmatrix}$$

and the lower left element is

$$p s_l + p^3 s_k^2 s_l - p s_k - p^3 s_l^2 s_k \equiv p(s_l - s_k) \pmod{p^2}.$$

The latter expression is not divisible by p^2 as $s_k \not\equiv s_l$ modulo p.

Further,

$$\beta_{t+\delta_t p^2} \gamma_l^{-1} = \begin{pmatrix} 1 & 0 \\ (t+\delta_t p^2)p & 1 \end{pmatrix} \begin{pmatrix} p s_l & 1 - s_l^2 p^2 \\ -1 - s_l^2 p^2 & (s_l p)^3 \end{pmatrix}$$

and the lower left element is

$$p^2 s_l (t + \delta_t p^2) - 1 - s_l^2 p^2 \equiv -1 \pmod{p^2}.$$

The latter expression is not divisible by p^2.

Finally,

$$\beta_{t+\delta_t p^2}\gamma_{l+\delta_l p^2}^{-1} = \begin{pmatrix} 1 & 0 \\ (t+\delta_t p^2)p & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ (-l-\delta_l p^2)p & 1 \end{pmatrix}$$

and the lower left element is

$$p(t - l + p^2(\delta_t - \delta_l)) \equiv p(t-l) \pmod{p^2}.$$

The latter expression is not divisible by p^2 as $t \not\equiv l$ modulo p.

□

Lemma 2.2.1 differs from the lemma 2.1.1, as it gives representatives from the subgroup $\Gamma(2)$. As a corollary, there is an isomorphism between a subgroup

$$\Gamma \setminus \Gamma(2) = \Gamma_0(p^2) \cap \Gamma(2) \setminus \Gamma(2)$$

and $\mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z}) \sim \Gamma_0(p^2) \setminus \mathrm{SL}_2(\mathbb{Z})$.

Lemma 2.2.2. *[4, Lemma 2.4] The mapping*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} c & d \end{pmatrix}$$

is an isomorphism betwenn $\Gamma \setminus \Gamma(2)$ *and* $\mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})$.

Proof. The map is injective by definition of equality in $\mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})$ since $\Gamma-$equivalent matrices have rows that differ by a unity in $\mathbb{Z}/p^2\mathbb{Z}$. By the lemma 2.3 cardinalities of sets $\Gamma \setminus \Gamma(2)$ and $\mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})$ coincide, so the mapping is an isomorphism.

□

2.3 Relative homologies for X_Γ

Since Γ is a subgroup of $\Gamma(2)$, the mapping

$$\pi_0 : \Gamma \setminus \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) \to \Gamma(2) \setminus \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$$

given by $\pi_0(\Gamma z) = \Gamma(2)z$ is well-defined. The group $\Gamma(2)$ has three cusps [5, §3.8]. As a representatives one can take $\Gamma(2)0$, $\Gamma(2)1$ and $\Gamma(2)\infty$. Indeed, assume that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)$. Then a and d are odd, b and c are even. The relation

$$\frac{a \cdot 0 + b}{c \cdot 0 + d} = 1$$

is impossible since $b \neq d$. The relation

$$\frac{a \cdot \infty + b}{c \cdot \infty + d} = 1$$

is impossible since $a \neq c$. The relation

$$\frac{a \cdot \infty + b}{c \cdot \infty + d} = 0$$

is impossible since $a \neq 0$.

Preimages of cusps for $\Gamma(2)$ in X_Γ are given by

$$P_- = \pi_0^{-1}(\Gamma(2)1), P_+ = \pi_0^{-1}(\{\Gamma(2)0, \Gamma(2)\infty\}).$$

Following two properties of relative homology groups $H_1(X_\Gamma - P_-, P_+, K)$ and $H_1(X_\Gamma - P_+, P_-, K)$ were proved in [1]. They are stated in terms of two operators:

for every $g \in \Gamma \setminus \Gamma(2)$ the homological class in X_Γ of a geodesics joining $g0$ and $g\infty$ is denoted by $[g]^0$ and the homological class in X_Γ of a geodesics joining $g1$ and $g(-1)$ is denoted by $[g]_0$.

Theorem 2.3.1. *[1, Th. 5] Mapping $g \to [g]_0$ extends to an isomorphism*

$$\zeta_0 : K^{\Gamma\backslash\Gamma(2)} \to H_1(X_\Gamma - P_+, P_-, K).$$

Mapping $g \to [g]^0$ extends to an isomorphism

$$\zeta^0 : K^{\Gamma\backslash\Gamma(2)} \to H_1(X_\Gamma - P_-, P_+, K).$$

Remark. The theorem states that the relative homology group $H_1(X_\Gamma - P_+, P_-, K)$ consists of $K-$linear combinations of paths joining cusps from P_- and the relative homology group $H_1(X_\Gamma - P_-, P_+, K)$ consists of $K-$linear combinations of paths joining cusps from P_+.

Theorem 2.3.2. *[1, Th. 6] For any $g, h \in \Gamma(2)$ the intersection pairing of $[g]_0$ and $[h]^0$ is given by*

$$[g]_0 \circ [h]^0 = \begin{cases} 1, & \Gamma g = \Gamma h \\ 0, & \Gamma g \cap \Gamma h = \emptyset \end{cases}$$

The structure of a set P_- can be specified via Lemma 2.2.1.

Lemma 2.3.1. *[4, Lemma 2.7] Every element in P_- is equal to Γk for some*

$$k \in \left\{1, \frac{1}{p^2}, \frac{1}{s_p}, \ldots, \frac{1}{s_{(p-1)p}}\right\}$$

Proof. The set P_- consists of cusps in Γ that equivalent to 1 modulo $\Gamma(2)$, i.e. cusps of the form $\Gamma\theta 1$. For the complete set of representatives we take matrices from Lemma 2.3. Then all of them except β_j with $j+1$ divisible by p give the same cusp.

□

Let $\pi : \Gamma \setminus \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) \to X_0(p^2)$ be the mapping

$$\pi(\Gamma z) = \Gamma_0(p^2)z$$

and let $\pi' : \Gamma \setminus \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) \to X_0(p^2)$ be the mapping

$$\pi(\Gamma z) = \Gamma_0(p^2)\frac{z+1}{2}.$$

These mappings will allow to transfer the Eisenstein element from the modular curve X_Γ to the modular curve $X(\Gamma_0(p^2))$.

Proposition 2.3.1. *π' is well-defined.*

Proof. Assume that $\Gamma z_1 = \Gamma z_2$. Then there exists $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$ such that

$$\frac{az_1+b}{cz_1+d} = z_2.$$

Condition $\gamma \in \Gamma = \Gamma_0(p^2) \cap \Gamma(2)$ means that $a \equiv d \equiv 1 \pmod 2$, $b \equiv c \equiv 0 \pmod 2$ and $p^2|c$. Consider matrix $\sigma = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Then

$$z_2 + 1 = \sigma(z_2) = \sigma\gamma(z_1) = \sigma\gamma\sigma^{-1}(z_1+1).$$

We compute the product

$$\sigma\gamma\sigma^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a+c & b+d-a-c \\ c & d-c \end{bmatrix}$$

Observe that $b+d-a-c \equiv 0+1-1-0 = 0 \pmod 2$, so that the matrix

$$\tilde{\gamma} = \begin{bmatrix} a+c & \frac{b+d-a-c}{2} \\ 2c & d-c \end{bmatrix} \in \Gamma_0(p^2)$$

For this matrix

$$\tilde{\gamma}\frac{z_1+1}{2} = \frac{(a+c)\frac{z_1+1}{2} + \frac{b+d-a-c}{2}}{2c\frac{z_1+1}{2} + d - c} = \frac{1}{2}\frac{(a+c)(z_1+1) + (b+d-a-c)}{c(z_1+1)+d-c} =$$

$$= \frac{1}{2}\sigma\gamma\sigma^{-1}(z_1+1) = \frac{z_2+1}{2}$$

Hence, $\Gamma_0(p^2)z_1 = \Gamma_0(p^2)z_2$.

$\square$

From the explicit form of local coordinates in a neighborhood of any cusp in P_- [5, §2.2] one can deduce the next result.

Lemma 2.3.2. *[4, Lemma 2.8] For any rational function $f : X_0(p^2) \to \mathbb{C}$ the function $\frac{(f\circ\pi)^2}{f\circ\pi'}$ has no zeroes or poles in P_-.*

Proof. Local coordinates around cusps $\Gamma_0(p^2)0$, $\Gamma_0(p^2)\infty$, $\Gamma_0(p^2)\frac{s}{tp}$ are given by mappings $q_0(z) = e^{2\pi i \frac{1}{-p^2 z}}$, $q_\infty(z) = e^{2\pi i z}$, $q_{s/tp}(z) = e^{2\pi i \frac{z}{s(-tpz+s)}}$ (local coordinates were introduced in section 1.3).

Local coordinates around cusps $\Gamma 1$, $\Gamma\frac{1}{p^2}$, $\Gamma\frac{1}{s_k p} \in P_-$ on the curve X_Γ are given by mappings $q_1(z) = e^{2\pi i \frac{z}{2(-z+1)}}$, $q_\infty(z) = e^{2\pi i \frac{1}{2(-p^2 z+1)}}$, $q_{1/s_z p}(z) = e^{2\pi i \frac{z}{2(-s_k pz+1)}}$.

It follows from shift invariance that

$$q_0(\pi z) = e^{2\pi i \frac{1}{-p^2 z}} = e^{2\pi i \frac{1}{p^2(-z+1)}} = q_1^2(z)$$

and

$$q_0(\pi' z) = e^{2\pi i \frac{2}{-p^2(z+1)}} = q_1^4(z).$$

For any analytic function f the order of $f\circ\pi'$ at $\Gamma 1$ coincides with the order of $(f\circ\pi)^2$ and the ratio $\frac{(f\circ\pi)^2}{f\circ\pi'}$ has no zeroes or poles.

Further, at a point $\Gamma\frac{1}{p^2}$ relations

$$q_{1/p^2}(\pi z) = q_{1/p^2}^2(z), q_{1/p^2}(\pi' z) = q_{1/p^2}^4(z)$$

imply that for any analytic function f the order of $f\circ\pi'$ at $\Gamma\frac{1}{p^2}$ coincides with the order of $(f\circ\pi)^2$ and the ratio $\frac{(f\circ\pi)^2}{f\circ\pi'}$ has no zeroes or poles.

Finally,

$$q_{\frac{s_k}{(1+s_k p)}}(\pi' z) = q^2_{\frac{s_k}{(1+2s_k p)p}}(\pi z)$$

and for any analytic function f the order of $f \circ \pi'$ at $\Gamma_{\frac{1}{s_k p}}$ coincides with the order of $(f \circ \pi)^2$ and the ratio $\frac{(f \circ \pi)^2}{f \circ \pi'}$ has no zeroes or poles.

$\square$

Chapter 3

Eisenstein series for $\Gamma_0(p^2)$

3.1 Basic Eisenstein series

A Dirichlet character modulo N is a mapping $\phi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ which is a multiplicative homomorphism of a group of units modulo N into the group of non-zero complex numbers, i.e. $\phi(a \cdot b) = \phi(a)\phi(b)$ for all $a, b \in: (\mathbb{Z}/N\mathbb{Z})^*$. A Dirichlet character ϕ is non-trivial if $\phi(a) \neq 1$ for all a. If M divides N then any Dirichlet character ϕ modulo M induces a Dirichlet character ψ modulo N by the rule

$$\psi(a) = \phi(a \bmod M).$$

A Dirichlet character is primitive if it is not induced by a Dirichlet character of a smaller modulus.

Every Dirichlet character ϕ defines an eigenspace of the space of modular forms. The $\phi-$eigenspace is defined by

$$\mathcal{M}_k(N, \phi) = \{f \in \mathcal{M}_k(\Gamma_1(N))|\ f[\gamma]_k = \phi(d_\gamma)f \text{ for all } \gamma \in \Gamma_0(N)\},$$

where $\gamma = \begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix}$.

In particular, $\mathcal{M}_k(\Gamma_0(N))$ is an eigenspace corresponding to the trivial character,

$\mathcal{M}_k(\Gamma_0(N)) = \mathcal{M}_2(N,1)$.

Consider the Eisenstein series

$$E_2'(\tau) = -\frac{1}{24} + \sum_{n\geq 1} \sigma_1(n) q^n$$

where $\sigma_1(n) = \sum_{m|n} m$.

Let $A_{p^2,2}$ be the set of all triples (ϕ, ψ, t), where ϕ and ψ are primitive Dirichlet characters modulo u and v such that $\phi\psi = 1$, and $1 < tuv|p^2$. Possible cases are the following:

- $u = v = p$ and $t = 1$. The corresponding Eisenstein series is

$$E_2^{\phi,\bar{\phi}}(\tau) = \sum_{n\geq 1} \sigma_1^{\phi,\bar{\phi}}(n) q^n, \;\; q = e^{2\pi i \tau}.$$

  $\sigma_1^{\phi,\bar{\phi}}(n) = \sum_{m|n} \phi(\frac{n}{m})\phi(m)m$.

- $u = v = 1$ and $t = p$. The corresponding Eisenstein series is

$$E_1(\tau) = E_2'(\tau) - pE_2'(p\tau).$$

- $u = v = 1$ and $t = p^2$. The corresponding Eisenstein series is

$$E_2(\tau) = E_2'(\tau) - p^2 E_2'(p^2\tau).$$

A specification of [5, Th. 4.6.2.] to the case $N = p^2$ implies that the series $E_1, E_2, E_2^{\phi,\bar{\phi}}$ for all non-trivial Dirichlet characters modulo p form a basis for $E_2(\Gamma_0(p^2))$. Using this result period homomorphism is computed for basic Eisenstein series and the answer is given in terms of function F_E.

3.2 Divisors

For any compact Riemann surface X a divisor is a formal sum of integer multiples of points of X,

$$D = \sum_{x \in X} n_x x,$$

where only finitely many coefficients $n_x \neq 0$. Divisors form an Abelian group $Div(X)$. Every nonzero meromorphic function f on X defines a divisor

$$div(f) = \sum_{x} \nu_x(f) x,$$

where $\nu_x(f)$ is the order of x (as a zero or a pole of f). By $Div^0(X)$ we denote the subgroup of all divisors of meromorphic functions.

By [8, §1.8] the space $E_2(\Gamma_0(N))$ is isomorphic to the abelian group $Div^0(\text{cusps})$ (viewed as a K-module). The isomorphism is given by

$$\delta(E) = \sum_{x \in \text{cusps}(\Gamma_0(p^2))} e_{\Gamma_0(p^2)}(x) a_0(E[x])\{x\},$$

where $e_{\Gamma_0(p^2)}(x)$ is a ramification degree of a canonical mapping $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) \to X_0(p^2)$ at a point x.

3.3 Properties of π_E

The Dedekind sum of integers u, v is given by

$$S(u,v) = \sum_{r=1}^{v-1} \frac{r}{v}\left(\frac{ur}{v} - \left[\frac{ur}{v}\right] - \frac{1}{2}\right).$$

Then for the Eisenstein series E_2 and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p^2)$

$$\frac{1}{\pi i} L\left(E_2 \left[\begin{pmatrix} 1 & -d \\ 0 & c \end{pmatrix} \right], 1 \right) = -sgn(c)(S(d,|c|) - S(d,|c|/p^2))$$

This value of an $L-$function is connected to the $\pi_E(\gamma)$ by [8]

$$\pi_E(\gamma) = \begin{cases} \frac{a+d}{c} a_0(E) - \frac{1}{2\pi i} L(E_2[\begin{pmatrix} 1 & -d \\ 0 & c \end{pmatrix}], 1), & c \neq 0 \\ \frac{b}{d} a_0(E), & c = 0 \end{cases}$$

Chapter 4

Eisenstein element

4.1 Eisenstein element for X_Γ

For an Eisenstein series $E \in E_2(\Gamma_0(p^2))$ the function $\psi_E(c) = \int_c k^*(\omega_E)$ is the integral along $c \in H_1(X_\Gamma - P_+, P_-, K)$ of a logarithmic derivative of a function $\frac{(\lambda_E \circ \pi)^2}{\lambda_E \circ \pi'}$ where the logarithmic derivative of $\lambda_E : X_0(p^2) \to \mathbb{C}$ is equal to $2\pi i \omega_E = 2\pi i E(z)dz$. There exist an Eisenstein element $\mathcal{E}_0 \in H_1(X_\Gamma - P_-, P_+, K)$ such that

$$\mathcal{E}_0 \circ c = \psi_E(c).$$

By Theorem 2.3.1 this element is a sum of basis elements

$$\mathcal{E}_0 = \sum_{g \in \mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})} F_0(g)\zeta^0(g).$$

In fact, coefficients $F_0(g)$ are given by the function F_E.

Lemma 4.1.1. *[4, Lemma 4.1] For every* $g \in \mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})$

$$\psi_E(\zeta_0(g)) = F_E(g)$$

Proof. For each $x \in \mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})$ we compute the value of $\psi_E(\zeta_0(x))$. Points of the projective line are classified along the lines of the proposition 1.6.2.

- Case $x = (\overline{r-1}, \overline{r+1})$ for some $r \in \mathbb{Z}$ such that p does not divide r and 4 divides $r-1$ (in particular, r is odd). r is coprime with $4p^2$ and there exists an integer $s \in \mathbb{Z}$ such that $4p^2$ divides $rs-1$. Consider matrix

$$V(r,s) = \begin{bmatrix} \frac{r-3}{2} & \frac{r-1}{2} \\ \frac{1-r}{2} & \frac{-1-r}{2} \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{s-3}{2} & \frac{s-1}{2} \\ \frac{1-s}{2} & \frac{-1-s}{2} \end{bmatrix}$$

4 divides $r-1$, hence $\frac{r-1}{2}$ is even, $\frac{r-3}{2} = \frac{r-1}{2} - 1$, $\frac{-1-r}{2} = -1 - \frac{r-1}{2}$ are odd. Matrix

$$g = \begin{bmatrix} \frac{r-3}{2} & \frac{r-1}{2} \\ \frac{1-r}{2} & \frac{-1-r}{2} \end{bmatrix} \in \Gamma(2).$$

Further,

$$g(-1) = \frac{3-r+r-1}{r-1-1-r} = -1$$

and

$$V(r,s)(-1) = \begin{bmatrix} \frac{r-3}{2} & \frac{r-1}{2} \\ \frac{1-r}{2} & \frac{-1-r}{2} \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} (-1) = \begin{bmatrix} \frac{r-3}{2} & \frac{r-1}{2} \\ \frac{1-r}{2} & \frac{-1-r}{2} \end{bmatrix} 1 = g(1)$$

By definition of ψ_E,

$$\psi_E(\zeta_0(x)) = \int_{g(1)}^{g(-1)} \left(2E(z)dz - E\left(\frac{z+1}{2}\right)d\left(\frac{z+1}{2}\right)\right) =$$

$$= \int_{V(r,s)(-1)}^{-1} \left(2E(z)dz - E\left(\frac{z+1}{2}\right)d\left(\frac{z+1}{2}\right)\right) =$$

Introduce matrix $h = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$

$$= 2\int_{V(r,s)(-1)}^{-1} E(z)dz - \int_{V(r,s)(-1)}^{-1} E(h(z))dh(z) =$$

$$= 2\int_{V(r,s)(-1)}^{-1} E(z)dz - \int_{hV(r,s)(-1)}^{h(-1)} E(z)dz =$$

$$= 2\int_{V(r,s)(-1)}^{-1} E(z)dz - \int_{hV(r,s)h^{-1}(h(-1))}^{h(-1)} E(z)dz = -2\pi_E(V(r,s)) + \pi_E(hV(r,s)h^{-1})$$

To express values of π_E in terms of $L-$functions, we will use the Atkin-Lehner involution law

$$\pi_E \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \pi_E \begin{bmatrix} a & c/p^2 \\ p^2 b & d \end{bmatrix}$$

By proposition 3.2 the mapping $\pi_E : \Gamma_0(p^2) \to \mathbb{C}$ is a homeomorphism. The matrix $V(r,s) \in \Gamma_0(p^2)$ (its left lower element is $\frac{rs-1}{2}$). Consider matrices $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$. Both are in $\Gamma_0(p^2)$ and they are inverses one to another, so

$$\pi_E \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \pi_E \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = 1$$

and

$$\pi_E(V(r,s)) = \pi_E \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \pi_E \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \pi_E(V(r,s)) =$$

$$= \pi_E \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} V(r,s) \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} =$$

$$= \pi_E \begin{bmatrix} s & 2 \\ \frac{rs-1}{2} & r \end{bmatrix} = \pi_E \begin{bmatrix} s & \frac{rs-1}{2p^2} \\ 2p^2 & r \end{bmatrix} = \frac{s+r}{2p^2} a_0(E) - \frac{1}{2\pi i} L\Big(E \begin{bmatrix} 1 & -r \\ 0 & 2p^2 \end{bmatrix}, 1\Big)$$

Similarly,

$$\pi_E(hV(r,s)h^{-1}) = \pi_E \begin{bmatrix} s & 1 \\ rs-1 & r \end{bmatrix} =$$

$$= \pi_E \begin{bmatrix} s & \frac{rs-1}{p^2} \\ p^2 & r \end{bmatrix} = \frac{s+r}{p^2} a_0(E) - \frac{1}{2\pi i} L\Big(E \begin{bmatrix} 1 & -r \\ 0 & p^2 \end{bmatrix}, 1\Big)$$

So,

$$F_E(x) = \frac{1}{2\pi i}\left(2L\left(E\begin{bmatrix}1 & -r\\ 0 & 2p^2\end{bmatrix}, 1\right) - L\left(E\begin{bmatrix}1 & -r\\ 0 & p^2\end{bmatrix}, 1\right)\right)$$

- Let $x = (\overline{1}, \overline{(-k)p+1}) = (\overline{kp+1}, \overline{1})$ (the last equality follow from the fact that $\overline{kp+1}$ is an inverse to $\overline{(-k)p+1}$). In this case x corresponds to the matrix

$$\beta_{1+s_kp} = \begin{bmatrix}1 & 0\\ 1+s_kp & 1\end{bmatrix}$$

where $s_k = k$ if k is odd, and $s_k = k - p$ when k is even. Now

$$\beta_{1+s_kp}1 = \frac{1}{2+s_kp}, \beta_{1+s_kp}(-1) = \frac{1}{s_kp},$$

and

$$\psi_E(\zeta_0(x)) = \int_{\beta_{1+s_kp}1}^{\beta_{1+s_kp}(-1)} \left(2E(z)dz - E\left(\frac{z+1}{2}\right)d\left(\frac{z+1}{2}\right)\right) =$$

introduce a function $f(z) = 2E(z) - \frac{1}{2}E(\frac{z+1}{2})$

$$= \int_{\frac{1}{2+s_kp}}^{\frac{1}{s_kp}} f(z)dz =$$

limits of integration are $\nabla_k 0$ and $\nabla_k\infty$ for $\nabla_k = \begin{bmatrix}1 & 1\\ s_kp & 2+s_kp\end{bmatrix}$

$$= \int_{\nabla_k 0}^{\nabla_k\infty} f(z)dz = 2\int_0^\infty f[\nabla_k](z)dz$$

where 2 comes from the determinant of ∇_k. In this case

$$F_E(x) = 2\int_0^\infty f[\nabla_k](z)dz,\ f(z) = 2E(z) - \frac{1}{2}E\left(\frac{z+1}{2}\right)$$

- Let $x = (\bar{1}, \bar{1})$, $y = (\overline{-1}, \bar{1})$. Corresponding matrices are

$$\beta_{1+p^2} = \begin{bmatrix} 1 & 0 \\ 1+p^2 & 1 \end{bmatrix}, \beta_{-1-p^2} = \begin{bmatrix} 1 & 0 \\ -1-p^2 & 1 \end{bmatrix}$$

$\beta_{1+p^2}1 = \frac{1}{2+p^2}, \beta_{1+p^2}(-1) = \frac{1}{p^2}$ and

$$\psi_E(\zeta_0(x)) = \int_{\frac{1}{2+p^2}}^{\frac{1}{p^2}} f(z)dz,$$

where $f(z) = 2E(z) - \frac{1}{2}E(\frac{z+1}{2})$. Assume that E has real Fourier coefficients. Since f is $\Gamma(2)$-invariant, it is written as

$$f(z) = \sum_{n=0}^{\infty} a_n e^{\pi i n z}.$$

Consequently, the complex conjugate of $f(z)$ is $\sum_{n=0}^{\infty} a_n e^{-\pi i n \tilde{z}}$, where $\tilde{z}$ is the complex conjugate of z :

$$\tilde{f}(z) = f(-\tilde{z}).$$

Then

$$\psi_E(\zeta_0(x)) = \int_{\frac{1}{2+p^2}}^{\frac{1}{p^2}} f(-\tilde{z})d\tilde{z} =$$

$$= \int_{-\frac{1}{p^2}}^{-\frac{1}{2+p^2}} f(z)dz = \psi_E(\zeta_0(y)).$$

The last transition follows from $\beta_{-1-p^2}1 = -\frac{1}{p^2}, \beta_{-1-p^2}(-1) = -\frac{1}{p^2+2}$.

Further, we observe that for the matrix $\sigma = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ we have

$$\beta_{1+p^2}\sigma = \begin{bmatrix} 0 & -1 \\ 1 & -1-p^2 \end{bmatrix}$$

And this product sends 1 to $\frac{1}{p^2}$ and -1 to $\frac{1}{2+p^2}$. So,

$$\psi_E(\zeta_0(x)) = \int_{\frac{1}{2+p^2}}^{\frac{1}{p^2}} f(z)dz = \int_{\beta_{1+p^2}\sigma(-1)}^{\beta_{1+p^2}\sigma(1)} f(z)dz =$$

introduce a matrix $\sigma_{p^2} = \begin{bmatrix} 1-p^2 & -p^2 \\ p^2 & 1+p^2 \end{bmatrix}$

$$= \int_{\sigma_{p^2}^{-1}\beta_{1+p^2}\sigma(-1)}^{\sigma_{p^2}^{-1}\beta_{1+p^2}\sigma(1)} f(\sigma_{p^2}(z))d\sigma_{p^2}(z) =$$

since $f(z)dz$ is invariant

$$= -\int_{\sigma_{p^2}^{-1}\beta_{1+p^2}\sigma(1)}^{\sigma_{p^2}^{-1}\beta_{1+p^2}\sigma(-1)} f(z)dz$$

We compute the product

$$\sigma_{p^2}^{-1}\beta_{1+p^2}\sigma\beta_{-1-p^2}^{-1} = \begin{bmatrix} p^6-p^4-2p^2-1 & p^4-2p^2-1 \\ p^6+2p^4-p^2 & p^4+p^2-1 \end{bmatrix}$$

and it belongs to $\Gamma_0(p^2) \cap \Gamma(2)$. So, the matrix $\sigma_{p^2}^{-1}\beta_{1+p^2}\sigma$ is $\Gamma-$equivalent to β_{-1-p^2} and

$$\int_{\sigma_{p^2}^{-1}\beta_{1+p^2}\sigma(1)}^{\sigma_{p^2}^{-1}\beta_{1+p^2}\sigma(-1)} f(z)dz = \psi_E(\zeta_0(y))$$

It follows that $\psi_E(\zeta_0(x)) = -\psi_E(\zeta_0(y))$ and finally

$$\psi_E(\zeta_0(x)) = \psi_E(\zeta_0(y)) = 0.$$

□

4.1.1 Subgroups $\Gamma_0(N)$ for $N = p^3$ or $N = pq$

Next two cases show that there are no such simple description of the projective line over $\mathbb{Z}/N\mathbb{Z}$ when N is not a square of a prime.

Consider an element $(p, 1) \in \mathbb{P}^1(\mathbb{Z}/p^3\mathbb{Z})$. Take $\lambda = 2(p^2+p+1)$. Since λ is coprime with p, it represents a unit $\bar{\lambda}$ in $\mathbb{Z}/p^3\mathbb{Z}$. For this choice of λ

$$(p, 1) \sim (\lambda p, \lambda) = (2(p^3 + p^2 + p), 2(p^2 + p + 1)) \equiv$$

modulo p^3

$$\equiv (2(p^2 + p), 2 + 2(p^2 + p)) = (r - 1, r + 1),$$

where $r = 1 + 2(p^2 + p)$. Further, $r = 1 + 2p(p + 1) \equiv 1$ modulo 4, since $p + 1$ is even and $2p(p + 1)$ is divisible by 4. Inverse of r modulo $4p^3$ is $s = 1 + 2(p^2 - p)$. Indeed,

$$rs = (1 + 2p^2 + 2p)(1 + 2p^2 - 2p) = (1 + 2p^2)^2 - 4p^2 = 1 + 4p^4 \equiv 1 \pmod{4p^3}$$

Now let p and q be distinct odd primes. We check that if $p \equiv 1 \pmod{q}$, then $(p, 1) \in \mathbb{P}^1(\mathbb{Z}/pq\mathbb{Z})$ cannot be written as $(r - 1, r + 1)$. Indeed, assume there is a unit λ in $\mathbb{Z}/pq\mathbb{Z}$ such that modulo pq

$$\lambda p \equiv r - 1, \lambda \equiv r + 1.$$

Then

$$(r + 1)p \equiv \lambda p \equiv r - 1$$

and

$$r(p - 1) + (p + 1) \equiv 0$$

It means that pq divides $r(p - 1) + (p + 1)$. But by assumption q divides $p - 1$, so q divides $p + 1$ and q divides $2 = (p + 1) - (p - 1)$ which is impossible.

4.2 Eisenstein element for X_Γ

Proposition 4.2.1. *[4, Prop. 4.2] If the element $\mathcal{E}_0 \in H_1(X_\Gamma - P_-, P_+, K)$ is defined by*

$$\mathcal{E}_0 = \sum_{g \in \mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})} F_E(g)\zeta^0(g),$$

then

$$\mathcal{E}_0 \circ c = \psi_E(c),\ c \in H_1(X_\Gamma - P_-, P_+, K)$$

Proof. It is enough to check equality for $c = [h]_0$. Then

$$\mathcal{E}_0 \circ c = \sum_{g \in \mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})} F_E(g)[g]^0 \circ [h]_0 =$$

the bilinear pairing is 1 when $g = h$ and 0 otherwise

$$= F_E(h) = \psi_E(c)$$

where the last equality follwos from Lemma 4.1.1.

□

4.3 Fourier coefficients of Eisenstein series at cusps and the main theorem

Result of the proposition 4.2.1 gives the Eisenstein element corresponding to $E \in E_2(\Gamma_0(p^2))$ in the relative homology $H_1(X_\Gamma - P_-, P_+, K)$. By specifying values of basic Eisenstein series at cusps the representation will be extended to the modular curve $X_0(p^2)$.

Lemma 4.3.1. *[4, Lemma 4.3] Fourier coefficient at $\frac{1}{kp}$ of $E_2^{\phi,\bar{\phi}}$ is a constant multiple of $\phi(k)t_\phi$, where*

$$t_\phi = \sum_{d,e=0}^{p-1} \phi(d)^2 \sum_{l \equiv (d+ep)(mod p^2), l \neq 0} \frac{1}{l^2}$$

Proof. The proof relies on properties of the series [5, §4.2]

$$E_2^{\bar v}(z) = \sum_{(c,d)\equiv \bar v (\mathrm{mod}\ p^2)} \frac{1}{(cz+d)^2},$$

where $\bar v \in (\mathbb{Z}/p^2\mathbb{Z})^2$. By [5, Prop. 4.2.1],

$$E_2^{\bar v}[\gamma]_2 = E_2^{\overline{v\gamma}}.$$

It follows that the same property holds for

$$G_2^{\bar v}(z) = \sum_{(c,d)\equiv \bar v (\mathrm{mod} p^2)} \frac{1}{(cz+d)^2} = \sum_{n\in(\mathbb{Z}/p^2\mathbb{Z})^*} \zeta_+^n(2) E_2^{n^{-1}\bar v}(z)$$

The latter equality follows from [5, §4.2]. The series $E_2^{\phi,\bar\phi}$ is given in terms of Fourier series which coincides up to a constant multiple with the Fourier series of

$$G_2^{\phi,\bar\phi}(z) = \sum_{c,d,e=0}^{p-1} \phi(c)\phi(d) G_2^{\overline{(cp,d+ep)}}(z)$$

[5, Th. 4.5.1]. So, it is enough to find the constant Fourier coefficient of $G_2^{\phi,\bar\phi}$ at the cusp $\frac{1}{kp}$. By the calculation in Lemma 2.1.2,

$$\frac{1}{kp} = \beta_{kp}(\infty).$$

Hence, the needed Fourier coefficient is found from

$$G_2^{\phi,\bar\phi}[\beta_{kp}]_2 = \sum_{c,d,e=0}^{p-1} \phi(c)\phi(d) G_2^{\overline{(cp,d+ep)\beta_{kp}}} =$$

$$= \sum_{c,d,e=0}^{p-1} \phi(c)\phi(d) G_2^{\overline{(cp+kp(d+ep),d+ep)}}$$

By [5, Th. 4.2.3] the constant term of $G_2^{\bar v}$ is non-zero if and only if $c_v \equiv 0 \pmod{p^2}$

(the first component of $\bar{v}$). In our case this reduces to $p|c+kd$, or

$$c \equiv -kd \pmod p.$$

As ϕ is a Dirichlet character modulo p,

$$\phi(c) = \phi(-k)\phi(d).$$

Further, by [5, Th.4.2.3] the coefficient is exactly $\sum_{l\equiv(d+ep)(modp^2),l\neq 0}\frac{1}{l^2}$ and the constant Fourier coefficient at $\frac{1}{kp}$ is a multiple of

$$\phi(-k)\sum_{d,e=0}^{p-1}\phi(d)^2 \sum_{l\equiv(d+ep)(modp^2),l\neq 0}\frac{1}{l^2} = \phi(-k)t_\phi.$$

□

Lemma 4.3.2. *[4, Lemma 4.4] Fourier coefficient at $\frac{1}{kp}$ of E_1 is $\frac{p-1}{24}$. Fourier coefficient at $\frac{1}{kp}$ of E_2 is* 0.

Proof. Since $\beta_{kp}\infty = \frac{1}{kp}$ what must be shown is that the constant terms of the Fourier expansion at ∞ of $E_2[\beta_{kp}]_2$ is zero.

The Ramanujan cusp form is

$$\Delta(z) = 216000G_4^3(z) - 529200G_6^2(z),$$

where $G_k(z) = \sum_{(c,d)\in\mathbb{Z}^2-\{(0,0)\}}\frac{1}{(cz+d)^k}$. The form Δ is the basis of the one-dimensional space $\mathcal{S}_{12}(\mathrm{SL}_2(\mathbb{Z}))$. Its logarithmis derivative satisfies

$$\frac{d}{dz}\log\Delta(\beta_{kp}(z)) = 12\frac{d}{dz}\log(kpz+1) + \frac{d}{dz}\log\Delta(z)$$

and

$$\frac{d}{dz}\log\Delta\Big(\begin{pmatrix}p & l\\ k & m\end{pmatrix}(z-l/p)\Big)) = 12\frac{d}{dz}\log(kpz+1) + \frac{d}{dz}\log\Delta(z-l/p)$$

It remains to substitute $E_2 = \frac{1}{2\pi i}\frac{d}{dz}\log\frac{\Delta(p^2z)}{\Delta(z)}$ and get that $a_0(E_2[\beta_{kp}]) = 0$.

Since $E_1 = \frac{1}{2\pi i}\frac{d}{dz}\log\frac{\Delta(pz)}{\Delta(z)}$ and all cusps $\frac{1}{kp}$ represent ∞ for $\Gamma_0(p)$ it follows that values at cusps are equal and equal to $\frac{p-1}{24}$.

□

The mapping $\pi : X_\Gamma \to X_0(p^2)$ is defined by $\pi(\Gamma z) = \Gamma_0(p^2)z$. It defines naturally a mapping

$$\pi_* : H_1(X_\Gamma \setminus P_-, P_+, K) \to H_1(X_0(p^2), \text{cusps}, K).$$

π_* sends a path $\gamma(t)$ in X_Γ into a path $\pi(\gamma(t))$. The boundary operator

$$\partial : H_1(X_0(p^2), \text{cusps}, K) \to H_0(X_0(p^2), \text{cusps}, K)$$

sends a path $(\gamma(t))_{t\in[0,1]}$ into a formal difference of endpoints, $\partial(\gamma) = \gamma(1) - \gamma(0)$. So, a boundary operator acts from the homological group of cycles into formal linear combination of cusps.

Two propositions below compute boundaries of elements $\pi_*(\mathcal{E}_0), \mathcal{E} \in H_1(X_0(p^2), \text{cusps}, K)$ by relating them with divisors (i.e. a formal linear combination of cusps). With an Eisenstein series E there is associated a divisor

$$\delta(E) = p^2 a_0(E[0])\{0\} + \sum_{k=1}^{p-1} a_0(E[1/kp])\{1/kp\} + a_0(E[\infty])\{\infty\}$$

The notation means that the divisor $\delta(E)$ assigns value $p^2 a_0(E[0])$ to the cusp 0, the value $a_0(E[1/p])$ to the cusp $1/p$, and so on. Here for any cusp x $E[x]$ denotes $E[\alpha]$

for a matrix α such that $\alpha\infty = x$. Let

$$\pi_*(\mathcal{E}_0) = \sum_{g \in \mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})} F_E(g)\zeta(g)$$

be the image in $X_0(p^2)$ of the modular symbol $\mathcal{E}_0$.

Proposition 4.3.1. *[4, Prop. 4.5] The boundary of $\pi_*(\mathcal{E}_0)$ is a constant multiple of $\delta(E)$.*

Proof. Using complete set of coset representatives of $\mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})$ from lemma 2.1.1, we write the boundary of an element $\pi_*(\mathcal{E}_0)$ as follows

$$\partial(\pi_*(\mathcal{E}_0)) = F_E((0,1))\partial(\zeta(I)) + \sum_{t=0}^{p^2-1} F_E((1,t))\partial(\zeta(\alpha_t)) +$$

$$+ \sum_{k=1}^{p-1} F_E((kp,1))\partial(\zeta(\beta_{kp}))$$

For each summand we find the boundary

$$\partial(\zeta(I)) = \{I\infty\} - \{I0\} = \{\infty\} - \{0\}$$

$$\partial(\zeta(\alpha_t)) = \{\alpha_t\infty\} - \{\alpha_t 0\} = \{0\} - \{-\frac{1}{t}\}$$

$$\partial(\zeta(\beta_{kp})) = \{\beta_{kp}\infty\} - \{\beta_{kp}0\} = \{\frac{1}{kp}\} - \{0\}$$

If t is coprime with p, then we can write $nt + mp^2 = 1$ for some integers n, m. The matrix

$$\begin{bmatrix} n & -1 \\ mp^2 & t \end{bmatrix} \in \Gamma_0(p^2)$$

takes 0 to $-\frac{1}{t}$ and $\{0\} = \{-\frac{1}{t}\}$. Summands coresponding to α_t when t is coprime with p do not contribute to the boundary. We regroup remained summands as

$$\partial(\pi_*(\mathcal{E}_0)) = F_E((0,1))(\{\infty\} - \{0\}) + F_E((1,0))(\{0\} - \{\infty\}) +$$

$$+\sum_{k=1}^{p-1}\left(F_E((kp,1))(\{\frac{1}{kp}\}-\{0\})+F_E((1,kp))(\{0\}-\{-\frac{1}{kp}\})\right)$$

Let $g=(\overline{kp},\bar{1})\in\mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})$. Since $\lambda=2+2kp=2(1+kp)$ is a unit in $\mathbb{Z}/p^2\mathbb{Z}$,

$$g=(\overline{\lambda kp},\bar{\lambda})=(\overline{2kp+2k^2p^2},\overline{2+2kp})=(\overline{2kp},\overline{2+2kp})=(\overline{r-1},\overline{r+1})$$

for $r=1+2kp$. In this case we take $s=1-2kp$ so that $rs=1-4k^2p^2\equiv 1$ (modulo $4p^2$).

Let $g=(\bar{1},\overline{-kp})\in\mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})$. Since $\lambda=-2+2kp=2(-1+kp)$ is a unit in $\mathbb{Z}/p^2\mathbb{Z}$,

$$g=(\bar{\lambda},\overline{-\lambda kp})=(\overline{-2+2kp},\overline{2kp-2k^2p^2})=(\overline{-2+2kp},\overline{2kp})=(\overline{r-1},\overline{r+1})$$

for $r=-1+2kp$. In this case we take $s=-1-2kp$ so that $rs=1-4k^2p^2\equiv 1$ (modulo $4p^2$).

By the lemma 4.1.1

$$F_E((kp,1))=-2\pi_E(V(2kp+1,-2kp+1))+\pi_E(hV(2kp+1,-2kp+1)h^{-1})$$

$$F_E((1,-kp))=-2\pi_E(V(2kp-1,-2kp-1))+\pi_E(hV(2kp-1,-2kp-1)h^{-1})$$

Explicitly,

$$V(2kp+1,-2kp+1)=\begin{bmatrix}2k^2p^2-2kp+1 & 2k^2p^2-4kp+2\\ -2k^2p^2 & -2k^2p^2+2kp+1\end{bmatrix},$$

$$V(2kp-1,-2kp-1)=\begin{bmatrix}2k^2p^2-2kp-1 & 2k^2p^2-4kp+2\\ -2k^2p^2 & -2k^2p^2+2kp-1\end{bmatrix}$$

and from formulas of chapter 3, we deduce

$$F_E((kp,1))=-F_E((1,-kp))$$

Let

$$\alpha = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \beta = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

Then

$$a_0(E[\beta_{kp}]) = \pi_{E[\beta_{kp}]}(\alpha) = \int_{z_0}^{\alpha z_0} E[\beta_{kp}](z)dz$$

$$2a_0(E[\beta_{kp}]) = \pi_{E[\beta_{kp}]}(\beta) = \int_{z_0}^{\beta z_0} E[\beta_{kp}](z)dz$$

Since $\beta_{kp}\beta\beta_{kp}^{-1} = \begin{bmatrix} 1-2kp & 2 \\ -2k^2p^2 & 1+2kp \end{bmatrix}$, from explicit formulas we have

$$2a_0(E[\beta_{kp}]) = \int_{z_0}^{\beta z_0} E[\beta_{kp}](z)dz = \int_{\beta_{kp}z_0}^{(\beta_{kp}\beta\beta_{kp}^{-1})\beta_{kp}z_0} E(z)dz =$$

$$= \pi_E(\beta_{kp}\beta\beta_{kp}^{-1}) = \pi_E(V(1-2kp, 1+2kp))$$

Similarly, $a_0(E[\beta_{2kp}]) = \pi_E(hV(1+2kp, 1-2kp)h^{-1})$ and

$$F_E(kp, 1) = -4a_0(E[\beta_{kp}]) + a_0(E[\beta_{2kp}])$$

The boundary of $\pi_*(\mathcal{E}_0)$ is

$$\partial(\pi_*(\mathcal{E}_0)) = -\sum_{k=1}^{p-1} 2\Big(4a_0(E[1/kp]) - a_0(E[1/2kp])\Big)\{\frac{1}{kp}\} - 6a_0(E)\{\infty\}+$$

$$+\Big(\sum_{k=1}^{p-1} 2\Big(4a_0(E[1/kp]) - a_0(E[1/2kp])\Big) + 6a_0(E)\Big)\{0\}$$

Consider the basic series $E = E^{\phi,\bar{\phi}}$. The constant Fourier coefficient of E at the cusp $\frac{1}{kp}$ is a constant multiple of $\phi(k)$. Then the boundary $\partial(\pi_*(\mathcal{E}_0))$ assigns to the cusp $\frac{1}{kp}$ the value that is proportional to

$$-2(4\phi(k) - \phi(2k)) = (2\phi(2) - 8)\phi(k)$$

But the value of a divisor $\delta(E)$ at $[1/kp]$ is $a_0(E[1/kp])$ which is a constant multiple of $\phi(k)$. So, $\partial(\pi_*(\mathcal{E}_0))$ is a constant multiple of $\delta(E)$.

Consider the basic series E_1. By the lemma 4.3.2, the value of E_1 at all cusps is constant and equal to $a_0(E_1) = \frac{p-1}{24}$. The boundary becomes

$$\partial(\pi_*(\mathcal{E}_0)) = -\sum_{k=1}^{p-1} 6a_0(E_1)\{\frac{1}{kp}\} - 6a_0(E_1)\{\infty\} + 6pa_0(E_1)\{0\} = -6\delta(E_1).$$

Consider the basic series E_2. By the lemma 4.3.2, the value of E_2 at all cusps except ∞ is zero. The boundary becomes

$$\partial(\pi_*(\mathcal{E}_0)) = -6a_0(E_2)\{\infty\} = -6\delta(E_2)$$

$\square$

Proposition 4.3.2. *[4, Prop. 4.7] Let $\mathcal{E} \in H_1(X_0(p^2), cusps, K)$ be the Eisenstein element corresponding to $E \in E_2(\Gamma_0(p^2))$. Its boundary is equal to $-\delta(E)$.*

Proof. Eisenstein element has a representation

$$\mathcal{E} = \sum_{g \in \mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})} G_E(g)\zeta(g)$$

for some coefficients $G_E(g)$. Taking the boundary operator, we get similarly to proposition 4.5

$$\partial(\mathcal{E}) = G_E((0,1))(\{\infty\} - \{0\}) + G_E((1,0))(\{0\} - \{\infty\}) +$$

$$+\sum_{k=1}^{p-1} \left(G_E((kp,1))(\{\frac{1}{kp}\} - \{0\}) + G_E((1,kp))(\{0\} - \{-\frac{1}{kp}\}) \right)$$

Let $\rho = \frac{1+i\sqrt{3}}{2}$, $\rho^* = \frac{-1+i\sqrt{3}}{2}$. For any $g \in SL_2(\mathbb{Z})$ denote by $g\{\rho, \rho^*\}$ the image in $X_0(p^2)$ of the geodesics in $\mathbb{H}$ joining $g(\rho)$ and $g(\rho^*)$. By definition, $\zeta(k)$ is the image in $X_0(p^2)$ of the geodesics joining $k(0)$ and $k(\infty)$. Let

$$s = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

By [10],

$$\zeta(g) \circ h\{\rho, \rho^*\} = \begin{cases} 1, & \text{if } \Gamma_0(p^2)g = \Gamma_0(p^2)h \\ -1, & \text{if } \Gamma_0(p^2)g = \Gamma_0(p^2)hs \\ 0, & \text{otherwise} \end{cases}$$

By definition of the Eisenstein element,

$$\mathcal{E} \circ h\{\rho, \rho^*\} = \pi_E(h\{\rho, \rho^*\}) = \int_{h(\rho)}^{h(\rho^*)} E(z)dz$$

On the other hand, matrices $g \in \mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})$ form a complete set of representatives for $\Gamma_0(p^2) \setminus SL_2(\mathbb{Z})$. So, if $\Gamma_0(p^2)h \neq \Gamma_0(p^2)hs$, in the sum

$$\mathcal{E} \circ h\{\rho, \rho^*\} = \sum_{g \in \mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})} G_E(g)\zeta(g) \circ h\{\rho, \rho^*\}$$

there is a summand corresponding to g such that $\Gamma_0(p^2)g = \Gamma_0(p^2)h$ (that contributes with $+G_E(h)$) and a summand corresponding to g such that $\Gamma_0(p^2)g = \Gamma_0(p^2)hs$ (that contributes with $-G_E(hs)$).Then

$$\mathcal{E} \circ h\{\rho, \rho^*\} = \int_{h(\rho)}^{h(\rho^*)} E(z)dz = G_E(h) - G_E(hs)$$

Take $h = \beta_{kp}$, $\beta_{kp}(\infty) = \frac{1}{kp}$. We observe that $\Gamma_0(p^2)\beta_{kp} \neq \Gamma_0(p^2)\beta_{kp}s$ since

$$\beta_{kp} s \beta_{kp}^{-1} = \begin{bmatrix} 1 & 0 \\ kp & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -kp & 1 \end{bmatrix} = \begin{bmatrix} kp & -1 \\ 1 + k^2p^2 & -kp \end{bmatrix} \notin \Gamma_0(p^2)$$

Then

$$G_E(\beta_{kp}) - G_E(\beta_{kp}s) = \int_{\beta_{kp}\rho}^{\beta_{kp}\rho^*} E(z)dz =$$

since $\rho = \frac{1+i\sqrt{3}}{2} = \rho^* + 1 = \alpha\rho^*$ for $\alpha = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

$$= \int_{\beta_{kp}\alpha\rho^*}^{\beta_{kp}\rho^*} E(z)dz$$

and

$$G_E(\beta_{kp}s) - G_E(\beta_{kp}) = \int_{\beta_{kp}\rho^*}^{\beta_{kp}\alpha\rho^*} E(z)dz = \int_{\rho^*}^{\alpha\rho^*} E[\beta_{kp}](z)dz =$$

by proposition 2.3.3, (d) in [8]

$$= a_0(E[\beta_{kp}]) = a_0(E[1/kp])$$

(since β_{kp} sends ∞ to the cusp $1/kp$). Since

$$\beta_{kp}s = \begin{bmatrix} 0 & -1 \\ 1 & -kp \end{bmatrix}$$

we find that the coefficient near $\{1/kp\}$ in the boundary $\partial(\mathcal{E})$ is

$$G_E(1, kp) - G_E(1, -kp) = G_E(\beta_{kp}) - G_E(\beta_{kp}s) = -a_0(E[1/kp])$$

Since $s \notin \Gamma_0(p^2)$, we have $\Gamma_0(p^2)I \neq \Gamma_0(p^2)s$ and

$$G_E(s) - G_E(I) = \int_{\rho^*}^{\rho} E(z)dz = \int_{\rho^*}^{\alpha\rho^*} E(z)dz = a_0(E)$$

The coefficient near $\{\infty\}$ in the boundary $\partial(\mathcal{E})$ is

$$G_E(0, 1) - G_E(1, 0) = G_E(I) - G_E(s) = -a_0(E)$$

Coefficients of $\partial(\mathcal{E})$ and $-\delta(\mathcal{E})$ coincide. Since coefficients sum to zero ($\delta(\mathcal{E})$ is an element of Div^0) we obtain the equality $\partial(\mathcal{E}) = -\delta(\mathcal{E})$.

□

Let $\mathcal{E} \in H_1(X_0(p^2), \text{cusps}, K)$ and $\mathcal{E}_0 \in H_1(X_\Gamma - P_-, P_+, K)$ be Eisenstein elements corresponding to the Eisenstein series $E \in E_2(\Gamma_0(p^2))$. The mapping $\pi : X_\Gamma \to X_0(p^2)$ is given by $\pi\Gamma z = \Gamma_0(p^2)z$. It induces the element $\pi_*(\mathcal{E}_0) \in H_1(X_0(p^2), \text{cusps}, K)$. Explicitly, for $g \in \Gamma \setminus \Gamma(2)$ we consider $\zeta^0(g)$ – the image in X_Γ of the geodesic in $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ joining $g0$ and $g\infty$; and $\zeta(g)$ – the image in $X_0(p^2)$ of the geodesic in $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ joining $g0$ and $g\infty$. Then $\pi_*(\zeta^0(g)) = \zeta(g)$.

Lemma 4.3.3. *[4, Lemma 4.9] The integrals of every holomorphic differential over $\mathcal{E}$ and $\pi_*(\mathcal{E}_0)$ are zeroes.*

Proof. Let λ_E be the rational function on $X_0(p^2)$ whose logarithmic derivative is $2\pi i E(z)dz$. Let $y \in H_1(X_\Gamma - P_+, P_-, K)$. Denote by $(\lambda_E)_*(y)$ the corresponding path in $H_1(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) - \{0, \infty\}, 1, K)$. By proposition 4.2.1,

$$\mathcal{E}_0 \circ y = \psi_E(y) = \frac{1}{2\pi i} \int_y \frac{d\lambda_E}{\lambda_E} = \gamma_1 \circ (\lambda_E)_*(y),$$

where γ_1 is the path in $H_1(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) - \{1\}, \{0, \infty\}, K)$ that connects 0 to ∞ (the latter relation is the definition of the period homomorphism). So,

$$\mathcal{E}_0 = (\lambda_E)^*(\gamma_1)$$

Now, for any holomorphic differential ω on $X_0(p^2)$ we have

$$\int_{\pi_*(\mathcal{E}_0)} \omega = \int_{\gamma_1} (\lambda_E)_*(\omega \circ \pi) = 0.$$

The latter equality follows from the fact that the differential $(\lambda_E)_*(\omega \circ \pi)$ is holomorphic on $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ (no zeroes or poles occur at 1 by lemma 2.3.2).

□

Theorem 4.3.1. *[4, Th. 1.1] Let $E \in E_2(\Gamma_0(p^2))$ be an Eisenstein series with coefficients at infinity from a fixed number field K. If E is a basic series from section 3.1, then the corresponding Eisenstein element is given by*

$$\mathcal{E} = \sum_{g \in \mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})} F_E(g)\zeta(g).$$

In all other cases there is similar representation with $F_E(g)$ changes to an explicitly computable function $G_E(g)$.

Proof. Let $\mathcal{E} \in H_1(X_0(p^2), \text{cusps}, K)$ be the Eisenstein element corresponding to the basic Eisenstein series E (i.e. E is one of the series E_1, E_2 or $E_2^{\phi,\bar{\phi}}$). Also, let

$$\pi_*(\mathcal{E}_0) = \sum_{g \in \mathbb{P}^1\mathbb{Z}/p^2\mathbb{Z}} F_E(g)\zeta(g) \in H_1(X_0(p^2), \text{cusps}, K).$$

From propositions 4.3.1 and 4.3.2 it follows that the boundary of $\mathcal{E}$ is a constant multiple of $\pi_*(\mathcal{E}_0)$:

$$\partial(\mathcal{E} - k\pi_*(\mathcal{E}_0)) = 0.$$

We will check that $\mathcal{E} - c\pi_*(\mathcal{E}_0) \in H_1(X_0(p^2), K)$. After that the theorem will be proved. Indeed, by the lemma 4.3.3 every holomorphic differential is integrated to zero over $\mathcal{E} - c\pi_*(\mathcal{E}_0)$ which implies that $\mathcal{E} = c\pi_*(\mathcal{E}_0)$ (the last conclusion follows from the fact the intersection pairing is perfect).

Let $\{\beta_1, \ldots, \beta_m\}$ be cusps in $X_0(p^2)$. Write

$$\mathcal{E} - k\pi_*(\mathcal{E}_0) = \sum_{1 \le i < j \le m} c_{ij}\{\beta_i, \beta_j\}. \tag{1}$$

Here the modular symbol $\{\beta_i, \beta_j\}$ is the geodesics from β_i to β_j. The representation (1) is the general form of an element of $H_1(X_0(p^2), \text{cusps}, K)$, because the first relative homology is the group of curves with endpoints in the set cusps.

We use the condition of zero boundary:

$$0 = \sum_{1 \le i < j \le m} c_{ij} \partial\{\beta_i, \beta_j\} = \sum_{1 \le i < j \le m} c_{ij} (\{\beta_j\} - \{\beta_i\}) =$$

$$= \sum_{j=1}^{m} \Big(\sum_{i: i<j} c_{ij} \Big) \{\beta_j\} - \sum_{i=1}^{m} \Big(\sum_{j: j>i} c_{ij} \Big) \{\beta_i\}.$$

Gathering coefficients near $\{\beta_i\}$ we get that for every $i \in \{1, \dots, m\}$:

$$\sum_{j: j<i} c_{ji} = \sum_{j: j>i} c_{ij}.$$

Solving with respect to c_{im} we get

$$c_{im} = \sum_{j: j<i} c_{ji} - \sum_{j: i<j \le m-1} c_{ij}.$$

Finally,

$$\sum_{1 \le i < j \le m} c_{ij} \{\beta_i, \beta_j\} =$$

$$= \sum_{1 \le i < j \le m-1} c_{ij} \{\beta_i, \beta_j\} + \sum_{i=1}^{m-1} c_{im} \{\beta_i, \beta_m\} =$$

$$= \sum_{1 \le i < j \le m-1} c_{ij} \{\beta_i, \beta_j\} + \sum_{i=1}^{m-1} \Big(\sum_{j: j<i} c_{ji} - \sum_{j: i<j \le m-1} c_{ij} \Big) \{\beta_i, \beta_m\} =$$

$$= \sum_{1 \le i < j \le m-1} c_{ij} \{\beta_i, \beta_j\} + \sum_{j=1}^{m-1} \Big(\sum_{i: i<j} c_{ij} \Big) \{\beta_j, \beta_m\} - \sum_{i=1}^{m-1} \Big(\sum_{j: i<j \le m-1} c_{ij} \Big) \{\beta_i, \beta_m\} =$$

$$= \sum_{1 \le i < j \le m-1} c_{ij} \Big(\{\beta_i, \beta_j\} + \{\beta_j, \beta_m\} - \{\beta_i, \beta_m\} \Big) =$$

$$= \sum_{1 \le i < j \le m-1} c_{ij} \Big(\{\beta_i, \beta_j\} + \{\beta_j, \beta_m\} + \{\beta_m, \beta_i\} \Big)$$

In the latter expression the sum $\{\beta_i, \beta_j\} + \{\beta_j, \beta_m\} + \{\beta_m, \beta_i\}$ is a cycle, i.e. an element of $H_1(X_0(p^2), \mathbb{Z})$.

So, $\mathcal{E} - c\pi_*(\mathcal{E}_0) \in H_1(X_0(p^2), K)$ hence, by perfect intersection pairing it is zero.

□

Denote by $\{0,\infty\}$ the image in $H_1(X_0(p^2), \text{cusps})$ of the geodesics joining 0 and ∞. The winding element e_{p^2} is a modular symbol such that defines an integration of a holomorphic form along $\{0,\infty\}$.

The exact expression for e_{p^2} is obtained by integrating a holomorphic form ω over the Eisenstein element $\mathcal{E}_2$, where $\mathcal{E}_2$ corresponds to the basic form E_2. We recall that by the main theorem,

$$\mathcal{E}_2 = \sum_{g\in\mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})} F_{E_2}(g)\zeta(g).$$

Corollary 4.10.

$$\frac{p^2-1}{4}e_{p^2} = -\sum_{x\in(\mathbb{Z}/p^2\mathbb{Z})^*} F((1,-x))0, \frac{1}{x}$$

Proof. The structure of a projective line $\mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})$ is the following:

$$\mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z}) = \{(0,1),(1,0),(1,1),\dots,(1,p^2-1),(p,1),\dots,((p-1)p,1)\}$$

(each pair is an element of $(\mathbb{Z}/p^2\mathbb{Z})^2$).

For each g we find the modular symbol $\zeta(g)$. It is the image in $H_1(X_0(p^2))$ of the geodesics that connects $g(0)$ to $g(\infty)$.

$(0,1)$ is the second row of the identity matrix I. $\zeta((0,1)) = \{0,\infty\}$

$(1,0)$ is the second row of the matrix $\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}$. $\zeta((1,0)) = \{\infty,0\} = -\{0,\infty\}$.

For $t\in\{1,2,\dots,p^2-1\}$

$(1,t)$ is the second row of the matrix $\begin{bmatrix}0 & -1\\ 1 & t\end{bmatrix}$. $\zeta((1,t)) = \{-\frac{1}{t},0\}$

For $k\in\{1,2,\dots,p-1\}$

$(kp,1)$ is the second row of the matrix $\begin{bmatrix}1 & 0\\ kp & 1\end{bmatrix}$. $\zeta((kp,1)) = \{0,\frac{1}{kp}\}$.

For any holomorphic differential ω, $\int_{\mathcal{E}_2} \omega = 0$, i.e.

$$\sum_{g \in \mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z})} F_{E_2}(g) \int_{\zeta(g)} \omega = 0$$

In this sum the coefficient near $\int_{\{0,\infty\}} \omega$ is

$$F_{E_2}((0,1)) - F_{E_2}((1,0)).$$

We compute this coefficient using the definition of the function F_{E_2}. Since 2 is a unit modulo p^2, $(0,1) = (0,2) = (1-1, 1+1)$. We apply the definition of $F_{E_2}((r-1, r+1))$ with $r = 1$:

$$F_{E_2}((0,1)) = \frac{1}{2\pi i}\left(2L\left(E_2 \begin{bmatrix} 1 & -1 \\ 0 & 2p^2 \end{bmatrix}, 1\right) - L\left(E_2 \begin{bmatrix} 1 & -1 \\ 0 & p^2 \end{bmatrix}, 1\right)\right) =$$

$$= -S(1, 2p^2) + S(1,2) + \frac{1}{2}S(1, p^2) - \frac{1}{2}S(1,1).$$

Here $S(u, v)$ is the Dirichlet sum,

$$S(u,v) = \sum_{t=1}^{v-1} \bar{B}_1(\frac{tu}{v})\bar{B}_1(\frac{t}{v}),$$

$\bar{B}_1(x) = x - \frac{1}{2}$, $0 < x < 1$, $\bar{B}_1(0) = 0$ and $\bar{B}_1$ is 1-periodic. We compute

$$S(1,v) = \sum_{t=1}^{v-1} \bar{B}_1(\frac{t}{v})^2 = \sum_{t=1}^{v-1} \left(\frac{t}{v} - \frac{1}{2}\right)^2 =$$

$$= \frac{1}{v^2}\sum_{t=1}^{v-1} t^2 - \frac{1}{v}\sum_{t=1}^{v-1} t + \frac{v-1}{4} =$$

$$= \frac{(v-1)v(2v-1)}{6v^2} - \frac{v(v-1)}{2v} + \frac{v-1}{4} = \frac{(v-1)(2v-1)}{6v} - \frac{v-1}{4} = \frac{(v-1)(v-2)}{12v}$$

It follows that

$$F_{E_2}((0,1)) = \frac{(p^2-1)(p^2-2)-(2p^2-1)(2p^2-2)}{24p^2} = \frac{-p^2+1}{8}$$

Similarly, we find $F_{E_2}((1,0))$. Since $2p^2-2$ is a unit modulo p^2, $(1,0)=(2p^2-2, 2p^2)$ and we apply the definition of $F_{E_2}((r-1, r+1))$ with $r = 2p^2-1$.

$$F_{E_2}((1,0)) = \frac{1}{2\pi i}\left(2L\left(E_2\begin{bmatrix}1 & -2p^2+1\\ 0 & 2p^2\end{bmatrix}, 1\right) - L\left(E_2\begin{bmatrix}1 & -2p^2+1\\ 0 & p^2\end{bmatrix}, 1\right)\right) =$$

$$= -S(2p^2-1, 2p^2) + S(2p^2-1, 2) + \frac{1}{2}S(2p^2-1, p^2) - \frac{1}{2}S(2p^2-1, 1).$$

We compute Dirichlet sums: $S(2p^2-1, 1) = 0$,

$$S(2p^2-1, 2) = \bar{B}_1(\frac{2p^2-1}{2})\bar{B}_1(\frac{1}{2}) = 0$$

$$S(2p^2-1, 2p^2) = \sum_{t=1}^{2p^2-1} \bar{B}_1(\frac{t(2p^2-1)}{2p^2})\bar{B}_1(\frac{t}{2p^2}) =$$

by periodicity

$$= \sum_{t=1}^{2p^2-1} \bar{B}_1(-\frac{t}{2p^2})\bar{B}_1(\frac{t}{2p^2}) = \sum_{t=1}^{2p^2-1}\left(-\frac{t^2}{4p^4}+\frac{1}{4}\right) =$$

$$= \frac{2p^2-1}{4} - \frac{1}{4p^4}\sum_{t=1}^{2p^2-1} t^2 = \frac{2p^2-1}{4} - \frac{(2p^2-1)2p^2(4p^2-1)}{24p^4} = -\frac{(p^2-1)(2p^2-1)}{12p^2}$$

$$S(2p^2-1, p^2) = \sum_{t=1}^{p^2-1} \bar{B}_1(\frac{t(2p^2-1)}{p^2})\bar{B}_1(\frac{t}{p^2}) =$$

by periodicity

$$= \sum_{t=1}^{p^2-1} \bar{B}_1(-\frac{t}{p^2})\bar{B}_1(\frac{t}{p^2}) = \sum_{t=1}^{p^2-1}\left(-\frac{t^2}{p^4}+\frac{1}{4}\right) =$$

$$= \frac{p^2-1}{4} - \frac{1}{p^4}\sum_{t=1}^{p^2-1} t^2 = \frac{p^2-1}{4} - \frac{(p^2-1)p^2(2p^2-1)}{6p^4} = -\frac{(p^2-1)(p^2-2)}{12p^2}$$

It follows that

$$F_{E_2}((1,0)) = \frac{(p^2-1)(2p^2-1)}{12p^2} - \frac{(p^2-1)(p^2-2)}{24p^2} = \frac{p^2-1}{8}$$

The coefficient near $\int_{\{0,\infty\}} \omega$ in $\int_{\mathcal{E}_2} \omega$ is $-\frac{p^2-1}{4}$. It follows that

$$\frac{p^2-1}{4} e_{p^2} = \sum_{g \neq (1,0),(0,1)} F_{E_2}(g)\zeta(g).$$

Similar calculations for $g = (kp, 1)$ and $g = (1, kp)$ show that corresponding terms will cancel.

$\square$

References

[1] L. Merel, "L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$," *Journal fur die reine und angewandte Mathematik*, vol. 477, pp. 71–116, 1996.

[2] J. I. Manin, "Parabolic points and zeta-functions of modular curves," *Mathematics of the USSR-Izvestiya*, vol. 6.1, pp. 1–19, 1972.

[3] V. G. Drinfeld, "Two theorems on modular curves," *Akademija Nauk SSSR. Funk. An. Pr.*, vol. 7(2), pp. 83–84, 1973.

[4] D. Banerjee, "A note on the Eisenstein elements of prime square level," *Proceedings of the American Mathematical Society*, vol. 142.11, pp. 3675–3686, 2014.

[5] F. Diamond and J. M. Shurman, *A first course in modular forms.* New York: Springer, 2005.

[6] P. Griffiths and J. Harris, *Principles of algebraic geometry.* John Wiley & Sons, 2014.

[7] A. Ogg, *Modular forms and Dirichlet series.* Benjamin, 1969.

[8] G. Stevens, *Arithmetic on modular curves.* Springer Science & Business Media, 2012.

[9] J. B. Conway, *Functions of one complex variable.* Springer Science & Business Media, 2012.

[10] H. A. Verrill, "Transportable modular symbols and the intersection pairing," *Lecture Notes in Comput. Sci.*, vol. 2369, pp. 219–233, 2002.