SOME APPLICATIONS OF THE CHEBOTAREV DENSITY THEOREM

A REPORT

submitted in partial fulfillment of the requirements

for the award of the degree of

Master of Science

in

MATHEMATICS

by

ANIRUDDHA S

(180401)

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH BHOPAL
BHOPAL - 462066

May 2021

CERTIFICATE

This is to certify that **Aniruddha S**, Integrated PhD (Mathematics), has completed bonafide work on the thesis entitled **'Some Applications of The Chebotarev Density Theorem'** under my supervision and guidance.

May 2021
IISER Bhopal

Dr Jyoti Prakash Saha

Committee Member	**Signature**	**Date**

ACADEMIC INTEGRITY AND COPYRIGHT DISCLAIMER

I hereby declare that this project report is my own work and due acknowledgement has been made wherever the work described is based on the findings of other investigators. This report has not been accepted for the award of any other degree or diploma at IISER Bhopal or any other educational institution. 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 certify that all copyrighted material incorporated into this document is in compliance with the Indian Copyright (Amendment) Act (2012) and that I have received written permission from the copyright owners for my use of their work, which is beyond the scope of the law. I agree to indemnify and safeguard IISER Bhopal from any claims that may arise from any copyright violation.

May 2021 **Aniruddha S**
IISER Bhopal

ACKNOWLEDGEMENT

I would like to thank my father who instilled the joy of mathematics in me. I wouldn't be pursuing mathematics if it weren't for his enthusiasm while teaching it. I also thank my family members who encouraged me to pursue a career in research.

For my bachelors, I went to Jain University, Bangalore, where I met two people, Mr. J. V. Ramana Raju and Mr. Shiva Hegde, who provided an environment to discuss mathematics. The former is an assistant professor at the institute, who held weekly discussions on mathematics with other interested students.

I then joined the Integrated PhD program in mathematics at IISER Bhopal. I was lucky to have great teachers such as Dr. Saurabh Shrivastava, Dr. Prahlad Vaidyanathan and many more. I am thankful to Dr. Ajit Bhand for his immense support and encouragement. I also want to thank Dr. Kumar Balasubramanian for his wonderful course on representation theory and helping me with concepts from ℓ-adic Lie groups.

I am greatful for being taught by Dr. Karam Deo Shankhadhar who was the instructor for the courses on analytic number theory and modular forms. He has encouraged me since my first course with him and has always helped me in clearing doubts regarding my thesis. The first flavour of algebraic geometry, one of the prerequisites for my thesis, I got was in the course on commutative algebra taught by Dr. Vivek Sadhu. Later, I attended the course on algebraic geometry taught by him and had a wonderful experience. I thank Karam Sir and Vivek Sir for being part of my project evaluation committee and their continuous support.

In the summer of 2019, after my first year at IISER, I got an opportunity to do some reading under Dr. Manish Kumar from the Indian Statistical Institute, Bangalore. I am very thankful to him for giving me the flavour of algebraic number theory, which is one of the main area of this thesis.

I express my sincere gratitude to Dr Jyoti Prakash Saha, my thesis advisor. His friendly nature, support and guidance, helping me with my doubts, in the last two years has been immense. His course on algebraic number theory introduced me to valuation theory and local theory, which are necessary

for this thesis. Since then, I have been reading under his guidance.

I would like to thank the staff members, post docs, PhD students and BS-MS students of the IISER Bhopal Mathematics department for their support.

Lastly, I thank my friends Shashank, Pankaj, Shreyas, Chakradhar, Tanvi, Prachi, Himanshi, Shubham, Harsh, Divyashree, Sourayan, Sreshta, Ashutosh, Krishna, Diksha, Rishab, Adarsh, Shubhojit and others who I might have missed, for their support and being there when I needed them.

Aniruddha S

ABSTRACT

This thesis aims to present some applications of the Chebotarev Density Theorem to the theory of elliptic curves and modular forms, as seen in the paper [Ser81] by Jean-Pierre Serre. We start by introducing the algebraic theory of elliptic curves, consisting of topics such as the group law on elliptic curves, Weierstrass equations, isogenies and Tate modules. We also look at ℓ-adic representations attached to elliptic curves and their properties. We move on to the statement of Chebotarev's theorem and look at certain effective forms of the theorem and a generalization to the ℓ-adic case. In the case of elliptic curves without complex multiplication, calculating the density of the set of primes p such that $a_p(E) = h$ is one of the applications of the Chebotarev's theorem. We then move on to non-lacunarity of Fourier coefficients associated to Hecke eigenforms and calculate the density of the non-zero Fourier coefficients. We conclude with non-lacunarity of a general modular form of weight $k \geq 2$.

LIST OF SYMBOLS OR ABBREVIATIONS

$\mathbb{Z}$	set of integers
$\mathbb{R}$	set of real numbers
$\mathbb{C}$	set of complex numbers
C/K	curve C defined over K.
$C(K)$	K-rational points in C.
GRH	Generalized Riemann Hypothesis
$T_\ell(E)$	Tate module of the elliptic curve E
$\mathcal{O}_F$	ring of integers in a number field F.
$\sigma_\mathfrak{p}$	Frobenius substitution (or element) at $\mathfrak{p}$.
$D_\mathfrak{p}(\overline{K})$	a decomposition group at $\mathfrak{p} \subseteq \mathcal{O}_K$ in $\mathrm{Gal}(\overline{K}/K)$.
$I_\mathfrak{p}(\overline{K})$	an inertia group at $\mathfrak{p} \subseteq \mathcal{O}_K$ in $\mathrm{Gal}(\overline{K}/K)$.
I_K	Inertia group of a local field K in $\mathrm{Gal}(\overline{K}/K)$.
$M_k(N, \omega)$	Modular forms of level N and type (k, ω)
$S_k(N, \omega)$	Space of cusp forms in $M_k(N, \omega)$
$E_k(N, \omega)$	Space of Eisenstein series in $M_k(N, \omega)$
$a_f(n)$	The n-th Fourier coefficient of the modular form f.
$M_f(x)$	$\#\{1 \leq n \leq x \mid a_f(n) \neq 0\}$
$S_{\mathrm{cm}}(k, N, \omega)$	$\langle\{f(dz)$, where $f(z)$ is a CM newform$\}\rangle$
$S_{\mathrm{cm}}^{\mathrm{non}}(k, N, \omega)$	$\langle\{f(dz)$, where $f(z)$ is a non-CM newform$\}\rangle$

CONTENTS

Certificate i

Academic Integrity and Copyright Disclaimer ii

Acknowledgement iii

Abstract v

List of Symbols or Abbreviations vi

1. Introduction 1

2. Algebraic Theory of Elliptic Curves 4
2.1 The Riemann–Roch Theorem 4
2.2 Applications of the Riemann–Roch Theorem 8
2.2.1 A Group Law on Elliptic Curves 8
2.2.2 Another Group Law on Elliptic Curves 10
2.2.3 The Two Group Laws are Same 10
2.2.4 The Geometric Group Law 11
2.3 Weierstrass Equation 12
2.3.1 Existence of a Weierstrass Equation 15
2.3.2 Quantities Attached to a Weierstrass Equation 18
2.4 Isogenies 19
2.4.1 Highlights From The Group Law 19
2.4.2 Isogenies 20
2.4.3 Isogenies are Homomorphisms 23
2.4.4 Dual Isogeny 24
2.5 Tate Modules 28
2.5.1 Cyclotomic Characters 28
2.5.2 Tate Module of an Elliptic Curve 30
2.5.3 Tate Modules and Isogenies 30
2.6 Weil Pairing 35
2.6.1 The Weil Pairing on the Tate Module 35

2.7 Structure of the Endomorphism Ring . . . 41
2.7.1 The Invariant Differential . . . 41
2.7.2 A Special Ring Structure . . . 43

3. The Chebotarev Density Theorem . . . 48
3.1 Effective Forms of the Theorem of Chebotarev . . . 48
3.1.1 The Theorem of Chebotarev . . . 48
3.1.2 An Effective Form of the Theorem . . . 50
3.2 Chebotarev Like Theorem: ℓ-adic case . . . 52
3.2.1 Proof of Theorem 3.9 . . . 54

4. An Application to Elliptic Curves . . . 58
4.1 Elliptic Curves over the Rationals and their reductions . . . 58
4.1.1 The Néron–Ogg–Shafarevich Theorem . . . 59
4.1.2 Galois representations . . . 61
4.2 The Set-up . . . 62
4.2.1 Number of primes $p \leq x$ such that $a_p(E)$ has a given value . . . 63

5. Applications to Modular Forms . . . 64
5.1 Definitions from Modular Forms . . . 64
5.2 Non-vanishing of Multiplicative Functions . . . 65
5.2.1 Proof of Theorem 5.4 . . . 67
5.2.2 Direct Proof of Theorem 5.7 . . . 71
5.3 Hecke eigenvalues of a Polynomial Type . . . 74
5.3.1 Proof of Theorem 5.18 . . . 76
5.4 Non-lacunarity of Hecke eigenforms . . . 78
5.4.1 Forms not of type CM . . . 79
5.4.2 Calculating the density . . . 80
5.4.3 Forms of type CM . . . 83
5.5 Non-lacunarity of Modular Forms of weight greater than 1 . . . 84
5.5.1 The Space $M_k(N, \omega)$ . . . 84
5.5.2 Proof of Theorem 5.36 . . . 88

Appendices . . . 90

A. . . . 91
I Maps Between Curves . . . 91
I.1 Maps Between Smooth Curves . . . 92
I.2 Frobenius Morphisms . . . 93
II Divisors . . . 94

III Derivations . . . 97
IV Differentials . . . 99
IV.1 Differentials on Curves . . . 100
V Ramification of Maps . . . 102
V.1 Ramification of elements from $\overline{K}(C)$ . . . 103
VI Galois Theory of Elliptic Function Fields . . . 104

B. . . . 107
I ℓ-adic Theory . . . 107
I.1 M-dimension . . . 108
II Galois representations . . . 108
III Dirichlet Characters and their Conductors . . . 110
III.1 Primitive Characters . . . 110

Bibliography . . . 113

1. INTRODUCTION

This thesis consists mainly of two parts:

- Theory of elliptic curves.
- Applications of Chebotarev's theorem.

We start with the theory of elliptic curves and cover topics such as: Weierstrass equations for elliptic curves, Isogenies, Tate modules, Weil pairing and end it with a structure theorem for the endomorphism ring of elliptic curves. The theory (including the Appendix) we give covers most of the sections from the first 3 chapters of [Sil06]. The ℓ-adic representation attached to an elliptic curve is used later in the section relating applications of Chebotarev's theorem to elliptic curves.

Elliptic curves over a field K are smooth projective curves of genus 1 with a specified rational point. Every elliptic curve over K has a Weierstrass equation of the type:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K.$$

Elliptic curves are special in the sense that they are groups with respect to an addition law induced from the Riemann–Roch Theorem. This group law also has a geometric realization. We deal with the category of elliptic curves where maps between two elliptic curves are *isogenies*: a map which is a morphism of varieties and a homomorphism of groups.

Let E/K be an elliptic curve and ℓ be a prime. The ℓ-adic Tate module of E is the inverse limit of the groups $E[\ell^m]$ containing points of order ℓ^m. The Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ acts on the Tate module, giving us an ℓ-adic representation

$$\psi_\ell : G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell).$$

The representation ψ_ℓ is unramified almost everywhere and, when E doesn't have complex multiplication, $\psi_\ell(G_K)$ is open in $\mathrm{GL}_2(\mathbb{Z}_\ell)$. The latter is an involved theorem by Serre (cf. [Ser98]).

The chapter on elliptic curves ends with the following classification of the endomorphism ring of an elliptic curve. Let E/K be an elliptic curve, then $\mathrm{End}(E)$ is one of the following:

- An order in $\mathbb{Q}$.
- An order in an imaginary quadratic field.
- An order in a quaternion algebra.

Next, we move on to the Chebotarev density theorem, its statement and effective versions of it, as seen in [Ser81]. One of the main theorem which is used time and again is the following Chebotarev like Theorem. Let $\pi_C(x) = \#\{p \leq x \mid \sigma_p \in C\}$.

Theorem 1.1 (cf. Theorem 10, [Ser81], or Theorem 3.9 below)**.** *Let d be a real number such that $0 \leq d < N$ and let $\dim_M C \leq d$. Taking $\alpha = (N-d)/N$, we have:*

i)

$$\pi_C(x) = O\left(\frac{\mathrm{Li}(x)}{\epsilon(x)^\alpha}\right) \quad as\ x \to \infty, \tag{1.1}$$

where,

$$\epsilon(x) = \log x (\log\log x)^{-2} (\log\log\log x)^{-1}. \tag{1.2}$$

ii) (Assuming GRH)

$$\pi_C(x) = O\left(\frac{\mathrm{Li}(x)}{\epsilon_R(x)^\alpha}\right) \quad as\ x \to \infty, \tag{1.3}$$

where,

$$\epsilon_R(x) = x^{1/2} (\log x)^{-2}. \tag{1.4}$$

We use the above theorem in the context of elliptic curves to get a bound for $P_{E,h}(x) = \#\{p \leq x \mid a_p(E) = h\}$, where $h \in \mathbb{Z}$, E is an elliptic curve, $\tilde{E}(p)$ is the reduction mod p of E, $\tilde{E}(\mathbb{F}_p)$ is the $\mathbb{F}_p$ rational points on $\tilde{E}(p)$ and $a_p(E) = 1 + p - |\tilde{E}(\mathbb{F}_p)|$ is the trace of the Frobenius endomorphism of the elliptic curve $\tilde{E}(p)$. We also prove that the natural density of the set of primes $\{p \leq x \mid a_p(E) = h\}$ is 0.

The last chapter deals with Fourier coefficients of Modular forms for the congruence subgroup $\Gamma_0(N)$ of Nebentypus ω and of weight $k > 1$. First, we deal with Hecke eigenforms of type CM and non-CM. In the case when f is a non-CM Hecke eigenform, we get the asymptotic behaviour of $M_f(x) = \#\{n \leq x \mid a_f(n) \neq 0\}$. More precisely, there is an $\alpha > 0$ such that

$$M_f(x) \sim \alpha x.$$

In this case, we see some examples, one of which is the Ramanujan Delta function. We prove that the the set $M_\Delta(x)$ has density

$$\prod_{\tau(p)=0}\left(1-\frac{1}{p+1}\right).$$

When f is a Hecke eigenform of type CM, we have

$$M_f(x) \sim \alpha x/(\log x)^{1/2}.$$

In this case we see that the density of $M_f(x)$ is 0.

We end the thesis with a result regarding general modular forms in $M_k(N,\omega)$. More precisely, we prove the following theorem:

Theorem 1.2 (cf. Theorem 17, [Ser81], Theorem 5.36 below)**.** *Let $f \in M_k(N,\omega)$, with $k \geq 2$.*

(*i*) *If $f \notin S_{\mathrm{cm}}(k,N,\omega)$, we have*

$$M_f(x) \asymp x \quad \text{as } x \to \infty.$$

(*ii*) *If $f \in S_{\mathrm{cm}}(k,N,\omega)$ and $f \neq 0$, we have*

$$M_f(x) \asymp x/(\log x)^{1/2} \quad \text{as } x \to \infty.$$

2. ALGEBRAIC THEORY OF ELLIPTIC CURVES

In this chapter, we study the Riemann–Roch Theorem which gives information about dimensions of certain function spaces and introduces the concept of *genus* of a curve. This will be needed in defining an *elliptic curve*. A good reference for the algebraic geometric background are the first two chapters of [Sil06]. Some of the prerequisites can be found in the Appendices as well.

We work with the usual notations found in [Sil06]. Let

K	perfect field.
$\overline{K}$	fixed algebraic closure of K.
C/K	curve C defined over K.
$C(K)$	K-rational points in C.

2.1 The Riemann–Roch Theorem

For a smooth curve C, we define a partial order on $\mathrm{Div}(C)$ as follows.

Definition 2.1. For a divisor $D = \sum n_P(P)$, we say that $D \geq 0$ if $n_P \geq 0$ for all $P \in C$. Similarly, for $D_1, D_2 \in \mathrm{Div}(C)$, we say that $D_1 \geq D_2$ if $D_1 - D_2 \geq 0$.

Example 2.2.

(*a*) Let $f \in \overline{K}(C)^*$ be such that f is regular everywhere except at a point P, with a pole of order at most n_P. This can be written as

$$\mathrm{div}(f) \geq -n_P(P).$$

Similarly,

$$\mathrm{div}(f) \geq (Q) - n_P(P)$$

says that f has a zero at Q.

(*b*) We saw earlier that if $C : y^2 = (x - e_1)(x - e_2)(x - e_2)$ then

$$\mathrm{div}(y) = (P_1) + (P_2) + (P_3) - 3(P_\infty)$$

, where $P_i = [e_i, 0, 1]$ and $P_\infty = [0, 1, 0]$. Hence, in the above language, we have

$$\mathrm{div}(y) \geq -3(P_\infty).$$

Definition 2.3. For $D \in \mathrm{Div}(C)$, define

$$\mathcal{L}(D) = \{f \in \overline{K}(C)^* \mid \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

For $D = 0$, we have $\mathcal{L}(0) = \{f \mid \mathrm{ord}_P(f) \geq 0 \ \forall P \in C\}$. We know that $\deg(\mathrm{div}(f)) = 0$ and hence for an $f \notin \overline{K}^*$, we f should have a pole, i.e. a point $Q \in C$ such that $\mathrm{ord}_Q(f) < 0$. Hence

$$\mathcal{L}(0) = \overline{K}$$

Proposition 2.4. (*a*) *If* $\deg(D) < 0$ *then* $\mathcal{L}(D) = \{0\}$.

(*b*) $\mathcal{L}(D)$ *is a finite dimensional vector space over* $\overline{K}$. *More specifically, If* $\ell(D)$ *is the dimension of* $\mathcal{L}(D)$, *then*

$$\ell(D) \leq \deg(D) + 1.$$

Proof. Let Let $D = \sum n_P(P)$.

(*a*) We prove the contrapositive of the statement. If $f \neq 0 \in \mathcal{L}(D)$ then as $\mathrm{div}(f) + D \geq 0$ we have

$$\deg(\mathrm{div}(f)) + \deg(D) = \deg(D) \geq 0.$$

(*b*) First we see that $\mathcal{L}(D)$ forms a $\overline{K}$-vector space. For $f, g \in \mathcal{L}(D)$ and $\alpha \in \overline{K}$ we have

$$\mathrm{ord}_P(f + \alpha g) \geq \min\{\mathrm{ord}_P(f), \mathrm{ord}_P(g)\} \geq n_P.$$

Hence we see that $f + \alpha g \in \mathcal{L}(D)$.

Let Q be such that $D - (Q) \geq 0$ and let $t = t_Q$ be a uniformiser at Q. Define the $\overline{K}$-linear map $T : \mathcal{L}(D) \to \overline{K}$ by

$$T(f) = t^{n_Q} f(Q).$$

This is well defined as $\mathrm{ord}_Q(f) \geq -n_Q$. The kernel of T is seen to be $\mathcal{L}(D-(Q))$ and hence we have an injecition

$$\frac{\mathcal{L}(D)}{\mathcal{L}(D-(Q))} \longrightarrow \overline{K}.$$

Therefore we have $\ell(D) \leq 1 + \ell(D-(Q))$. By doing the same process, as only finitely many n_Q's are non-zero, we get

$$\ell(D) \leq 1 + \deg(D)$$

□

We say that two divisors D_1, D_2 are linearly equivalent if they represent the same element in $\mathrm{Pic}(C)$.

Proposition 2.5. *If D_1 and D_2 are linearly equivalent, then $\mathcal{L}(D_1) \cong \mathcal{L}(D_2)$.*

Proof. Let $f \in \overline{K}(C)$ such that $D_1 = \mathrm{div}(f) + D_2$. Consider the map $\phi : \mathcal{L}(D_1) \to \mathcal{L}(D_2)$ defined by

$$\phi(g) = fg.$$

This is seen to be an isomorphism of $\overline{K}$-vector spaces. □

Example 2.6. Let K_C be a canonical divisor, say $K_C = \mathrm{div}(\omega)$. For a function $f \in \mathcal{L}(K_C)$, we have

$$\mathrm{div}(f) \geq -\mathrm{div}(\omega)$$

Hence $f\omega$ is a holomorphic form, that is $\mathrm{ord}_P(f\omega) \geq 0$ for all P. Similarly, for a holomorphic form $f\omega$ we have $f \in \mathcal{L}(D)$. As all differential forms in $\Omega(C)$ are of the form $f\omega$ for some $f \in \overline{K}(C)^*$, we have the following isomorphism.

$$\{\text{Holomorphic forms in } \Omega(\mathrm{C})\} \cong \mathcal{L}(K_C).$$

Now let us see the statement of our main result.

Theorem 2.7 (Riemann–Roch)**.** *Let C be a smooth curve and K_C be a canonical divisor of C. There exists an integer g, called the* genus*, such that for all $D \in \mathrm{Div}(C)$, we have*

$$\ell(D) - \ell(K_C - D) = \deg(D) - g + 1.$$

Corollary 2.8. (a) $\ell(K_C) = g$

(b) $\deg(K_C) = 2g - 2$

(c) If $\deg(D) > 2g - 2$, we have

$$\ell(D) = \deg(D) - g + 1$$

Proof. (a) Immediate from the Riemann–Roch Theorem for $D = 0$.
(b) For $D = K_C$.
(c) If $\deg(D) > 2g - 2 = \deg(K_C)$, then $\deg(K_C - D) < 0$. Therefore, $\ell(K_C - D) = 0$ and $\ell(D) = \deg(D) - g + 1$. □

Example 2.9. Let $C : XY = Z^2$ be the hyperbola and $x = X/Z = Z/Y : C \to \mathbb{P}^1$ be the rational map defined by

$$[a, b, 1] \mapsto [a, 1]$$
$$[0, 1, 0] \mapsto [0, 1]$$
$$[1, 0, 0] \mapsto [1, 0]$$

For a point $P = [a, b, 1]$, consider $x - a \in \overline{K}(C)$. We have

$$M_P = (x - a, y - b) = \left(x - a, \frac{1}{x} - \frac{1}{a}\right) = (x - a)$$

implying $x - a$ is a uniformiser at P. For the point $P_0 = [0, 1, 0]$ we have

$$M_{P_0} = (X/Y, Z/Y) = (Z/Y) = (x)$$

as $X/Y = (Z/Y)^2$. Therefore, x is a uniformiser at P_0. For $P_1 = [1, 0, 0]$ we have $Z/X = 1/x$ as a uniformiser and hence $\mathrm{ord}_{P_1}(dx) = -2$. From all this we get,

$$\mathrm{div}(dx) = -2(P_1)$$

So, for $K_C = \mathrm{div}(dx)$, we have $2g - 2 = \deg(K_C) = -2$ and hence $g = 0$.

Example 2.10 (Elliptic Curves)**.** Let $C : y^2 = (x - e_1)(x - e_2)(x - e_3)$, we know that

$$\mathrm{div}(dx/y) = 0.$$

Hence we can take $K_C = 0$ and get

$$g = \ell(K_C) = \ell(0) = 1.$$

By the Riemann–Roch Theorem (2.7), for any divisor D with $\deg(D) \geq 1$ we have

$$\ell(D) = \deg(D).$$

Let us see some special consequences.

(*i*) For a point $P \in C$, we have $\ell((P)) = \deg((P)) = 1$ and hence $\mathcal{L}((P)) = \overline{K}$. What this says is that there doesn't exist a non constant $f \in \overline{K}(C)$ with $\operatorname{div}(f) + (P) \geq 0$, or equivalently having a simple pole at only P.

(*ii*) Let $P_\infty = [0, 1, 0]$ and $D = 2(P_\infty)$. We have $\ell(D) = 2$ and as $\operatorname{div}(x - e_i) = 2(P_i) - 2(P_\infty) \in \mathcal{L}(D)$, we have $\{1, x\}$ to be a basis for $\mathcal{L}(D)$.

(*iii*) Similarly, $\{1, x, y\}$ forms a basis for $\mathcal{L}(3(P_\infty))$.

2.2 Applications of the Riemann–Roch Theorem

We shall look at certain applications of the Riemann–Roch theorem, which will also help us later in proving that *isogenies of elliptic curves* are homomorphisms.

Definition 2.11 (Elliptic Curve)**.** An *elliptic curve* over K is a smooth projective curve of genus 1 with a distinguished point $\mathcal{O}$. It is denoted as $(E, \mathcal{O})$.

2.2.1 A Group Law on Elliptic Curves

For an elliptic curve $(E, \mathcal{O})$, recall that two divisors $D_1, D_2 \in \operatorname{Div}(E)$ are linearly equivalent (written $D_1 \sim D_2$) if there is an $f \in \overline{K}(E)^*$ such that

$$D_1 - D_2 = \operatorname{div}(f).$$

Proposition 2.12. *For $P, Q \in E$, we have a unique $R \in E$ such that*

$$(P) + (Q) \sim (R) + (\mathcal{O})$$

as divisors.

Proof. First we shall prove the existence. Let $D = (P)+(Q)-(\mathcal{O}) \in \operatorname{Div}(E)$, we have $\deg(D) = 1$ implying $\ell(D) = 1$ by Riemann–Roch Theorem. For a nonzero $f \in \mathcal{L}(D)$, we have

$$\operatorname{div}(f) + D = \operatorname{div}(f) + (P) + (Q) - (\mathcal{O}) \geq 0.$$

Let $\operatorname{div}(f) + D = \sum_S n_S(S)$, we have $n_S \geq 0$ and

$$\sum_S n_S = \deg(\operatorname{div}(f) + D) = \deg(\operatorname{div}(f)) + \deg(D) = 1.$$

This can happen only when one of the coefficients $n_R = 1$ for some R, and $n_S = 0$ for $S \neq R$. Hence, $\operatorname{div}(f) + D = (R)$ for some $R \in E$. Hence

$$(P) + (Q) \sim (R) + (\mathcal{O})$$

for some $R \in E$.

Now for the uniqueness, let $R_1, R_2 \in E$ such that

$$(P) + (Q) \sim (R_1) + (\mathcal{O}) \sim (R_2) + (\mathcal{O}).$$

We have $(R_1) \sim (R_2)$, hence

$$\operatorname{div}(f) = (R_1) - (R_2)$$

for some $f \in \overline{K}(E)^*$. This says that $f \in \mathcal{L}(R_2)$. From the Riemann–Roch Theorem, we know that $\mathcal{L}(R_2) = \overline{K}$, implying that $f \in \overline{K}^*$. Therefore, we have

$$(R_1) = (R_2) + \operatorname{div}(f) = (R_2).$$

□

Remark 2.13. We see that the above proposition can be stated in a more general way as it works for any divisor $D \in \operatorname{Div}(E)$ with $\deg(D) = 1$ in place of $(P) + (Q) - (\mathcal{O})$. That is, for a divisor $D \in \operatorname{Div}(E)$ with degree 1, we have a unique $Q \in E$ such that $D \sim (Q)$.

Consider the map $\sigma : E \times E \to E$ defined by $(P, Q) \mapsto R$, where R was the unique point as in Proposition 2.12. The map σ is surjective as $(R, \mathcal{O}) \mapsto R$ for every $R \in E$. We can define addition of two points P, Q to be the point $R = \sigma(P, Q)$.

We see that (E, σ) forms an abelian group. It is clear to see the identity is $\mathcal{O}$ and $\sigma(P, Q) = \sigma(Q, P)$. Let us prove the *associativity* of this addition law. Let $P, Q, R \in E$, $\sigma(P, Q) = S$ and $\sigma(Q, R) = T$. We should show that

$$\sigma(S, R) = \sigma(P, T).$$

We have

$$\begin{aligned}(\sigma(S, R)) + (\mathcal{O}) &\sim (S) + (R) \\ &\sim (P) + (Q) - (\mathcal{O}) + (R) \\ &\sim (P) + (T) \\ &\sim (\sigma(P, T)) + (\mathcal{O}).\end{aligned}$$

Hence, $\sigma(S, R) = \sigma(P, T)$ and this proves the associativity. For the inverse, consider a point $P \in E$. We can apply the remark (2.13) for the divisor $D = 2(\mathcal{O}) - (P)$ to get the inverse $Q \in E$ of P.

2.2.2 Another Group Law on Elliptic Curves

As before, let $(E, \mathcal{O})$ be an elliptic curve.

Proposition 2.14. *For a divisor $D \in \mathrm{Div}^0(E)$, there exists a unique $P \in E$ such that*

$$D \sim (P) - (\mathcal{O}).$$

Proof. Use of remark 2.13 for the divisor $D + (\mathcal{O})$. □

Define $\tau : \mathrm{Div}^0(E) \to E$ by $\tau(D) = P$, for P as in the above proposition. The map τ is surjective as $\tau((P) - (\mathcal{O})) = P$.

Proposition 2.15. *For two divisors $D_1, D_2 \in \mathrm{Div}^0(E)$,*

$$D_1 \sim D_2 \text{ if and only if } \tau(D_1) = \tau(D_2).$$

Proof. Let $\tau(D_1) = \tau(D_2) = Q$, then

$$D_1 \sim (Q) - (\mathcal{O}) \sim D_2.$$

If $D_1 \sim D_2$, then

$$D_1 \sim (\tau(D_1)) - (\mathcal{O}) \sim D_2.$$

Implying $\tau(D_1) = \tau(D_2)$. □

Therefore, from the above proposition, we get the induced bijection

$$\tau : \mathrm{Pic}^0(E) \to E,$$

from which we can put a group structure on E. Let us denote the group by (E, τ).

2.2.3 The Two Group Laws are Same

We just have to verify that $\tau : \mathrm{Pic}^0(E) \to (E, \sigma)$ is a homomorphism. It is enough to show that

$$\tau(D_1 + D_2) = \sigma(\tau(D_1), \tau(D_2)),$$

for $D_1, D_2 \in \mathrm{Div}^0(E)$. Let $\tau(D_1 + D_2) = Q$, we have $(Q) - (\mathcal{O}) \sim D_1 + D_2$. Hence,

$$\begin{aligned}(Q) + (\mathcal{O}) &\sim (D_1 + (\mathcal{O})) + (D_2 + (\mathcal{O})) \\ &\sim (\tau(D_1)) + (\tau(D_2)).\end{aligned}$$

Therefore, $\tau(D_1 + D_2) = Q = \sigma(\tau(D_1), \tau(D_2))$. So, for $d_1 = \overline{D_1}, d_2 = \overline{D_2} \in \mathrm{Pic}^0(E)$, we have

$$\tau(d_1 + d_2) = \tau(D_1 + D_2) = \sigma(\tau(d_1), \tau(d_2)),$$

as $\tau(\overline{D}) = \tau(D)$.

2.2.4 The Geometric Group Law

Let $(E, \mathcal{O})$ be an elliptic curve. For $P, Q \in E$, consider the line passing through them and let it intersect the elliptic curve at a third point R. Take the line passing through R and $\mathcal{O}$, define $P + Q$ to be the third point of intersection of this line with E. This makes E into a group with identity $\mathcal{O}$. This addition law is called as the *geometric group law*.

We will see that the geometric group law is the same as the two group laws mentioned above.

Theorem 2.16. *The map $\tau : \mathrm{Pic}^0(E) \to E$ defined above is an isomorphism of groups, where E has the geometric group law.*

Proof. It is enough to prove that

$$\tau(D_1 + D_2) \sim \tau(D_1) + \tau(D_2) \quad \forall\ D_1, D_2 \in \mathrm{Div}^0(E).$$

Let $\tau(D_1) = P$ and $\tau(D_2) = Q$, we have

$$D_1 \sim (P) - (\mathcal{O}) \text{ and } D_2 \sim (Q) - (\mathcal{O}).$$

We have $D_1 + D_2 \sim (P) + (Q) - 2(\mathcal{O})$ and hence, we need to show $\sigma(P, Q) = P + Q$.

Consider the line $L_1 : f(X, Y, Z) = aX + bY + cZ = 0$ passing through P, Q and meeting at R. As $Y/Z \in \mathcal{L}(3(\mathcal{O}))$ and $\mathrm{ord}_{\mathcal{O}}(Y) = 0$, we have $\mathrm{ord}_{\mathcal{O}} Z = 3$. We also have $\mathrm{ord}_X(f) = 1$ for $X = P, Q, R$. Therefore for $f/Z \in \overline{K}(E)^*$ we see that

$$\mathrm{div}(f/Z) = (P) + (Q) + (R) - 3(\mathcal{O}).$$

Similarly, if $L_2 : g(X, Y, Z) = pX + qY + rZ = 0$ is the line through $R, \mathcal{O}$ and $P + Q$, we have

$$\mathrm{div}(g/Z) = (R) + (P + Q) - 2(\mathcal{O}).$$

Therefore, we have

$$\mathrm{div}\left(\frac{f}{g}\right) = (P) + (Q) - (P + Q) - (\mathcal{O}).$$

Hence, $\sigma(P, Q) = P + Q$. □

Remark 2.17. By the above discussions, all the group laws which we defined on E are isomorphic. We therefore have the following exact sequence,

$$1 \to \overline{K}^* \hookrightarrow \overline{K}^*(E) \xrightarrow{\mathrm{div}} \mathrm{Div}^0(E) \xrightarrow{\tau} E \to 0$$

as $E \cong \mathrm{Pic}^0(E)$.

2.3 Weierstrass Equation

The definition given for an elliptic curve is usually not the working definition. It is a curve, so we want an equation satisfied by the points on the elliptic curve. Indeed, there exists (cf. §2.3.1 below) a Weierstrass equation of the elliptic curve. We will again use the Riemann–Roch Theorem to prove that every elliptic curve has a Weierstrass equation.

From now on, we use a short-hand notation and just write E for the elliptic curve $(E, \mathcal{O})$.

Definition 2.18. An elliptic curve E is isomorphic to a curve given by an equation of type,

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

in the projective plane $\mathbb{P}^2$. The above equation is called as a *Weierstrass equation* for an elliptic curve.

If $a_i \in K$, we say the elliptic curve is *defined* over K. In most cases, given a Weierstrass equation for E, we write it in its non-homogeneous form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with the point $[0, 1, 0]$ at infinity.

If $\mathrm{Char}K \neq 2$, we can change the coordinates to bring the equation to a much simpler form,

$$E : y^2 = x^3 + b_2x^2 + b_4x + b_6,$$

by the transformation $y \mapsto (y - a_1x - a_3)/2$, where

$$b_2 = a_1^2 + 4a_4, \qquad b_4 = 3a_4 + a_1a_3, \qquad b_6 = a_3^2 + 4a_6.$$

If we further assume that $\mathrm{Char}(K) \neq 3$, then by a similar transformation we bring the equation to the form $y^2 = f(x)$, where $f(x)$ is a depressed cubic.

Definition 2.19. We define the *invariant differential* attached to the Weierstrass equation of the elliptic curve E as

$$\omega = \frac{dx}{2y + a_1x + a_3} = -\frac{dy}{3x^2 + 2a_2x + a_4 - a_1y} \tag{2.1}$$

Remark 2.20. Before going further, let us fix some notations. Taking $F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$, we write the elliptic curve $E : F(x, y) = 0$. Also, we write (a, b) to denote the point $[a, b, 1] \in E$.

Earlier, we saw that for an elliptic curve of the form $y^2 = (x - e_1)(x - e_2)(x - e_3)$, the invariant differential ω is such that $\mathrm{div}(\omega) = 0$. This is true for a general elliptic curve, as we prove below.

Theorem 2.21. *The invariant differential ω attached to an elliptic curve E satisfies*

$$\mathrm{div}(\omega) = \sum_{P \in E} \mathrm{ord}_P(\omega)(P) = 0.$$

Proof. Let $P = (a, b) \in E$. We have

$$\omega = \frac{d(x-a)}{F_y(x,y)} = -\frac{d(y-b)}{F_x(x,y)}$$

First, let us assume $\mathrm{Char}(K) \neq 2$. Consider the map $\phi : E \to \mathbb{P}^1$ sending $[x, y, 1] \to [x, 1]$. We have $\deg(\phi) = 2$, as $\overline{K}(E) = \overline{K}(x, y)$ and $\phi^*(\overline{K}(\mathbb{P}^1)) = \overline{K}(x)$. We have the following extensions of fields and DVR's,

$$\begin{array}{ccc} \mathcal{O}_X & \xrightarrow{\quad i \quad} & \overline{K}(E) \\ \Big| & & \Big| \\ \phi^*(\mathcal{O}_{\phi(P)}) & \xrightarrow{\quad i \quad} & \phi^*(\overline{K}(\mathbb{P}^1)) \end{array}$$

for $X = P, Q$ and where i is the inclusion map. So, by factorization of ideals in extensions of Dedekind domains, we get

$$\phi^*(M_{\phi(P)}) = M_P M_Q$$

for $P, Q \in E$ such that $\phi(P) = \phi(Q) = [a, 1]$. As $M_{\phi(P)} = (x - a)$, we have

$$\mathrm{ord}_P(\phi^*(x-a)) = \begin{cases} 2 & \text{if } P = Q \ (\mathrm{ord}_P(F_y(x,y)) = 1) \\ 1 & \text{otherwise } (\mathrm{ord}_P(F_y(x,y)) = 0). \end{cases}$$

For $x = a$, we get

$$y^2 + (a_1 a + a_3)y - (a^3 + a_2 a^2 + a_4 a + a_6) = 0.$$

So, $P = Q$ if and only if the above equation is not separable, and this is equivalent to saying $F_y(a, b) = 0$. As $\mathrm{Char}(K) \neq 2$, we have

$$\begin{aligned} \mathrm{ord}_P(\omega) = \mathrm{ord}_P(d(x-a)/F_y(x,y)) &= \mathrm{ord}_P(d(x-a)) - \mathrm{ord}_P(F_y(x,y)) \\ &= \mathrm{ord}_P(x-a) - 1 - \mathrm{ord}_P(F_y(x,y)). \end{aligned}$$

We have $\phi^*(x-a) = x - a \in \overline{K}(E)$, where the latter $x = X/Z$. Hence from the above equation and using the above order formula we have

$$\mathrm{ord}_P(\omega) = 0.$$

For $\mathrm{Char}(K) = 2$, consider the rational map $\psi : [x, y, 1] \to [y, 1]$. This has degree 3 and

$$\phi^*(M_{[b,1]}) = M_P M_Q M_R,$$

where $\psi(P) = \psi(Q) = \psi(R) = [b, 1]$. We, similarly as before have,

$$\mathrm{ord}_P(y-b) = \begin{cases} 3 & \text{if } P = Q = R \ (\mathrm{ord}_P(F_x(x,y)) = 2) \\ 1 & \text{if } P \neq Q \neq R \ (\mathrm{ord}_P(F_x(x,y)) = 0) \\ 2 & \text{otherwise } (\mathrm{ord}_P(F_x(x,y)) = 1). \end{cases}$$

Hence, by a similar argument as above, we have $\mathrm{ord}_P(\omega) = 0$.

Now, we need to check at $\mathcal{O} = [0, 1, 0]$. For a uniformiser t at $\mathcal{O}$, we have $x = t^{-2}g$ and $y = t^{-3}f$, where $f, g \notin M_{\mathcal{O}}$. So, by substituting this in our formula for ω, we get

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{-2t^{-3}gdt + t^{-2}dg}{2t^{-3}f + a_1t^{-2}g + a_3} = \frac{-2g + t(dg/dt)}{2f + a_1tg + a_3t^3}dt.$$

It is now clear to see that $\mathrm{ord}_{\mathcal{O}}(\omega) = 0$ if $\mathrm{Char}(K) \neq 2$. If $\mathrm{Char}(K) = 2$, then we consider

$$\omega = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y} = \frac{-3f + t(df/dt)}{3g^2 + 2a_2t^2g + a_4t^4 - a_1tf}dt.$$

Hence, even in this case, $\mathrm{ord}_P(\omega) = 0$. □

The next theorem classifies curves with singular Weierstrass equation.

Theorem 2.22. *Let E be a singular curve with a Weierstrass equation. Then there is a rational map $\phi : E \to \mathbb{P}^1$ with $\deg(\phi) = 1$.*

Proof. Let E be a singular elliptic curve and by linear transformations, we can assume the singular point is $(0, 0)$. From this we have the Weierstrass equation to be

$$y^2 + a_1xy = x^3 + a_2x^2.$$

Let $\phi : E \to \mathbb{P}^1$ be a rational map defined by $[a, b, 1] \mapsto [a, b]$. By taking $t = y/x$, we have $t^2 + a_1t - a_2 = x$. Hence we have the inverse map $\psi : \mathbb{P}^1 \to E$ defined by

$$[1, t] \mapsto [t^2 + a_1t - a_2, t^3 + a_1t^2 - a_2t].$$

We have $\phi \circ \psi$ =Id on $\mathbb{P}^1$ and hence, $\psi^* \circ \phi^*$ =Id on $\overline{K}(\mathbb{P}^1)$. From this $\psi^* : \overline{K}(E) \to \overline{K}(\mathbb{P}^1)$ is surjective, implying $\overline{K}(\mathbb{P}^1) \cong \overline{K}(E)$. □

2.3.1 Existence of a Weierstrass Equation

For the theorem that follows regarding the existence of Weierstrass equation, we need some lemmas.

Lemma 2.23 (cf. [Sil06], Proposition 5.8)**.** *If C is a smooth curve defined over K and $D \in \mathrm{Div}_K(C)$, then $\mathcal{L}(D)$ has a basis of elements in $K(C)$.*

Lemma 2.24. *If $f_1, \cdots, f_n \in \overline{K}(C)$ are defined over K and are linearly dependent over $\overline{K}$, then they are linearly dependent over K.*

Proof. Let

$$a_1 f_1 + \cdots + a_n f_n = 0,$$

where $a_i \in \overline{K}$. WLOG, we can take $a_1 = 1 \neq 0$ by the fact that one of a_i is non-zero and we can divide by it in the equation. Consider the smallest Galois extension containing a_i's, call it L. For any $\sigma \in \mathrm{Gal}(L/K)$, by its action on $\overline{K}(C)$, we have

$$\sum_{i=1}^{n} (a_i f_i)^\sigma = \sum_{i=1}^{n} \sigma(a_i) f_i = 0$$

as f_i's are defined over K. By summing the equation over $\sigma \in \mathrm{Gal}(L/K)$, we get

$$\sum_{\sigma} \sum_{i=1}^{n} \sigma(a_i) f_i = \sum_{i=1}^{n} \left(\sum_{\sigma} \sigma(a_i) \right) f_i = \sum_{i=1}^{n} \mathrm{Tr}_{L/K}(a_i) f_i = 0.$$

As $\mathrm{Tr}_{L/K}(a_i) \in K$ and $\mathrm{Tr}_{L/K}(a_1) = \mathrm{Tr}_{L/K}(1) \neq 0$, we have proved the lemma. □

Theorem 2.25. *Let E be an elliptic curve defined over K.*

(a) There exists $x, y \in K(E)$ such that the map $\phi : E \to \mathbb{P}^2$ defined by

$$\phi = [x, y, 1] \text{ and } \phi(\mathcal{O}) = [0, 1, 0]$$

is an isomorphism from E to a curve

$$Y^2 Z + a_1 XYZ + a_3 YZ^2 = X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3,$$

where $a_i \in K$. In this case, we call x, y to be the Weierstrass coordinates for the elliptic curve.

(*b*) *Any two Weierstrass coordinates* (x, y) *and* (X, Y) *for* E *are related by the following transformation,*

$$X = u^2x + b, \qquad Y = u^3y + su^2x + c$$

where $u \in K^*, b, s, c \in K$.

(*c*) *A smooth cubic curve* C *with a Weierstrass equation is an elliptic curve with the point* $[0, 1, 0]$ *at infinity.*

Proof. (*a*) From the Riemann–Roch Theorem, we have

$$\ell(n(\mathcal{O})) = n \qquad \forall\ n \geq 1.$$

So from Lemma 2.23, there exists $x, y \in K(E)$ such that $\{1, x\}$ forms a basis for $\mathcal{L}(2(\mathcal{O}))$ and $\{1, x, y\}$ forms a basis for $\mathcal{L}(3(\mathcal{O}))$. Due to this, we see that x and y have a pole of order exactly 2 and 3 respectively, at $\mathcal{O}$. From this we have the follwing seven elements

$$1, x, x^2, x^3, xy, y, y^2 \in \mathcal{L}(6(\mathcal{O})).$$

As $\ell(6(\mathcal{O})) = 6$, the above seven elements are linearly independent over $\overline{K}$. That is, we have

$$A_0 + A_1x + A_2x^2 + A_3x^3 + B_0y + B_1xy + B_2y^2 = 0,$$

where $A_i, B_i \in \overline{K}$ and for some A_i or B_i non-zero. The interesting part is that we can assume $A_i, B_i \in K$ from Lemma 2.24.

We see $A_3 = 0$ implies $B_2y^2 + B_1xy \in \mathcal{L}(4(O))$, which is a contradiction as

$$\mathrm{ord}_{\mathcal{O}}(B_2y^2 + B_1xy) \geq 5.$$

So $A_3 \neq 0$. Similarly, $B_2 \neq 0$. To bring the above equation into the required Weierstrass form, we take $y = A_3^2B_2Y$ and $x = -A_3B_2X$. The new equation is,

$$-(a_0 + a_1X + a_2X^2 + X^3) + b_0Y + b_1XY + Y^2 = 0$$

After dividing by $A_3^4B_2^3$. As X, Y are just multiples of x, y, we take them to be our new x, y.

So the map $\phi : E \to \mathbb{P}^2$ defined by

$$\phi = [x, y, 1] \qquad , \phi(\mathcal{O}) = [0, 1, 0]$$

maps E onto the curve $C : a_0 + a_1X + a_2X^2 + X^3 = b_0Y + b_1XY + Y^2$. It is worth noting that this map is well defined, as

$$\phi(\mathcal{O}) = \left[\frac{x}{y}(\mathcal{O}), 1, \frac{1}{y}(\mathcal{O})\right] = [0, 1, 0].$$

Now we show that $\deg(\phi) = 1$. We have $\phi^* : \overline{K}(C) \to \overline{K}(E)$, so we need to show that $\phi^*(\overline{K}(C)) = \phi^*(\overline{K}(X, Y)) = \overline{K}(x, y) = \overline{K}(E)$. Consider the rational map $f = [x, 1] : E \to \mathbb{P}^1$. The point(s) $P \in E$ such that $f(P) = [1, 0]$ are the pole(s) of x, i.e., $P = \mathcal{O}$. Hence, as Y/X is a uniformiser at $[1, 0]$, we have

$$e_f(\mathcal{O}) = \deg(f) = \mathrm{ord}_{\mathcal{O}}(f^*(Y/X)) = \mathrm{ord}_{\mathcal{O}}(x^{-1}) = 2.$$

Therefore, $[\overline{K}(C) : \overline{K}(x)] = 2$. Similarly, degree of the map $[y, 1] : E \to \mathbb{P}^1$ is 3 and we have $[\overline{K}(E)) : \overline{K}(y)] = 3$. Hence we get $[\overline{K}(E) : \overline{K}(x, y)] = 1$, as it divides both 2 and 3.

The curve C is non-singular. If it weren't, by Theorem 2.22, we have a rational map

$$E \xrightarrow{\phi} C \to \mathbb{P}^1$$

where the latter map is $(a, b) \mapsto [a, b]$. The two maps have degree 1 and hence, their composition has degree 1. By the following two lemmas, we get a contradiction to the fact that C was singular.

Lemma 2.26. *Let $\phi : C_1 \to C_2$ be a rational map between two smooth curves of degree 1. Then ϕ is an isomorphism.*

Lemma 2.27. *If a curve C is isomorphic to $\mathbb{P}^1$, then C has genus 0.*

Lemma 2.26 tells that the map $E \to \mathbb{P}^1$ is an isomorphism and Lemma 2.27 says that E should have genus 0. This is the required contradiction.

From the above discussion, we have $\phi : E \to C$ to be a degree 1 map between smooth curves. So, from Lemma 2.26, we have ϕ to be an isomorphism.

(*b*) We know that $\{1, x\}$ and $\{1, x, y\}$ forms a basis for $\mathcal{L}(2(\mathcal{O}))$ and $\mathcal{L}(3(\mathcal{O}))$ respectively. As $X \in \mathcal{L}(2(\mathcal{O}))$ and $Y \in \mathcal{L}(3(\mathcal{O}))$, we have

$$X = ax + b, \qquad Y = c + dx + ey^2$$

for $a, b, c, d, e \in K$ as X, Y are defined over K. To bring it in the required form, we see that $a^3 = e^2 = 1$, as leading coefficients of x^3 and y^2 are 1 in the Weierstrass equation. By taking $u = e/a \in K^*$ and $s = d/u^2$, we get

$$X = u^2x + b, \qquad Y = c + u^2sx + u^3y^2.$$

(c) Let g be the genus of C and ω be the invariant differential. We saw in Theorem 2.21 that

$$\operatorname{div}(\omega) = 0.$$

So by taking $K_C = 0$ and applying the Riemann–Roch theorem, we get

$$g = \ell(K_C) = \ell(0) = 1.$$

Hence, $(C, [0, 1, 0])$ is an elliptic curve.

□

2.3.2 Quantities Attached to a Weierstrass Equation

Consider an elliptic curve E/K with the following non-homogeneous Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We define,

$$\begin{aligned} b_2 &= a_1^2 + 4a_4, \\ b_4 &= 3a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= b_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \\ \Delta(E) &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \text{ and} \\ j &= \frac{c_4^3}{\Delta}. \end{aligned} \tag{2.2}$$

Here, $\Delta(E)$ is called as the *discriminant* of the Weierstrass equation and j is called as the *j-invariant* of the elliptic curve E. The motivation for defining such quantities may be seen better when $\operatorname{Char}(K) \neq 2, 3$. In this case, we can transform the Weierstrass equation to the form

$$y^2 = 4x^3 - g_2x - g_3 = 4x^3 - \frac{c_4}{12}x - \frac{c_6}{216}.$$

From this we also see that

$$16\Delta = 16(g_2^3 - 27g_3^2) = \Delta',$$

where Δ' is the discriminant of the cubic $4x^3 - g_2x - g_3$.

2.4 Isogenies

In this section, we talk about special morphisms between elliptic curves that preserve the point at infinity. We will first see that the addition and inverse maps on the elliptic curve are morphisms, thus making it an abelian variety.

2.4.1 Highlights From The Group Law

We shall give the equations for the group law and not prove them.

Proposition 2.28. *Let $P = (x_1, y_1), Q = (x_2, y_2)$ be points on the elliptic curve E. We have*

$$P + Q := (x_3, y_3) = (-x_1 - x_2 + \lambda^2 + a_1\lambda - a_2, -(\lambda + a_1)x_3 - \nu - a_3)$$

where $\lambda x + \nu$ is the line passing through P, Q (or the tangent at P if $P = Q$). More specifically,

$$(\lambda, \nu) = \begin{cases} \left(\dfrac{y_2 - y_1}{x_2 - x_1}, \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}\right) & \text{if } x_1 \neq x_2, \\ \left(\dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y}{2y_1 + a_1x + a_3}, \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x + a_3}\right) & \text{if } x_1 = x_2. \end{cases}$$

From the proposition, we have the *duplication formula*,

$$x(2P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}, \tag{2.3}$$

Where $x(2P)$ is the x-coordinate of $2P$ and b_i's as defined in (2.2).

For an elliptic curve $(E, \mathcal{O})$, we have two operations from the group law. Namely,

$$\begin{aligned} &+ : E \times E \to E \ ; \quad (P, Q) \mapsto P + Q, \\ &- : E \to E \ ; \quad P \mapsto -P. \end{aligned}$$

Analogous to the cases of topological groups, where the group operations are continuous maps, and Lie groups, where the group operations are smooth maps, we have $+$ and $-$ to be morphisms between varieties.

Remark 2.29 (Segre Embedding)**.** For a projective variety $V \subseteq \mathbb{P}^n$, we look at $V \times V$ as a projective variety with respect to the *Segre embedding* of $\mathbb{P}^n \times \mathbb{P}^n$ into $\mathbb{P}^{n(n+2)}$.

Let $\{X_0, \cdots, X_n\}, \{Y_0, \cdots, Y_m\}$ be coordinates for $\mathbb{P}^n, \mathbb{P}^m$ respectively. We define the map $\phi : \mathbb{P}^n \times \mathbb{P}^m \longrightarrow \mathbb{P}^N$ as

$$\phi([X_0, \cdots, X_n], [Y_0, \cdots, Y_m]) = [X_0Y_0, X_0Y_1, \cdots, X_iY_j, \cdots, X_nY_m],$$

where $N = (n+1)(m+1) - 1$. The map ϕ defined is called as the Segre embedding. We see that ϕ maps $\mathbb{P}^n \times \mathbb{P}^m$ to a projective variety in $\mathbb{P}^N$, hence for projective varieties $V \subseteq \mathbb{P}^n, W \in \mathbb{P}^m$, $\phi(V \times W)$ is a variety in $\mathbb{P}^N$.

In our case, we look at $E \times E$ as a projective variety in $\mathbb{P}^5$.

Theorem 2.30. *The maps $+$ and $-$ defined above are morphisms.*

Proof. cf. Silverman [Sil06], Chapter III, Theorem 3.6. □

2.4.2 Isogenies

Let $(E_1, \mathcal{O}_1)$ and $(E_2, \mathcal{O}_2)$ be two elliptic curves, where $\mathcal{O}_i$ is the identity elements in the group $(E_i, +)$ for $i = 1, 2$. As always, we will denote an elliptic curve $(E, \mathcal{O})$ by just E and $\mathcal{O}$ for $\mathcal{O}_1$ and $\mathcal{O}_2$, where it will be clear which $\mathcal{O}_i$ we are talking about.

Definition 2.31. An *isogeny* between two elliptic curves E_1 and E_2 is a morphism

$$\phi : E_1 \to E_2, \text{ such that } \phi(\mathcal{O}) = \mathcal{O}.$$

We then say E_1 is *isogeneuos* to E_2.

Example 2.32. Consider the elliptic curve E with the Weierstrass equation $y^2 = x^3 - x$. Consider the map $E \to E$ defined by

$$(x, y) \mapsto (-x, iy), \quad \mathcal{O} \mapsto \mathcal{O}.$$

This is a rational map, hence a morphism, fixing $\mathcal{O}$. So, this is an isogeny from E to itself.

Example 2.33 (The Frobenius Endomorphism)**.** Let K be a field of characteristic $p > 0$ and $q = p^r$. For a curve C/K given by the the equation $F(X, Y, Z) = 0$, we can define a new curve $C^{(q)}$ as the zero set for the polynomial whose coefficients are q^{th} powers of coefficients of F.

There is a natural map $\phi_q : C \to C^{(q)}$ defined by

$$\phi_q[x_0, x_1, x_2] = [x_0^q, x_1^q, x_2^q].$$

Consider an elliptic curve E, then we see that $E^{(q)}$ has a Weierstrass equation. To see that it is non-singular, we have

$$\Delta_q = \Delta^q$$

where Δ and Δ_q are the discriminants of E and $E^{(q)}$ respectively. Hence, the Frobenius map

$$\phi_q : E \to E^{(q)}, \quad (x, y) \mapsto (x^q, y^q)$$

is a morphism and hence an isogeny.

If we take $K = \mathbb{F}_q$, then $E^{(q)} = E$ and hence $\phi_q \in \mathrm{End}(E)$. This is called as the *Frobenius Endomorphism.*

Example 2.34 (Multiplication-by-2 map)**.** Let E be an elliptic curve with the Weierstrass equation

$$y^2 + a_1xy + a_2y = x^3 + a_2x^2 + a_4x + a_6,$$

and $P = (x, y) \in E$. From the formulas of the group operation on E, we have

$$2P = (a, b) = (-2x + \lambda^2 + a_1\lambda - a_2, -(\lambda + a_1)a - \nu - a_3)$$

for λ and ν as in Theorem 2.28. Hence, the map $[2] : P \mapsto 2P$ is a rational map, and therefore a morphism. We also have $\mathcal{O} \mapsto \mathcal{O}$, implying that $[2] : E \to E$ is an isogeny.

We can talk about the set of isogenies between two elliptic curves E_1 and E_2, denoted by $\mathrm{Hom}(E_1, E_2)$, and give it a group structure. For $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$, we define their addition by

$$(\phi + \psi)(P) = \phi(P) + \psi(P).$$

But we should verify that $\phi + \psi$ is an isogeny. This is our next theorem.

Theorem 2.35. *The set* $\mathrm{Hom}(E_1, E_2)$ *forms an abelian group under* $+$*.*

Proof. It can be easily verified that, the identity element is $[0] : P \mapsto \mathcal{O}$. For an element $\phi \in \mathrm{Hom}(E_1, E_2)$, we have $-\phi$ defined by $P \mapsto -\phi(P)$. This satisfies

$$\phi + (-\phi) = [0].$$

The only thing left is to show that $\phi + \psi \in \mathrm{Hom}(E_1, E_2)$. We can see the map $\phi + \psi$ as composition of maps,

$$E_1 \xrightarrow{\phi \times \psi} E_2 \times E_2 \xrightarrow{+} E_2.$$

Let $P \in E_1$ and $\phi = [f_1, \cdots, f_r], \psi = [g_1, \cdots, g_r]$ in a neighbourhood of P. This implies that $\phi \times \psi = [f_1, \cdots, f_r, g_1, \cdots, g_r]$ is a rational map. By Theorem 2.30, $+$ is a rational map. Hence, the composition of these rational maps, $\phi + \psi$, is a rational map. As E_i's are smooth, $\phi + \psi$ is a morphism, which also satisfies $(\phi + \psi)(\mathcal{O}) = \mathcal{O}$. This proves the theorem. □

If we consider $E_1 = E_2 = E$, then we denote the set by $\mathrm{End}(E)$ and call it the *endomorphism ring* of E. This forms a ring under the multiplication,

$$(\phi\psi)(P) = \phi(\psi(P)).$$

Example 2.36 (Multiplication-by-m map)**.** We can proceed by induction to see that

$$[m] : E \to E, \quad P \mapsto mP$$

is an isogeny. [1] is the identity map and hence is an isogeny. For $m \geq 2$, we see that

$$[m] = [m-1] + [1]$$

implying $[m]$ is an isogeny. Therefore, $[m] \in \mathrm{End}(E)$.

From the above example, we have an injection of rings

$$\mathbb{Z} \longrightarrow \mathrm{End}(E)$$

defined by $m \mapsto [m]$. An elliptic curve in which that above map isn't surjective is called an elliptic curve with *complex multiplication*, or a CM elliptic curve for short.

We now see that the map $[m]$ is a non-constant map for $m \neq 0$, implying that it is surjective.

Proposition 2.37. *Let E/K,E_1/K and E_2/K be elliptic curves.*

(*a*) *The map $[m] : E \to E$ is a non-constant rational map for $m \neq 0$.*

(*b*) $\mathrm{Hom}(E_1, E_2)$ *is a torsion free abelian group.*

(*c*) $\mathrm{End}(E)$ *is a ring of characteristic* 0 *with no zero divisors.*

Proof. (*a*) Let us first prove that $[2] : E \to E$ is non-constant. From equation (2.3), we see that

$$2P = \mathcal{O} \quad \text{iff } 4x^3 + b_2x^2 + 2b_4x + b_6 = 0$$

at P.

If $\mathrm{Char}(K) \neq 2$, then the above polynomial is a non-zero polynomial and hence has only finitely many roots, implying that [2] can't be constant. If $\mathrm{Char}(K) = 2$, then [2] is a constant map iff $b_2x^2 + b_6 = 0$ at all P. This happens only when $b_2 = b_6 = 0$, implying that $\Delta = 0$. Hence, [2] is a non-constant map. From this, we also have $[2^n] = [2]^n$ to be non-constant, as [2] is surjective.

If we prove that $[m]$ is non-constant for an odd m, then, by compositing $[m]$ with $[2^n]$, we can prove it for all $m \neq 0$. The idea is to find an element Q of order 2, as it would imply that $[m]Q \neq \mathcal{O}$. The polynomial $f = 4x^3 + b_2x^2 + 2b_4x + b_6$ doesn't divide $g = x^4 - b_4x^2 - 2b_6x - b_8$, as $\Delta \neq 0$. Hence, we have a root $\alpha \in \overline{K}$ of f, such that $g(\alpha) \neq 0$. For $\beta \in \overline{K}$ such that $Q = [\alpha, \beta, 1] \in E$, we see that $x(2P)$ has a pole at Q. Hence, $2Q = \mathcal{O}$.

(*b*) Let $\phi \in \mathrm{Hom}(E_1, E_2)$ be an element of finite order, say m. This says that

$$m\phi = \underbrace{\phi + \cdots + \phi}_{m \text{ times}} = [m] \circ \phi = [0].$$

But as $[m] : E_2 \to E_2$ is non-constant, we have $\phi = [0]$.

(*c*) From (*b*), we have that $\mathrm{End}(E)$ has characteristic 0. If $\phi, \psi \in \mathrm{End}(E)$, then

$$\phi \circ \psi = [0]$$

implies that one of them must be the constant map, i.e. $\phi = [0]$ or $\psi = [0]$.

□

2.4.3 Isogenies are Homomorphisms

In this section, we prove that isogenies are homomorphisms of groups.

For a rational map $\phi : C_1 \to C_2$ between two curves C_1 and C_2 defined over K, we have the induced map on the function fields fixing $\overline{K}$

$$\begin{aligned} \phi^* &: \overline{K}(C_2) \to \overline{K}(C_1), \quad \phi^*(g) = g \circ \phi, \\ \phi_* &: \overline{K}(C_1) \to \overline{K}(C_2), \quad \phi_*(f) = (\phi^*)^{-1}(\mathbf{N}(f)), \end{aligned}$$

where $\mathbf{N}$ is the norm on $\overline{K}(C_1)$ over $\phi^*(\overline{K}(C_2))$. We also have the induced map on the divisor groups

$$\phi_* : \mathrm{Div}(C_1) \to \mathrm{Div}(C_2), \quad \sum_{P \in C_1} n_P(P) \mapsto \sum_{P \in C_1} n_P(\phi(P)).$$

Lemma 2.38 (cf. [Sil06], Proposition II.3.6. (*d*)). *For an $f \in \overline{K}(C_1)^*$, we have*

$$\phi_*(\mathrm{div}(f)) = \mathrm{div}(\phi_* f).$$

Theorem 2.39. *An isogeny between two elliptic curves is a homomorphism of groups.*

Proof. Let $\phi : E_1 \to E_2$ be an isogeny. If ϕ is the constant map, then it is the trivial homomorphism. Assume ϕ is non-constant, there is the induced map

$$\phi_* : \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2),$$

as $\phi_*(\mathrm{div}(f)) = \mathrm{div}(\phi_*(f))$. From the following commutative diagram,

$$\begin{array}{ccc} E_1 & \xrightarrow{\tau^{-1}} & \mathrm{Pic}^0(E_1) \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi_*} \\ E_2 & \xleftarrow[\tau]{} & \mathrm{Pic}^0(E_2) \end{array}$$

as τ, τ^{-1} and ϕ_* are homomorphisms, we have ϕ to be a homomorphism. □

2.4.4 Dual Isogeny

In this section, we look at the *dual* of an isogeny. The definition follows from the theorem below.

Theorem 2.40 (cf. [Sil06], Theorem III.6.1.)**.** *For a non-constant isogeny $\phi : E_1 \to E_2$,*

(a) There exists a unique isogeny $\widehat{\phi} : E_2 \to E_1$ such that

$$\widehat{\phi} \circ \phi = [\deg(\phi)] \quad \text{on } E_1$$

(b) Let τ_1 and τ_2 be the maps

$$\tau_1 : \mathrm{Div}^0(E_1) \to E_1, \quad \sum_Q n_Q(Q) \mapsto \sum_Q [n_Q]Q$$
$$\tau_2 : E_2 \to \mathrm{Div}^0(E_2), \quad P \mapsto (P) - (\mathcal{O})$$

and let

$$\phi^* : \mathrm{Div}^0(E_2) \to \mathrm{Div}^0(E_1), \quad (Q) \mapsto \sum_{P \in \phi^{-1}\{Q\}} e_\phi(P)(P).$$

be the homomorphism induced by ϕ. Then, we have

$$\widehat{\phi} = \tau_1 \circ \phi^* \circ \tau_2 : E_2 \to E_1$$

as homomorphisms.

Definition 2.41. For a non-constant isogeny $\phi : E_1 \to E_2$, there exists a unique isogeny, by Theorem 2.40, $\widehat{\phi} : E_2 \to E_1$ such that

$$\widehat{\phi} \circ \phi = [\deg(\phi)] \quad \text{on } E_1.$$

Example 2.42. Let E be an elliptic curve over a field K with $\mathrm{Char}(K) = 0$. It is easy to see that $\#\ker[2] = 4 = \deg[2]$. Hence, as

$$[2] \circ [2] = [4] = [\deg[2]],$$

we have $\widehat{[2]} = [2]$. We shall see later that this holds in general for the map $[m] : E \to E$, where $m \in \mathbb{Z}$ is non-zero, and for an arbitrary elliptic curve E.

Example 2.43. Let $\mathrm{Char}(K) \neq 2$ and

$$E_1 : y^2 = x^3 + ax^2 + bx,$$
$$E_2 : Y^2 = X^3 + AX^2 + BX$$

be two elliptic curves such that

$$A = -2a \quad \text{and} \quad B = a^2 - 4b.$$

Consider the isogeny $\phi : E_1 \to E_2$ defined by

$$\phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right).$$

For another isogeny $\psi : E_2 \to E_1$ defined by

$$\psi(X, Y) = \left(\frac{Y^2}{4X^2}, \frac{Y(B - X^2)}{8X^2} \right),$$

we see that $\psi \circ \phi = [2]$ on E_1. Therefore, as

$$\deg(\phi)\deg(\psi) = \deg[2] = \#\ker[2] = 4,$$

we see that $\deg(\phi), \deg(\psi)$ take values $1, 2$ or 4. Let $T = (0, 0) \in E_1 \cap E_2$, we see that

$$\begin{aligned}
\phi(T) &= [y^3, y^2(b - x^2), yx^2](T) \\
&= [xy(x^2 + ax + b), x(x^2 + ax + b)(b - x^2), yx^2](T) \\
&= [y(x^2 + ax + b), (x^2 + ax + b)(b - x^2), yx](T) \\
&= [0, 1, 0] = \mathcal{O}.
\end{aligned}$$

Similarly, we have $\psi(T) = \mathcal{O}$. This says that ϕ, ψ cannot be isomorphisms, as $T \in \ker\phi, \ker\psi$ and moreover $\deg(\phi), \deg(\psi) \neq 1$. Hence, as

$$\psi \circ \phi = [2] = [\deg(\phi)],$$

implying $\psi = \widehat{\phi}$.

Now we shall look at certain properties of the dual isogeny.

Proposition 2.44 (cf. [Sil06], Theorem III.6.2.)**.** *Let $\phi : E_1 \to E_2$ be an isogeny.*

(*a*) *We have*
$$\widehat{\phi} \circ \phi = [\deg(\phi)] \quad \textit{and} \quad \phi \circ \widehat{\phi} = [\deg(\phi)].$$

(*b*) *We have*
$$\deg(\widehat{\phi}) = \deg(\phi) \ \ \textit{and} \ \ \widehat{\widehat{\phi}} = \phi.$$

(*c*) *For another isogeny $\psi : E_2 \to E_3$,*
$$\widehat{\psi \circ \phi} = \widehat{\phi} \circ \widehat{\psi}.$$

(*d*) *For another isogeny $\lambda : E_1 \to E_2$, we have*
$$\widehat{\lambda + \phi} = \widehat{\lambda} + \widehat{\phi}.$$

(*e*) *For a non-zero $m \in \mathbb{Z}$,*
$$\deg[m] = m^2 \ \ \textit{and} \ \ \widehat{[m]} = [m].$$

From Proposition 2.44, we have $\widehat{\lambda + \phi} = \widehat{\lambda} + \widehat{\phi}$ and from this, we get

$$\begin{aligned} \widehat{\lambda} \circ \phi + \widehat{\phi} \circ \lambda &= [\deg(\lambda + \phi)] - [\deg(\phi)] - [\deg(\lambda)] \\ &= [\deg(\lambda + \phi) - \deg(\phi) - \deg(\lambda)]. \end{aligned}$$

We also have the injection $[\cdot] : \mathbb{Z} \to \mathrm{End}(E)$, defined by $m \mapsto [m]$. From this, we have the following proposition.

Proposition 2.45. *The map*
$$\langle\ ,\ \rangle : \mathrm{Hom}(E_1, E_2) \times \mathrm{Hom}(E_1, E_2) \longrightarrow \mathbb{Z}$$
defined by $\langle \lambda, \phi \rangle = \deg(\lambda + \phi) - \deg(\phi) - \deg(\lambda)$ is bilinear.

Proof. We see that, from above discussion,
$$[\langle \lambda, \phi \rangle] = \widehat{\lambda} \circ \phi + \widehat{\phi} \circ \lambda$$
As RHS is bilinear and using the injection $\mathbb{Z} \to \mathrm{End}(E_2)$, the proposition follows. □

Let us recall the definition of quadratic form.

Definition 2.46. Let G be an abelian group and

$$d : G \to \mathbb{R}$$

be a map. It is said to be a *quadratic form* on G if

(i) $d(g) = d(-g)$ for $g \in G$.

(ii) The pairing $\langle\ ,\ \rangle : G \times G \to \mathbb{R}$ defined by

$$\langle g, h\rangle = d(g+h) - d(g) - d(h)$$

is bilinear.

Moreover, it is said to be *positive definite* if $d(g) \geq 0$ for all $g \in G$ and $d(g) = 0$ if and only if $g = 0$.

Proposition 2.47. *The map*

$$\deg : \mathrm{Hom}(E_1, E_2) \longrightarrow \mathbb{Z}$$

is a positive definite quadratic form on $\mathrm{Hom}(E_1, E_2)$.

Proof. It is clear from the definitions and Proposition 2.45. □

The kernel of the map $[m]$ is also denoted by $E[m]$ and is called the *m-torsion points of* E.

Theorem 2.48 (cf. [Sil06], Corollary III.6.4.)**.** *Let E be an elliptic curve and $m \in \mathbb{Z}$ be non-zero. Then,*

(*a*) *If $m \neq 0$ in K, we have*

$$E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

(*b*) *If* $\mathrm{Char}(K) = p$*, we either have*

$$E[p^e] = \{\mathcal{O}\} \text{ for all } e \geq 0, \quad \text{or}$$
$$E[p^e] = \frac{\mathbb{Z}}{p^e\mathbb{Z}} \text{ for all } e \geq 0.$$

2.5 Tate Modules

2.5.1 Cyclotomic Characters

Let K be a field with $\mathrm{Char}(K) = p \geq 0$ and $\overline{K}$ be a fixed algebraic closure of K. We shall denote the set

$$\mu_m = \{a \in \overline{K} \mid a^m = 1\}$$

for the m^{th} roots of unity in $\overline{K}$. For a prime number ℓ, we have the natural maps

$$\mu_{\ell^n} \xrightarrow{a \to a^\ell} \mu_{\ell^{n-1}} \quad \text{for all } n \geq 0.$$

We see that $(\mu_{\ell^n}, \{a \mapsto a^\ell\})$ forms an *inverse system* and therefore we can talk about the *inverse limit*.

Definition 2.49. The *Tate module* of K, denoted by $T_\ell(K^*)$, is defined as the inverse limit of the inverse system $(\mu_{\ell^n}, \{a \mapsto a^\ell\})$. i.e.

$$T_\ell(K^*) := \varprojlim_n \mu_{\ell^n}.$$

Let

$$\mathbb{Z}_\ell := \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z} = \left\{ (a_n) \in \prod_{n=1}^{\infty} \frac{\mathbb{Z}}{\ell^n\mathbb{Z}} \mid a_{n+1} \equiv a_n \ (mod\ \ell^n) \right\}$$

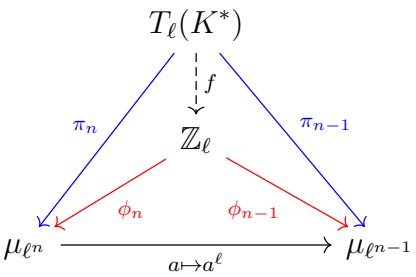
be the ring of ℓ-adic integers.

Proposition 2.50 (Structure of Tate Module of K)**.** *If $p = \mathrm{Char}(K)$, then*

$$T_\ell(K^*) \cong \begin{cases} \mathbb{Z}_\ell & \text{if } \ell \neq p, \\ \{0\} & \text{if } \ell = p. \end{cases}$$

where the isomorphism is of abelian groups.

Proof. Let $\ell \neq p$. We have the isomorphism $\mu_{\ell^n} \cong \mathbb{Z}/\ell^n\mathbb{Z}$ for all $n \geq 0$. Let $\{\zeta_n\}$ be a compatible set of generators of μ_{ℓ^n}, i.e. $\zeta_{n-1} = \zeta_n^\ell$. We have the following commutative diagrams for all $n \geq 0$.



Here π_n is the projection map and $\phi_n : 1 \mapsto \zeta_n$. This ensures the unique homomorphism $f : T_\ell(K^*) \to \mathbb{Z}_\ell$ defined by $(\zeta_n^{a_n}) \mapsto (a_n)$. The map f is easily seen to be an isomorphism.

For $\ell = p$, we have $\mu_{p^n} = \{1\}$ for all $n \geq 0$, implying $T_p(K^*) \cong \{0\}$. □

We know that $G_{\overline{K}/K} = \mathrm{Gal}(\overline{K}/K)$ acts on $T_\ell(K^*)$ as follows,

$$\sigma \cdot (\zeta_n^{a_n}) = (\sigma(\zeta_n)^{a_n}).$$

This action induces a representation $G_{\overline{K}/K} \longrightarrow \mathrm{Aut}(T_\ell(K^*))$. By the isomorphism f, we get the representation

$$\chi_\ell : G_{\overline{K}/K} \longrightarrow \mathrm{GL}_1(\mathbb{Z}_\ell) \hookrightarrow \mathrm{GL}_1(\mathbb{Q}_\ell).$$

The degree 1 representation χ_ℓ is called the *ℓ-adic cyclotomic character* over $\overline{K}^*$.

When $K = \mathbb{Q}$, χ_ℓ is surjective. For any $(m_n) \in \mathbb{Z}_\ell^*$, we have $\sigma_n \in G_\mathbb{Q}$ such that $\sigma_n(\zeta_n) = \zeta_n^{m_n}$ for all n. Let

$$B(\tau, F) = \{\sigma \in G_\mathbb{Q} \mid \sigma|_F = \tau|_F\}$$

denote a basic open ball around τ in $G_\mathbb{Q}$. Hence, we have a

$$\sigma \in \bigcap_{n \geq 1} B(\sigma_n, \mathbb{Q}(\zeta_n)),$$

such that $\chi_\ell(\sigma) = (m_n)$.

Proposition 2.51. *The representation χ_ℓ is unramified at primes $p \neq \ell$. Moreover, if σ_p is a Frobenius substitution for the prime p, then*

$$\sigma(\zeta_n) = \zeta_n^{\chi_\ell(\sigma)}, \quad \text{for all } \sigma \in G_\mathbb{Q}, \zeta_n \in \mu_{\ell^n} \tag{2.4}$$

$$\text{and} \quad \chi(\sigma_p) = p. \tag{2.5}$$

Proof. According to Remark B.8, χ_ℓ is unramified at a prime p if and only if p is unramified in the fixed field of $\ker \chi_\ell$. In this case, $\ker \chi_\ell = \mathbb{Q}(\cup_n \mu_{\ell^n})$. We know that only the prime ℓ ramifies in $\ker \chi_\ell$, implying that χ_ℓ is unramified at primes $p \neq \ell$.

The equations (2.4) and (2.5) follow from definitions. □

2.5.2 Tate Module of an Elliptic Curve

Let ℓ be a prime. For $n \geq 1$, we have the natural maps

$$\phi_{n-1}^{n} : E[\ell^n] \to E[\ell^{n-1}], \quad P \mapsto [\ell]P.$$

Definition 2.52. The *Tate Module* of an elliptic curve E, denoted by $T_\ell(E)$, is defined to be the projective limit of the inverse system $(E[\ell^n], \{\phi_{n-1}^{n} \mid n \geq 1\})$. i.e.

$$T_\ell(E) := \varprojlim_n E[\ell^n].$$

The next proposition, similar to that of Proposition 2.50, gives the structure for a Tate module of an elliptic curve.

Proposition 2.53 (Structure of Tate Module of E)**.** *If $p = \mathrm{Char}(K)$, then*

$$T_\ell(E) \cong \begin{cases} \mathbb{Z}_\ell \times \mathbb{Z}_\ell & \text{if } \ell \neq p, \\ \{0\} \text{ or } \mathbb{Z}_p & \text{if } \ell = p. \end{cases}$$

where the isomorphism is of abelian groups.

Proof. We know that

$$E[\ell^n] \cong \begin{cases} \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z} & \text{if } \ell \neq p, \\ \{0\} \text{ or } \mathbb{Z}/p^n\mathbb{Z} & \text{if } \ell = p. \end{cases}$$

The proof then is similar to Proposition 2.50. □

Remark 2.54. Let us from now on denote ℓ for a prime not equal to the characteristic of K.

The action of $G_{\overline{K}/K}$ on $E[\ell^n]$ induces an action on $T_\ell(E)$. This gives rise to a representation $G_{\overline{K}/K} \longrightarrow \mathrm{Aut}(T_\ell(E))$, which in turn gives a representation

$$\rho_\ell : G_{\overline{K}/K} \longrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell).$$

2.5.3 Tate Modules and Isogenies

Let $\phi : E_1 \to E_2$ be an isogeny. As it is a homomorphism, we have the induced map from $E_1[\ell^n] \to E_2[\ell^n]$ respectively. This in turn induces a homomorphism

$$\phi_\ell : T_\ell(E_1) \to T_\ell(E_2), \quad (P_n) \mapsto (\phi(P_n)).$$

Proposition 2.55. *The map*

$$\hom(E_1, E_2) \to \hom(T_\ell(E_1), T_\ell(E_2)), \quad \phi \mapsto \phi_\ell$$

is injective.

Proof. The above map is a homomorphism, hence it is enough to show that $\phi_\ell = 0$ implies $\phi = 0$.

We have $\phi_\ell = 0$ implies $\phi(P_n) = 0$ for all $P_n \in E[\ell^n]$ and for all $n \geq 0$. This says that

$$E[\ell^n] \subseteq \ker \phi.$$

We have $[\ell^n] : E_1 \to E_1$ to be separable for all $n \geq 0$ and we have $\lambda_n : E_1 \to E_2$ such that

$$\lambda_n \circ [\ell^n] = \phi.$$

Assume ϕ is non-constant, implying $\deg(\phi) < \infty$, we have

$$\deg(\phi) = \deg(\lambda_n \circ [\ell^n]) \geq \deg[\ell]^n = \ell^{2n} \quad \text{for all } n \geq 1.$$

As the right hand side is unbounded, we get a contradiction. Therefore, $\phi = 0$. □

Remark 2.56. We can also prove Proposition 2.55 as follows. Assuming ϕ is non-constant, for $Q \in E_2[\ell]$ we have $P \in E_1$ such that $\phi(P) = Q$. As $\mathrm{ord}(Q) = \ell$ divides $\mathrm{ord}(P)$, we have $\mathrm{ord}(P) = \ell^r k$ for some $r \geq 1$ and $\gcd(\ell, k) = 1$. Taking $P' = [k]P$ and $Q' = [k]Q$, we have

$$Q' = \phi(P') = 0 \quad (\text{as } P' \in E[\ell^r] \subseteq \ker \phi).$$

We get the desired contradiction.

We have a more stronger theorem than Proposition 2.55. Before going into that, let us look at some preliminaries.

We know that $\hom(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module. For $S = \mathbb{Z} - \{0\}$, we have the following maps

$$\hom(E_1, E_2) \hookrightarrow \hom(E_1, E_2)S^{-1} \xrightarrow{\cong} \hom(E_1, E_2) \otimes \mathbb{Q}$$

where the tensor product is between $\mathbb{Z}$-modules. Therefore, one can regard $\hom(E_1, E_2)$ as a subgroup of $\hom(E_1, E_2) \otimes \mathbb{Q}$ by the map $\phi \mapsto \phi \otimes 1$. For a sub-module M of $\hom(E_1, E_2)$, we define

$$M^{\mathrm{div}} := \{\phi \in \hom(E_1, E_2) \mid [m] \circ \phi \in M \text{ for some } m \geq 1\}.$$

We see that $M^{\text{div}} = (M \otimes \mathbb{Q}) \cap \hom(E_1, E_2)$ as a subgroup of $M \otimes \mathbb{Q}$. To see this, we have the map

$$M^{\text{div}} \to (M \otimes \mathbb{Q}) \cap \hom(E_1, E_2), \quad \phi \mapsto ([m] \circ \phi) \otimes 1/m.$$

It is seen that, as $\phi \otimes 1 = ([m] \circ \phi) \otimes 1/m$, the map is well defined. For $\psi \otimes p/q \in (M \otimes \mathbb{Q}) \cap \hom(E_1, E_2)$, we have

$$\psi \otimes p/q = \phi \otimes 1$$

for some $\phi \in \hom(E_1, E_2)$. From this we have $[p] \circ \psi = [q] \circ \phi$. Hence, $\phi \in M^{\text{div}}$ and

$$\psi \otimes p/q = ([q] \circ \phi) \otimes 1/q.$$

This shows surjectivity, and the injectivity follows by definition.

Proposition 2.57. *If M is finitely generated, then M^{div} is finitely generated.*

Proof. We can extend the degree map $\deg : \hom(E_1, E_2) \longrightarrow \mathbb{Z}$ to the map

$$\deg : \hom(E_1, E_2) \otimes \mathbb{Q} \longrightarrow \mathbb{Q}, \quad \phi \otimes p/q \mapsto (p/q)^2 \deg(\phi).$$

The fact that this is well defined follows immediately from definitions (Ref. 2.58). This can be extended to the map

$$\deg : \hom(E_1, E_2) \otimes \mathbb{R} \to \mathbb{R}, \quad \phi \otimes r \mapsto r^2 \deg(\phi)$$

on the real vector space $\hom(E_1, E_2) \otimes \mathbb{R}$. The restriction of this map to $M \otimes \mathbb{R}$ gives us a quadratic form on the finite dimensional vector space. As a quadratic form is given by a homogeneous quadratic polynomial, the degree map is continuous on $M \otimes \mathbb{R}$.

As M is a finitely generated subgroup of a torsion-free group, M is free. Hence, we have the inclusion $M \otimes \mathbb{Q} \hookrightarrow M \otimes \mathbb{R}$ induced by the inclusion $\mathbb{Q} \subset \mathbb{R}$. By this inclusion, we can look at M^{div} as a subset of $M \otimes \mathbb{R}$.

For $\psi \otimes 1 \in M^{\text{div}}$, consider the open set

$$U_\psi = \{\phi \otimes 1 \in M^{\text{div}} \mid \deg(\phi - \psi) < 1\} = \deg^{-1}(-\infty, 1) \cap M^{\text{div}}.$$

This is just the singleton $\{\psi \otimes 1\}$. Hence, M^{div} is a discrete subgroup of the finite dimensional vector space $M \otimes \mathbb{R}$. Hence, it is finitely generated. □

Remark 2.58. We look at the extension of the degree map to $M \otimes \mathbb{Q}$. For

$$\phi \otimes p/q = \psi \otimes r/s$$

we have $[sp] \circ \phi = [rq] \circ \psi$. Therefore,

$$\deg(\phi \otimes p/q) = \frac{p^2}{q^2}\deg(\phi) = \frac{r^2}{s^2}\deg(\psi) = \deg(\psi \otimes r/s).$$

This will also be a a quadratic form on the vector space $\hom(E_1, E_2) \otimes \mathbb{Q}$ as follows:

$$qs(\phi \otimes p/q + \psi \otimes r/s) = ([p]\phi + [r]\psi) \otimes 1,$$

implies that we have

$$\begin{aligned}(qs)^2\deg(\phi \otimes p/q + \psi \otimes r/s) &= \deg([ps]\phi + [qr]\psi) \\ &= p^2s^2\deg(\phi) + q^2r^2\deg(\psi) + pqrs\langle\phi, \psi\rangle.\end{aligned}$$

This gives

$$\deg(\phi \otimes p/q + \psi \otimes r/s) - \deg(\phi \otimes p/q) - \deg(\psi \otimes r/s) = pr/qs\langle\phi, \psi\rangle.$$

Hence, the degree map is a quadratic form.

Now we are ready to prove the stronger theorem. Let $\hom(T_\ell(E_1), T_\ell(E_2))$ denote the set of $\mathbb{Z}_\ell$-linear maps from $T_\ell(E_1)$ into $T_\ell(E_2)$. For an $\alpha = (a_n) \in \mathbb{Z}_\ell$, we have the natural action on $\hom(T_\ell(E_1), T_\ell(E_2))$,

$$(\alpha \cdot \psi)(P_n) = \psi(a_n P_n).$$

Theorem 2.59. *The map*

$$\hom(E_1, E_2) \otimes \mathbb{Z}_\ell \to \hom(T_\ell(E_1), T_\ell(E_2)), \quad \phi \otimes \alpha \mapsto \alpha \cdot \phi_\ell$$

is an injection.

Proof. Let $\phi = \sum_{i=1}^{k} \phi_i \otimes \alpha_i$ be in the kernel of that map. i.e. $\phi_\ell := \sum_{i=1}^{k} \alpha_i \cdot (\phi_i)_\ell = 0$. Let M be the subgroup of $\hom(E_1, E_2)$ generated by $\{\phi_i\}_{i=1}^k$ and M^{div} be generated by $\{\psi_j\}_{j=1}^s$. As they are subgroups of a torsion-free group, M and M^{div} are free. We have unique β_j'$s \in \mathbb{Z}_\ell$ such that

$$\phi = \sum_{j=1}^{s} \psi_j \otimes \beta_j.$$

So we have $\sum_{j=1}^{k} \beta_j \cdot (\psi_j)_\ell = 0$. Let $b_1, \cdots, b_s$ be the $\mathbb{Z}/\ell^n\mathbb{Z}$ components of $\beta_1, \cdots, \beta_s$ respectively. For

$$\phi_n = \sum_{j=1}^{s} [b_j] \circ \psi_j \in M^{\text{div}}$$

we have $E[\ell^n] \subseteq \ker \phi_n$ implying that there exists a $\lambda : E_1 \to E_2$ such that

$$\lambda \circ [\ell^n] = [\ell^n] \circ \lambda = \phi_n.$$

This says that $\lambda \in M^{\text{div}}$ and hence we have the unique decomposition $\lambda = [c_1] \circ \psi_1 + \cdots + [c_s] \circ \psi_s$. This says,

$$[\ell^n c_1] \circ \psi_1 + \cdots + [\ell^n c_s] \circ \psi_s = [\ell^n] \circ \lambda = \phi_n = [b_1] \circ \psi_1 + \cdots + [b_s] \circ \psi_s.$$

As $\{\psi_j\}$ forms a basis, we have $b_j = \ell^n c_j$, implying $b_j \equiv 0 \ (mod\ \ell^n)$. As n was arbitrary, we have $\beta_j = 0$ for all $j = 1, \cdots, s$. Hence, $\phi = 0$. □

Corollary 2.60. The rank of $\hom(E_1, E_2)$ as a free $\mathbb{Z}$-module is finite and is bounded by 4.

Proof. From the previous theorem, we have the injection of $\mathbb{Z}_\ell$-modules

$$\hom(E_1, E_2) \otimes \mathbb{Z}_\ell \to \hom(T_\ell(E_1), T_\ell(E_2)).$$

As $T_\ell(E_1), T_\ell(E_2)$ are isomorphic to $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$, we have a (non-canonical) isomorphism between $\hom(T_\ell(E_1), T_\ell(E_2))$ and $\text{Aut}(\mathbb{Z}_\ell \times \mathbb{Z}_\ell)$. The rank of $\hom(T_\ell(E_1), T_\ell(E_2))$ as $\mathbb{Z}_\ell$-module is 4 by the following isomorphisms,

$$\hom(T_\ell(E_1), T_\ell(E_2)) \longrightarrow \text{Aut}(\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \cong \text{M}_2(\mathbb{Z}_\ell) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell \times \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

As $\hom(E_1, E_2)$ is torsion-free, we have

$$\text{rank}_{\mathbb{Z}} \ \hom(E_1, E_2) = \text{rank}_{\mathbb{Q}} \ \hom(E_1, E_2) \otimes \mathbb{Q}$$

and

$$(\hom(E_1, E_2) \otimes \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong (\hom(E_1, E_2) \otimes \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Therefore, we have,

$$\begin{aligned} \text{rank}_{\mathbb{Z}} \ \hom(E_1, E_2) &= \text{rank}_{\mathbb{Q}} \ \hom(E_1, E_2) \otimes \mathbb{Q} \\ &= \text{rank}_{\mathbb{Z}_\ell} \ \hom(E_1, E_2) \otimes \mathbb{Z}_\ell \\ &\leq \text{rank}_{\mathbb{Z}_\ell} \ \hom(T_\ell(E_1), T_\ell(E_2)) \\ &= 4. \end{aligned}$$

□

Remark 2.61. In particular, we have $\text{rank}_{\mathbb{Z}}\text{End}(E) \leq 4$. This will help us later in studying the structure of the endomorphism ring.

2.6 Weil Pairing

Let E/K be an elliptic curve and $m \in \mathbb{Z}$ be an integer such that $m \neq 0$ in K. We know that

$$E[m] \simeq \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}. \quad (E[m] \text{ is a free } \mathbb{Z}/m\mathbb{Z}\text{-module of rank 2})$$

By a *pairing* on a free module M, we just mean a (nice) map on $M \times M$. One of the basic pairings on $E[m]$ is the *determinant pairing*. For a $\mathbb{Z}/m\mathbb{Z}$-basis $\{T_1, T_2\}$ of $E[m]$, we have the determinant map

$$\det : E[m] \times E[m] \to \mathbb{Z}/m\mathbb{Z}, \quad \det(aT_1 + bT_2, cT_1 + dT_2) = ad - bc.$$

It is easy to see that this pairing is independent of the basis for $E[m]$. This pairing need not commute with the action of the Galois group $G_{\overline{K}/K}$. i.e. $\det(P^\sigma, Q^\sigma)$ need not be same as $\det(P, Q)^\sigma$. Here, the action of $G_{\overline{K}/K}$ on $\mathbb{Z}/m\mathbb{Z}$ is the identity action.

Examples 2.62. Let $\mathrm{Char}(K) \neq 2$ and $E : y^2 = x^3 - 2$. Let $e_i = 2^{1/3}\omega^i$ for $i = 0, 1, 2$ and where ω is a primitive 3^{rd} root of unity. For $T_i = (e_i, 0)$, we have $E[2] = \{\mathcal{O}, T_0, T_1, T_2\}$. Consider an element $\sigma \in G_{\overline{K}/K}$ such that

$$\sigma : 2^{1/3} \mapsto 2^{1/3}\omega, \quad \omega \mapsto \omega^2.$$

Let $\{T_0, T_1\}$ be a basis for $E[2]$, we have

$$\det(T_0, T_2) = \det(T_0, T_0 + T_1) = 1$$
$$\det(T_0^\sigma, T_2^\sigma) = \det(T_1, T_0) = -1.$$

Hence, $\det(T_0, T_2) \neq \det(T_0^\sigma, T_2^\sigma)$.

2.6.1 The Weil Pairing on the Tate Module

We will first define the Weil e_m-pairing on $E[m] = \ker[m]$, which commutes with the action of the Galois group (Galois invariant). Let us make some observations before the definition.

We know that a divisor $D = \sum_P n_P(P) \in \mathrm{Div}(E)$ is principal if and only if

$$\sum_P n_P = 0 \quad \text{and} \quad \sum_P [n_P]P = 0.$$

Let $T \in E[m]$, we have an $f \in \overline{K}(E)$ such that

$$\mathrm{div}(f) = m(T) - m(\mathcal{O}).$$

Similarly, for T' such that $T = [m]T'$, we have a $g \in \overline{K}(E)$ such that

$$\begin{aligned}\operatorname{div}(g) &= [m]^*(T) - [m]^*(\mathcal{O}) \\ &= \sum_{R \in E[m]} (T' + R) - (R).\end{aligned}$$

We also see that $[m]^* f = f \circ [m]$ and g^m have the same divisor. Hence, we can assume, by multiplying f by a constant, $[m]^* f = g^m$.

Let $S \in E[m]$ and $X \in E$ be any point, we have

$$g^m(X + S) = (f \circ [m])(X + S) = f([m]X + [m]S) = (f \circ [m])(X) = g^m(X).$$

Hence, we have the rational function $(g \circ \tau_S)/g$ to have a finite image, the m^{th} roots of unity in $\overline{K}$. Therefore,

$$\frac{g \circ \tau_S}{g} : E \longrightarrow \mathbb{P}^1$$

as a rational function is not surjective, hence a constant.

Definition 2.63. Let μ_m denote the multiplicative group of m^{th} roots of unity in $\overline{K}$. For $T, S \in E[m]$, we define the *Weil-e_m Pairing* by the map

$$e_m : E[m] \times E[m] \to \mu_m, \quad (S, T) \mapsto \left(\frac{g \circ \tau_S}{g}\right)(X) = \frac{g(X + S)}{g(X)}.$$

Remark 2.64. Note that the selection of g depends on the choice of T. Let us call that *g is wrt T*.

Proposition 2.65 (Properties of the Weil-e_m pairing)**.**

(*a*) *Bilinearity:*

$$\begin{aligned}e_m(S, T_1 + T_2) &= e_m(S, T_1) e_m(S, T_2) \\ e_m(S_1 + S_2, T) &= e_m(S_1, T) e_m(S_2, T).\end{aligned}$$

(*b*) *For any $S, T \in E[m]$,*

$$e_m(T, T) = 1 \quad \textit{and} \quad e_m(S, T)^{-1} = e_m(T, S).$$

(*c*) *It is non-degenerate: If $e_m(T, S) = 1$ for every $S \in E[m]$, we have $T = \mathcal{O}$.*

(*d*) *It is Galois Invariant:*

$$e_m(T^\sigma, S^\sigma) = e_m(T, S)^\sigma \quad \textit{for all } \sigma \in G_{\overline{K}/K}.$$

(e) *Compatibility: For $S \in E[mn]$ and $T \in E[m]$, we have*

$$e_{mn}(S,T) = e_m([n]S,T).$$

Proof. (a) Let g be wrt T_1+T_2, and g_i be wrt T_i for $i=1,2$. We know that

$$(T_1+T_2)+(\mathcal{O}) = (T_1)+(T_2)+\mathrm{div}(h)$$

for some $h \in \overline{K}(E)$. This implies

$$(T_1+T_2)-(\mathcal{O}) = ((T_1)-(\mathcal{O}))+((T_2)-(\mathcal{O}))+\mathrm{div}(h)$$

and hence,

$$[m]^*((T_1+T_2)-(\mathcal{O})) = [m]^*((T_1)-(\mathcal{O}))+[m]^*((T_2)-(\mathcal{O}))+[m]^*\mathrm{div}(h).$$

By definition, we have

$$\mathrm{div}(g) = \mathrm{div}(g_1)+\mathrm{div}(g_2)+\mathrm{div}([m]^*h).$$

Therefore, $g/g_1g_2 = h \circ [m]$[1]. We have

$$\begin{aligned} e_m(S,T_1+T_2) &= \frac{g(X+S)}{g(S)} \\ &= \left(\frac{g_1(X+S)}{g_1(X)}\right)\left(\frac{g_2(X+S)}{g_2(X)}\right)\left(\frac{[m]^*h(X+S)}{[m]^*h(X)}\right). \end{aligned}$$

We have

$$\frac{[m]^*h(X+S)}{[m]^*h(X)} = \frac{h([m]X+[m]S)}{h([m]X)} = 1 \qquad (\text{as } S \in E[m])$$

hence,

$$e_m(S,T_1+T_2) = e_m(S,T_1)e_m(S,T_2).$$

The other equation is fairly simple. Let g be wrt T, we have

$$\begin{aligned} e_m(S_1+S_2,T) = \frac{g(X+S_1+S_2)}{g(X)} &= \frac{g(X+S_1+S_2)}{g(X+S_1)}\frac{g(X+S_1)}{g(X)} \\ &= e_m(S_1,T)e_m(S_2,T). \end{aligned}$$

[1] We have left out a scalar multiple here as it doesn't trouble us.

(*b*) We have $f \in \overline{K}(E)$ such that $\mathrm{div}(f) = m(T) - m(\mathcal{O})$. For $Q \in E$, Let τ_Q denote the usual translation-by-Q map. We have

$$\begin{aligned}\mathrm{div}\left(\prod_{n=0}^{m-1} \tau_{[n]T}^* f\right) &= \sum_{n=0}^{m-1} \tau_{[n]T}^* \mathrm{div}(f) \\ &= \sum_{n=0}^{m-1} \tau_{[n]T}^* (m(T) - m(\mathcal{O})) \\ &= m\left[\sum_{n=0}^{m-1} ([n]T) - ([-n-1]T)\right] \\ &= 0.\end{aligned}$$

This implies $\prod_{n=0}^{m-1} f \circ \tau_{[n]T}$ is a constant. So, for a T' such that $[m]T' = T$, we have

$$\begin{aligned}\prod_{n=0}^{m-1} f \circ \tau_{[n]T} = \prod_{n=0}^{m-1} f \circ [m] \circ \tau_{[n]T'} &= \prod_{n=0}^{m-1} g^m \circ \tau_{[n]T'} \\ &= \left(\prod_{n=0}^{m-1} g \circ \tau_{[n]T'}\right)^m \\ &= \text{constant}.\end{aligned}$$

Therefore, $\prod_{n=0}^{m-1} g \circ \tau_{[n]T'}$ is a constant. From this, we get

$$\prod_{n=0}^{m-1} (g \circ \tau_{[n]T'})(X) = \prod_{n=0}^{m-1} (g \circ \tau_{[n]T'})(X + T').$$

On simplifying, we have

$$\begin{aligned}&g(X)g(X+T')\cdots g(X+[m-1]T') \\ &\qquad = g(X+T')\cdots g(X+[m-1]T')g(X+T).\end{aligned}$$

By cancellation, we have

$$e_m(T,T) = \frac{g(X+T)}{g(X)} = 1.$$

To prove the next part, we see that for any $S, T \in E[m]$, we have

$$\begin{aligned}1 &= e_m(S+T, S+T) \\ &= e_m(S,S)e_m(S,T)e_m(T,S)e_m(T,T) \quad \text{(due to bilinearity)} \\ &= e_m(S,T)e_m(T,S).\end{aligned}$$

(*c*) We have $e_m(S,T) = g(S+X)/g(X) = 1$ for all $S \in E[m]$. This implies

$$(\tau_S^* g)(X) = g(X+S) = g(X), \quad \text{implying that } \tau_S^* g = g \ \ \forall S \in E[m].$$

By the fact that $m \neq 0$ in K, we have $[m]$ to be a separable map. This implies that $\overline{K}(E)$ is Galois over $[m]^*\overline{K}(E)$ and the Galois group is the set $\{\tau_S^* \mid S \in E[m]\}$. Hence, as g is fixed by every element of the Galois group, we have $g \in [m]^*\overline{K}(E)$. Let's say $g = [m]^*h$ for some $h \in \overline{K}(E)$. We have

$$[m]^*\mathrm{div}(h) = \mathrm{div}(g) = [m]^*((T) - (\mathcal{O}))$$

implying that

$$\mathrm{div}(h) = (T) - (\mathcal{O}).$$

We have seen before that this can only happen if $T = \mathcal{O}$.

(*d*) For a $\sigma \in G_{\overline{K}/K}$, we have

$$\mathrm{div}(g^\sigma) = (\mathrm{div}(g))^\sigma = [m]^*((T^\sigma) - (\mathcal{O})).$$

Hence,

$$e_m(S^\sigma, T^\sigma) = g^\sigma(X^\sigma + g^\sigma)/g^\sigma(X^\sigma) = (g(X+S)/g(X))^\sigma = e_m(S,T)^\sigma.$$

(*e*) Let $\mathrm{div}(g_1) = [mn]^*((T) - (\mathcal{O}))$ and $\mathrm{div}(g_2) = [m]^*((T) - (\mathcal{O}))$, we have

$$\mathrm{div}(g_1) = [n]^*\mathrm{div}(g_2), \quad \text{i.e. } g_1 = \lambda(g_2 \circ [n]) \text{ for some } \lambda \in \overline{K}.$$

For $S \in E[mn]$, we have

$$e_{mn}(S,T) = \frac{g_1(X+S)}{g_1(X)} = \frac{g_2([n]X + [n]S)}{g_2([n]X)} = e_m([n]S, T).$$

□

Let $\phi : E_1 \to E_2$ be a map between elliptic curves and $\widehat{\phi}$ be its dual. Let us recall that

$$\widehat{\phi} = \tau_1 \circ \phi^* \circ \tau_2 : E_2 \to E_1$$

as homomorphisms, where

$$\tau_1 : \mathrm{Div}^0(E_1) \to E_1, \quad \sum_Q n_Q(Q) \mapsto \sum_Q [n_Q]Q$$
$$\tau_2 : E_2 \to \mathrm{Div}^0(E_2), \quad P \mapsto (P) - (\mathcal{O})$$

and $\phi^* : \mathrm{Div}^0(E_2) \to \mathrm{Div}^0(E_1)$ is the induced homomorphism by ϕ.

We have also seen that $\ker \tau_1$ is the subgroup of principal divisors. Hence, for a point $Q \in E_2$, we have

$$\tau_1((\widehat{\phi}(Q)) - (\mathcal{O})) = \widehat{\phi}(Q) = \tau_1(\phi^*(\tau_2(Q))) = \tau_1(\phi^*((Q) - (\mathcal{O}))).$$

Hence, there exists an $h \in \overline{K}(E_1)$ such that

$$(\widehat{\phi}(Q)) - (\mathcal{O}) = \phi^*((Q) - (\mathcal{O})) + \mathrm{div}(h).$$

By these observations, we prove the next theorem involving the pairings in $E_1[m]$ and $E_2[m]$.

Theorem 2.66. *Let $\phi : E_1 \to E_2$ be a map between two elliptic curves and $\widehat{\phi}$ be its dual. For $S \in E_1[m]$ and $T \in E_2[m]$, we have*

$$e_m(S, \widehat{\phi}(T)) = e_m(\phi(S), T).$$

Proof. Let $g \in \overline{K}(E_1)$ and $\widehat{g} \in \overline{K}(E_2)$ be such that

$$\mathrm{div}(g) = [m]^*((T) - (\mathcal{O})) \quad \text{and} \quad \mathrm{div}(\widehat{g}) = [m]^*((\widehat{\phi}(T)) - (\mathcal{O})).$$

From the discussion before, we have

$$[m]^*((\widehat{\phi}(T)) - (\mathcal{O})) = \phi^*([m]^*((T) - (\mathcal{O}))) + \mathrm{div}([m]^*h),$$

hence,

$$\mathrm{div}(\widehat{g}) = \mathrm{div}(\phi^* g) + \mathrm{div}([m]^*h).$$

From this, we get $\widehat{g} = \lambda(\phi^* g)(h \circ [m])$ for some scalar $\lambda \in \overline{K}$.

We have

$$\begin{aligned} e_m(\phi(S), T) = \frac{g(\phi(S) + \phi(X))}{g(\phi(X))} &= \frac{(\phi^* g)(X + S)}{(\phi^* g)(X)} \\ &= \frac{\widehat{g}(X + S)}{\widehat{g}(X)} \cdot \frac{(h \circ [m])(X)}{(h \circ [m])(X + S)} \\ &= e_m(S, \widehat{\phi}(T)). \end{aligned}$$

□

We now extend the pairings on $E[\ell^n]$ to the *Weil pairing* on the Tate module $T_\ell(E)$. Let $S = (S_n)$ and $T = (T_n)$ be points in $T_\ell(E)$. Define $e : T_\ell(E) \times T_\ell(E) \to T_\ell(K)$ by

$$e(S, T) = (e_{\ell^n}(S_n, T_n)).$$

Recall that

$$T_\ell(K) := \varprojlim_n \mu_{\ell^n}.$$

To see that the pairing is well defined, we show

$$e_{\ell^n}(S_n, T_n) = e_{\ell^{n+1}}(S_{n+1}, T_{n+1})^\ell,$$

using bi-linearity and the compatibility conditions. We have,

$$\begin{aligned} e_{\ell^{n+1}}(S_{n+1}, T_{n+1})^\ell &= e_{\ell^{n+1}}(S_{n+1}, [\ell]T_{n+1}) \\ &= e_{\ell^n}([\ell]S_{n+1}, [\ell]T_{n+1}) \\ &= e_{\ell^n}(S_n, T_n). \end{aligned}$$

The properties of the Weil pairing is same as that of Proposition 2.65.

2.7 Structure of the Endomorphism Ring

In this section we look at what the endomorphism ring of an elliptic curve E looks like. First we give a general description in $\mathrm{Char}(K) = 0$ and then prove that there are only 3 possibilities. They are,

- An order in $\mathbb{Q}$.
- An order in an imaginary quadratic field.
- An order in a quaternion algebra.

2.7.1 The Invariant Differential

We look at some properties of the invariant differential ω attached to an elliptic curve and then in the end prove that the endomorphism ring $\mathrm{End}(E)$ is an integral domain, when the base field is of characteristic 0.

For a Weierstrass equation

$$E : y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$$

of the elliptic curve E, we have the attached invariant differential

$$\omega = \frac{dx}{2y + a_1x + a_3}.$$

We know justify the name invariant.

Proposition 2.67. *Let E be an elliptic curve and τ_Q denote the translation-by-Q map. We have*

$$\tau_Q^*\omega = \omega.$$

Remark 2.68. Let us recall the *push forward* of a differential by a map $\phi : C_1 \to C_2$ between curves. For $gdf \in \Omega(C_1)$, we define $\phi^*(gdf) = (\phi^* g)d(\phi^* f)$. One of the properties we will use in the next proof is that

$$\phi^*(\mathrm{div}(gdf)) = \mathrm{div}(\phi^* gdf).$$

Proof. Let $Q \in E$. As $\Omega(E)$ is a 1-dimensional $\overline{K}(E)$ vector space, we have an $f_Q \in \overline{K}(E)$ such that

$$f_Q = \frac{\tau_Q^*\omega}{\omega} = \left(\frac{d(\tau_Q^* x)}{dx}\right)\left(\frac{2y + a_1 x + a_3}{2(\tau_Q^* y) + a_1(\tau_Q^* x) + a_3}\right).$$

So, for $P \in E$, we have

$$f_Q(P) = \frac{d(\tau_Q^* x)}{dx}(P)\left(\frac{2y(P) + a_1 x(P) + a_3}{2y(P+Q) + a_1 x(P+Q) + a_3}\right).$$

We also have

$$\mathrm{div}(f_Q) + \mathrm{div}(\omega) = \mathrm{div}(\tau_Q^*\omega) = \tau_Q^*(\mathrm{div}(\omega)).$$

As $\mathrm{div}(\omega) = 0$, we have f_Q to be a constant map. For a fixed $P \in E$, as $f_Q(P)$ is a rational function in $x, y, \tau_Q^* x$ and $\tau_Q^* y$, we have $g(Q) := [f_Q(P), 1]$ to be a rational map. As g misses $[0,1]$ and $[1,0]$, g is a constant map. Hence, $g(Q) = g(\mathcal{O}) = 1$, implying $\tau_Q^*\omega = \omega$. □

The next theorem is the theorem required to prove that $\mathrm{End}(E)$ is an integral domain, when $\mathrm{Char}(K) = 0$. It also helps us to see that for an $m \in \mathbb{Z}$ which is co-prime to the characteristic of K, the map $[m] : E \to E$ is separable.

Theorem 2.69 (cf. [Sil06], Theorem III.5.2.)**.** *Let E_1, E_2 be elliptic curves and ω be an invariant differential*[2] *for E_1. For isogenies $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$, we have*

$$(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega.$$

[2] Note that the invariant differential is for a Weierstrass equation and an elliptic curve can have more than one Weierstrass equation.

Corollary 2.70. For an $m \in \mathbb{Z}$, we have

$$[m]^*\omega = m\omega.$$

Moreover, $[m]$ is separable if and only if $m \neq 0$ in K.

Corollary 2.71. For an element $\phi \in \mathrm{End}(E)$, we have $a_\phi \in \overline{K}$ such that

$$\phi^*\omega = a_\phi\omega.$$

Moreover, we have a homomorphism

$$\mathrm{End}(E) \to \overline{K}, \quad \phi \mapsto a_\phi.$$

More specifically, if $\mathrm{Char}(K) = 0$, then the above map is an inclusion (hence, implying $\mathrm{End}(E)$ is commutative).

Proof. We have an $a_\phi \in \overline{K}(E)$ such that

$$\phi^*\omega = a_\phi\omega.$$

Similarly as before,

$$\begin{aligned}\mathrm{div}(a_\phi) &= \mathrm{div}(\phi^*\omega) - \mathrm{div}(\omega) \\ &= \phi^*(0) - 0 \\ &= 0.\end{aligned}$$

Implying $a_\phi \in \overline{K}$. The map

$$\mathrm{End}(E) \longrightarrow \overline{K}, \quad \phi \mapsto a_\phi$$

is a homomorphism due to Theorem 2.69. If ϕ is in the kernel, we see that $\phi^*\omega = 0$, implying that ϕ is inseparable. If $\mathrm{Char}(K) = 0$, as the $[0]$ map is the only inseparable map, implying that $\mathrm{End}(E) \hookrightarrow \overline{K}$. □

2.7.2 A Special Ring Structure

From our earlier discussions, we have the following structure of the endomorphism ring of an elliptic curve.

- It is a ring with characteristic 0 with no zero-divisors.
- It is a free $\mathbb{Z}$-module of rank at most 4.

- There is a dual map (sometimes called as an anti-involution)

$$\mathrm{End}(E) \to \mathrm{End}(E), \quad \phi \mapsto \widehat{\phi}$$

with properties,

  - For a $\phi \in \mathrm{End}(E)$, we have $\widehat{\phi}\phi \in \mathbb{Z}_{\geq 0}$. (Note that $\mathbb{Z}$ here is the isomorphic image of $\{[m] \in \mathrm{End}(E) \mid m \in \mathbb{Z}\}$.) We also have $\widehat{\phi}\phi = 0$ if and only if $\phi = 0$.
  - For $\phi, \psi \in \mathrm{End}(E)$,

$$\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi} \quad \text{and} \quad \widehat{\phi\psi} = \widehat{\psi}\widehat{\phi}.$$

We see that any ring with the above properties can only have three possibilities as we stated at the start of this section.

Definition 2.72. Let K be a finitely generated algebra (not necessarily commutative) over $\mathbb{Q}$. A subring R of K is called as an *order* in K if,

(a) R is a finitely generated $\mathbb{Z}$-module.

(b) $R \otimes \mathbb{Q} \cong K$.

Example 2.73. For a number field $K/\mathbb{Q}$, the ring of integers $\mathcal{O}_K$ in K is an order in K.

For the number field $K = \mathbb{Q}(\sqrt{-D})$, where $D > 0$, we see that $R = \mathbb{Z} + n\mathcal{O}_K$ is an order in K for $n \in \mathbb{N}$. If $\mathcal{O}_K = \mathbb{Z} + \alpha\mathbb{Z}$, then $R = \mathbb{Z} + n\alpha\mathbb{Z}$.

Example 2.74. Let $K = M_n(\mathbb{Q})$ be the set of $n \times n$ matrices with rational entries. The subring $M_n(\mathbb{Z})$ is an order in K.

Definition 2.75. A quaternion algebra over $\mathbb{Q}$ is the algebra $\mathbb{Q}(\alpha, \beta)$ such that

$$\alpha^2, \beta^2, (\alpha\beta)^2 < 0 \quad \text{and } \alpha\beta = -\beta\alpha.$$

The next general theorem will help us characterize $\mathrm{End}(E)$.

Theorem 2.76. *Let R be a ring with the following properties.*

(*a*) *It is a ring with characteristic* 0 *with no zero-divisors and* $1 \in R$.

(*b*) *It is a free $\mathbb{Z}$-module of rank at most* 4.

(*c*) *There is a dual map $a \mapsto \widehat{a}$ (sometimes called as an anti-involution) satisfying,*

- *For $a \in R$, we have $\widehat{a}a \in \mathbb{Z}_{\geq 0}$ and $\widehat{a}a = 0$ if and only if $a = 0$.*
- *For $a \in R$, we have*

$$\widehat{\widehat{a}} = a, \quad \widehat{ab} = \widehat{b}\widehat{a}, \quad \widehat{a+b} = \widehat{a} + \widehat{b}$$

and for $a \in \mathbb{Z}$, we have $\widehat{a} = a$.

Then, R is one of the following.

(*i*) *An order in $\mathbb{Q}$.*

(*ii*) *An order in an imaginary quadratic field.*

(*iii*) *An order in the quaternion algebra.*

Proof. It is enough to show that $K = R \otimes \mathbb{Q}$ is either $\mathbb{Q}$ or an imaginary quadratic field or a quaternion algebra.

We can extend the anti-involution to K by defining

$$\widehat{\phi \otimes a} = \widehat{\phi} \otimes a.$$

For $\psi = \phi \otimes a$, we have

$$\widehat{\psi}\psi = \left(\widehat{\phi \otimes a}\right)(\phi \otimes a) = \widehat{\phi}\phi \otimes a^2 = 1 \otimes (\widehat{\phi}\phi)a^2.$$

Consider the map $N : K \to \mathbb{Q}$ defined by $\psi \mapsto (\widehat{\phi}\phi)a^2$. For $\psi \in K$, we have

$$N(1 - \psi) = 1 - (\psi + \widehat{\psi}) + N(\psi).$$

This ensures the map $T : K \to \mathbb{Q}$ defined by $\psi \mapsto \widehat{\psi} + \psi$.

For a non-zero $\psi \in K$ such that $T(\psi) = 0$, we have $\widehat{\psi} = -\psi$. This implies

$$\psi^2 = -N(\psi) < 0.$$

If $K = \mathbb{Q}$, we are done. If not, for $\alpha \in K \setminus \mathbb{Q}$, we have $T(\alpha - T(\alpha)) = 0$. Hence, by replacing α by $\alpha - T(\alpha)$, we take α such that $T(\alpha) = 0$. This implies $\alpha^2 < 0$ and hence, $\mathbb{Q}(\alpha) \subseteq K$.

If $K = \mathbb{Q}(\alpha)$, we are done. If not, then there is a $\beta \in K \setminus \mathbb{Q}(\alpha)$ such that $T(\beta) = 0$. We also want $T(\alpha\beta) = 0$, so we consider $\beta' = a\alpha + b\beta \in \mathbb{Q}(\alpha, \beta)$ such that $T(\alpha\beta') = 0$. By solving the two equations, we get

$$\beta' = -b\frac{T(\alpha\beta)}{2\alpha^2}\alpha + b\beta.$$

So, by taking β instead of β', we have $\mathbb{Q}(\alpha, \beta) \subseteq K$. As K is a vector space of dimension ≤ 4, it is enough to show that $\{1, \alpha, \beta, \alpha\beta\}$ is a linearly independent set. Let

$$a + b\alpha + c\beta + d\alpha\beta = 0.$$

By applying T both sides, we have $a = 0$. By multiplying by α both sides, we have

$$b\alpha^2 + c\beta\alpha = d\alpha^2\beta.$$

As $\beta \notin \mathbb{Q}(\alpha)$, we have $d = 0$. By the same argument, $b = c = 0$. Hence, $K = \mathbb{Q}(\alpha, \beta)$, a quaternion algebra. □

Corollary 2.77. The Endomorphism ring of an elliptic E, $\mathrm{End}(E)$, is either an order in $\mathbb{Q}$ or an imaginary quadratic field or a quaternion algebra. If $\mathrm{Char}(K) = 0$, then it is only the first two.

Proof. This follows from the above theorem and by the fact that $\mathrm{End}(E)$ is commutative when $\mathrm{Char}(K) = 0$. □

Examples 2.78.

1. The elliptic curve $E : y^2 = 4x^3 + x + 1$ over $\mathbb{C}$ has no complex multiplication as it's j-invariant, $j = 24^3/35$, is not an algebraic integer.

2. Consider the elliptic curve $E : y^2 = x^3 - x$ over $\mathbb{C}$. We have the isogeny

   $$[i] : (x, y) \mapsto (-x, iy).$$

   As $[i]^2 : (x, y) \mapsto (x, -y)$ and $-(x, y) = (x, -y)$, we have $[i]^2 = [-1]$. Hence,

   $$\mathrm{End}(E) \cong \mathbb{Z}(i).$$

3. For $q = p^r$, let $K = \mathbb{F}_q$ be a finite field and E be an elliptic curve over K. We have the Frobenius endomorphism $(x, y) \mapsto (x^p, y^p)$ of degree p. This is not a multiplication-by-m map for any m as the latter has degree m^2. Hence, $\mathrm{End}(E) \neq \mathbb{Z}$.

4. Let $K = \mathbb{F}_q$ and $E : y^2 = x^3 - x$. Let i denote the square root of -1 in $\overline{\mathbb{F}_q}$, we have the map (as in Example 2) $[i] : E \to E$ defined by $(x, y) \mapsto (-x, iy)$. If $p \equiv 3 \ (mod\ 4)$, then we have $\mathrm{End}(E) \neq \mathbb{Z}[i]$, as the Frobenius endomorphism ϕ_p is not there in $\mathbb{Z}[i]$. This is seen as follows.

   If $\phi_p = [a] + [b][i]$, then $\widehat{\phi_p} = [a] - [b][i]$. This implies,

   $$[p] = [\deg \phi_p] = \widehat{\phi_p}\phi_p = ([a] - [b][i])([a] + [b][i]) = [a^2 + b^2].$$

Hence, $p = a^2 + b^2$. By Fermat's two square theorem, we have $p \equiv 1 \ (mod\ 4)$. Hence, for $p \equiv 3 \ (mod\ 4)$, the $\mathrm{End}(E)$ is an order in a quaternion algebra.

3. THE CHEBOTAREV DENSITY THEOREM

The Chebotarev Density Theorem is a theorem about the density of certain primes. More precisely, given a finite Galois extension E/K with Galois group G, the theorem states that the set of primes whose Frobenius substitutions lie in a conjugacy class C of G are equally distributed.

In this section, we first look at the classical Chebotarev Theorem for finite Galois extensions and later move on to the case of an infinite Galois extension whose Galois group is a compact ℓ-adic Lie group. In the latter, we find a bound for the the set $\{p \leq x \mid \sigma_p \in C\}$, for a closed set C of G which is stable under conjugation.

The reference for this section is §2 of [Ser81].

3.1 Effective Forms of the Theorem of Chebotarev

3.1.1 The Theorem of Chebotarev

Let E/K be a finite Galois extension of number fields, an let $G = \mathrm{Gal}(E/K)$. Let us stick to the following notations:

$$n_E = [E : \mathbb{Q}], n_K = [K : \mathbb{Q}],$$
$$n = [E : K] = n_E/n_K = |G|.$$

Let us recall that a *place* in a number field K is an equivalence class of absolute values on K. Moreover, let Σ_K denote the set of places corresponding to non-archimedean absolute values. A place $v \in \Sigma_K$ corresponds (one-one) to a prime ideal $\mathfrak{p}_v$ in $\mathcal{O}_K$. We denote $\mathrm{N}v$ to be the norm of $\mathfrak{p}_v$, $\mathrm{N}\mathfrak{p}_v$, in $\mathcal{O}_E$.

Recall that a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ *ramifies* in E if there is a prime ideal $\mathfrak{P}$ in $\mathcal{O}_E$ such that $\mathfrak{P}^2|\mathfrak{p}$. Similarly, a place v of K *ramifies* in E if $\mathfrak{p}_v$ ramifies in E. Let,

$$V(E/K) = \{v \in \Sigma_K \mid v \text{ ramifies in } E\}.$$

Let $v \in \Sigma_K - V(E/K)$ and $w \in \Sigma_E$ be an extension of v (i.e. $w|v$). Consider the exact sequence,

$$1 \longrightarrow I(w/v) \longrightarrow \mathrm{Gal}(E_w/K_v) \longrightarrow \mathrm{Gal}(\mathbb{F}_w/\mathbb{F}_v) \longrightarrow 1,$$

where $\mathbb{F}_v$ and $\mathbb{F}_w$ are the residue fields of K_v and E_w, $I(w/v)$ is the inertia group of w over v. As v is unramified in E, $I(w/v) = 1$ and hence we have the isomorphism

$$\mathrm{Gal}(E_w/K_v) \cong \mathrm{Gal}(\mathbb{F}_w/\mathbb{F}_v).$$

Define the *Frobenius element* of w to be the element $\sigma_w \in \mathrm{Gal}(E_w/K_v)$ such that, under the above isomorphism, it maps the the Frobenius automorphism in $\mathrm{Gal}(\mathbb{F}_w/\mathbb{F}_v)$. Therefore, it satisfies

$$\sigma_w(a) \equiv a^{\mathrm{N}v} \bmod \mathfrak{p}_v.$$

If we take another place w' lying above v, then σ_w and $\sigma_{w'}$ are conjugates. We call an element or the whole conjugacy class as the *Frobenius substitution* at v in E. We denote this conjugacy class or any other element of it by σ_v.

For a subset C of G, closed under conjugation, let

$$\Sigma_C = \{v \in \Sigma_K - V(E/K) \mid \sigma_v \in C\}.$$

Now we are ready to see the statement of the classical Chebotarev density theorem which was first, conjectured by Frobenius, proved by Chebotarev.

Theorem 3.1. *The density of the set Σ_C in Σ_K is $|C|/|G|$.*

To be precise, let $\pi_K(x) = \#\{v \in \Sigma_K \mid \mathrm{N}v \leq x\}$ and $\pi_C(x) = \#\{v \in \Sigma_C \mid \mathrm{N}v \leq x\}$. According to the *prime number theorem* on K, we have

$$\pi_K(x) \sim x/\log x \quad \text{as } x \to \infty. \tag{3.1}$$

Saying that Σ_C has density $\lambda = |C|/|G|$ means that,

$$\lim_{x\to\infty} \pi_C(x)/\pi_K(x) = \lambda, \tag{3.2}$$

In other words,

$$\pi_C(x) = \lambda x/\log x + o(x/\log x) \quad \text{as } x \to \infty. \tag{3.3}$$

Theorem 3.1 says that the Frobenius substitutions are equally distributed amongst the conjugacy classes of G.

Remark 3.2. Taking $K = \mathbb{Q}$ and $E = \mathbb{Q}(\zeta_m)$, the m-th cyclotomic extension of $\mathbb{Q}$, and applying the Chebotarev density theorem for a conjugacy class $\{a + m\mathbb{Z}\}$ with $(a, m) = 1$, we have a stronger version of the *Dirichlet's theorem for primes in arithmetic progression*. i.e. Given an arithmetic progression $a + m\mathbb{Z}$, where $\gcd(a, m) = 1$, the density of primes in this arithmetic progression is $1/\phi(m)$.

3.1.2 An Effective Form of the Theorem

By an effective form, we mean giving a bound for the error term $o(x/\log x)$ in (3.3). The bound involves an *exceptional root* of the Dedekind zeta function for E.

The Dedekind zeta function for E is the analytic (meromorphic) continuation, also denoted ζ_E, of the function

$$\zeta_E(s) = \sum_{\mathfrak{m}\subseteq\mathcal{O}_E} \mathrm{N}\mathfrak{m}^{-s}, \quad \mathrm{Re}(s) > 1,$$

to $\mathbb{C}$. When $E = \mathbb{Q}$, we have $\zeta_E(s) = \zeta(s)$, the usual Riemann zeta function.

Let d_E denote the absolute value of the *discriminant* of E. According to Lemma 3 of [Sta74], we have the following theorem about real zeros of ζ_E.

Proposition 3.3. *There is at most one real zero $s > 0$ such that,*

$$1 - s \leq 1/(4 \log d_E).$$

If this zero exists, then denote it by β.

The following theorem (cf. §2.2, [Ser81]) gives an effective form of the Chebotarev Density Theorem due to Lagarias and Odlyzko. As before, let C be a subset of G closed under conjugation and let $|\tilde{C}|$ denote the number of conjugacy classes in C.

Theorem 3.4. *There exists absolute constants $c_1, c_2, c_3 > 0$ such that*

$$\left|\pi_C(x) - \frac{|C|}{|G|}\mathrm{Li}(x)\right| \leq \frac{|C|}{|G|}\mathrm{Li}(x^\beta) + c_1|\tilde{C}|x\exp\left(-c_2 n_E^{-1/2}\log^{1/2} x\right) \tag{3.4}$$

for all $x \geq 2$ such that $\log x \geq c_3 n_E \log^2 d_E$.

In the above Theorem 3.4, by an *absolute constant*, we mean a constant independent of E, K, C, G and x. Moreover, in (3.4), if there doesn't exist a real zero β, then we delete the term $\dfrac{|C|}{|G|}\mathrm{Li}(x^\beta)$.

Example 3.5. Consider $K = \mathbb{Q}$ and a conjugacy class C of $G = \mathrm{Gal}(E/\mathbb{Q})$.

If we assume (GRH), then β doesn't exist. If it did exist, then $\beta = 1/2$, implying that

$$\log d_E \leq 1/2, \quad \text{i.e. } d_E \leq \sqrt{e}.$$

This implies $d_E = 1$, i.e. $E = \mathbb{Q}$. Now we know that the Riemann zeta function $\zeta(s)$ doesn't have a real positive root.

We have,

$$\left|\pi_C(x) - \frac{|C|}{|G|}\mathrm{Li}(x)\right| \leq c_1 x\exp\left(-c_2|G|^{-1/2}\log^{1/2} x\right).$$

Remark 3.6. For an exceptional zero $\beta < 1$, we see that

$$\mathrm{Li}(x^\beta) = O(x/(\log x)^2). \tag{3.5}$$

To see (3.5), we note that $\mathrm{Li}(x) = x/\log x + O(x/(\log x)^2)$ and hence,

$$\mathrm{Li}(x^\beta) = \frac{x^\beta}{\beta\log x} + O(x/(\log x)^2).$$

As $\beta < 1$, we have

$$\frac{x^\beta}{\log x} = O(x/(\log x)^2),$$

hence proving (3.5). Hence, we have

$$\pi_C(x) = \frac{|C|}{|G|}\frac{x}{\log x} + O(x/(\log x)^2). \tag{3.6}$$

Remark 3.7 (Effective form of the Theorem under (GRH))**.** According to Serre [Ser81], Section §2.4, there exists an absolute constant c_6 such that

$$\left|\pi_C(x) - \frac{|C|}{|G|}\mathrm{Li}(x)\right| \leq c_6 \frac{|C|}{|G|} x^{1/2}(\log d_E + n_E \log x). \tag{3.7}$$

Let us now see a bound for $\pi_C(x)$ due to Lagarias-Montgomory-Odlyzko, which will be used later in the proof of Theorem 3.9.

Proposition 3.8 (cf. §2.3, Theorem 3, [Ser81])**.** *For a finite Galois extension E/K with Galois group G, a subset C of G closed under conjugation and discriminant d_E, there exists absolute constants c_4, c_5 such that*

$$\pi_C(x) \leq c_4 \frac{|C|}{|G|}\mathrm{Li}(x) \tag{3.8}$$

for $x \geq 3$ such that

$$\log x \geq c_5(\log d_E)(\log\log d_E)(\log\log\log 6d_E). \tag{3.9}$$

3.2 Chebotarev Like Theorem: ℓ-adic case

Let G be a *compact ℓ-adic Lie group*, C be a closed subset of G which is stable under conjugation, and let E be an infinite Galois extension of K, with Galois group G, unramified outside a finite set $S \subseteq \Sigma_K$.

This set-up usually occurs when we have a Galois representation $\rho : G_K \to \mathrm{GL}_n(\mathbb{Q}_\ell)$, unramified outside a finite set, and the image of ρ is an open subset, hence a submanifold, of the ℓ-adic Lie group $\mathrm{GL}_n(\mathbb{Q}_\ell)$. As G_K is compact in its Krull topology and the Galois representation is continuous, the image of ρ, call it G_ρ, is a compact ℓ-adic Lie group. Moreover,

$$G_\rho = \mathrm{Gal}(K_\rho/K), \quad K_\rho = \text{fixed field of } \ker\rho.$$

Similarly as before, for a place $v \in \Sigma_K - S$, we have the Frobenius substitution (defined up to conjugacy) at v with respect to E/K. Let us denote

$$\Sigma_C = \{v \in \Sigma_K - S \mid \sigma_v \in C\},$$
$$\pi_C(x) = \#\{v \in \Sigma_C \mid \mathrm{N}v \leq x\}.$$

The applications of the following Chebotarev like theorem are seen in the sections on applications to modular forms and elliptic curves.

Theorem 3.9 (cf. Theorem 10, [Ser81]). *Let d be a real number such that $0 \leq d < N$ and let $\dim_M C \leq d$. Taking $\alpha = (N-d)/N$, we have:*

i)

$$\pi_C(x) = O\left(\frac{\mathrm{Li}(x)}{\epsilon(x)^\alpha}\right) \quad as\ x \to \infty, \tag{3.10}$$

where,

$$\epsilon(x) = \log x (\log\log x)^{-2} (\log\log\log x)^{-1}. \tag{3.11}$$

ii) (Assuming GRH)

$$\pi_C(x) = O\left(\frac{\mathrm{Li}(x)}{\epsilon_R(x)^\alpha}\right) \quad as\ x \to \infty, \tag{3.12}$$

where,

$$\epsilon_R(x) = x^{1/2} (\log x)^{-2}. \tag{3.13}$$

Here, $\dim_M C$ is the M-dimension of the closed subset C (cf. Appendix).

Corollary 3.10. For all $\epsilon > 0$, we have

$$\pi_C(x) = O(x/(\log x)^{1+\alpha-\epsilon}). \tag{3.14}$$

and, under (GRH), we have

$$\pi_C(x) = O(x^{1-\alpha/2+\epsilon}). \tag{3.15}$$

Proof of Corollary. It follows from the following facts,

$$\begin{aligned} \mathrm{Li}(x) &\sim x/\log x, \\ \epsilon(x)^{-1} &= O((\log x)^{-1+\delta}) \quad \text{for all } \delta > 0, \\ \epsilon_R(x)^{-1} &= O(x^{-1/2+\delta}) \quad \text{for all } \delta > 0. \end{aligned}$$

□

Example 3.11 (Cyclotomic Extensions). Consider the ℓ-adic cyclotomic character,

$$\chi_\ell : G_{\mathbb{Q}} \to \mathbb{Z}_\ell^*,$$

induced by the action of $G_{\mathbb{Q}}$ on $T_\ell(\mathbb{Q}) = \varprojlim \mu_{\ell^n}$. If $K_\ell = \mathbb{Q}(\cup_n \mu_{\ell^n})$ is the unramified extension containing all the ℓ^n-th roots of unity, then $\ker \chi_\ell = \mathrm{Gal}(\overline{Q}/K_\ell)$ and

$$\mathrm{Gal}(K_\ell/\mathbb{Q}) \cong \mathbb{Z}_\ell^*. \tag{*}$$

As $\mathbb{Z}_\ell^*$ is abelian, every conjugacy class is singleton. We also know that the extension K_ℓ is unramified at all primes $p \neq \ell$. From the above notation, we have $S_K = \{\ell\}$.

For the Frobenius substitution $\sigma_p \in \mathrm{Gal}(K_\ell/\mathbb{Q})$ at a prime $p \neq \ell$, we have

$$\sigma_p(\zeta_n) = \zeta_n^p, \quad \text{for } \zeta_n \in \mu_{\ell^n}.$$

For $(a_n) \in \mathbb{Z}_\ell^*$, let $\sigma_p \in \{(a_n)\}$, i.e. the image of σ_p under the above isomorphism (*) is (a_n). Hence, we have

$$p \equiv a_n \bmod \ell^n \quad \text{for all } n.$$

When we apply Theorem 3.9 in this set-up, for the conjugacy class $C = \{(a_n)\}$, we have $\alpha = 1$ and

$$\pi_C(x) = O(\mathrm{Li}(x)/\epsilon(x)) \quad \text{as } x \to \infty.$$

Moreover, from Corollary 3.10, we get

$$\pi_C(x) = O(x/(\log x)^{2-\epsilon}).$$

3.2.1 Proof of Theorem 3.9

Let $\mathfrak{g}$ be the Lie algebra of G. We have the logarithm map $\log_G : G \to \mathfrak{g}$, which is a local isomorphism. Moreover (cf. [Ser81] §4.2) we have an open normal subgroup $G(0)$ of G and a $\mathbb{Z}_\ell$-lattice $\mathfrak{g}(0)$ such that $\log_G : G(0) \to \mathfrak{g}(0)$ is an isomorphism of ℓ-adic Lie groups.

Define $\mathfrak{g}(n) = \ell^n \mathfrak{g}(0)$ and

$$G(n) = \{g \in G(0) \mid \log_G g \in \mathfrak{g}(n)\} = \log_G^{-1}(\mathfrak{g}(n)).$$

For an $h \in G$, $g \in G(0)$, we have

$$hg^n h^{-1} = (hgh^{-1})^n.$$

As $G(0)$ is normal, $G(n)$ is also normal in G. From the fact that $\mathbb{Z}_\ell$ is open in $\mathbb{Q}_\ell$, we have $\mathfrak{g}(n)$ to be an open subset of $\mathfrak{g}$. Hence, the group $G(n)$ is an open normal subgroup of G.

Let us define $G_n = G/G(n)$, we have

$$|G_n| = [G : G(0)][G(0) : G(n)].$$

By the $\log_G$ map, we have a bijection

$$G(0)/G(n) \to \mathfrak{g}(0)/\mathfrak{g}(n).$$

Hence, $[G(0) : G(n)] = |\mathfrak{g}(0)/\mathfrak{g}(n)| = \ell^{nN}$. Call $[G : G(0)] = a$, we have

$$G_n = a\ell^{nN}. \tag{3.16}$$

Let $C_n = \{c+G(n) \mid c \in C\}$ be the image of C under the projection $G \to G_n$. By the hypothesis $\dim_M(C) \leq d$, we have

$$|C_n| = O(\ell^{nd}) \quad \text{as } x \to \infty.$$

Hence, using (3.16), we have

$$|C_n|/|G_n| = O(1/|G_n|^{\alpha}) \quad \text{where } \alpha = (N-d)/N. \tag{3.17}$$

From the fundamental theorem of infinite Galois theory, as $G(n)$ is closed (as it is open) in G, we have a finite Galois extension E_n/K such that its Galois group is G_n. Note that, the map $G \to G_n$ is just the restriction-to-E_n map, with kernel $G(n)$.

Lemma 3.12. *We have the inequality $\pi_C(x) \leq \pi_{C_n}(x)$.*

Proof. For $v \in \Sigma_C$, we have

$$\sigma_v(a) \equiv a^{\mathrm{N}v} \bmod \mathfrak{P}, , \quad \text{for all } a \in \mathcal{O}_E$$

where $\mathfrak{P}$ is the prime in E above $\mathfrak{p}_v$. Therefore, by restricting σ_v to E_n, we have

$$\sigma_{v,n}(a) := \sigma_v|_{E_n}(a) \equiv a^{\mathrm{N}v} \bmod \mathfrak{P}_n, \quad \text{for all } a \in \mathcal{O}_{E_n}$$

where $\mathfrak{P}_n$ is the prime in E_n above $\mathfrak{p}_v$. Hence, $\sigma_{v,n}$ is a Frobenius substitution at v in E_n. Moreover, $\sigma_{v,n} \in C_n$ as it is the image of σ_v under the restriction map $G \to G_n$. □

Proof of (i)**:**

Our aim is to find a suitable n and use Proposition 3.8 to the finite Galois extension E_n.

Let $b \in \mathbb{R}$ such that $bc_5 n_k < 1$. If x is large enough, there exists a unique $n = n(x)$ such that

$$b\ell^{-N}\epsilon(x) < |G_n| \leq b\epsilon(x). \tag{3.18}$$

By calculation, such an $n = \log(a^{-1}b\epsilon(x))/N \log \ell$.

Proposition 3.13. *For such an n, we have*

$$\log x \geq c_5(\log d_{E_n})(\log\log d_{E_n})(\log\log\log 6d_{E_n}).$$

Proof. According to Equation (76) of [Ser81], we have

$$\log d_{E_n} \leq (n_K + o(1))|G_n| \log |G_n|.$$

From (3.18), we have

$$\begin{aligned}\log d_{E_n} &\leq (n_K + o(1))b\epsilon(x)\log\epsilon(x)\\ &\leq (n_K + o(1))b\log x(\log\log x)^{-1}(\log\log\log x)^{-1}.\end{aligned}$$

Now taking log both sides in the above inequality, we have

$$\begin{aligned}\log\log d_{E_n} &\leq \log((n_K b + o(1))) + (\log\log x) + (\log\log\log x) + (\log\log\log\log x)\\ &= (\log\log x)(1 + o(1)).\end{aligned}$$

Similarly, we get

$$\log\log\log 6d_{E_n} \leq (1 + o(1))(\log\log\log x).$$

Multiplying them out, we have

$$\begin{aligned}c_5 \log d_{E_n}(\log\log d_{E_n})(\log\log\log 6d_{E_n}) &\leq (c_5 n_K b + o(1))\log x.\\ &\leq \log x.\end{aligned}$$

The last inequality follows from the fact that $c_5 n_K b < 1$ and the fact that we can choose and x large such that $c_5 n_K b + o(1) \leq 1$. □

Therefore, for such an x, we have

$$\pi_C(x) \leq \pi_{C_n}(x) \leq c_4 \frac{|C_n|}{|G_n|}\mathrm{Li}(x), \tag{3.19}$$

for an absolute constant c_4 as in Proposition 3.8. Hence,

$$\pi_C(x) = O\left(\frac{|C_n|}{|G_n|}\mathrm{Li}(x)\right) = O\left(\frac{\mathrm{Li}(x)}{\epsilon(x)^\alpha}\right), \quad \text{from (3.17) and (3.18).}$$

This proves Theorem 3.9 (i).

Proof of (ii) assuming (GRH):

As before, we have a unique $n = n(x)$ such that

$$\ell^N \epsilon_R(x) < |G_n| \leq \epsilon_R(x). \tag{3.20}$$

From (3.7), we have

$$\pi_C(x) \leq \pi_{C_n}(x) \leq \frac{|C_n|}{|G_n|}(\mathrm{Li}(x) + c_6 x^{1/2}(\log d_{E_n} + n_{E_n} \log x)).$$

As $c_6 x^{1/2} \log d_{E_n}$ and $c_6 n_{E_n} x^{1/2} \log x$ are $O(\mathrm{Li}(x))$, we have

$$\pi_C(x) = O\left(\frac{|C_n|}{|G_n|}\mathrm{Li}(x)\right).$$

Similarly as before, from (3.20) and (3.17), we have

$$\pi_C(x) = O\left(\frac{\mathrm{Li}(x)}{\epsilon_R(x)^\alpha}\right).$$

4. AN APPLICATION TO ELLIPTIC CURVES

In this chapter, we look at elliptic curves over rationals and their reductions at primes. Given a prime p of good reduction for E, we have an elliptic curve $\tilde{E}(p)$ over $\mathbb{F}_p$. If $a_p(E)$ is the trace of the Frobenius endomorphism of $\tilde{E}(p)$, then we prove the following statement:

Given $h \in \mathbb{Z}$, the density of primes p such that $a_p(E) = h$ is zero.

4.1 Elliptic Curves over the Rationals and their reductions

An elliptic curve over $\mathbb{Q}$ has a Weierstrass equation of the type:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_i \in \mathbb{Q}$. By a change of variable, $Y = u^3y$ and $X = u^2x$ for a suitable $u \in \mathbb{Q}^*$, we can assume $a_i \in \mathbb{Z}$.

For a prime $p \in \mathbb{Z}$, let v_p be the p-adic valuation on $\mathbb{Q}$. Define,

$$v_p(E) = \min_{E'}\{v_p(\Delta(E'))\},$$

where E' is a Weierstrass equation for E with integer coefficients and $\Delta(E')$ is its discriminant. By a change of variables, the discriminant changes by a factor of u^{12}. i.e. If E' and E'' are integral Weierstrass equations for E, and E'' is got by a change of variables $Y = u^3y + su^2x + c$ and $X = u^2x + b$, then

$$\Delta(E'') = \Delta(E')/u^{12}.$$

Hence, $v_p(\Delta(E')) \equiv v_p(\Delta(E''))$ mod 12 for all integral Weierstrass equations E', E'' for E. Therefore, if $v_p(\Delta(E')) < 12$, then

$$v_p(\Delta(E')) = v_p(E).$$

Definition 4.1. The *global minimal discriminant* of E is defined as

$$\Delta_{\min}(E) = \prod_p p^{v_p(E)}.$$

Proposition 4.2 (cf. [DS10], Ex. 8.3.2)**.** *There is a Weierstrass equation E' for E such that $\Delta(E') = \Delta_{\min}(E)$.*

Let us assume from now on that, the elliptic curve E has a minimal Weierstrass equation with discriminant $\Delta_{\min}(E)$. For each prime p, we have the natural reduction mod p map $\mathbb{Z} \to \mathbb{F}_p$, from which we get a Weierstrass equation in $\mathbb{F}_p$ by reducing the coefficients of the Weierstrass equation of E. This mod p Weierstrass equation is non-singular if and only if $p \nmid \Delta_{\min}(E)$.

Definition 4.3. The *reduction* of E mod p, denoted $\tilde{E}(p)$, is an elliptic curve over $\mathbb{F}_p$ for all $p \nmid \Delta_{\min}(E)$. These primes p are called as *primes of good reduction.*

Note that primes of bad reduction are finite.

For a prime p, consider the elliptic curve $E/\mathbb{Q}$ as an elliptic curve $E/\mathbb{Q}_p$ using the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. We immediately see that:

Proposition 4.4. *E has good reduction at p if and only if $\Delta_{\min}(E) \in \mathbb{Z}_p^*$.*

4.1.1 The Néron–Ogg–Shafarevich Theorem

Let K be a local field with maximal ideal $\mathfrak{p}$ and residue field k with q elements. Let $T_\ell(E)$ be the ℓ-adic Tate module of an elliptic curve E/K. We have the natural action of $G_K = \mathrm{Gal}(\overline{K}/K)$ on $T_\ell(E)$ which induces an ℓ-adic representation

$$\rho_\ell : G_K \longrightarrow \mathrm{Aut}(T_\ell(E)).$$

Our example of a local field in mind is a finite extension of $\mathbb{Q}_p$, for a prime p. For the theory of elliptic curves over local fields, we refer [Sil06]. The following version of the theorem is given in [Bel08].

Theorem 4.5. *Let E/K be an elliptic curve with minimal Weierstrass equation and $\tilde{E}$ be its reduction* (mod $\mathfrak{p}$)*. We have:*

i) E/K has good reduction if and only if $T_\ell(E)$ is unramified (ρ_ℓ is unramified).

ii) If E/K has good reduction, then $T_\ell(E) \cong T_\ell(\tilde{E})$, via the reduction map, and the following diagram commutes,

$$\begin{array}{ccccccc} 1 & \longrightarrow & I_K & \longrightarrow & G_K & \xrightarrow{\pi_K} & \mathrm{Gal}(\overline{k}/k) \xrightarrow{\cong} 1 \\ & & & & \downarrow{\scriptstyle \rho_\ell} & & \downarrow{\scriptstyle \tilde{\rho}_\ell} \\ & & & & \mathrm{Aut}(T_\ell(E)) & \xrightarrow{\cong} & \mathrm{Aut}(T_\ell(\tilde{E})) \end{array} \tag{4.1}$$

where I_K is the inertia group of K.

The commutativity of the diagram means the following: For a point $P = [x, y, z] \in E(\overline{K})$, after multiplication, we can assume $x, y, z \in \overline{R}$, the valuation ring of $\overline{K}$, and atleast one is non-zero. Consider the reduction mod $\overline{\mathfrak{p}}$ map

$$\tilde{\pi} : E(\overline{K}) \to \tilde{E}(\overline{k}), \quad [x, y, z] \mapsto [\tilde{x}, \tilde{y}, \tilde{z}].$$

. Let $\phi : T_\ell(E) \to T_\ell(\tilde{E})$ be the isomorphism in (4.1), defined by,

$$\phi(P_n) = (\tilde{\pi}(P_n)).$$

Let $\mathcal{P} \in T_\ell(E)$, then for $\sigma \in G_K$, we have $\rho_\ell(\sigma)(\mathcal{P}) \in T_\ell(E)$, whence $\phi(\rho_\ell(\sigma)(\mathcal{P})) \in T_\ell(\tilde{E})$. Moreover, if $\tilde{\rho}_\ell$ is the induced representation by the action of G_k on $T_\ell(\tilde{E})$, then $\tilde{\rho}_\ell(\pi_K(\sigma))\phi(\mathcal{P}) \in T_\ell(\tilde{E})$. The commutativity of the diagram means,

$$\phi(\rho_\ell(\sigma)(\mathcal{P})) = \tilde{\rho}_\ell(\pi_K(\sigma))\phi(\mathcal{P}) \quad \text{for all } \mathcal{P} \in T_\ell(E). \tag{4.2}$$

Corollary 4.6. Let E/K have good reduction. Then,

$$\det(\rho_\ell(\sigma_\mathfrak{p})) = \chi_\ell(\sigma_\mathfrak{p}) = q, \tag{4.3}$$

$$\mathrm{Tr}(\rho_\ell(\sigma_\mathfrak{p})) = a_\mathfrak{p}(E), \tag{4.4}$$

where $a_\mathfrak{p}(E) = 1 + q - |\tilde{E}(k)|$.

Proof. The fact that E/K has good reduction implies that ρ_ℓ is unramified, hence we can talk about the Frobenius element $\sigma_\mathfrak{p}$.

To calculate the determinant of $\rho_\ell(\sigma_\mathfrak{p})$, we use the Weil pairing on $T_\ell(E)$. Recall that it is a map

$$e : T_\ell(E) \times T_\ell(E) \to T_\ell(K),$$

which is linear and Galois invariant. So, for $\sigma_\mathfrak{p} \in G_K$ and $S, T \in T_\ell(E)$, we have

$$\begin{aligned} \sigma_\mathfrak{p}(e(S,T)) &= e(S^{\sigma_\mathfrak{p}}, T^{\sigma_\mathfrak{p}}) \\ &= e(S,T)^{\det \rho_\ell(\sigma_\mathfrak{p})}. \quad \text{(Properties of } e\text{)} \end{aligned} \tag{4.5}$$

Also, the action of any $\sigma \in G_{\mathbb{Q}}$ on $T_\ell(K)$ is given by the ℓ-adic cyclotomic character χ_ℓ. More precisely, as $e(S,T) \in T_\ell(K)$,

$$\sigma_{\mathfrak{p}}(e(S,T)) = e(S,T)^{\chi(\sigma_{\mathfrak{p}})} = e(S,T)^q. \tag{4.6}$$

Hence, from (4.5) and (4.6), we have $\det \rho_\ell(\sigma_p) = q$.

Using (4.2), we see that the eigenvalues of $\rho_\ell(\sigma_{\mathfrak{p}})$ is same as that of $\tilde{\rho}_\ell(\pi_K(\sigma_{\mathfrak{p}}))$, implying that

$$\mathrm{Tr}(\rho_\ell(\sigma_{\mathfrak{p}})) = \mathrm{Tr}\tilde{\rho}_\ell(\sigma_q),$$

where $\pi_K(\sigma_{\mathfrak{p}}) = \pi_K(\sigma_{\mathfrak{p}})$ is the Frobenius element in G_k. We know that,

$$\begin{aligned}\mathrm{Tr}\tilde{\rho}_\ell(\sigma_q) &= 1 + \det(\tilde{\rho}_\ell(\sigma_q)) - \det(1 - \tilde{\rho}_\ell(\sigma_q)) \\ &= 1 + q - \det(1 - \tilde{\rho}_\ell(\sigma_q)).\end{aligned}$$

By Tate's isogeny theorem for finite fields, for the Frobenius endomorphism

$$\varphi_q : \tilde{E}(\overline{k}) \to \tilde{E}(\overline{k}), \quad [x,y,z] \mapsto [x^q, y^q, z^q],$$

we have

$$\det(1 - \tilde{\rho}_\ell(\sigma_q)) = \det(1 - \varphi_q) = |\tilde{E}(k)|.$$

Therefore, $\mathrm{Tr}(\rho_\ell(\sigma_{\mathfrak{p}})) = a_{\mathfrak{p}}(E)$.

□

4.1.2 Galois representations

For an elliptic curve $E/\mathbb{Q}$, we have the attached ℓ-adic representation

$$\psi_\ell : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell) \hookrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell).$$

For a prime p, an inclusion $G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$ gives a representation $\rho_\ell : G_{\mathbb{Q}_p} \longrightarrow \mathrm{Aut}(T_\ell(E))$, induced by ψ_ℓ, such that the following diagram commutes.

$$\begin{array}{ccc} G_{\mathbb{Q}} & \xrightarrow{\psi_\ell} & \mathrm{Aut}(T_\ell(E)) \\ \uparrow & \nearrow_{\rho_\ell} & \\ G_{\mathbb{Q}_p} & & \end{array}$$

Note that the action of the inertia group on $T_\ell(E)$, the determinant and trace of the image of the Frobenius map remain the same when we change the inclusion $G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$, as they remain unchanged under conjugation. Thus, from Corollary 4.6, we have the following theorem regarding the ℓ-adic Galois representation attached to an elliptic curve over $\mathbb{Q}$.

Theorem 4.7. *The Galois representation ψ_ℓ is unramified at all primes $p \neq \ell$ where the elliptic curve E has good reduction. Moreover, if σ_p is the Frobenius substitution at p, then*

$$\mathrm{Tr}(\psi_\ell(\sigma_p)) = a_p(E), \tag{4.7}$$
$$\det(\psi_\ell(\sigma_p)) = p. \tag{4.8}$$

Proof. Let p be a prime of good reduction, consider the representation, as above,

$$\rho_\ell : G_{\mathbb{Q}_p} \longrightarrow \mathrm{Aut}(T_\ell(E)),$$

induced by ψ_ℓ. Note that, here the Tate module $T_\ell(E)$ is of the elliptic curve $E/\mathbb{Q}_p$. As $\sigma_p \in G_{\mathbb{Q}_p}$, using Corollary 4.6 for the elliptic curve $E/\mathbb{Q}_p$, we have

$$\mathrm{Tr}(\psi_\ell(\sigma_p)) = \mathrm{Tr}(\rho_\ell(\sigma_p)) = a_p(E),$$
$$\det(\psi_\ell(\sigma_p)) = \det(\rho_\ell(\sigma_p)) = p.$$

□

4.2 The Set-up

Let $E/\mathbb{Q}$ be an elliptic curve, S_E be the primes of bad reduction of E (this set is finite as they are the divisors of $\Delta_{\min}(E)$). Let p be a prime not in S_E and let $\tilde{E}(p)$ be reduction of E mod p, which is an elliptic curve over $\mathbb{F}_p$. Let π_p be the Frobenius endomorphism of $\tilde{E}(p)$, and $a_p(E)$ be its trace (cf. [Sil06], Remark V.2.6). We have,

$$a_p(E) = 1 + p - |\tilde{E}(p)(\mathbb{F}_p)|. \tag{4.9}$$

Recall that we had the ℓ-adic representation $\psi_\ell : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ attached to the elliptic curve E, induced by the action of $G_{\mathbb{Q}}$ on the Tate module $T_\ell(E)$.

Theorem 4.8 (Properties of ψ_ℓ)**.** *The representation $\psi_\ell : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell)$ is continuous with respect to the Krull topology on $G_{\mathbb{Q}}$. According to Serre* [Ser98]*, if E doesn't have complex multiplication* ($\mathrm{End}(E) = \mathbb{Z}$)*, then $\psi_\ell(G_{\mathbb{Q}})$ is open in $\mathrm{GL}_2(\mathbb{Q}_\ell)$. Moreover, except for finitely many (almost all) primes ℓ, $\psi_\ell(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}_\ell)$.*

For an elliptic curve E without complex multiplication, the set-up we have is

- $G_\ell = \psi_\ell(G_{\mathbb{Q}})$ is an ℓ-adic Lie subgroup of $\mathrm{GL}_2(\mathbb{Q}_\ell)$ of dimension 4.

- From the first isomorphism theorem and infinite Galois theory, we have

$$G_\ell \cong G_{\mathbb{Q}}/\ker(\psi_\ell) = \mathrm{Gal}(K/\mathbb{Q}),$$

  where K = fixed field of $\ker(\psi_\ell)$.

- The representation is unramified outside primes in S_E. From Remark B.8, K is unramified outside the finite set S_E.

4.2.1 Number of primes $p \leq x$ such that $a_p(E)$ has a given value

For $h \in \mathbb{Z}$, the set

$$C_{\ell,h} = \{s \in G_\ell \mid \mathrm{Tr}(s) = h\}$$

is a closed subset of G_ℓ which is stable under conjugation. Moreover, it is a level set of the trace map $\mathrm{Tr} : G_\ell \to \mathbb{Z}_\ell$, implying that it is a manifold over $\mathbb{Q}_\ell$ of dimension 3. Note that we are now in the set-up of Theorem 3.9. Let

$$P_{E,h}(x) = \{p \leq x \mid a_p = h\}.$$

Theorem 4.9 (cf. [Ser81], Theorem 20)**.** *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Then:*

(a) $P_{E,h} = O(\mathrm{Li}(x)/\epsilon(x)^{1/4})$ *for* $x \to \infty$.

(b) *(GRH)* $P_{E,h}(x) = O(\mathrm{Li}(x)/\epsilon_R(x)^{1/4})$ *for* $x \to \infty$.

Where the functions $\epsilon(x)$ and $\epsilon_R(x)$ are same as in Theorem 3.9.

Proof. As $\dim C_{\ell,h} = 3$, we have $\dim_M C_{\ell,h} \leq 3$ (cf. [Ser81], §4, Theorem 8). Take $\psi_\ell^{-1}(G_\ell) = G$ and $\psi_\ell^{-1}(C_{\ell,h}) = C$, $d = 3$ and $N = 4$ in Theorem 3.9. □

From the above Theorem 4.9, we see that

$$\frac{P_{E,h}(x)}{\pi(x)} = O\left(\frac{\mathrm{Li}(x)}{\pi(x)\epsilon(x)^{1/4}}\right) = O\left(\frac{1}{\epsilon(x)^{1/4}}\right),$$

as $\pi(x) \sim \mathrm{Li}(x)$. As $\epsilon(x) \to \infty$ as $x \to \infty$, we have

$$\lim_{x\to\infty} \frac{P_{E,h}(x)}{\pi(x)} = 0. \tag{4.10}$$

That is, *The density of primes p such that $a_p(E) = h$ is* 0.

5. APPLICATIONS TO MODULAR FORMS

We look at certain density theorems on non-nullity of multiplicative functions, and later move on to non-lacunarity of *non-CM Hecke eigenforms*. We calculate the density of non-zero coefficients for CM and non-CM eigenforms. Here, out of the two examples, we see the density of nonzero coefficients of the Ramanujan delta function. Finally, we finish with conditions for non-lacunarity of a general modular form in $M_k(N, \omega)$.

5.1 Definitions from Modular Forms

For an natural number N, denote

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \bmod N \right\}.$$

Given a Dirichlet character ω mod N, we say $f : \mathbb{H} \to \mathbb{C}$ is a *modular form* of weight $k \geq 1$ and of type (ω, N) (or with Nebentypus ω) if f is a holomorphic function satisfying the modularity condition:

$$f(\gamma z) = \omega(d)(cz + d)^k f(z) \;\text{ where } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N). \tag{5.1}$$

We denote $M_k(N, \omega)$ for the $\mathbb{C}$-vector space of modular forms with Nebentypus ω. Recall that, for $f \in M_k(N, \omega)$, we have the attached *Fourier series*

$$f(z) = \sum_{n=0}^{\infty} a_f(n) q^n; \quad q = e^{2\pi i z}.$$

We call $a_f(n)$'s as the *coefficients of* $f(z)$. An $f \in M_k(N, \omega)$ is said to be a *cusp form* if it vanishes at all cusps.

There are special operators of arithmetical interest that act on the space of modular forms. We are interested in the *Hecke Operators* T_p and U_p,

where p is a prime (The notation used here is of [Ser81].) They are defined as follows: For $f \in M_k(N, \omega)$,

$$f|U_p(z) = \sum_{n=0}^{\infty} a_f(pn)q^n \quad \text{if } p|N \tag{5.2}$$

$$f|T_p(z) = \sum_{n=0}^{\infty} a_f(pn)q^n + \omega(p)p^{k-1}\sum_{n=0}^{\infty} a_f(n)q^{pn} \quad \text{if } p \not| N \tag{5.3}$$

Given a set S of Hecke operators, there exists a common eigen function for S. This follows as the Hecke operators commute with each other. We call such a common eigen function to be a *Hecke eigenform* for S.

Proposition 5.1. *If $f \in M_k(N, \omega)$ is an eigenform for T_p (or U_p) and $a_f(1) \neq 0$, then the eigenvalue of f is $a_f(p)/a_f(1)$. In particular, if $a_f(1) = 1$, then $a_f(p)$ is the eigenvalue for f.*

Proof. If λ is the eigenvalue of f, then

$$f|T_p(z) = \sum_{n=0}^{\infty} a_f(pn)q^n + \omega(p)p^{k-1}\sum_{n=0}^{\infty} a_f(n)q^{pn} = \sum_{i=1}^{\infty} \lambda a_f(n)q^n.$$

Equating the coefficients, we have $\lambda a_f(1) = a_f(p)$. □

Example 5.2 (Ramanujan Delta Function)**.** Let $k = 12, N = 1$. The Delta function,

$$\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24},$$

is an eigenform for all T_p (hence for all T_m, $m \in \mathbb{N}$). This fact helps us in proving the first two conjectures of Ramanujan about the τ-function. The third one of course was proved by Pierre Deligne as a consequence of the Weil conjectures.

5.2 Non-vanishing of Multiplicative Functions

Let K be a number field of finite degree n_K. We define

$$M_K = \{\text{non-zero ideals of } \mathcal{O}_K\}.$$

The multiplication of ideals in M_K makes it a monoid. The identity of M_K is denoted by 1.

Definition 5.3. Let R be an integral domain, a function $a : M_K \to R$ is said to be a *multiplicative function* if:

$$\begin{aligned} a(1) &= 1; \\ a(\mathfrak{m}\mathfrak{m}') &= a(\mathfrak{m})a(\mathfrak{m}') \quad \text{for co-prime ideals } \mathfrak{m}, \mathfrak{m}' \in M_K. \end{aligned}$$

For example, if $K = \mathbb{Q}$, then we have $M_K \simeq \mathbb{N}$, and the above conditions for $n \mapsto a(n)$ to be multiplicative is in the *usual* sense.

In what follows, we will focus on nullity and non-nullity of $a(\mathfrak{m})$. Let $x \geq 0$, we define,

$$M_a(x) = \#\{\mathfrak{m} \in M_K \mid a(\mathfrak{m}) \neq 0 \text{ for } \mathrm{N}\mathfrak{m} \leq x\}, \tag{5.4}$$

$$P_a(x) = \#\{v \in \Sigma_K \mid a(\mathfrak{p}_v) = 0 \text{ for } \mathrm{N}v \leq x\}. \tag{5.5}$$

Recall that $\mathrm{N}\mathfrak{m}$ denotes the norm of the ideal $\mathfrak{m}$ in $\mathcal{O}_K$, and for a place $v \in \Sigma_K$, we define $\mathrm{N}v = \mathrm{N}\mathfrak{p}_v$.

The next theorem says that, the asymptotic behaviour of the function $P_a(x)$ "almost" determines the behaviour of $M_a(x)$.

Theorem 5.4. *Suppose that we have*

$$P_a(x) = \lambda x/\log x + O(x/(\log x)^{1+\delta}) \quad \text{as } x \to \infty, \tag{5.6}$$

with $0 \leq \lambda < 1$ *and for some* $\delta > 0$. *We then have,*

$$M_a(x) \sim \gamma_a x/(\log x)^{\lambda} \quad \text{as } x \to \infty \tag{5.7}$$

for a constant $\gamma_a > 0$.

The proof will be given in the next section.

Remark 5.5. Later, we will see the case $\lambda = 0$ (cf. Theorem 5.7), and prove it using a weaker condition

$$\sum_{a(\mathfrak{p}_v)=0} \frac{1}{\mathrm{N}v} < \infty. \tag{5.8}$$

The Theorem 5.4 asserts that,

$$M_a(x) \sim \gamma_a x, \quad \text{where } \gamma_a > 0. \tag{5.9}$$

If $M_1(x) = \{\mathfrak{m} \in M_K \mid \mathrm{N}\mathfrak{m} \leq x\}$, we know (due to Dedekind, cf. [Ser81]) that $M_1(x) \sim \gamma_1 x$, where γ_1 is the residue (at 1) of the zeta function of K. Seen in (5.9), we have

$$M_a(x)/M_1(x) \sim \gamma_a/\gamma_1, \quad \text{as } x \to \infty. \tag{5.10}$$

Definition 5.6. A subset $A \subset M_K$ has *density* α if,

$$\#\{\mathfrak{m} \in A \mid \mathrm{N}\mathfrak{m} \leq x\} = \alpha M_1(x) + o(x).$$

We reformulate Theorem 5.4 in the following manner:

Theorem 5.7. *If* (5.8) *is satisfied, the set* $\mathfrak{M}_a = \{\mathfrak{m} \in M_K \mid a(\mathfrak{m}) \neq 0\}$ *has density* $\gamma_a/\gamma_1 > 0$.

5.2.1 Proof of Theorem 5.4

We will follow the proof in [Ser81]. For $\mathfrak{m} \in M_K$, let:

$$a^0(\mathfrak{m}) = \begin{cases} 0 & \text{if } \ a(\mathfrak{m}) = 0, \\ 1 & \text{if } \ a(\mathfrak{m}) \neq 0. \end{cases}$$

The map $a^0 : M_K \to \mathbb{Z}$ is a characteristic function for $\mathfrak{M}_a$ and it defines a multiplicative function. It is clear that $M_a = M_{a^0}$ and $P_a = P_{a^0}$. Hence, it suffices to demonstrate Theorem 5.4 for $a = a^0$, i.e. when a takes only 0 and 1 values.

Suppose this is the case. Consider the Dirichlet series,

$$\phi(s) = \sum_{\mathfrak{m}} a(\mathfrak{m}) \mathrm{N}\mathfrak{m}^{-s}, \tag{5.11}$$

which converges for $\mathrm{Re}(s) > 1$. If we write this in the form,

$$\phi(s) = \sum_{n \geq 1} b(n) n^{-s}, \quad \text{where} \quad b(n) = \sum_{\mathrm{N}\mathfrak{m}=n} a(\mathfrak{m}), \tag{5.12}$$

we have,

$$M_a(x) = \sum_{\mathrm{N}\mathfrak{m} \leq x} a(\mathfrak{m}) = \sum_{n \leq x} b(n). \tag{5.13}$$

In other words, $M_a(x)$ is the summatory function of the coefficients of ϕ.

Recall, given an arithmetical function $f : \mathbb{N} \to \mathbb{C}$, its *summatory function* is the function $F : \mathbb{R} \to \mathbb{C}$ defined by,

$$F(x) = \sum_{n \leq x} f(n).$$

The multiplicativity of a implies that of b. We can therefore write ϕ as the *Euler product*,

$$\phi(x) = \prod_{p} \phi_p(s),$$

where

$$\phi_p(s) = 1 + \sum_{n\geq 1} b(p^n)p^{-ns} = \prod_{v|p}(1 + \sum_{n\geq 1} a(\mathfrak{p}_v^n)\mathrm{N}v^{-s}). \tag{5.14}$$

Lemma 5.8. *We have*

$$\sum_{\mathrm{N}v\leq x} a(\mathfrak{p}_v) = (1-\lambda)x/\log x + O(x/(\log x)^{1+\delta}), \tag{5.15}$$

with $\delta > 0$.

Proof. As $a(\mathfrak{p}_v) = 0$ or 1, we have

$$P_a(x) = \sum_{\mathrm{N}v\leq x}(1 - a(\mathfrak{p}_v)) = \pi_K(x) - \sum_{\mathrm{N}v\leq x} a(\mathfrak{p}_v). \tag{5.16}$$

From the *prime number theorem* for K, we have

$$\pi_K(x) = x/\log x + O(x/(\log x)^2). \tag{5.17}$$

Combining (5.17) with (5.6), and assuming $\delta < 1$, we have (5.15). When $\delta \geq 1$, then the error term is $O(x/(\log x)^2)$. □

Lemma 5.9. *Moreover, we have*

$$\sum_{p\leq x} b(p) = (1-\lambda)x/\log x + O(x/(\log x)^{1+\delta}), \tag{5.18}$$

where the sum is over the rational primes.

Proof. By definition, $b(p) = \sum_{\mathrm{N}v=p} a(\mathfrak{p}_v)$. We have

$$\sum_{\mathrm{N}v\leq x} a(\mathfrak{p}_v) = \sum_{p} b(p) + \sum_{}^{'} a(\mathfrak{p}_v),$$

where $'$ denotes the sum is taken over places v with $\mathrm{N}v \leq x$ and having residue degree $f_v > 1$. We know that

$$\sum_{}^{'} a(\mathfrak{p}_v) \leq \#\{v \in \Sigma_K \mid f_v > 1\} = O(\sqrt{x}/\log x) = O(x/(\log x)^{1+\delta}),$$

which implies $\sum_{\mathrm{N}v\leq x} a(\mathfrak{p}_v) = \sum_{p} b(p) + O(x/(\log x)^{1+\delta})$, and therefore (5.18).

□

Remark 5.10. We see why $\#\{v \in \Sigma_K \mid f_v > 1\} = O(\sqrt{x}/\log x)$. Given a prime p, there exists at most $[K : \mathbb{Q}] = n_K$ places lying above it. If v is a place such that $\mathrm{N}v = p^{f_v} \leq x$ with $f_v \geq 2$, then we have $p \leq x^{1/f_v} \leq x^{1/2}$. So, for each place v with $f_v > 1$, we have a prime number $p \leq x^{1/2}$ and the number of places producing the same prime p is bounded by n_K. Hence,

$$\#\{v \in \Sigma_K \mid f_v > 1\} \leq n_K \pi(\sqrt{x}) = O(\sqrt{x}/\log x).$$

Lemma 5.11. *We have*

$$\sum_p b(p)p^{-s} = (\lambda - 1)\log(s-1) + \epsilon_1(s), \tag{5.19}$$

for a real $s > 1$, and $\epsilon_1(s)$ continuous at $s = 1$.

Proof. Let $\alpha : \mathbb{N} \to \{1, 0\}$ be the prime counting function. i.e.

$$\alpha(n) = \begin{cases} 1 & \text{if } n \text{ is a prime,} \\ 0 & \text{otherwise.} \end{cases}$$

So, $\displaystyle\sum_{p \leq x} b(p)p^{-s} = \sum_{n \leq x} b(n)\alpha(n)n^{-s}$. If $\displaystyle A(x) = \sum_{n \leq x} b(n)\alpha(n) = \sum_p b(p)$ and $\phi(y) = y^{-s}$, then by Abel summation formula, we have

$$\begin{aligned} \sum_{p \leq x} b(p)p^{-s} &= A(x)\phi(x) - \int_1^x A(y)\phi'(y)dy \\ &= A(x)x^{-s} + s\int_2^x A(y)y^{-s-1}dy. \end{aligned}$$

Hence, taking $x \to \infty$, we have

$$\sum_p b(p)p^{-s} = s\int_2^\infty A(y)y^{-s-1}dy.$$

From (5.18), we have $A(y) = (1-\lambda)y/\log y + \rho(y)$ where $\rho(y) = O(y/(\log y)^{1+\delta})$, from which,

$$\begin{aligned} \sum_p b(p)p^{-s} &= s\int_2^\infty (1-\lambda)\frac{y^{-s}}{\log y}dy + \int_2^\infty \rho(y)y^{-s-1}dy \\ &= s\int_2^\infty (1-\lambda)\frac{y^{-s}}{\log y}dy + O\left(\int_2^\infty \frac{y^{-s}}{(\log y)^{1+\delta}}dy\right). \end{aligned}$$

We have,

$$s\int_2^\infty (1-\lambda)\frac{y^{-s}}{\log y}dy = (1-\lambda)\int_{(s-1)\log 2}^\infty e^{-t}t^{-1}dt = -(1-\lambda)\log(s-1)+\epsilon_2(s),$$

where ϵ_2 is continuous at 1. We have,

$$\sum_p b(p)p^{-s} = -(1-\lambda)\log(s-1) + \underbrace{\epsilon_2(s) + \int_2^\infty \rho(y)y^{-s-1}dy}_{\epsilon_1(s)}$$

□

[If $E_1(z) = \int_z^\infty u^{-1}e^{-u}du$, then we use the known fact that $E_1(z) = -\gamma - \log z + O(z)$ as $z \to 0$, where γ is the Euler's constant, to see that $\int_2^\infty (y^{-s}/\log y)dy = -\log(s-1) + \epsilon_2(s)$.]

Lemma 5.12. *There exists a constant $u > 0$ such that*

$$\phi(s) \sim u/(s-1)^{1-\lambda} \quad \text{for } s \to 1 \text{ (real } s > 1). \tag{5.20}$$

Proof. According to (5.14), we have

$$\log\phi(s) = \sum_p \log\phi_p(s) = \sum_p b(p)p^{-s} + \epsilon_3(s),$$

where $\epsilon_3(s)$ is continuous at $s = 1$ (and even be extended to the half plane $\mathrm{Re}(s) > 1/2$). See 5.19, this gives

$$\log\phi(s) = (\lambda-1)\log(s-1) + \epsilon_4(s),$$

where $\epsilon_4(s)$ is continuous at 1. So, we have

$$\phi(s) = e^{e_4(s)}(s-1)^{\lambda-1},$$

implying (5.20). □

Lemma 5.13. *We have*

$$\sum_{n\le x} b(n)/n \sim u(\log x)^{1-\lambda}/\Gamma(2-\lambda) \quad \text{as } x \to \infty. \tag{5.21}$$

This follows from Lemma 5.12 and by a tauberian theorem due to G. H. Hardy and J. E. Littlewood (cf. [HL14], Theorem 16, or the remark below).

Remark 5.14 (Hardy–Littlewood's Tauberian Theorem)**.**

Let $f(s) = \sum_{n=1}^{\infty} c_n n^{-s}$ be a Dirichlet series with positive coefficients and

$$f(s) \sim \frac{A}{(s-1)^{\alpha}} L\left(\frac{1}{s-1}\right)$$

for $L(u) = (\log u)^{\alpha_1}(\log\log u)^{\alpha_2}\cdots$. Moreover, assume $\alpha, \alpha_1, \alpha_2, \cdots$ are such that $(\log n)^{\alpha} L(\log n)$ tends to a positive limit or infinity as $n \to \infty$. Then we have,

$$\sum_{n \le x} \frac{c_n}{n} \sim \frac{A}{\Gamma(\alpha+1)} (\log n)^{\alpha} L(\log n).$$

Here, we take $\alpha = 1 - \lambda$ and $\alpha_1 = \alpha_2 = \cdots = 0$.

Lemma 5.15. *We have*

$$M_a(x) = \sum_{n \le x} b(n) \sim (1-\lambda) \frac{x}{\log x} \sum_{n \le x} \frac{b(n)}{n} \quad \text{as } x \to \infty. \tag{5.22}$$

This follows from the Lemma 5.9, and the multiplicativity of the function b, according to Wirsing [Wir61], Hilfssatz (Proposition) 2, page 93.

By combining Lemmas 5.13 and 5.15, we have

$$M_a(x) \sim \gamma_a x/(\log x)^{\lambda} \quad \text{as } x \to \infty,$$

where

$$\gamma_a = \frac{(1-\lambda)u}{\Gamma(2-\lambda)} = \frac{u}{\Gamma(1-\lambda)}, \tag{5.23}$$

finishing our proof of Theorem 5.4.

5.2.2 Direct Proof of Theorem 5.7

We want to prove $M_a(x) \sim \gamma_a x$ as $x \to \infty$, assuming (5.8).

Define $c : M_K \to \mathbb{Z}$ by,

$$c(\mathfrak{m}) = \sum_{\mathfrak{m}' | \mathfrak{m}} \mu(\mathfrak{m}') a(\mathfrak{m}/\mathfrak{m}'),$$

where μ is the Möbius function. That is, c is a multiplicative function satisfying

$$a(\mathfrak{m}) = \sum_{\mathfrak{m}' | \mathfrak{m}} c(\mathfrak{m}'). \tag{5.24}$$

We have,

$$\begin{aligned} M_a(x) = \sum_{\mathrm{N}\mathfrak{m}\leq x} a(\mathfrak{m}) &= \sum_{\mathrm{N}\mathfrak{m}\leq x}\sum_{\mathfrak{m}'|\mathfrak{m}} c(\mathfrak{m}') \\ &= \sum_{\mathrm{N}\mathfrak{m}'\leq x}\sum_{\mathrm{N}\mathfrak{n}\leq x/\mathrm{N}\mathfrak{m}'} c(\mathfrak{m}') \\ &= \sum_{\mathrm{N}\mathfrak{m}'\leq x} c(\mathfrak{m}')M_1(x/\mathrm{N}\mathfrak{m}'), \end{aligned} \tag{5.25}$$

where $M_1(x)$, as before (Remark 4), is the set of $\mathfrak{m} \in M_K$ with $\mathrm{N}\mathfrak{m} \leq x$. As wen have noted before,

$$M_1(x) = \gamma_1 x + \psi(x), \quad \text{where } \psi(x) = o(x), \tag{5.26}$$

where γ_1 is the residue of the zeta function for K. We deduce,

$$\begin{aligned} M_a(x) &= \sum_{\mathrm{N}\mathfrak{m}\leq x} c(\mathfrak{m})(\gamma_1 x/\mathrm{N}\mathfrak{m} + \psi(x/\mathrm{N}\mathfrak{m})) \\ &= \gamma_1 x \sum_{\mathrm{N}\mathfrak{m}\leq x} c(\mathfrak{m})/\mathrm{N}\mathfrak{m} + \sum_{\mathrm{N}\mathfrak{m}\leq x} \psi(x/\mathrm{N}\mathfrak{m})c(\mathfrak{m}). \end{aligned} \tag{5.27}$$

We now prove that

$$\sum_{\mathfrak{m}} c(\mathfrak{m})/\mathrm{N}\mathfrak{m} = \lim_{x\to\infty} \sum_{\mathrm{N}\mathfrak{m}\leq x} c(\mathfrak{m})/\mathrm{N}\mathfrak{m} < \infty.$$

By definition,

$$c(\mathfrak{p}_v^n) = a(\mathfrak{p}_v^n) - a(\mathfrak{p}_v^{n-1}) = \begin{cases} 1 & \text{if } a(\mathfrak{p}_v^n) = 1 \text{ and } a(\mathfrak{p}_v^{n-1}) = 0, \\ 0 & \text{if } a(\mathfrak{p}_v^n) = a(\mathfrak{p}_v^{n-1}) \\ -1 & \text{if } a(\mathfrak{p}_v^n) = 0 \text{ and } a(\mathfrak{p}_v^{n-1}) = 1, \end{cases} \tag{5.28}$$

for all $v \in \Sigma_K$ and $n \geq 1$. Let us pose,

$$\alpha_v = 1 + \sum_{n=1}^{\infty} c(\mathfrak{p}_v^n)/\mathrm{N}v^n = (1 - 1/\mathrm{N}v)(1 + \sum_{n=1}^{\infty} a(\mathfrak{p}_v^n)/\mathrm{N}v^n). \quad \text{(from (5.28))} \tag{5.29}$$

We have,

$$\alpha_v = \begin{cases} 1 + O(1/\mathrm{N}v^2) & \text{if } \ a(\mathfrak{p}_v) = 1, \\ 1 - 1/\mathrm{N}v + O(1/\mathrm{N}v^2) & \text{if } \ a(\mathfrak{p}_v) = 0. \end{cases} \tag{5.30}$$

Using (5.8), We see that,

$$\alpha = \prod_v \alpha_v < \infty. \tag{5.31}$$

and the product converges to $\sum_{\mathfrak{m}} c(\mathfrak{m})/\mathrm{N}\mathfrak{m}$. From this, we have the following proposition.

Proposition 5.16. *We have*

$$\sum_{\mathrm{N}\mathfrak{m}\le x} \psi(x/\mathrm{N}\mathfrak{m})c(\mathfrak{m}) = o(x).$$

Proof. We see that

$$\frac{1}{x}\sum_{\mathrm{N}\mathfrak{m}\le x} \psi(x/\mathrm{N}\mathfrak{m})c(\mathfrak{m}) = \sum_{\mathrm{N}\mathfrak{m}\le x} \left(\frac{\psi(x/\mathrm{N}\mathfrak{m})}{x/\mathrm{N}\mathfrak{m}}\right) c(\mathfrak{m})/\mathrm{N}\mathfrak{m}.$$

As $\psi(x) = o(x)$, for a given $\epsilon > 0$, we have an $N_1 \in \mathbb{N}$ such that

$$|\psi(t)| < \frac{\epsilon}{M+\alpha} t \quad \forall t \ge N_1,$$

where $M = \sup(\psi(t)/t)$. Moreover, let $N_2 \in \mathbb{N}$ such that

$$\left|\sum_{\mathrm{N}\mathfrak{m}\ge m} c(\mathfrak{m})/\mathrm{N}\mathfrak{m}\right| < \frac{\epsilon}{M+\alpha}, \quad \forall m \ge N_2.$$

Now, for $x \ge N_1 N_2$, we see that

$$\begin{aligned}\left|\frac{1}{x}\sum_{\mathrm{N}\mathfrak{m}\le x} \psi(x/\mathrm{N}\mathfrak{m})c(\mathfrak{m})\right| &= \sum_{\mathrm{N}\mathfrak{m}>x/N_1} \frac{c(\mathfrak{m})}{\mathrm{N}\mathfrak{m}}\left(\frac{\psi(x/\mathrm{N}\mathfrak{m})}{x/\mathrm{N}\mathfrak{m}}\right) + \sum_{\mathrm{N}\mathfrak{m}\le x/N_1} \frac{c(\mathfrak{m})}{\mathrm{N}\mathfrak{m}}\left(\frac{\psi(x/\mathrm{N}\mathfrak{m})}{x/\mathrm{N}\mathfrak{m}}\right) \\ &\le M \sum_{\mathrm{N}\mathfrak{m}>x/N_1} \frac{c(\mathfrak{m})}{\mathrm{N}\mathfrak{m}} + \sum_{\mathrm{N}\mathfrak{m}<x/N_1} \frac{c(\mathfrak{m})}{\mathrm{N}\mathfrak{m}}\left(\frac{\epsilon}{M+\alpha}\right) \\ &\le \epsilon.\end{aligned}$$

□

Therefore we have, from (5.27),

$$M_a(x)/x \to \alpha\gamma_1 \quad \text{as } x \to \infty.$$

That is,

$$M_a(x) \sim \alpha\gamma_1 x \quad \text{as } x \to \infty, \tag{5.32}$$

which proves Theorem 5.7, and at the same time proves that the density of the set $\mathfrak{M}_a$ of $\mathfrak{m} \in M_K$ such that $a(\mathfrak{m}) \neq 0$ is equal to α. Therefore we have, from (5.27),

$$M_a(x)/x \to \alpha\gamma_1 \quad \text{as } x \to \infty.$$

That is,

$$M_a(x) \sim \alpha\gamma_1 x \quad \text{as } x \to \infty, \tag{5.33}$$

which demonstrates Theorem 5.7, and at the same time proves that the density of the set $\mathfrak{M}_a$ of $\mathfrak{m} \in M_K$ such that $a(\mathfrak{m}) \neq 0$ is equal to α.

Remark 5.17 (Proving equation (5.31))**.** Let $\alpha_v = 1 + b_v$ when $a(\mathfrak{p}_v) = 1$, and $\alpha_v = 1 - 1/\mathrm{N}v + c_v$ when $a(\mathfrak{p}_v) = 0$. We have,

$$\prod_v \alpha_v = \prod_{a(\mathfrak{p}_v)=1} (1 + b_v) \prod_{a(\mathfrak{p}_v)=0} (1 + (-1/\mathrm{N}v + c_v))$$

As $b_v = O(1/\mathrm{N}v^2)$, we have $\sum_v b_v = O(\sum_v \mathrm{N}v^{-2}) = O(1)$ as,

$$\sum_v \mathrm{N}v^{-2} = \sum_p p^{-2} \sum_{\mathrm{N}v=p} 1 \leq n_K \sum_p p^{-2} < \infty.$$

Similarly, $\sum_v c_v = O(1)$. Also, assuming (5.8), we have $\sum_v 1/\mathrm{N}v < \infty$. As

$$\sum b_v, \ \sum (c_v - 1/\mathrm{N}v)$$

converge, the product converges. More specifically, by its form, it converges to the sum $\sum_{\mathfrak{m}} c(\mathfrak{m})/\mathrm{N}\mathfrak{m}$.

5.3 Hecke eigenvalues of a Polynomial Type

Let $f \in M_k(N, \omega)$ be a nonzero eigenform for T_p ($p \not| N$) with eigenvalue a_p. i.e.

$$f|T_p = a_p f \quad (p \not| N). \tag{5.34}$$

Let us work with the following assumptions.

(*a*) $k \geq 2$.

(*b*) f is a cusp form (parabolic).

(*c*) f is not of type CM in the sense of Ribet (i.e. there doesn't exist an imaginary quadratic field $L/\mathbf{Q}$ such that $a_p = 0$ if and only if p is inert in L).

Let $h(x)$ be a polynomial with complex coefficients. Denote

$$\Sigma_{f,h} = \{p \not| N \mid a_p = h(p)\}, \quad \text{and} \tag{5.35}$$
$$P_{f,h}(x) = \{p \in \Sigma_{f,h} \mid p \leq x\}. \tag{5.36}$$

An important example is when $h = 0$, we have $P_{f,h}(x) = \{p \leq x \mid a_p = 0\}$. We will use this in result in the next section.

The following theorem gives us a majorization of the function $P_{f,h}(x)$.

Theorem 5.18. *Under* $(a), (b)$ *and* (c) *above, we have*

$$P_{f,h}(x) = O(\mathrm{Li}(x)/\epsilon(x)^{1/4}) \quad x \to \infty. \tag{5.37}$$

Moreover, assuming (GRH)*, we have*

$$P_{f,h}(x) = O(\mathrm{Li}(x)/\epsilon_R(x)^{1/4}) \quad x \to \infty. \tag{5.38}$$

Recall the functions $\epsilon(x)$ and $\epsilon_R(x)$ are given by the following formulas.

$$\epsilon(x) = \log x (\log\log x)^{-2} (\log\log\log x)^{-1},$$
$$\epsilon_R(x) = x^{1/2} (\log x)^{-2}.$$

Corollary 5.19. We have,

$$P_{f,h}(x) = O(x/(\log x)^{5/4-\delta}) \quad \text{for all } \delta > 0, \tag{5.39}$$

and, under (GRH), we have

$$P_{f,h}(x) = O(x^{7/8} (\log x)^{1/2}). \tag{5.40}$$

Corollary 5.20. For $h = 0$, then we have

$$P_{f,0}(x) = O(x/(\log x)^{3/2-\delta}) \quad \text{for all } \delta > 0, \tag{5.41}$$

and, under (GRH), we have

$$P_{f,0}(x) = O(x^{3/4}). \tag{5.42}$$

5.3.1 Proof of Theorem 5.18

We first start with an ℓ-adic representation attached to the modular form f due to Pierre Deligne.

Let F be a number field containing a_p and $\omega(p)$ for all $p \nmid N$. We claim that there is an ultra-metric λ on F such that F_λ, the completion of F with respect to λ, is isomorphic to $\mathbb{Q}_\ell$ for some ℓ. Say $F = \mathbb{Q}(\alpha)$ and g be the minimal polynomial of α. We can find a prime ℓ such that g has a root in $\mathbb{F}_\ell$. So, from Hensel's Lemma, we have $\mathbb{Q}_\ell(\alpha) = \mathbb{Q}_\ell$. We also have a prime $\mathfrak{L}$ lying above ℓ such that the residue degree $f(\mathfrak{L}/\ell) = 1$. Therefore, taking λ to be the $\mathfrak{L}$-adic metric on F, we get $F_\lambda \cong \mathbb{Q}_\ell$. Hence, we identify a_p and $\omega(p)$ as elements in $\mathbb{Q}_\ell$.

According to Deligne, we have a representation,

$$\rho_\ell : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(F_\lambda) \cong \mathrm{GL}_2(\mathbb{Q}_\ell),$$

satisfying:

i) ρ_ℓ is unramified at primes $p \nmid N\ell$.

ii) Let $p \nmid N\ell$ and σ_p be the Frobenius element at p, we have

$$\mathrm{Tr}(\rho_\ell(\sigma_p)) = a_p \tag{5.43}$$

$$\det \rho_\ell(\sigma_p) = \omega(p)p^{k-1}. \tag{5.44}$$

From the representation ρ_ℓ, we have the group $G_\ell = \mathrm{Im}(\rho_\ell)$, which is isomorphic to $\mathrm{Gal}(\overline{\mathbb{Q}}/E_\ell)$, where E_ℓ is the fixed field of $\ker \rho_\ell$. We want to now show that G_ℓ is an ℓ-adic Lie group of dimension 4, and then try to use Theorem 3.9.

Proposition 5.21. *The group G_ℓ is an open subgroup of $\mathrm{GL}_2(\mathbb{Q}_\ell)$.*

Proof. To be filled later. □

From the above proposition, we have,

$$\dim G_\ell = \dim \mathrm{GL}_2(\mathbb{Q}_\ell) = 4.$$

Let $h(x)$ be a polynomial with complex coefficients. We assume that the coefficients of h are in F, otherwise $\Sigma_{f,h}$ would be finite. Let e be the order of the character ω and $m = (k-1)e$. The choice of this m will be clear later.

Lemma 5.22. *There exists a polynomial $H(s,t)$ in two variables s,t such that,*

$$H(s,t^m) = \prod_{\zeta\in\mu_m} (s - h(\zeta t)),$$

where μ_m is the set of m-th roots of unity. the polynomial H has coefficients in F.

Proof. Let $h(x) = b_0 + b_1 x + \cdots + b_r x^r$, where b_i's are in F. We have,

$$\prod_{\zeta\in\mu_m} (s - h(\zeta t)) = s^m - \sum_{\zeta} h(\zeta t) s^{m-1} + \sum_{\zeta_1\neq\zeta_2} h(\zeta_1 t)h(\zeta_2 t)s^{m-2} + \cdots + \prod_{\zeta} h(\zeta t).$$

We want to prove that the coefficient polynomials in variable t, are actually polynomials in t^m. We will prove it for the coefficients of s^{m-1} and s^{m-2}, the other cases follow similarly.

We see that,

$$\sum_{\zeta} h(\zeta t) = \sum_i b_i t^i \sum_{\zeta} \zeta^i.$$

Using the fact that $\sum_{\zeta} \zeta^i = 0$ if and only if $m \nmid i$, we see that $\sum_{\zeta} h(\zeta t)$ is a polynomial in t^m.

For the coefficient of s^{m-2}, we have

$$\sum_{\zeta_1\neq\zeta_2} h(\zeta_1 t)h(\zeta_2 t) = \sum_{\zeta_1\neq\zeta_2} \sum_{i+j=n} b_i b_j t^n \zeta_1^i \zeta_2^j = \sum_{i+j=n} b_i b_j t^n \sum_{\zeta_1\neq\zeta_2} \zeta_1^i \zeta_2^j$$

The sum $\sum_{\zeta_1\neq\zeta_2} \zeta_1^i \zeta_2^j$ is non-zero only when $m|i,j$. In particular $m|n$, implying the coefficient of s^{m-2} is a polynomial in t^m.

The polynomial H has coefficients which are linear combination of multiples of coefficients of h, hence they are in F. □

Consider the set

$$C = \{s \in G_\ell \mid H(\mathrm{Tr}(s), \det(s)^e) = 0\}. \tag{5.45}$$

It is a closed subset and an ℓ-adic submanifold of G_ℓ with co-dimension 1. i.e. $\dim C = 3$. From Proposition B.4, we have $\dim_M C \leq 3$. Let $p \nmid N\ell$

be a prime and σ_p be the Frobenius substitution at p. If $p \in \Sigma_{f,h}$, then we have

$$\begin{aligned} H(\mathrm{Tr}(\rho_\ell(\sigma_p)), \det(\rho_\ell(\sigma_p))^e) &= H(a_p, (\omega(p)p^{k-1})^e) \\ &= H(h(p), p^m) \\ &= \prod_\zeta (h(p) - h(\zeta p)) = 0. \end{aligned} \tag{5.46}$$

Therefore, we have

$$\Sigma_{f,h} \subseteq \Sigma_C \cup \{\ell\}, \tag{5.47}$$

Implying that

$$P_{f,h}(x) \leq \pi_C(x) + 1. \tag{5.48}$$

Using the Theorem 3.9 for C and G_ℓ, we have $\alpha = 1/4$, which proves Theorem 5.18.

5.4 Non-lacunarity of Hecke eigenforms

Let $f = \sum_{n\geq 0} a_f(n)q^n$ be a modular form, and for $x \geq 1$, let

$$M_f(x) = \#\{1 \leq n \leq x \mid a_f(n) \neq 0\}. \tag{5.49}$$

Definition 5.23. The modular form $f = \sum_{n\geq 0} a_f(n)q^n$ is said to be of type CM (complex multiplication) if there exists an imaginary quadratic extension L of $\mathbb{Q}$ such that, for $p \nmid N$, $a_f(p) = 0$ if and only if p inert in L.

Definition 5.24. A modular form $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n$ is said to be *non-lacunary* if the set $\{n \leq x \mid a_f(n) \neq 0\}$ has positive density. i.e.

$$\lim_{x\to\infty} \frac{\#\{n \leq x \mid a_f(n) \neq 0\}}{x} > 0. \tag{5.50}$$

In the following sections, we see the following:

1. A Hecke eigenform $f \in M_k(N, \omega)$ for U_p, T_p, and not of CM type is non-lacunary. We will also see two important examples.
2. A Hecke eigenform $f \in M_k(N, \omega)$ for U_p, T_p, and of CM type is lacunary.
3. An $f \in S_{\mathrm{cm}}(k, N, \omega)$ is lacunary.

5.4.1 Forms not of type CM

Theorem 5.25. *Let $f \in M_k(N, \omega)$ be non-zero for $k \geq 2$. Suppose that f is an eigenform for the operators U_p and T_p, and that f is non* CM*. There exists an $\alpha > 0$ such that,*

$$M_f(x) \sim \alpha x \quad \text{as } x \to \infty. \tag{5.51}$$

In other words, the set of positive integers n such that $a_f(n) \neq 0$ has density $\alpha > 0$.

Proof. Let $a_n = a_f(n)$ and assume that $a_1 \neq 0$. So WLOG, we can assume $a_1 = 1$. i.e. f is a normalized eigenform for the operators U_p and T_p. We therefore have,

$$f|U_p = a_p f \quad \text{for } p|N \quad \text{and} \quad f|T_p = a_p f \quad \text{for } p \nmid N.$$

Moreover, the function $n \mapsto a_n$ is multiplicative. Let us distinguish the two cases:

(a) *f is a cusp form*

According to Corollary 5.20,

$$\#\{p \leq x \mid a_p = 0\} = O(x/(\log x)^{1+\delta}),$$

with $\delta = 1/3$. When we apply Theorem 5.4 of Section 5 to the map $n \mapsto a_n$, with $K = \mathbb{Q}$ and $\lambda = 0$, we get (5.51).

(b) *f is not a cusp form*

From the Remark 5.26, we have

$$a_p = \chi(p) + \chi^{-1}(p)\omega(p)p^{k-1} \quad \text{when } p \nmid N. \tag{5.52}$$

Hence, as $k \geq 2$, $a_p \neq 0$ for all $p \nmid N$. Let S denote the set of primes $p|N$ such that $a_p = 0$. We have $a_n = 0$ if and only if there exists a prime divisor p of n such that $p \in S$. Therefore, we have $M_f(x) = \{n \leq x \mid \gcd(n, p) = 1 \text{ for all } p \in S\}$. So, we have

$$M_f(x) = \alpha x + O(1), \quad \text{where } \alpha = \prod_{p \in S} \left(1 - \frac{1}{p}\right).$$

That is, the density of $M_f(x)$ is α.

□

Remark 5.26. The definitions and notations used here are from [Miy89]. We know that $M_k(N,\omega) = E_k(\omega) \oplus S_k(\omega)$, where $E_k(\omega)$ is the space generated by the Eisenstein series and $S_k(\omega)$ is the space of cusp forms. Let $f = e + g$, where $e \in E_k(\omega)$ and $g \in S_k(\omega)$. For $p \not| N$, we have

$$f|T_p = e|T_p + g|T_p = a_p e + a_p g.$$

As $E_k(\omega)$ and $S_k(\omega)$ are closed under T_p, we have

$$e|T_p = a_p e \quad \text{and} \quad g|T_p = a_p g.$$

Similarly, for $p|N$,

$$e|U_p = a_p e \quad \text{and} \quad g|U_p = a_p g.$$

If $g = \sum_{n\geq 1} b_n q^n$ is non-zero, then we have $b_p = b_1 a_p$ for all primes p. Moreover, we have

$$b_n = b_1 a_n.$$

That is, $g = b_1 \sum_{n\geq 1} a_n q^n$. Similarly, as e is non-zero, $e = c_1 \sum_{n\geq 0} a_n q^n$ for a constant c_1. From this, we get that the constant map $b_1 c_1 a_0 = b_1 e - c_1 g \in M_k(N,\chi)$, which is a contradiction. Hence, $g = 0$ and $f = e \in E_k(\omega)$. Let $\{f_i\}_{i=1}^k$ be the set of linearly independent normalized Eisenstein series spanning $E_k(\omega)$ and let $f = \sum_{i=1}^k \lambda_i f_i$. We have, for $p \not| N$,

$$\begin{aligned} f|T_p &= \sum_{i=1}^k \lambda_i (f_i|T_p) \\ &= a_p \sum_{i=1}^k \lambda_i f_i. \end{aligned}$$

Hence, as f_i's are eigenforms, we have $f_i|T_p = a_p f_i$. If a_n^i denotes the n-th Fourier coefficient of f_i, then we have $a_p^i = a_p a_1^i = a_p$ for all $i = 1, \cdots, k$. Let χ_i be characters mod N such that $f_i = f(z, \chi_i, \chi_i^{-1}\omega)$, we have $a_p = a_p^i = \chi_i(p) + \chi_i^{-1}(p)\omega(p)p^{k-1}$.

5.4.2 Calculating the density

In this section, we calculate $\alpha = \lim_{x\to\infty} x^{-1} M_f(x)$.

Suppose,

$$a_n^0 = \begin{cases} 1 & \text{if } a_f(n) \neq 0, \\ 0 & \text{if } a_f(n) = 0. \end{cases} \tag{5.53}$$

and

$$\alpha_p = (1 - p^{-1})(1 + \sum_{n=1}^{\infty} a_{p^n}^0 p^{-n}). \tag{5.54}$$

As seen before, for $c : \mathbb{N} \to \mathbb{C}$ such that $a_n^0 = \sum_{d|n} c(d)$, we have

$$1 + \sum_{n=1}^{\infty} c(p^n)p^{-n} = \alpha_p.$$

We therefore have,

$$\alpha = \prod_p \alpha_p. \tag{5.55}$$

Let us distinguish the two cases:

(i) $p|N$

We have $a_{p^n}^0 = (a_p^0)^n$, giving us,

$$\alpha_p = \begin{cases} 1 - p^{-1} & \text{if } a_p^0 = 0, \ (a_p = 0) \\ 1 & \text{if } a_p^0 = 1. \ (a_p \neq 0) \end{cases} \tag{5.56}$$

(ii) $p \not| N$

If β_p and γ_p are such that

$$1 - a_p T + \omega(p)p^{k-1}T^2 = (1 - \beta_p T)(1 - \gamma_p T),$$

then we have

$$a_{p^m} = \sum_{i=0}^{m} \beta_p^i \gamma_p^{m-i} = \begin{cases} (m+1)\beta_p^m & \text{if } \beta_p = \gamma_p, \\ (\beta_p^{m+1} - \gamma_p^{m+1})/(\beta_p - \gamma_p) & \text{if } \beta_p \neq \gamma_p. \end{cases} \tag{5.57}$$

The formula $a_p a_{p^n} = \sum_{d|(p,p^n)} \omega(d)d^{k-1}a_{\frac{p^{n+1}}{d}} = a_{p^{n+1}} + \omega(p)p^{k-1}a_{p^n}$, and induction on n proves (5.57).

So, $a_{p^m} = 0$ if and only if β_p/γ_p is an $m+1$-th root of unity. Whence:

$$\alpha_p = \begin{cases} 1 & \text{If } \beta_p = \gamma_p \text{ or } \beta_p/\gamma_p \text{ is not a root of unity,} \\ 1 - \dfrac{p-1}{p^{r(p)}-1} & \text{If } \beta_p/\gamma_p \text{ is a root of unity of order } r(p) \geq 2. \end{cases} \tag{5.58}$$

In particular, $a_p = 0 \iff r(p) = 2 \iff \alpha_p = 1 - 1/(p+1)$.

Examples 5.27. We are interested in the case when $\omega = 1$ (imposing that k is even), and the case when a_n's are integers. We have:

Proposition 5.28. *Let p be a prime and let β_p/γ_p be an $r(p)$-th primitive root of unity. If:*

(a) $p = 2$, then $a_2 = \pm 2^{k/2}$, $r(2) = 4$ and $\alpha_2 = 14/15$;

(b) $p = 3$, then $a_3 = \pm 3^{k/2}$, $r(3) = 6$ and $\alpha_3 = 363/364$.

(c) $p > 3$, then $r(p) = 2$ and $\alpha_p = 1 - 1/(1+p)$.

Proof. Let us observe that, as $a_p \in \mathbb{Z}$, β_p and γ_p belong to a quadratic extension L of $\mathbb{Q}$. Therefore, we have the field extensions

$$\mathbb{Q} \subset \mathbb{Q}(\beta_p/\gamma_p) \subseteq L.$$

As β_p/γ_p is a primitive $r(p)$-th root of unity, we have $\phi(r(p)) = 2$. Hence, $r(p) = 2, 3, 4$ or 6.

1) $(r(p) \neq 3)$ We see that $a_{p^2} = 0$ in this case, implying that

$$a_p^2 = p^{k-1},$$

which is a contradiction as k is even.

2) $(r(p) = 4)$ We have,

$$a_p^2 = \beta_p^2 + \gamma_p^2 + 2\beta_p\gamma_p = 2p^{k-1}.$$

For $p \geq 3$, we can't have the above. For $p = 2$, we have $a_p^2 = 2^k$, i.e. $a_p = \pm 2^{k/2}$.

3) $(r(p) = 6)$ We have,

$$a_p^3 = \beta_p^3 + \gamma_p^3 + 3\beta_p\gamma_p(\beta_p + \gamma_p) = 3p^{k-1}a_p.$$

We therefore have $p = 3$ is the only possibility, and in this case $a_3 = \pm 3^{k/2}$.

Hence, for a prime $p > 3$, we have $r(p) = 2$. □

Eg. 1: Let $k = 2,\ N = 11$, and

$$f = q\prod_{n\geq 1}(1-q^n)^2(1-q^{11n})^2 = \eta^2(z)\eta^2(11z)$$

.

We have $a_2 = -2,\ a_3 = -1$ and $a_{11} = -1$. From where, $\alpha_2 = 14/15$, $\alpha_3 = \alpha_{11} = 1$, and for $p \neq 2, 3, 11$, $\alpha_p = 1$ if $a_p \neq 0$ and $\alpha_p = 1-1/(p+1)$ if $a_p = 0$. Hence, the density

$$\alpha = \frac{14}{15}\prod_{a_p=0}(1-1/(p+1)). \tag{5.59}$$

In (5.59), it can be deduced that $\alpha < 0.847$. It is probable that $\alpha \geq 0.845$, but, for a proof, it is convenient to find an explicit, but non-trivial, bound for the number of primes $p \leq x$ such that $a_p = 0$.

Eg. 2: (Ramanujan Δ function) Let $k = 12,\ N = 1$ and

$$f = \Delta = q\prod_{n\geq 1}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n.$$

We have $\tau(2) = -24$ and $\tau(3) = 252$. From which we have, $\alpha_2 = \alpha_3 = 1$, $\alpha_p = 1$ for all $\tau(p) \neq 0$ and, $\alpha_p = 1 - 1/(p+1)$ for all $\tau(p) = 0$. We have the density α of n's such that $\tau(n) \neq 0$ to be,

$$\alpha = \prod_{\tau(p)=0}\left(1-\frac{1}{p+1}\right). \tag{5.60}$$

In fact, the *Lehmer's conjecture* says that $\tau(n) \neq 0$ for all $n \geq 1$.

5.4.3 Forms of type CM

Let $k \geq 2$ and $f = \sum_{n=0}^{\infty} a_n q^n \in M_k(N, \omega)$ be an eigenform for the operators U_p and T_p.

Definition 5.29. The modular form f is said to be of type CM (complex multiplication) if there exists an imaginary quadratic extension L of $\mathbb{Q}$ such that, for $p \not| N$, $a_p = 0$ if and only if p inert in L.

Proposition 5.30. *Let $f \not\equiv 0$, be an eigenform for the operators U_p and T_p, such that f is of type* CM. *Then there exists an $\alpha > 0$ such that*

$$M_f(x) \sim \alpha x/(\log x)^{1/2}, \quad \text{as } x \to \infty. \tag{5.61}$$

(As in Theorem 5.25, we assume $a_f(1) = 1$ and $n \mapsto a_f(n)$ is multiplicative.)

Proof. Let $P(x) = \#\{v \in \Sigma_L \mid a_f(\mathfrak{p}_v) = 0\} = \#\{p \text{ inert in } L \mid \mathrm{N}p = p^2 \leq x\}$, then

$$P(x) = \frac{x}{2\log x} + O(x/(\log x)^2). \quad \text{(cf. (5.62) below)}$$

Using Theorem 5.4 for $K = \mathbb{Q}$, $\lambda = 1/2$ and $\delta = 1$, we get the proposition. □

Remark 5.31 (Density of primes inert in a quadratic extension)**.** Leaving out finitely many, we either have a prime that splits or a prime that is inert in a quadratic extension $L/\mathbb{Q}$. We have,

- $\mathrm{Frob}_p = \{1\}$, if p splits.
- Frob_p generates $\mathrm{Gal}(L/\mathbb{Q})$, if p is inert.

Using the Chebotarev Density Theorem for the conjugacy class $\{\mathrm{Frob}_p\}$, we get the density of primes inert in L is equal to $1/2$. Moreover, using (3.6), if $P(x) = \#\{p \text{ inert in } L \mid \mathrm{N}p \leq x\}$, then

$$P(x) = \frac{x}{2\log x} + O(x/(\log x)^2). \tag{5.62}$$

5.5 Non-lacunarity of Modular Forms of weight greater than 1

5.5.1 The Space $M_k(N, \omega)$

Let us recall that $M_k(N, \omega)$, the space of modular forms of type (k, ω) on $\Gamma_0(N)$, has the following direct sum decomposition,

$$M_k(N, \omega) = S_k(N, \omega) \oplus E_k(N, \omega), \tag{5.63}$$

where $S_k(N, \omega)$ is the space of cusp forms and $E_k(N, \omega)$ is the space of Eisenstein series, which is also the null space of $S_k(N, \omega)$ with respect to the Peterson inner product (cf, [Miy89], Theorem 4.7.2). This decomposition is stable under U_p and T_p.

Let $\mathfrak{M} = \mathfrak{M}(N, \omega)$ be the set of positive divisors M of N such that the *conductor* of ω divides M (If ω is primitive, then $\mathfrak{M} = \{N\}$). For $M \in \mathfrak{M}$, let ω_M be the character, mod M, that coincides with ω for all entries co-prime to N. i.e.

$$\omega_M(n) = \omega(n), \quad \text{for all } (n, N) = 1. \quad (\omega_M \text{ induces } \omega)$$

Proposition 5.32. *Let $M \in \mathfrak{M}$, $f \in S_k(M, \omega_M)$, for a positive number d such that $d|N/M$, we define $f_d(z) := f(dz)$. We have $f_d \in S_k(N, \omega)$.*

Definition 5.33. A non-zero $g \in S_k(N, \omega)$ is called an *oldform* of level N and weight k, if it is of the form f_d, for some $d > 1$. An eigenform $f \in S_k(N, \omega)$ for all T_p's, $p \not| N$, that is not an oldform is called as a *newform*.

Let P_M be the set of new forms of level M and of type (k, ω_M). Moreover, we have

$$\{f_d \mid d|N/M \text{ and } f \in P_M\}$$

to be a basis for $S_k(N, \omega)$ (cf. (5.35) for examples). Denote $S_{\text{cm}}(k, N, \omega)$, respectively $S_{\text{cm}}^{\text{non}}(k, N, \omega)$, the space generated by $\{f_d\}$ when f has CM, respectively doesn't have CM. We have,

$$S_k(N, \omega) = S_{\text{cm}}(k, N, \omega) \oplus S_{\text{cm}}^{\text{non}}(k, N, \omega). \tag{5.64}$$

The spaces $S_{\text{cm}}(k, N, \omega)$ and $S_{\text{cm}}^{\text{non}}(k, N, \omega)$ are stable under the operators U_p and T_p. This is seen by the following proposition:

Proposition 5.34. *For all $M \in \mathfrak{M}$, $f \in P_M$ and a positive divisor d of N/M, we have:*

$$f_d|T_p = a_f(p) f_d \quad \text{if } p \not| N, \tag{5.65}$$

$$f_d|U_p = \begin{cases} f_{d/p} & \text{if } p|d, \\ a_f(p) f_d & \text{if } p \not| d \text{ and } p|m, \\ a_f(p) f_d - \omega_M(p) p^{k-1} f_{dp} & \text{if } p \not| dM \text{ and } p|N. \end{cases} \tag{5.66}$$

Proof. Let $f(z) = \sum_{n=1}^{\infty} a_f(n) q^n \in P_M$. We know that $f|T_p = a_f(p) f$ for all $p \not| M$, implying

$$\begin{aligned} a_f(np) &= a_f(p) a_f(n) \quad \text{if } p \not| n, \\ a_f(p) a_f(n) &= a_f(np) + \omega_M(p) p^{k-1} a_f(n/p) \quad \text{if } p|n. \end{aligned} \tag{5.67}$$

We have, $f_d(z) = \sum_{n=1}^{\infty} a_f(n)q^{nd} = \sum_{n=1}^{\infty} b_n q^n$, where $b_n = 0$ if $d \not| n$, and $b_n = a_f(n/d)$ if $d|n$. For $p \not| N$, we have

$$f_d|T_p = \sum_{n=1}^{\infty} c_n q^n, \quad \text{where } c_n = \sum_{d|(p,n)} \omega(d) d^{k-1} b_{np/d^2}.$$

If $d \not| n$, then

$$c_n = b_{np} + \omega(p)p^{k-1}b_{n/p} = 0. \quad (\text{as } d \not| np \text{ and } n/p)$$

If $n = dm$, then

$$c_n = b_{np} + \omega(p)p^{k-1}b_{n/p} = a_f(mp) + \omega(p)p^{k-1}a_f(m/p) = a_f(p)a_f(m).$$

Hence, we get (5.65).

To prove (5.66), we see that $f_d|U_p = \sum_{n=1}^{\infty} b_{np} q^n$.

- If $p|d$,
$$f_d|U_p = \sum_{d|np} a_f(np/d)q^n = f_{d/p}.$$

- If $p \not| d$ and $p|M$, then
$$f_d|U_p = \sum_{d|n} a_f(np/d)q^n = a_f(p)f_d.$$

- If $p \not| dM$ and $p|N$, we have $f|T_p = a_f(p)f$, and therefore have (5.67). Therefore, we have
$$\begin{aligned} f_d|U_p &= \sum_{m=1}^{\infty} a_f(mp)q^{md} \\ &= \sum_{m=1}^{\infty} a_f(p)a_f(m)q^{md} + c(p,m)\sum_{m=1}^{\infty} a_f(m/p)q^{md}, \end{aligned}$$
where $c(p,m) = 0$ if $p \not| m$, and $c(p,m) = -\omega_M(p)p^{k-1}$, otherwise.

We have proved (5.66). □

Examples 5.35. 1. Let $\eta(z) = e^{2\pi z/24}\prod_{n=1}^{\infty}(1-e^{2\pi nz})$ be the Dedekind eta function, and let $f(z) = (\eta(z)\eta(2z))^8$. We see that $f \in S_8(\Gamma_0(2))$ and is a newform. To see this, we have $\dim S_8(\Gamma_0(2)) = 1$, which follows form a more general formula (cf. Stein [SGS07])

$$\begin{aligned}\dim S_k(\Gamma_0(N) = (k-1)(g_0(N)-1) + (k/2-1)C_0(N)\\ + \mu_{0,2}(N)\left[\frac{k}{4}\right] + \mu_{0,3}(N)\left[\frac{k}{3}\right].\end{aligned}$$

In the case of $N = 2$ and $k = 8$, we have

$$\mu_{0,2}(N) = 1,\ \mu_{0,3}(2) = 0,\ C_0(2) = 2 \text{ and } g_0(2) = 0.$$

2. The space $S_{12}(\Gamma_0(2))$ is spanned by $\Delta(z) = \eta(z)^{24}$ and $\Delta(2z)$. This can be seen by the linear independence of $\Delta(z), \Delta(2z)$ and the fact that $\dim S_k(\Gamma_0(2)) = 2$.

Hence, we see that $M_k(N,\omega)$ has the following decomposition of spaces invariant under U_p and T_p.

$$M_k(N,\omega) = S_{\text{cm}}^{\text{non}}(k,N,\omega) \oplus S_{\text{cm}}(k,N,\omega) \oplus E_k(N,\omega). \tag{5.68}$$

Theorem 5.36. *Let $f \in M_k(N,\omega)$, with $k \geq 2$.*

(i) If $f \notin S_{\text{cm}}(k,N,\omega)$, we have

$$M_f(x) \asymp x \quad \text{as } x \to \infty.$$

(ii) If $f \in S_{\text{cm}}(k,N,\omega)$ and $f \neq 0$, we have

$$M_f(x) \asymp x/(\log x)^{1/2} \quad \text{as } x \to \infty.$$

Recall the notation $\phi \asymp \psi$ means that $\phi = O(\psi)$ and $\psi = O(\phi)$.

Remark 5.37. In Theorem 5.36, the statement (ii) says that a modular form $f \in S_{\text{cm}}(k,N,\omega)$ is Lacunary. i.e. $\lim_{x\to\infty} M_f(x)x^{-1} = 0$.

5.5.2 Proof of Theorem 5.36

We have $M_f(x) = O(x)$, as $M_f(x) \leq x$, and if $f \in S_{\mathrm{cm}}(k, N, \omega)$, we have

$$M_f(x) = O(x/(\log x)^{1/2}). \tag{5.69}$$

To see (5.69), assume $f = \sum_{n=1}^{\infty} a_f(n)q^n = \sum_{i=1}^{k} g^i_{d_i}$, where g^i's are CM forms. Let $g^i = \sum_{n=1}^{\infty} a^i(n)q^n$, and let $g^i_{d_i} = \sum_{n=1}^{\infty} b^i(n)q^n$ for

$$b^i(n) = \begin{cases} 0 & \text{if } d_i \not| n, \\ a^i(n/d_i) & \text{if } d_i | n. \end{cases}$$

We have

$$a_f(n) = \sum_{i=1}^{k} b^i(n).$$

Hence, $a_f(n) \neq 0$ implies $b^i(n) \neq 0$ for some i, and hence $a^i(n/d_i) \neq 0$.Therefore, we have

$$M_f(x) \leq \sum_{i=1}^{k} M_{g^i}(x/d_i).$$

As $M_{g^i}(x/d_i) = O(x/(\log x)^{1/2})$, we have (5.69).

Let us define

$$R_i = \{f \in M_k(N, \omega) \mid \liminf_{x\to\infty} x^{-1} M_f(x)(\log x)^i = 0\}.$$

We are interested in R_0 and $R_{1/2}$. More precisely, to prove Theorem 5.36, we show that

$$R_0 = S_{\mathrm{cm}}(k, N, \omega) \quad \text{and} \quad R_{1/2} = 0.$$

Let us denote $\mathfrak{H}$, for the $\mathbb{C}$-algebra of endomorphisms of $M_k(N, \omega)$ generated by U_p and T_p, for all p.

Lemma 5.38. *The set R_i is stable under $\mathfrak{H}$. In particular, R_0 and $R_{1/2}$ are stable under $\mathfrak{H}$.*

Proof. For $f(z) = \sum_{n=0}^{\infty} a_n q^n$, let $f|T_p = \sum_{n=0}^{\infty} b_n q^n$, where

$$b_n = a_{np} + \omega(p)p^{k-1}a_{n/p}.$$

As $b_n \neq 0$ if and only if $a_{np} \neq 0$ or $a_{n/p} \neq 0$, we have

$$M_{f|T_p}(x) \leq M_f(x/p) + M_f(xp) \leq 2M_f(xp). \tag{5.70}$$

If $f \in R_i$, then $\liminf x^{-1}M_f(x)(\log x)^i = 0$, i.e. there is a sequence $x_n \to \infty$ such that $x_n^{-1}M_f(x_n)(\log x_n)^i \to 0$. From (5.70), we have $f|T_p \in R_i$.

Similarly, for $A \in \mathfrak{H}$, we have a constants m_A and C_A such that

$$M_{Af}(x) \leq C_A M_f(m_A x). \tag{5.71}$$

Therefore, using (5.71), $Af \in R_i$. □

To see (5.71), we have

$$M_{f+g}(x) \leq M_f(x) + M_g(x). \tag{5.72}$$

for any $f, g \in M_k(N, \omega)$.

Now we resume the proof of Theorem 5.36. From (5.69), we see that $S_{\mathrm{cm}}(k, N, \omega) \subseteq R_0$. We need to prove the equality, as mentioned before. Consider $f \in R_0 \setminus S_{\mathrm{cm}}(k, N, \omega)$ of the form,

$$f = g + h, \quad g \in S_{\mathrm{cm}}(k, N, \omega) \text{ and } h \in S_{\mathrm{cm}}^{\mathrm{non}}(k, N, \omega) \oplus E_k(N, \omega).$$

(Note that $h \neq 0$.) As $M_h(x) \leq M_f(x) + M_g(x)$ and $M_g(x) = o(x)$, we have $h \in R_0$. Therefore, $\mathfrak{H}h$ is an $\mathfrak{H}$-module. It has a *simple* $\mathfrak{H}$-submodule Σ. As $\Sigma \subseteq M_k(N, \omega)$ is a finite dimensional $\mathbb{C}$-subspace, we can use Schur's Lemma (See 5.39 below) to obtain an eigenform, say $\hat{h}$, for T_p and U_p. As $\hat{h}$ is not of type CM, we have an $\alpha > 0$ such that $M_{\hat{h}}(x) \sim \alpha x$, contradicting the fact that $\hat{h} \in R_0$. This says that $R_0 = S_{\mathrm{cm}}(k, N, \omega)$, thereby proving (i) of Theorem 5.36.

Proposition 5.39 (Schur's Lemma)**.** *Let A be an algebra over an algebraically closed field F, and M be a finitely dimensional (over F) simple A-module. Then, an endomorphism of M is a multiplication by an element in F.*

For part (ii) of Theorem 5.36, we should prove $R_{1/2} = 0$. Let $f \in R_{1/2}$ be non-zero. Similarly as before, there is an eigenform $\hat{f}$ for U_p and T_p. Moreover, as $\hat{f}$ is of the type CM, we have an $\alpha > 0$ such that

$$M_{\hat{f}}(x) \sim \alpha x/(\log x)^{1/2},$$

contradicting the fact that $\hat{f} \in R_{1/2}$.

Appendices

Appendix A

I Maps Between Curves

Let K be a field, $\overline{K}$ be a fixed algebraic closure of K. A *curve* is a projective variety of dimension 1 in a projective space $\mathbb{P}^n$.

Let us recall the definition of a coordinate ring of a projective algebraic set.

Definition A.1. Let $Y \subseteq \mathbb{P}^n$ be an algebraic set and $S = \overline{K}[x_0, \cdots, x_n]$. Define $\mathcal{I}(Y)$ to be the ideal generated by

$$\{f \in S \mid f \textit{ is homogeneous },\ f(P) = 0 \ \ \forall\ P \in Y\}$$

The coordinate ring of Y, denoted $S(Y)$, is defined as

$$S(Y) := S/\mathcal{I}(Y)$$

Definition A.2 (Function field)**.** The function field of a projective variety Y is the subfield of the field of quotients of $S(Y)$ consisting of elements f/g, where f, g are homogeneous of same degree and $g \neq 0$. It is denoted by $\overline{K}(Y)$.

Now let us define a rational map between two projective varieties.

Definition A.3. Let $U \subseteq \mathbb{P}^n, V \subseteq \mathbb{P}^m$ be two projective varieties. A *rational map* $\phi : U \to V$ is of the form

$$\phi(P) = [f_1(P), \cdots, f_m(P)]$$

where $f_1, \cdots, f_m \in \overline{K}(U)$.

Example A.4.

(a) Consider the circle $C : X^2 + Y^2 = Z^2$ and the map $\phi : C \to \mathbb{P}^1$ defined by

$$\phi[X, Y, Z] = [X, Y].$$

We also have a map $\psi : \mathbb{P}^1 \to C$ defined by

$$\psi[S, T] = [S^2 - T^2, 2ST, S^2 + T^2].$$

(*b*) Consider the hyperbola $C : XY = Z^2$ and the map $x = X/Z : C \to \mathbb{P}^1$ defined by

$$x[X, Y, Z] = [X/Z, 1].$$

We note that a rational map $\phi : U \to V$ may not be defined for all points on U, but we can calculate at some special points called *regular points*.

Definition A.5. Let $\phi = [f_1, \cdots, f_k] : U \to V$ be a rational map. A point $P \in U$ is said to be a *regular point* if there exists a $g \in \overline{K}(U)$ such that $gf_i(P) \neq 0$ for some $i = 1, \cdots, k$. We then define $\phi(P) = [gf_1, \cdots, gf_k]$.

Example A.6. Let $C : XY = Z^2$ and $x = [X/Z, 1] : C \to \mathbb{P}^1$. By the definition of x, we can't evaluate it at $P = [1, 0, 0]$. But we can evaluate it as follows,

$$x(P) = [X/Z, 1](P) = [X, Z](P) = [1, 0].$$

Similarly, for $Q = [0, 1, 0]$ we evaluate it as follows,

$$x(P) = [X/Z, 1](P) = [Z/Y, 1](P) = [0, 1].$$

For a more abstract definition of a rational map between projective varieties X and Y, we refer [Har77].

I.1 Maps Between Smooth Curves

Rational maps between smooth curves are of two types: they are either constant or they are surjective.

For a curve C/K, we have the identification (cf. [Sil06], Example II.2.2)

$$\overline{K}(C) \longleftrightarrow \{\text{maps } C \to \mathbb{P}_1 \text{ defined over } K\}.$$

Given a non-constant rational map $\phi : C_1 \to C_2$ between two smooth curves, we define the map

$$\phi^* : \overline{K}(C_2) \to \overline{K}(C_1), \quad f \mapsto f \circ \phi.$$

The map is a ring homomorphism and , as ϕ is not constant, is an injection of function fields.

Definition A.7. Let $\phi : C_1 \to C_2$ be a rational map between two smooth curves.

1. If ϕ is constant, we say *degree* of ϕ is 0. Otherwise, we say *degree* of ϕ is the degree of the extension $\overline{K}(C_1)/\phi^*(\overline{K}(C_2))$.

2. Assume ϕ is not constant. We say ϕ is *separable* if $\overline{K}(C_1)/\phi^*(\overline{K}(C_2))$ is a separable extension. Moreover,

I.2 Frobenius Morphisms

Let K be a field of characteristic $p > 0$ and $q = p^r$. For a curve C/K given by the the equation $F(X, Y, Z) = 0$, we can define a new curve $C^{(q)}$ as the zero set for the polynomial whose coefficients are q^{th} powers of coefficients of F.

Example A.8. Let $K = \mathbb{F}_3[i]$, where i is the square root of -1 in $\overline{\mathbb{F}_3}$. Consider $E : y^2 = x^3 + ix$, we have

$$E^{(3)} : y^2 = x^3 - ix.$$

There is a natural map $\phi_q : C \to C^{(q)}$ defined by

$$\phi_q[x_0, x_1, \cdots, x_n] = [x_0^q, x_1^q, \cdots, x_n^q].$$

This map is called as the q-th Frobenius morphism. The next proposition states some properties of this map.

Proposition A.9. *Let $\phi_q : C \to C^{(q)}$ be the q-th Frobenius morphism. We have*

- $\phi_q^*(\overline{K}(C^{(q)})) = \overline{K}(C)^q$.
- *ϕ_q is purely inseparable.*
- $\deg(\phi_q) = q$.

Proof. cf. [Sil06], Proposition II.2.11. □

Remark A.10. Let $E/\mathbb{F}_q$ be an elliptic curve. As $E^{(q)} = E$, we have the q-th *Frobenius endomorphism*

$$\phi_q : E \to E, \quad [x, y] \mapsto [x^q, y^q, z^q].$$

Also, we see that the $\mathbb{F}_q$ rational points on the elliptic curve E are precisely the elements of $\ker(\phi_q - 1)$.

Lemma A.11. *If $\psi : C_1 \to C_2$ is a morphism between two smooth curves C_1 and C_2, then there exists a separable morphism $\lambda : C_1^{(q)} \to C_2$ and a Frobenius morphism $\phi : C_1 \to C_1^{(q)}$, where $q = \deg_i(\psi)$, such that $\psi = \lambda \circ \phi$. i.e.*

$$\psi : C_1 \xrightarrow{\phi} C_1^{(q)} \xrightarrow{\lambda} C_2.$$

Proof. Let $\mathbf{F}$ be the separable closure of $\phi^*(\overline{K}(C_2))$ inside $\overline{K}(C_1)$. As the extension $\overline{K}(C_1)/\mathbf{F}$ is purely inseparable, we have $f^q \in \mathbf{F}$ for all $f \in \overline{K}(C_1)$, i.e. $\overline{K}(C_1)^q \subseteq \mathbf{F}$, where $q = \deg_i(\psi)$. From Proposition A.9, we have $\overline{K}(C_1)^q = \mathbf{F}$. Hence, we have the field extensions

$$\psi^*(\overline{K}(C_2)) \hookrightarrow \overline{K}(C_1)^q \hookrightarrow \overline{K}(C_1).$$

The first inclusion is induced by a separable morphism $\lambda : C_1^{(q)} \to C_2$ and the other inclusion by the Frobenius map $\phi : C_1 \to C_1^{(q)}$. It is clear that, as $\psi^* = (\lambda \circ \phi)^*$, $\psi = \lambda \circ \phi$. □

II Divisors

Let C be a curve over K in the projective plane $\mathbb{P}^2 = \mathbb{P}^2_{\overline{K}}$.

Definition A.12. The divisor group of the curve C is the free abelian group generated by the points on C. It is denoted by $\mathrm{Div}(C)$. An element of this group is called a divisor.

A divisor is of the form

$$D = \sum_{P \in C} n_P(P)$$

where $n_P = 0$ for all but finitely many. The **degree** of D is defined to be $\sum_{P \in C} n_P$ and is denoted by $\deg(D)$. We see that the set, $\{D \in \mathrm{Div}(C) \mid \deg(D) = 0\}$ forms a subgroup of the divisor group. This is denoted by $\mathrm{Div}^0(C)$.

We see that $G_K = \mathrm{Gal}(\overline{K}/K)$ acts on the points on C as follows, For $P = [x_0, x_1, x_2] \in C$ and $\sigma \in G_K$

$$P^\sigma := [\sigma(x_0), \sigma(x_1), \sigma(x_2)]$$

We can extend this action to $\mathrm{Div}(C)$ as follows

$$D^\sigma = \sum_{P \in C} n_P(P^\sigma)$$

As $\deg(D) = \deg(D^\sigma)$ we see that G_K similarly acts on $\mathrm{Div}^0(C)$.

Definition A.13. A divisor $D \in \mathrm{Div}(C)$ is said to be defined over K if $D = D^\sigma$ for all $\sigma \in G_K$.

Example A.14. Let $C:\ XY = Z^2$ be a hyperbola over $\mathbb{Q}$. We see that

$$C = \{[x, y, 1] \in \mathbb{P}^2_{\overline{\mathbb{Q}}} \mid xy = 1\} \cup \{[0, 1, 0], [1, 0, 0]\}$$

Let $P_1 = [i, -i, 1],\ P_2 = [-i, i, 1]$ then $D = n_1((P_1) + (P_2))$ is defined over $\mathbb{Q}$.

The set of divisors defined over K forms a group denoted by $\mathrm{Div}_K(C)$. Similarly, $\mathrm{Div}^0_K(C)$ denotes the group $\mathrm{Div}_K(C) \cap \mathrm{Div}^0(C)$.

For a smooth curve C, we know that

$$\mathcal{O}_P := \left\{ \frac{h}{g} \in \overline{K}(Y) \mid g(P) \neq 0 \right\}$$

is a DVR with the valuation $\mathrm{ord}_P : \overline{K}(Y)^* \to \mathbb{Z}$ for all $P \in C$. For $f \in \overline{K}(C)^* = \overline{K}(C) - \{0\}$ we define

$$\mathrm{div}(f) := \sum_{P \in C} \mathrm{ord}_P(f)(P)$$

The above definition is well defined as it follows from the theorem below.

Theorem A.15. *Let C be a smooth curve and $f \in \overline{K}(C)^*$. Then there are only finitely many points at which f either has a zero or a pole.*

Example A.16. Lets consider the same example of the hyperbola, $C : XY = Z^2$ and $f = X^2/ZY \in \overline{K}(C)^*$. It has poles at $Z = 0$ an $Y = 0$, i.e at $[1, 0, 0]$ on C. What about $[0, 1, 0]$?

$$f = \frac{(Z^2/Y)^2}{ZY} = \frac{Z^4}{ZY^3} = \frac{Z^3}{Y^3}$$

Hence $f[0, 1, 0] = 0$. We see that these are the only zeros and poles of f.

There is an action on $\overline{K}(C)$ by the Galois group G which acts on the coefficients of the polynomial. For $\sigma \in G_K$ we denote the action on f by f^σ.

Proposition A.17. *For $\sigma \in G_K$,*

$$\mathrm{div}(f^\sigma) = (\mathrm{div}(f))^\sigma$$

Proposition A.18. *The maps*

$$\mathrm{div} : \overline{K}(C)^* \to \mathrm{Div}(C)$$
$$\mathrm{div}|_{K(C)} : K(C)^* \to \mathrm{Div}_K(C)$$

are homomorphisms of abelian groups.

Definition A.19. A divisor $D \in \mathrm{Div}(C)$ is called principal if $D = \mathrm{div}(f)$ for some $f \in \overline{K}(C)$. Define an equivalence relation on D by $D_1 \sim D_2$ if $D_1 - D_2$ is principal. The divisor class group of C, denoted by $\mathrm{Pic}(C)$, is defined by

$$\mathrm{Pic}(C) = \mathrm{Div}(C)/\mathrm{Img}(\mathrm{div})$$

Define $\mathrm{Pic}_K(C) \subseteq \mathrm{Pic}(C)$ to be the divisors fixed by G_K.

Theorem A.20. *Let C be a smooth curve and $f \in \overline{K}(C)^*$. Then,*
(a) $\mathrm{div}(f) = 0$ *if and only if* $f \in \overline{K}^*$.
(b) $\deg(\mathrm{div}(f)) = 0$.

To prove the first part, we require the following lemma.

Lemma A.21. *If $\phi : C_1 \to C_2$ is a rational map between two smooth curves C_1 and C_2, then ϕ is a constant map or a surjection.*

For part (b), we refer to [Sil06].

Example A.22. Lets first look at Lemma 1. If we take $C_2 = \mathbb{P}^1$ then the Lemma 1 states that for a point $[a, b] \in \mathbb{P}^1$, we have a point $P \in C_1$ such that $\phi(P) = [a, b]$. More specifically, If $\phi := [f, g]$ for $f, g \in \overline{K}(C)^*$, then f and g have zeros on C.

Example A.23. Let us consider the smooth curve $C = \mathbb{P}^1$. We saw that in general, every principal divisor is of degree 0. In this case, we see that any divisor of degree 0 is principal. Let $D = \sum_{P \in \mathbb{P}^1} n_P(P)$ be a divisor of degree 0. i.e. $\sum_P n_P = 0$. For $P = [a_P, b_P]$, consider the function

$$f = \prod_{P \in \mathbb{P}^1} (Xb_P - Ya_P)^{n_P}$$

As $\sum_P n_p = 0$ we have $f \in \overline{K}(\mathbb{P}^1)$. For $P \in \mathbb{P}^1$, we have $M_P = \{g \in \overline{K}(\mathbb{P}^1) \mid g(P) = 0\} = \langle Xb_P - Ya_P \rangle$ and hence $\mathrm{ord}_P(f) = n_P$. Therefore,

$$\mathrm{div}(f) = \sum_{P \in \mathbb{P}^1} n_P(P) = D$$

From the above result, we see that the map, $\deg : \mathrm{Div}(\mathbb{P}^1) \to \mathbb{Z}$ defined by $D \mapsto \deg(D)$ has kernel = Img(div). This induces an isomorphism from $\mathrm{Pic}(\mathbb{P}^1)$ to $\mathbb{Z}$. We have the following exact sequence

$$1 \longrightarrow \overline{K}^* \longrightarrow \overline{K}(C)^* \xrightarrow{\mathrm{div}} \mathrm{Div}(C) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 1$$

Example A.24 (Elliptic Curve)**.** Consider the curve $C: y^2 = (x-e_1)(x-e_2)(x-e_3)$ where $e_1, e_2, e_3 \in K$ are distinct. If $Char(K) \neq 2$, then this forms a smooth curve in $\mathbb{P}^2$ with the point $P_\infty = [0,1,0]$ at infinity. Let $P_i = [e_i, 0, 1]$ for $i = 1, 2, 3$. We have $M_{P_i} = \langle x - e_i, y \rangle$ by which $y^2 \in M_{P_i}^2$. As $y^2 = (x-e_i)\prod_{i \neq j}(x-e_j)$ we have

$$(x-e_i) = y^2 \prod_{i \neq j}(x-e_j)^{-1} \in M_{P_i}^2$$

as $(x-e_j)$ is a unit in $\mathcal{O}_{P_i}$ for $i \neq j$. Hence the vector space $M_{P_i}/M_{P_i}^2$ is generated by y, implying $M_{P_i} = (y)$. We therefore have $\mathrm{ord}_{P_i}(x-e_j) = 2\delta_{ij}$. The point $[0,1,0]$ at infinity lies on zero set of $x - e_i$ as this is equivalent to $X - e_i Z$. When we look locally in the open set $Y \neq 0$, we see that by a similar argument $\mathrm{ord}_{P_\infty}(x-e_i) = -2$. This also follows from the fact that $\deg(\mathrm{div}(x-e_i)) = 0$. Summarizing the results we get

$$\mathrm{div}(x-e_i) = 2(P_i) - 2(P_\infty)$$

Similarly,

$$\mathrm{div}(y) = (P_1) + (P_2) + (P_3) - 3(P_\infty).$$

III Derivations

Let K be a function field of one variable over an algebraically closed field k (a finitely generated k-algebra of transcendence degree 1) and E be a K-vector space.

Definition A.25. A derivation of K into E is a map $D : K \to E$ satisfying the properties
(a) $D(f+g) = Df + Dg$.
(b) $D(fg) = f(Dg) + g(Df)$
(c) $Da = 0$ for $a \in k$
We denote the K-vector space of derivations of K into E as $\mathrm{Der}_k(K, E)$.

Note that the above properties imply that a derivation $D \in \mathrm{Der}_k(K, E)$ is also a k-linear map.

Example A.26. Let $K = k(x)$ be a rational field, we see that $\mathrm{Der}_k(K, E)$ is isomorphic to E as follows. Consider the map $\phi : \mathrm{Der}_k(K, E) \to E$ defined by

$$\phi(D) = D(x).$$

This map is linear and if $D \in \mathrm{Ker}(\phi)$ then $D(x) = 0$. This implies $D(f) = 0$ for any $f \in k(x)$ from the properties of derivation. Hence $\mathrm{Ker}(\phi) = 0$. ϕ is also a surjection as for any $e \in E$, we can define $D(x) = e$ and extend it to a derivation on K using the above properties.

Now let us look at derivations of extensions of K. The following theorem says that there is a unique 'lift' of a derivation of K to a derivation of L when the latter is a finite separable extension of K.

Theorem A.27. *Let L be a finite separable extension of K. Then the restriction map $\mathrm{Der}_k(L, E) \longrightarrow \mathrm{Der}_k(K, E)$ is a bijection, and hence an isomorphism.*

Proof. As $L|K$ is finite separable, it is a simple extension. Let $y \in L$ be such that $L = K(y)$. First let's prove the uniqueness of lifts. Say, there are two derivations D_1, D_2 of L which when restricted to K give $D \in \mathrm{Der}_k(K, E)$.

let $P(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \in K[x]$ be the minimal polynomial of y over K. We see that

$$D_1(P(y)) = \sum_{i=0}^{n-1} D_1(a_i y^i) + D_1(y^n) = D_1(y)P'(y) + P^D(y) = 0$$

where $P^D(y) = \sum_{i=0}^{n-1} D(a_i)y^i$. As y is separable, $p'(y) \neq 0$ and hence

$$D_1(y) = -\frac{P^D(y)}{P'(y)}$$

Similarly we get

$$D_2(y) = -\frac{P^D(y)}{P'(y)} = D_1(y)$$

Hence $D_1 = D_2$.

The existence of such a derivation can be shown by taking $D_1(y) = -P^D(y)/P'(y)$ and extending it to $K(y)$ gives a derivation that extends D. □

This has interesting corollaries.

Corollary A.28. If there exists $y \in K$ such that $K/k(y)$ is finite separable then $\mathrm{Der}_k(K, E)$ is isomorphic to E as a K vector space.

Proof. From the above theorem we get $\mathrm{Der}_k(K, E) \cong \mathrm{Der}_k(k(y), E)$. The latter is again isomorphic to E from Example A.26. The explicit isomorphism is the following map

$$D \in \mathrm{Der}_k(K, E) \longrightarrow D|_{k(y)} \longrightarrow D(y) \in E$$

□

Corollary A.29. Assume the Hypothesis of Corollary A.28. If $f, g \in K$ and $g \notin k$, then for any two derivations $D_1, D_2 \in \mathrm{Der}_k(K, K)(= \mathrm{Der}_k(K))$ we have

$$\frac{D_1(f)}{D_1(g)} = \frac{D_2(f)}{D_2(g)}$$

Proof. From Corollary A.28, we know that $\mathrm{Der}_k(K, K)$ is a 1 dimensional vector space over K. Hence, any two derivations D_1, D_2 are such that $D_1 = aD_2$ for $a \in K$. This implies

$$\frac{D_1(f)}{D_1(g)} = \frac{aD_2(f)}{aD_2(g)} = \frac{D_2(f)}{D_2(g)}$$

□

IV Differentials

Definition A.30. The dual space of $\mathrm{Der}_k(K, E)$ is defined to be the space of E-valued differentials, denoted by $\mathrm{Diff}_k(K, E)$

Assume K as in Corollary A.28 and $E = K$, then $\mathrm{Diff}_k(K, K) = \mathrm{Diff}_k(K)$ is a 1 dimensional K-vector space. The elements of $\mathrm{Diff}_k(K)$ are called as *differential* 1 *forms* on K. For an element $f \in K$ we can define a differential 1 form $df : \mathrm{Der}_k(K) \longrightarrow K$ defined by

$$df(D) = D(f)$$

This in turn gives us a mapping $d : K \to \mathrm{Diff}_k(K)$ defined by $f \mapsto df$. The map d is not sujective as it is only k-linear and not K-linear and one can easily verify that d is a derivation.

Let $f, g \in K$ and $g \notin k$, then

$$\frac{df}{dg}(D) := \frac{df(D)}{dg(D)} = \frac{D(f)}{D(g)} = \text{Constant}$$

Let us denote $D_g(f)$ for $D(f)/D(g)$.

let x be a transcendental element over k and let $K = k(x)$. Consider $f(x) = a_0 + a_1x + \cdots + a_nx^n \in k[x] \subseteq K$. We see that

$$\frac{df}{dx}(D) = a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

This is the usual derivative $f'(x)$ of f wrt x. This can be extended to whole of K, meaning, for $h = f/g \in K$ where $f, g \in k[x]$. Hence,

$$\frac{dh}{dx}(D) = D_x(f/g) = \frac{gD(f) - fD(g)}{g^2D(x)} = \frac{gf'(x) - fg'(x)}{g^2} = h'(x)$$

A differential of the form df is called as an *exact* differential and the space of exact differentials $d(K)$ forms a k-subspace of $\mathrm{Diff}_k(K)$.

IV.1 Differentials on Curves

Let K be a field and $\overline{K}$ be a fixed algebraic closure of K. Given a curve C over K, we have the associated function field $\overline{K}(C)$. Consider the following two lemmas.

Lemma A.31. *Let C be a curve over K, P be a smooth point on C and $t = t_P$ be a uniformisor at P. Then $K(C)$ is a finite separable extension of $K(t)$.*

Proof. cf. [Sil06], Proposition II.1.4. □

Lemma A.32. *There exists a non singular point on any variety. In particular, this holds for a curve.*

Proof. According to [Har77], Theorem I.5.3, the set of singular points of a variety Y form a *proper closed subset* of Y. □

We see that $\overline{K}(C)$ satisfies the hypothesis of Corollary A.28. Hence the space of differential 1 forms, denoted by $\Omega(C)$, on $\overline{K}(C)$ is a 1 dimensional $\overline{K}(C)$ vector space.

Let C_1, C_2be two curves and $\phi : C_1 \to C_2$ be a rational map. This induces a $\overline{K}$-algebra homomorphism $\phi^* : \overline{K}(C_2) \to \overline{K}(C_1)$ defined by $\phi^*(f) = f \circ \phi$. Recall that ϕ is said to *separable* if $\overline{K}(C_1)$ is a separable extension of $\phi^*(\overline{K}(C_2))$.

Remark A.33. In defining ϕ^*, we are identifying $\overline{K}(C)$ with the set of non constant rational maps $C \to \mathbb{P}^1$ defined over $\overline{K}$.

ϕ^* induces a $\overline{K}(C)$ linear map $\phi^* : \Omega(C_2) \to \Omega(C_1)$ defined by $\phi^*(df) = d(\phi^* f)$. This method in general is known as push forwards of differentials.

Theorem A.34. *(a) dx is a basis for $\Omega(C)$ if and only if $\overline{K}(C)$ is a finite separable extension of $\overline{K}(x)$.*

(b) ϕ is separable if and only if $\phi^* : \Omega(C_2) \to \Omega(C_1)$ is injective.

Proof. cf. [Sil06], §II, Proposition 4.2. □

Before looking at more properties of the differential, let us consider a remark which will be used in the proof of the next proposition.

Remark A.35. We see that for a uniformisor $t \in \mathcal{O}_P$ and an $f \in \mathcal{O}_P$, we can attach a formal power series to f in t. That is, we have a $\overline{K}$ linear map $T : \mathcal{O}_P \to \overline{K}[[t]]$ defined by $T(f) = a_0 + a_1 t + a_2 t^2 + \cdots$, where $a_0 = f(P)$, $a_1 = (f - a_0)t^{-1}(P), \ldots$, so on. This map can then be extended to an embedding $T : \overline{K}(C) \to \overline{K}((t))$ of $\overline{K}(C)$, where $\overline{K}((t))$ is the field of Laurent series in t. We have the following extensions of fields $\overline{K}(t) \subseteq T(\overline{K}(C)) \subseteq \overline{K}((t))$, where the first extension is finite separable.

Proposition A.36 (cf. [Sil06], Proposition II.4.3.)**.** *Let C be a curve, P be a smooth point and $t = t_P$ be a uniformiser at P.*

(a) For an $\omega \in \Omega(C)$, there exists a unique function $g \in \overline{K}(C)$ such that

$$\omega = g dt$$

(b) If $f \in \mathcal{O}_P$, then $df/dt = D_t(f) \in \mathcal{O}_P$.

Proof. (a) The existence of g follows from Lemma A.31 and the fact that $\Omega(C)$ is a 1 dimensional $\overline{K}(C)$ vector space. This expression is unique as dt is a basis from Theorem A.34.

(b) cf. II.3.10, [Rob72].

□

Corollary A.37. If t, s are two uniformisers for $\mathcal{O}_P$, then $\mathrm{ord}_P(dt/ds) = 0$.

Proof. As dt/ds and ds/dt are both in $\mathcal{O}_P$, we have $\mathrm{ord}_P(dt/ds) = 0$ □

Corollary A.38. Let t be a uniformisor for $\mathcal{O}_P$. For $\omega = f dt \in \Omega(C)$, the quantity $\mathrm{ord}_P(f)$ is independent of the uniformiser.

Proof. If $\omega = f dt = g ds$, where t, s are uniformisers for $\mathcal{O}_P$. Taking orders both sides, we have $\mathrm{ord}_P(f) = \mathrm{ord}_P(g)$. □

Definition A.39. Let P be a smooth point and t be a uniformisor at P. The order of a differential $\omega = fdt$ is defined to be $\mathrm{ord}_P(f)$ and is denoted by $\mathrm{ord}_P(\omega)$.

Proposition A.40. *Let $f, x \in \overline{K}(C)$ and $x(P) = 0$, let $p = \mathrm{Char}K$. Then we have*

$$\begin{aligned} \mathrm{ord}_P(fdx) &= \mathrm{ord}_P(f) + \mathrm{ord}_P(x) - 1 \quad \textit{when } p = 0 \textit{ or } p \not| \mathrm{ord}_P(x) \\ \mathrm{ord}_P(fdx) &\geq \mathrm{ord}_P(f) + \mathrm{ord}_P(x) \quad \textit{when } p > 0 \textit{ and } p | \mathrm{ord}_P(x) \end{aligned}$$

V Ramification of Maps

Consider two curves C_1 and C_2 defined over K, and a non-constant rational map $\phi : C_1 \to C_2$. We have the induced map injective $\phi^* : K(C_2) \to K(C_1)$ defined by $f \mapsto f \circ \phi$.

Definition A.41. Let C_1 and C_2 be two smooth curves. The ramification index of the map $\phi : C_1 \to C_2$ at the point $P \in C_1$, denoted by $e_\phi(P)$, is defined by

$$e_\phi(P) = \mathrm{ord}_P(\phi^*(t_{\phi(P)}))$$

where $t_{\phi(P)}$ is a uniformiser at $\phi(P)$. If $e_\phi(P) > 1$, then we say that ϕ *ramifies* at P. Otherwise, we say it is *unramified*.

Example A.42. Let $C_2 = \mathbb{P}^1$ and $C_1 : X^2 + Y^2 = Z^2$. Consider the rational map $\phi : C_1 \to \mathbb{P}^1$ defined by

$$\phi[X, Y, Z] = [X, Y].$$

It is seen that ϕ is well defined and is a rational map. Let us try to calculate the ramification index of ϕ at $P_1 = [1, 0, 1] \in C_1$. A uniformiser at $\phi(P_1) = [1, 0]$ is Y and

$$\phi^*(Y) = Y \circ \phi : [X, Y, Z] \mapsto [X, Y] \mapsto Y.$$

As Y is a uniformiser at P_1, $e_\phi(P_1) = 1$. Let $P_2 = [-1, 0, 1]$, even now we have $\phi(P_2) = [1, 0]$ and $e_\phi(P_2) = 1$. Consider a point at infinity $P_\infty = [i, 1, 0]$, then $\phi(P_\infty) = [i, 1]$, $t_{\phi(P_\infty)} = X - iY$ and

$$\phi^*(X - iY) : [X, Y, Z] \mapsto X - iY.$$

A uniformiser at P_∞ can be seen to be Z and hence, as

$$X - iY = \frac{Z^2}{X + iY},$$

$e_\phi(P_\infty) = 2$.

We see that in the above example, for $Q \in \mathbb{P}^1$ we have

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = 2.$$

This is a special case of the below proposition.

Proposition A.43. *Let $\phi : C_1 \to C_2$ be a rational map between smooth curves. Define the* degree *of ϕ, denoted as* $\deg(\phi)$*, to be the dimension of $\overline{K}(C_1)$ over $\phi^*(\overline{K}(C_2))$. For $Q \in C_2$, we have*

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi).$$

V.1 Ramification of elements from $\overline{K}(C)$

An element $f \in \overline{K}(C)$ can be thought of as a rational map $f : C \to \mathbb{P}^1$ defined by

$$f(P) = \begin{cases} [f(P), 1] & \text{if } f \text{ is regular at } P, \\ [1, 0] & \text{otherwise.} \end{cases}$$

We see that the ramification index of f at P is

$$e_f(P) = \operatorname{ord}_P(f - f(P))$$

So if we assume that $f : C \to \mathbb{P}^1$ ramifies at finitely many points, we get $f - f(P)$ to be a uniformiser at all points P except for finitely many. The excluded points are the poles of f and the points at which f ramifies. In fact, it is true that f ramifies at only finitely many points, so we state this as a lemma below.

Lemma A.44. *For $f \in \overline{K}(C)^*$, the map $f : C \to \mathbb{P}^1$ ramifies at finitely many points. Moreover, $f - f(P)$ is a uniformiser at all regular points except for finitely many.*

Proposition A.45. *Let $\omega \neq 0 \in \Omega(C)$. Then*

$$\operatorname{ord}_P(\omega) = 0$$

for all but finitely many $P \in C$.

By the above proposition we can attach a divisor to a differential $\omega \in \Omega(C)$ as follows.

$$\operatorname{div}(\omega) = \sum_{P \in C} \operatorname{ord}_P(\omega)(P).$$

A divisor of this form is called a *canonical divisor*. For any two differentials $\omega_1, \omega_2 \in \Omega(C)$ we have an $f \in \overline{K}(C)^*$ such that $\omega_1 = f\omega_2$ and hence

$$\operatorname{div}(\omega_1) = \operatorname{div}(f) + \operatorname{div}(\omega_2)$$

So we see that $\deg(\operatorname{div}(\omega_1)) = \deg(\operatorname{div}(\omega_2))$.

Definition A.46. A differential $\omega \in \Omega(C)$ is said to be holomorphic if $\operatorname{ord}_P(\omega) \geq 0$ for all $P \in C$.

Example A.47 (Elliptic Curves)**.** Consider the curve

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3) = f(x)$$

with the point $P_\infty = [0, 1, 0]$ at infinity and let $P_i = [e_i, 0, 1]$, as before, for $i = 1, 2, 3$. Let us consider the map

$$x = \frac{X}{Z} : C \longrightarrow \mathbb{P}^1.$$

For a point $P = [a, b, 1] \neq P_i$ we see that $(x - a)$ is a uniformiser and hence $\operatorname{ord}_P(dx) = \operatorname{ord}_P(d(x - a)) = 0$. At P_i, we know that y is a uniformiser and $\operatorname{ord}_{P_i}(dx) = 1$ as

$$dx = \frac{2y}{f'(x)} dy.$$

At P_∞, we have X/Y to be a uniformiser and we see that

$$\operatorname{ord}_{P_\infty}(x) = \operatorname{ord}_{P_\infty}(X/Z) = \operatorname{ord}_{P_\infty}(X/Y) - \operatorname{ord}_{P_\infty}(Z/Y) = -2$$

and hence we get $\operatorname{ord}_{P_\infty}(dx) = -3$. So we have

$$\operatorname{div}(dx) = (P_1) + (P_2) + (P_3) - 3(P_\infty) = \operatorname{div}(y).$$

Therefore, we have that dx/y is a holomorphic differential form on C.

VI Galois Theory of Elliptic Function Fields

By an *elliptic function field*, we mean the function field of an elliptic curve. Consider a non-constant isogeny $\phi : E_1 \to E_2$ between two elliptic curves. This induces the field extensions

$$\begin{array}{c} \overline{K}(E_1) \\ \big| \text{ Purely inseparable} \\ \mathbf{F} \\ \big| \text{ separable} \\ \phi^*(\overline{K}(E_2)) \end{array}$$

where $\deg_s(\phi) = [\mathbf{F} : \phi^*(\overline{K}(E_2))]$ and $\deg_i(\phi) = [\overline{K}(E_1) : \mathbf{F}]$.

Theorem A.48. *Let $\phi : E_1 \to E_2$ be a non-constant isogeny.*

(*a*) *For every $Q \in E_2$,*
$$\#\phi^{-1}\{Q\} = \deg_s(\phi).$$

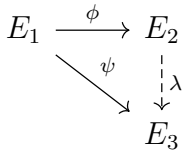
(*b*) *For all $P \in E_1$,*
$$e_\phi(P) = \deg_i(\phi).$$

(*c*) *Let $T_P : E_1 \to E_1$ denote the translation-by-P map. The map*
$$\ker\phi \longrightarrow \mathrm{Aut}(\overline{K}(E_1)/\phi^*(\overline{K}(E_2)))$$
defined by $P \mapsto T_P^*$ is an isomorphism.

(*d*) *If ϕ is separable, then $\#\ker\phi = \deg(\phi)$ and $\overline{K}(E_1)$ is a Galois extension of $\phi^*(\overline{K}(E_2))$.*

Proof. cf. [Sil06], Chapter III, Theorem 4.1. □

Corollary A.49. Let $\phi : E_1 \to E_2$ and $\psi : E_1 \to E_3$ be isogenies such that ϕ is separable. If $\mathrm{Ker}(\phi) \subseteq \mathrm{Ker}(\psi)$, then we have a unique isogeny $\lambda : E_2 \to E_3$ such that the following diagram commutes.



That is, $\lambda \circ \phi = \psi$.

Proof. By Theorem A.48(*d*), we have $\overline{K}(E_1)/\phi^*(\overline{K}(E_2))$ to be a Galois extension and, as $\ker(\phi) \subseteq \ker(\psi)$, we have
$$\mathrm{Aut}(\overline{K}(E_1)/\phi^*(\overline{K}(E_2))) \subseteq \mathrm{Aut}(\overline{K}(E_1)/\psi^*(\overline{K}(E_3))).$$
From this, we see that $\psi^*(\overline{K}(E_3)) \subseteq \phi^*(\overline{K}(E_2)) \subseteq \overline{K}(E_1)$. To proceed further, we use the following lemma.

Lemma A.50. *Let C_1, C_2 be curves defined over K. For an injective ring homomorphism $i : K(C_2) \to K(C_1)$, there exists a unique morphism $\lambda : C_1 \to C_2$ such that $\lambda^* = i$.*

From this lemma, as $(\phi^*)^{-1}\psi^* : \overline{K}(E_3) \to \overline{K}(E_2)$ is an injection, we have $\lambda : E_2 \to E_3$ such that

$$\lambda^* = (\phi^*)^{-1}\psi^* \; ; \quad (\lambda \circ \phi)^* = \phi^*\lambda^* = \psi^*.$$

It follows from the next lemma that $\lambda \circ \phi = \psi$. □

Lemma A.51. *Let $\lambda_1, \lambda_2 : C_1 \to C_2$ be two morphisms between smooth curves defined over K. Then, $\lambda_1^* = \lambda_2^*$ implies $\lambda_1 = \lambda_2$.*

Proof. Let $\lambda_1 = [g_0, g_1, g_2]$ and $\lambda_2 = [f_0, f_1, f_2]$ near a point $P \in C_1$. We can, WLOG, assume $g_0(P) \neq 0$. Let $h_i = [X_i, X_0] \in \overline{K}(C_2)$ for $i = 1, 2$, we have

$$[g_i, g_0] = h_i \circ \lambda_1 = h_i \circ \lambda_2 = [f_i, f_0].$$

This implies that

$$f_i = \frac{f_0}{g_0} g_i.$$

Hence, $\lambda_1 = \lambda_2$ as morphisms. □

Appendix B

I ℓ-adic Theory

Let $\mathbb{Q}_\ell$ be the field of ℓ-adic rational numbers.

Definition B.1 (Lie group over $\mathbb{Q}_\ell$)**.** A topological group G is a Lie group if it is a manifold over $\mathbb{Q}_\ell$ and the maps

$$\begin{aligned} m : G \times G \to G, \quad (a, b) \mapsto ab, \\ i : G \to G, \quad a \mapsto a^{-1} \end{aligned}$$

are *locally analytic*.

From the definition, we see that the left-multiplication-by-g map,

$$\ell_g : G \to G, \quad \ell_g(h) = gh$$

and the conjugation-by-g map

$$\tau_g : G \to G, \quad \tau_g(h) = ghg^{-1}$$

are locally analytic. Moreover, they are Lie group isomorphisms.

Definition B.2 (Lie algebra of G)**.** The Lie algebra $\mathfrak{g}$ of G is the $\mathbb{Q}_\ell$-vector space $T_e(G)$, with the Jacobian product,

$$[X_e, Y_e](f) := X_e(Y(f)) - Y_e(X(f)),$$

where $X, Y : G \mapsto T(G)$ are (left invariant) vector fields defined by

$$X_g = T_e\ell_g(X_e), \quad Y_g = T_e\ell_g(Y_e).$$

Let G be an ℓ-adic Lie group, $\mathfrak{g} = (T_e(G), [\cdot, \cdot])$ be its Lie algebra, on which G acts by the *adjoint representation*. Recall the adjoint representation of the Lie group G is the representation

$$\mathrm{Ad} : G \to \mathrm{GL}(\mathfrak{g}),$$

where $\mathrm{Ad}(g) = T_e\tau_g : \mathfrak{g} \xrightarrow{\sim} \mathfrak{g}$.

I.1 M-dimension

For $N \geq 0$, consider $X = (\mathbb{Z}_\ell)^N$. As $\mathbb{Z}_\ell$ is open in $\mathbb{Q}_\ell$, X is an N dimensional manifold over $\mathbb{Q}_\ell$. For $n \geq 0$, we define

$$X_n := X/\ell^n X = (\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)^N \cong (\mathbb{Z}/\ell^n\mathbb{Z})^N.$$

Consider a closed subset Y of X and its image, call it Y_n, under the quotient map $\pi_n : X \to X_n$. We see that $Y = \varprojlim Y_n$, projective limit of compact Hausdorff topological spaces Y_n. We have the commutative diagram,

$$\begin{array}{ccc} Y & \xrightarrow{\pi_n} & Y_n \\ & \searrow^{\pi_m} & \downarrow \\ & & Y_m \end{array}$$

for all m, n. This induces a continuous map $\pi = (\pi_n) : Y \to \varprojlim Y_n$. The injectivity follows from definition. Let $(y_n) \in \varprojlim Y_n$, we have a sequence $(s_n) \in Y$ such that $\pi_n(s_n) = y_n$. Also, as $\varprojlim Y_n \subseteq \varprojlim X_n \cong X$, we have an $x \in X$ such that $\pi_n(x) = y_n$ for all n. Therefore, $x - s_n \in \ell^n X$ for all n. As $\{\ell^n X\}_n$ forms a collection of basic neighbourhood around 0, we have $s_n \to x$ as $n \to \infty$, implying that $x \in Y$.

As $Y_n \subseteq X_n$, we have $|Y_n| \leq |X_n| = \ell^{nN}$.

Definition B.3. We define the M-dimension of a closed subset Y of X, denoted $\dim_M Y$, as

$$\dim_M Y = \inf\{d \geq 0 \mid |Y_n| = O(\ell^{dN}) \text{ for all } n\}. \tag{B.1}$$

Theorem 3.9 is for closed subsets C of certain M-dimension. We now see a proposition, which helps us weaken the hypothesis in the Theorem.

Proposition B.4 (cf. §3, Theorem 8, [Ser81])**.** *If C is a closed submanifold of an ℓ-adic manifold X of dimension d, then* $\dim_M C \leq d$.

II Galois representations

A good reference for this section is [Bel08].

Let K be a number field.

Definition B.5. Let k be a topological field and $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of the field K. A *Galois representation* of G_K is a continuous group homomorphism

$$\rho : G_K \longrightarrow \mathrm{GL}_n(k).$$

Note that G_K has the *Krull topology* and $\mathrm{GL}_n(k)$ has the induced topology from k. Galois representations usually arise when we have an action of the absolute Galois group on a vector space over k. We will work with $k = \mathbb{Q}_\ell$.

Let us recall a bit of valuation theory. For a prime $\mathfrak{p}$ in $\mathcal{O}_K$, we have a prime $\overline{\mathfrak{p}}$ in $\mathcal{O}_{\overline{K}}$ such that $\overline{\mathfrak{p}} \cap K = \mathfrak{p}$.

$$D_{\mathfrak{p}}(\overline{K}) = \{\sigma \in G_K \mid \sigma\overline{\mathfrak{p}} = \overline{\mathfrak{p}}\} \qquad \text{(Decomposition Group)} \quad \text{(B.2)}$$

$$I_{\mathfrak{p}}(\overline{K}) = \{\sigma \in G_K \mid \sigma(x) - x \in \overline{\mathfrak{p}} \text{ for all } x \in \mathcal{O}_{\overline{K}}\} \text{ (Inertia Group).} \quad \text{(B.3)}$$

That is, we have the exact sequence

$$1 \longrightarrow I_{\mathfrak{p}}(\overline{K}) \longrightarrow D_{\mathfrak{p}}(\overline{K}) \longrightarrow \mathrm{Gal}(\overline{\mathbb{F}_{\mathfrak{p}}}/\mathbb{F}_{\mathfrak{p}}) \longrightarrow 1,$$

where $\mathbb{F}_{\mathfrak{p}}$ is the field with $\mathrm{N}\mathfrak{p}$ elements.

If $v = v_{\mathfrak{p}}$ is the valuation wrt $\mathfrak{p}$ and K_v is the completion of K wrt v, then $D_{\mathfrak{p}}(\overline{K}) \cong \mathrm{Gal}(\overline{K}_v/K_v)$ and $I_{\mathfrak{p}}(\overline{K}) \cong \mathrm{Gal}(\overline{K}_v/\overline{K}_{ur})$, where $\overline{K}_{ur}$ is the maximal unramified extension of K in $\overline{K}$. The isomorphism is induced by the inclusion map,

$$\mathrm{Gal}(\overline{K}_v/K_v) \hookrightarrow \mathrm{Gal}(\overline{K}/K), \quad \sigma \mapsto i \circ \sigma \circ i^{-1},$$

where $i : \overline{K} \hookrightarrow \overline{K}_v$ is the inclusion induced by $\overline{\mathfrak{p}}$.

Remark B.6. The decomposition group and the inertia group are well defined up to conjugacy, as they depend on the prime $\overline{\mathfrak{p}}$ in $\mathcal{O}_{\overline{K}}$ which lies above $\mathfrak{p}$. In the definitions to follow, we see that they are same up to conjugacy. i.e. That definitions doesn't depend on the decomposition group we choose.

Definition B.7. A representation $\phi : G_K \to \mathrm{GL}_n(k)$ is said to be *unramified* at prime $\mathfrak{p}$ if it acts trivially on the inertia group $I_{\mathfrak{p}}(\overline{K})$. i.e.

$$\phi(I_{\mathfrak{p}}(\overline{K})) = 1.$$

For an prime $\mathfrak{p}$ where ϕ is unramified, we can talk about the image of the Frobenius substitution $\sigma_{\mathfrak{p}}$ (also denoted $\mathrm{Frob}_{\mathfrak{p}}$).

Remark B.8. Say we have a Galois representation $\phi : G_K \to \mathrm{GL}_n(k)$ which is unramified at a prime $\mathfrak{p}$. By continuity of ϕ, $\ker\phi$ is a closed normal subgroup of G_K. By infinite Galois theory, we have a Galois extension L/K such that $\ker\phi = \mathrm{Gal}(\overline{K}/L)$. As ϕ is unramified at $\mathfrak{p}$, we have $I_{\mathfrak{p}}(\overline{K}) \subseteq \mathrm{Gal}(\overline{K}/L)$, implying that $L \subseteq \overline{K}_{ur}$. As the latter is unramifed at $\mathfrak{p}$, L is also unramified at $\mathfrak{p}$.

Moreover, if L is unramifed at $\mathfrak{p}$, then, by a similar argument as above, $I_{\mathfrak{p}}(\overline{K}) \in \ker\phi$. i.e. ϕ is unramified at $\mathfrak{p}$.

To summarise, if L is the fixed field of $\ker\phi$, we have a bijection between the sets

$$\begin{array}{c}\{\text{primes at which } \phi \text{ is unramified }\}\\ \updownarrow \\ \{\text{primes at which } L \text{ is unramified }\}\end{array}$$

III Dirichlet Characters and their Conductors

A *Dirichlet character* χ mod N is an arithmetical function induced by a character (1-dim representation) χ on $(\mathbb{Z}/N\mathbb{Z})^*$. We can talk about the Dirichlet series $L(s,\chi)$ attached to a Dirichlet character χ.

Examples B.9.

(i) If $N=1$, then there is only one Dirichlet character, which maps every n to 1, mod 1. The Dirichlet series attached to this is the *Riemann zeta function.*

(ii) If $N=3$, and we have the character $\chi:\{\overline{1},\overline{2}\}\to\{\pm 1\}$, the induced Dirichlet character is,

$$\chi(n)=\begin{cases}0 & \text{if } 3|n,\\ 1 & \text{if } 3|n-1,\ (n\equiv 1)\\ -1 & \text{if } 3|n-2.\ (n\equiv 2)\end{cases}$$

The Dirichlet series attached to this is

$$L(s,\chi)=\sum_{n\equiv 1} n^{-s}-\sum_{n\equiv 2} n^{-s}.$$

III.1 Primitive Characters

Let χ_N mod N be a character and M be a multiple of N. We define a character χ_M mod M *induced* by χ_N, as $\chi_M(a)=\chi_N(a)$. The well-definedness follows as $a\equiv b \bmod M$ implies $a\equiv b \bmod N$. We see that, if χ_M is induced by χ_N, then $\chi_M(a)=\chi_M(b)$ implies that $\chi_N(a-b)=0$, i.e. there is a divisor d, *induced modulus* of χ, of N such that $a\equiv b \bmod d$. In particular, it holds for $d=N$.

Definition B.10. A character χ mod M is said to be *primitive* if the smallest induced modulus is M.

Two characters $\chi_1 \bmod N_1$ and $\chi_2 \bmod N_2$ are said to be *co-trained* if there exists an N such that, $N_1, N_2 | N$ and

$$\chi_1(n) = \chi_2(n) \quad \text{for all } (n, N) = 1.$$

This is equivalent to saying that there exists a character $\chi \bmod N$ induced by both χ_1 and χ_2. The co-trained relation between two characters is an equivalence relation on the set of characters.

Proposition B.11. *Two characters are co-trained if and only if they are induced by a character.*

Proof. Let $\chi_1 \bmod N_1$ and $\chi_2 \bmod N_2$ be characters, $\chi_D \bmod D$ be a character induces them. We have $\chi_1(a) = \chi_D(a)$ for $(a, N_1) = 1$, and $\chi_2(a) = \chi_D(a)$ for $(a, N_2) = 1$. Let $N = N_1 N_2$, we have $\chi_1(n) = \chi_2(n) = \chi_D(n)$ for $(n, N) = 1$.

Let χ_N be induced by χ_1 and χ_2. Let D be the smallest number such that $\chi_N(a) = 1$ when $a \equiv 1 \bmod D$. The character χ_D defined by $\chi_D(a) = \chi_N(a)$ induces χ_1 and χ_2. □

Definition B.12. The *conductor* of a character ω is the least modulus of a character in the equivalence class of ω.

By definition, the character with this least modulus is primitive.

Examples B.13. The character χ in Example (ii) is primitive, hence its conductor is 3.

BIBLIOGRAPHY

[Bel08] Joel Bellaiche, *Galois representations*, Notes (2008).

[DS10] F. Diamond and J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, Springer New York, 2010.

[Har77] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag New York, 1977.

[HL14] G. H. Hardy and J. E. Littlewood, *Tauberian theorems concerning power series and dirichlet's series whose coefficients are positive*, Proceedings of the London Mathematical Society **s2-13** (1914), no. 1, 174–191.

[Miy89] T Miyake, *Modular forms*, Graduate Texts in Mathematics, Springer-Verlag, Berlin, 1989.

[Rob72] Alian Robert, *Elliptic curves*, Lecture Notes in Mathematics, Springer Berlin Heidelberg, 1972.

[Ser81] Jean-Pierre Serre, *Quelques applications du théorème de densité de chebotarev*, Publications Mathématiques de l'IHÉS **54** (1981), 123–201 (fr). MR 83k:12011

[Ser98] ———, *Abelian ℓ-adic representations and elliptic curves*, Research Notes in Mathematics (A K Peters), Vol 7, Peters, 1998.

[SGS07] W. A. Stein, P. E. Gunnells, and American Mathematical Society, *Modular forms, a computational approach*, Graduate studies in mathematics, American Mathematical Society, 2007.

[Sil06] Joseph H Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer Verlag New York, 2006.

[Sta74] H. M. Stark, *Some effective cases of the brauer-siegel theorem*, Inventiones mathematicae **23** (1974), no. 2, 135–152.

[Wir61] Eduard Wirsing, *Das asymptotische verhalten von summen über multiplikative funktionen*, Mathematische Annalen **143** (1961), no. 1, 75–102.